HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration Guide HiLCOS
Rel. 10.34

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2025 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You can get the latest version of this manual on the Internet at:
https://www.doc.hirschmann.com

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany

Contents

Safety instructions 24

Copyright of Integrated Software 25

Related Documents 27

Key 29

1 Device Roles 31

1.1 Access Point 33
1.2 WLAN Bridge (point-to-point) 34
1.3 WLAN Bridge Relay 36
1.4 WLAN Distribution Point - (Point-to-Multipoint) 37
1.5 WLAN Client 38
1.6 WLAN Roaming Clients 39

2 Configuration Tools 41

2.1 Startup Behavior 43
2.1.1 Factory-Default Network-Exposed Services 43
2.2 Online versus Offline Configuration 44
2.3 Downloading the Configuration File 45

3 Configuring the Device 47

3.1 Creating a Configuration File 48

3.2 Access Point for Multiple Wireless Clients 51
- 3.2.1 Creating a New Configuration File 52
- 3.2.2 Configuring Basic Settings 55
- 3.2.3 Configuring Wireless LAN Settings 63

3.3 Access Point & DHCP Server for Multiple Wireless Clients 82
- 3.3.1 Creating a New Configuration File 83
- 3.3.2 Changing the Existing Network to a Wired LAN 83
- 3.3.3 Create a New DHCP Wireless LAN 86

3.4 Wireless Client 89
- 3.4.1 Creating a New LANconfig File for a Client 89
- 3.4.2 Configuring Basic Settings 92
- 3.4.3 Configuring Wireless LAN Settings 98

3.5 WLAN Bridge: Single Subnet 109
- 3.5.1 Configuring the LEFT Device 109
- 3.5.2 Configuring the RIGHT Device 136

3.6 WLAN Bridge: Two Subnets 146
- 3.6.1 Creating Two LANconfig Files 147
- 3.6.2 Creating Two Transfer Network Entries 149
- 3.6.3 Routing the Transfer Networks 154

3.7 WLAN Bridge Relay: 1 Radio 159
- 3.7.1 Creating Three LANconfig Files 160
- 3.7.2 Configure the LEFT Device 165
- 3.7.3 Configure the MIDDLE Device 171
- 3.7.4 Configure the RIGHT Device 176

3.8 WLAN Bridge Relay: 2 Radios 181
- 3.8.1 Creating Three LANconfig Files 182
- 3.8.2 Configuring the MIDDLE Device 183
- 3.8.3 Configuring the LEFT Device 195
- 3.8.4 Configuring the RIGHT Device 198

3.9 Manual configuration of P2P connections 201

4 Configuring WLAN Parameters 205

4.1 General WLAN Settings 206
4.1.1 WLAN band steering 207
4.1.2 Adaptive noise immunity for reducing interference on the WLAN 210
4.1.3 UUID Information Element for WLAN Access Points 210
4.1.4 PMK Caching in the WLAN Client Mode 212
4.1.5 Advanced ARP handling 212
4.1.6 Pre-authentication in WLAN Client Mode 213
4.1.7 Time-staggered Roaming for Dual-radio Client WLAN Modules 214
4.1.8 Greenfield Mode for Access Points with IEEE 802.11n 215
4.1.9 Maximum EIRP value depends on the transmission standard 217
4.1.10 Automatic adjustment of multicast and broadcast transmission rates 217
4.1.11 Converting DHCP responses from broadcast to unicast 218

4.2 WLAN Security Settings 219
4.2.1 General settings 220
4.2.2 Filter protocols 221

4.3 Controlling WLAN Access 228

4.4 Encryption 230
4.4.1 WPA and Private WEP Settings 231
4.4.2 WEP Group Keys 236
4.4.3 Group key per VLAN 237

4.5 Physical WLAN Interfaces 242
4.5.1 Operation Settings 243
4.5.2 Radio Settings 245
4.5.3 Performance 252
4.5.4 Point-to-Point 253
4.5.5 Client Mode 255

4.6 Point-to-Point Partners 259
4.6.1 Automatic Configuration of WLAN P2P Connections via Serial Interfaces 260

4.7 Logical WLAN Networks 262
4.7.1 Network Settings 262
4.7.2 Transmission Settings 267
4.7.3 STBC / LDPC 271

4.8 Beaconing and Roaming 273
4.8.1 Beaconing 273
4.8.2 Roaming 275
4.9 Device Authentication 279
4.9.1 Authentication via RADIUS 279
4.9.2 Re-Authentication via IEEE 802.1x and EAP 281
4.10 Trace 283
4.11 Redundant connections using PRP 285
4.11.1 Basic function 286
4.11.2 Advantages of WLAN PRP 287
4.11.3 Implementation of PRP in the access points 288
4.11.4 Implementing PRP exclusively over WLAN 289
4.11.5 Smart roaming 289
4.11.6 Diagnostic options 291
4.11.7 Tutorial: Setting up a PRP connection over a point-to-point network (P2P) 291
4.11.8 Tutorial: Roaming with a dual-radio client and PRP 296
4.12 Adjustable rate adaptation algorithm 302
4.12.1 Enhancements in the menu system 302

5 Central WLAN Management 305

5.1 Application Examples 306
5.1.1 Managed Mode 306
5.1.2 WLAN Bridge to Access Point – Managed and Unmanaged Mixed 308

5.2 Introduction 309
5.2.1 The CAPWAP Standard 310
5.2.2 The Smart Controller Technology 310
5.2.3 Communication between Access Point and WLAN-Controller 314
5.2.4 Zero-Touch Management 317
5.2.5 Split Management 317
5.2.6 Inheritance of Parameters 317
5.2.7 Opportunistic key caching (OKC) 319
5.2.8 Fast roaming 320
5.2.9 Hirschmann Active Radio Control (ARC) 322

5.3 Configuration of the WLC 324
5.3.1 General settings 324
5.3.2 Profiles 325
5.3.3 List of Access Points 336
5.3.4 Station Table (ACL Table) 340
5.3.5 Options for the WLAN-Controller 340

5.4 Configuring the Access Points 342

5.5 Managing the Access Points 344
5.5.1 Accepting new Access Points manually into the WLAN structure 344
5.5.2 Removing Access Points manually from the WLAN structure 348
5.5.3 Deactivating or Permanently Removing Access Points from the WLAN Structure 349
5.5.4 Managing the Access Points 350
5.5.5 Backing up the Certificates 351
5.5.6 Saving and Restoring more files of the SCEP-CA 353

5.6 Interference Detection in the Frequency Range (Spectral Scan) 356
5.6.1 Functions of the Software Module 357
5.6.2 Starting a Spectral Scan 357
5.6.3 Spectral Scan Analysis Window 361

5.7 Extended WLC Functions 365
5.7.1 Automatic Radio-Field Optimization with Hirschmann WLAN-Controllers 365
5.7.2 Central Firmware and Script Management 367
5.7.3 Checking WLAN Clients with RADIUS (MAC Filter) 373
5.7.4 Separate RADIUS Server for Each SSID 375
5.7.5 IP-dependent auto configuration of APs 377
5.7.6 Dynamic VLAN Assignment 380
5.7.7 Load Balancing between the WLAN-Controllers 383
5.7.8 WLAN Layer-3 Tunneling 384
5.7.9 Switching off CAPWAP/SCEP in the WLC 387
5.8 Application Examples 388
5.8.1 "Overlay Network": Separating Networks for Access Points without VLAN 388
5.8.2 "Layer-3 Roaming" 395
5.8.3 WLAN Controller with Public Spot 398

6 Public Spot 409

6.1 What is a Public Spot? 410
6.1.1 The solution: (W)LAN technology 410
6.1.2 User authorization and authentication 411
6.1.3 Accounting 412
6.1.4 Logging 412

6.2 Overview of the Public Spot module 414
6.2.1 Open User Authentication (OUA) 414
6.2.2 Security in the (W)LAN 416
6.2.3 Setup wizard for Public Spots 418
6.2.4 Wizard for creating and managing users 418

6.3 Basic configuration 419
6.3.1 Basic installation of a Public Spot for simple scenarios 419
6.3.2 Setting default values for the Public Spot wizard 443
6.3.3 Setting up limited administrator rights for Public Spot managers 446
6.3.4 Setting up and managing Public Spot users for simple scenarios 449

6.4 Security settings 459
6.4.1 Traffic limit option 459
6.4.2 Restricting access to the configuration 461

6.5 Extended functions and settings 462
6.5.1 Multiple logins 463
6.5.2 Open access networks (no login) 465
6.5.3 Managing Public Spot users via the web API 467
6.5.4 Bandwidth profile 474
6.5.5 Clear user list automatically 476
6.5.6 Station monitoring 476
6.5.7 WLAN handover of sessions between devices 478
6.5.8 Authentication via RADIUS 481
6.5.9 Billing without a RADIUS accounting server 484
6.5.10 Billing via RADIUS accounting server 484
6.5.11 Multi-level certificates for PublicSpots 487
6.5.12 Assigning users to individual VLANs 488
6.5.13 Error page in case of WAN connection failure 490

6.6 Alternative login methods 492
6.6.1 Overview of authentication modes 492
6.6.2 Independent user authentication (Smart Ticket) 496

6.6.3 Automatic re-login 508
6.6.4 Automatic authentication with the MAC address 509
6.6.5 Automatic authentication via WISPr 512
6.7 IEEE 802.11u and Hotspot 2.0 517
6.7.1 Hotspot operators and service providers 519
6.7.2 Functional description 519
6.7.3 Recommended general settings 522
6.7.4 Configuration menu for IEEE 802.11u / Hotspot 2.0 523
6.8 XML interface 545
6.8.1 Function 545
6.8.2 Setting up the XML interface 548
6.8.3 Analyzing the XML interface using cURL 550
6.8.4 Commands 551
6.9 Internal and customized voucher and authentication pages (templates) 559
6.9.1 Possible authentication pages 559
6.9.2 Pre-installed default pages 563
6.9.3 Customizing the standard pages 565
6.9.4 Configuration of user-defined pages 569
6.9.5 Setting up a customized template page 572
6.9.6 User-defined pages via HTTP redirect 574
6.9.7 User-defined pages via page templates 575
6.9.8 URL placeholder (template variables) 577
6.9.9 Tags and syntax of page templates 580
6.9.10 Page template identifiers 581
6.9.11 Graphics in user-defined pages 586
6.10 Access to the Public Spot 587
6.10.1 Requirements for logging in 587
6.10.2 Logging in to the Public Spot 589
6.10.3 Session information 590
6.10.4 Logging out of the Public Spot 591
6.10.5 Advice and help 592
6.11 Commonly transmitted RADIUS attributes 595
6.11.1 Messages to/from the authentication server 595
6.11.2 Messages to/from the accounting server 600
6.12 Tutorials for setting up and using Public Spots 605
6.12.1 Setting up an external RADIUS server for user administration 605

6.12.2 Internal and external RADIUS servers combined 608
6.12.3 Checking WLAN clients with RADIUS (MAC filter) 613
6.12.4 Setting up an external SYSLOG server 614

7 Virtual Private Networks – VPN 617

7.1 What are the Benefits of VPN? 618
7.1.1 Private IP Addresses on the Internet? 619
7.1.2 Security of Data Traffic on the Internet? 620

7.2 VPN at a Glance 623
7.2.1 VPN Application Example 623
7.2.2 Functions of VPN 625

7.3 Configuration of VPN Connections 626
7.3.1 VPN Tunnel: Connection between VPN Remote Terminals 626
7.3.2 1-Click VPN for Hirschmann Advanced VPN 628
7.3.3 Client VPN remote access wizard in WEBconfig: 629
7.3.4 Viewing VPN Rules 629
7.3.5 Manually Setting up VPN Connections 631
7.3.6 IKE Config Mode 632
7.3.7 Establishing VPN Network Relationships 634
7.3.8 Collective Establishment of Security Associations 637
7.3.9 VPN Connection Diagnostics 639

7.4 IPSec over HTTPS 640
7.4.1 Introduction 640
7.4.2 Configuring the IPSec over HTTPS Technology 640
7.4.3 Status Displays for IPSec over HTTPS Technology 643

7.5 Use of Digital Certificates 644
7.5.1 Basics 644
7.5.2 Advantages of certificates 652
7.5.3 Structure of certificates 653
7.5.4 Security 655
7.5.5 Certificates in VPN connection setup 656
7.5.6 Certificates from certificate service providers 658
7.5.7 Structure of one's own CA 659
7.5.8 Requesting a certificate with the standalone Windows CA 660
7.5.9 Exporting the certificate to a PKCS#12 file 662
7.5.10 Creating certificates with OpenSSL 665
7.5.11 Loading certificates into the Hirschmann device 668
7.5.12 Backing up and uploading certificates with LANconfig 669
7.5.13 Adjusting VPN connections to certificate support 670
7.5.14 Creating certificate-based VPN connections

for LAN coupling using the Setup Wizard 677
7.5.15 Simplified network connection with certificates – pro-adaptive VPN 679
7.5.16 Requesting certificates by means of CERTREQ 681
7.5.17 Certificate revocation list - CRL 681
7.5.18 Diagnosis of the VPN certificate connections 685
7.6 Multilevel certificates for SSL/TLS 686
7.6.1 Introduction 686
7.6.2 SSL/TLS with multilevel certificates 688
7.6.3 VPN with multilevel certificates 688
7.7 Certificate enrollment via SCEP 689
7.7.1 SCEP server and SCEP client 690
7.7.2 The process sequence of a certificate distribution 690
7.7.3 Configuration of SCEP 693
7.8 Extended Authentication Protocol (XAUTH) 699
7.8.1 Introduction 699
7.8.2 XAUTH in HiLCOS 700
7.8.3 Configuration of XAUTH 700
7.9 How does VPN operate? 703
7.9.1 IPSec – the basis for VPN 703
7.9.2 Alternatives to IPSec 704
7.10 The standards behind IPSec 707
7.10.1 Modules of IPSec and their tasks 707
7.10.2 Security Associations – numbered tunnels 708
7.10.3 Encryption of the packets – the ESP protocol 708
7.10.4 Authentication – the AH protocol 711
7.10.5 Management of the keys – IKE 715
7.11 Improved phase 1 rekeying 717
7.12 Intelligent Precalculation of DH Keys 718
7.13 MPPE encryption for PPTP tunnel 719
7.13.1 Enhancements in the menu system 719

8 Security 721

8.1 A WLAN Security Overview 722
8.1.1 Basic Considerations 722
8.1.2 IEEE 802.11i /WPA2 723
8.1.3 TKIP and WPA 723
8.1.4 WEP 723
8.1.5 LEPS: Hirschmann Enhanced Passphrase 724
8.1.6 Security Background WLAN Scanning 725

8.2 Securing the Configuration 726
8.2.1 Using the Check Security Settings Wizard 726
8.2.2 Passwords 727
8.2.3 Login Barring 729
8.2.4 Restricting Configuration Access Rights 730
8.2.5 Closed-network Function: Suppress SSID broadcast 733
8.2.6 Post-Initial-Password Security Hardening 734

8.3 Automatic generation of device-specific SSH keys 735

8.4 Suppress security confirmations during SSH key generation 736

9 Virtual LANs 737

9.1 What is a Virtual LAN? 738

9.2 Configuring VLANs 739
9.2.1 VLAN and ARF 739
9.2.2 General VLAN Settings 740
9.2.3 The Network Table 741
9.2.4 The Port Table 742

9.3 Configuring VLAN IDs 745
9.3.1 Assigning Different VLAN IDs to WLAN Clients 745
9.3.2 Special VLAN ID for DSL Interfaces 746

9.4 VLAN Tagging on Ethernet Layers 2 and 3 747
9.4.1 Introduction 747
9.4.2 Configuration of VLAN tagging on layer 2/3 748

10 LLDP 751

10.1 How it works 752
10.2 Structure of LLDP Messages 754
10.3 Supported Operating Systems 756
10.4 Configuration 757

11 Routing and WAN Connections 759

11.1 General aspects of WAN connections 760
11.1.1 Bridges for Standard Protocols 760

11.2 IP Routing 762
11.2.1 The Routing Table 762
11.2.2 Policy Based Routing 766
11.2.3 Local Routing 770
11.2.4 Dynamic Routing with IP RIP 771
11.2.5 SYN/ACK Speedup 779

11.3 Advanced Routing and Forwarding 780
11.3.1 Introduction 780
11.3.2 Definition of networks and Assignment of Interfaces 786
11.3.3 Assigning Logical Interfaces to Bridge Groups 787
11.3.4 Interface Tags for Remote Sites 788
11.3.5 Routing tags for DNS forwarding 790
11.3.6 Virtual Routers 794
11.3.7 NetBIOS Proxy 795

11.4 Source tags for firewall rules 797

11.5 Configuring Remote Stations 798
11.5.1 Remote Site (Peer) List 798
11.5.2 Communication Layers List 800

11.6 IP Masquerading 803
11.6.1 Simple Masquerading 803
11.6.2 Inverse Masquerading 806

11.7 Demilitarized Zone (DMZ) 811
11.7.1 Assigning Networks to the DMZ 812
11.7.2 Address Checking 813
11.7.3 Unmasked Internet Access for a Server in the DMZ 813

11.8 N:N Mapping 815
11.8.1 Application Examples 816
11.8.2 Configuring Address Translation 821

11.9 Establishing Connection with PPP 824
11.9.1 The Point-to-Point Protocol (PPP) 824
11.9.2 Checking the Connection with LCP 827
11.9.3 Assignment of IP Addresses via PPP 828
11.9.4 Configuring PPP Negotiation Settings 830

11.9.5 The DEFAULT Remote Site 832
11.9.6 RADIUS authentication of PPP connections 833
11.10 PPPoE Servers 835
11.10.1 Introduction 835
11.10.2 Example Application 836
11.10.3 Configuring PPPoE 839
11.11 DSL Dial-in over PPTP 841
11.12 Keep Alive: Extended Connections for Flat Rates 843
11.13 Revised flow control 844
11.14 Callback Functions 845
11.14.1 Callback for Microsoft CBCP 846
11.14.2 Fast Callback 847
11.14.3 Callback via RFC 1570 (PPP LCP Extensions) 848
11.14.4 Overview of WEBconfig, Terminalprogram and Telnet 848
11.15 Operating a modem over the serial interface 850
11.15.1 System Requirements 851
11.15.2 Installation 851
11.15.3 Configuring the serial interface for modem operation 852
11.15.4 Configuring Modem Parameters 853
11.15.5 Direct Entry of AT Commands 855
11.15.6 Statistics 855
11.15.7 Trace Output 856
11.15.8 Configuring Remote Sites for V.24 WAN Interfaces 857
11.15.9 Configuring a Backup Connection on the Serial Interface 858
11.15.10 Contact Assignment of Modem Connectors 861
11.16 Manual Definition of the MTU 862
11.16.1 Configuring the MTU 862
11.16.2 Statistics 863
11.17 WAN RIP 864
11.18 The Rapid Spanning Tree Protocol 867
11.18.1 Classic and Rapid Spanning Tree 868
11.18.2 RSTP Improvements 869
11.18.3 Configuring the Spanning Tree Protocol 870
11.18.4 Status Reports for Spanning Tree 872

11.19 The Action Table 876
11.19.1 Actions for Dynamic DNS 876
11.19.2 Action Examples 882
11.19.3 Configuring action table entries 885
11.20 Using the LAN Serial Interface 889
11.20.1 Operating Modes 890
11.20.2 Configuring the Serial Interface 890
11.20.3 Configuring the COM Port Server 891
11.20.4 WAN Device Configuration 899
11.20.5 Serial Connection Status Information 900
11.20.6 CPM Port Adapters 904
11.21 IGMP Snooping 905
11.21.1 Introduction 905
11.21.2 IGMP Snooping Operation 907
11.21.3 IGMP snooping through multiple bridges 908
11.21.4 Configuring IGMP Snooping 911
11.21.5 IGMP Status 916

12 Configuring the Firewall 921

12.1 The Device Firewall 922
12.1.1 Tips for Configuring the Firewall 922

12.2 Firewall Configuration: LANconfig 925
12.2.1 General Firewall Parameters 925
12.2.2 Creating a New IPv4 Firewall Filter Rule 930
12.2.3 Firewall filter rule settings and actions 932
12.2.4 Applying firewall rules to FTP and IRC connections 941
12.2.5 Defining Firewall Objects 944

12.3 Configuring the IPv4 Firewall: WEBconfig and Telnet 948
12.3.1 Rules Table 948
12.3.2 Objects Table 949
12.3.3 Action Table 951

12.4 Firewall Diagnosis 952
12.4.1 The Firewall Log Table 952
12.4.2 The Filter List 954
12.4.3 The Connection List 956
12.4.4 Port Block List 957
12.4.5 Host Block List 958

12.5 Firewall Limitations 959

12.6 Combating intrusion attempts Intrusion detection 960
12.6.1 Examples of Break-in Attempts 960
12.6.2 Configuring the IDS 961

12.7 Protection from denial of service attacks 963
12.7.1 Configuring DoS Blocking 963

13 IPv6 967

13.1 IPv6 basics 968
13.1.1 Why Use IPv6-standard IP Addresses? 968
13.1.2 IP Address Structure According to the IPv6 Standard 969
13.1.3 Stages of Migration 970

13.2 IPv6 Tunneling Technologies 971
13.2.1 6in4 Tunneling 971
13.2.2 6rd Tunneling 972
13.2.3 6to4 Tunneling 973

13.3 DHCPv6 975
13.3.1 DHCPv6 Server 975
13.3.2 DHCPv6 Client 976

13.4 IPv4 VPN Tunnel via IPv6 977
13.4.1 Setup Wizard: IPv4 VPN Tunnel via IPv6 Setup 978

13.5 Dual-Stack Lite (DS-Lite) 980

13.6 IPv6 support for RAS services 983

13.7 IPv6 Firewall 986
13.7.1 Function 986
13.7.2 Configuration 986
13.7.3 Default Entries for the IPv6 Firewall Rules 987
13.7.4 IPv6 Firewall Log Table 988

13.8 Additional Command-line Commands 992
13.8.1 IPv6 Addresses 992
13.8.2 IPv6 Prefixes 994
13.8.3 IPv6 Interfaces 994
13.8.4 IPv6 Neighbor Cache 995
13.8.5 IPv6 DHCP Server 996
13.8.6 IPv6 DHCP Client 997
13.8.7 IPv6 Route 997
13.8.8 Release IPv6 Address 998
13.8.9 Overview of Parameters 998

13.9 Enhancements to LANconfig 1000
13.9.1 IPv6 configuration menu 1000
13.9.2 Configuring PPP Negotiation Settings 1023
13.9.3 IP Routing Tables 1025
13.9.4 Separate Views for the IPv4 and IPv6 Firewalls 1027

13.9.5 IPv6 DNS Hosts in the DNS List 1027
13.9.6 Configuring the IPv6 Firewall Rules 1028
13.10 Tutorials 1048
13.10.1 Setting up IPv6 Internet Access 1048
13.10.2 Setting up a 6to4 Tunnel 1061

14 Quality of Service 1073

14.1 QoS Objectives 1074
14.2 Which packets to prioritize? 1075
14.3 Configuration of QoS 1076
14.3.1 Evaluating ToS and DiffServ fields 1076
14.3.2 Granting Minimum Bandwidths 1079
14.3.3 Configuring the send/receive direction 1080
14.3.4 Reducing Packet Length 1081
14.4 QoS for WLANs: IEEE802.11e (WMM/WME) 1084

15 Additional Services 1087

15.1 IP Address Administration via DHCP 1088
15.1.1 Introduction 1088
15.1.2 Configuring DHCP parameters in LANconfig 1090
15.1.3 Configuring DHCP parameters via WEBconfig or Telnet 1097
15.1.4 DHCP Relay Server 1105
15.1.5 Configuring Clients 1107
15.1.6 Checking IP Addresses in the LAN 1108

15.2 Vendor class and User class identifiers 1110

15.3 DNS 1111
15.3.1 DNS Functions 1111
15.3.2 DNS Forwarding 1113
15.3.3 Configuring the DNS Server 1115
15.3.4 URL Blocking 1121
15.3.5 Dynamic DNS 1122

15.4 Setting up an e-mail address to send messages 1125

15.5 Accounting 1128
15.5.1 Configuring General Accounting Parameters 1128
15.5.2 Configuring the Snapshot 1130

15.6 Call Charge Management 1131
15.6.1 Connection limits for DSL and cable modem 1131

15.7 Time Server 1134
15.7.1 Configuring the time server with LANconfig 1134
15.7.2 Configuring the time server with WEBconfig 1136
15.7.3 Configuring NTP Clients 1136

15.8 Scheduled Events 1140
15.8.1 CRON Jobs With Time Delay 1141
15.8.2 Configuring a CRON Job 1141

15.9 RADIUS 1145
15.9.1 How RADIUS Works 1147
15.9.2 Configuring RADIUS as Authenticator or NAS 1148
15.9.3 Configuring the RADIUS Server 1157

15.10 RADSEC 1174
15.10.1 Configuring RADSEC in the OpenBAT device 1174
15.10.2 Certificates for RADSEC 1175

15.11 TACACS+ 1177
15.11.1 Introduction 1177
15.11.2 Configuring TACACS+ 1179
15.11.3 Configuring the TACACS+ Server 1183
15.11.4 Login to the TACACS+ Server 1184
15.11.5 TACACS+ Login via Telnet or SSH 1187
15.11.6 Assigning Rights Under TACACS+ 1188
15.11.7 Authorization Functions 1188
15.12 Login to the HiLCOS administration interface via RADIUS 1191
15.13 Support from TLS 1.1 / 1.2 1196

A Glossary 1197

B Index 1205

C Maintenance 1213

D Further Support 1214

Addendum HiLCOS Rel. 9.00 1216

Addendum HiLCOS Rel. 9.10 1365

Addendum HiLCOS Rel. 9.12 1665

Addendum HiLCOS Rel. 10.12 1674

Addendum HiLCOS Rel. 10.32 2157

Addendum HiLCOS Rel. 10.34 2322

Safety instructions

Important Information

Notice: Read these instructions carefully, and look at the equipment to become familiar with the device before trying to install, operate, or maintain it. The following special messages may appear throughout this documentation or on the equipment to warn of potential hazards or to call attention to information that clarifies or simplifies a procedure.

The addition of this symbol to a Danger or Warning safety label indicates that an electrical hazard exists, which will result in personal injury if the instructions are not followed.

This is the safety alert symbol. It is used to alert you to potential personal injury hazards. Obey all safety messages that follow this symbol to avoid possible injury or death.

⚠ DANGER

DANGER indicates an imminently hazardous situation which, if not avoided, **will result in** death or serious injury.

⚠ WARNING

WARNING indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury.

⚠ CAUTION

CAUTION indicates a potentially hazardous situation which, if not avoided, **can result in** minor or moderate injury.

Copyright of Integrated Software

Open Source Software used in the product

The product contains, among other things, Open Source Software files, as defined below, developed by third parties and licensed under an Open Source Software license. These Open Source Software files are protected by copyright. Your right to use the Open Source Software is governed by the relevant applicable Open Source Software license conditions.
Your compliance with those license conditions will entitle you to use the Open Source Software as foreseen in the relevant license. In the event of conflicts between other Hirschmann Automation and Control GmbH license conditions applicable to the product and the Open Source Software license conditions, the Open Source Software conditions shall prevail. The Open Source Software is provided royalty-free (i.e. no fees are charged for exercising the licensed rights). Open Source Software contained in this product and the respective Open Source Software licenses are stated below.

If Open Source Software contained in this product is licensed under GNU General Public License (GPL), GNU Lesser General Public License (LGPL), Mozilla Public License (MPL) or any other Open Source Software license, which requires that source code is to be made available and such source code is not already delivered together with the product, you can order the corresponding source code of the Open Source Software from Hirschmann Automation and Control GmbH - against payment of the shipping and handling charges - for a period of at least 3 years since purchase of the product. Please send your specific request, within three years of the purchase date of this product, together with the name and ID number of the product to be found at the label of the product to:

Hirschmann Automation and Control GmbH
Head of R&D
Stuttgarter Strasse 45-51
72654 Neckartenzlingen
Germany

Warranty regarding further use of the Open Source Software

Hirschmann Automation and Control GmbH provides no warranty for the Open Source Software contained in this product, if such Open Source Software is used in any manner other than intended by Hirschmann Automation and Control GmbH. The licenses listed below define the warranty, if any, from the authors or licensors of the Open Source Software. Hirschmann Automation and Control GmbH specifically disclaims any warranty for defects caused by altering any Open Source Software or the product's configuration. Any warranty claims against Hirschmann Automation and Control GmbH in the event that the Open Source Software contained in this product infringes the intellectual property rights of a third party are excluded.

The following disclaimer applies to the GPL and LGPL components in relation to the rights holders:

"This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License and the GNU Lesser General Public License for more details."
For the remaining open source components, the liability exclusions of the rights holders in the respective license texts apply.
Technical support, if any, will only be provided for unmodified software.

Software contained in the product

You can find the software components which are part of the product and the applicable license terms in the licenses_HiLCOS_10_34.txt file respectively license folder that is included in the HiLCOS 10.34 software bundle.

Related Documents

Further documentation can be found as PDF files for downloading on the Internet at:
https://www.doc.hirschmann.com

Key

The designations used in this manual have the following meanings:

▶	List
☐	Work step
	Subheading
Link	Cross-reference with link
Note:	A note emphasizes an important fact or draws your attention to a dependency.
`Courier`	ASCII representation in user interface

Execution in the Graphical User Interface (Web-based Interface user interface)

Execution in the Command Line Interface user interface

Symbols used:

	WLAN access point
	Router with firewall
	Switch with firewall
	Router
	Switch
	Bridge

	Hub
	A random computer
	Configuration Computer
	Server
	PLC - Programmable logic controller
	I/O - Robot

1 Device Roles

Wireless local area networks (WLANs) can either extend or replace a traditional cable-based network. In some cases, a wireless LAN provides new application design possibilities, providing streamlined work flows and cost savings.

Note: Graphics displayed in the manual may differ from those displayed on your PC as a consequence of hardware and firmware revisions.

You can use the OpenBAT device in many different roles, depending upon the specific features and the requirements of your network design. These roles include:

- Access Point:
  The OpenBAT device enables Client devices to gain wireless access to a cable-based local area network.
- WLAN Bridge:
  Two OpenBAT devices provide a wireless point-to-point communication link between two typically cable-based LANs.
- WLAN Bridge Relay:
  Two or more dual-radio OpenBAT devices serve as message relay stations, providing a communication link between two typically cable-based LANs.
- WLAN Distribution Point:
  A single master OpenBAT device connects multiple slave Access Points to a central LAN in a point-to-multipoint design.

- WLAN Client:
  A OpenBAT device is designed or configured to serve as Ethernet adapter and provide a wireless communication link to a WLAN Access Point.
- WLAN Roaming Client:
  WLAN clients wirelessly connect one or more mobile units as they move between multiple WLAN access points, providing continuous, dynamic communications.

Each of these roles is briefly described below. The following chapter describes how to configure OpenBAT devices to perform each of these roles.

1.1 Access Point

The OpenBAT device can function as central Access Point, connected to multiple wireless clients. In this application example, a OpenBAT device provides client access to one or more WLANs and regulates:

– each client's rights to access the radio cell
– communications between clients
– access to networks linked to other networks

In larger scale WLAN scenarios (e.g. in companies with facilities extending between several buildings or floors), multiple Access Points can provide WLAN Clients with access to a common, shared network. The clients can roam between the different Access Points, if necessary. Such a design is commonly referred to as campus coverage because this solution has been adopted by a large number of colleges and universities to provide students and staff with network access.

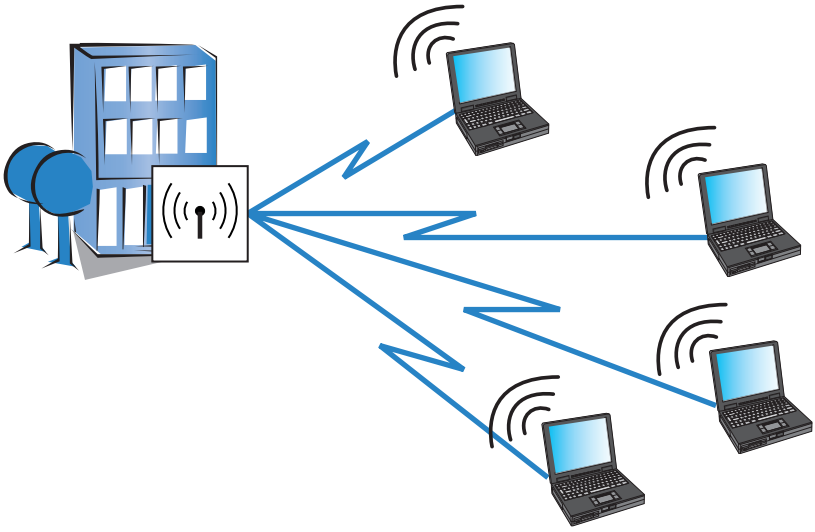


Figure 1: A single access point connected to wireless clients

1.2 WLAN Bridge (point-to-point)

Outdoor WLAN systems are especially useful for providing a point-to-point (P2P) link between two Access Points. This design makes it possible, for example, to easily integrate a remote production building into the company network using two OpenBAT devices.

Figure 2: A wireless link between two access points

You can also use a point-to-point connection to span difficult terrain (such as mountainous areas or water) to provide network access in areas where cabling would be too expensive. With a direct line of sight between the two access points and a sufficient Fresnel zone, you can bridge distances of several kilometers by this type of wireless link.

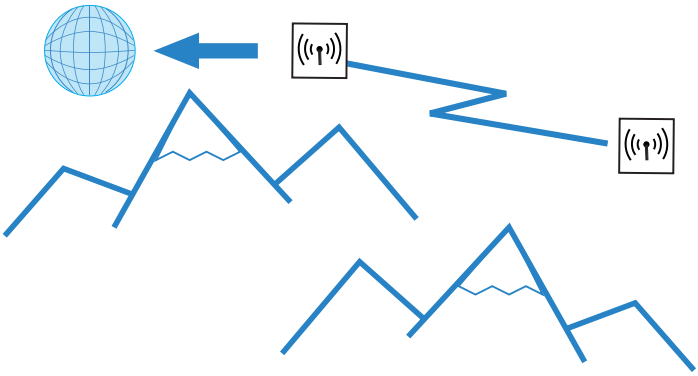


Figure 3: Point-to-point connection with a direct line of sight

1.3 WLAN Bridge Relay

Sometimes the required distance between two Access Points may exceed the maximum radio range of a wireless link. Also, physical obstacles may exist that prevent an uninterrupted line-of-sight connection between two Access Points.

In these cases, you can connect the two end points by stringing together multiple Access Points, where each intermediate Access Point is equipped with two radios. Because the intermediate Access Points often operate solely as relay stations, this design is referred to as Relay mode.

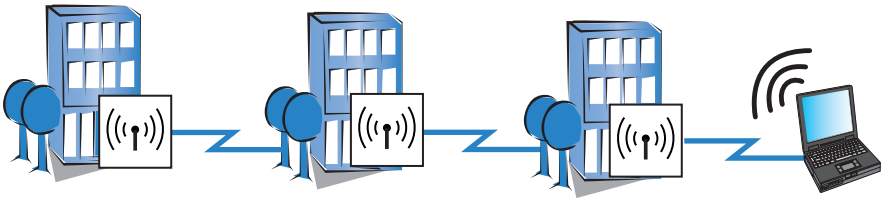


Figure 4: WLAN bridge in relay mode

OpenBAT Devices can run several P2P connections simultaneously on each wireless module, in addition to supporting WLAN Clients. However, for performance reasons, we recommend the use of OpenBAT devices with two wireless modules for the relay stations. If you use directional antennas, the relay station needs to be equipped with two radios.

1.4 WLAN Distribution Point - (Point-to-Multipoint)

A special type of wireless link is the connection of several distributed access points to a central point—the point-to-multipoint (P2MP) WLAN or Wireless Distribution System (WDS). With this mode of operation you can establish connections for several buildings on a company's premises with the central administrative building, for example. This mode of operation makes it possible, for example, for several buildings on a company's premises to be connected to the central administrative building. The central access point or wireless router is configured as 'master' and the remote stations as 'slaves'.

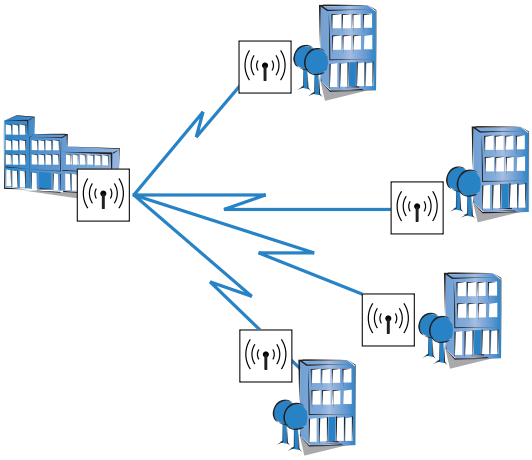


Figure 5: Point-to-multipoint wireless LAN

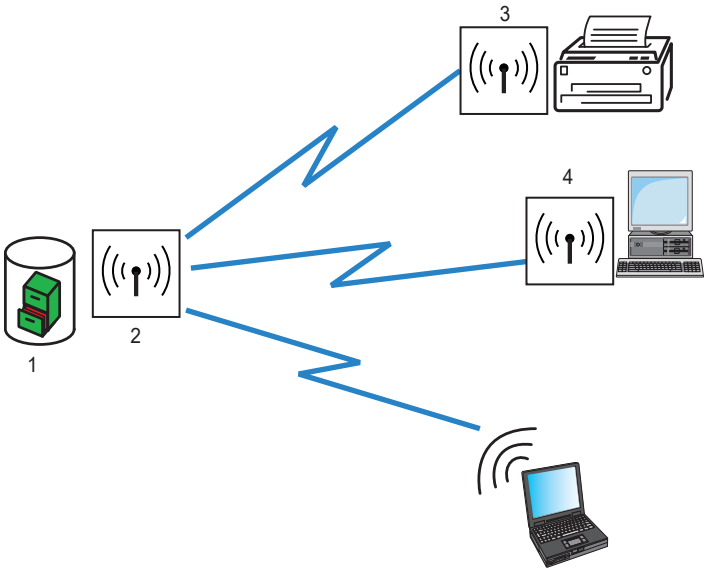
Note: A device can simultaneously establish both point-to-point and point-to-multipoint links.

1.5 WLAN Client

A WLAN Client can be either:

- equipped with an Ethernet interface (for example, a PC or printer), or
- an Access Point that is configured to serve as conventional wireless LAN adapter and not utilize its full capability as Access Point.

You can purchase special OpenBAT devices that can operate exclusively as WLAN Clients.



1: Authentication, Authorization and Accounting server	3: WLAN client with printer
2: WLAN device in Access Point mode	4: WLAN client with PC

1.6 WLAN Roaming Clients

Using OpenBAT devices, you can develop WLAN systems in industrial environments for the transmission of data to mobile objects. In the following logistics example, fork-lift trucks remain continuously connected to the company network via the WLAN. When combined with mobile barcode scanners, this system permits real-time monitoring of the inventory flow within a warehouse. Data obtained in this system pass through to an inventory control system, which continuously provides up-to-the-minute information on current inventories.

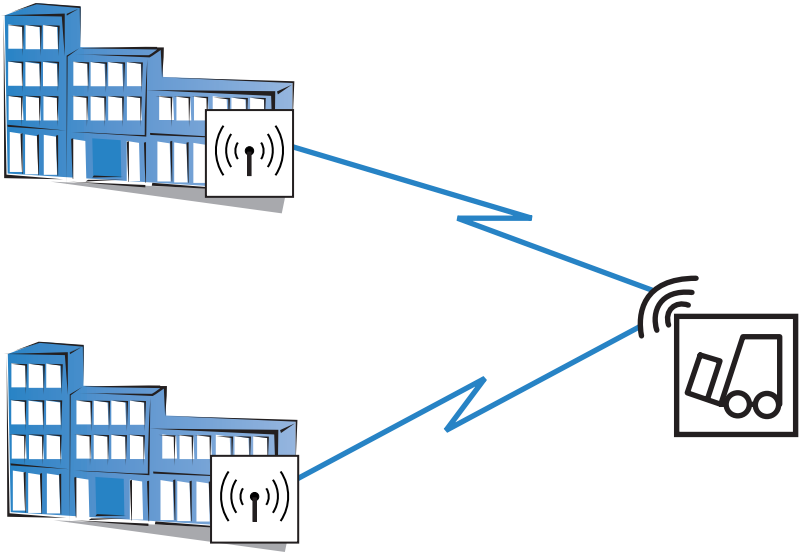


Figure 6: A WLAN client roaming between access points

2 Configuration Tools

The OpenBAT devices support a broad range of configuration software.

- LANconfig: OpenBAT device parameters can be set quickly and easily using this Windows-based application. Outband, inband and remote configurations are simultaneously supported, even for multiple devices.

- WEBconfig: This software is permanently installed in the device. All that is required on the configuration workstation is a web browser. In HiLCOS version 8.80 and above you can alternatively use the LANconfig-internal browser for accessing WEBconfig.
  WEBconfig itself works independently of the OS you run. Inband and remote configurations are supported.

- Configuring via SNMP: Device-independent applications for the management of IP networks are generally based on the SNMP protocol. The SNMP-based configuration of OpenBAT devices can be accomplished by both inband and remote access.

- Terminal program, Telnet: You can configure a OpenBAT device with a terminal program via the configuration interface (e.g. HyperTerminal) or within an IP network (e.g. Telnet).

- tftp: Trivial file transfer protocol (tftp) can also be used within IP networks (inband and remote configuration) to configure a OpenBAT device.

The following chapters of this manual present numerous configuration instructions for the OpenBAT devices. These instructions are presented using the LANconfig software.

The LANconfig menu structure for configuring an OpenBAT device:

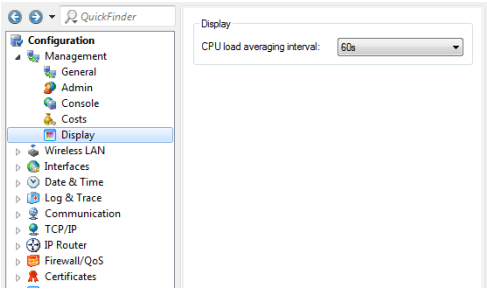
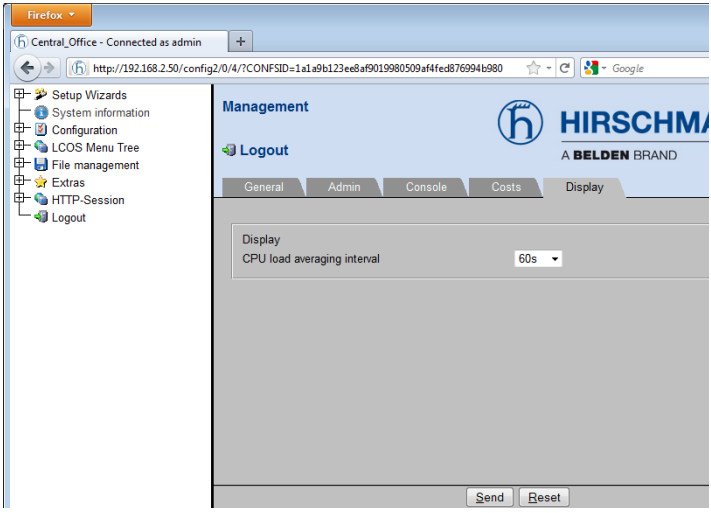


Figure 7: New Configuration of a Device

The WEBconfig menu structure for configuring an OpenBAT device:



2.1 Startup Behavior

When an OpenBAT device is shipped from the factory, it comes pre-configured with the following default settings:

- Each WLAN radio interface is turned OFF.
- The WLAN operation mode is set to ‘Managed’.

Consequently, the initial configuration of an OpenBAT device cannot be performed over the WLAN. Instead, use another means of access (e.g., via a wired LAN connection) to perform the initial configuration.

Alternatively, you can use a BAT controller to configure the Access Points conveniently from a central instance. You will find information on configuring the BAT controller under „Central WLAN Management“.

2.1.1 Factory-Default Network-Exposed Services

Upon first power-up, HiLCOS ships with a predefined set of network services and built-in network functions in its factory-default state to support out-of-the-box connectivity, management, and diagnostics. For details, see here.

2.2 Online versus Offline Configuration

You can configure an OpenBAT device either online or offline. Each approach has its advantages:

- Online configuration is immediate—you are configuring device properties in real time.
- Offline configuration can be conducted in the controlled environment of your configuration PC. Offline configuration produces a configuration file that can be modified and re-used for similar devices.

2.3 Downloading the Configuration File

After you have created a configuration file offline, you can assign this configuration to a specific device using the LANconfig software.

☐ Use automatic discovery to 'find' the device:

  ☐ Select `File : Find devices`. The LANconfig software searches for all devices and lists the devices found.

☐ Select the device you want to configure, then go to the main menu and select: `Device : Configuration Management : Restore from file`

☐ In the 'Restore Configuration' dialog, navigate to and select the saved configuration file for the selected device, and click 'Open'.

The selected configuration file settings are applied to the device.

Note: For a more detailed description of the process of loading a configuration file to a device, see the "HiLCOS Operation and Maintenance Guide".

3 Configuring the Device

The following examples describe how you can configure OpenBAT devices in offline mode for use in the following specific applications.

- WLAN Bridge (same subnet): Two OpenBAT devices configured as Access Points, forming a point-to-point WLAN bridge connecting two segments of the same subnet
- WLAN Bridge (different subnets): Two OpenBAT devices in router mode configured as Access Points, forming a point-to-point WLAN bridge connecting two segments of different subnets
- WLAN Bridge Relay (same subnet): Two OpenBAT devices configured as Access Points, connected via a third OpenBAT device that serves as a relay device. Together, they form a point-to-point WLAN bridge.
- Point-to-Multipoint (same subnet): A single OpenBAT device configured as an Access Point for WLAN Clients, where both the wireless network and the wired network backbone are part of the same subnet
- Point-to-Multipoint (different subnets): A single OpenBAT device configured both as Access Point and as DHCP server for WLAN Clients. In this example, WLAN and wired network are located on different subnets.
- Roaming Client (different subnets): An example of a WLAN device that is configured to access a wireless LAN and obtain its IP address from a DHCP server.

In each of these examples, an OpenBAT device is configured offline, then the configuration file is downloaded to the individual device.

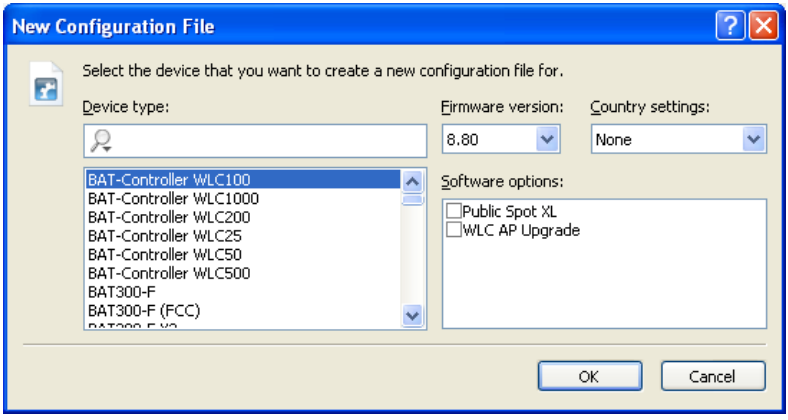
3.1 Creating a Configuration File

For all offline configurations, begin by creating a configuration file. The configuration file will contain the settings required to configure the device for service in a specific role. There are two ways to begin to create a new file:

- In the LANconfig tool's main menu, select:
  `Edit :New Configuration File`, or
- In Windows Explorer, within a folder that you have created to hold your configuration files, click the right mouse button to open a pop-up menu, then select:
  `New : Hirschmann LANconfig Configuration`

In either case, the 'New Configuration File' dialog opens. Follow the work-steps, set forth below, to create a new LANconfig file.

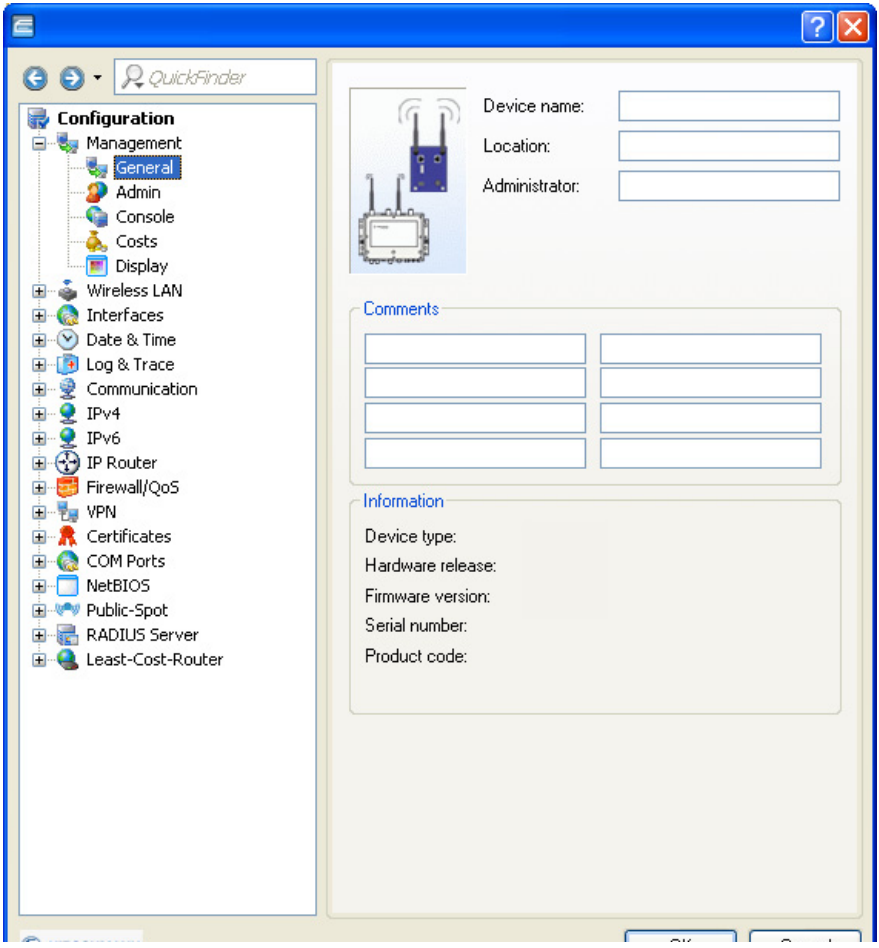
☐ In the 'New Configuration File' dialog, specify both the 'Device type' and the 'Firmware version' of the OpenBAT device you want to configure:



In this example, do the following:
– Device Type: Select a device.
– Firmware version: 8.80

– Country settings: Select a country. To ensure your device operates WLAN networks with the correct parameters, the device must be introduced to its national site. If you don't select any country settings, the device will allow only parameters that are permitted worldwide!
– Software options: Add configuration settings for additionally purchased software options to the basic configuration dialog by selecting its dedicated entry.
– Click ‘OK’.

The following dialog opens:



☐ Do the following:

  ☐ Type in a Device name. In this example, type in ‘LEFT’.

  ☐ Click ‘OK’ to save the device configuration file.

☐ Do one of the following:

  – If you are working in the LANconfig tool, the ‘Save Configuration File’ dialog opens. After navigating to the desired storage location, click ‘Save’ to save the new file.

  – If you are working in Windows Explorer, the ’Advanced’ dialog opens. Click ’Cancel’ to close this dialog. The new LANconfig file is saved in the Windows Explorer folder in which you are working.

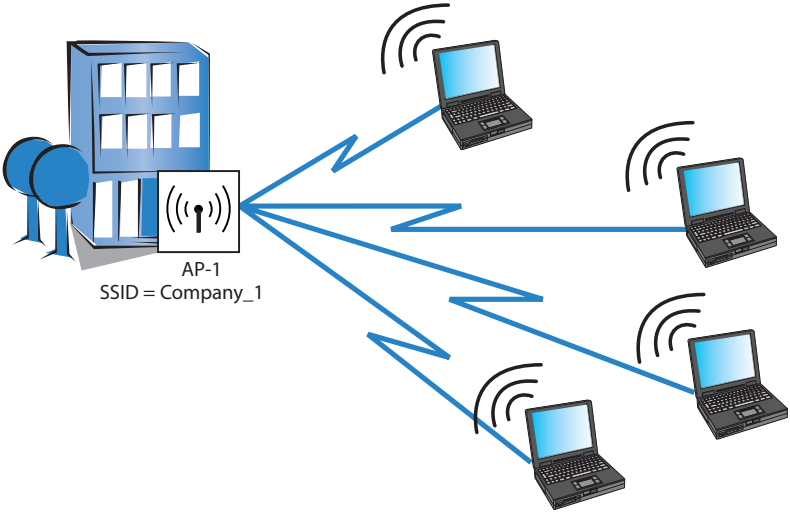
You have created and saved a new LANconfig file. The following sections describe how to configure this file for use in a specific role.

3.2 Access Point for Multiple Wireless Clients

This example describes the configuration of a single OpenBAT device (AP-1) to serve as Access Point connecting multiple WLAN Clients to a wired network. Both the wired and wireless networks are part of the same subnet. Each WLAN Client needs to select the network name (SSID) and input a pre-configured passphrase to gain access to the wireless network.

The particular IP address of any device, including both the Access Point and any WLAN Client, is not important to this design. Although the IP address for the Access Point is manually input in this example, it could instead be assigned by a DHCP server.

By deploying the completed device configuration file to multiple Access Points connected to your wired network backbone – and only changing the IP address for each Access Point – a WLAN Client could roam and stay connected to the network through a number of different Access Points.



Refer to the sample WLAN Client configuration (see on page 89) for instructions on how to set-up the clients.

The significant configuration settings for the device are as follows:

Station Name:	AP-1
Role:	Access Point
Number of interfaces/channels used:	1/1
Network name (SSID):	Company_1
WPA passphrase:	CompanyPW

Perform the following tasks to create a configuration for a OpenBAT device used in this role:

☐ Create a new configuration file

☐ Configure the basic settings

☐ Configure the wireless LAN settings

3.2.1 Creating a New Configuration File

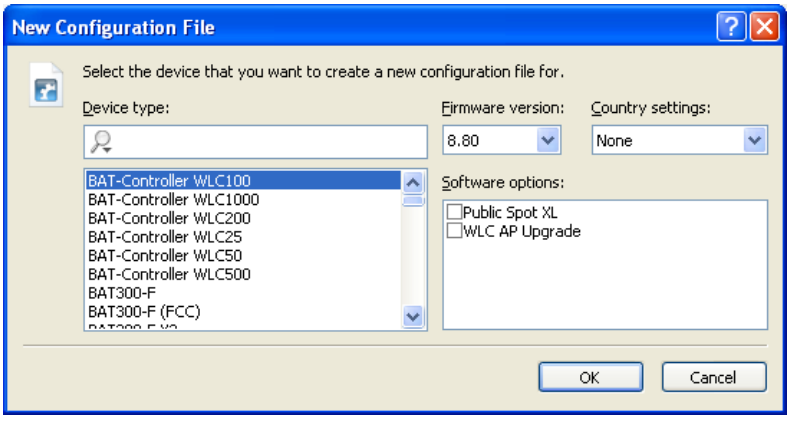
There are two ways to create a new configuration file:

☐ In the LANconfig tool's main menu, select:
`Edit :New Configuration File`, or

☐ In Windows Explorer, within a folder that you have created to hold your configuration files, click the right mouse button to open a pop-up menu, then select:
`New : Hirschmann LANconfig Configuration`

In either case, the ‘New Configuration File’ dialog opens. Follow the work-steps, set forth below, to create a new LANconfig file.

☐ In the ‘New Configuration File’ dialog, specify both the ‘Device type’ and the ‘Firmware version’ of the OpenBAT device you want to configure:

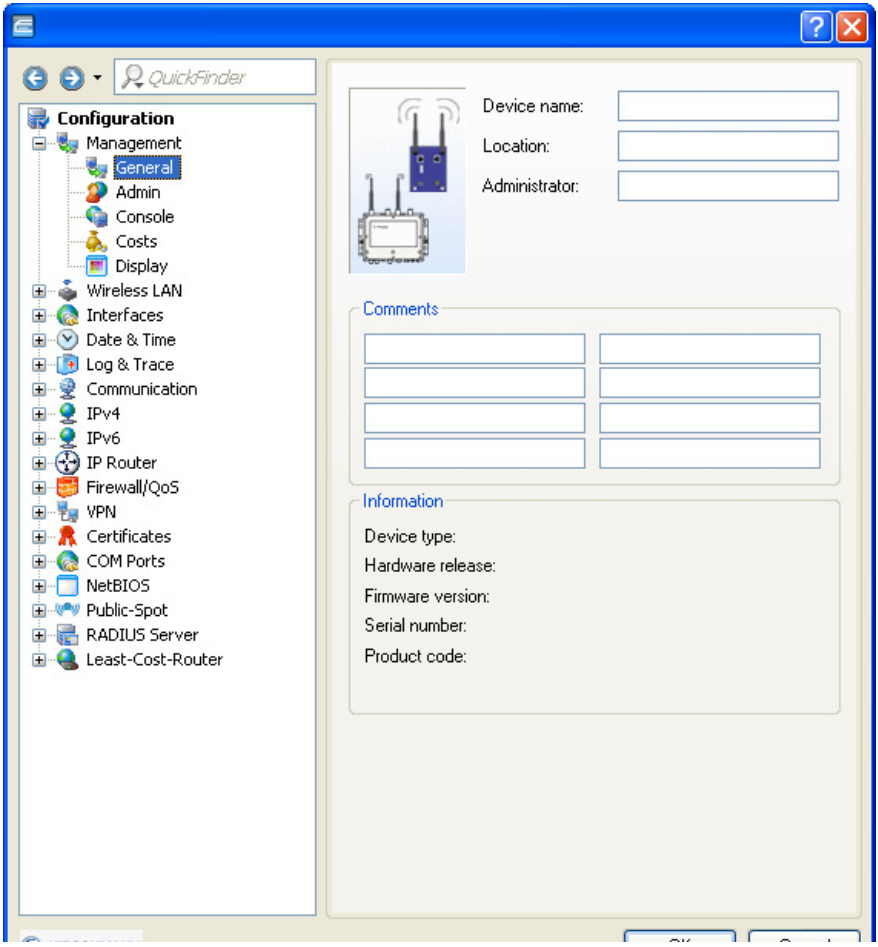


In this example, do the following:

– Device Type: Select a device.
– Firmware version: 8.80
– Country settings: Select a country. To ensure your device operates WLAN networks with the correct parameters, the device must be introduced to its national site. If you don't select any country settings, the device will allow only parameters that are permitted worldwide!

– Software options: Add configuration settings for additionally purchased software options to the basic configuration dialog by selecting its dedicated entry.
– Click ‘OK’.

The following dialog opens:



☐ Do the following:

☐ Type in a Device name. In this example, type in 'AP-1'.

☐ Click 'OK' to save the device configuration file.

☐ Do one of the following:

– If you are working in the LANconfig tool, the 'Save Configuration File' dialog opens. After navigating to the desired storage location, click 'Save' to save the new file.

– If you are working in Windows Explorer, the 'Advanced' dialog opens. Click 'Cancel' to close this dialog. The new LANconfig file is saved in the Windows Explorer folder in which you are working.

☐ Open Windows Explorer, navigate to the new file, and change its name to `AP-1.lcf`.

You have created and saved a new LANconfig file. The following sections describe how to configure this file for use as a wireless access point.

3.2.2 Configuring Basic Settings

Use the LANconfig Setup Wizard to configure the following basic settings for the device configuration file:

– device name

– password

– DHCP mode

– TCP/IP settings

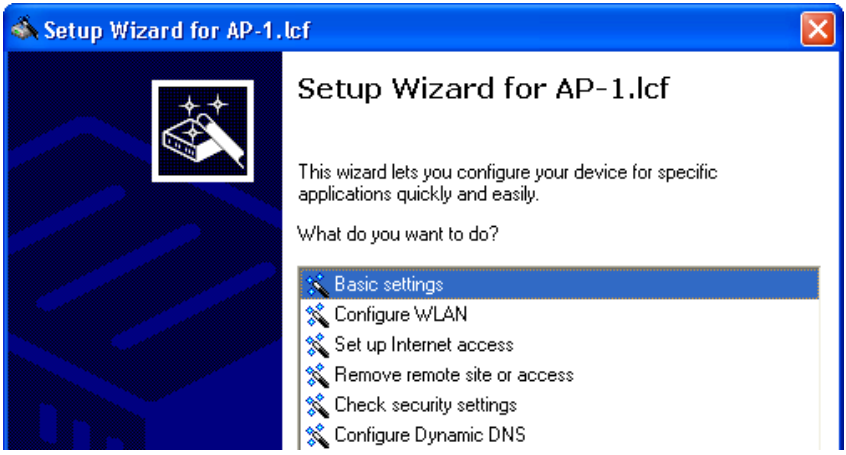
– time synchronization settings
– optional device descriptions

☐ To start the Setup Wizard:

☐ In Windows Explorer, select the newly created LANconfig file, then

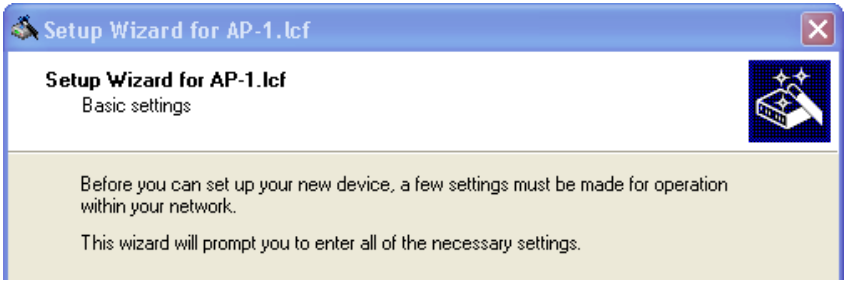
☐ Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the Setup Wizard, select 'Basic settings':



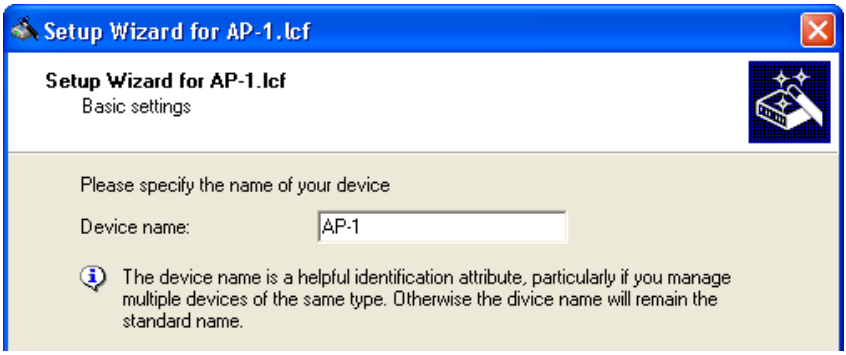
Click 'Next'.

☐ The wizard displays the following introduction:



Click ’Next’.

☐ Input a device name:



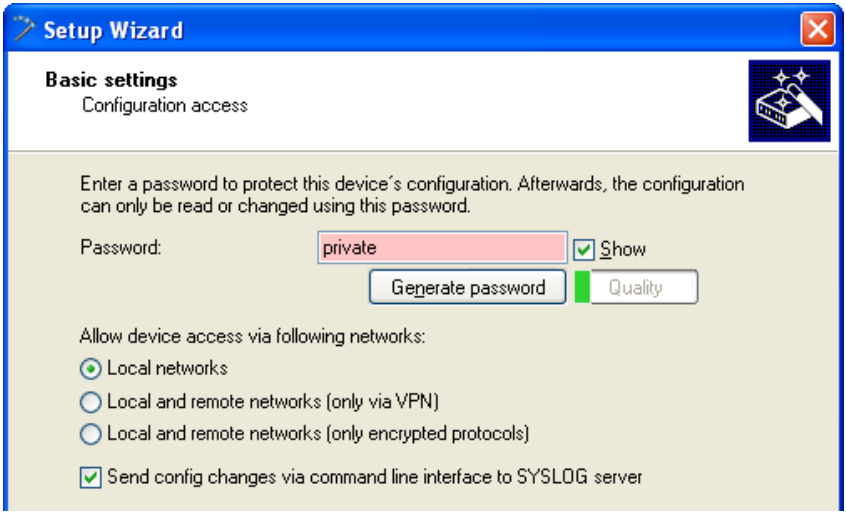
For the purpose of this example, use the name ’AP-1’.

Note: The default device name is a concatenation of the device part number and the last 3 octets of the device MAC address.

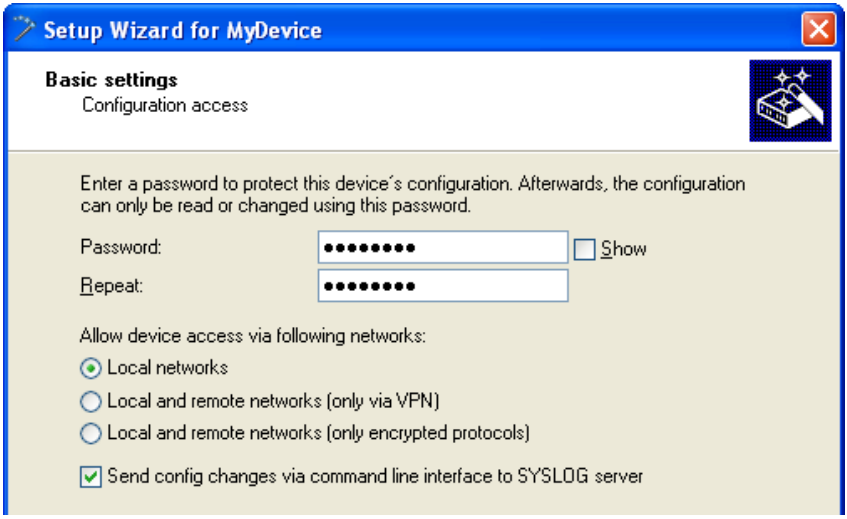
Click ’Next’.

☐ The following screen opens, where you need to enter a password in one of the following ways:

- Select 'Show' (below) to display the default password ('private') then do one of the following:
  - accept the default password
  - type in a new password
  - click 'Generate password' to let the wizard input a new password



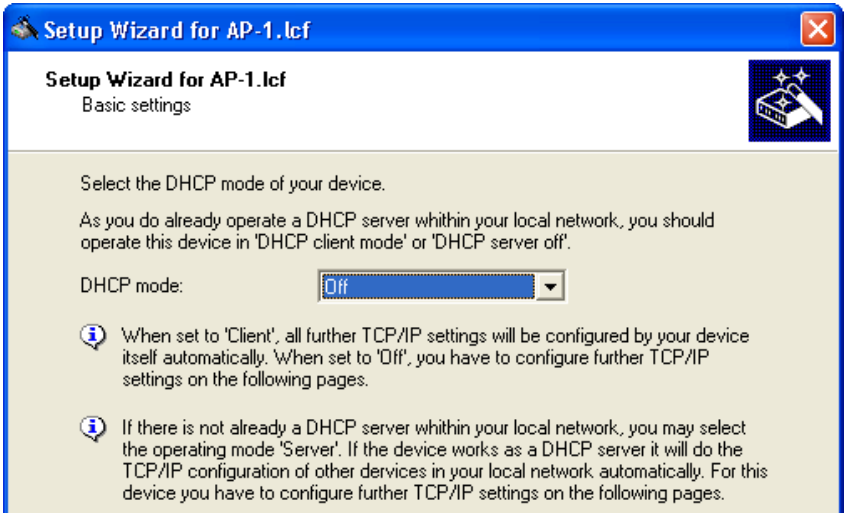
- De-select 'Show' (below) then either accept the default password ('private') or type in a new one. In either case, re-type the password in the 'Repeat' field.



▶ Set the networks permitted to access the device. If you restrict access to local networks, only PCs that are directly connected to the local area network by cable or wireless can access the device configuration.

Note: The assistent indicates the different security levels of passwords color-coded. Insecure passwords are highlighted in red, conditionally secure ones are highlighted in yellow, and secure to very secure ones are highlighted in white.

☐ Identify the DHCP mode of the OpenBAT device:



Select one of the following DHCP modes:

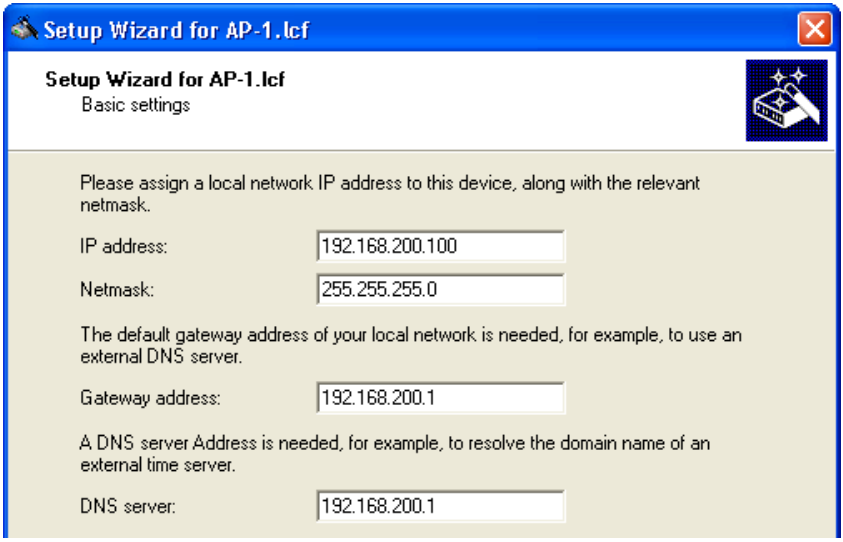
– Off:
  The device functions neither as DHCP client nor as DHCP server. In this mode, you need to manually input the IP address settings.
– Server:
  The OpenBAT device functions as DHCP server and provides IP address settings to other network devices.
– Client:
  This setting causes the OpenBAT device to request the IP address settings from a DHCP server on the network.

If a DHCP server exists on your network, select the ‘DHCP mode’ of ‘Off’. The default ‘DHCP mode’ setting of ‘Client’ can override a manually assigned IP address.

Note: Your DHCP mode selection determines the next screen displayed by the Setup Wizard.

For the purpose of this example, select ’Off’, then click ’Next’.

☐ Input the TCP/IP settings for the OpenBAT device:

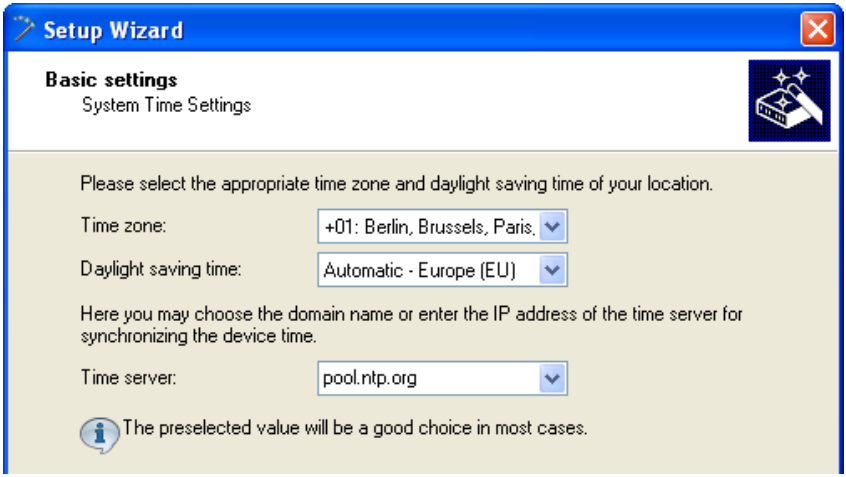


For the purpose of this example, these settings are:

– IP address: 192.168.200.100
– Netmask: 255.255.255.0
– Gateway address: 192.168.200.1
– DNS server: 192.168.200.1

Click 'Next'.

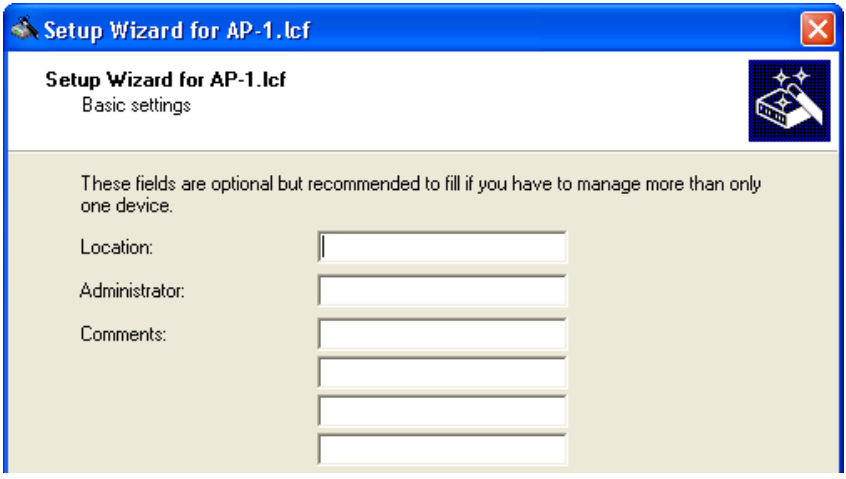
☐ The wizard prompts you to identify your national timezone, prevailing changeover rules and a time synchronization server that will set the system time for the OpenBAT device:



Select a time server from the list, or type in its IP address.

Click 'Next'.

☐ The wizard shows the following screen for optional information on the location of the device, its administrator, and any comments relating to the OpenBAT device.



Click ’Next’.

☐ Click ’Finish’ to complete configuration of the basic settings (below):

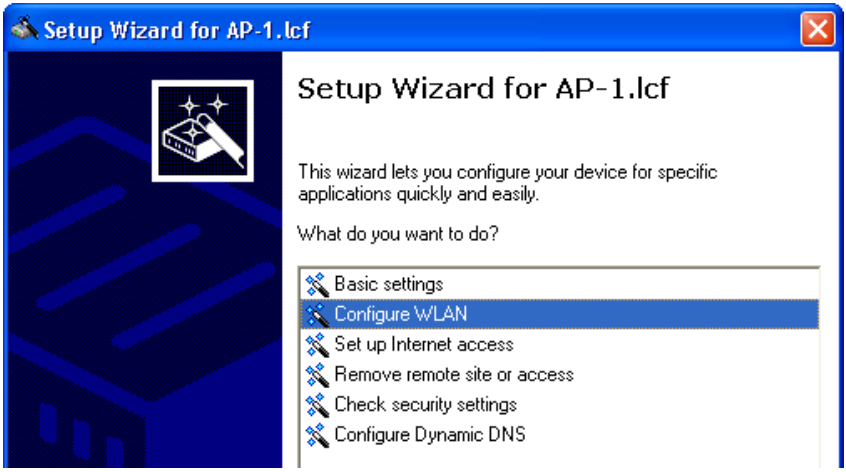
3.2.3 Configuring Wireless LAN Settings

WLAN settings can be made using either the LANconfig tool’s discrete configuration screens or the Setup Wizard. This task is most easily accomplished using the wizard.

☐ To start the Setup Wizard:

- ☐ In Windows Explorer, select the current LANconfig file, then
- ☐ Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the wizard, select ’Configure WLAN’ (below):



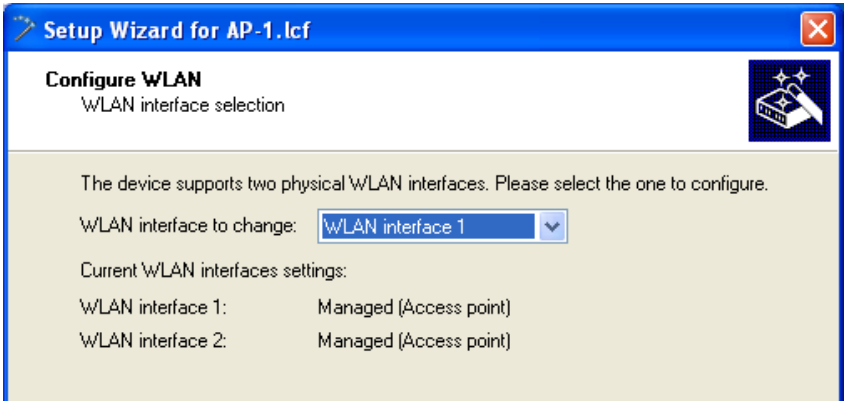
Click 'Next'.

☐ Select the country in which the OpenBAT device is operated:

Note: The country designation determines the available frequencies.

Click 'Next'.

☐ Select a WLAN interface to configure:

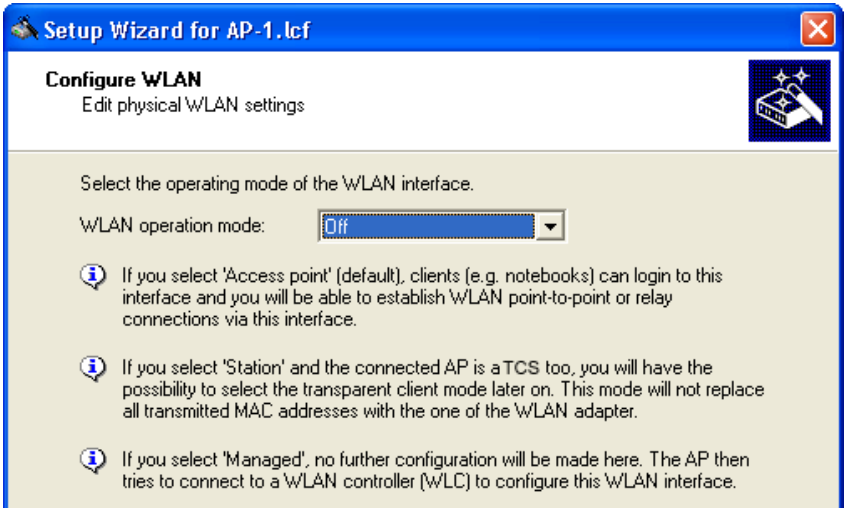


A device can have multiple WLAN interfaces. Here, the selected device has two (2) interfaces. By default, both interfaces are enabled.

Note: You can configure one WLAN interface at a time. After selecting an interface, proceed through the wizard's remaining pages and finish configuration for the selected interface. Thereafter, re-start the Configure WLAN wizard and configure the other WLAN interface.

Select 'WLAN interface 2' as the WLAN interface to configure (above), then click 'Next'.

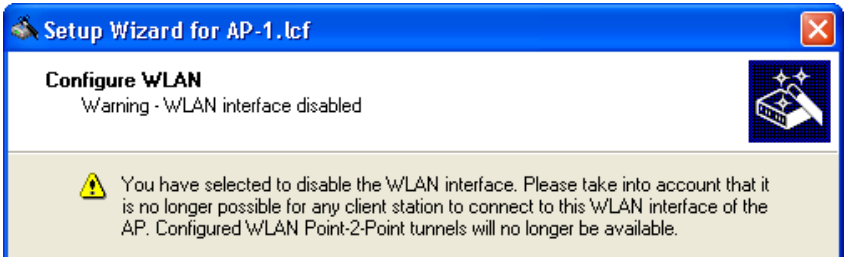
☐ The next step is to enable or disable the selected WLAN interface:



A point-to-point WLAN bridge requires just a single interface. In this example, the currently selected interface—WLAN interface 2—will be disabled. (You will later configure WLAN interface 1 to support the point-to-point WLAN bridge.)

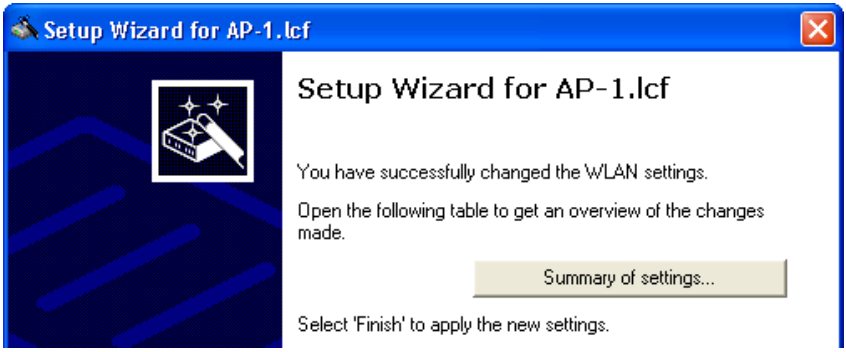
Disable WLAN interface 2 by setting its ’WLAN operation mode’ to ’Off’ (above), then click ‘Next’.

☐ The wizard notifies you that you are about to disable interface 2:



Click ’Next’.

☐ Complete the configuration of WLAN interface 2:



Click ’Finish’.

☐ Return to the Windows Explorer folder where the file LANconfig file is saved, then do the following:

– select the LANconfig file (`AP-1.lcf`)

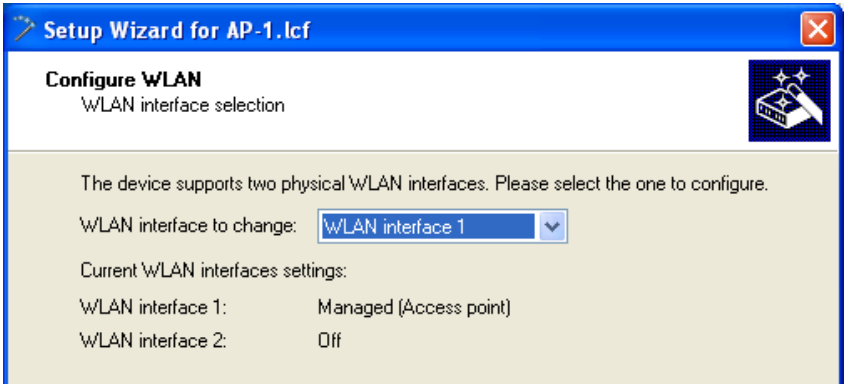
– click the right mouse button to open a pop-up menu

– select `Setup Wizard`

☐ In the LANconfig Setup Wizard:

☐ select ’Configure WLAN’

☐ click ’Next’ two times, or until the wizard displays the WLAN interface selection screen

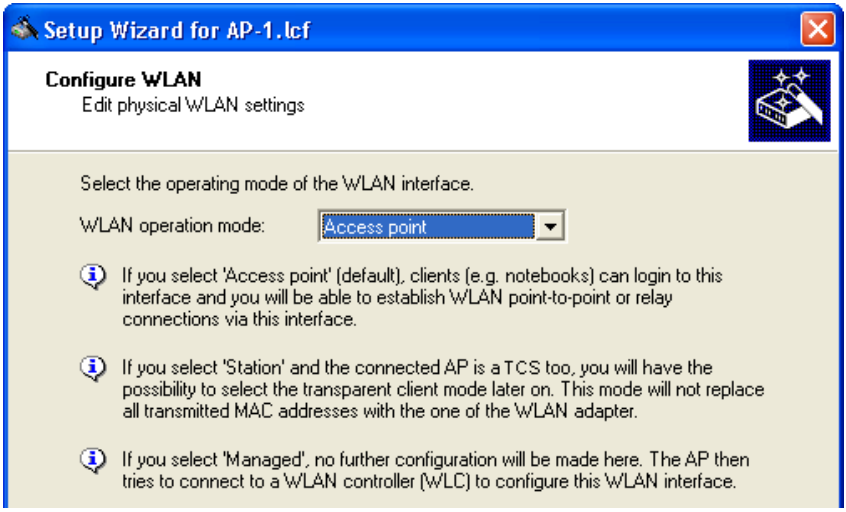


Note: This screen indicates that WLAN interface 2 has been turned off. The next step is to configure WLAN interface 1.

Select 'WLAN interface 1' as the 'WLAN interface to change'.

Click 'Next'.

☐ Specify an operation mode for the interface (WLAN interface 1):



WLAN operation modes include:

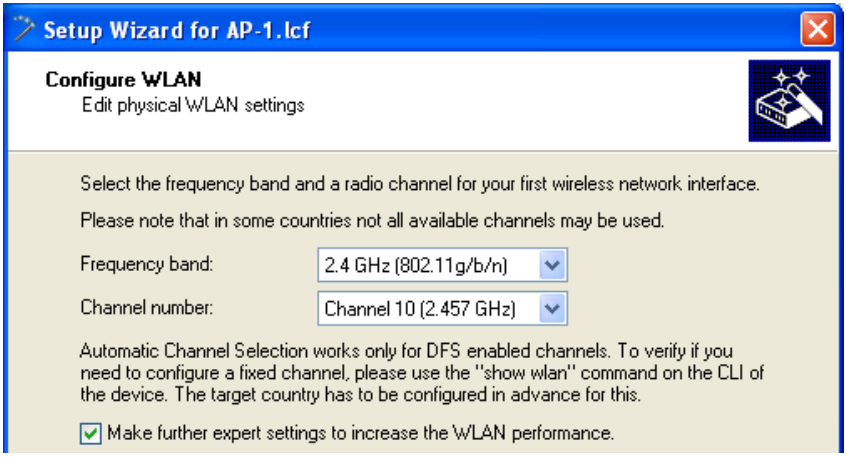
– Access Point:
The device serves as a base station, and can establish links to another access point (point-to-point), to remote clients, or to both remote access points and remote clients.

– Client:
The device serves as Client and needs to log into an Access Point. In this role, the device can link a cabled network to a WLAN over a wireless connection.

– Managed (Access point):
The device operates as an Access point, but searches for a central WLAN controller it can obtain a configuration from.

Select 'Access point', then click 'Next'.

☐ Enter settings for the wireless frequency and channels over which the device will operate, and indicate whether you wish to configure additional performance-enhancing settings:



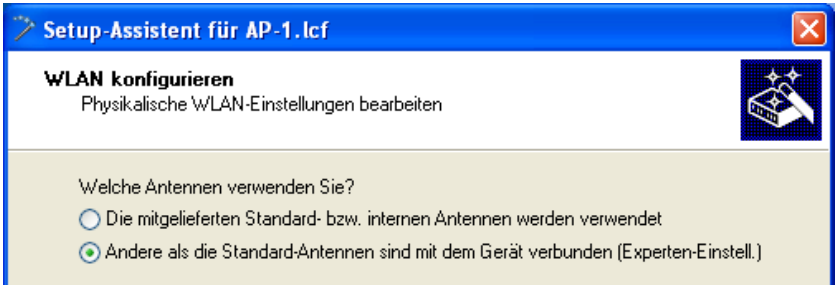
The specific antennas you plan to use will determine how you complete this dialog. For the purpose of this example, enter the following settings:

– Frequency band: 2.4 GHz

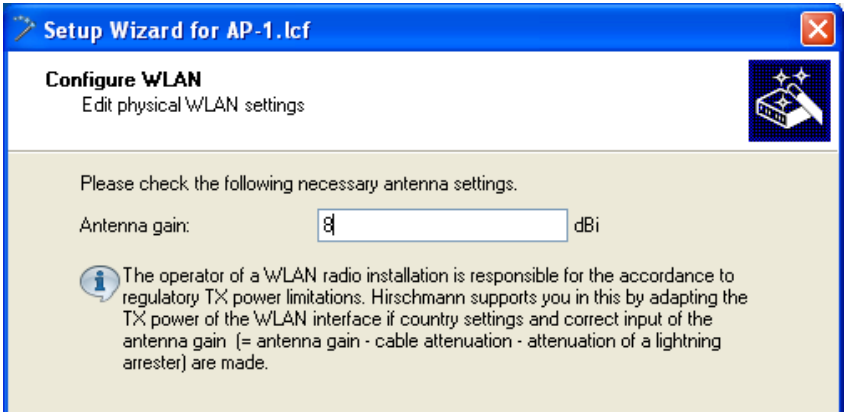
– Channel number: Channel 10 (2.457 GHz)

– Select 'Make further explicit settings to increase the WLAN performance'.
(This option gets the set-up wizard to display additional configuration screens for QoS and IGMP snooping.)

– Choose: 'Antennas other than the default antennas are connected to the device.'

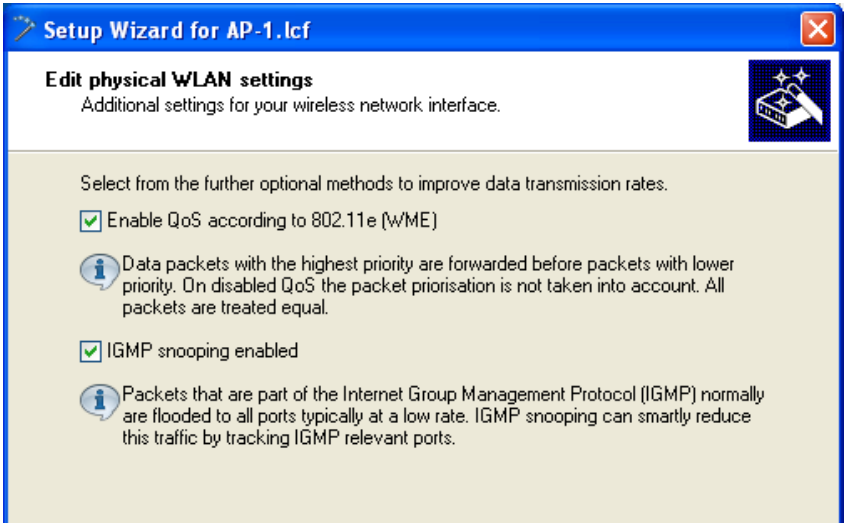


☐ Check the antenna settings:



the calculated antenna gain is 8 dBi for this example

☐ Click 'Next'.
The wizard presents settings that can be used to increase data transmission rates:



You can enable or disable the following services:

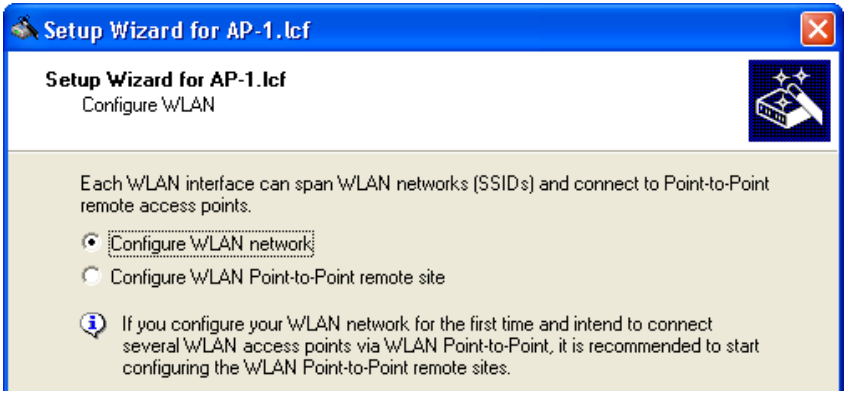
– QoS

– IGMP Snooping

For the purpose of this example, all available data rate enhancing options are selected.

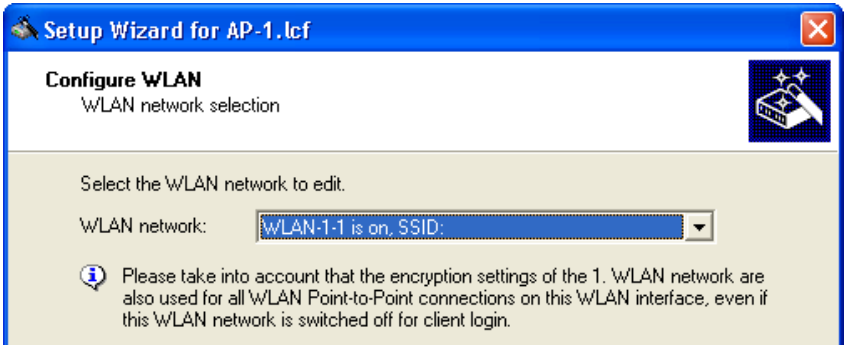
Click 'Next'.

☐ Indicate what will be configured—a point-to-point site or a WLAN network:



Select 'Configure WLAN network', then click 'Next'.

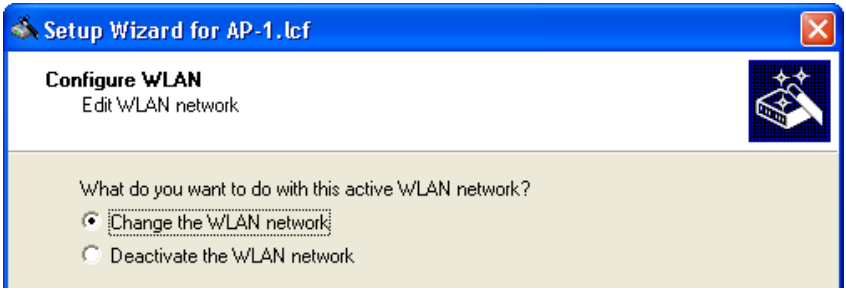
☐ Select the network to configure:



For the WLAN network, select 'WLAN-1-1'. This indicates that this access point will use channel 1 on interface 1.

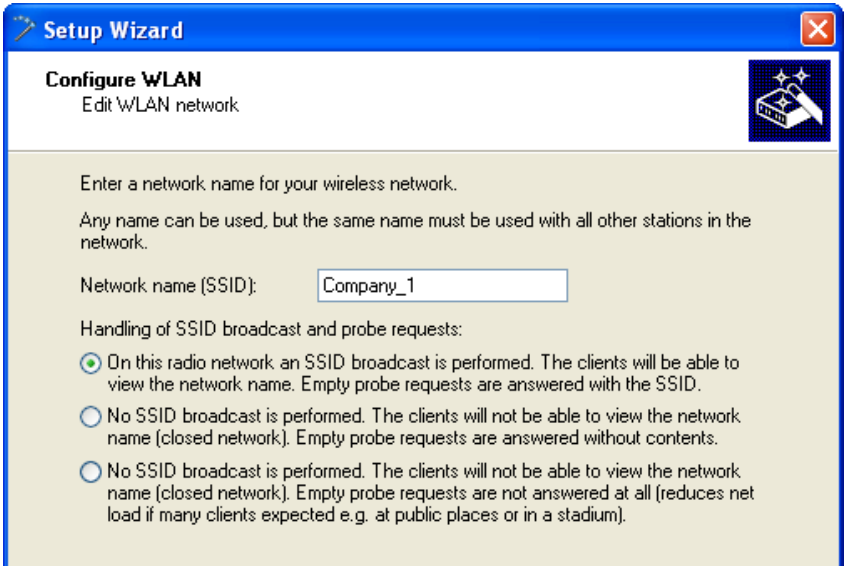
Click 'Next'.

☐ Indicate that changes are to be made to the WLAN network:



Select 'Change the WLAN network, then click 'Next'.

☐ Enter the Network name (also known as the Service Set Identifier or 'SSID'):



Also, select whether the device should propagate the specified SSID in its wireless network. If you disable the SSID broadcast, the device does not transmit any SSID. This can help keep rogue wireless client devices from detecting the existence of this network.

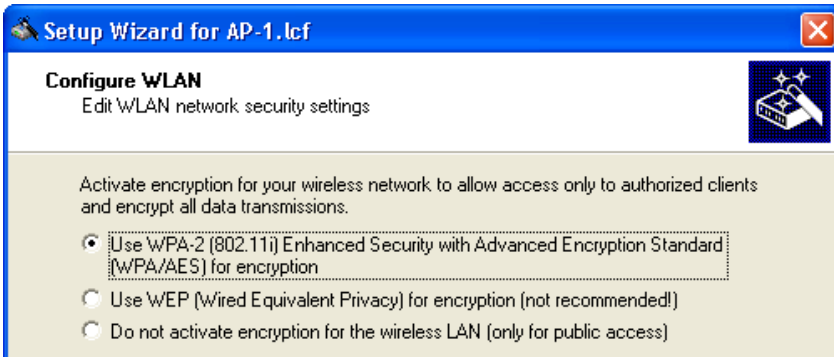
For the purpose of this example:

– Change the SSID to ’Company_1’

– Option "No SSID broadcast is performed […]".

Click ’Next’.

☐ Specify the transmission encryption protocol:

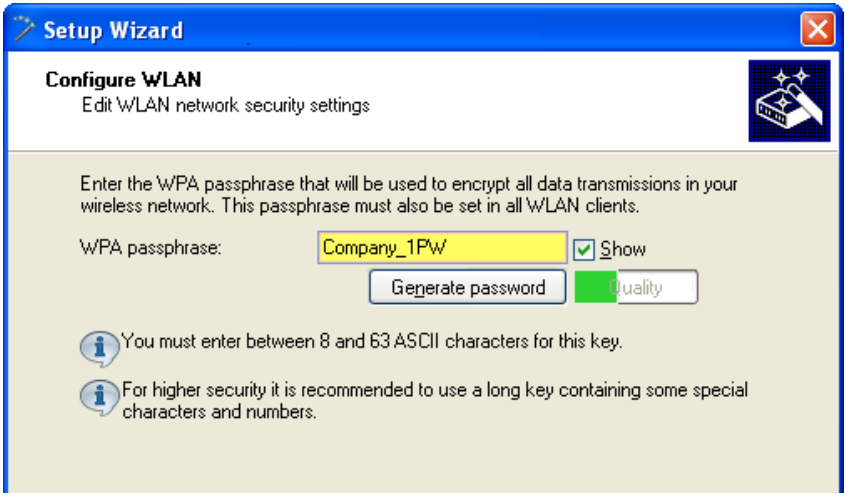


Note: Hirschmann recommends the use of WPA-2 to provide enhanced security.

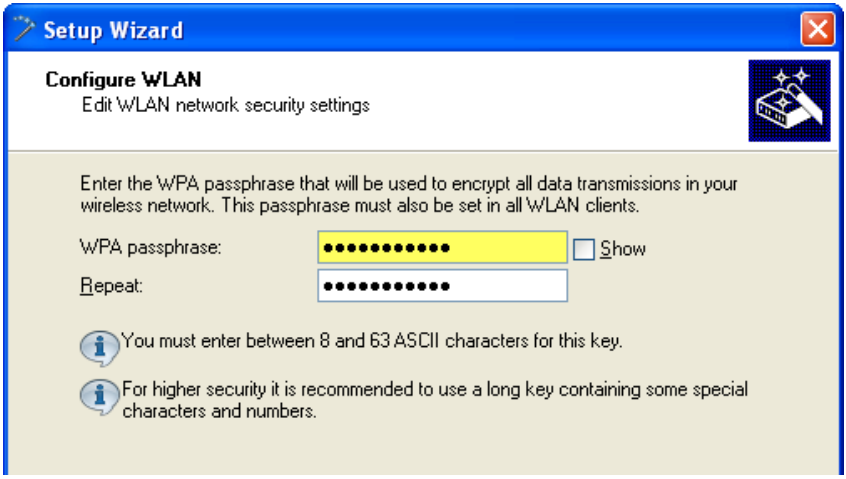
Click ’Next’.

☐ The following screen opens, where you enter a password in one of the following ways:

– Select 'Show' (below) to enter a WPA passphrase then either:
  - type in a new passphrase
  - click 'Generate password' to let the wizard input a new passphrase



– deactivate the 'Show' checkbox (below) and enter a new WPA passphrase. For this you use a key with 8 to 63 ASCII characters, using special characters and numbers if possible. Then repeat the entry in the 'Repeat' field.



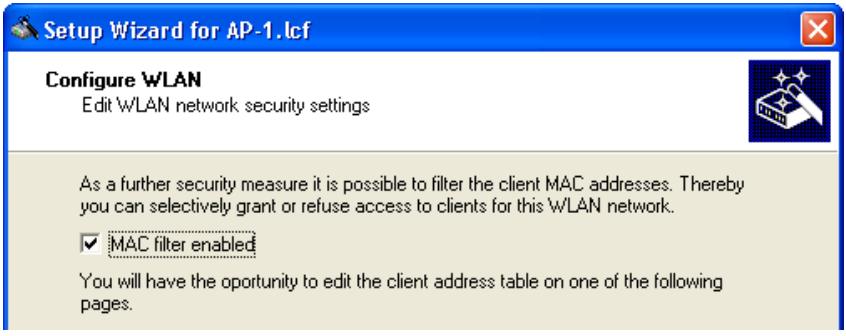
The role of an OpenBAT device in the point-to-point connection determines how the passphrase is used. If the device is configured as:

– Master: the passphrase is used to check a slave's authorization to access the network.

– Slave: the passphrase is transferred to the Master to gain wireless access to the network.

In this example, accept the default password, then click 'Next'.

☐ Indicate whether the MAC filter will be used by this WLAN:



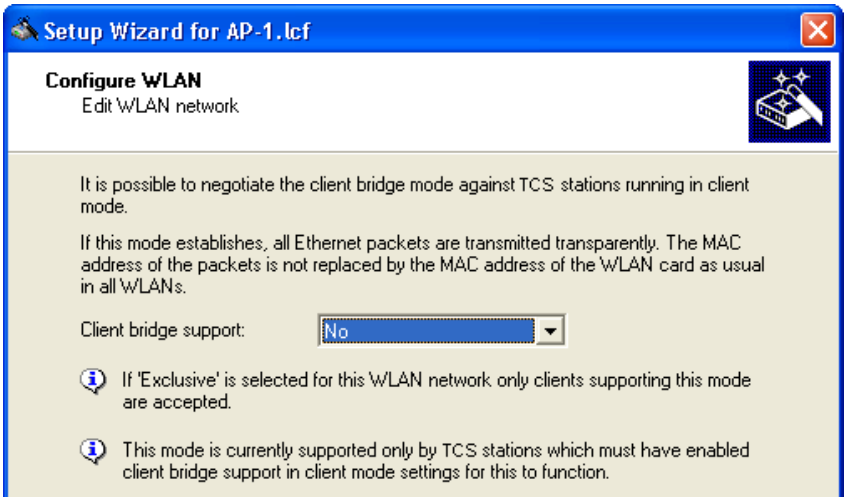
The OpenBAT device can filter WLAN Client devices based on a list of MAC addresses. The list can be either a:

- blacklist, denying network access to listed MAC addresses, or
- whitelist, limiting network access exclusively to listed MAC addresses

Select the 'MAC filter enabled' checkbox. Later, the MAC filter will be configured for use as a blacklist.

Click 'Next'.

☐ Indicate whether client bridge support will be enabled:



Client bridge support relates to a network design that consists of:

– an OpenBAT device in the role of Access Point

– an OpenBAT device in the role of client

– one or more remote Ethernet devices connected to the client OpenBAT device in client mode

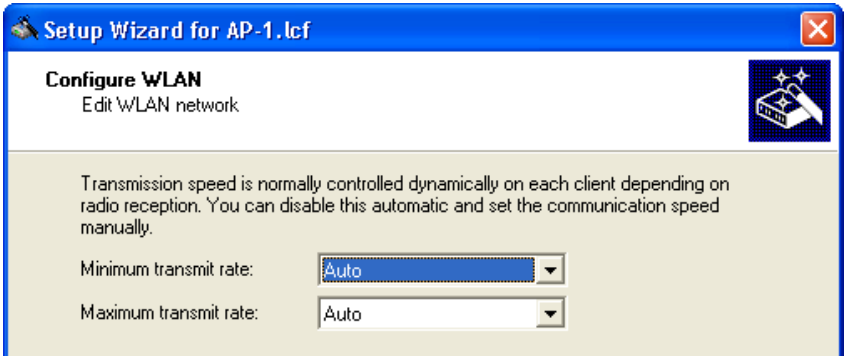
Typically, packets sent from a remote Ethernet device to the access point via the wireless client contain the MAC address of the wireless client, exclusively. Enabling client bridge support also includes the MAC address of the remote device.

Client bridging options are:

– No: client bridging support by the access point is disabled
– Yes: client bridging support by the access point is enabled
– Exclusive: wireless clients with enabled client bridging can communicate with the access point

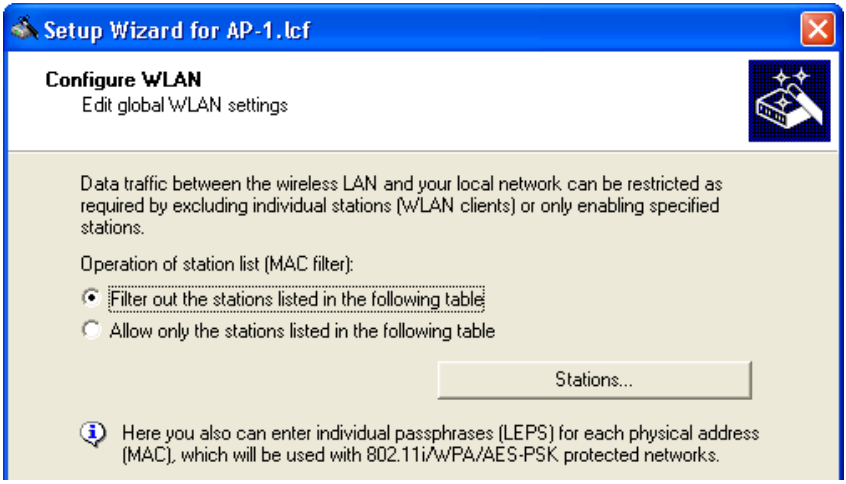
For this example, select 'No' to disable client bridging, then click 'Next'.

☐ Specify how transmission speed between the access point and wireless clients will be determined:



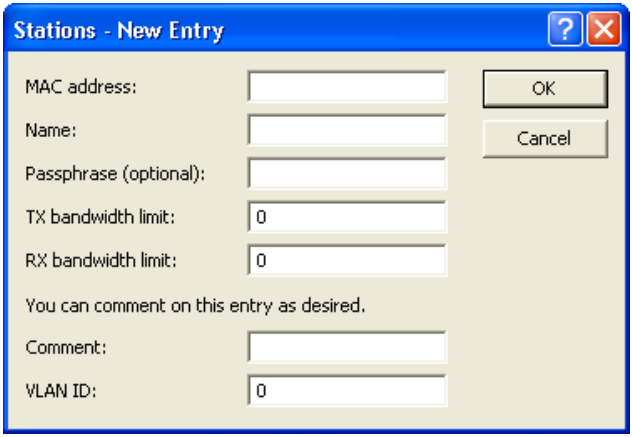
Select 'Auto' for both the 'Minimum transmit rate' and the 'Maximum transmit rate', then click 'Next'.

☐ Enter settings for the MAC filter:



☐ Select 'Filter out the stations listed in the following table' (above), then click the 'Stations...' button to open the following table:

☐ Click 'Add...' (above) to open the 'New Entry' dialog (below):

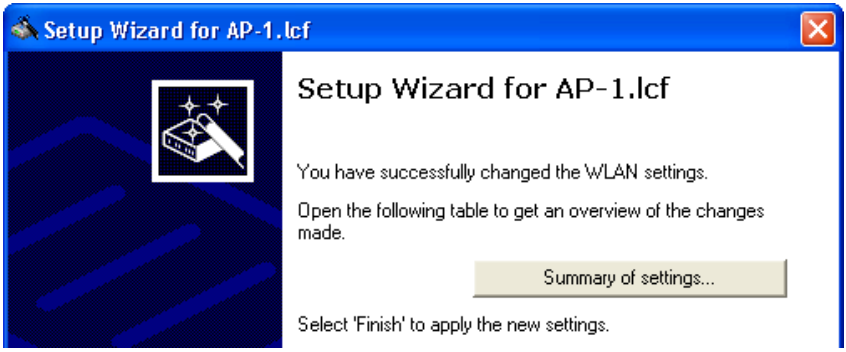


Use the' New Entry' dialog to add individual wireless client stations that will be denied access to the network. The lone parameter that needs to be configured for access denial is 'MAC address'.

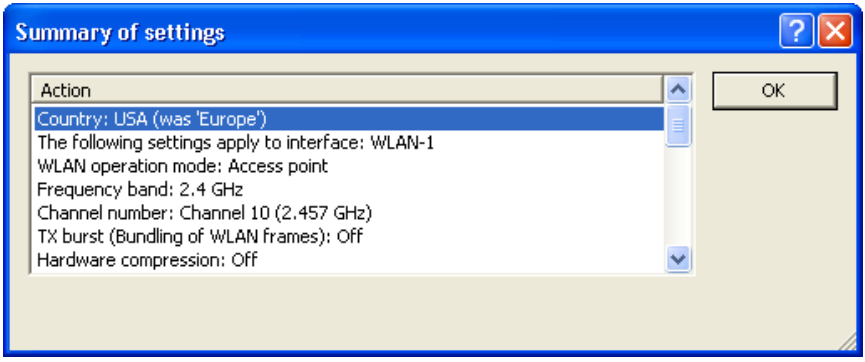
Note: When creating a 'whitelist', you can use:
- the Passphrase field to assign a device-specific passphrase
- the Bandwidth fields to restrict transmissions to a specific bandwidth
- the VLAN ID field to assign a client device to a VLAN

Click 'OK' to add a station. After all stations are added (one at a time), click 'OK' to close the list and return to the Configure WLAN wizard.

☐ You are now ready to complete the configuration of the access point for the wireless network:



☐ Click on the ’Summary of settings...’ button to display a list of all WLAN configuration settings:



Click ’OK’ to close the ‘Summary of settings’ window.

Click ’Finish’ to complete the wizard and save the settings for this wireless network access point.

3.3 Access Point & DHCP Server for Multiple Wireless Clients

This example builds on the previous configuration of an Access Point for multiple WLAN clients (see on page 51), by configuring the OpenBAT device (in this example, AP-2) to perform the additional role of DHCP server. In this example, the wired and wireless networks are located on different subnets. As before, each WLAN Client needs to select the network name (SSID) and input a pre-configured passphrase to gain access to the wireless network.

When a WLAN Client initially accesses the wireless network, the Access Point - in its role as DHCP server - dynamically assigns the client an IP address. Because the WLAN Clients are located on their own subnet, WLAN Clients are not able to transmit broadcasts or other unwanted data traffic that might flood the wired network backbone.

The tasks to be performed in this configuration example include:

- Create a new configuration file (`AP-2.lcf`) by copying the previously created file (`AP-1.lcf`).
- Edit the existing 'INTRANET' IP network to serve exclusively as wired LAN.
- Create and configure a new DHCP network to serve exclusively as wireless LAN.

3.3.1 Creating a New Configuration File

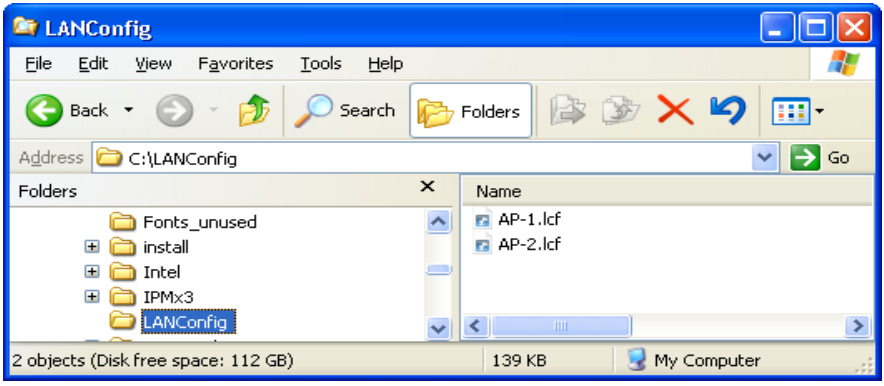
To create a new LANconfig configuration file, follow these steps:

☐ In Windows Explorer, navigate to the folder where the file `AP-1.lcf` is located and copy it.

☐ Paste the copied file into your choice of folder in Windows Explorer.

☐ Rename the new file `AP-2.lcf`.

If you copied the new file into the same folder as the old one, Windows Explorer contains the following files:

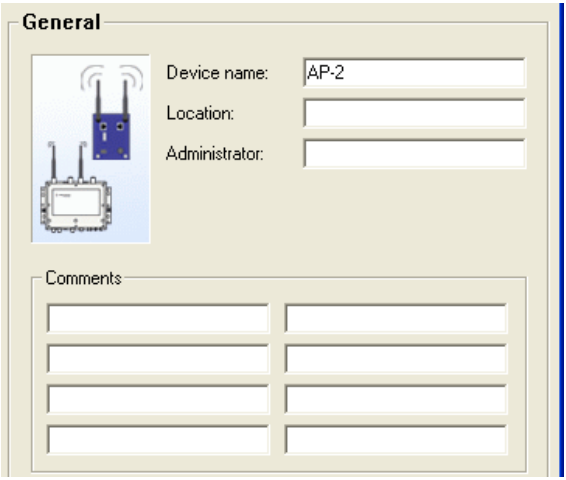


3.3.2 Changing the Existing Network to a Wired LAN

Configure the existing INTRANET IP network to serve exclusively as a wired LAN:

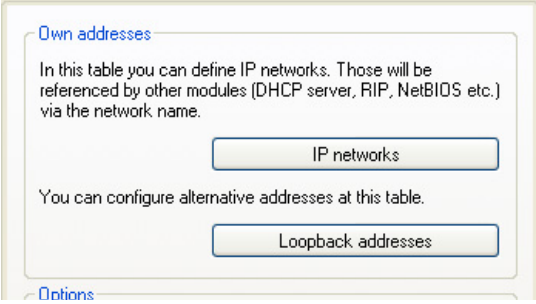
☐ In Windows Explorer, double-click the file `AP-2.lcf` to open it for editing.

☐ Open the `Configuration : Management : General` dialog:

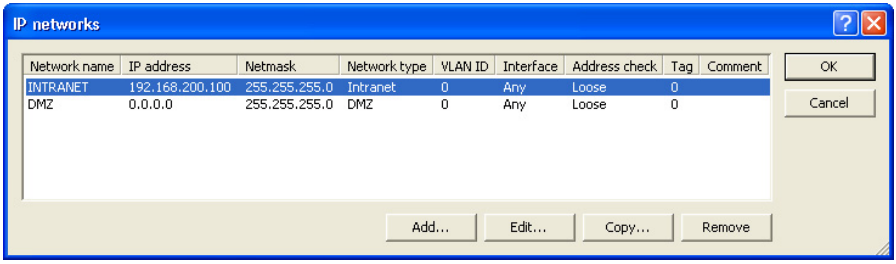


Change the Device name to ’AP-2’.

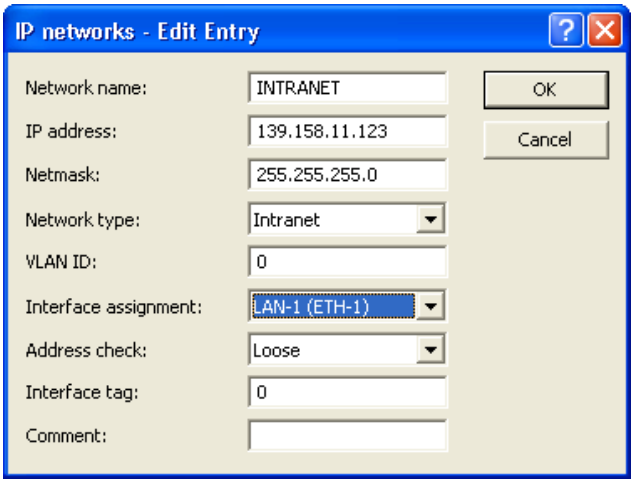
☐ Open the `Configuration : IPv4 : General`.



Click the ’IP networks’ button (above) to open the ‘IP networks’ window (below):



☐ Select the 'INTRANET' network in the list, then click on 'Edit...' to open the 'Edit Entry' dialog, below:

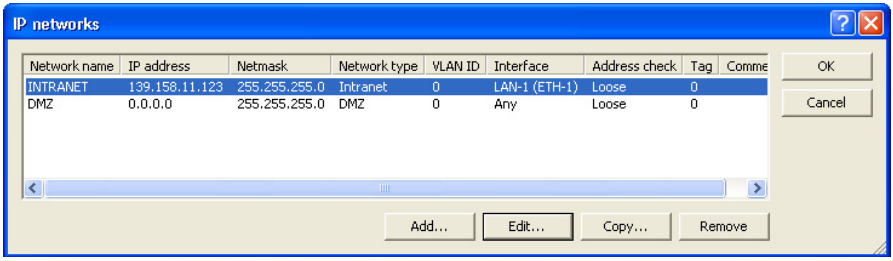


Convert the existing INTRANET network to a wired Ethernet LAN by editing the following settings:

– IP address: 139.158.11.123

– Interface assignment: LAN-1 (ETH-1)

Click 'OK' to close the 'Edit Entry' dialog and return to the 'IP networks' window, below:



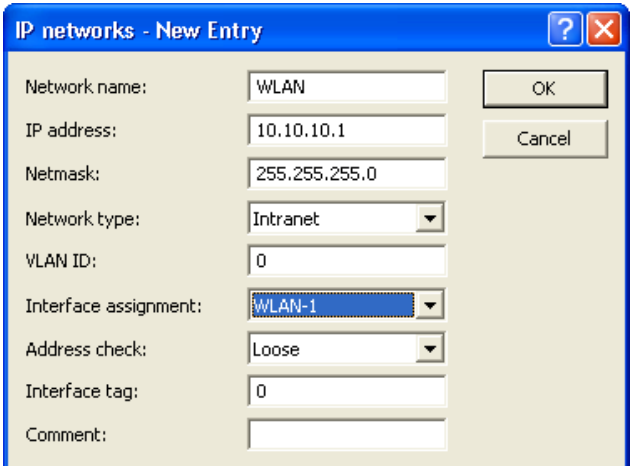
Leave the ‘IP networks’ window open.

3.3.3 Create a New DHCP Wireless LAN

Next, create a new DHCP network to be used exclusively as a Wireless LAN:

☐ In the ‘IP networks’ window, click ’Add...’ to open the ‘New Entry’ dialog.

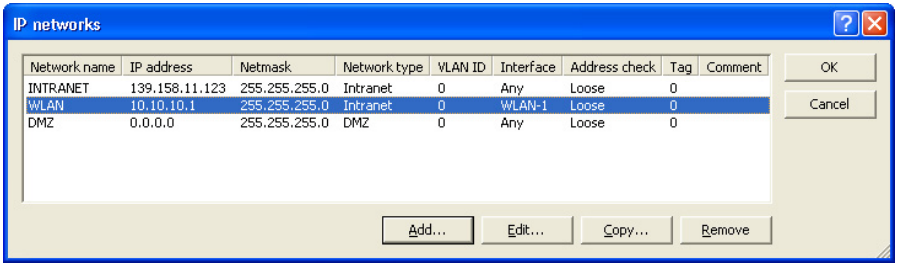
☐ In the ‘New Entry’ dialog, below, create a new wireless LAN network:



Enter the following settings for the new wireless LAN network:

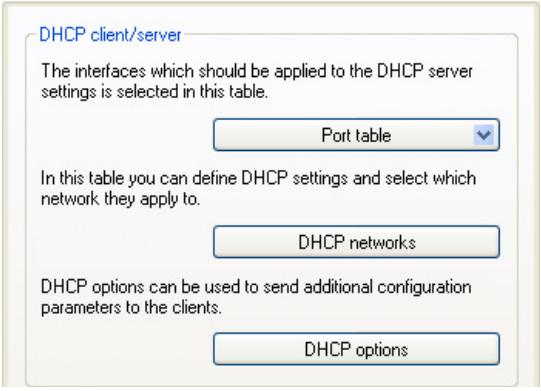
– Network name: 'WLAN'
– IP address: '10.10.10.1'
– Network type: 'Intranet'
– Interface assignment: 'WLAN-1'

Click 'OK' to close the 'New Entry' dialog and add the new wireless LAN network to the IP network list (below):

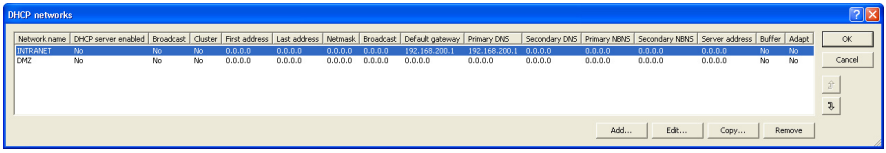


Click 'OK' again to close the 'IP networks' window (above).

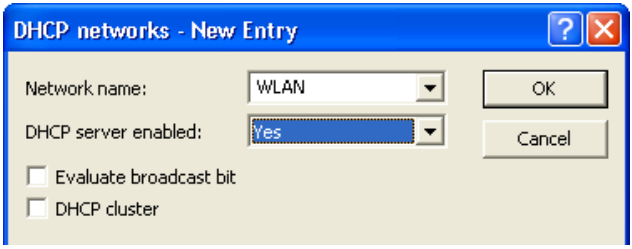
☐ The DHCP server is enabled inside the `Configuration : IPv4 : DHCPv4` dialog.



Click the 'DHCP networks...' button (above) to open the 'DHCP networks' window (below):



☐ In the ‘DHCP networks’ window (above), click ’Add...’ to open the ‘New Entry’ dialog (below):

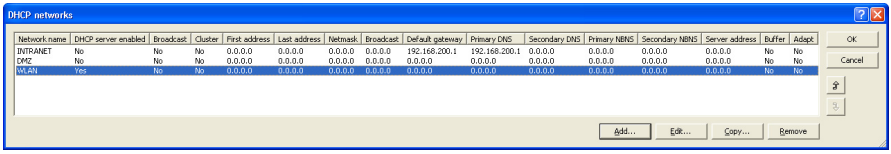


Edit the following fields by making the following selections:

– Network name: ’WLAN’

– DHCP server enabled: ’Yes’

Click ’OK’ to close the ‘New Entry’ dialog.
A new DHCP network appears in the DHCP networks window, below:



☐ Click ’OK’ to close the DHCP networks window.

Click ’OK’ again to close the LANconfig file and save your edits.

The `AP-2.lcf` file is configured for use as both a Wireless access point and a DHCP server.

3.4 Wireless Client

This example shows you how to configure a OpenBAT device that is designed exclusively for the role of WLAN Client. The most significant settings to be configured are the:

– SSID or name of the wireless network to which the Client will be connected, and

– DHCP mode (in this case DHCP client), indicating the source of the device's IP address settings

The following tasks are described in this example:

- Create a new LANconfig file
- Configure basis settings for the client device
- Configure WLAN settings for the client device

3.4.1 Creating a New LANconfig File for a Client

Follow these steps to create a new client LANconfig file:

In either case, the 'New Configuration File' dialog opens. Follow the work-steps, set forth below, to create a new LANconfig file.

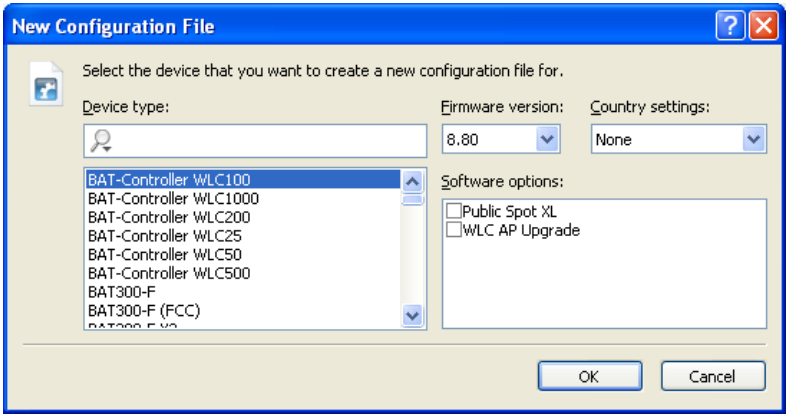
☐ In Windows Explorer, do the following:

☐ Navigate to, or create, a folder where you save the new client LANconfig file. In this example, the file is stored in the folder 'C:\LANconfig'

☐ Click the right mouse button, then select:
`New : LANconfig Configuration`

The New Configuration File dialog opens.

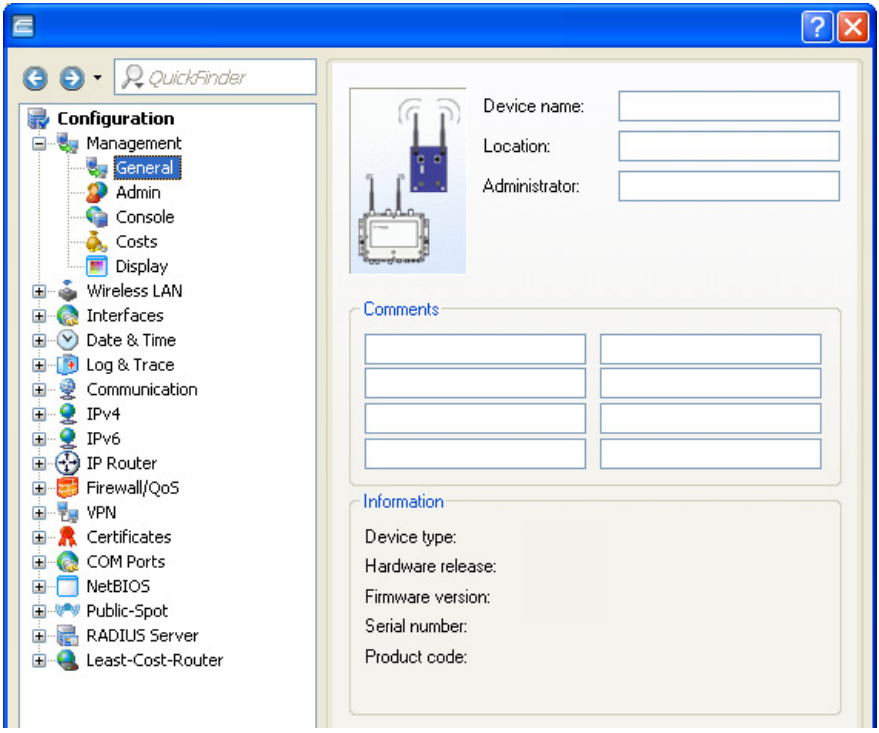
☐ In the 'New Configuration File' dialog, specify both the 'Device type' and the 'Firmware version' of the OpenBAT device you want to configure:



In this example, do the following:

– Device Type: Select a device.
– Firmware version: 8.80
– Country settings: Select a country. To ensure your device operates WLAN networks with the correct parameters, the device must be introduced to its national site. If you don't select any country settings, the device will allow only parameters that are permitted worldwide!
– Software options: Add configuration settings for additionally purchased software options to the basic configuration dialog by selecting its dedicated entry.
– Click 'OK'.

The following dialog opens:

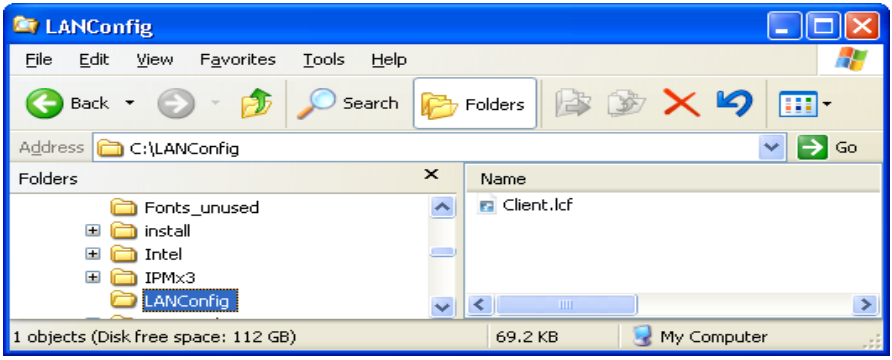


☐ Do the following:

☐ Type in a Device name. In this example, type in 'Client'.

☐ Click 'OK' to save the device configuration file.

☐ In Windows Explorer, navigate to the new file (`New LANconfig Configuration.lcf`, and change its name to `Client.lcf`:



You have created and saved a new LANconfig file. The following sections describe how to configure this file for use as a wireless client.

3.4.2 Configuring Basic Settings

Use the LANconfig Setup Wizard to configure the following basic settings for the device configuration file:

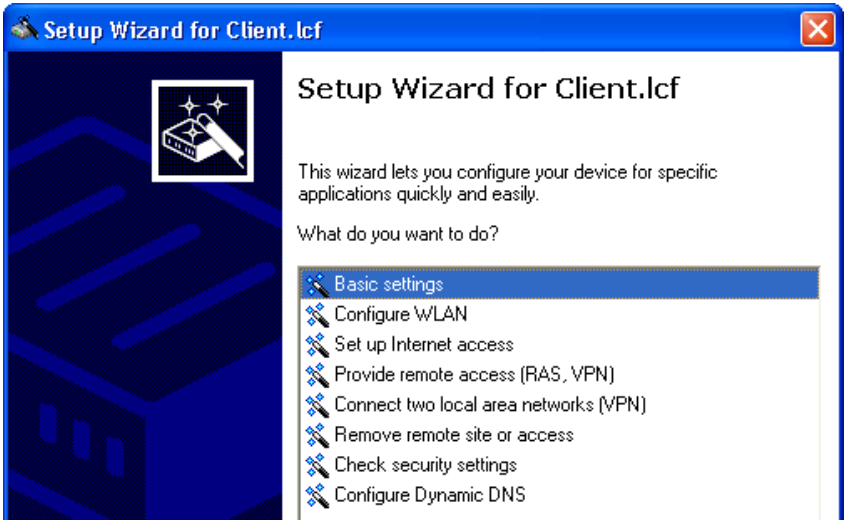
– device name
– password
– DHCP mode
– TCP/IP settings
– time synchronization settings
– optional device descriptions

☐ To start the Setup Wizard:

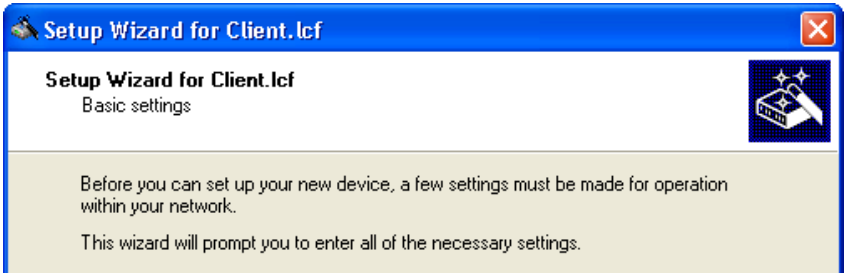
– In Windows Explorer, select the newly created LANconfig file, then

– Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the Setup Wizard, select 'Basic settings':

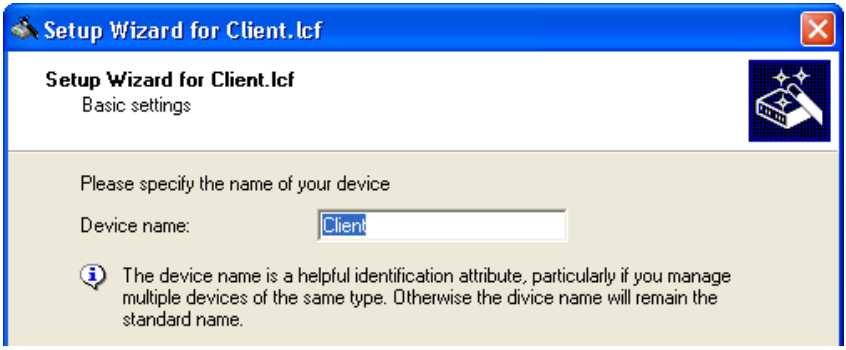


☐ Click 'Next'. The wizard displays the following introduction:



Click 'Next'.

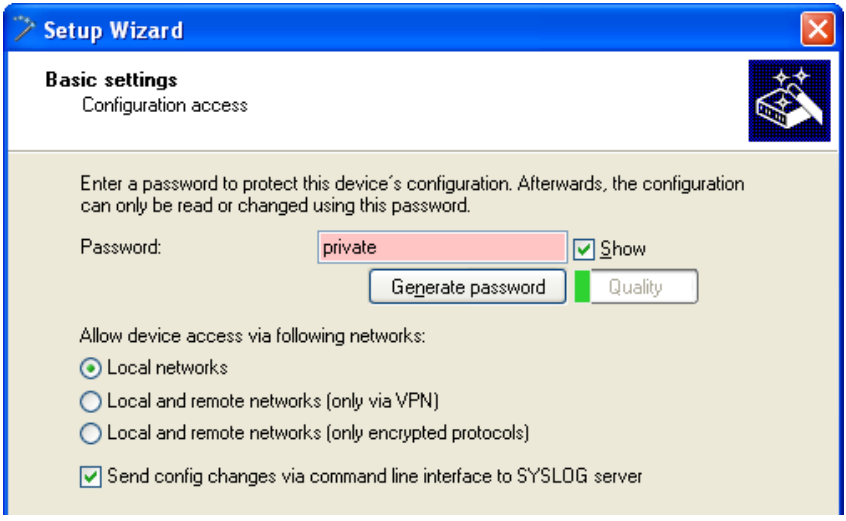
☐ Input a device name:



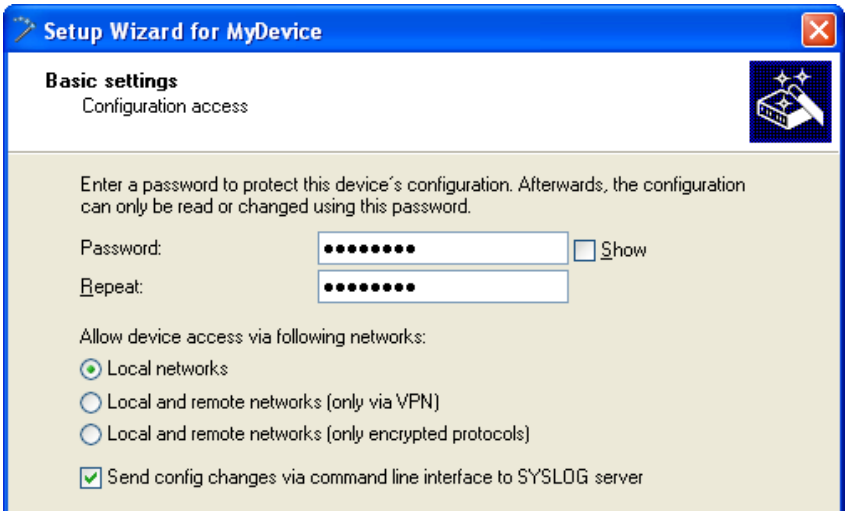
For the purpose of this example, use the name ’Client’.

☐ Click ’Next’. The following screen opens, where you need to enter a password in one of the following ways:

▶ Select ’Show’ (below) to display the default password (’private’) then do one of the following:
- accept the default password
- type in a new password
- click ’Generate password’ to let the wizard input a new password



- De-select 'Show' (below) then either accept the default password ('private') or type in a new one. In either case, re-type the password in the 'Repeat' field.

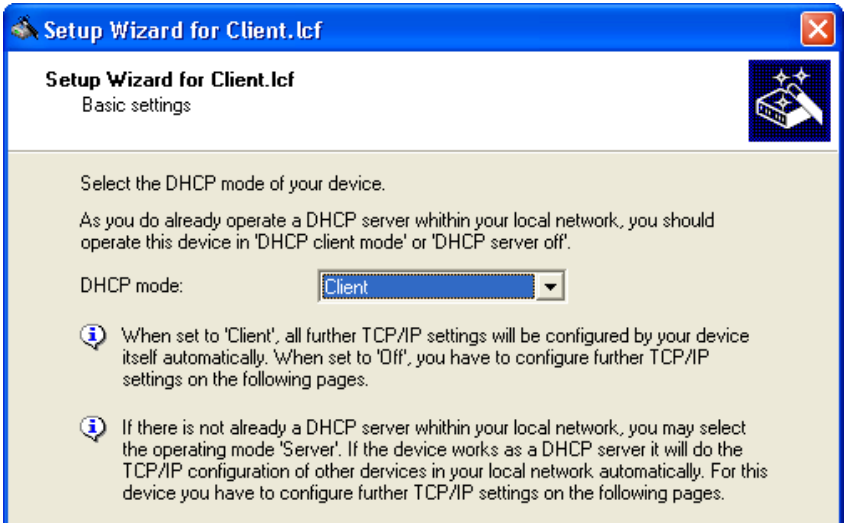


- Set the networks permitted to access the device. If you restrict access to local networks, only PCs that are directly connected to the local area network by cable or wireless can access the device configuration.

Note: The assistent indicates the different security levels of passwords color-coded. Insecure passwords are highlighted in red, conditionally secure ones are highlighted in yellow, and secure to very secure ones are highlighted in white.

In this example, accept the default password, then click 'Next'.

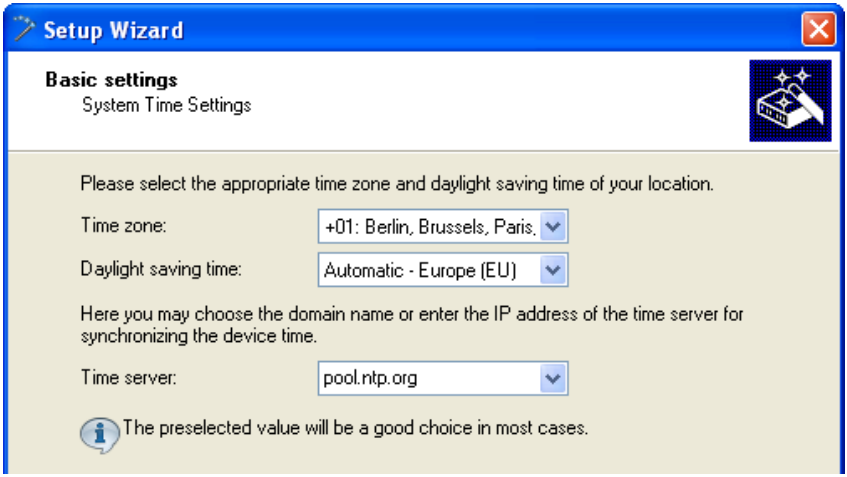
☐ Configure the OpenBAT device as DHCP client:



When the device is turned on, it will request its IP address settings from a DHCP server on the network.

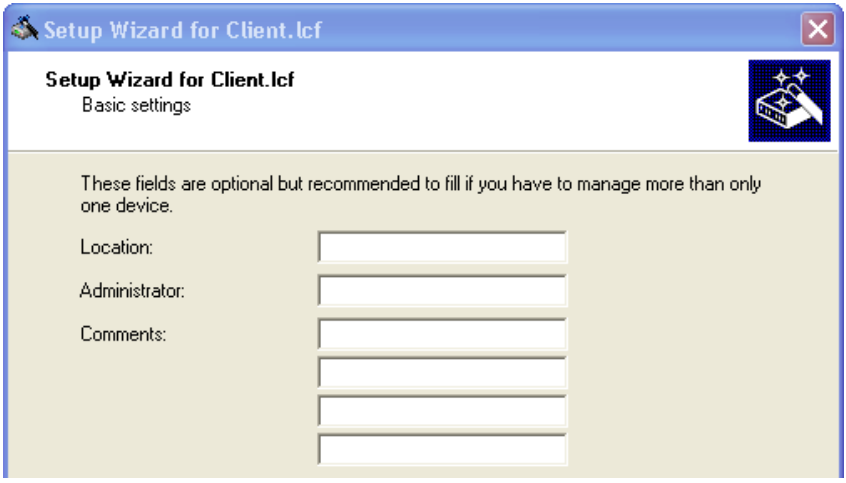
Click ’Next’.

☐ The wizard prompts you to identify your national timezone, prevailing changeover rules and a time synchronization server that will set the system time for the OpenBAT device:



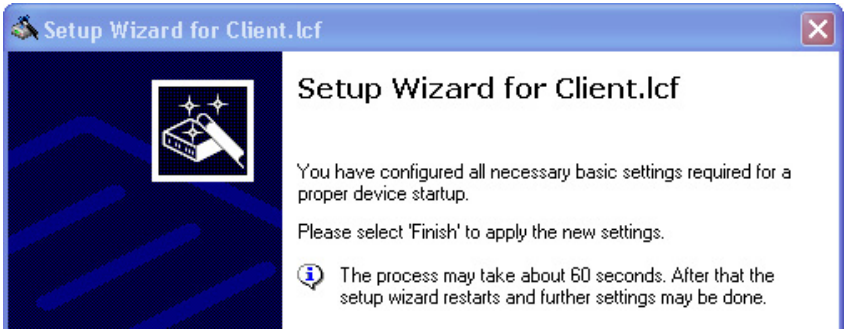
Select a time server from the list, or type in its IP address.

☐ Click 'Next'. The wizard shows the following screen for optional information on the location of the device, its administrator, and any comments relating to the OpenBAT device.



Click ’Next’.

☐ Click ’Finish’ to complete configuration of the basic settings (below):



3.4.3 Configuring Wireless LAN Settings

WLAN settings can be made using either the LANconfig tool's discrete configuration screens or the Setup Wizard. This task is most easily accomplished using the wizard.

☐ To start the setup wizard:

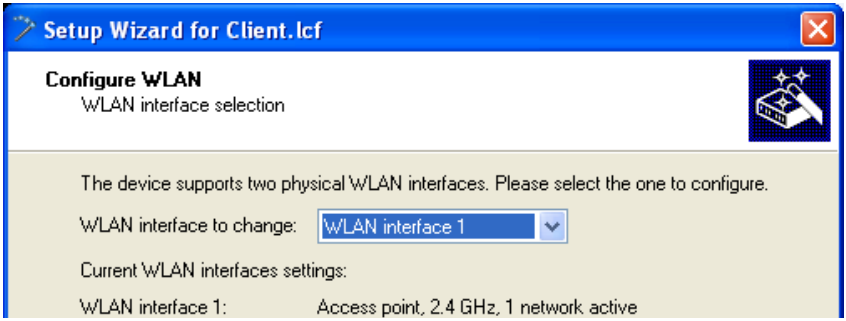
– In Windows Explorer, select the `Client.lcf` configuration file, then

– Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the LANconfig Setup Wizard:

☐ select 'Configure WLAN'

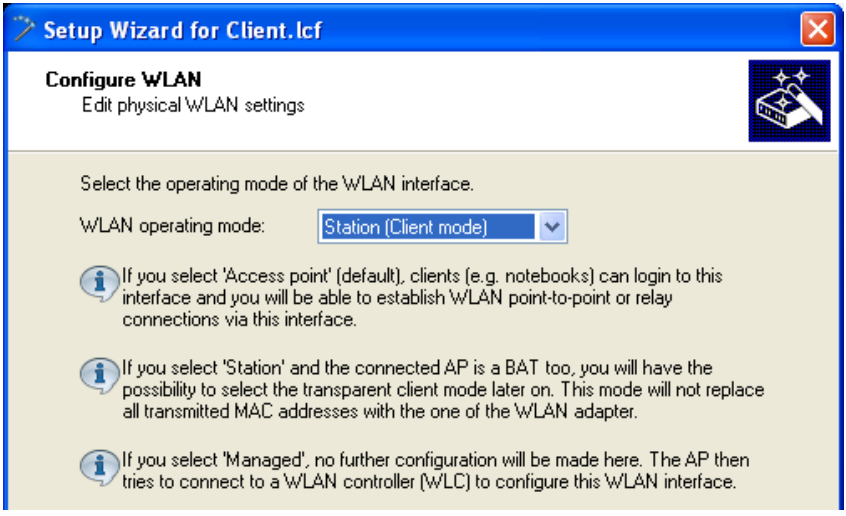
☐ click 'Next' two times, or until the wizard displays the WLAN interface selection screen



Select 'WLAN interface 1' as the 'WLAN interface to change'.

Click 'Next'.

☐ Specify an operation mode for the interface (WLAN interface 1):



WLAN operation modes include:

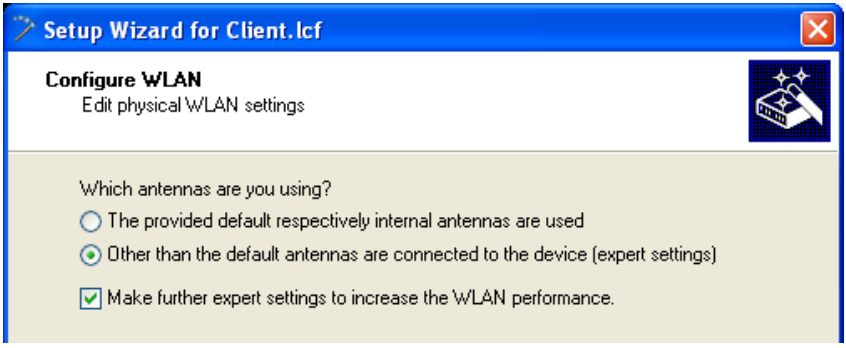
– Access Point:
The device serves as a base station, and can establish links to another access point (point-to-point), to remote clients, or to both remote access points and remote clients.

– Client:
The device serves as Client and needs to log into an Access Point. In this role, the device can link a cabled network to a WLAN over a wireless connection.

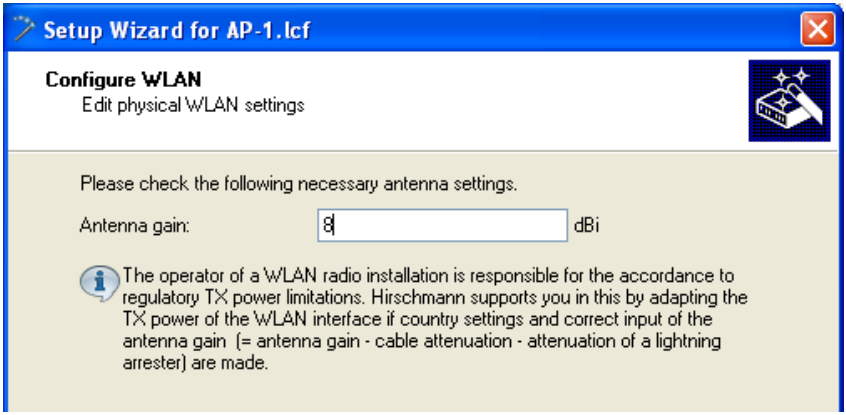
– Managed (Access point):
The device operates as an Access point, but searches for a central WLAN controller it can obtain a configuration from.

Select 'Client', then click 'Next'.

☐ Check the antenna settings:

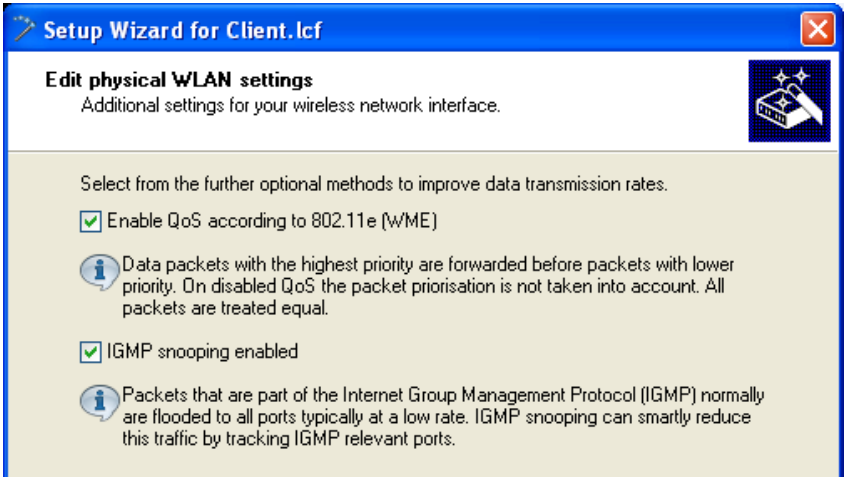


☐ Check the antenna settings:



the calculated antenna gain is 8 dBi for this example

☐ Click 'Next'.
The wizard presents settings that can be used to increase data transmission rates:



You can enable or disable the following services:

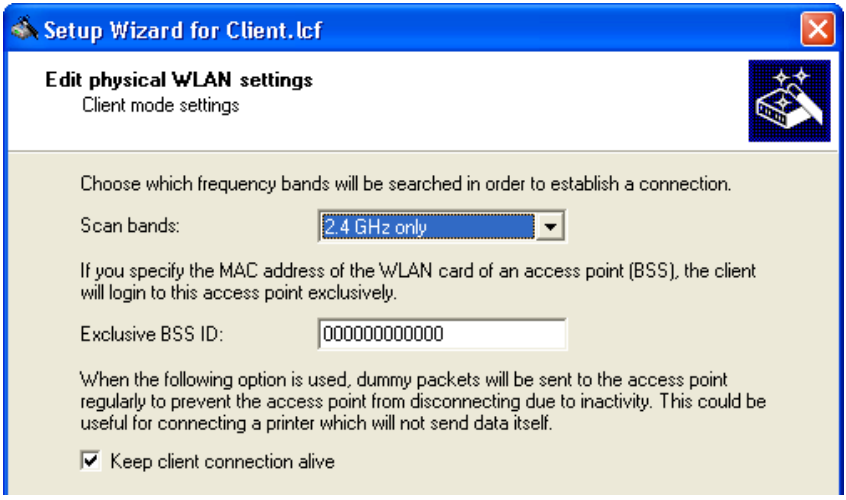
– QoS

– IGMP Snooping

For the purpose of this example, all available data rate enhancing options are selected.

Click ’Next’.

☐ The wizard presents the following screen:



In this screen, enter settings for the following fields:

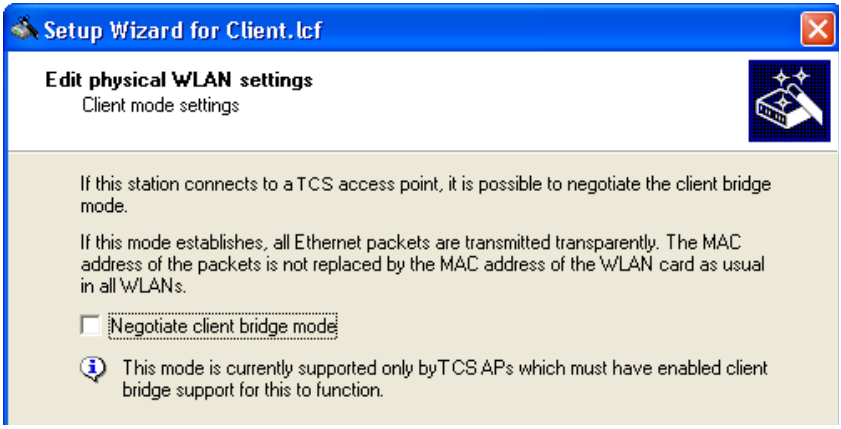
– Scan bands: Select the frequency bands to be scanned by the client when it attempts to establish a connection. In this example, select ’2.4 GHz only’.

– Exclusive BSS ID: If you want the client to connect to a specific access point, type in its MAC address. In this example, type in a value consisting exclusively of zeroes, indicating no device is specified, to configure a roaming client.

– Select ’Keep client connection alive’.

Click ’Next’.

☐ De-select the ’Negotiate client bridge mode’ option, below:



Client bridge support relates to a network design that consists of:

– an OpenBAT device in the role of Access Point

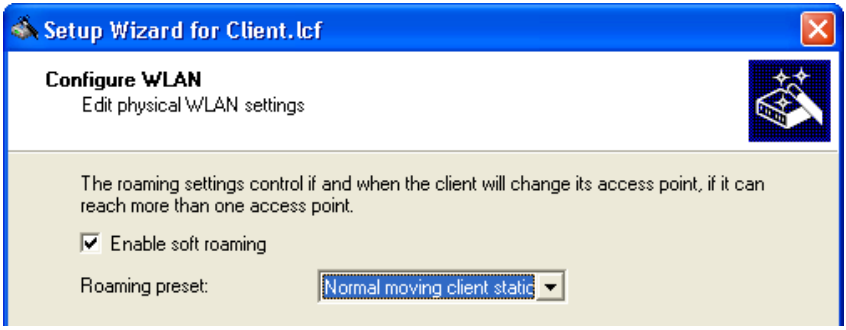
– an OpenBAT device in the role of Client

– one or more remote Ethernet devices connected to the Client OpenBAT device in Client mode

Typically, packets sent from a remote Ethernet device to the access point via the wireless client contain the MAC address of just the wireless client. Enabling client bridge support also includes in the packet the MAC address of the remote device.

For this example, de-select ’Negotiate client bridge mode’, then click ’Next’.

☐ Use the next screen to enable soft roaming for the client:



Enabling soft roaming helps provide a seamless transition for a wireless client when it roams between access points. Do the following:

– Select ’Enable soft roaming’

– Set the Roaming preset field to ’Normal moving client station’.

Click ’Next’.

☐ Enter the Network name (also known as the Service Set Identifier or ’SSID’):

For the purpose of this example, use the SSID ’Company_1’.

Click ’Next’.

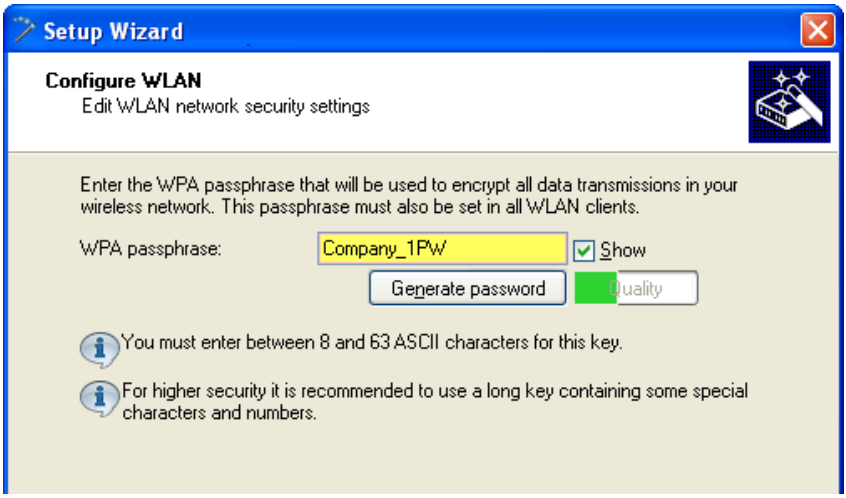
☐ Specify the transmission encryption protocol:

Note: Use WPA-2 for increased security.

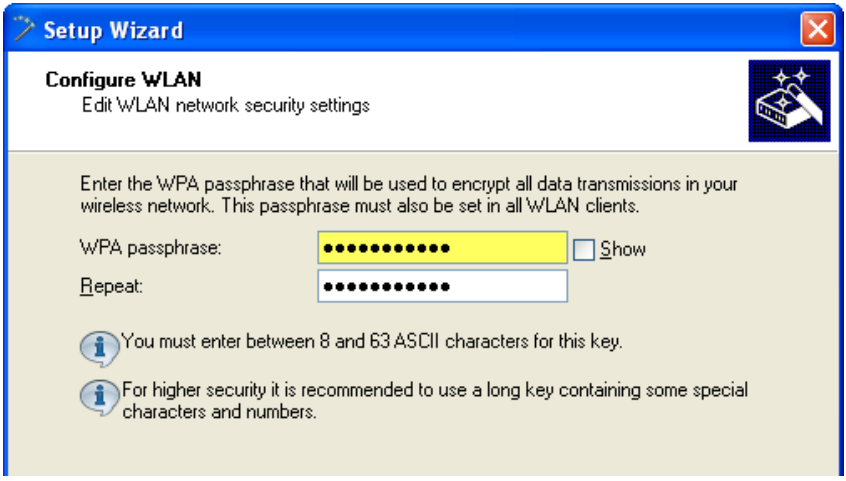
Click 'Next'.

☐ The following screen opens, where you need to enter a WPA passphrase in one of the following ways:

– Select 'Show' (below), then do one of the following:
  - type in a new WPA passphrase
  - click 'Generate password' to let the wizard input a new passphrase

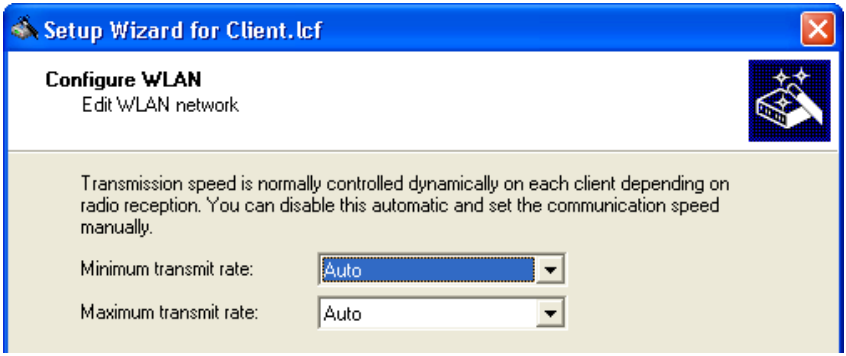


– De-select 'Show' (below) then type in a new WPA passphrase. In this case, re-type the password in the 'Repeat' field:



In this example, type in the passphrase 'CompanyPW', then click 'Next'.

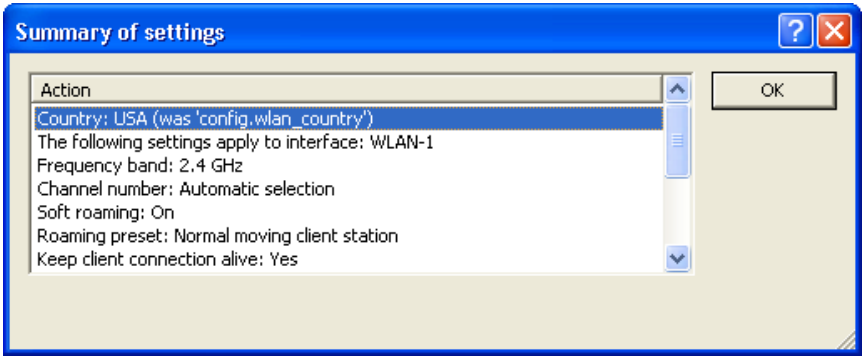
☐ Specify how transmission speed between the wireless client and any access point will be determined:



Select 'Auto' for both the Minimum transmit rate and the Maximum transmit rate, then click 'Next'.

☐ You are now ready to complete the configuration of the wireless client:

☐ Click on the 'Summary of settings...' button to display a list of all configuration settings for the wireless client device:

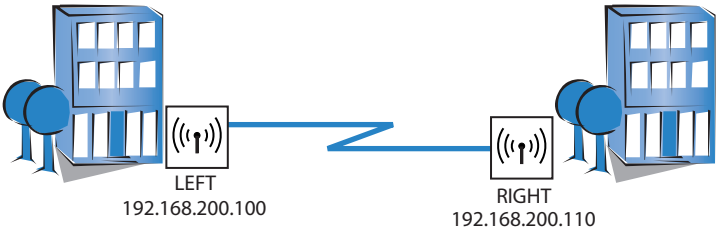


Click ’OK’ to close the Summary window.

Click ’Finish’ to complete the wizard and save the settings for this wireless client.

3.5 WLAN Bridge: Single Subnet

This example shows how to configure two OpenBAT devices as Access Points to form a point-to-point WLAN bridge connecting two segments of the same subnet. Each Access Point is configured to allow access only by its direct bridge partner. None of the devices is configured to provide routing functionality.



The significant configuration settings for each device are as follows:

Station Name:	LEFT	RIGHT
Role:	Access Point	Access Point
IP address:	192,168,200,100	192,168,200,110
Subnet Mask:	255.255.255.0	255.255.255.0
Channel Selection Scheme	Master	Slave
Point-to-Point Partner	RIGHT	LEFT

3.5.1 Configuring the LEFT Device

Create a new device configuration file using either the LANconfig software's individual configuration pages or its Setup Wizard. The easier approach is to use the Setup Wizard to configure the following groups device settings:

- Basic Settings
- WLAN Settings

Configuring Basic Settings

After you have created a new configuration file (see on page 48), the next task is to input the basic Ethernet communication settings for the OpenBAT devices. Basic settings include:

– device name
– password
– DHCP mode
– TCP/IP settings
– time synchronization settings
– optional device descriptions

☐ In Windows Explorer, do the following:

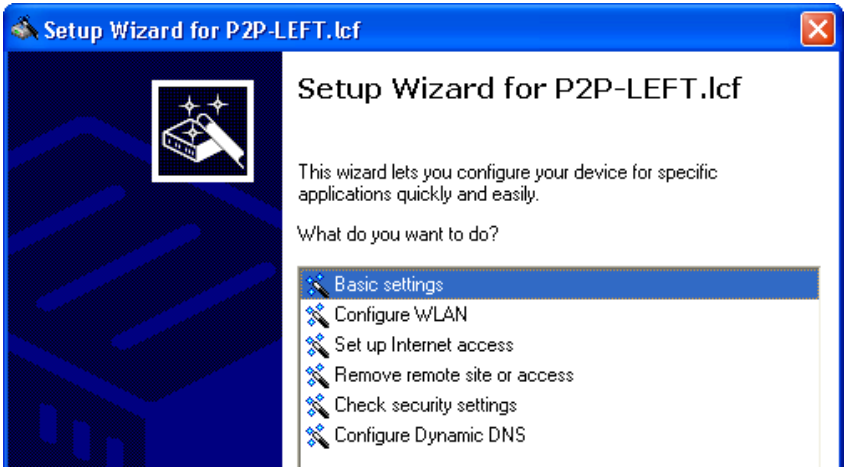
– Select the configuration file.

– Click the right mouse button and select `Rename`.

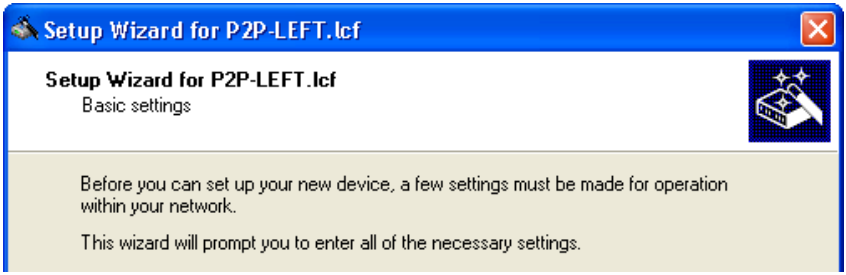
– Type in a new name for the file: `P2P-LEFT.lcf`.

☐ To start the Setup Wizard, click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the Setup Wizard, select 'Basic settings':

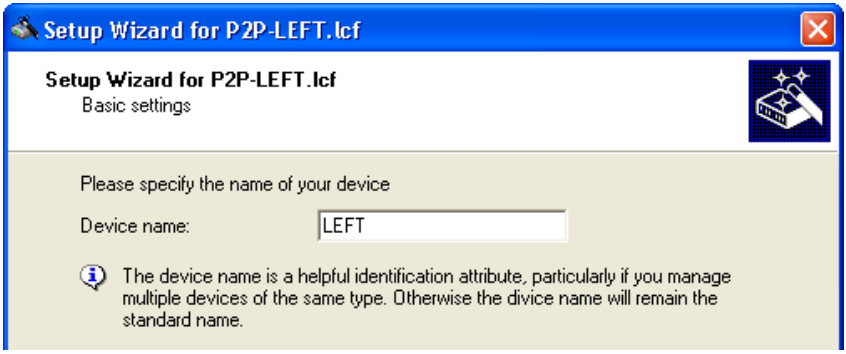


Click 'Next'. The wizard displays the following introduction:



☐ Click ‘Next’.

☐ Confirm the device name:

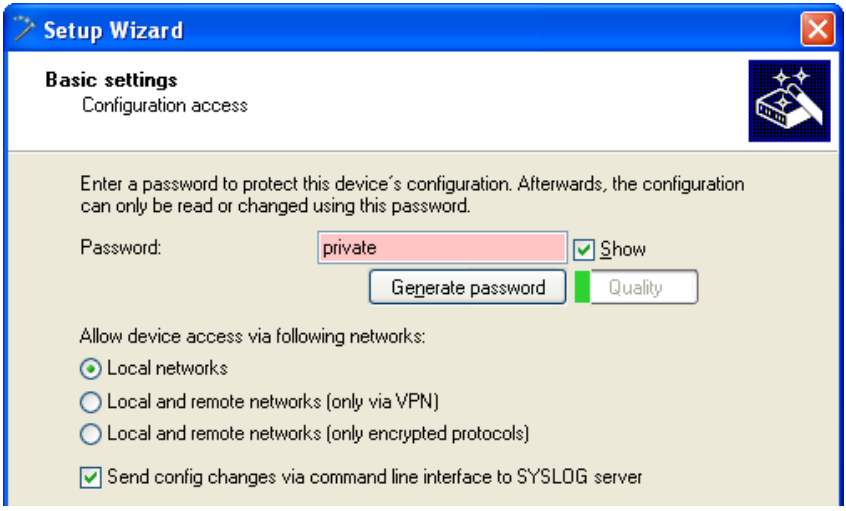


The wizard displays the Device name you previously input (’LEFT’).

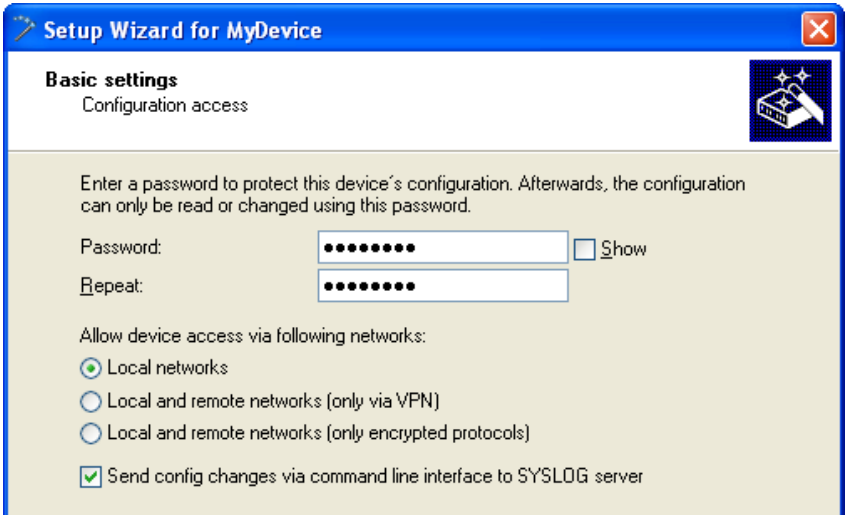
Note: The default device name is a concatenation of the device part number and the last 3 octets of the device MAC address.

☐ Click 'Next'. The following screen opens, where you need to enter a password in one of the following ways:

▶ Select 'Show' (below) to display the default password ('private') then do one of the following:
- accept the default password
- type in a new password
- click 'Generate password' to let the wizard input a new password



▶ De-select 'Show' (below) then either accept the default password ('private') or type in a new one. In either case, re-type the password in the 'Repeat' field.

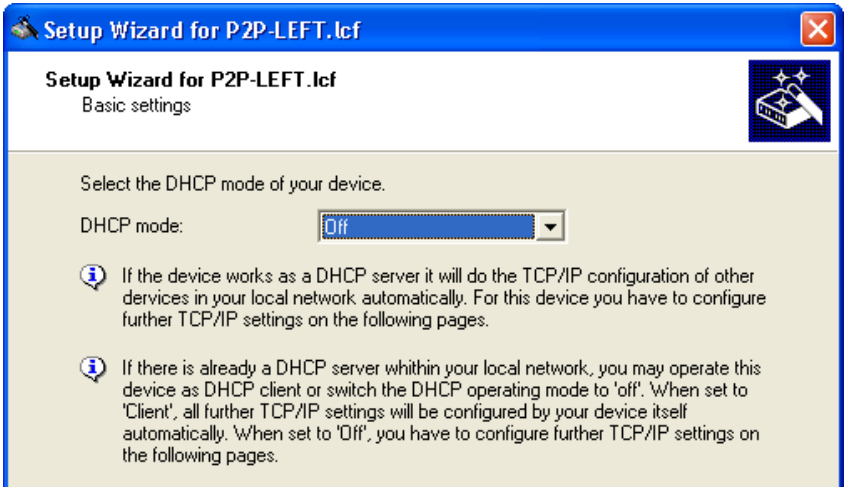


- Set the networks permitted to access the device. If you restrict access to local networks, only PCs that are directly connected to the local area network by cable or wireless can access the device configuration.

Note: The assistent indicates the different security levels of passwords color-coded. Insecure passwords are highlighted in red, conditionally secure ones are highlighted in yellow, and secure to very secure ones are highlighted in white.

In this example, accept the default password, then click ’Next’.

☐ Define the DHCP mode of the OpenBAT device:



Select one of the following DHCP modes:

– Off:
The device functions neither as DHCP client nor as DHCP server. In this mode, you need to manually input the IP address settings.

– Server:
The OpenBAT device functions as DHCP server, and assigns IP address settings to other network devices.

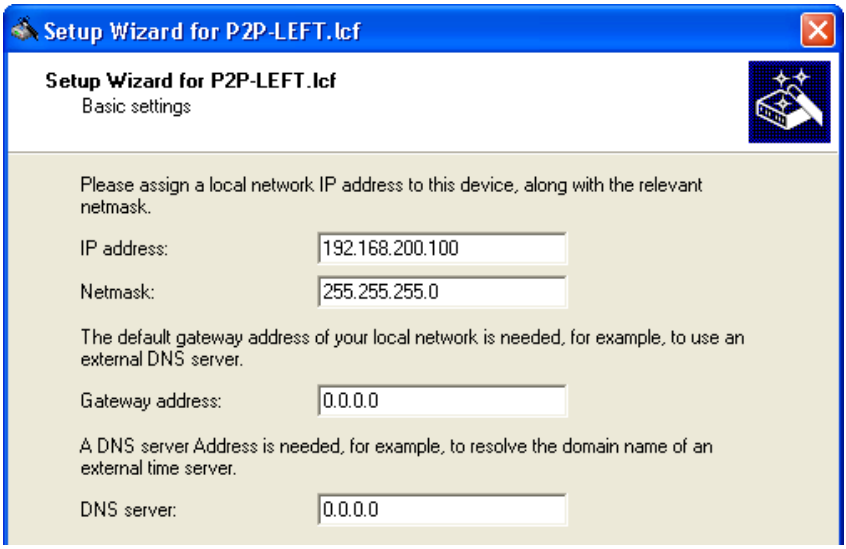
– Client:
This setting causes the OpenBAT device to request the IP address settings from a DHCP server on the network.

If a DHCP server exists on your network, select the ‘DHCP mode’ of ‘Off’. The default ‘DHCP mode’ setting of ‘Client’ can override a manually assigned IP address.

Note: Your DHCP mode selection determines the next screen displayed by the Setup Wizard.

Click ‘Next’.

- If you selected 'Off' for the DHCP mode, manually input the TCP/IP settings for the OpenBAT device:



Enter values for both the ’IP address’ and the ’Netmask’.
For the purpose of this example, these settings are:

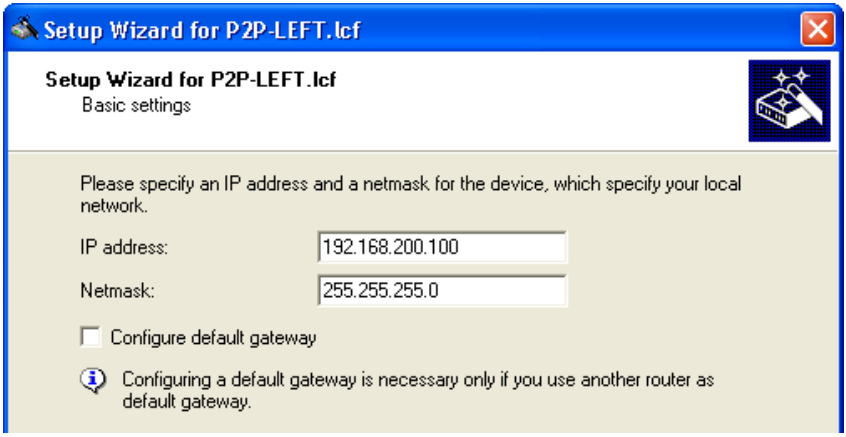
– IP address: 192.168.200.10

– Netmask: 255.255.255.0

Note: For a point-to-point link, settings for Gateway address and DNS server are not required.

Click ‘Next’.

- If you selected ’Server’ for the DHCP mode, the wizard displays the following screen for TCP/IP settings:



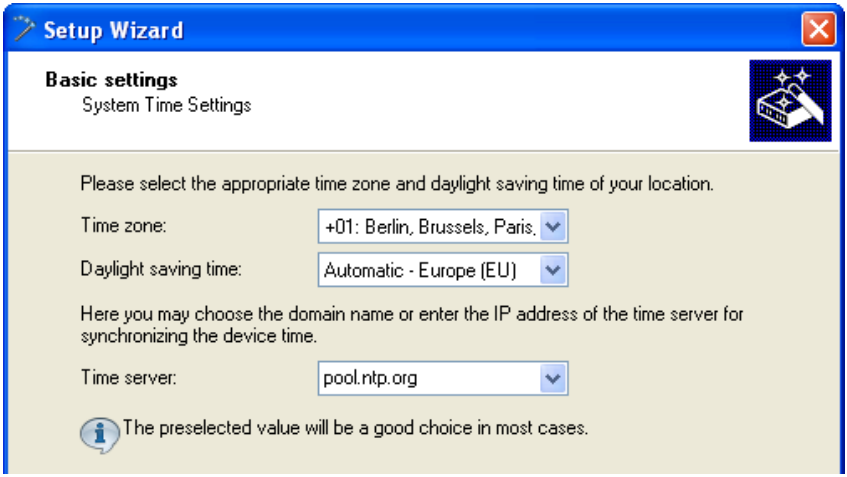
Do the following:

☐ Enter values for the ’IP address’ and ’Netmask’.

☐ For a point-to-point link, settings for ‘Gateway address’ and ‘DNS server’ are not required.

☐ Click ’Next’.

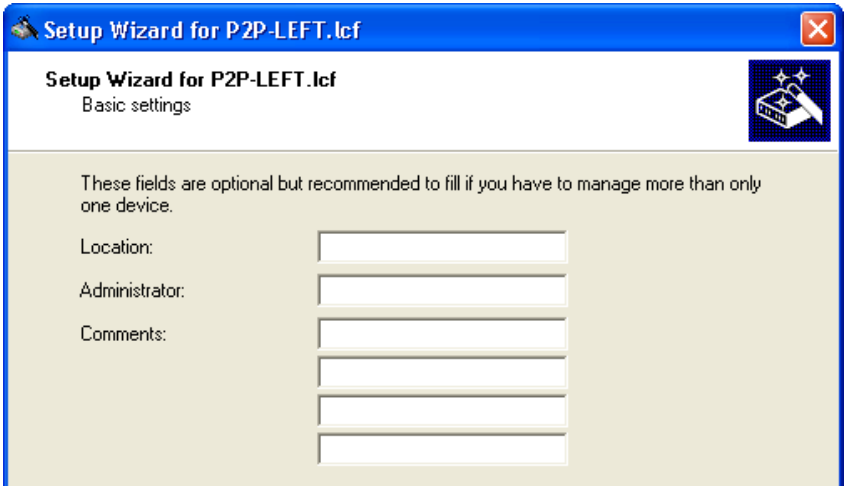
☐ The wizard prompts you to identify your national timezone, prevailing changeover rules and a time synchronization server that will set the system time for the OpenBAT device:



Select a time server from the list, or type in its IP address.

Click 'Next'.

☐ The wizard shows the following screen for optional information on the location of the device, its administrator, and any comments relating to the OpenBAT device.



Click ‘Next’.

☐ Click 'Finish' to complete the configuration of the basic settings (below):

Configuring WLAN Settings

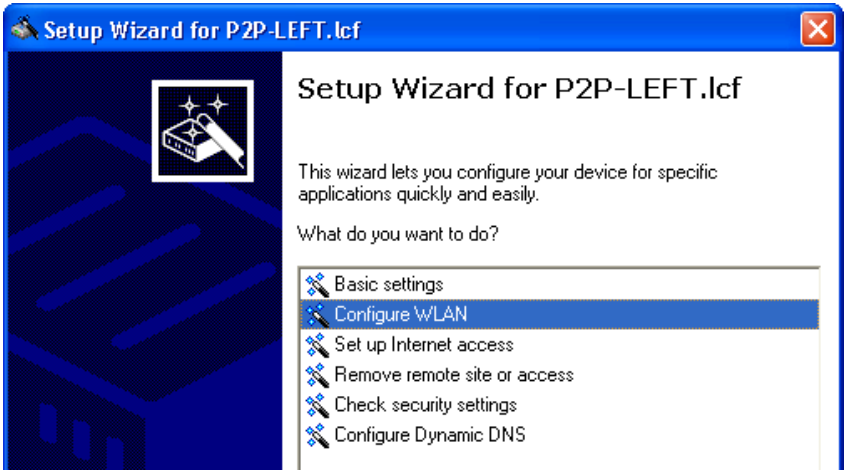
WLAN settings can be made using either the LANconfig tool’s discrete configuration screens or the Setup Wizard. This task is most easily accomplished using the wizard.

☐ To start the Setup Wizard:

– In Windows Explorer, select the `P2P-LEFT.lcf` LANconfig file, then

– Click the right mouse button to open a pop-up menu, then select `Setup Wizard`.

☐ In the wizard, select ’Configure WLAN’ (below):



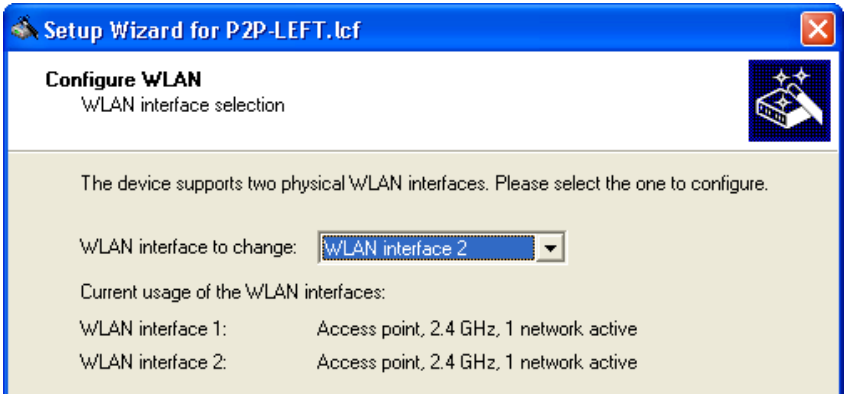
Click ‘Next’.

☐ Select the country in which the OpenBAT device is operated:

Note: The country designation determines both the available frequency bands, and the limits for output power considered by the device.

Click ‘Next’.

☐ The wizard prompts you to select a WLAN interface to configure:

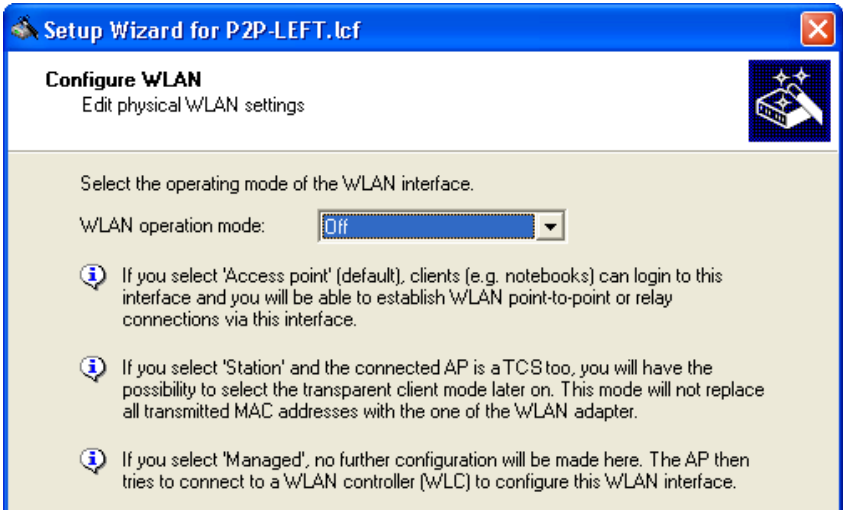


A device can have multiple WLAN interfaces. Here, the selected device has two interfaces. By default, both interfaces are enabled.

Note: You can configure just one WLAN interface at a time. After selecting interface 2, proceed through the wizard's remaining pages and finish configuration for that interface. Next, re-start the Configure WLAN wizard and configure interface 1.

Select 'WLAN interface 2' as the WLAN interface to configure, then click 'Next'.

☐ The next step is to enable or disable the selected WLAN interface:

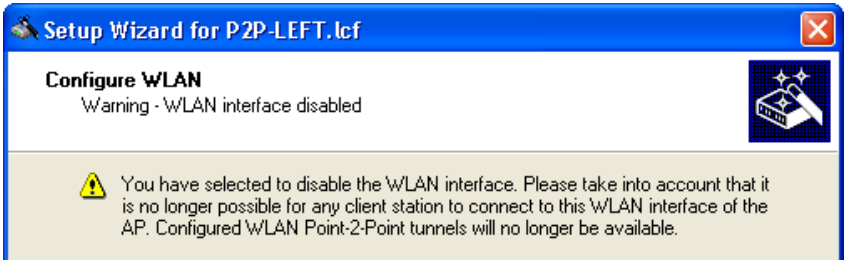


A point-to-point WLAN bridge requires just one interface. In this example, the currently selected interface—WLAN interface 2—will be disabled. (You will later configure WLAN interface 1 to support the point-to-point WLAN bridge.

Disable WLAN interface 2 by setting its 'WLAN operation mode' to 'Off'.

Click 'Next'.

☐ The wizard notifies you that you are about to disable interface 2:



Click ‘Next’.

☐ Complete the configuration of WLAN interface 2:

Click ’Finish’.

☐ Return to the Windows Explorer folder where the file LANconfig file is saved, then do the following:

– select the LANconfig file (`AP-1.lcf`)

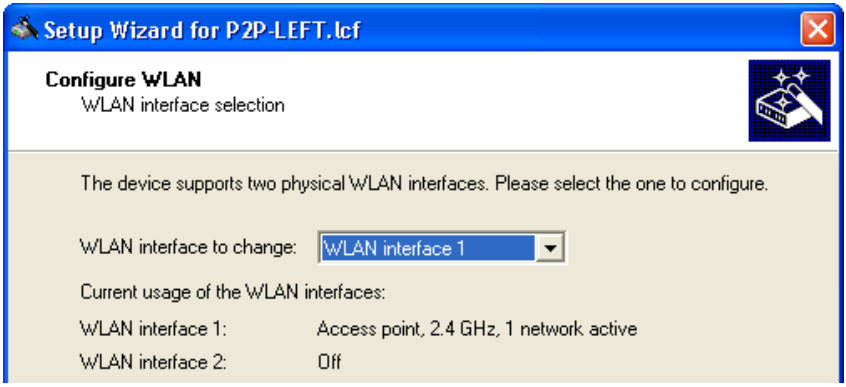
– click the right mouse button to open a pop-up menu

– select `Setup Wizard`

☐ In the LANconfig Setup Wizard:

– select ’Configure WLAN’

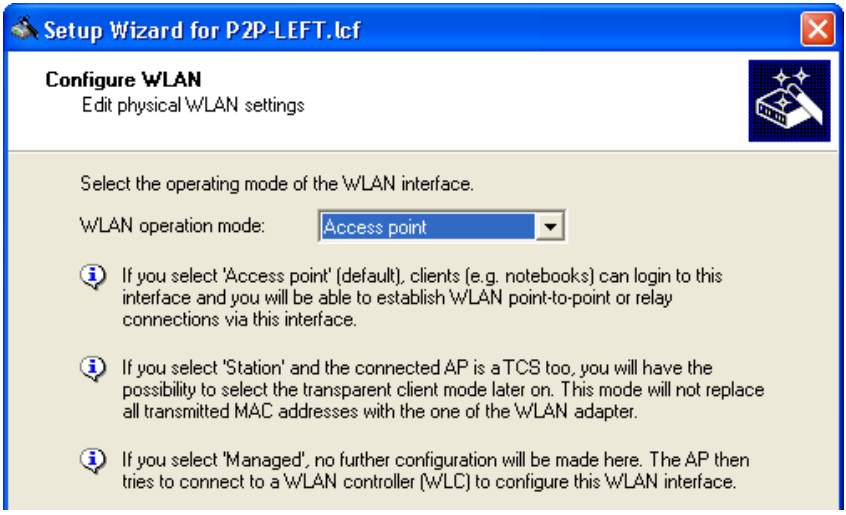
– click ’Next’ two times, or until the wizard displays the WLAN interface selection screen



Note: This screen indicates that WLAN interface 2 has been turned off. The next step is to configure WLAN interface 1.

Select 'WLAN interface 1' for the configuration and click 'Next'.

☐ Specify an operation mode for the interface (WLAN interface 1):



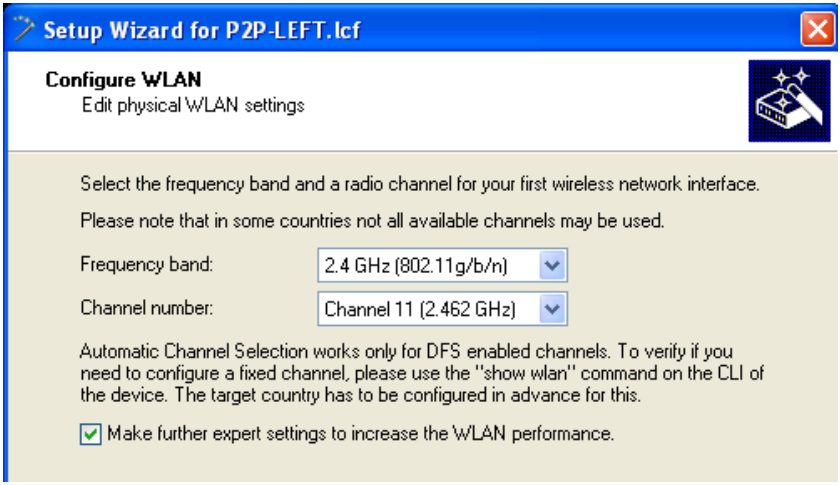
WLAN operation modes include:

– Access Point:
The device serves as Access Point and can establish connections to other Access Points (point-to-point), to remote clients, or to both Access Points and Clients.

– Client:
The device serves as Client and needs to log into an Access Point. In this role, the device can connect a cabled network to a WLAN over a wireless connection.

Select 'Access point', then click 'Next'.

☐ Enter settings for the wireless frequency and channels over which the device will operate, and indicate whether you wish to configure additional performance-enhancing settings:



The specific antennas you plan to use will determine how to complete this dialog. Depending upon the capacity of your chosen antennas, complete the following settings:

– Frequency band: 2.4 GHz or 5 GHz

– Channel number: A list of available channels. When the frequency band is set to 5 GHz, this field is set to 'Automatic selection'.

– Make further explicit settings to increase the WLAN performance: Selecting this causes the Configure WLAN wizard to display additional configuration screens relating to hardware compression, QoS and IGMP snooping.

For the purpose of this example, the settings displayed (above) are used.

Click 'Next'.

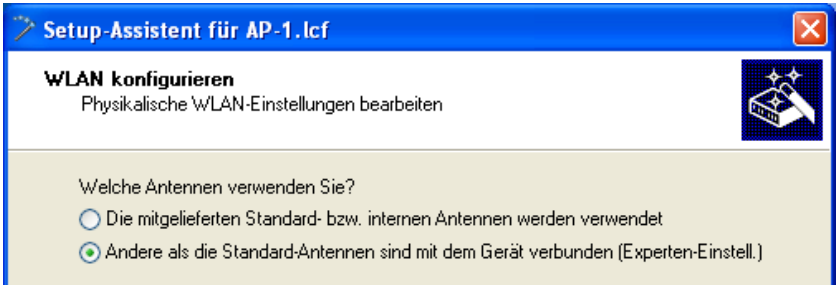
☐ The specific antennas you plan to use will determine how you complete this dialog. For the purpose of this example, enter the following settings:

– Frequency band: 2.4 GHz

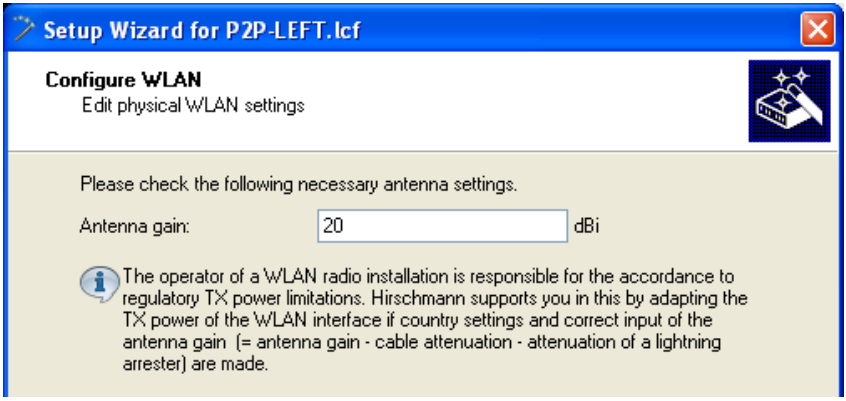
– Channel number: Channel 10 (2.457 GHz)

– Select 'Make further explicit settings to increase the WLAN performance'.
(This option gets the set-up wizard to display additional configuration screens for QoS and IGMP snooping.)

– Choose: 'Antennas other than the default antennas are connected to the device.'



☐ If you elected to use 'Other than the default antennas...', specify how your antennas will be used:



How you configure this dialog depends on:

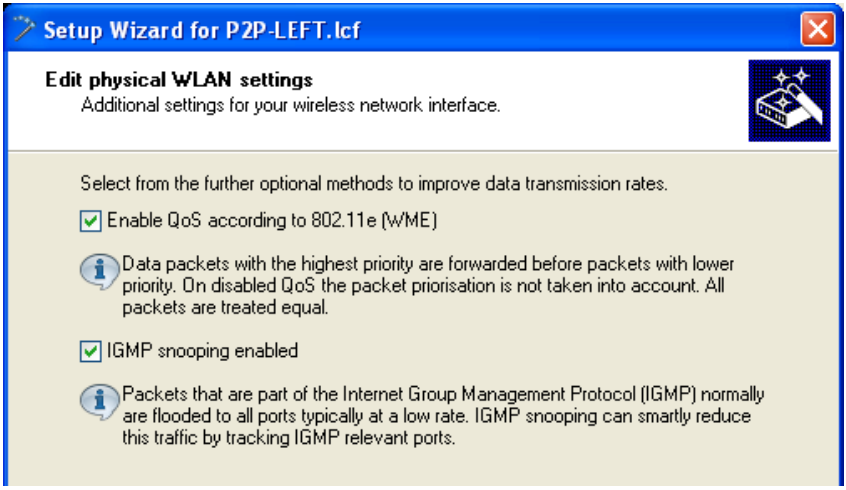
– the calculated antenna gain of the selected antennas

For the purpose of this example:

– antenna gain is 20 dBi

Click 'Next'.

☐ If you elected to 'Make further expert settings...', the wizard presents settings that can be used to increase data transmission rates:



You can enable or disable the following services:

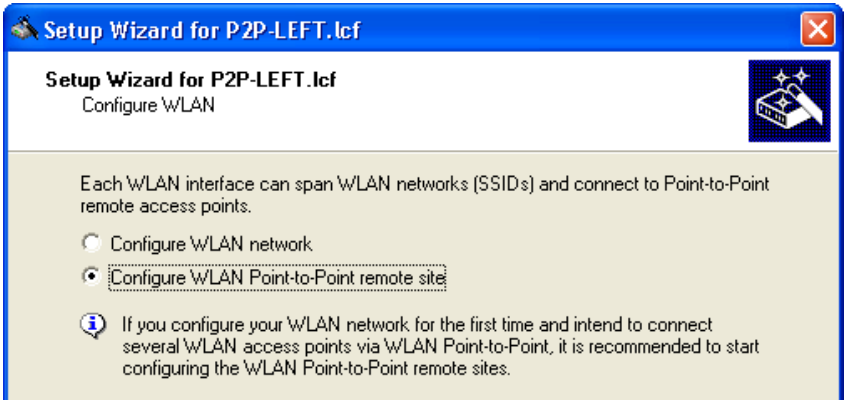
– QoS

– IGMP Snooping

For the purpose of this example, all available data rate enhancing options are selected.

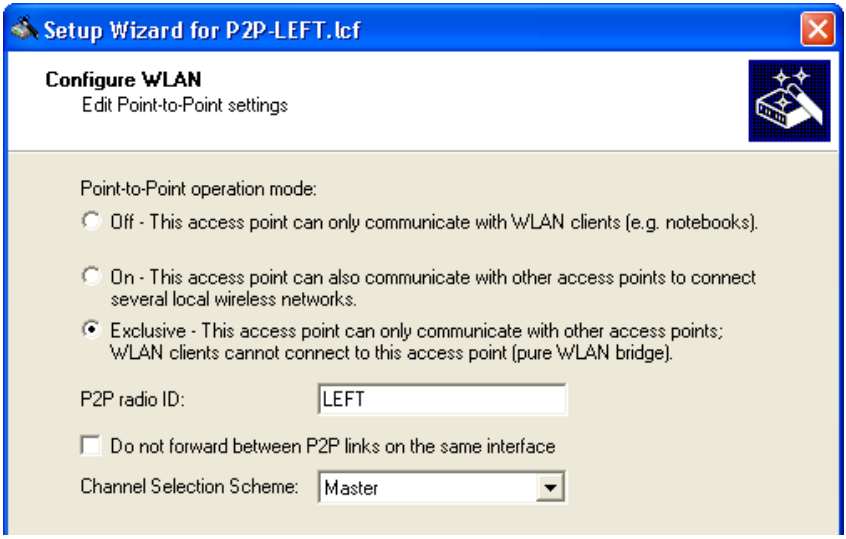
Click ‘Next’.

☐ Specify how this WLAN interface will be used:



Select 'Configure WLAN Point-to-Point remote site', then click 'Next'.

☐ Specify the devices that will be permitted to communicate with this OpenBAT device:



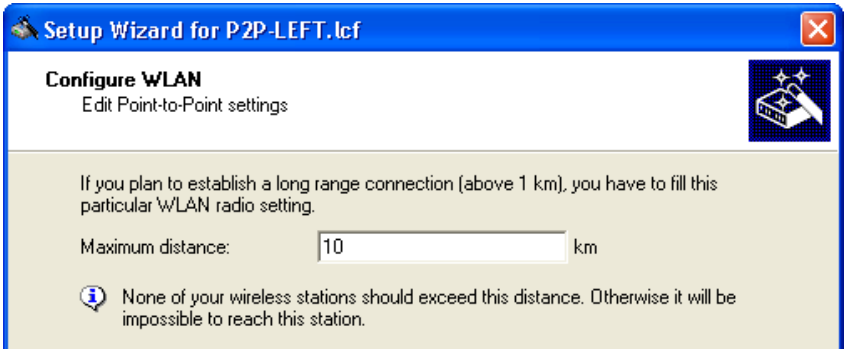
Configure the following configuration settings:

– Point-to-Point operation mode: determines which remote devices can wirelessly communicate with this WLAN device. The following options can be selected:
  - Off: only Clients
  - On: both Access Points and Clients
  - Exclusive: other Access Points exclusively
– P2P radio ID: a user-defined name for this OpenBAT device.
– Do not forward data between P2P connections of the same WLAN interface.
– Channel Selection Scheme: because both OpenBAT devices forming the point-to-point connection are Access Points, one needs to be configured as the master and one as the slave.

For the purpose of this example, the displayed settings (above) are selected.

Click ‘Next’.

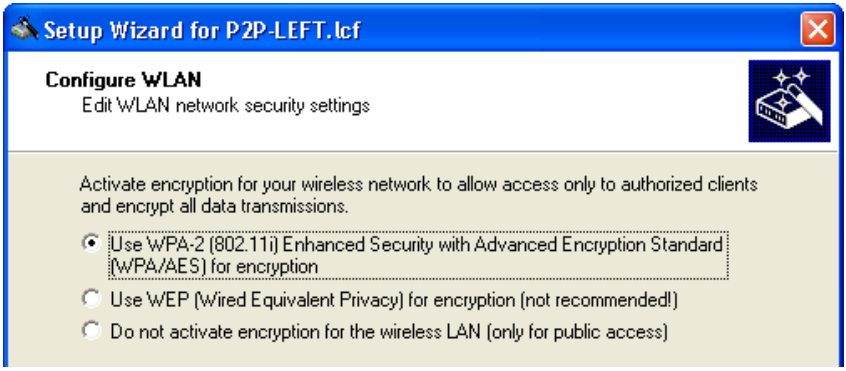
☐ Specify the maximum distance—in km—between the two access points forming the point-to-point WLAN bridge.



In this example, a value of 10 km is used.

Click ‘Next’.

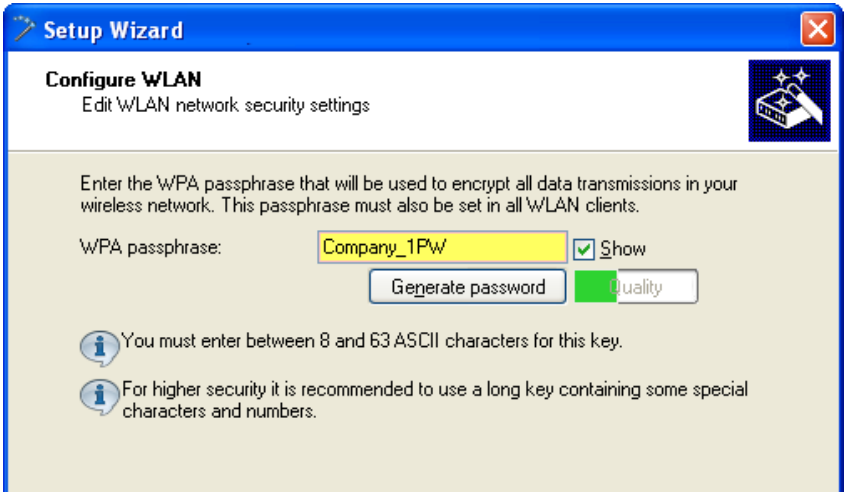
☐ Specify the transmission encryption protocol:



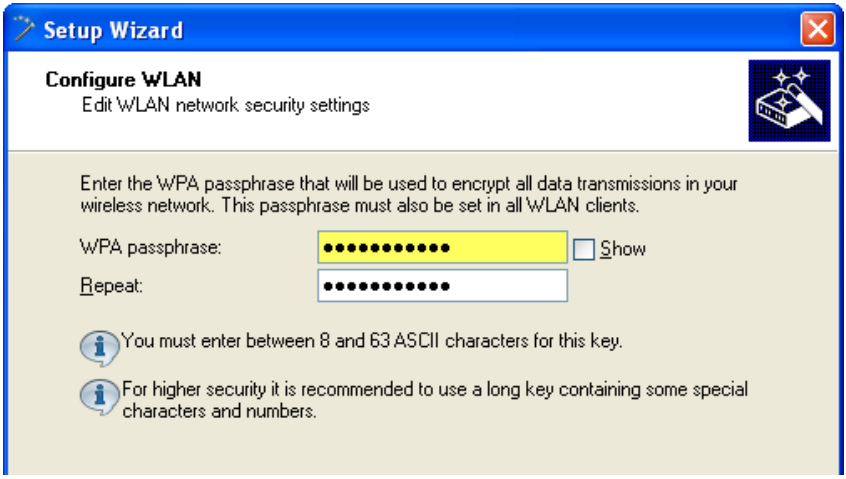
Note: Hirschmann recommends the use of WPA-2, to provide enhanced security.

Click ‘Next’.

- If you selected the WPA-2 encryption protocol, the following screen opens, where you enter a WPA passphrase—a string from 8 to 63 ASCII characters long—in one of the following ways:
  - Select ’Show’ (below), then do one of the following:
    - type in a new WPA passphrase
    - click ’Generate password’ and the wizard inputs a new string



  - De-select ’Show’ (below) then type in a new WPA passphrase. In this case, you also re-type the password in the ’Repeat’ field:



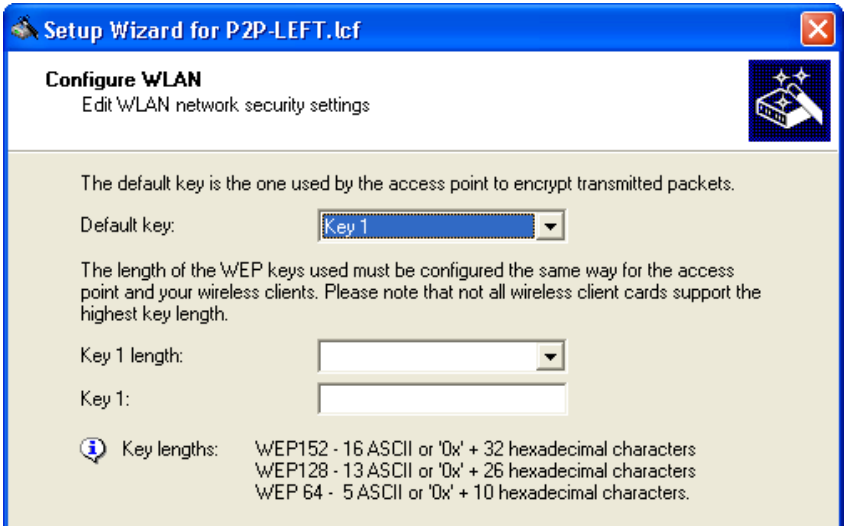
The role of the OpenBAT device in the point-to-point connection determines how the passphrase is used. If the device is configured as a:

– Master: the passphrase is used to check a slave's authorization to access the network.

– Slave: the passphrase is transferred to the Master to gain wireless access to the network.

In this example, type in the passphrase ’CompanyPW’, then click ’Next’.

▶ If you selected the WEP encryption protocol, the wizard prompts you to configure WEP keys:

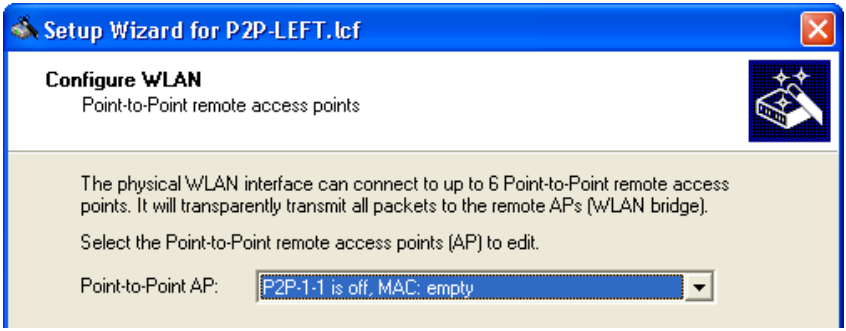


Use the WEP encryption configure the following settings:

– Default key: Select the key to be used for encrypting the packets sent by the access point. In this example, ‘Key 1’.
– Key 1 length: Select the key length to be used for the encryption of data packets on the WLAN. Please be aware that not every wireless card supports all key lengths.
– Key 1: Type in a passphrase value, for example, ‘private’.

Click ’Next’.

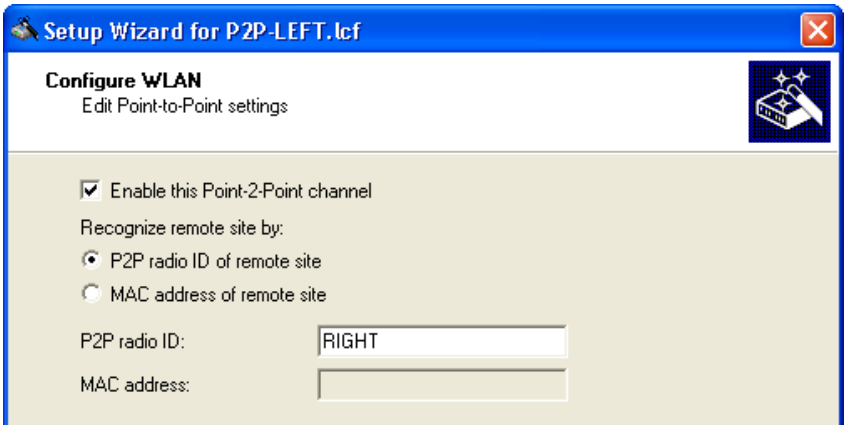
☐ Assign a point-to-point identifier to this WLAN interface:



Each OpenBAT device supports up to 6 point-to-point channels. Select an available point-to-point channel for this WLAN interface.

In this example, select the first available channel (’P2P-1-1’), then click ’Next’.

☐ Enable the assigned point-to-point channel:



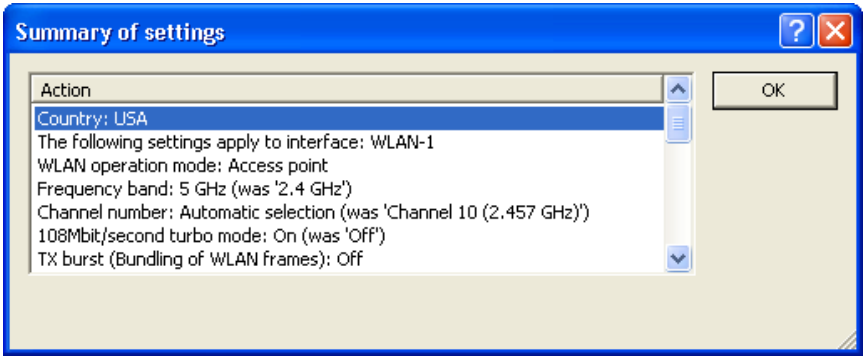
Select the ’Enable the Point-2-Point channel’ checkbox. Then indicate how to identify the remote access point at the other end of the point-to-point WLAN bridge, either by:

– its MAC Address
– a user-defined P2P radio identifier

In this example, use a user-defined P2P radio ID (’RIGHT’), then click ’Next’.

☐ You are now ready to complete the WLAN configuration.

Click on the 'Summary of settings... ' button to display a list of all the settings for this device.



Click 'OK' to close the summary.

Click 'Finish' to close the wizard and save your settings.

3.5.2 Configuring the RIGHT Device

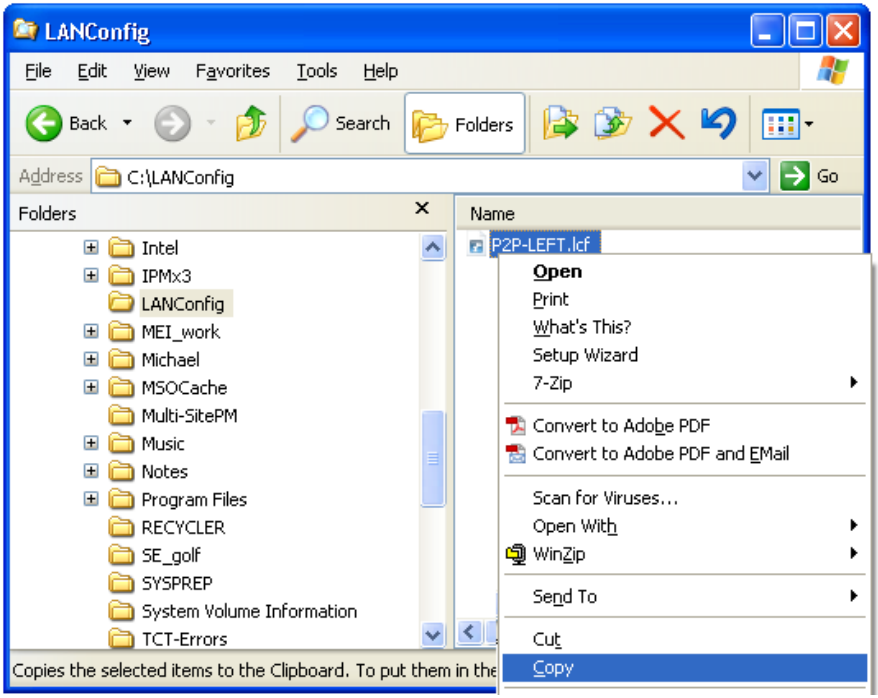
Both the LEFT and RIGHT OpenBAT devices are of the same device type equipped with the same firmware version. Consequently, the quickest way to create a configuration file for the RIGHT device is to copy the configuration file of the LEFT device and edit a few settings.

Creating a New Configuration File

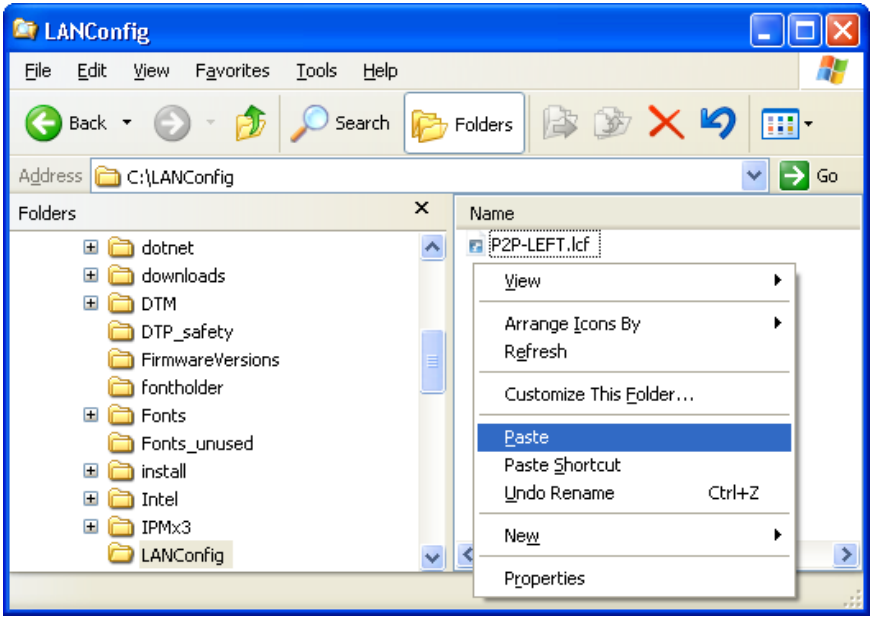
To begin the process of configuring the RIGHT device, locate the LANconfig file for the LEFT device on your PC's hard drive.

☐ Open Windows Explorer and navigate to the folder containing the LANconfig file `P2P-LEFT.lcf`.

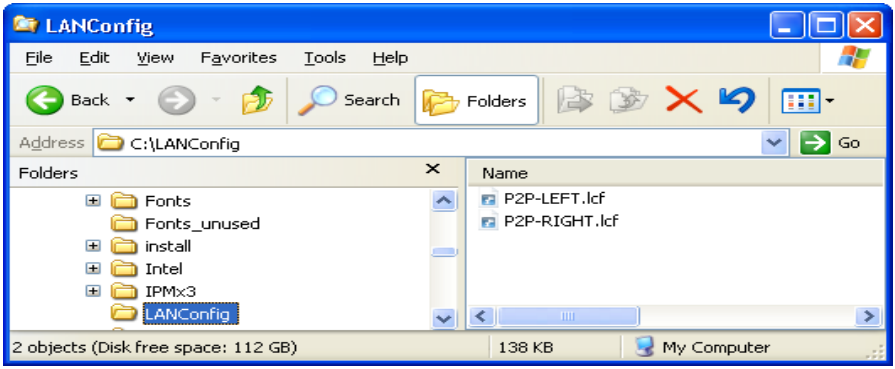
☐ Copy the LANconfig file `P2P-LEFT.lcf`:



☐ Paste the copied file into the same folder in Windows Explorer.

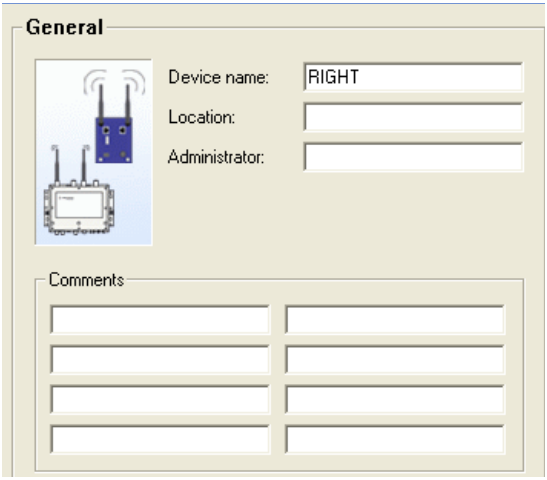


☐ Rename the copied file to `P2P-RIGHT.lcf`.



☐ Select the `P2P-RIGHT.lcf` file in Windows Explorer, then double-click the left mouse button. The LANconfig software opens for editing the RIGHT device configuration file.

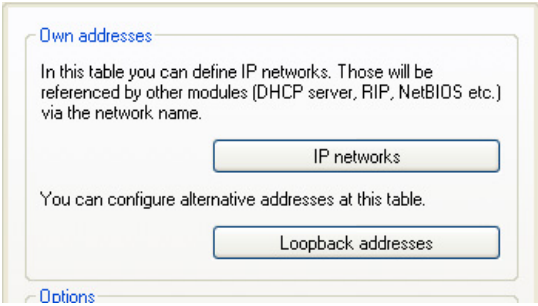
☐ Open the `Configuration : Management : General`.



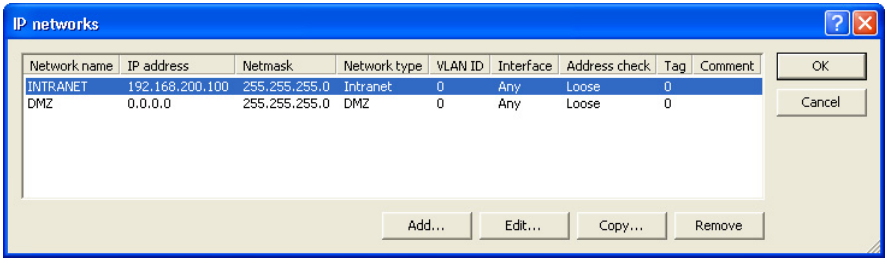
Type in ’RIGHT’ as the new ’Device name’.

☐ Edit the device IP address. To do this, navigate through several software screens, as follows:

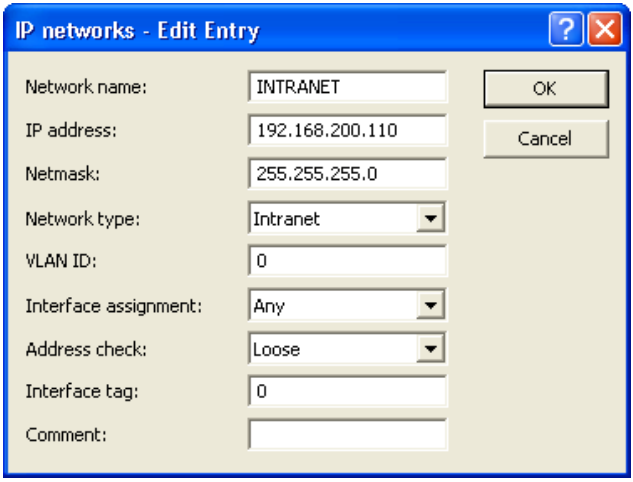
☐ Open the `Configuration : IPv4 : General` dialog.



☐ Click on the 'IP networks...' button (above) to open the 'IP networks' window (below):



☐ Click on the 'Edit...' button (above) to open the 'Edit Entry' dialog (below):



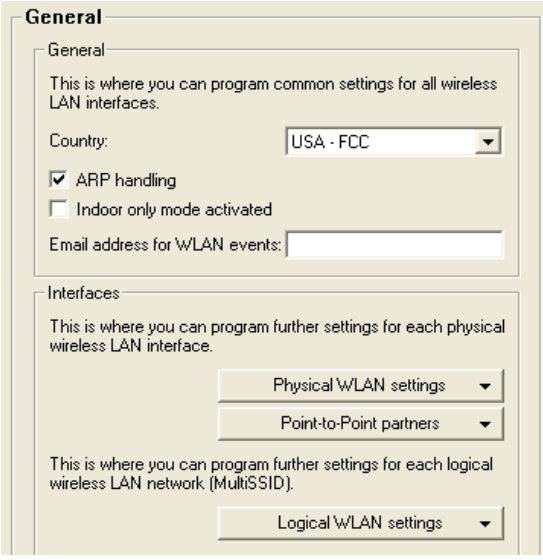
In the ‘Edit Entry’ dialog change the IP address to 192.168.200.110.

Click ’OK’ to close the ‘Edit Entry’ dialog.

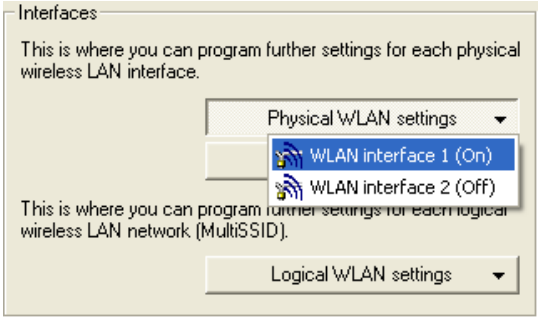
Click ’OK’ a second time to close the ‘IP networks’ dialog and return to the `Configuration : IPv4 : General` dialog.

☐ Edit the station name and channel selection scheme for this OpenBAT device. In this case, the station name is 'RIGHT' and the channel selection scheme is 'Slave'. As before, navigate through the following software screens:

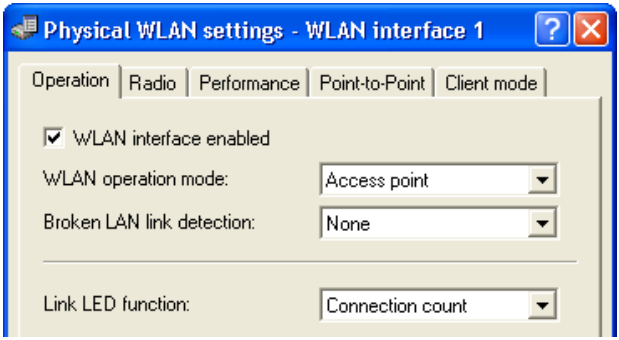
☐ Open the `Configuration : Wireless LAN : General` dialog:



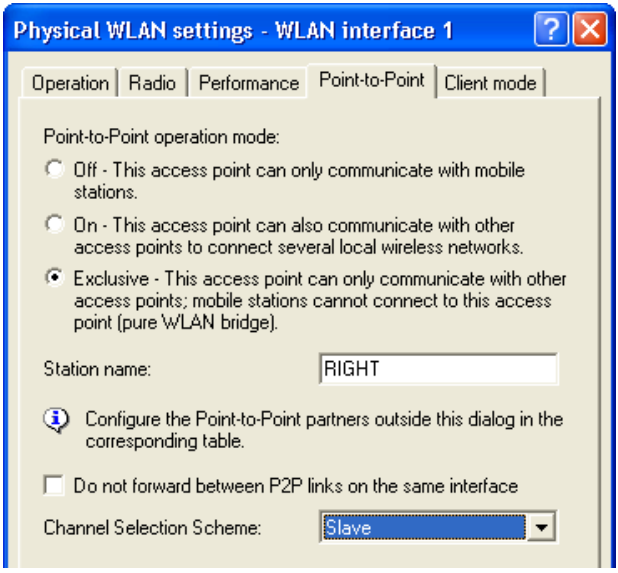
☐ Click on the 'Physical WLAN settings' button (above). If your device has two WLAN interfaces, select 'WLAN interface 1':



A dialog for editing the physical WLAN settings of WLAN interface 1 opens:



☐ Select the 'Point-to-Point' tab (above) to display a dialog for where you can configure point-to-point operation settings (below):



Make the following edits:.

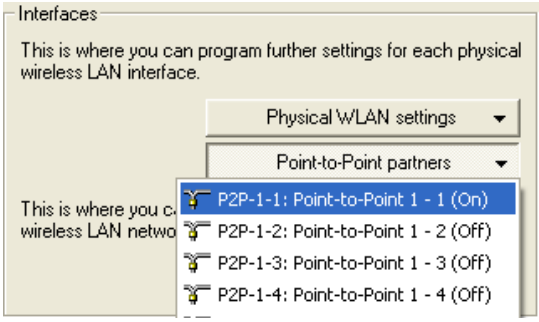
- Station name: ’RIGHT’

-Channel Selection Scheme: ’Slave’

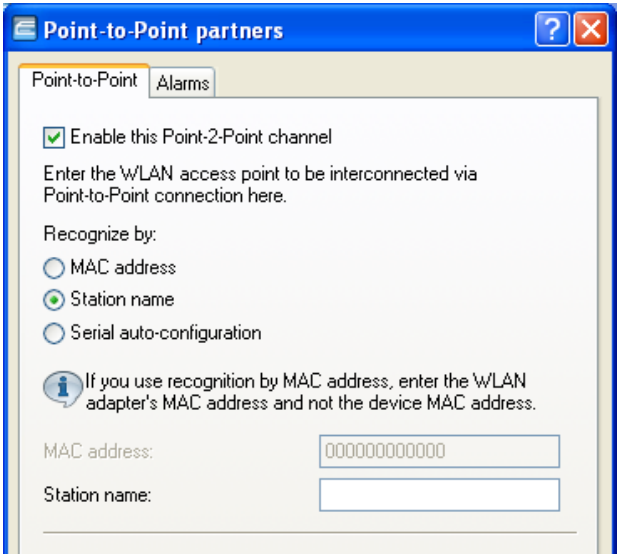
Click ‘Next’.

☐ The final edit is to change the station name of the point-to-point partner. In this case, the partner is the ’LEFT’ device. Navigate to the screen where you can make this edit, as follows:

☐ In the Wireless LAN configuration dialog, click on the ’Point-to-Point partners’ button, and select ’P2P-1-1’ (below):



☐ The next dialog for editing the Point-to-Point channels opens:



Change the partner ’Station name’ to ’LEFT’.

Click ’OK’ to close the dialog.

Click ’OK’ again to close the file and save your edits.

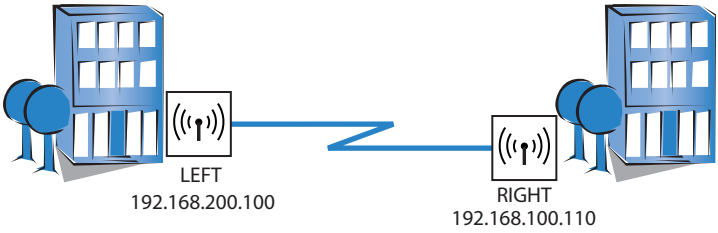
3.6 WLAN Bridge: Two Subnets

This example shows the creation of a WLAN bridge between 2 OpenBAT devices that are situated in different subnets by:

- ☐ creating a dedicated transfer network connecting the two OpenBAT devices, then
- ☐ routing the data traffic from one subnet to the other over the newly created transfer network

The transfer network's single purpose is to connect the two OpenBAT devices and thereby establishing a connection between the two subnets.

As before, each Access Point is configured to deny access to devices other than its bridge partner. This example builds on the previous configurations of the RIGHT and LEFT devices (see on page 109) and enables routing between these two devices.



The significant configuration settings for the device are as follows:

Station Name:	LEFT	RIGHT
Role:	Access Point	Access Point
IP address:	192,168,200,100	192,168,100,110
Subnet Mask:	255.255.255.0	255.255.255.0
Channel Selection Scheme	Master	Slave
Point-to-Point Partner	RIGHT	LEFT

3.6.1 Creating Two LANconfig Files

Creating a WLAN bridge between two different subnets involves the creation and configuration of two LANconfig files, one for the LEFT device and one for the RIGHT device. Because these two files contain virtually the same Basic settings (see on page 110) and WLAN settings (see on page 118) as in the previous example, the easiest way to begin is to copy and re-name previously created files. After new files are created, their configuration settings can be edited.

To create two LANconfig files, follow these steps:

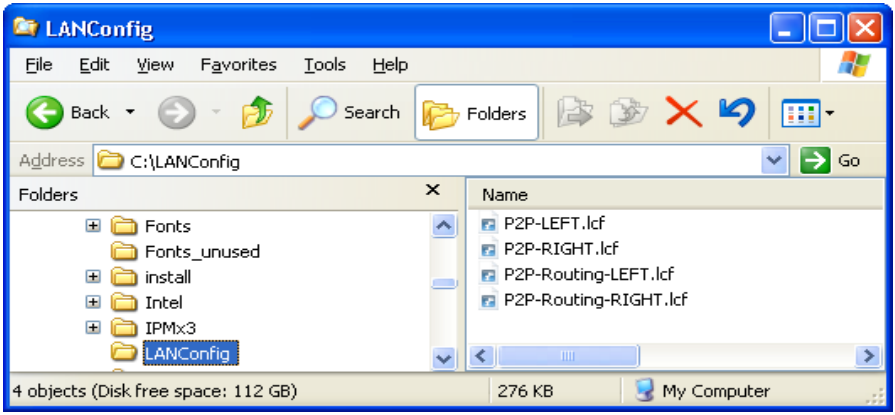
☐ Create a new LANconfig file: `P2P-Routing-LEFT.lcf`:

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-LEFT.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Routing-LEFT.lcf`.

☐ Create a new LANconfig file: `P2P-Routing-RIGHT.lcf`.

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-RIGHT.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Routing-RIGHT.lcf`.

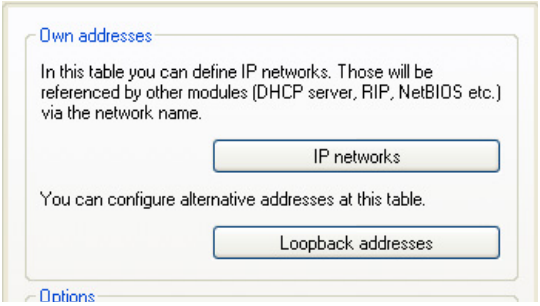
Windows Explorer now contains the following files:



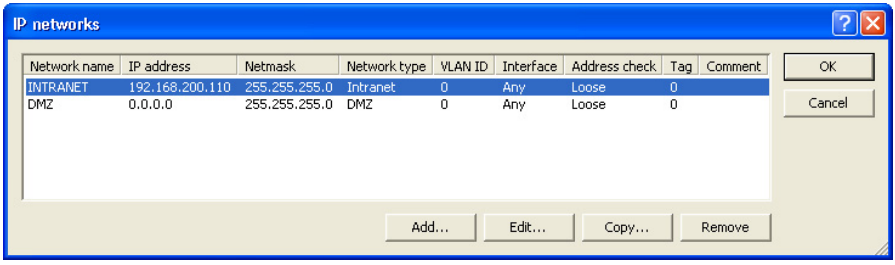
☐ The next step is to edit the IP address of the RIGHT device:

☐ In Windows Explorer, double-click on the file: `P2P-Routing-RIGHT.lcf`.

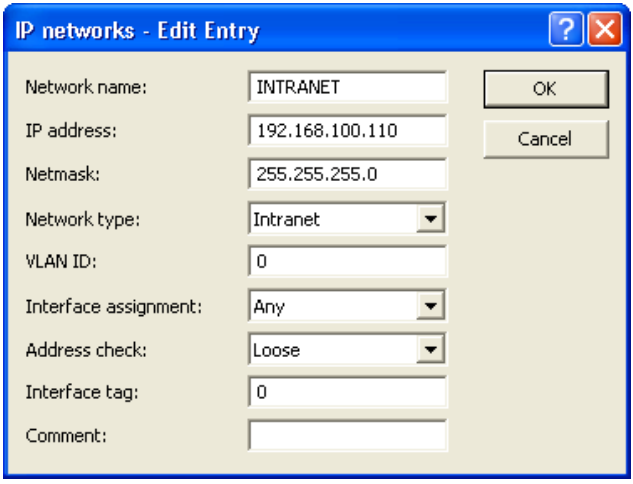
☐ Open the `Configuration : IPv4 : General` dialog.



☐ Click the 'IP networks...: button (above) to open the 'IP networks' window (below):



☐ In the ‘IP networks’ window (above) select the INTRANET network, then click on the ’Edit...’ button to open the ‘Edit Entry’ dialog (below):



☐ In the ‘Edit Entry’ dialog, edit the IP address of the RIGHT device configuration file to 192.168.100.110.

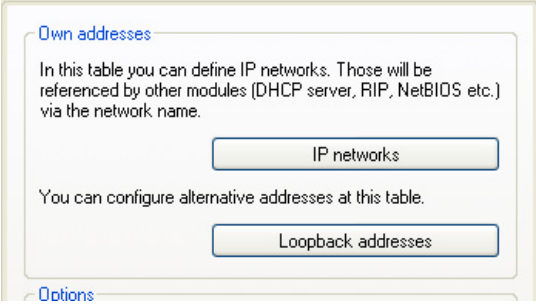
☐ Click ’OK’ three times to close the open dialogs, save your edits and close the file `P2P-Router-RIGHT.lcf`.

3.6.2 Creating Two Transfer Network Entries

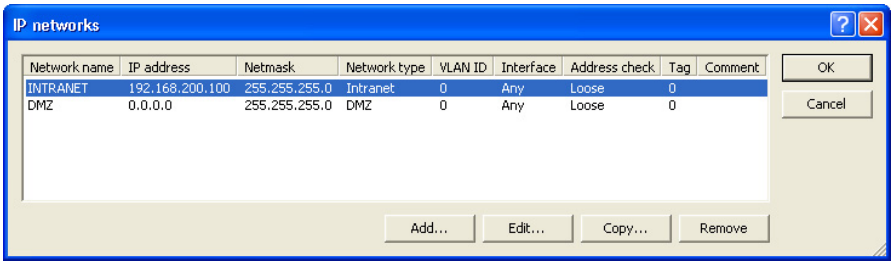
The next task is to create a transfer network in each device. This is accomplished by adding a new network entry to each device configuration file.

☐ In Windows Explorer, click on the file `P2P-Routing-LEFT.lcf` to open it for editing.

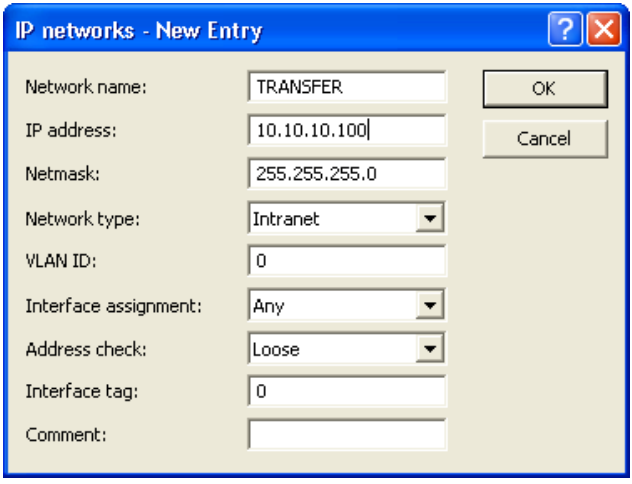
☐ Open the `Configuration : IPv4 : General` dialog.



☐ Click the 'IP networks...: button (above) to open the 'IP networks' window (below):



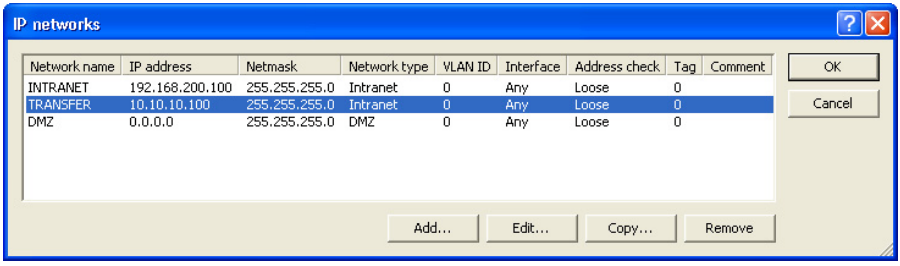
☐ In the 'IP networks' window (above), click the 'Add...' button to open the 'New Entry' dialog (below):



☐ In the ‘New Entry’ dialog (above), create a new network for this device configuration file by inputting the following settings:

– Network name: TRANSFER
– IP address: 10.10.10.100
– Network type: Intranet (the default)
– VLAN ID: 0 (the default)
– Interface assignment: Any (the default)
– Address check: Loose (the default)
– Interface tag: 0 (the default)
– Comment: <leave blank>

Click ’OK’ to add the new network to the network list in the ‘IP networks’ window (below):



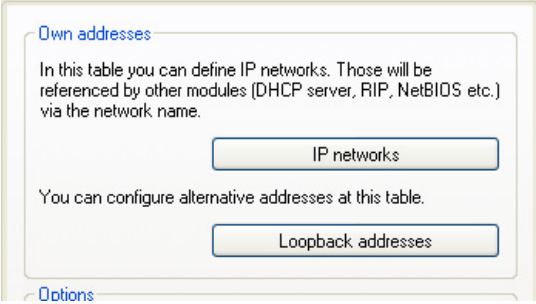
☐ Click ’OK’ again to close the ‘IP networks’ window for the LEFT device.

Note: Leave open the `P2P-Routing-LEFT.lcf` LANconfig file for further editing.

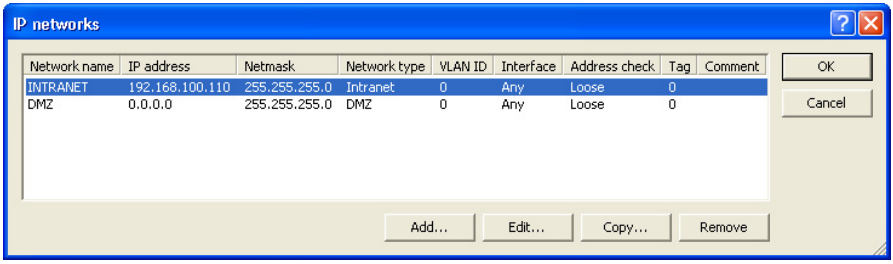
The next step is to create a new network entry for the RIGHT device, as described, below.

☐ In Windows Explorer, click on the file `P2P-Routing-RIGHT.lcf` to open it for editing.

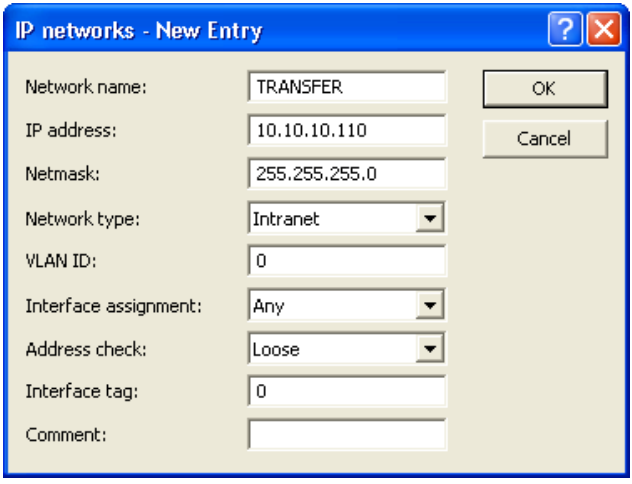
☐ Open the `Configuration : IPv4 : General dialog`.



☐ Click on the 'IP networks...' button (above) to open the 'IP networks' window (below):



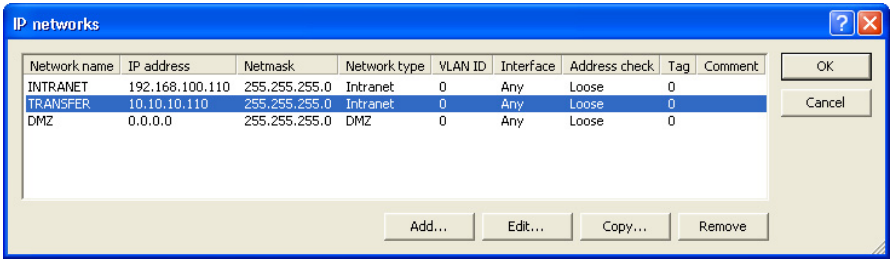
☐ In the 'IP networks' window (above), click the 'Add...' button to open the 'New Entry' dialog (below):



☐ In the ‘New Entry’ dialog (above), create a new network for this device configuration file by inputting the following settings:

– Network name: TRANSFER
– IP address: 10.10.10.110
– Network type: Intranet (the default)
– VLAN ID: 0 (the default)
– Interface assignment: Any (the default)
– Address check: Loose (the default)
– Interface tag: 0 (the default)
– Comment: <leave blank>

Click ’OK’ to add the new network to the network list in the ‘IP networks’ window (below):



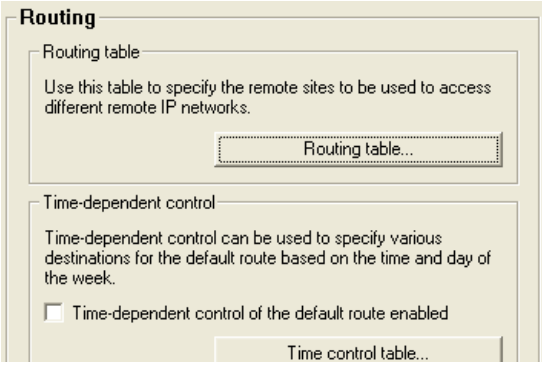
☐ Click ’OK’ again to close the ‘IP networks’ window for the RIGHT device.

Note: Leave open the `P2P-Routing-RIGHT.lcf` LANconfig file for further editing.

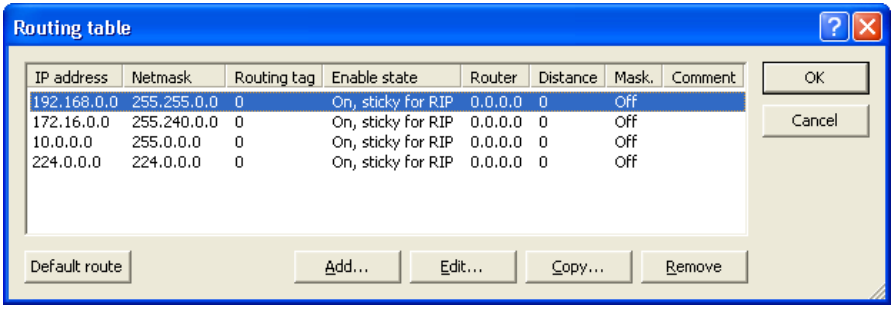
3.6.3 Routing the Transfer Networks

The next step is to link together the two new transfer networks. This is accomplished by assigning each new network to the same routing address.

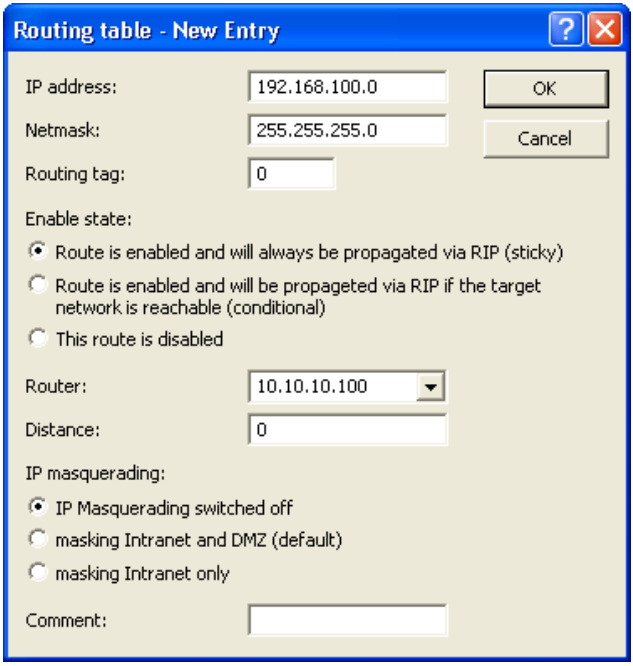
☐ Return to the configuration file `P2P-Routing-LEFT.lcf` (which remains open) and open the `Configuration : IP Router : Routing` dialog:



☐ Click on the 'Routing table...' button (above) to open the routing table for the LEFT device (below):



☐ In the 'Routing table' (above), click on the 'Add...: button to open the 'New Entry' dialog (below):

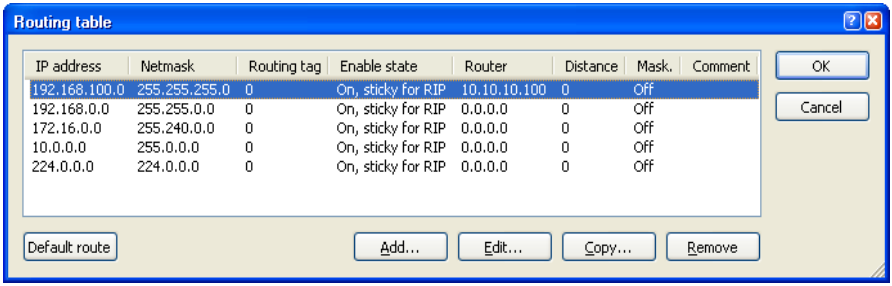


☐ In the ‘New Entry’ dialog (above), create a new routing entry and associate that routing entry with the network of the RIGHT device, as follows:

– IP address: 192.168.100.0
– Netmask: 255.255.255.0
– Router: 10.10.10.100

Accept the remaining default values.

Click ’OK’ to save the new routing entry, and add it to the Routing table (below):



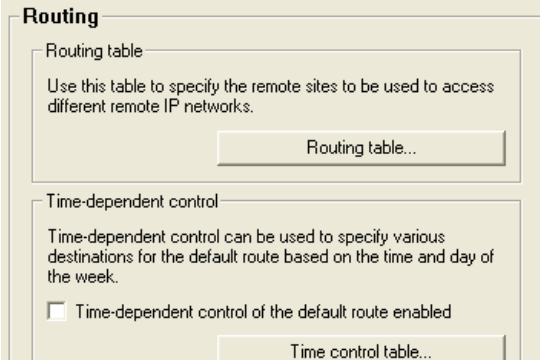
☐ Click 'OK' to close the routing table (above) for the LEFT device.

Click 'OK' a second time to save both the new network and the routing settings for the `P2P-Routing-LEFT.lcf` configuration file.

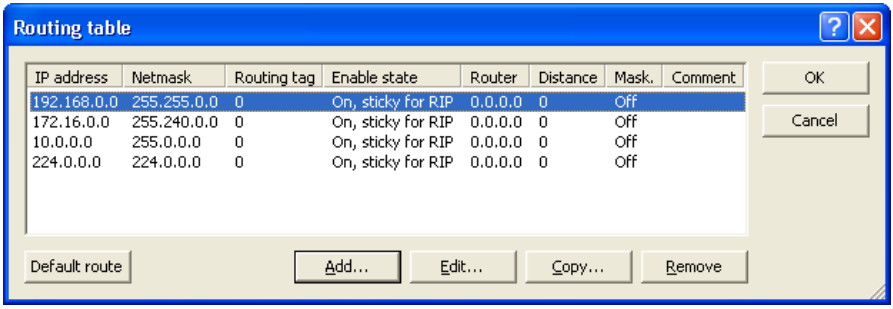
The next task is to create a new routing table entry for the RIGHT device.

☐ Return to the configuration file `P2P-Routing-RIGHT.lcf` (which remains open).

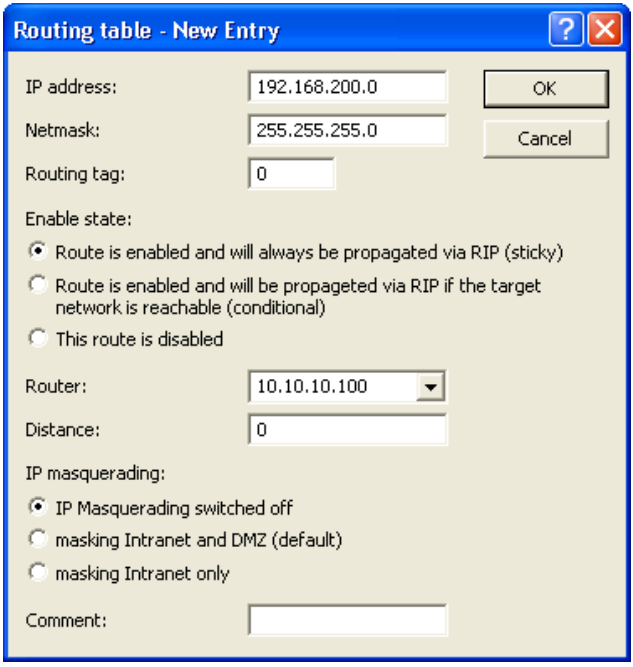
☐ Open the `Configuration : IP Router : Routing` dialog:



☐ Click on the 'Routing table...' button (above) to open the routing table for the RIGHT device (below):



☐ In the ‘Routing table’ (above), click on the ’Add...: button to open the ‘New Entry’ dialog (below):

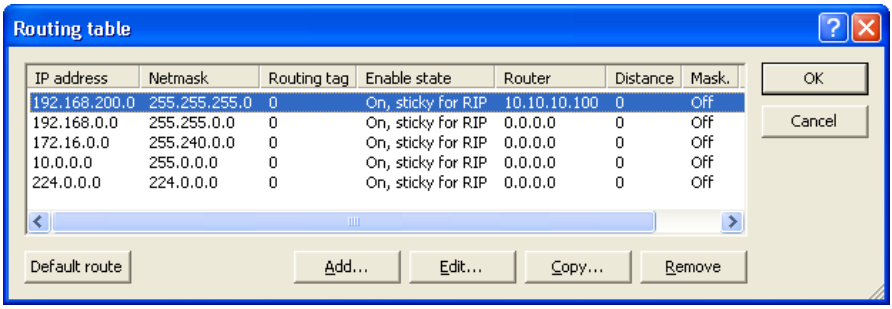


☐ In the ‘New Entry’ dialog (above), create a new routing entry and associate that routing entry with the network of the LEFT device, as follows:

– IP address: 192.168.200.0
– Netmask: 255.255.255.0
– Router: 10.10.10.100

Accept the remaining default values.

Click ’OK’ to save the new routing entry, and add it to the Routing table (below):



☐ Click ’OK’ to close the routing table (above) for the RIGHT device.

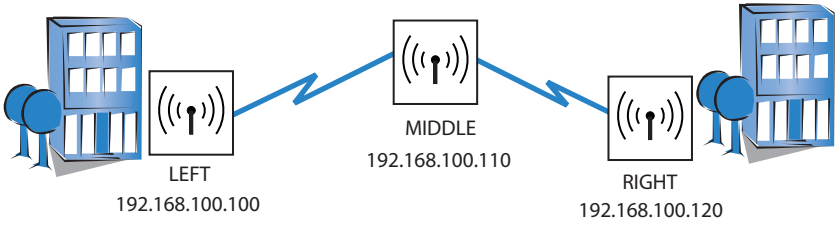
Click ’OK’ a second time to save both the new network and the routing settings for the `P2P-Routing-RIGHTT.lcf` configuration file.

Configurations for the transfer network are complete.

3.7 WLAN Bridge Relay: 1 Radio

This example employs three OpenBAT devices (named LEFT, CENTER, and RIGHT) to implement a WLAN bridge relay. All devices are located in the same subnet.

The CENTER device serves as a repeater and relays messages between the LEFT and RIGHT devices. The CENTER device communicates with both the LEFT and RIGHT devices via two different channels over a single radio interface. Because the relay device employs just a single radio, this design reduces the effective bandwidth of the connection by a factor of 50%.



The significant configuration settings for the device are as follows:

Station Name:	LEFT	CENTER	RIGHT
Role:	Access Point	Access Point	Access Point
IP address:	192,168,100,100	192,168,100,110	192,168,100,120
Subnet Mask:	255.255.255.0	255.255.255.0	255.255.255.0
Number of interfaces used:	1	1	1
Number of channels used:	1	2	1
Channel Selection Scheme	Slave	Master	Slave
Point-to-Point Partner	CENTER	LEFT/RIGHT	CENTER

Each Access Point is configured to deny access to devices other than its immediate bridge partner. This example builds on the previous configurations of the LEFT and RIGHT devices (see on page 109).

3.7.1 Creating Three LANconfig Files

Creating a WLAN bridge relay involves the creation and configuration of three LANconfig files, one for the LEFT device, one for the MIDDLE device, and one for the RIGHT device. Because each of these files contain virtually the same Basic settings (see on page 110) and WLAN settings (see on page 118) as in the original example, the easiest way to begin is to make 3 copies of the previously `P2P-LEFT.lcf` file. After new files are created, their configuration settings can be edited.

To create three new LANconfig files, follow these steps:

☐ Create a new LANconfig file: `P2P-Relay-1Radio-LEFT.lcf`:

- ☐ In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- ☐ Copy the file `P2P-LEFT.lcf`.
- ☐ Paste the copied file into the same Windows Explorer folder.
- ☐ Rename the new file `P2P-Relay-1Radio-LEFT.lcf`.

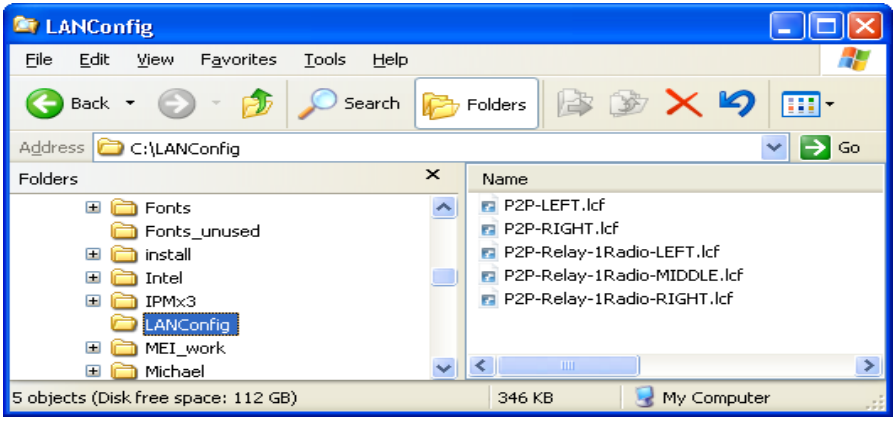
☐ Create a new LANconfig file: `P2P-Relay-1Radio-MIDDLE.lcf`:

- ☐ In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- ☐ Copy the file `P2P-LEFT.lcf`.
- ☐ Paste the copied file into the same Windows Explorer folder.
- ☐ Rename the new file `P2P-Relay-1Radio-MIDDLE.lcf`.

☐ Create a new LANconfig file: `P2P-Relay-1Radio-RIGHT.lcf`.

- ☐ In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- ☐ Copy the file `P2P-LEFT.lcf`.
- ☐ Paste the copied file into the same Windows Explorer folder.
- ☐ Rename the new file `P2P-Relay-1Radio-RIGHT.lcf`.

Windows Explorer now contains the following files:



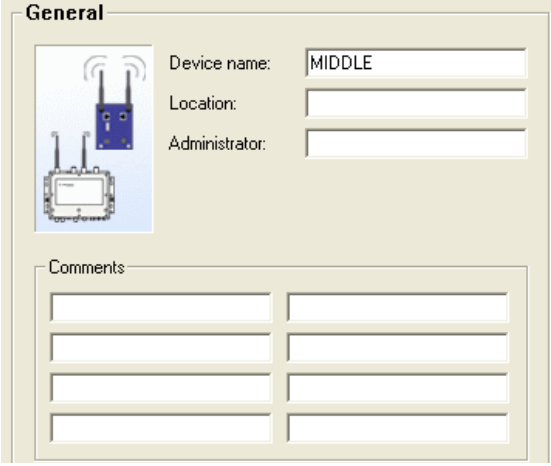
The next tasks are to edit the names and IP addresses of both the MIDDLE and RIGHT devices.

Note: The file `P2P-Relay-1Radio-LEFT.lcf` should be configured with the:
- Device name = 'LEFT', and
- IP address = '192.168.100.100'

☐ To edit the name and IP address of the MIDDLE device:

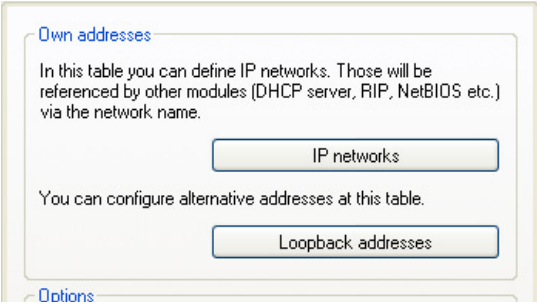
☐ In Windows Explorer, double-click on the file: `P2P-Relay-1Radio-MIDDLE.lcf`.

☐ Open the `Configuration : Management : General` dialog.

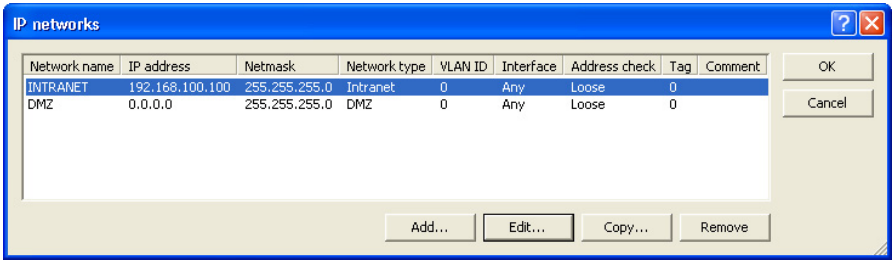


☐ Change the Device name to 'MIDDLE'.

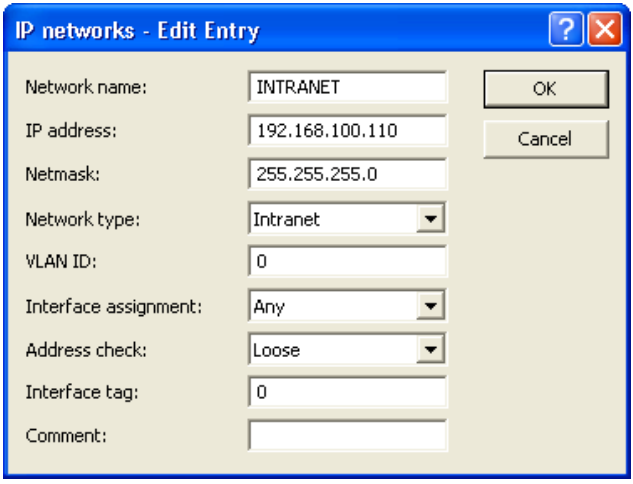
☐ Open the `Configuration : IPv4 : General` dialog.



☐ Click the 'IP networks...' button (above) to open the 'IP networks' window (below):



☐ In the ‘IP networks’ window (above), select the INTRANET network, then click the ’Edit...’ button to open the ‘Edit Entry’ dialog (below):



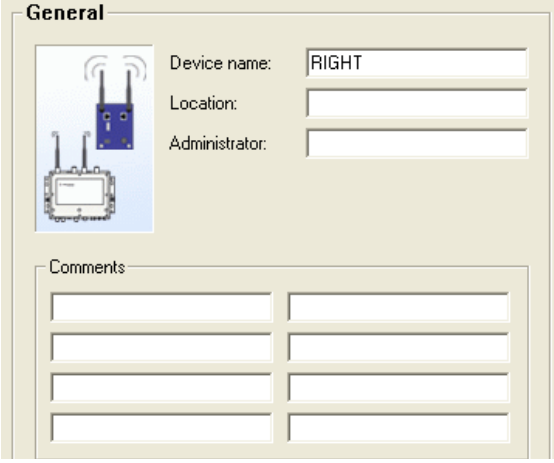
☐ In the ‘Edit Entry’ dialog, change the IP address of the MIDDLE device configuration file to ’192.168.100.110’.

☐ Click ’OK’ twice. Leave the configuration file open for later editing.

☐ To edit the name and IP address of the RIGHT device:

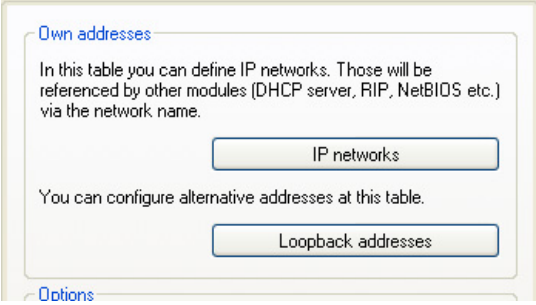
☐ In Windows Explorer, double-click on the file: `P2P-Relay-1Radio-RIGHT.lcf`.

☐ Open the `Configuration : Management : General` dialog:

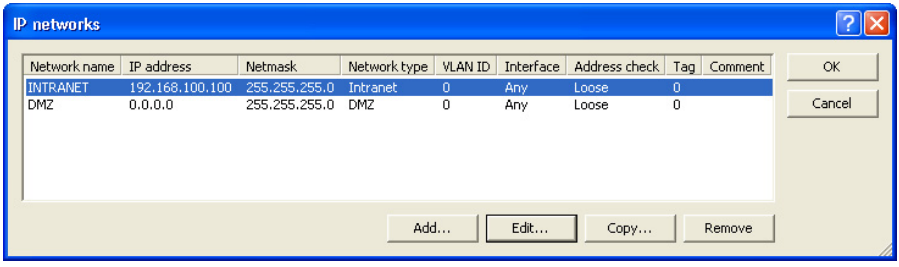


☐ Change the Device name to 'RIGHT'.

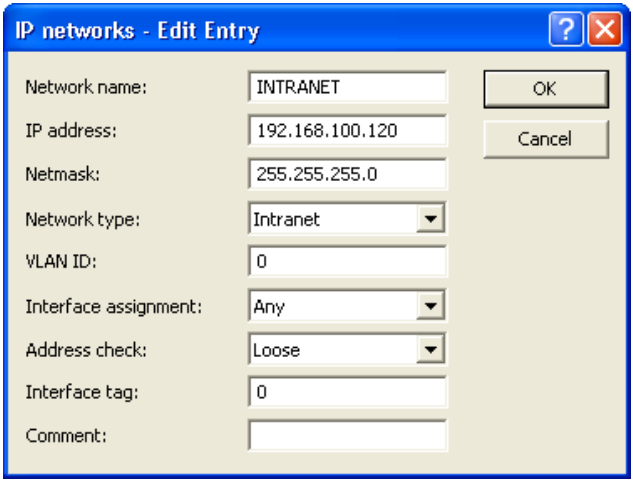
☐ Open the `Configuration : IPv4 : General` dialog.



☐ Click the 'IP networks...' button (above) to open the 'IP networks' window (below):



☐ In the ‘IP networks’ window (above), select the INTRANET network, then click the ’Edit...’ button to open the ‘Edit Entry’ dialog (below):



☐ In the ‘Edit Entry’ dialog, change the IP address of the RIGHT device configuration file to ’192.168.100.120’.

☐ Click ’OK’ twice in order to close the two open dialogs. Leave the configuration file open for later editing.

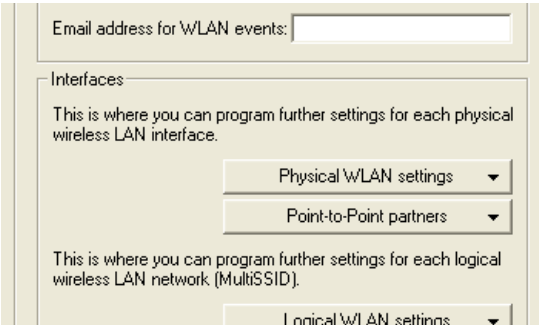
3.7.2 Configure the LEFT Device

The next task is to configure the LEFT device by:

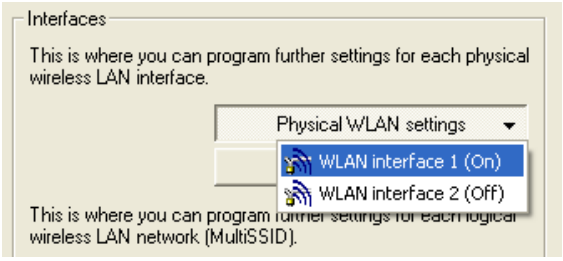
– enabling a single interface
– enabling a single channel on that interface

– designating the LEFT device as a slave
– identifying the MIDDLE device as its Point-to-Point partner

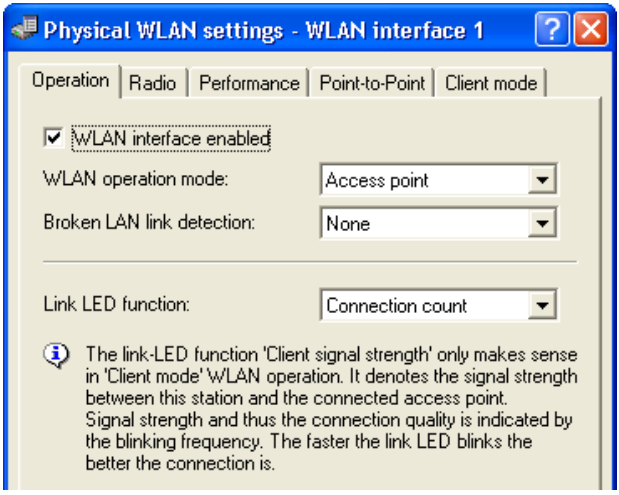
☐ In the `P2P-Relay-1Radio-LEFT.lcf` file, open the `Configuration : Wireless LAN : General` dialog (below):



☐ Click the 'Physical WLAN settings' button, and select 'WLAN interface 1', as depicted below:

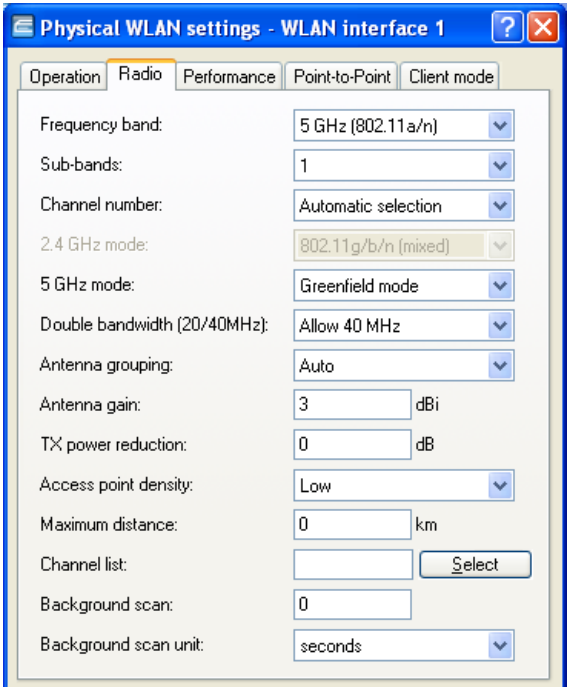


☐ In the WLAN Interface 1 window, click on the 'Operation' tab (below):



Confirm that ’WLAN interface enabled’ is selected.

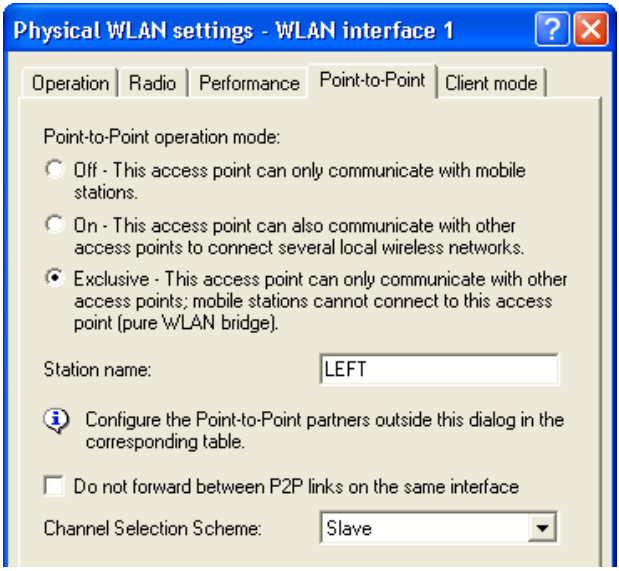
☐ Open the ’Radio’ tab (below) of the same dialog:



Edit the following properties:

– Frequency band: 5 GHz (802.11a/n)
– 5 GHz mode: Greenfield mode
– Antenna gain 9 dBi

☐ Click on the ’Point-to-Point’ tab (above) to open that dialog:

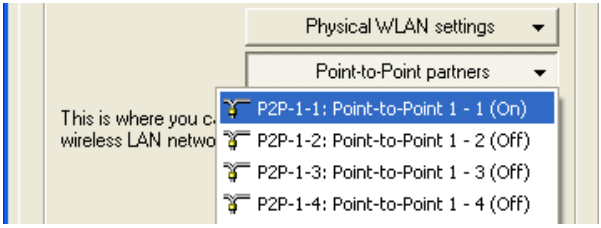


In the Point-to-Point tab, enter the following settings:

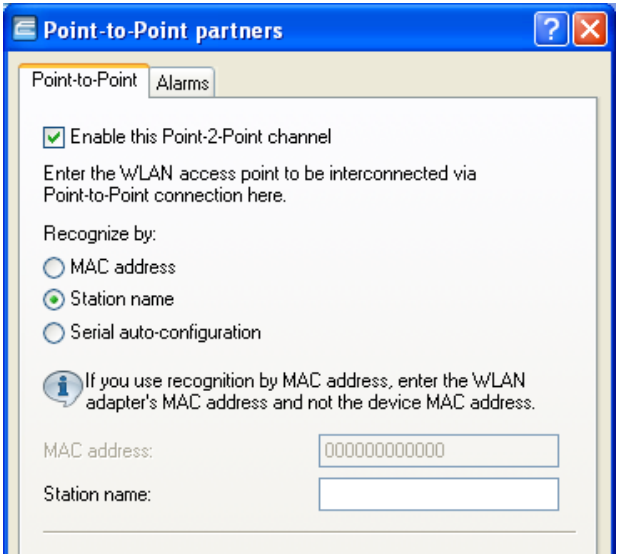
– Point-to-Point operation mode: 'Exclusive'
– Station name: 'LEFT'
– Channel Selection Scheme: 'Slave'

Click 'OK' to close the dialog.

☐ In the `Configuration: Wireless LAN : General` dialog, click the 'Point-to-Point partners' button, then select 'P2P-1-1' as depicted below:



☐ The ‘Point-to-Point partners’ dialog opens, displaying settings for P2P interface 1, channel 1 (below):



Enter the following settings:

– Select ’Enable this Point-2-Point channel’
– Select the ’Recognize by Station name’ option
– Change the Station name to: ’MIDDLE’

Click ’OK’ to close the ‘Point-to-Point partners’ dialog.

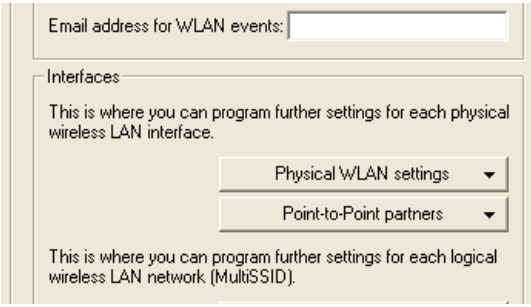
Click ’OK’ again to save configuration settings for the LEFT device.

3.7.3 Configure the MIDDLE Device

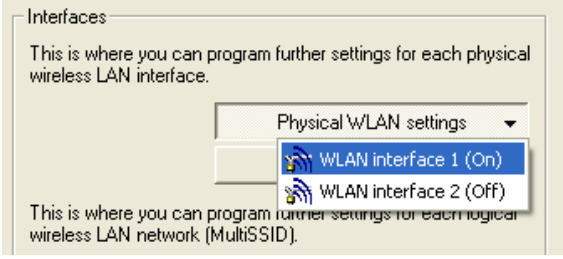
The next task is to configure the MIDDLE device by:

- enabling a single interface
- enabling two channels on that interface
- designating the MIDDLE device as the MASTER for each channel
- identifying the LEFT device as the Point-to-Point partner on channel 1
- identifying the RIGHT device as the Point-to-Point partner on channel 2

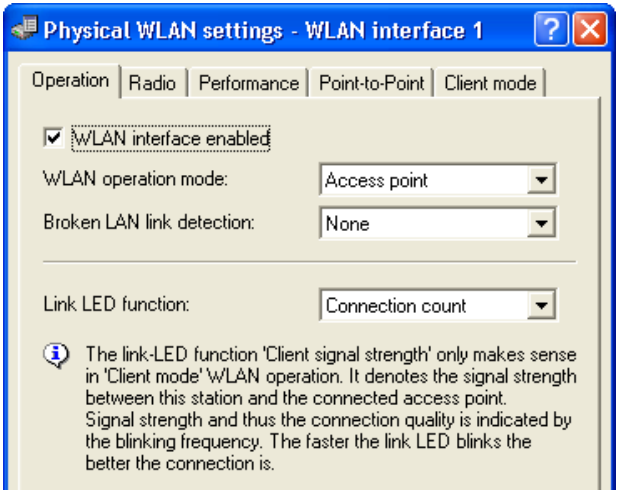
☐ In the `P2P-Relay-1Radio-MIDDLE.lcf` file, open the `Configuration : Wireless LAN : General` dialog (below):



☐ Click on the 'Physical WLAN settings' button, and select 'WLAN interface 1', as depicted below:

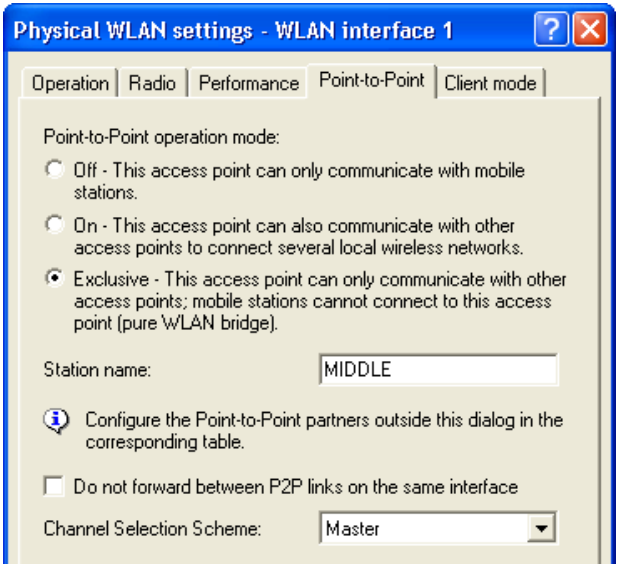


☐ In the 'WLAN Interface 1' dialog, click on the 'Operation' tab (below):



Confirm that ’WLAN interface enabled’ is selected, then click the ’Point-to-Point’ tab.

☐ The ‘Point-to-Point’ dialog opens:

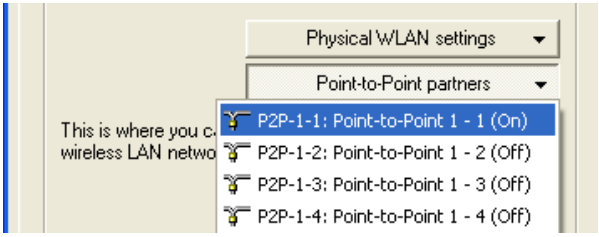


In the Point-to-Point tab, enter the following settings:

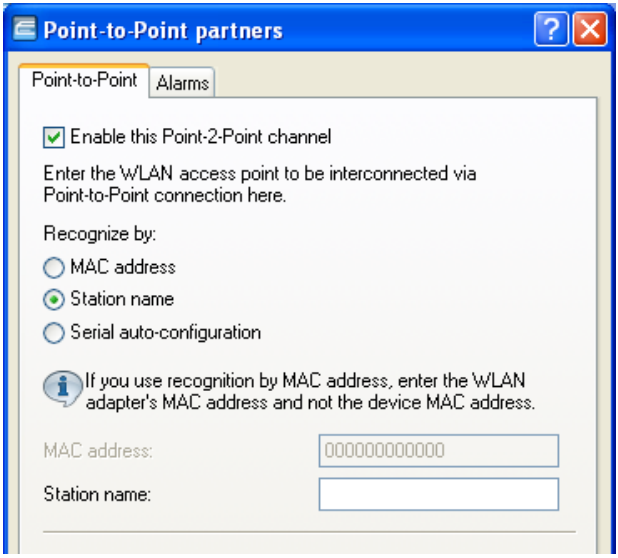
– Point-to-Point operation mode: 'Exclusive'
– Station name: 'MIDDLE'
– Channel Selection Scheme: 'Master'

Click 'OK'. The `Configuration : Wireless LAN : General` dialog opens. The next task is to identify the two point-to-point partners.

☐ Click the 'Point-to-Point partners' button, then select 'P2P-1-1' (interface 1, channel 1) as depicted below:



☐ The 'Point-to-Point partners' dialog opens, displaying settings for P2P interface 1, channel 1 (below):

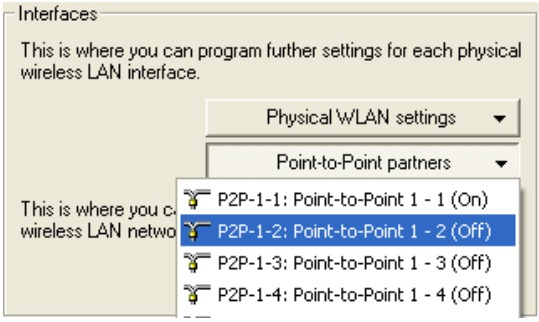


In this dialog identify the LEFT device as the channel 1 Point-to-Point partner device:

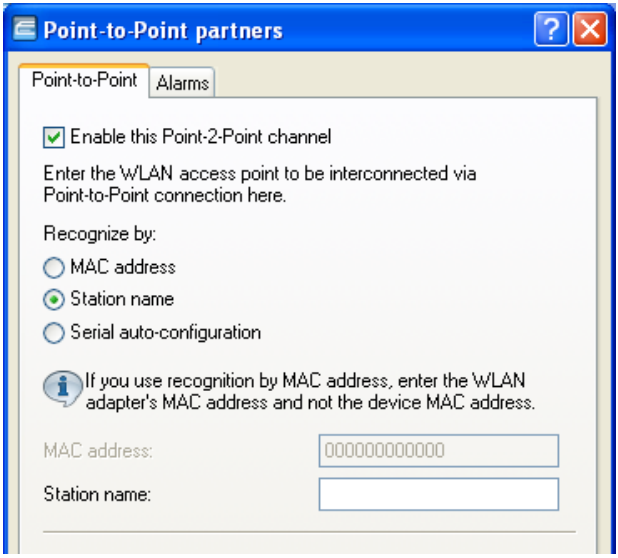
– Confirm that 'Enable this Point-2-Point channel' is selected
– Select 'Recognize by Station name'
– Change the partner Station name to 'LEFT'

Click 'OK' to close the 'Point-to-Point partners' dialog.

☐ In the `Configuration : Wireless LAN : General` dialog, click the 'Point-to-Point partners' button, then select 'P2P-1-2' (interface 1, channel 2) as depicted below:



☐ The ‘Point-to-Point partners’ dialog opens, displaying settings for P2P interface 1, channel 2 (below):



In this dialog, identify the RIGHT device as the channel 2 Point-to-Point partner device:

– Select ’Enable this Point-2-Point channel’
– Select ’Recognize by Station name’
– Change the partner Station name to ’RIGHT’

Click ’OK’ to close the ‘Point-to-Point partners’ dialog.

Click ’OK’ a second time to save settings for the MIDDLE device.

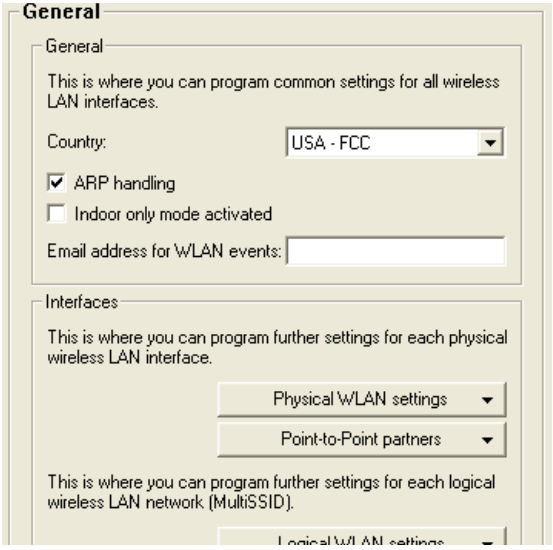
3.7.4 Configure the RIGHT Device

The next task is to configure the RIGHT device by:

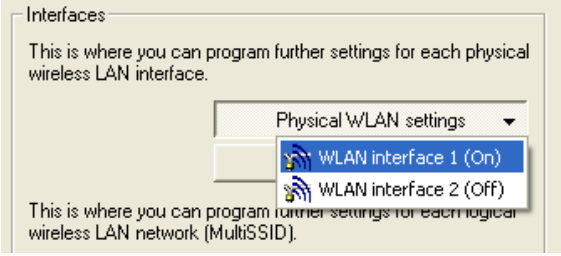
- enabling a single interface
- enabling a single channel on that interface

- designating the RIGHT device as a slave
- identifying the MIDDLE device as its Point-to-Point partner

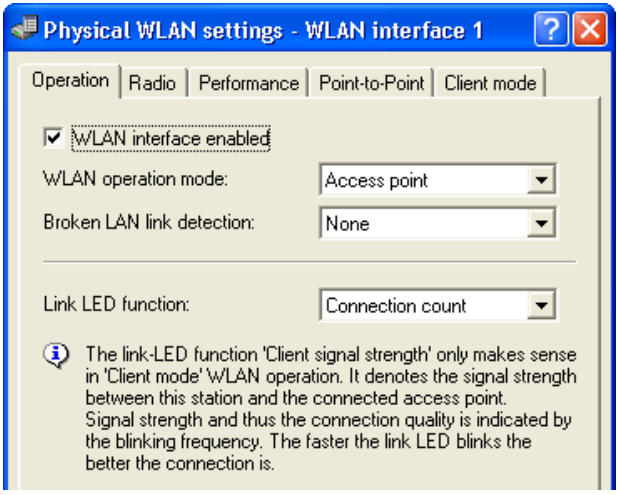
☐ In the `P2P-Relay-1Radio-RIGHT.lcf` file, open the `Configuration : Wireless LAN : General` dialog (below):



☐ Click on the 'Physical WLAN settings' button, and select 'WLAN interface 1', as depicted below:

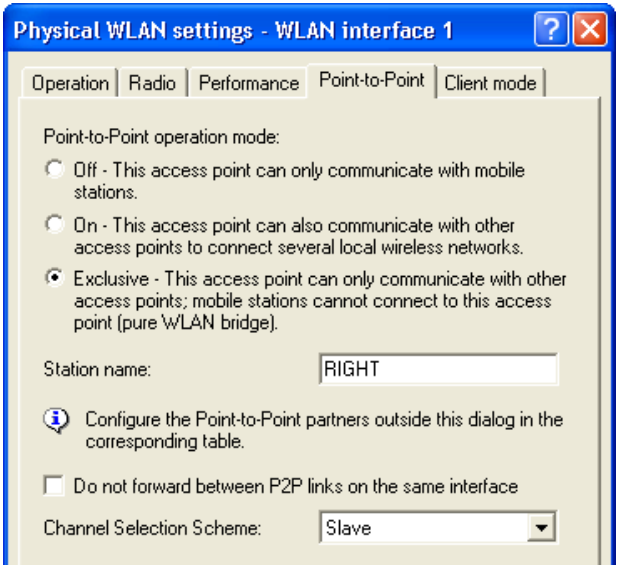


☐ In the 'WLAN Interface 1' dialog, click on the 'Operation' tab (below):



Confirm that 'WLAN interface enabled' is selected, then click on the 'Point-to-Point' tab.

☐ The 'Point-to-Point' dialog opens:

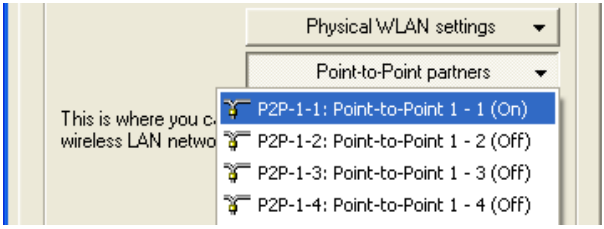


In the ‘Point-to-Point’ dialog, enter the following settings:

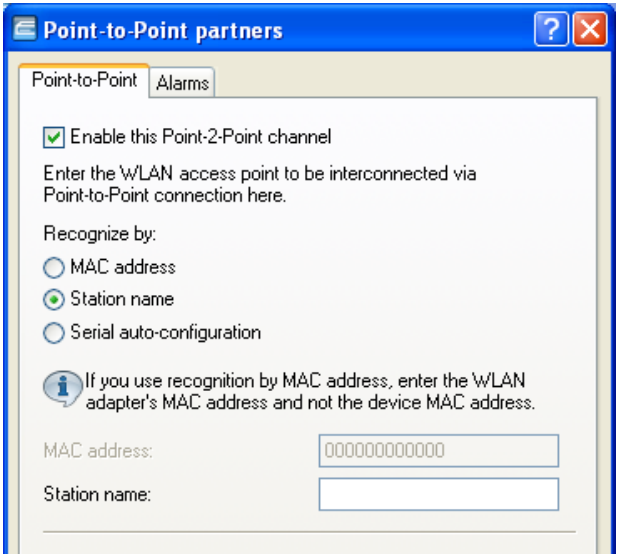
– Point-to-Point operation mode: ’Exclusive’
– Station name: ’RIGHT’
– Channel Selection Scheme: ’Slave’

Click ’OK’

☐ In the `Configuration : Wireless LAN : General` dialog, click the ’Point-to-Point partners’ button, then select ’P2P-1-1’ (interface 1, channel 1) as depicted below:



☐ The ‘Point-to-Point partners’ dialog opens, displaying settings for P2P interface 1, channel 1 (below):



Enter the following settings:

– Select ’Enable this Point-2-Point channel’
– Select ’Recognize by Station name’
– Station name: ’MIDDLE’

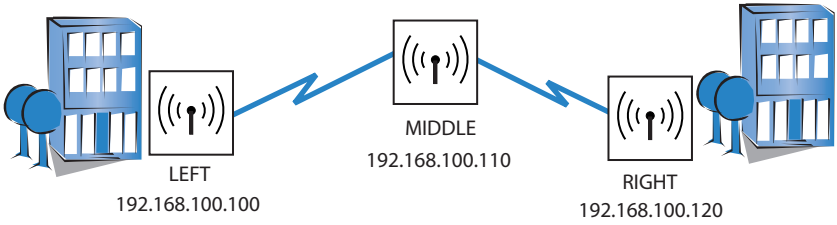
Click ’OK’ to close the ‘Point-to-Point partners’ dialog.

Click ’OK’ a second time to save settings for the CENTER device.

3.8 WLAN Bridge Relay: 2 Radios

This example employs three OpenBAT devices (named LEFT, CENTER, and RIGHT) to implement a WLAN bridge relay. All devices are located in the same subnet.

The CENTER device is a dual-radio device that serves as a repeater and relays messages between the LEFT and RIGHT devices. The CENTER device communicates with the LEFT device via radio interface 1, and with the RIGHT device via radio interface 2. Because the relay device uses just one channel per interface, 100% of the interface bandwidth for each connection.



The significant configuration settings for the device are as follows:

Station Name:	LEFT	CENTER	RIGHT
Role:	Access Point	Access Point	Access Point
IP address:	192,168,100,100	192,168,100,110	192,168,100,120
Subnet Mask:	255.255.255.0	255.255.255.0	255.255.255.0
Number of interfaces used:	1	2	1
Number of channels used:	1	2 (1 per interface)	1
Channel Selection Scheme	Master	Slave	Master
Point-to-Point Partner	CENTER-1	LEFT/RIGHT	CENTER-2

Each Access Point is configured to deny access to devices other than its immediate bridge partner. This example builds on the previous configurations of the RIGHT and LEFT(see on page 165), CENTER (see on page 171) and RIGHT(see on page 176) devices.

3.8.1 Creating Three LANconfig Files

Creating a WLAN bridge relay involves the creation and configuration of three LANconfig files, one for the LEFT device, one for the CENTER device, and one for the RIGHT device. Because each of these files contains virtually the same basic settings as the point-to-point relay example (1 radio) (see on page 159) , the easiest way to begin is to copy each of the 3 LANconfig files. After the files have been created, you can edit their configuration settings.

To create three new LANconfig files, follow these steps:

☐ Create a new LANconfig file: `P2P-Relay-2Radios-LEFT.lcf`:

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-Relay-1Radio-LEFT.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Relay-2Radios-LEFT.lcf`.

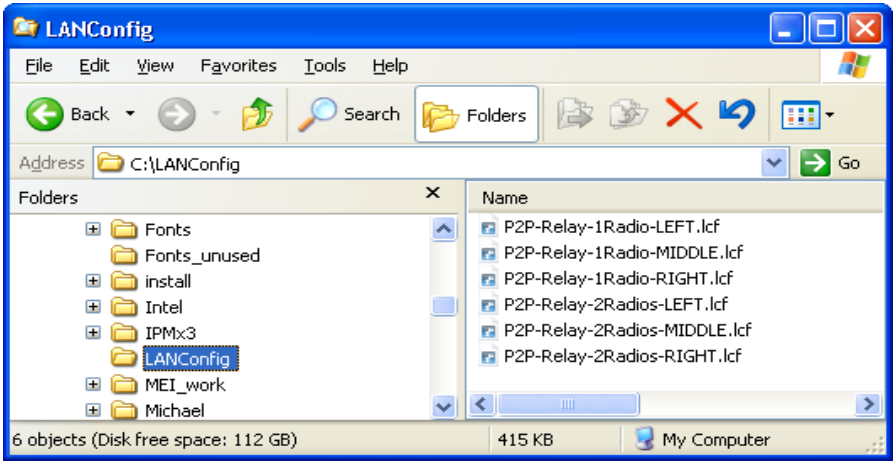
☐ Create a new LANconfig file: `P2P-Relay-2Radios-MIDDLE.lcf`:

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-Relay-1Radio-MIDDLE.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Relay-2Radios-MIDDLE.lcf`.

☐ Create a new LANconfig file: `P2P-Relay-2Radios-RIGHT.lcf`.

- In Windows Explorer, navigate to the folder where the previously created LANconfig files are saved.
- Copy the file `P2P-Relay-1Radio-RIGHT.lcf`.
- Paste the copied file into the same Windows Explorer folder.
- Rename the new file `P2P-Relay-2Radios-RIGHT.lcf`.

Windows Explorer now contains the following files:



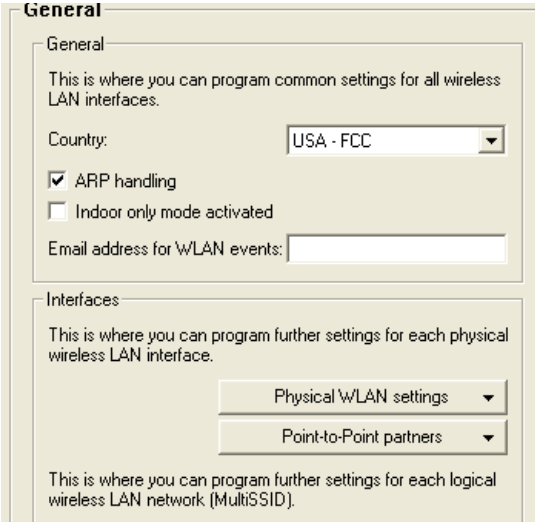
3.8.2 Configuring the MIDDLE Device

Most of the edits in this example are made to the MIDDLE device, which communicates to the LEFT and RIGHT devices via channels in separate radio interfaces. These edits include:

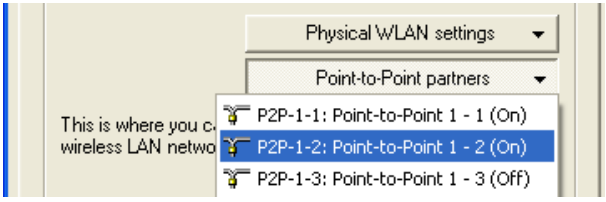
- Disabling Interface 1 / Channel 2
- Editing physical LAN settings for Interface 1
- Enabling and configuring Interface 2
- Enabling Interface 2 / Channel 1 and identifying a Point-to-Point partner
- Configuring encryption settings for Interface 2 / Channel 1

Disable Channel 2 on Interface 1

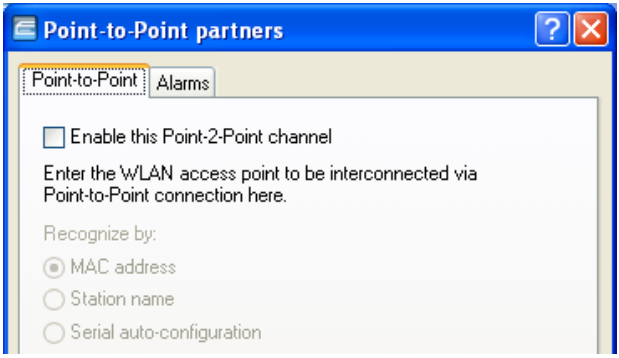
☐ In the `P2P-Relay-2Radios-MIDDLE.lcf` file, open the following dialog: `Configuration:Wireless LAN:General`.



☐ Click on the 'Point-to-Point partners' button (above), then select 'P2P-1-2' (below):



☐ The 'P2P-1-2 Point-to-Point partners' dialog opens:

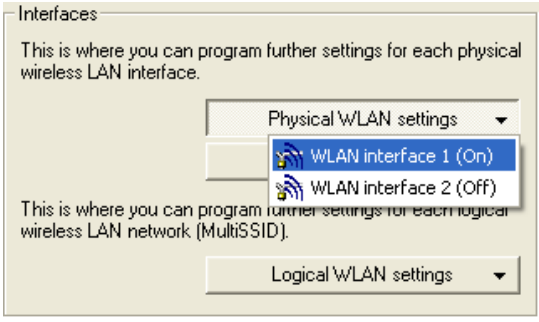


Disable Channel 2 of Interface 1 by de-selecting the checkbox (above).

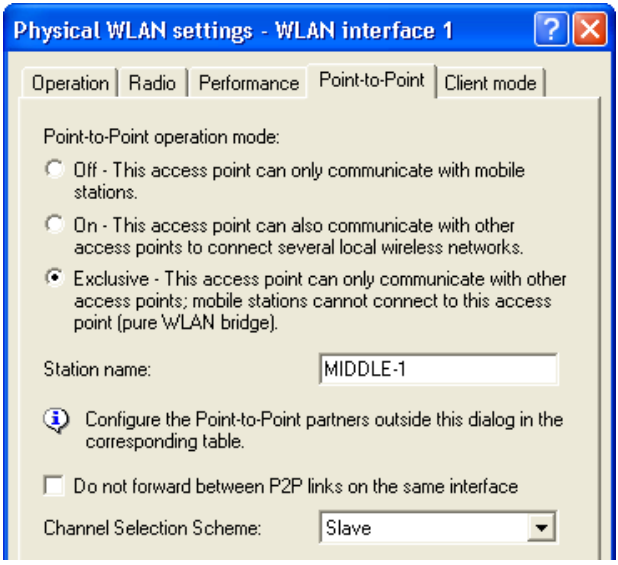
Click 'OK' to close this dialog.

Editing Physical LAN Settings for Interface 1

☐ In the `Configuration : Wireless LAN : General` dialog, click on the 'Physical WLAN settings' button, then select 'WLAN interface 1':



☐ Open the 'Point-to-Point' tab of the WLAN Interface 1 dialog (below):



Make the following edits in the Point-to-Point dialog:

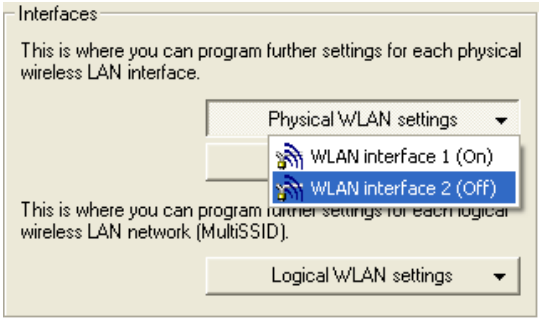
– Station name: ’MIDDLE-1’

– Channel Selection Scheme: ’Slave’

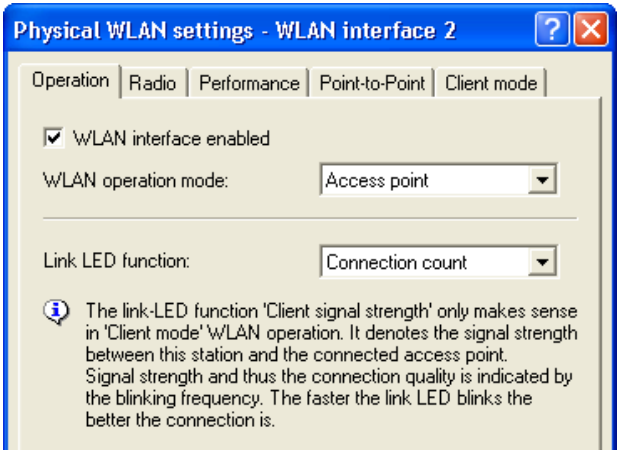
Click ’OK’.

Enabling and Configuring Interface 2

☐ Activate the PPPoE server in the `Configuration : Wireless-LAN : General` dialog, click on the 'Physical WLAN settings' button, then select 'WLAN interface 2', as shown below:

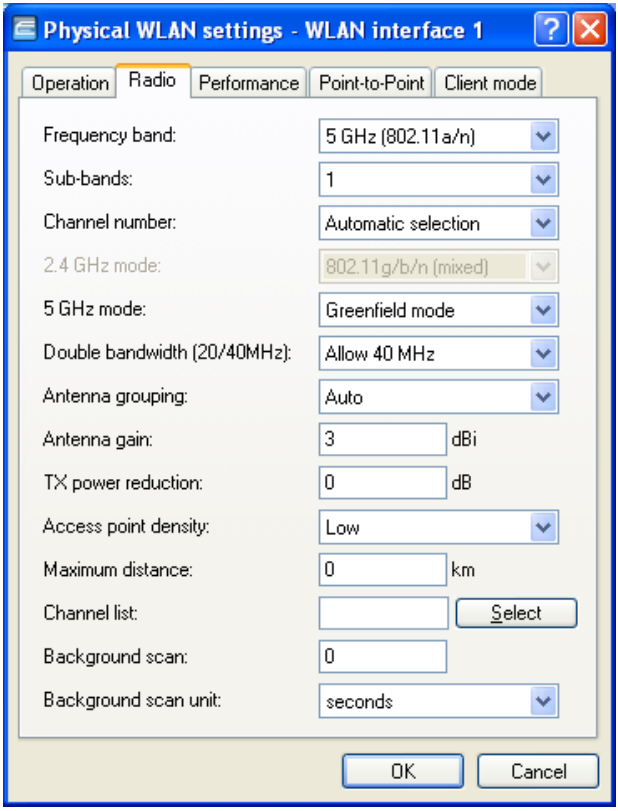


☐ Open the 'Operation' tab (below) of the WLAN interface 2 dialog:



Select 'WLAN interface enabled'.

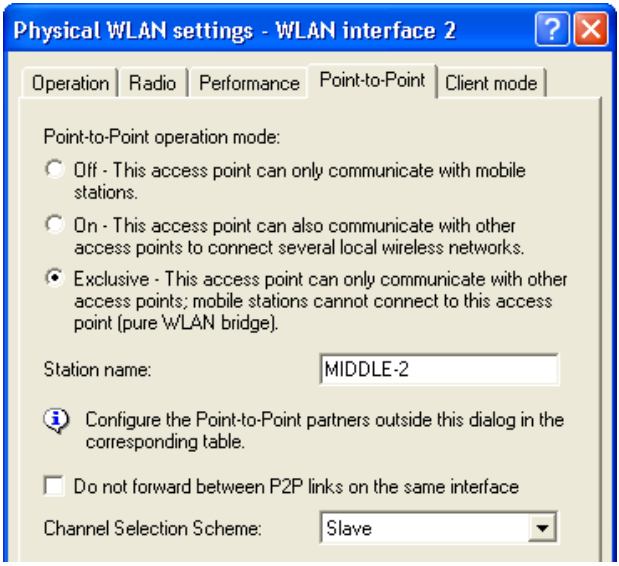
☐ Open the 'Radio' tab (below) of the same dialog:



Edit the following properties:

– Frequency band: 5 GHz (802.11a/n)
– 5 GHz mode: Greenfield mode
– Antenna gain 9 dBi

☐ Open the 'Point-to-Point' tab (below) in the same dialog:



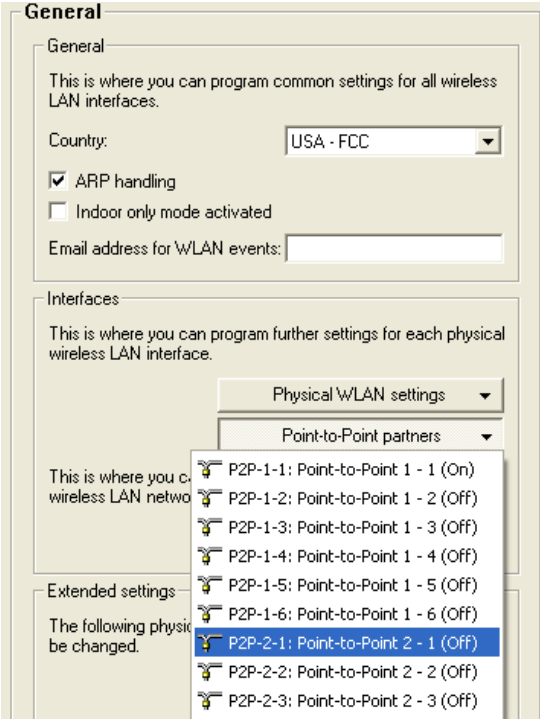
Make the following edits:

– Point-to-Point operation mode: ’Exclusive’
– Station name: ’MIDDLE-2’
– Channel Selection Scheme: ’Slave’

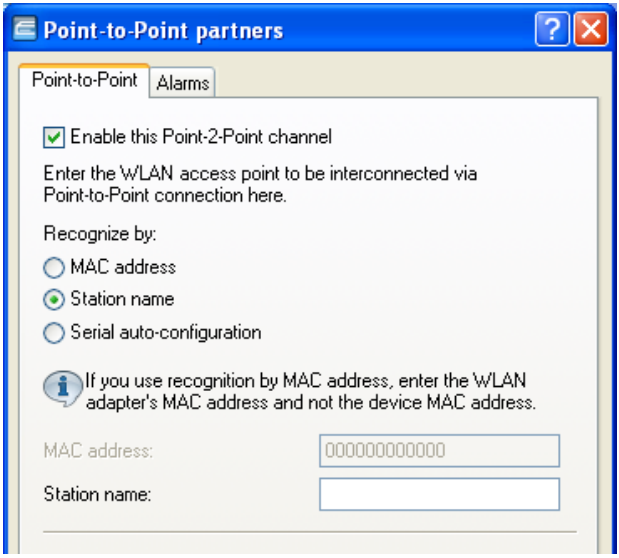
Click ’OK’.

Enabling Channel 1 on Interface 2; Specifying a P2P Partner

☐ In the `Configuration : Wireless LAN : General` dialog, click on the 'Point-to-Point partners' button, then select 'P2P-2-1, as depicted below:



☐ The P2P-2-1 Point-to-Point partners dialog (below) opens:



Use this dialog to enable this channel and identify the device that is the point-to-point partner of the MIDDLE device on this channel:

– Select ’Enable this Point-2-Point channel’, thereby enabling channel 1 of interface 2

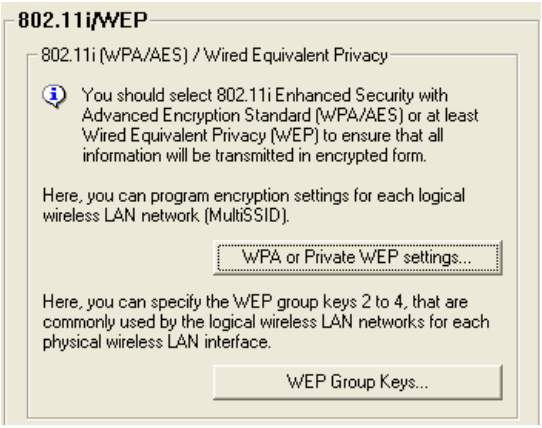
– Recognize by: ’Station name’

– Station name: ’RIGHT’

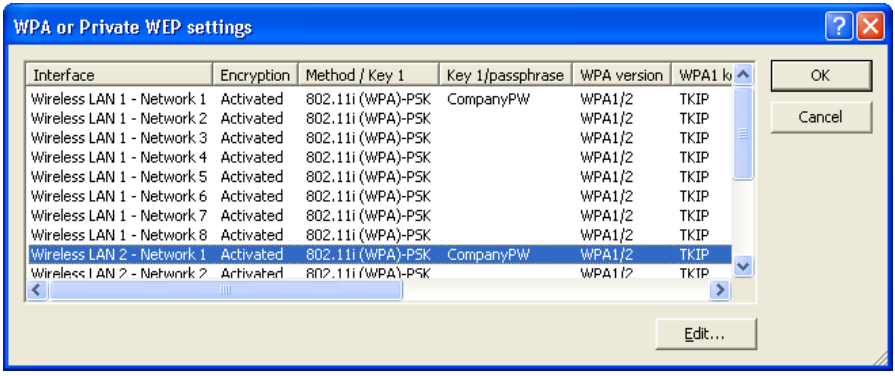
Click ’OK’.

Configure Encryption for Channel 1 on Interface 2

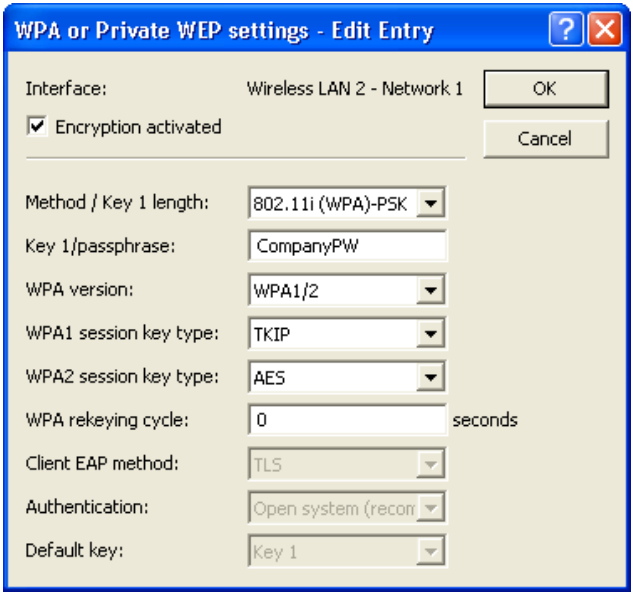
☐ Open the dialog
`Configuration : Wireless LAN : 802.11i/WEP`, below.



☐ Click on the 'WPA or Private WEP settings...' button (above) to open a list of networks (below):



☐ In the network list, select 'Wireless LAN 2 - Network 1' (above), then click 'Edit...'. The 'Edit Entry' dialog opens (below):



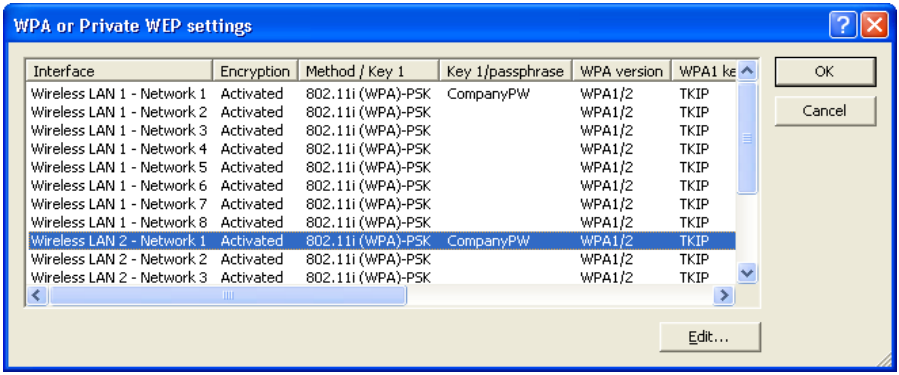
In the ‘Edit Entry’ dialog, enter the following settings for the encryption of the Interface 2 / Channel 1 network:

– Select ’Encryption activated’
– Method/Key 1 length: ’802.11i (WPA)-PSK’
– Key 1/passphrase: ’CompanyPW’

Accept the default settings for the remaining fields.

Click ’OK’ to close the dialog and return to the network list.

☐ The network list now displays P2P-2-1 as an activated network:



Click ’OK’ to close the window.

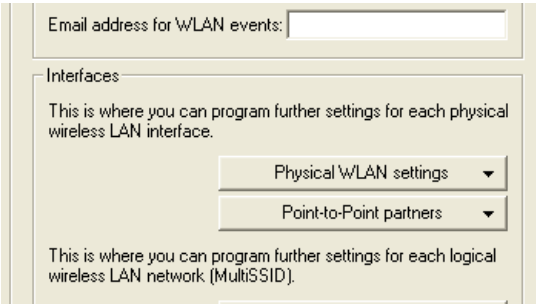
Click ’OK’ again to close the `P2P-Relay-2Radios-MIDDLE.lcf` file and save your configuration settings.

3.8.3 Configuring the LEFT Device

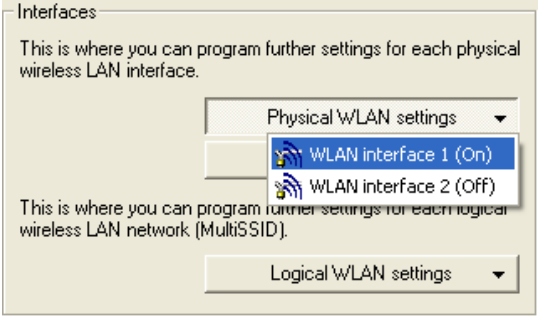
Configuring the LEFT device for service as part of a WLAN Bridge Relay is a much simpler task. The settings for this configuration are almost the same as for the LEFT device in a single radio relay design (see on page 165). Make the following configuration changes:

- Designate the LEFT device as the Master of the Point-to-Point link.
- Identify the MIDDLE-1 station as the LEFT device's Point-to-Point partner.

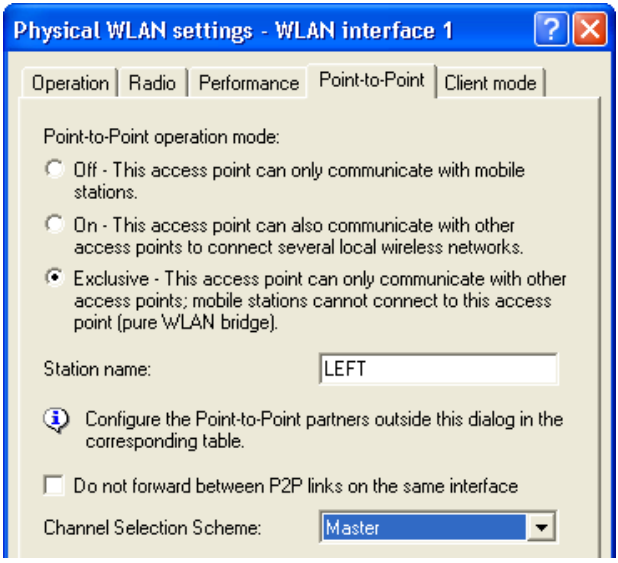
☐ Open the `P2P-Relay-2Radios-LEFT.lcf` file to the `Configuration : Wireless LAN : General` dialog:



☐ Click on the 'Physical WLAN settings' button, then select 'WLAN interface 1' (below):



☐ Open the 'Point-to-Point' tab of this dialog (below):



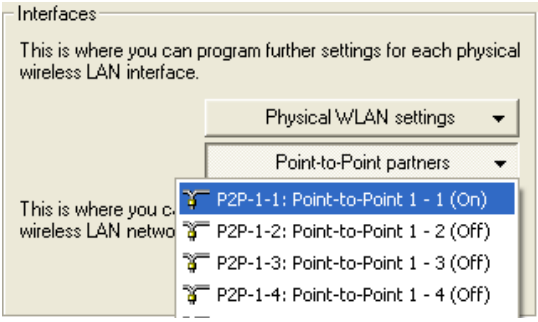
Make the following edits:

– Channel Selection Scheme: 'Master'

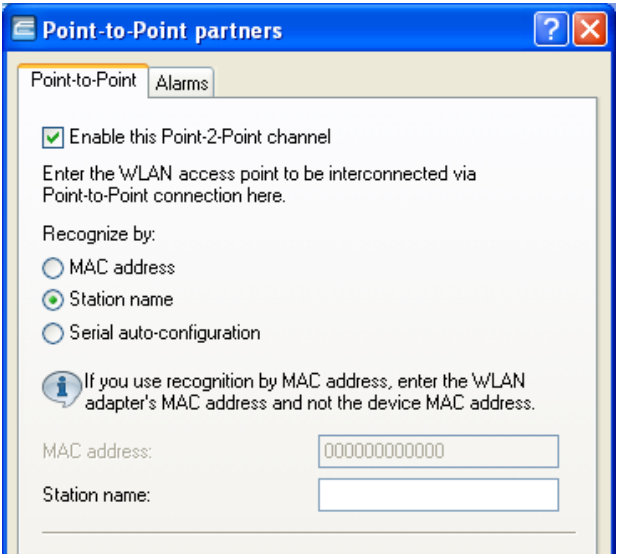
Leave the other settings in this dialog unchanged.

Click 'OK' to close the dialog.

☐ In the `Configuration : Wireless LAN : General` dialog, click the 'Point-to-Point partners' button, then select 'P2P-1-1' (below):



☐ In the Point-to-Point partners dialog, change the Station name to 'CENTER-1'.



Click 'OK' to close the dialog.

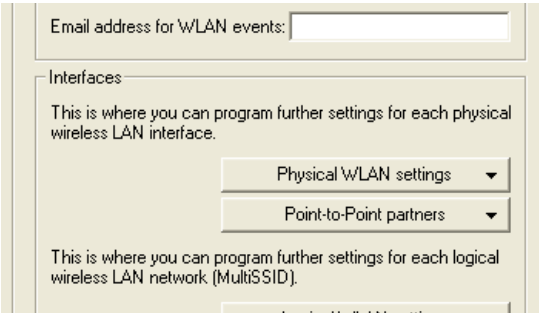
Click 'OK' again to close the `P2P-Relay-2Radios-LEFT.lcf` file and save your edits to the LEFT device.

3.8.4 Configuring the RIGHT Device

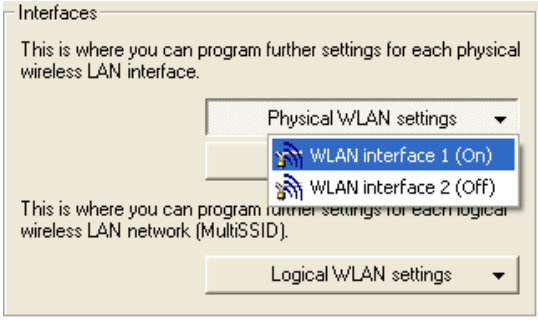
Configuring the RIGHT device for service as part of a WLAN Bridge Relay requires the virtually the same changes made to the LEFT device in the preceding section. Again, the settings for this configuration are almost the same as for the RIGHT device in a single radio relay design (see on page 176). Make the following configuration changes:

- Designate the RIGHT device as the Master of the Point-to-Point link.
- Identify the MIDDLE-2 station as the RIGHT device's Point-to-Point partner.

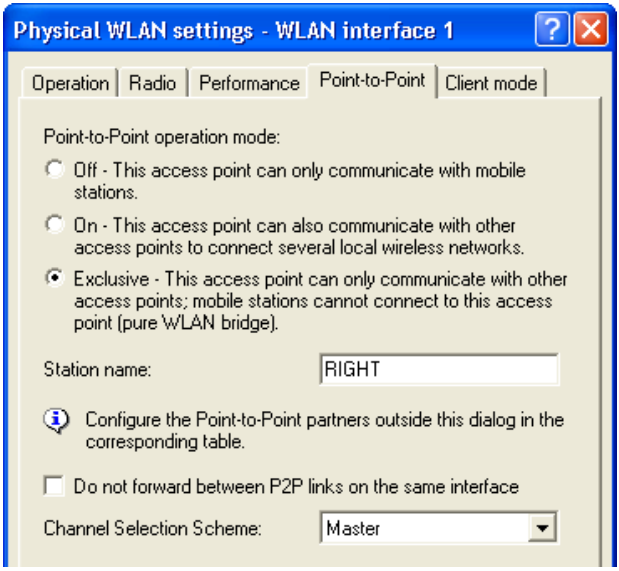
☐ In the `P2P-Relay-2Radios-RIGHT.lcf` file, open the following dialog: `Configuration:Wireless LAN:General`.



☐ Click on the 'Physical WLAN settings' button, then select 'WLAN interface 1' (below):



☐ Open the 'Point-to-Point' tab of this dialog (below):



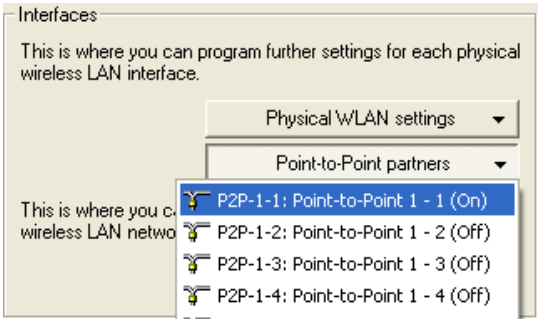
Make the following edits:

– Channel Selection Scheme: 'Master'

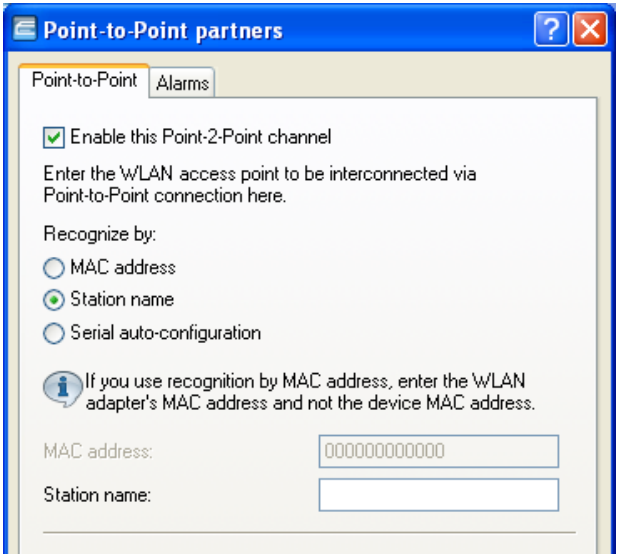
Leave the other settings in this dialog unchanged.

Click 'OK' to close this dialog.

☐ In the `Configuration : Wireless LAN : General` dialog, click the 'Point-to-Point partners' button, then select 'P2P-1-1' (below):



☐ In the Point-to-Point partners dialog, change the Station name to ’CENTER-2’.



Click ’OK’ to close this dialog.

Click ’OK’ again to close the `P2P-Relay-2Radios-RIGHT.lcf` file and save your edits to the RIGHT device.

3.9 Manual configuration of P2P connections

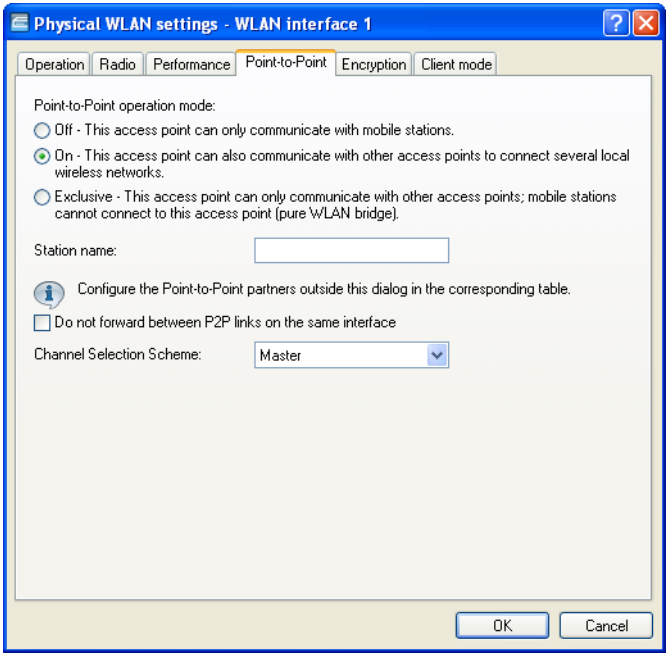
In the configuration of point-to-point (P2P) connections, enter the point-to-point operation mode and the channel selection scheme, along with the MAC addresses or station names of the remote sites. The configuration can be done in LANconfig either by using the Setup wizard "Configure WLAN" or manually using the configuration dialog.

The following steps show you how you create an encrypted or unencrypted P2P basic configuration.

Note: Along with a P2P connection, each of the APs automatically operates an SSID, the name of which is derived from the MAC address of the associated physical WLAN interface. This SSID works purely as an administrative network for establishing the connection and for the availability check ("Alive") of a point-to-point partner. It is not possible for the WLAN clients to connect to this network.

☐ Open the configuration dialog for the device that is to operate as the P2P master or P2P slave, and navigate to the page `Wireless LAN : General : Physical WLAN settings`.

☐ Select the WLAN interface which you want to use explicitly for the P2P connection and move to the tab "Point-to-Point".



☐ Enable the desired "Point-to-point operation mode", such as "On".

☐ Set the "Channel selection scheme" to "Master" or "Slave".

☐ Optional: If the remote site should identify the physical interface by an alias and not the MAC address, then enter a corresponding descriptor into the field "Station name", for example `P2P_MASTER` or `P2P_SLAVE`.

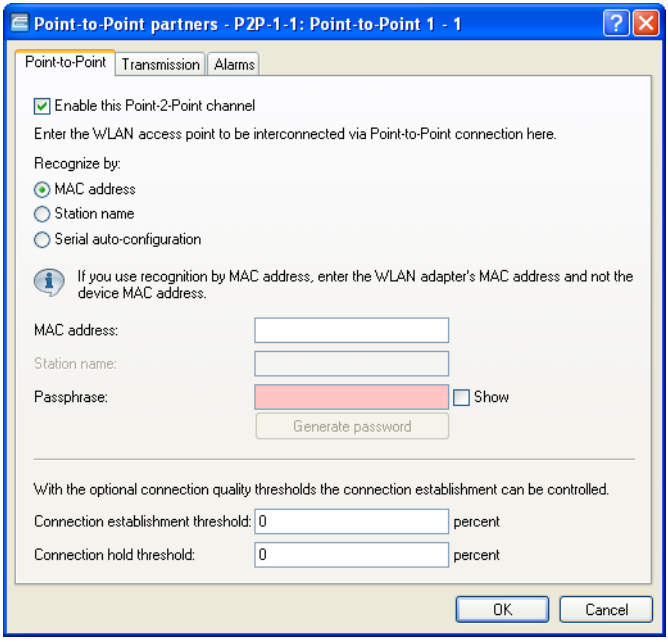
☐ Optional: Adjust the settings on the tab "P2P encryption" for the IEEE 802.11i encryption of the P2P connection, if necessary.

IEEE 802.11i can attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the Hirschmann Enhance Passphrase Security (LEPS).

The setting options are practically identical with those of the physical WLAN interfaces, . By default, P2P encryption is enabled and filled-out with meaningful values.

Note: In HiLCOS versions prior to 8.90, the settings for encryption are tied to the settings for the first logical WLAN network on the corresponding physical WLAN interface (i.e. WLAN-1 if you are using the first WLAN module for the P2P connection, WLAN-2 if you are using the second WLAN module for an access point with two WLAN modules). In this case, you find the settings under `Wireless LAN : 802.11i/WEP : WPA or private WEP settings`.

☐ Close the dialog with "OK" and under "Point-to-Point partners" on the same page of the configuration dialog select a logical P2P connection, such as "P2P-1-1".



☐ Enable the selected P2P channel on the "Point-to-Point" tab and specify whether the device identifies the remote station using a "MAC address" or a "Station name". Here you then enter either the MAC address of the physical WLAN interface which the remote station uses for the P2P connection, or its station name accordingly.

You will find the WLAN MAC address on a sticker located under each of the antenna connectors on the housing of the device. Only use the string that is marked as the "WLAN-MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.

Alternatively, you will also find the MAC address in the status menu under the WLAN statistics as Node-ID.

☐ In "Passphrase", enter a shared secret of at least 8 characters (recommended: 32 characters), which is used to additionally encrypt the P2P connection. The P2P encryption must be enabled for this (see above).

When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the access point transfers this information to register with the remote site.

☐ Optional: Move to the "Transmission" tab to enter the limits and settings for packet transmission.

The setting options are practically identical with those of the logical WLAN networks . By default, all parameters are adjusted for optimization and automatic operation.

☐ Close the dialog with "OK" and save the configuration to your device.

☐ You continue by performing the corresponding configuration steps for the remote station (slave or master).

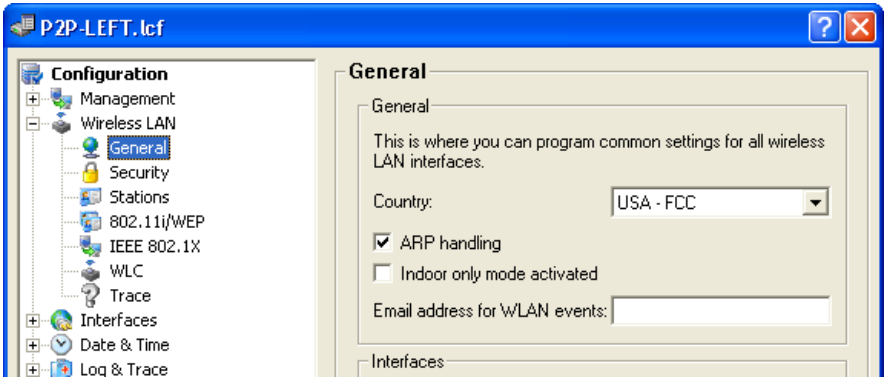
4 Configuring WLAN Parameters

This chapter describes how you can configure the WLAN parameters using either the LANconfig software or WEBconfig. The scope of WLAN settings varies according to the parameters edited. Parameters can relate to:

- A physical WLAN interface:
  Some OpenBAT devices include a single WLAN interface (i.e., one radio). Others include a second WLAN interface integrated into the device (i.e., two radios). The settings for the physical WLAN interface apply to all of the logical wireless networks supported by that interface. These parameters include, for example, the transmitting power of the antenna and the operating mode of the WLAN interface (i.e., Access Point or Client).
- A logical wireless network provided by a physical interface:
  These parameters include, for example, the SSID, or activation of the encryption, such as 802.11i with AES.
- Both WLAN and other interfaces:
  These parameters include, for example, the protocol filter in the LAN bridge.

4.1 General WLAN Settings

Open the `Configuration : Wireless LAN : General` dialog to access general WLAN settings:



Use the ‘General’ section of this dialog to configure the following settings:

- Country:
  Legal regulations for the operation of OpenBAT devices vary from country to country. Some countries prohibit the use of certain radio channels. When you select a specific country, the OpenBAT device is configured to observe the regulations of that country.
- ARP handling:
  Mobile stations that are on standby do not reliably respond to ARP requests from other network stations in the wireless network. If ARP handling is activated, the Access Point takes over this task and responds to the ARP requests on behalf of stations that are on standby.

- Indoor only mode activated:
  When selecting the frequency band (2.4 or 5 GHz), you need to determine the channels which can be used for transmission. Using the channel selection scheme, a OpenBAT — acting as wireless router — can select a free channel, thereby avoiding interference with other radio signals.

  In some countries, there are special regulations for frequency bands and channels that may be used for outdoor WLANs. Check with your local regulatory authority for more details.

  When 'Indoor only mode activated' is selected, the OpenBAT can be restricted to operating exclusively within enclosed buildings. This restriction also includes automated channel control via the automatic channel selection scheme.

  Note: The application of the 'Indoor only mode' depends on the selected 'Country'.

- E-mail address for WLAN events:
  Enter an e-mail address here to which the device will automatically mail information about WLAN events.

4.1.1 WLAN band steering

The IEEE 802.11 standard contains virtually no criteria by which a WLAN client should select the access point. While there are general guidelines according to which preference is given to an access point with a higher RSSI value (i.e. the received signal strength), for example, WLAN clients do not, in practice, adhere strictly to these definitions or the general guidelines. If both 2.4GHz and 5GHz are used to broadcast an SSID, there is normally no way of influencing the client as regards the preferred frequency band.

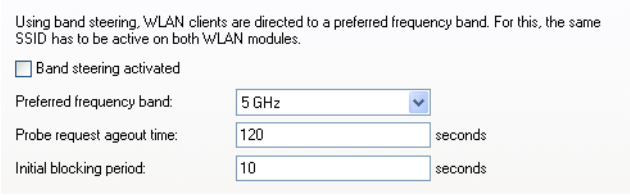
The steering of WLAN clients is based on the principle that many clients determine the available access points by means of an active scan. Active scanning here means that a client sends probe requests containing the network ID to which the client is to connect. Access points with this ID then send a test response, enabling the client to create a list of available access points. The vast majority of WLAN clients only connect to access points from which they have received a probe response, and this can be used to steer their selection process.

There are multiple, sometimes very advanced, criteria for steering. One of these criteria relates to the wireless frequency ranges used for client communication. Modern dual-band WLAN clients are expected to prefer the 5GHz frequency band over the (now) overcrowded 2.4GHz band. Band steering is the term given to purposefully assigning a WLAN client a particular frequency band or range.

The list of detected or "seen" clients contains all clients from which the access point has received a test request packet. In combination with the radio frequency on which the WLAN client sends the test request, this list is one of the bases on which the access point decides whether to respond to the request or not.

Other criteria depend on the reported client IDs and the configuration of the devices. It may be the case, for example, that fewer SSIDs are reported on the preferred frequency band than are on the one with the lower preference. Similarly, too low a transmit strength when SSIDs are reported can result in the client not receiving any probe responses at all on the preferred frequency band. For the latter scenario, it is important to ensure that the access point does not suppress probe responses on the less favored frequency band. This is controlled by the setting for minimum signal strength, which you set in LANconfg under `Wireless LAN:General:Logical WLAN settings:Network: Minimum client signal strength`.

The band steering of the access point itself is enabled and managed in LANconfig under `Wireless LAN:Band steering`.



In this window you have the following options:

- **Band steering activated**: Activates or deactivates this function.
- **Preferred frequency band**: Specifies the frequency band to which the device steers WLAN clients. Possible values are:
  - **2.4GHz**: The device routes clients to frequency band 2.4GHz.
  - **5GHz**: The device routes clients to frequency band 5GHz.
- **Probe request ageout time**: The time for which the access point steers the WLAN client to the preferred frequency band. The default value is 120 seconds.
- **Initial block time**

  If an access point with a 5-GHz DFS radio module is put into operation for the first time, and also following a restart, it cannot detect any dual-band capable WLAN clients during the DFS scan. As a result, the access point cannot direct a WLAN client to a preferred 5-GHz band. Instead, the 2.4-GHz radio module would answer the client request and forward it to the 2.4-GHz band.

  By setting an initial block time, the radio module that is configured to 2.4-GHz only responds to client requests after the specified delay. The default value is 10 seconds.

  The delayed response to the 2.4GHz probes causes WLAN clients, which would otherwise expect to find an access point in the 2.4GHz band, to scan again in the 5GHz band.

  Note: Registration of a purely 2.4-GHz WLAN client also occurs after this delay time. If no 5-GHz WLAN clients are present in the network, the delay time should be set to 0 seconds.

4.1.2 Adaptive noise immunity for reducing interference on the WLAN

A wireless LAN can be subjected to interference from various sources. Devices such as microwave ovens or cordless phones interfere with data transmission, and even the network devices themselves can emit interference and hinder communications. Each type of interference has its own characteristics. Adaptive noise immunity (ANI) enables the access point to use different error conditions to determine the best way to compensate for the interference. By automatically increasing noise immunity, the size of the radio cell can be reduced to mitigate the impact of interference on the data transfer.

The current values and any previous actions are to be found in WEBconfig under `Status:WLAN:Noise-Immunity`.

You can enable adaptive noise immunity in LANconfig under `Wireless LAN:General:Interfaces:Physical WLAN settings:Radio`.

To enable the adaptive noise immunity function, go to the Radio tab and set the value in the selection field "Adaptive noise immunity" to "On".

4.1.3 UUID Information Element for WLAN Access Points

Current Hirschmann devices are multi-SSID capable, i.e. you can simultaneously present different 'virtual' access points to multiple WLAN clients.

For devices with two radio modules (dual radio), the BSSIDs relate to the logical networks on the corresponding radio module. However, the MAC addresses of the two radio modules are completely independent of one another. Consequently, logical networks with different BSSIDs cannot be unequivocally related to a single device.

However, for the planning and monitoring of networks, it is often desirable to be able to relate logical networks to their respective devices (or radio modules).

The access points support an Aironet-compatible information element that contains the name of the device as assigned to it by the administrator. The transmission of this information is optional and many operators disable it for security reasons because they want to publish as little information as possible about the access point on the network.

Thus, this information either does not appear for network monitoring at all or, depending on the setting, the information may not identify the device as an access point.

Besides this, the access points possess a UUID (universally unique identifier), which is calculated from the device type and serial number and can identify the device uniquely on the network. By using encryption when generating the UUID, the device type or serial number can only be inferred with considerable effort (brute-force attack for all types of devices and serial numbers).

Transmission of the Aironet-compatible information element and of the UUID can be switched on or off independent of the radio module and logical network. This is done in the WEBconfig under

```
HiLCOS Menu Tree:Setup:Interfaces:WLAN:Network:Aironet-
Extensions
HiLCOS Menu Tree:Setup:Interfaces:WLAN:Network:Include-UUID
```

4.1.4 PMK Caching in the WLAN Client Mode

When establishing a connection from a WLAN client to an access point operating with 802.1x-authentication, the two stations negotiate a shared key, known as the Pairwise Master Key (PMK), for the subsequent encryption. In applications with mobile WLAN clients (laptops in large offices, moving objects with WLAN connections in the industrial sector), the WLAN clients often change the access points via which they are logged in to the WLAN network. And although WLAN clients roam back and forth between different access points, in most cases these tend to be the same ones.

Access points typically save a negotiated PMK for a certain period of time. WLAN devices in WLAN client mode also store PMKs. As soon as a WLAN client starts to login to an access point that it was previously connected to, the WLAN client can directly transfer the existing PMK to the access point. In this way, the two remote stations skip the PMK negotiation phase while establishing the connection, and the WLAN client and access point establish the connection much faster.

The WLAN client stores the negotiated PMK for the duration set under `Default lifetime`.

`HiLCOS Menu Tree:Setup:WLAN:PMK-Caching:Default-Lifetime`

4.1.5 Advanced ARP handling

As of HiLCOS version 8.90, access points can store more than one IP address per WLAN client.

`HiLCOS Menu Tree:Status:WLAN:ARP-Handling`

4.1.6 Pre-authentication in WLAN Client Mode

Fast authentication by means of the Pairwise Master Key (PMK) only works if the WLAN client was logged on to the access point previously. The WLAN client uses pre-authentication to reduce the time to logon to the access point at the first logon attempt.

`HiLCOS Menu Tree:Setup:WLAN:Encryption:Pre-authentication`

Usually, a WLAN client carries out a background scan of the environment to find existing access points that it could connect to. Access points that support WPA2/802.1x can communicate their pre-authentication capability to any WLAN clients that issue requests. A WPA2 pre-authentication differs from a normal 802.1x authentication as follows:

- The WLAN client logs on to the new access point via the infrastructure network, which interconnects the access points. This can be an Ethernet link, a WDS link (wireless distribution system), or a combination of both.
- A pre-authentication is distinguished from a normal 802.1x authentication by the differing Ethernet protocol (EtherType). This allows the current access point and all other network partners to treat the pre-authentication as a normal data transmission from the WLAN client.
- After successful pre-authentication, the negotiated PMK is stored to the new access point and the WLAN client.

  Note: The use of PMKs is a prerequisite for pre-authentication. Otherwise, pre-authentication is not possible.

- When the client wants to connect to the new access point, the stored PMK significantly accelerates the logon procedure. The further procedure is equivalent to that described under PMK caching(see page 212).

Note: On the client side, the number of concurrent pre-authentications is limited to four. This minimizes the network load on the central RADIUS server in network environments with large numbers of access points.

4.1.7 Time-staggered Roaming for Dual-radio Client WLAN Modules

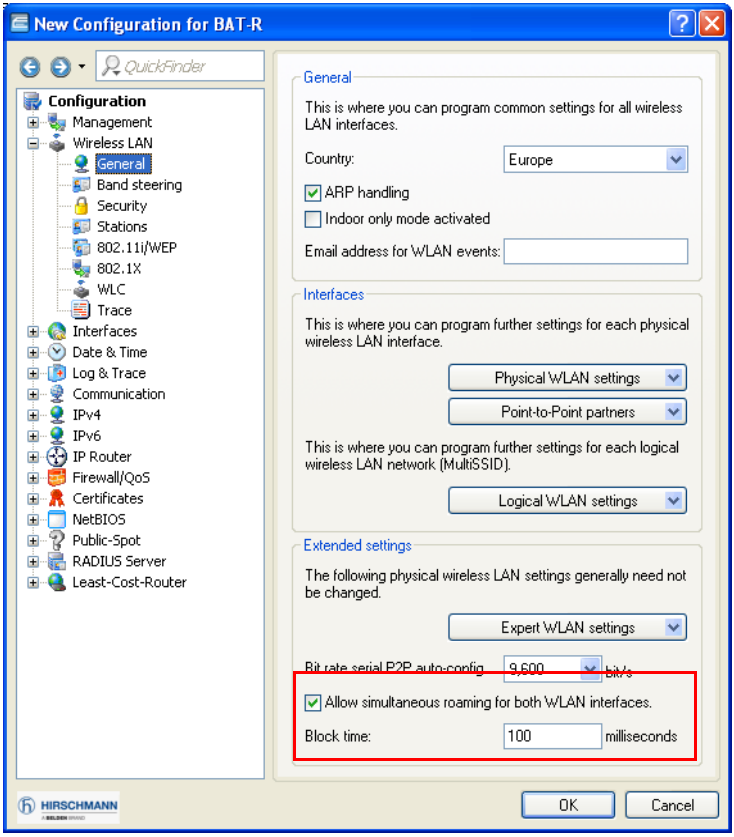
If a dual-radio client moves from a WLAN cell to an adjacent cell, multi-radio handover coordination in the device ensures that a WLAN module remains connected to the current access point until the second WLAN module is successfully logged in to the new WLAN cell.

If this function is enabled and there are one or more WLAN modules in the registration phase, the WLAN client locks the registration of the WLAN module with an existing connection. This prevents both of the modules simultaneously attempting to log in to the new cell, which would cause both WLAN connections to be lost.

If the locked WLAN module loses the data connection before one of the other modules has negotiated a new data connection, the client of this module unlocks it to negotiate a new data connection.

If the WLAN module has successfully logged in to the new WLAN cell, the other module remains connected for a minimum period (the "Block time"), so that the access point of the new cell has enough time to update its network entries. During this minimum period, this module performs no roaming and no background scanning.

Time-staggered roaming is enabled in LANconfig under `Wireless LAN:General:Extended settings:Allow simultaneous roaming for both WLAN interfaces`.



4.1.8 Greenfield Mode for Access Points with IEEE 802.11n

For access points that comply with the IEEE 802.11n standard, the physical WLAN settings provide the option to allow or restrict data transmission according to the IEEE 802.11n standard.

The IEEE 802.11n standard only allows data links that are either encrypted with WPA2/AES or unencrypted. WEP- and TKIP-based encryptions are not allowed in IEEE 802 11n. Please be aware of the following restrictions depending on the actual physical and logical WLAN settings:

Along with the selection of the individual a/b/g/n standards and a selection of mixed operating modes, the access points provide the option of using the Greenfield mode. Once activated in the physical WLAN settings for a WLAN interface, the Greenfield mode only allows WLAN clients that support the IEEE 802.11n standard to associate with the corresponding logical WLANs (SSIDs). Other WLAN clients that only work with the standards IEEE 802.11a/b/g cannot associate with these WLANs. In LANconfig, you activate the "Greenfield Mode" in the menu `Wireless LAN:General: Physical-WLAN-Settings:Radio:2.4-GHz mode`.

- If, in the Physical settings, you activate support of a mixed-mode which includes the IEEE 802.11n standard and individual WLAN clients on a logical network support WEP encryption only, then the access point will reduce the transmission rate to the 802.11a/b/g standard, because the higher transfer rates available with IEEE 802.11n are not supported in combination with WEP.
- If, in the Encryption settings for a logical WLAN network, you enable not only AES session keys but also TKIP session keys, then the access point will use only the AES session key for this WLAN, because TKIP is not supported by IEEE 802.11n.
- If, in the Encryption settings for a logical WLAN network, you enable only TKIP session keys, then the access point will reduce the transmission rate to the 802.11a/b/g standard, because the higher transfer rates available with IEEE 802.11n are not supported in combination with TKIP.

4.1.9 Maximum EIRP value depends on the transmission standard

In order to comply with the maximum transmission power density defined by the 802.11b transmission standard, the maximum available EIRP value is 18dBm. For the 802.11gn transmission standard, the EIRP value may not exceed 20dBm. As of HiLCOS 8.84, the maximum EIRP value for any OpenBAT device automatically concurs with the applicable transmission standard.

4.1.10 Automatic adjustment of multicast and broadcast transmission rates

Whereas with unicast broadcasts the access point and client can negotiate the optimum transfer rate between them, multicast and broadcast transmissions communicate in just one direction: From the access point to the client. The clients cannot report back the access point with their actual maximum transmission speeds.

The access point has two options for setting the transmission rate for multicast and broadcast transmissions:

- **Fixed bit rate**: The transfer rate is set so that the slowest client in the WLAN can receive error-free transmissions even under unfavorable conditions. This can lead to the situation that the device transmits at a lower rate sends than environmental conditions and the clients would actually allow. As a result, the access point slows down the communications in the WLAN unnecessarily.
- **Automatic bit rate**: By setting the transmission rate to auto, the access point collects information about the transmission rates of the various WLAN clients. Clients automatically notify the access point of this rate with each unicast communication. The access point takes the lowest transmission rate from the list of associated clients and applies this to all multicast and broadcast transmissions.

HiLCOS Menu Tree:Setup:Interfaces:WLAN:Transmission:Basic-Rate

4.1.11 Converting DHCP responses from broadcast to unicast

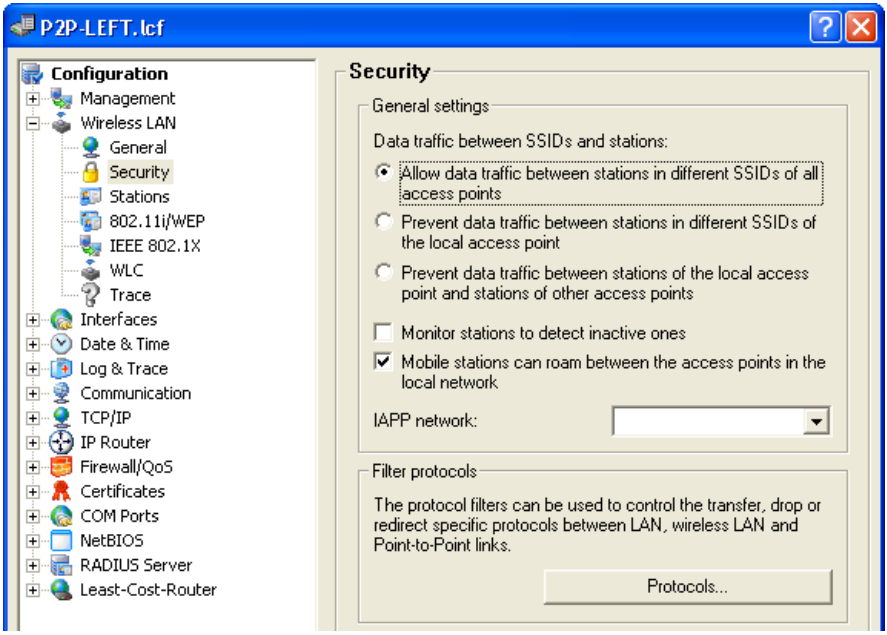
To improve the reliability of the delivery of DHCP responses on the WLAN, HiLCOS versions 8.90 and later give you the option to convert data packets which were sent as a broadcast (and which have no specific addressee, do not use optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and have a low data rate) into unicast data packets.

To achieve this in LANconfig, use the setting "Convert broadcast DHCP responses to unicast" in the dialog `Wireless LAN:General:Logical WLAN settings:WLAN network [...]:Transmission`.

Note: This function is already an integral part of the setting "Only transmit unicasts, suppress broadcast and multicasts" and does not need to be activated explicitly.

4.2 WLAN Security Settings

Open the `Configuration : Wireless LAN : Security`dialog to place limitations on the communications available to WLAN users. The device accomplishes this by filtering the data transferred between user groups, based on individual stations or the protocols used.



4.2.1 General settings

- Data traffic between SSIDs and stations:
  You can configure the OpenBAT device to allow or inhibit communication between two and among several wireless stations. Especially the OpenBAT device can:
  – Allow data traffic between stations in different SSIDs of all access points
  – Inhibit data traffic between stations in different SSIDs of the local access point
  – Inhibit data traffic between stations of the local access point and stations of other access points

  For OpenBAT devices with two radios, this setting applies globally to both radios and all WLANs.

  Note: Communications between clients in a logical WLAN are controlled separately by the logical WLAN settings (Inter-Station-Traffic). If the Inter-SSID-Traffic is activated and the Inter-Station-Traffic deactivated, a client in one logical WLAN can communicate with clients in another logical WLAN. This behavior can be controlled by the VLAN settings or protocol filter.

  For information on how to allow or inhibit data traffic between stations on the same SSID, refer to the configuration of individual wireless networks (see on page 262).

- Monitor stations to detect stations that are inactive:
  Public WLAN Access Points (public spots) recognize whether a stations is still active. This information is required for charging usage fees. The Access Point monitors client behavior by regularly sending packets to logged-in stations. If a station does not respond to these packets, the accounting system needs to recognize that the station is no longer active.

- Mobile stations can switch between base stations in the local network:
  In addition to controlling the communication between clients, you can also define whether neighboring access points can exchange information via the Inter Access Point Protocol (IAPP). IAPP controls communications between access points. Using IAPP an outgoing access point—one that is about to lose its connection with a client—receives information that its WLAN client is about to switch to a different access point. Based on this information, the outgoing access point removes the client from its list.

4.2.2 Filter protocols

Use the protocol filters to determine how the OpenBAT device will handle packets transferred from the WLAN to the LAN. This is based on the protocols identified in each packet. Protocol filters allow you to define:

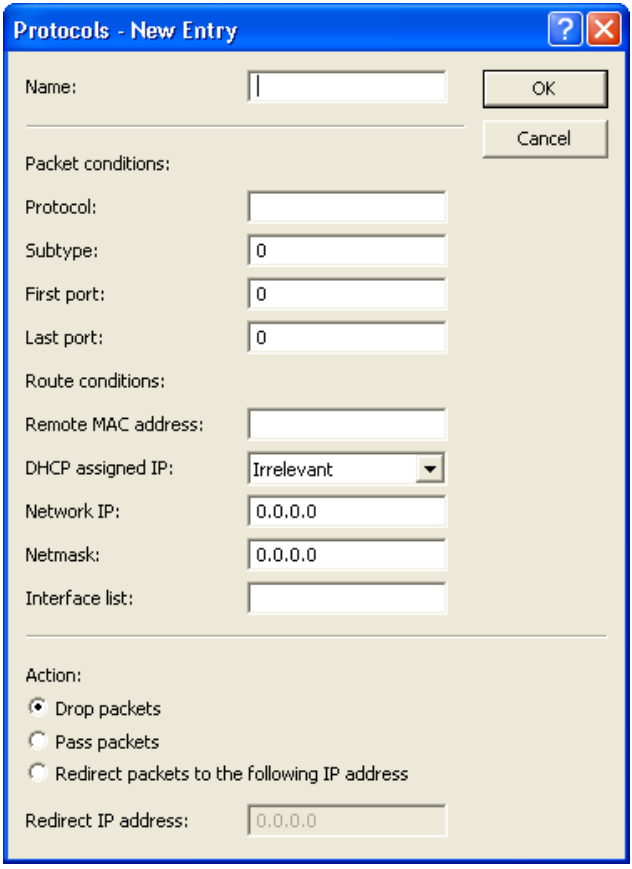
– the data packets inspected by the device
– the interfaces to which the filter is applied
– the actions the OpenBAT device should perform with respect to data packets

If no filter rules are defined for an interface, the device transmits all packets sent and received without modification. If you define a filter rule for this interface, the device checks all packets to be transmitted or received by this interface before processing them.

If one or more rules are defined for an interface, but no rule applies to a packet transmitted or received via the interface, the OpenBAT device applies a default rule to the packet. The initial default rule that comes pre-configured for each OpenBAT device is to 'drop' the packet.

The initial, pre-configured default rule is not visible in the protocol table, but can be modified. To modify the default rule for an interface, create a new rule with the name 'defaultdrop'. Then indicate the default action to be taken on a packet not covered by a specific rule. The 'defaultdrop' rule that you create can contain the name of the interface, wildcards, and the required action.

☐ Select `Configuration : Wireless LAN : Security`, then click ‘Protocols...’ to open the ‘Protocols’ table, then click `Add...` to open the ‘Protocols - New Entry’ dialog:



Similar to a firewall rule, a protocol filter consists of two parts:
– Packet conditions that need to be met before the device applies a filter to a packet
– The action the OpenBAT device takes when the packet conditions are met

A packet filter is defined by the following parameters:

- Name:
  A name of your choice for the filter entry
- Protocol:
  The protocol that this filter is valid for. If '0' is entered as the protocol, the filter applies to all packets.
- Subtype:
  The sub-protocol for which this filter is valid. If '0' is entered as the sub-protocol, the filter applies to all packets of the protocol entered.
- First port and Last port:
  The port range that this filter is to be valid for. If '0' is entered as the start port, this filter will be applied to all ports of the corresponding protocol/ sub-protocol. If '0' is entered as the end port, the start port becomes an end port.

  Note: Lists of the official protocol and port numbers are available in the Internet through www.iana.org.
- Remote MAC address:
  The MAC address of the client to which the packet is to be sent. If no destination MAC address is entered, the filter is applied to all packets.
- DHCP assigned IP:
  Enables DHCP address tracking:
  – Yes: The rule applies if the source MAC address of the packet is listed as an address which obtained an IP address using DHCP. You can view this list using the HTML-based WEBconfig tool at `HiLCOS : Status : LAN Bridge Statistics : DHCP Table`
  – No: The rule applies if the source MAC address is not listed, as described above.
  – Irrelevant: The source MAC address is not considered.

- Network IP and Netmask:
  The IP address of the network mask to which this filter applies. IP packets, whose source and destination IP addresses lie within this network, are captured by the rule. If no network is entered, the filter applies to all packets.
- Interface list:
  List of the interfaces to which the filter applies. All of the LAN interfaces, DMZ interfaces, logical WLAN networks and point-to-point connections in the WLAN may be entered as interfaces. The following examples illustrate how interfaces are specified: 'LAN-1' for the first LAN interface, 'WLAN-2-3' for the third logical WLAN network on the second physical WLAN interface, 'P2P-1-2' for the second point-to- point connection on the first physical WLAN interface. Groups of interfaces may be specified in the form 'WLAN-1-1~WLAN-1- 6' (logical WLANs 1 to 6 on the first physical WLAN interface) or with a wildcard as 'P2P-1-*' (all P2P connections on the first physical interface).

  Note: Active filter rules are those with valid entries in the interface list. A rule with no valid specification of the interfaces is ignored.

- Action:
  Action performed for the data packets captured using this rule:
  – Drop packets
  – Pass packets
  – Redirect packets to the following IP address
- Redirect IP address:
  Destination IP address for the redirect action. On redirection, the destination IP address of the packets is replaced by the Redirect IP address. Furthermore, the destination MAC address is replaced by the MAC address determined using ARP for the Redirect IP address.

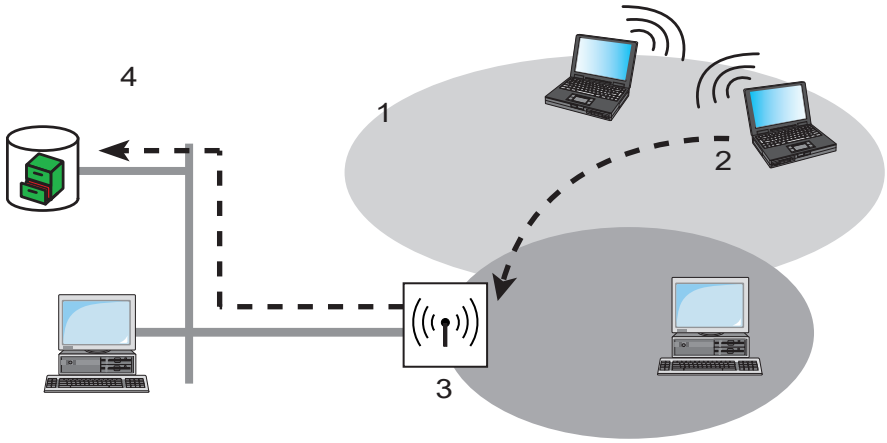
Redirect Function

With the Redirect action, IPv4 packets can be transferred and dropped, and also can be communicated specifically to a particular destination. As a general rule, the destination IP address of the packet is replaced by the Redirect IP address. The destination MAC address of the packet is replaced by the MAC address determined by ARP and associated with the Redirect IP address.

In order for the redirected packets to find the correct sender on their return trip, a dynamic table is compiled with automatic filter rules that apply to packets leaving via this interface. This table can be viewed in WEBconfig by navigating to:
`HiLCOS : Status : LAN bridge : Connection table`.
Rules in this table have a higher priority than other matching rules with the 'Transfer' or 'Drop' actions.

Clients within wireless networks often have one aspect in common: a high degree of mobility. Consequently, clients are not necessarily always connected to the same access point, but frequently change between access points and the related LANs.

The redirect function assists WLAN client applications in automatically finding the correct target computer in the LAN. If a WLAN client's http request from a particular logical wireless network is to be always directed to a particular server in the LAN, a filter setting with the redirect action can be set up for the appropriate protocol for the desired logical WLAN interface.



1: Logical WLAN on interface WLAN-1-2	3: Redirect http from WLAN-1-2 to 10.0.0.99
2: Http request 192.168.2.25	4: Server 10.0.0.99

All requests with this protocol from this logical wireless network are automatically redirected to the target server in the LAN. The returning data packets are sent to the senders' addresses and ports according to the entries in the connection statistics, enabling operation in both directions.

DHCP Address Tracking

DHCP address tracking keeps a record of which clients have received their IP addresses from a DHCP server. DHCP tracking is enabled for an interface if, for this interface, at least one rule is defined where the function 'DHCP-assigned IP' is activated.

You can configure the number of clients that connect to an interface via DHCP. Do the following:

☐ Use the WEBconfig tool to navigate to the following dialog: `HiLCOS menu tree: Setup : LAN Bridge : Port Data`, then edit the 'DHCP Limit' value.

Note: Setting the value to '0' means that any number of clients can register at this interface via DHCP. If the maximum number of DHCP clients is achieved by a further attempt to register, the device deletes the oldest entry from the list.

When the device checks data packets, it ignores IP addresses and the IP network masks defined in the rule. It does not perform any checks if the destination IP address of a packet lies within the specified range. Instead, it checks whether the source IP address of the packet matches the IP address assigned by the DHCP server. The device establishes the connection between the two IP addresses based on the source MAC address.

This check can be used to block clients which have received an IP address via DHCP, but which currently use a different IP address (either intentionally or inadvertently). The device ignores a rule in which the DHCP Source MAC address parameter is set to 'Yes' if the two addresses differ. In this case, the device applies a different rule or the default rule to the packet.

For DHCP tracking to function, define two more rules for this interface. These rules are independent of DHCP tracking. This is necessary because the required DHCP information will not be exchanged until the end of the DHCP handshake. Therefore packets to be sent beforehand need to be authorized by rules that do not use DHCP tracking. These rules usually include TCP/UDP packets on ports 67 and 68, and ARP packets.

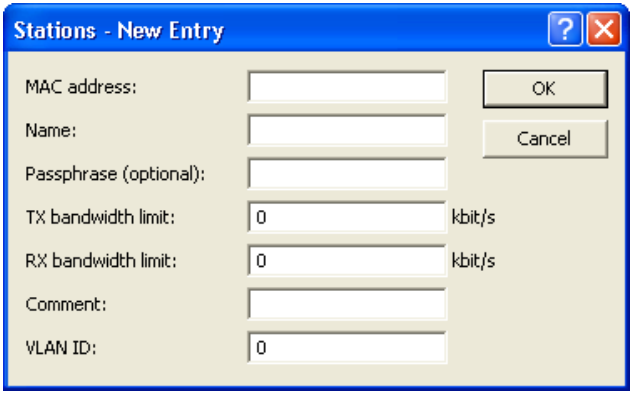
Note: If DHCP tracking is enabled for an interface, the device automatically drops the packets received on this interface from DHCP servers.

4.3 Controlling WLAN Access

A OpenBAT device used in Access Point mode can be configured to control access to the WLAN by wireless clients (referred to as 'stations'). This is accomplished by means of an access control list (ACL). The ACL can be either a whitelist (granting access to listed client stations) or a blacklist (denying access to listed client stations). Access is granted or denied based on the client station's MAC address. To add an item to the access control list:

☐ Navigate to `Configuration : Wireless LAN : Stations`.

☐ In the ‘Stations’ window, click ’Add...’ to open the ‘Stations - New Entry’ dialog (below):



Each new access control list item has the following properties:

- MAC address:
  MAC address of the WLAN Client for this entry.
- Name:
  WLAN Client name for easy identification, e.g. employee.

- Passphrase (optional):
  Passphrase for the WLAN Client in networks with 802.11i/WPA/AES-PSK.
- Tx and Rx bandwidth limits:
  Maximum send and receive bandwidth limits for this WLAN Client. The significance of the device's Tx and Rx bandwidth limits depends on the role of the device. If the device is configured as:
  - Access Point:
    –'Rx' stands for 'Send Data'
    –'Tx' stands for 'Receive Data'
  - Client:
    –'Rx' stands for 'Receive Data'
    –'Tx' stands for 'Send Data'
- Comment (optional): A user-defined comment.
- VLAN ID: The VLAN ID will be assigned to packets received from the client you are adding to the access control list. A VLAN ID set to '0' indicates the station is not assigned a specific VLAN ID. Instead, the VLAN ID for the radio (SSID) appears.

4.4 Encryption

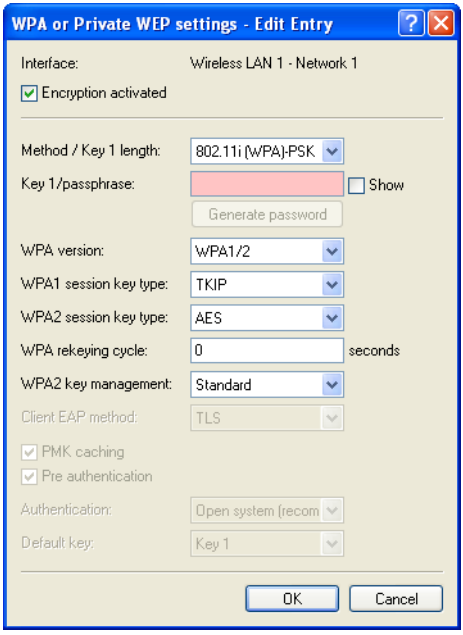
The OpenBAT device, in its role as Access Point, supports various methods for encrypting and securing data transferred over the wireless LAN.

- The IEEE standard 802.11i/WPA offers a heightened degree of security for WLAN connections. This standards employs AES-CCM ('Advanced Encryption Standard Counter with Cipher Block Chaining Message Authentication Code') which, in combination with other methods, achieves levels of security on the order of a VPN connection. When using AES-capable hardware (such as 54-Mbit WLAN clients and access points) WLAN transmissions operate at much faster speeds than VPN connections with comparable security.
- WEP ('Wired Equivalent Privacy'), which is typically employed by older WLAN hardware, is also supported. WEP is the encryption method originally incorporated in the 802.11 standard for the encryption of data in wireless transmission. This method uses keys that are 40 (WEP64), 104 (WEP128) or 128 (WEP152) bits long. However, because a number of security loopholes in WEP have been discovered, use 802.11i/WPA encryption methods wherever possible.

4.4.1 WPA and Private WEP Settings

Open the `Configuration : Wireless LAN : 802.11i/WEP` window and click on 'WPA or Private WEP settings...' to display a list of wireless LAN networks. To edit encryption for a WLAN network:

☐ Select a network in the list, then click 'Edit...' to open the 'WPA or Private WEP settings - Edit Entry' dialog:



Use this dialog to edit the following encryption parameters:

☐ **Enable encryption**

Enable or disable encryption for this WLAN interface.

☐ **Method/key 1 length**

Set the encryption method to be used here. Possible values are:

– 802.11i (WPA)-PSK – Encryption according to the 802.11i standard offers the highest security. The 128-bit AES encryption used here offers security equivalent to that of a VPN connection. Select this setting if no RADIUS server is available and authentication is based on a pre-shared key.

– 802.11i (WPA)-802.1x – If authentication is handled by a RADIUS server, select the option '802.11i (WPA)-802.1x'. When using this setting, additionally ensure that the RADIUS server is configured in the 802.1x settings.

– WEP 152, WEP 128, WEP 64 – encryption according to the WEP standard with key lengths of 128, 104 or 40 bits respectively. This setting is only to be recommended when the hardware used by the WLAN client does not support the modern method.

– WEP 152-802.1x, WEP 128-802.1x, WEP 64-802.1x – encryption according to the WEP standard with key lengths of 128, 104 or 40 bits respectively, and with additional authentication via 802.1x/EAP. This setting is also only to be recommended when the hardware used by the WLAN client does not support the 802.11i standard. The 802.1x/EAP authentication offers a higher level of security than WEP encryption alone.

☐ **Key 1/passphrase**

In line with the encryption method activated, you can enter a special WEP key for the respective logical WLAN interface or a passphrase when using WPA-PSK:

– The passphrase, or the 'password' for the WPA-PSK method, is entered as a string of at least 8 and up to 63 ASCII characters.

– The WEP key 1, that applies only to its respective logical WLAN interface, can be entered in different ways depending on the key length. Rules for entering the keys can be found in the description of the WEP group key.

Note: Please be aware that the security of this encryption method depends on the confidential treatment of this passphrase. Passphrases should not be made public to larger circles of users.

☐ **WPA version**

WPA version for encryption offered by the access point to the WLAN clients.

– WPA1: WPA2 only
– WPA2: WPA2 only
– WPA1/2: WPA1 and WPA2 in one SSID (radio cell)

☐ **WPA 1 session key type**

If '802.11i (WPA)-PSK' has been entered as the encryption method, the procedure for generating a session or group key for WPA 1 can be selected here:

– AES – the AES method will be used.
– TKIP – the TKIP method will be used.
– AES/TKIP – the AES method will be used. If the client hardware does not support the AES method, TKIP will be used.

☐ **WPA 2 session key type**

Procedure for generating a session or group key for WPA 2.

☐ **WPA2 key management**

Here you specify which standard the WPA2 key management should follow. Possible values are:

– Standard: Enables key management according to the standard IEEE 802.11i without fast roaming and with SHA-1 based keys. Depending on the configuration, the WLAN clients in this case must use opportunistic key caching, PMK caching or pre-authentication.
– SHA256: Enables key management according to the standard IEEE 802.11w with SHA-256 based keys.
– Fast roaming: Enables fast roaming as per 802.11r
– Combinations of the three settings

Important: Although it is possible to make multiple selections, this is advisable only if you are sure that the clients attempting to login to the access point are compatible. Unsuitable clients may refuse a connection if an option other than "Standard" is enabled.

☐ **WPA rekeying cycle**

A 48-bit long initialization vector (IV) impedes attackers in their attempts to calculate the WPA key. The true key consisting of the IV and WPA key only repeats every 16 million packets. In high-traffic WLANs, the key is repeated only after several hours. To avoid repetition of the key, WPA automatically renegotiates the key at regular intervals. This takes place before repetition of the key.

Enter a value in seconds after which the key is renegotiated.

The standard value is '0' and the key is not negotiated in advance.

☐ **Client EAP method**

Hirschmann access points in WLAN client operating mode can authenticate themselves to another access point using EAP/802.1X. To activate the EAP/802.1X authentication in client mode, the client EAP method is selected as the encryption method for the first logical WLAN network.
Please note that the selected client EAP method must match the settings of the access point that this Hirschmann access point is attempting to register with.

Note: In addition to setting the client EAP method, also be sure to observe the corresponding setting for the WLAN client operation mode. The client EAP method setting has no function on logical WLAN networks other than WLAN 1.

☐ **Authentication**

If the encryption method was set as WEP encryption, two different methods for the authentication of the WLAN client are available:

– The 'Open system' method does not use any authentication. The data packets must be properly encrypted from the start to be accepted by the access point.

– With the 'Shared key' method, the first data packet is transmitted unencrypted and must be sent back by the client correctly encrypted. This method presents potential attackers with at least one data packet that is unencrypted.

☐ **Default key**

If WEP encryption is selected, the access point can select from four different WEP keys for each logical WLAN interface:

– Three WEP keys for the physical interface

– An additional WEP key particular to each logical WLAN interface

The private WEP settings are used to set the additional key for each logical WLAN interface (see 'Key 1/passphrase'). You should also select which of the four keys is currently to be used for the encryption of the data (default key). This setting can be used to change the key frequently, so increasing security.

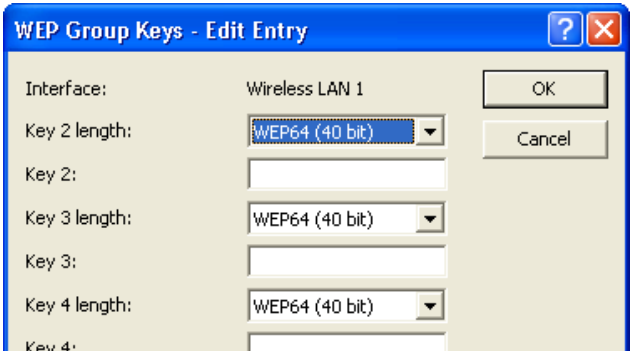
Rules for entering the keys can be found in the description of the WEP group key.

4.4.2 WEP Group Keys

The WEP method uses keys of 40 (WEP64), 104 (WEP128) or 128 (WEP152) bits in length. Each WLAN interface has four WEP keys: a special key for each logical WLAN interface and three common group WEP keys for each physical WLAN interface. If 802.1x/EAP is in use and the 'dynamic key generation and transmission' is activated, the group keys from 802.1x/EAP will be used and are consequently no longer available for WEP encryption. To enter group keys:

☐ Open the `Configuration : Wireless LAN : 802.11i/WEP` dialog and click on 'WEP Group Keys...' to open a window displaying the WLAN interfaces and their associated group keys.

☐ In the 'WEP Group Key' window, select an interface, then click 'Edit...' to open the 'WEP Group Key - Edit Entry' dialog:



Use this dialog to specify the length and setting for Group Keys 2, 3 and 4.

Rules for Entering WEP Keys

WEP keys can be entered as ASCII characters or in hexadecimal format. The hexadecimal format begins with the characters '0x'. Key length depends on the WEP method:

Method	ASCII	Hex
WEP 64	5 characters Example: aR45Z	10 characters Example: 0x0A5C1B6D8E
WEP 128	13 characters	26 characters
WEP 152	16 characters	32 characters

The ASCII character set includes the characters '0' to'9', 'a' to 'z', 'A' to 'Z' and the following special characters:
! ' # $ % & ´ () * + , - ./ : ; < = > ? @ [\ ] ^ _ ‘ { | } ~

The HEX form uses the numbers '0' to '9' and the letters 'A' to 'F' to display each character as a character pair, which is why twice the number of characters is required to display a HEX key.

Select the length and the format (ASCII or HEX) of the key depending on the most suitable option available in the wireless network cards that register with your WLAN. If the encryption in an access point is set to WEP 152, some clients may not be able to log into the WLAN as their hardware does not support the key length.

4.4.3 Group key per VLAN

The following section provides you with explanations of managing group keys in VLAN.

Introduction

In a VLAN environment, the central network management generally assigns a unique VLAN ID to each virtual network. Membership of a VLAN is usually via the physical connection by means of which the respective network client is connected to the network.
The central station managing the network (e.g. a VLAN-capable switch) assigns internally defined VLAN IDs to its ports. If a data packet is now received at a port, the device only forwards it internally to the ports with corresponding VLAN IDs. All the other network subscribers that are connected at ports with different VLAN IDs, or with no VLAN ID, do not receive any of these data packets.

If there are multiple VLANs with different service scopes, the separation of the data communication is usually effected via the assignment to different logical WLAN networks (SSIDs). For example, via a special SSID, employees are given access to the company network and the internet, while guests are only given restricted access to the internet via a different SSID.
Hirschmann Access Points also manage the assignment of WLAN clients to individual VLANs in VLAN network tables. In comprehensive network environments, a RADIUS server usually manages the access rights and the assignment of clients to the VLANs used. After successful authentication, the RADIUS server returns the data to the corresponding access point, which saves it in its VLAN network table for the duration of the client login.
Through the dynamic VLAN network tables in the access points, the various WLAN clients logged into the same access point receive different VLAN IDs, if required. The VLAN-internal communication is effected securely via a session key mediated at the access point during the login. Thus the data transmission of the clients in different VLANs is isolated, even though each client uses the same logical WLAN network (SSID) for the communication with the access point.
When a clients logs in at an access point of a WLAN network, it is also assigned a group key for receiving Broadcast or Multicast messages. Broadcast and Multicast messages do not support VLAN tagging. Therefore, there is no option to exclude WLAN clients that are located in an isolated VLAN from receiving these messages. In the best case, the WLAN clients ignore the communication via VLAN-external Broadcast and Multicast messages.
However, as these messages are increasingly used for the network configuration, the following problems arise:

- Network protocols such as “UPnP” and “Bonjour” use these messages to announce new services in the network.
  Therefore, WLAN clients may have the option to set up access to servers to which they have no access.
- Internet standard IPv6 uses Multicast transmissions to send router information to the clients.
  There is a risk of VLAN-external WLAN clients taking this information and thus withdrawing their access to the VLAN for which they are actually registered.

With the increased usage of IPv6, these client problems are likely to become more widespread.

To avoid these problems, instead of assigning a group key valid for all WLAN clients, the access point assigns a separate group key to every VLAN used. Therefore, it sends its Broadcast and Multicast transmissions only to a specific VLAN and to the clients registered there. The WLAN clients of other VLANs do not have access for these transmissions.

Note: The IEEE 802.11 standard only permits the management of 4 different keys. One key is always reserved for the secure Unicast communication between the access point and a WLAN client.

Therefore, in general a maximum of 3 separate VLANs manage their own group key. The respective group keys are either managed automatically by the access point or manually by the network administrator. When the WLAN client is logging into the network, the access point gives the client the related VLAN group key for encrypting all the Broadcast and Multicast transmissions intended for its VLAN.
Therefore, there are 2 possible scenarios:

- There is a maximum of 3 VLANs set up in the area of an access point: Due to the 3 specific VLAN group keys, these VLANs are securely isolated from each other.
- There are more than 3 VLANs in the area of an access point: Here, at least 2 VLANs share a group key. The administrator divides the shared group keys optimally among the VLANs.

The management of the VLAN group keys is performed in 2 tables:

- The configuration table, in which the assignment is performed manually by the administrator.
- The status table, in which the automatic group key assignment can be read by the access point.

Management of VLAN group keys

To use different VLAN IDs in a logical WLAN network (SSID), you assign the corresponding group key for Broadcast and Multicast transmissions. In LANconfig, you find this setting under `Wireless-LAN:802.11i/WEP:Advanced Settings:VLAN Group Key Assignment`

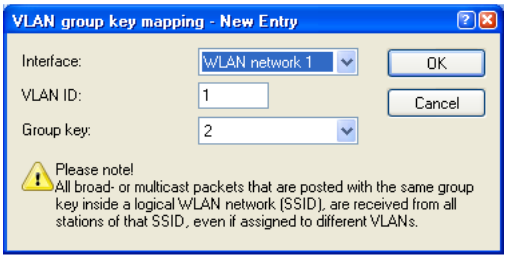


Figure 8: Assigning group key for Broadcast and Multicast transmissions

The automatic assignment of group keys is performed in the following steps:

- ☐ When a WLAN client logs in, the access point checks whether its VLAN ID is already listed in the status table, and is accordingly assigned to a group key.
- ☐ If there is no listed VLAN ID, the access point uses the configuration table to check whether there is a manual assignment, and in this case adds a correspondingly mapped entry to this table.
- ☐ If there is no manual assignment either, the access point adds a new entry and assigns the group key with the fewest subscribers to this client.

You will find the status table with the current automatic VLAN group key assignments for each SSID under `HiLCOS menu tree Status:WLAN:VLAN group key mapping`

Enhancements in the menu system

The table contains the assignments of the VLAN group keys to the logical WLAN networks.

- **SNMP ID:**
  2.12.70
- **Telnet path:**
  `Setup:WLAN:VLAN group key mapping`
- **Network**

Contains the name of a WLAN network registered in the device

- **SNMP ID:**
  2.12.70.1
- **Telnet path:**
  `Setup:WLAN:VLAN group key mapping`

▶ **VLAN ID**
Contains the VLAN ID assigned to the logical WLAN network

- **SNMP ID:**
  2.12.70.2
- **Telnet path:**
  `Setup:WLAN:VLAN group key mapping`
- **Possible values:**
  1 to 4094
- **Default:**
  1

▶ **Group key index**
The table contains the group key index.

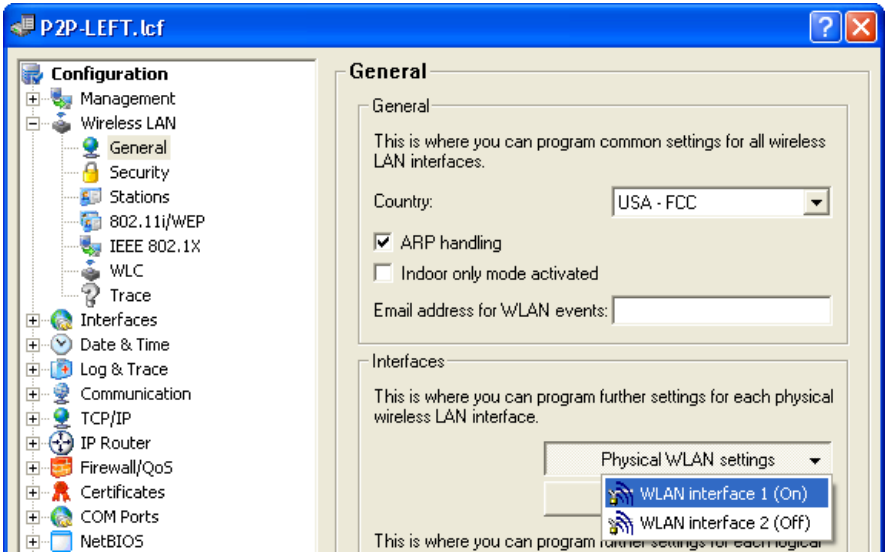
- **SNMP ID:**
  2.12.70.3
- **Telnet path:**
  `Setup:WLAN:VLAN group key mapping`
- **Possible values:**
  1 to 3

4.5 Physical WLAN Interfaces

A OpenBAT device can contain either one or two radios, also referred to as physical WLAN interfaces.This section describes the settings that apply to a radio in the OpenBAT device. To access these settings:

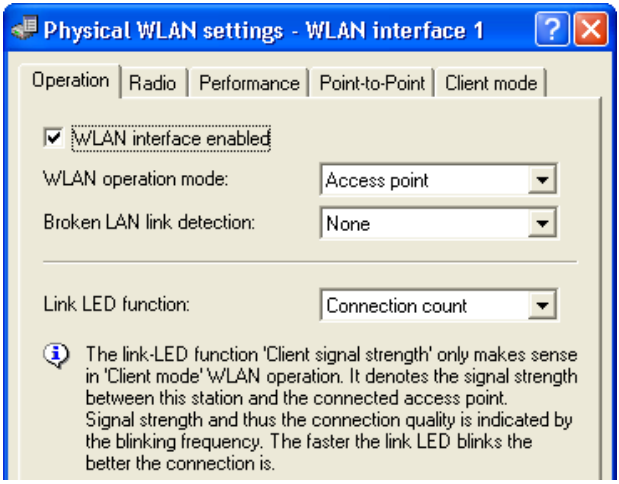
☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ In the Interfaces section, click 'Physical WLAN settings...' and select an interface:



☐ Click on a tab in the 'Physical WLAN settings' dialog to display and configure radio module settings, as described below.

4.5.1 Operation Settings



You can configure the following settings in the ‘Operation’ dialog:

- WLAN interface enabled:
  Select this to turn ON the selected WLAN interface.
- WLAN operating mode:
  The OpenBAT device can be operated in the following modes:
  – Access point: The device connects WLAN clients to the cabled LAN.
  – Client: The OpenBAT device acts as a client. It searches for a connection to an Access Point and attempts to log into a wireless network. If successful, the OpenBAT device links a cabled network device to an Access Point over a wireless connection.

- Broken LAN link detection:
  The device can detect if the link between the WLAN interface and the associated cabled LAN is lost. In this case, you can configure the behavior of the WLAN interface:
  – None: No action is taken
  – LAN-1: The WLAN interface will be disabled if its connection to LAN-1 is lost.
  – LAN-2: The WLAN interface will be disabled if its connection to LAN-2 is lost.

- Link LED function:
  When setting up point-to-point connections or operating the device as a WLAN client, you can approach an optimal antenna positioning by viewing a real-time measure of the signal strength that is achieved when you place the antenna in different positions. If 'Link LED function' is selected, the WLAN link LED (located on the face of the device) can be used to measure the signal quality during device set-up—the faster the LED blinks, the better the signal. The selections are:
  – Connection count: The WLAN link LED uses inverse flashing to display the number of WLAN Clients that are logged onto this Access Point. The WLAN link LED pauses for a short while after it has indicated the number of clients by flashing. Select this operating mode when you are operating the OpenBAT device in Access Point mode.
  – Client signal strength: The WLAN link LED displays the signal strength of the connection between the device (as client) and another Access Point with which the device has registered as WLAN Client. The faster the LED flashes, the better the signal. This should be selected only when you are operating the OpenBAT in client mode.
  – P2P-1 to P2P-6 signal strength: The WLAN link LED displays the signal strength of a connection between the OpenBAT device, in the role of Access Point, and a P2P partner. The faster the LED flashes, the better the signal.

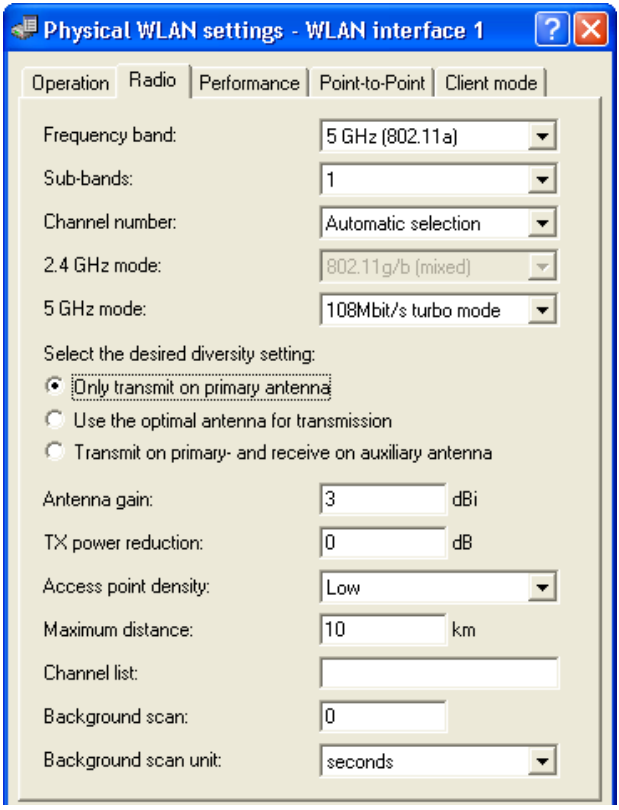
4.5.2 Radio Settings

Use the Radio dialog to configure the frequency, channel, and antenna parameters for the selected WLAN interface. To open this dialog in the LANconfig software:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ In the Interfaces section, click 'Physical WLAN settings...' and select an interface.

☐ Click on the 'Radio' tab to display and configure radio module settings, as described below.



You can configure the following settings in the ‘Radio’ dialog:

- Frequency band and Sub-bands:
  Select either:
  – 2.4 GHz
  – 5 GHz
  This selection determines the available radio channels. If you select the 5 GHz band, you also need to select a sub-band, which is linked to certain radio channels and maximum transmission powers.

  Note: Some countries require the Dynamic Frequency Selection (DFS) method for automatic channel selection. Selecting a sub-band defines the channels that are available for automatic channel selection. DFS selects an unused channel to avoid interference with radar systems, or to distribute channel links to individual wireless devices evenly over the selected frequency.

  Using DFS, the OpenBAT device performs a scan of available channels before selecting an unused channel. The channel scanning process takes about 60 seconds and produces a list of used and unused channels for the selected frequency band. The OpenBAT device refers to this list when it assigns a channel. By default, the OpenBAT performs a scan at initial boot-up and again when, after a lapse of 24 hours from the previous list creation, it detects radar signals or other interferences on a channel.

  To prevent the automatic scan - and the associated 60 second pause in communication - from occurring at an inconvenient time, you can use the 'Background scan' parameters in this dialog to schedule the time of the scan. One option is to define a cron job, e.g. '1,6,13' for a DFS scan at 01:00h, 06:00h or 13:00h, or '0-23/4' for a DFS scan between 0:00h and 23:00h every 4 hours. Time-controlled DFS scans require that the device is set with the correct system time.

- Channel number:
  Select one of the following:
  – Automatic selection: The OpenBAT device employs DFS to automatically select an unused channel.
  – A specific channel from the channel list.

  Note: In the 2.4 GHz frequency band, two adjacent wireless networks need to be assigned channels that are separated by at least 3 channel numbers to avoid interference.

- 2.4 GHz mode:
  Select the 2.4 GHz frequency band standard that applies to your network.

  Note: Clients supporting just the lower standards may not be able to register with the WLAN if this parameter is set to a high standard that supports faster speeds exclusively. Compatibility is always achieved at the expense of performance. Make the selection that is necessary for actual wireless LAN clients.

  Note: If all wireless network devices support 802.11n, select Greenfield mode to achieve the optimal throughput.

- 5 GHz mode:
  Select the operating mode for this 5GHz frequency band:
  – 54 Mbit/s mode
  – 108 Mbit/s turbo mode

  Note: Turbo mode uses two neighboring vacant channels to double the transfer speed. However, when an access point is configured for 108 Mbit/s turbo mode, clients also need to support this standard to be able to communicate with the access point.

  Note: If all wireless network devices support 802.11n, select Greenfield mode to optimize throughput.

- Double bandwidth (20/40 MHz):
  Devices that support the 802.11n standard can be configured to employ a transmission range of either:
  – 40 MHz, with 96 carrier signals (the default)
  – 20 MHz, with 48 carrier signals
  The default selection of 40 MHz can double the data throughput on the channel.

- Antenna grouping:
  A OpenBAT device that supports the 802.11n standard can use up to three antennas for transmitting and receiving data. You can use multiple antennas to improve either data throughput (via spatial multiplexing) or wireless coverage (via cyclic shift diversity (CSD)). Choose the option that fits your application:
  – Auto: All available antennas are used.
  – Antenna 1: Select this if your device is connected to just one antenna.

- Antenna 1+2, or Antenna 1+3: Select this for an application that works with 2 parallel data streams. For example, point-to-point links with appropriate dual slant antennas. The unused antenna port is deactivated.
- Antenna 1+2+3: Select this setting to connect wireless LAN clients when using the device in Access Point mode.

Note: Always use antenna port 1. Depending on the mounting and cabling, connect the second antenna either to port 2 or port 3. Keep in mind that the configuration of the device software needs to correspond to the actual antenna connections.

▶ Antenna diversity settings:
Specify which antennas should be used for transmission and for reception:
- Only transmit on primary antenna: (Default) The antenna connected to the Access Point's main connector is used for data transmission. For reception (RX), the device selects the antenna with the strongest signal (at Main or AUX).
- Automatically select the best antenna for transmission: If you apply the diversity function to transmission (TX) as well, the device selects the antenna with the strongest signal.
- Transmit on primary, and receive on auxiliary antenna: Only the main antenna is used for transmission; the antenna at the AUX port is preferred for reception. Using this alternative, high-performance antennas that are legally prohibited from transmitting can be used for reception.

- Antenna gain & TX power reduction:
  Where the transmission power of an antenna exceeds the levels permitted in the country of operation, use these settings to attenuate the antenna power:
  - Antenna gain:
    This setting equals the gain of the antenna minus the attenuation caused by the cables used and/or a surge arrestor. It is used to dynamically calculate and apply the maximum permissible antenna power taking into consideration other parameters, including country, data rate and frequency band.
  - TX power reduction:
    This setting causes a static reduction in the power by the value entered, and ignores the other parameters. The reception sensitivity (reception antenna gain) remains unaffected. This option is useful, for example, where large distances have to be bridged by radio when using shorter cables. The reception antenna gain can be increased without exceeding the legal limits on transmission power. This leads to an improvement in the maximum possible range and, in particular, optimized data transfer rates.
- Access point density:
  Use this parameter to control the receiver's sensitivity. This can be helpful in reducing the radius of a particular access point in case of a high density access point structure.
- Maximum distance:
  Increase the value of this parameter to also increase the wait time for transmission responses. This distance is converted into a time delay that can be applied to wireless communications.
- Channel list:
  Use this parameter to input a list of channels to which the OpenBAT device will be restricted when automatically assigning a channel number via automatic channel selection. If just one channel is entered, only this channel will be used and there will be no automatic selection. Therefore, when entering a channel number, be certain that it is available in the frequency band of the respective country. As long as radar pulse detection is enabled, the channels entered here are merely privileged. If these channels are affected by radar pulses, the device tries to switch to other channels which are not part of the list. Only when radar pulse

detection is disabled by selecting the 'Indoor Only' mode will the channel selection be exclusive. Enter any comma-separated list of channels to which the automatic selection shall be limited, e.g. '3,5,7'. With the instruction '1,7-9,13', for instance, only channels 1, 7 through 9 and 13 would be considered in the automatic channel selection.

Note: If the channel number is assigned via 'Automatic channel selection', this setting is not exclusive. An automatically assigned channel may be changed if it interferes with, for example, radar signals. You can configure an exclusive channel assignment for indoor operation by selecting 'Indoor only mode activated' in the General section of the `Configuration : Wireless LAN : General` dialog.

- Background scan interval:
  Use this option for the OpenBAT device to periodically search the active frequency band for accessible Access Points or wireless networks. Entering a non-zero value overwrites the default settings for this search (as described in the section 'Frequency band and sub-bands' above).

  The value of this parameter depends on the role of the OpenBAT device. If the device is used as:
  – Access Point: The background scan function can be used to detect rogue AP attacks. The scan interval should correspond to the time span within which unauthorized Access Points should be detected, e.g. 1 hour.
  – Client: Activate the background scan to improve mobile WLAN Client roaming. To achieve fast roaming, the scan time is limited to, e.g. 260 seconds here.

- Background scan unit:
  The time unit for the interval value specified in the 'Background scan' parameter.

  Note: To avoid adverse effects on data transfer rates, the interval between channel scans in a OpenBAT device is at least 20 seconds. Smaller values will be automatically re-set to this minimum interval.

DFS

As of HiLCOS version 8.80 all devices transmitting on the 5GHz WLAN frequencies support the standard ETSI EN 301 893 V1. 6. 1 ("DFS4").

For the DFS method (Dynamic Frequency Selection) required for 5 GHz WLANs, an unused frequency is automatically selected, for example, to avoid interference from radar systems. Occasionally, however, signals from weather radar stations cannot be identified reliably.

For this reason the European Commission is extending the requirements of the standards ETSI EN 301 893 V1.3.1 and ETSI EN 301 893 V1.4.1 to additionally avoid the use of three channels (120, 124 and 128) in subband 2 of the 5 GHz band. The use of these bands for automatic channel selection is prohibited until a process to auto-detect weather radar station signals becomes available. The versions EN 301 893 V1.3 and EN 301 893 V1.4 are referred to as "DFS2"

In the middle of 2010 the new version ETSI EN 301 893 V1.5.1 came into force, which was accompanied by changes in the usage of WLAN frequencies in the ranges 5.25 to 5.35 GHz and 5.47 to 5.725 GHz. The new Version 1.5.1 regulates the DFS (Dynamic Frequency Selection) method for the protection of radar stations from WLAN systems working in this frequency range. By using DFS to detect certain patterns in the radio signals received, it is now possible to detect active radar stations, and WLAN systems can automatically switch their operating channel. To differentiate from previous regulations, the new standard EN 301 893-V1.5 for the updated DFS is referred to as "DFS3".

A pulse pattern can generally be described in terms of its pulse rate, pulse width and the number of pulses. Former DFS technology was only able to detect fixed radar patterns as defined by the various combinations of pulse rates and pulse widths which were stored in the WLAN device. According to DFS3, the device is now able to recognize changing pulse rates and pulse widths as radar patterns. Furthermore, two or three different pulse rates may be used within a radar signal.

The version ETSI EN 301 893 V1.5.1 (DFS-3) expires on 01/01/2013. The new version ETSI EN 301 893 v1.6.1 (known as "DFS4"), which also detects shorter radar pulses, applies thereafter.

Note: The recognition of weather radar stations (channels 120, 124 and 128 in the 5.6 to 5.65 MHz frequency range) is subject to special conditions. The DFS implementation in HiLCOS does not support the more stringent recognition conditions. Therefore, these three channels will be omitted from newer versions of HiLCOS.

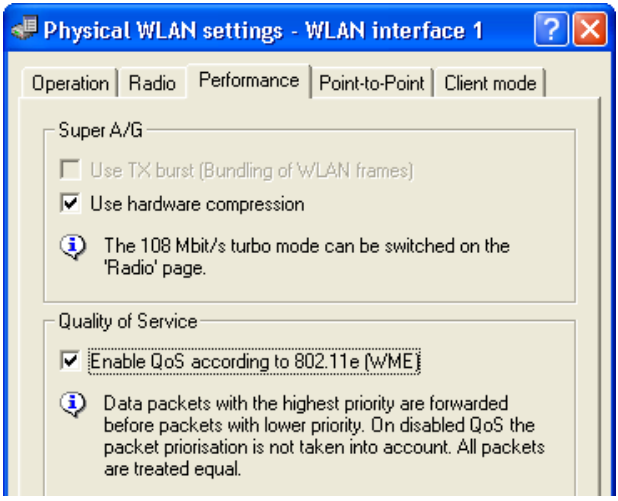
4.5.3 Performance

Use the settings in the ‘Performance’ dialog to increase data transmission rates. To open this dialog in the LANconfig software:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ In the Interfaces section, click ’Physical WLAN settings...’ and select an interface.

☐ Click on the `Performance` tab to display and configure radio module settings.



Use this dialog to configure the following parameters:

▶ Use TX burst (Bundling for WLAN frames):
Select this to enable packet bursting, thereby increasing data throughput for a single source device. Packet bursting involves the packaging of multiple Ethernet packets into a single WLAN frame to the fullest extent possible. However, bursting effectively prioritizes packets from a single source device, thereby delaying the handling of transmissions from other devices on the network.

Note: The ’use Tx bursting’ parameter, above, is disabled if the ’Enable QoS according to 802.11e (WME)’ parameter, below, is enabled.

- Use hardware compression:
  Turns ON (the default) or OFF hardware packet compression.
- Enable QoS according to 802.11e (WME):
  Select this option to enable QoS. If enabled, the OpenBAT device prioritizes packets in one of two possible procedures, depending on the contents of the packet:
  – If a packet contains a VLAN tag with a non-zero priority, this tag is used to establish packet priority in the WLAN.
  – Otherwise, the first three bits of the TOS/DiffServ field of the IP header are mapped according to IEEE 802.11e (table 20.23) to the four priority levels (voice, video, best effort and background) of the WLAN.

  As a precondition for setting priorities, both the WLAN Client and Access Point need to support 802.11e or WiFi Multimedia (WMM, formerly known as WME); in addition, the applications need to mark the data packets with the corresponding priorities.

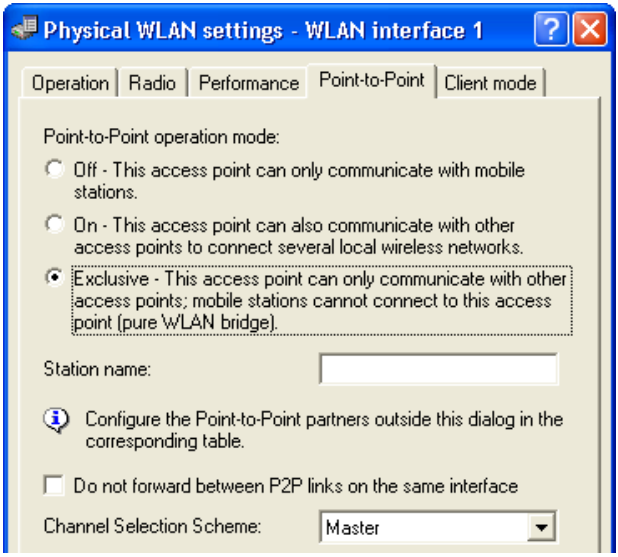
4.5.4 Point-to-Point

Access points can communicate with mobile clients, and also can transfer data from one access point to another. To open the ‘Point-to-Point’ dialog in the LANconfig software:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ In the Interfaces section, click ’Physical WLAN settings...’ and select an interface.

☐ Click on the ‘Point-to-Point’ tab to display and configure point-to-point communication settings.



Use this dialog to configure the OpenBAT device - in its role as Access Point - for point-to-point communication with other Access Points:

☐ Point-to-Point operation mode:
Select a mode:
- Off: The OpenBAT device can communicate exclusively with wireless clients.
- On: The OpenBAT device can communicate with both other Access Points and wireless clients.
- Exclusive: The OpenBAT device can communicate exclusively with other Access Points.

☐ Station name:
Enter a name for this interface that is unique within the WLAN. This name can be used by other wireless devices to make a point-to-point connection to this device.

Note: You can leave this field empty if this device has just one WLAN interface and already has a device name which is unique in the WLAN, or if the other base stations identify this interface by means of the WLAN adapter's MAC address.

☐ Do not forward between P2P links on the same device:
A single radio interface can have multiple point-to-point connections. Select this to disallow the transmission of packets between different connections on the same radio interface.

☐ Channel selection scheme:
Select a role for this device:
– Master: This access point takes over the leadership when selecting a free WLAN channel.
– Slave: All other access points will search for a channel until they have found a transmitting Master.

Configure one central access point as 'Master' and all other point-to-point partners as 'Slave'. This simplifies the process of establishing a point-to-point connection if ’Automatic selection’ of the ‘Channel number’ is configured.

Note: The settings made in this dialog are merely general point-to-point parameter settings. Point-to-point connections to remote WLAN stations are configured in LANconfig at the following location:
`Configuration : Wireless LAN : General : Point-to-Point Partners`

4.5.5 Client Mode

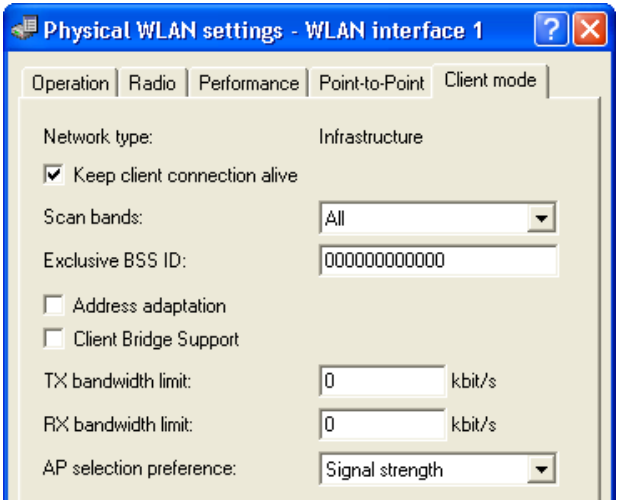
You can configure any OpenBAT device to perform the role of WLAN Client. Some devices are manufactured to operate exclusively as clients.

If the operating mode for this OpenBAT device is set to 'Access Point' in the 'Operation' dialog (see on page 243), any settings entered in the 'Client mode' dialog are ignored. To access this dialog:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ In the Interfaces section, click ’Physical WLAN settings...’ and select an interface.

☐ Click on the `Client mode` tab to display and configure client mode settings.



Use this dialog to display and configure the following parameters:

- Network type:
  (read-only) Set to 'Infrastructure'. By default, each OpenBAT device is designed to be employed as part of a network infrastructure involving the use of wireless Access Points.
- Keep client connection alive:
  Select this to configure the client device to periodically send dummy packets to the access point, thereby keeping open a connection between this client and the access point during time periods when no data packets are being transferred.
- Scan bands:
  Select the frequency bands this client device will scan attempting to establish a connection with an access station:
  – All (every available frequency band)
  – 2.4 GHz only
  – 5.0 GHz entry
- Exclusive BSS ID:
  Select one of the following:
  – The MAC address of the WLAN card in a specific access point: the client device can log in exclusively to this access point.
  – A string of one or more zeroes (the default): The client can log in to any access point on the wireless network.

- Address adaptation:
  if you select this, the client device will not substitute its own MAC address for the MAC address of the source device (e.g. a computer connected to the client via wired LAN) when forwarding the packet over the WLAN to an access point. The packet so transferred is said to be ‘transparent’, in that it contains the MAC address of the source device (and, in address adaptation, not the client device). This setting can be useful when:
  – the client device connects to a non-Hirschmann access point. In this case, the preferred configuration—client bridge support mode (see below)—is not available.
  – The client device's L2 masquerading behind the MAC address of its WLAN interface is not effective. This might occur, for example, if WLAN protocols are used that are not supported by masquerading (i.e. neither IP nor PPPoE).

  Note: Address adaptation works when just one remote computer is connected to the client station.

- Client Bridge Support:
  Select this to provide transparency to packets transmitted to a client device from multiple source devices (e.g. computers connected to the client via a wired LAN), then forwarded by the client over the WLAN to an access point. The transparency of a packet transferred in client bridge support mode includes not just the MAC address of the source computer, but also the MAC address of the client device. Client bridge support mode offers the following advantages, compared to a point-to-point design:
  - Client-bridge mode permits the creation of more than six connections (i.e., the point-to-point limitation).
  - Client bridge mode permits the client station to roam, which is not possible with a point-to-point design.

  Note: Client bridge support needs to be enabled in each device (access point and client station) before it can be used.

- Tx / Rx bandwidth limits:
  Enter both a transmit and receive bandwidth limit, in kbit/s, for the WLAN client. The client transmits this value while connecting to the access point. The access point will calculate a bandwidth minimum based on this value and its own potential bandwidth limits. A value of zero indicates no limits.

- AP (access point) selection preference:

  Indicates the basis the client device should use for connecting to an access point, when the client device detects the presence of more than 1 access point on the WLAN:

  Signal strength:
  The priority of the access point will be defined in following order:
  - The access point with the greatest signal strength will be selected.
  - If 2 or more access points have the same signal strength, then the access point with the lowest channel utilization will be selected.
  - If the above parameters match for 2 or more access points, then the access point with the lowest index will be selected.

  Profile:
  The priority of the access point will be defined in following order:
  - The access point with the lowest index will be selected.
  - If matched profile defined at same index, then the access point with the lowest channel utilization will be selected.
  - If the above parameters match for 2 or more access points, then the access point with the highest signal strength will be selected.

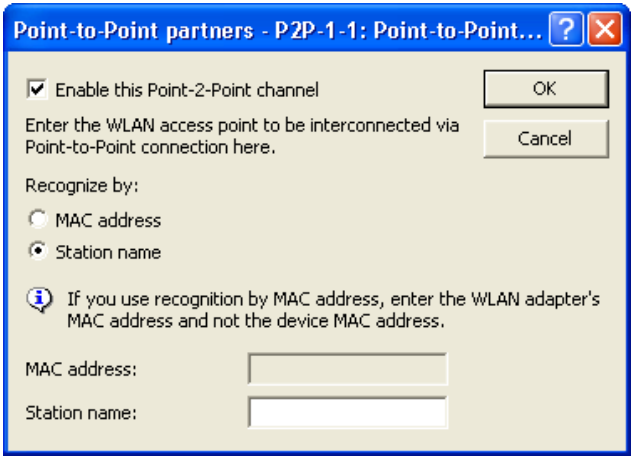
  Channel Utilization:
  The priority of the access point will be defined based on the parameters "Modem Channel Utilization" and "Number of stations connected to the AP". Users have the option to choose if the number of stations connected to the access point should be used for access point selection. This option can be enabled/disabled using the CLI command “/setup/wlan/ Selection-Preference-AP-Station”. Based on Channel Utilization information, the access point will be selected in the following order:
  - If the Selection-Preference-AP-Station parameter is enabled, the access point with the least stations connected to it will be selected.
  - If station count of 2 or more access points is the same. Selects the profile for the WLAN offering lowest access point Channel Utilization
  - If 2 or more access points have the same Channel Utilization and station count, then the access point offering the strongest signal will be selected.

4.6 Point-to-Point Partners

You can configure up to 16 point-to-point partners for each WLAN radio interface. To open the ‘Point-to-Point partners’ configuration dialog:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ In the Interfaces section, click ’Point-to-Point partners...’ and select a combination of interface and channel (e.g. P2P-1-1 indicates point-to-point interface 1, channel 1).



Use the ‘Point-to-Point partners’ dialog to configure the following properties for the selected interface and channel:

- Enable this Point-2-Point channel:
  Select this to enable this channel for point-to-point communication.
- Recognize by:
  Indicate how this OpenBAT device will identify its remote device point-to-point partner. The options are:
  – MAC address: If you select this option, you must also enter the MAC address of the wireless LAN adapter for the point-to-point partner.
  – Station Name: If you select this option, you must also enter a name for the point-to-point partner. This name can be the configured device name or the separately configured 'Station name' for a physical WLAN interface of the remote partner, (see on page 253) which is input in the 'Point-to-Point' dialog.

  Note: The automatic channel selection for P2P connections in the 5 GHz range is only active if the selected country profile supports DFS.

4.6.1 Automatic Configuration of WLAN P2P Connections via Serial Interfaces

When P2P connections are configured in the WLAN area, the remote terminals usually recognize each other based on a specific characteristic of the respective P2P partner: either the station name or the MAC address of the P2P partner is entered in the configuration of the Access Points.
With changing P2P partners, you cannot permanently set this characteristic in the configuration. For example, if you want to establish a P2P connection between two train cars to offer IP services in the entire train, the respective P2P remote terminals change with every modification in the sequence of train cars.

In these cases, the Access Points can communicate the respective MAC addresses via the serial interface. For this purpose, you connect the devices via two wires of the serial interface (see Installation Guide). Then you set the identification of the P2P remote site to the value ‘serial autoconfig.’ Configure the P2P connections as with a fixed installation of Access Points.In default state, the WLAN modules are deactivated. When you switch on the devices, they communicate the MAC addresses, and only then do they activate the WLAN modules and automatically set up the P2P connection.

4.7 Logical WLAN Networks

Each physical WLAN radio interface can support up to eight different logical wireless networks, each with its own service set identifier (SSID), or network name. You can separately configure parameters for each of these logical networks, without the need of additional access points. Use the ‘Logical WLAN settings’ dialog to configure parameters for each logical network and its data transmission rates.

Note: When you create multiple logical networks for a single physical network, the physical network’s available bandwidth is shared by the number of logical networks you create.

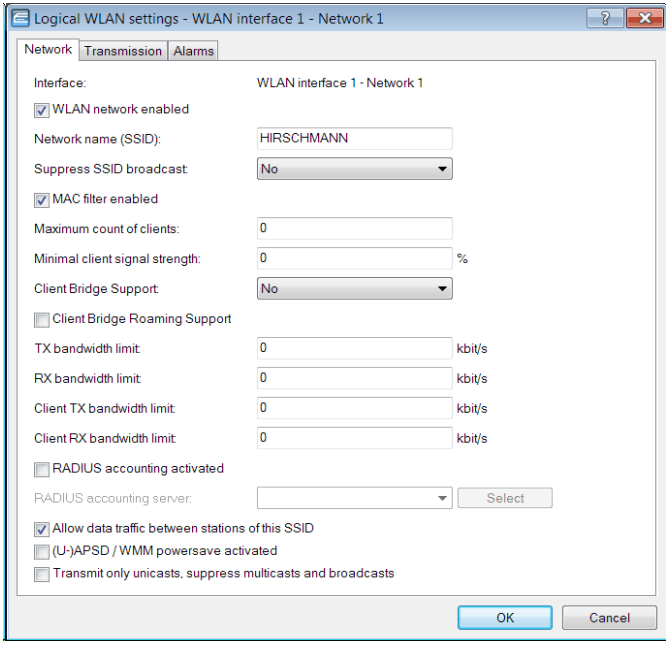
4.7.1 Network Settings

To open the ‘Network’ dialog:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ In the Interfaces section, click ’Logical WLAN settings...’ and select a combination of radio interface and logical network, for example: WLAN interface 1 - Network 1.

☐ Click on the `Network` tab.



You can display and configure the following parameters in this dialog:

- "WLAN network enabled"

  This switch enables or disenables the corresponding logical WLAN.

- "Network name" (SSID)

  Specify a unique SSID (the network name) for each of the required logical wireless LANs. Only network cards that have the same SSID can register with this wireless network.

- "Suppress SSID broadcast"

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option "Suppress SSID broadcast" provides the following settings:

- **No:** The access point publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).
- **Yes:** The access point does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID.
- **Tightened:** The access point does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device does not respond.

Note: Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

- "MAC filter enabled"

The MAC addresses of the clients that are allowed to associate with an access point are stored in the MAC filter list (`Wireless LAN:Stations:Stations`). The "MAC filter enabled" switch allows you to switch off the use of the MAC filter list for individual logical networks.

Note: Use of the MAC filter list is required for logical networks in which the clients register via LEPS with an individual passphrase. The passphrase used by LEPS is also entered into the MAC filter list. The access point always consults the MAC filter list for registrations with an individual passphrase, even if this option is deactivated here.

- "Maximum number of clients"

  Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected by the access point.

- "Minimum client signal strength"

  This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

  A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, as those offering only a weak connection at the client's current position are not listed.

- "Client-bridge support"

  Enable this option for an access point if you have enabled the client-bridge support for a client station in WLAN client mode ().

  Note: The client-bridge mode operates between two HiLCOS devices only.

- "Client Bridge Roaming Support"

  The Client Bridge Roaming Support improves the reliability and latency of the roaming process. It is useful in situations with many devices attached to the LAN of the Client and even more so, if most of the data traffic flows downstream; meaning, the traffic flows from the APs, through the Client to the attached devices. Enabling this feature on APs directly allows the APs to exchange information about the devices attached to a roaming Client. Enabling this feature on the Client allows freeing up the wireless link after roaming, which decreases roaming times. If this feature is enabled on the Client it will check on each roaming event if this improvement is possible or otherwise fall back on the default behavior.

- "TX bandwidth limit"

  With this setting, you define the overall bandwidth that is available for transmission within this SSID. A value of `0` disables the limit.

- "RX bandwidth limit"

  With this setting, you define the overall bandwidth that is available for reception within this SSID. A value of `0` disables the limit.

- "RADIUS accounting activated"

  Enable this option to switch on RADIUS accounting for this SSID.

- "RADIUS accounting server"

  Enter an alternative RADIUS accounting server for the respective logical WLAN network. If you leave this field empty, the device uses the globally configured accounting server under `Wireless LAN : Stations : RADIUS accounting servers`.

- "Allow traffic between stations of this SSID"

  Check this option if all stations logged on to this SSID are to be able to communicate with one another.

- "(U)APSD / WMM Power Save activated"

  Enable this option to signal stations that the power saving function (U)APSD ([Unscheduled] Automatic Power Save Delivery) is supported.

  (U)APSD is established in the 802.11e standard, and helps VoWLAN devices to increase their battery life. The related devices switch to power saving mode after login on a (U)APSD-capable access point. If the access point receives data packets for the related devices thereafter, it temporarily stores the data and waits until the VoWLAN device is available again. It then forwards the data. Afterwards, (U)APSD increases the latency time of the radio module, whereby it ultimately consumes less power. The individual rest periods may be so short that a VoWLAN device can still use the power saving function in the call state itself. However, the relevant devices must also support (U)APSD.

WWM (Wi-Fi Multimedia) Power Save is a power saving function of the Wi-Fi Alliance and is based on U-APSD. Certain Hirschmann access points are WMM® Power Save CERTIFIED by the Wi-Fi Alliance.

- "Only transmit unicasts, suppress broadcast and multicasts"

  Multicast and broadcast transmissions within a WLAN cell cause a load on the bandwidth of the cell, especially since the WLAN clients often do not know how to handle these transmissions. The access point already intercepts a large part of the multicast and broadcast transmissions in the cell with ARP spoofing. With the restriction to unicast transmissions it filters out unnecessary IPv4 broadcasts from the requests, such as Bonjour or NetBIOS.

  The suppression of multicast and broadcast transmissions is also a requirement from the HotSpot 2.0 specification.

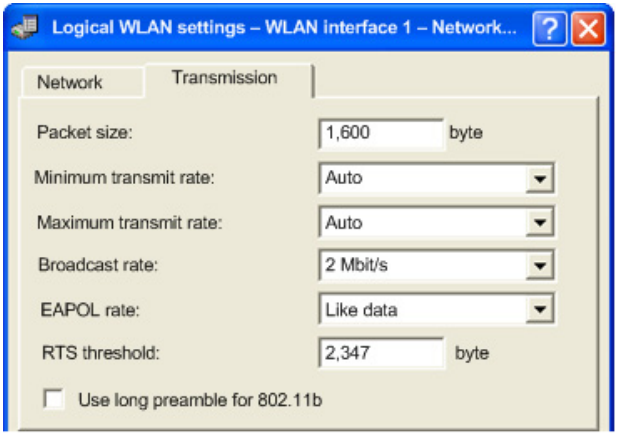
4.7.2 Transmission Settings

Details for the data transfer over the logical interface are set on the ‘Transmission’ dialog. To open this dialog:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ In the Interfaces section, click ’Logical WLAN settings...’ and select a combination of radio interface and logical network, for example: WLAN interface 1 - Network 1.

☐ Click on the `Transmission` tab.



Use this dialog to configure the following properties:

- Packet size:
  The maximum size of a WLAN packet that can be transmitted over this network:
  – Increase the default setting if your wireless network is largely free from interference.
  – Reduce the value to reduce the incidence of unintended transmission events.

  Smaller data packets cause fewer transmission events than larger packets, although the proportion of header information in the traffic increases, leading to a drop in the effective network load.
- Minimum / Maximum transmit rates:
  Accept the default setting (’Auto’) to let the access point negotiate the data transmission speeds with the connected WLAN clients continuously and dynamically. The access point adjusts these transmission speeds to the reception conditions. Alternatively, you can set fixed values for the minimum and maximum transmission speeds, thereby disabling dynamic speed adjustment.
- Broadcast rate:
  Select a broadcast rate, so that, even under unfavorable circumstances, the slowest clients can connect to the network.
- EAPOL Rate:
  Select an ‘Extensible Authentication Protocol Over LAN’ (EAPOL) rate.

Note: EAPOL can be used by WLAN clients for registration to access points via WPA and/or 802.1x. In this case, EAP packets are encapsulated in Ethernet frames for exchanging authentication information, to allow EAP communication via layer-2 connection.
The default selection 'Like Data' treats EAPOL packets as normal data packets and uses the common transmission rate for data packets.

In some cases it may be reasonable to use a lower data rate for transferring EAPOL packets than the data rate for user data. For some mobile WLAN clients, a higher data rate can lead to EAPOL packet loss, which can delay the authentication process. By specifying an EAPOL data rate, he authentication process can be stabilized.

- RTS threshold:
  Input the minimum WLAN packet size that triggers the activation of the Request to Send (RTS)/Clear to Send (CTS) 802.11 function. The RTS/ CTS function helps deter the occurrence of the ‘hidden station’ phenomenon.

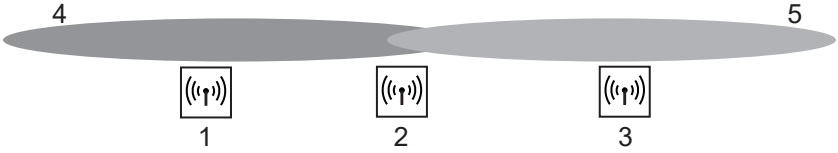
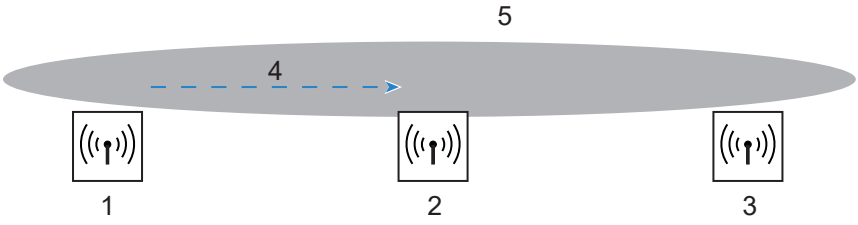


Figure 9: 1 - access point 1 (AP-1)
2 - access point 2 (AP-2)
3 - access point 3 (AP-3)
4 - network coverage area of access point 1
5 - network coverage of access point 3

In the example, above, three access points (1, 2, and 3) are positioned so that no direct wireless connection between AP-1 and AP-3 is possible. If AP-1 sends a packet to AP-2, AP-3 cannot detect this transmission, because it is outside of the AP-1 coverage area. AP-3 may attempt, during the transmission from AP-1 to AP-2, to send a packet to AP-2, because it is unaware that the wireless connection is in use. A collision results and neither transmission (from AP-1 to AP-2, or from AP-3 to AP-2) succeeds. The RTS/ CTS protocol is used to reduce the likelihood of such an event.



With RTS/CTS activated, AP-1 precedes its data transmission by sending an RTS packet to AP-2. AP-2 responds by transmitting a CTS packet.

Because AP-3 is within AP-2's coverage, it detects the CTS packet and waits to send its data transmission to AP-2.

RTS/CTS makes sense in the exclusive circumstance when long data packets are being used, thereby increasing the likelihood of collision. The optimal 'RTS threshold' value will be determined as a result of on-site testing.

Note: RTS/CTS also needs to be supported by, and enabled in, all client devices.

- Use long preamble for 802.11b:
  Select this to establish a longer, fixed preamble for clients communicating with his access point.

  Note: Clients in 802.11b mode usually negotiate the length of the preamble with the access point.

4.7.3 STBC / LDPC

Basics

Data transfers according to the IEEE-802.11n standard are performed using MIMO technology (multiple input, multiple output). The sender transmits data packets concurrently over multiple, spatially separated antennas, meaning that reflections and the resulting interference have little effect on the signal. However, the gain in throughput is less with each additional antenna, and the performance requirements for signal processing are increased.

Low Density Parity Check (LDPC)

Before the sender transmits the data packets, it expands the data stream with checksum bits depending on the modulation rate. These checksum bits allow the receiver to correct transmission errors. By default the 802.11n standard uses 'Convolution Coding' (CC) for error correction, which is well-known from the 802.11a and 802.11g standards; however, the 11n standard also provides for error correction according to the LDPC method (Low Density Parity Check).

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data transfer rate.

Space Time Block Coding (STBC)

The function 'STBC' (Space Time Block coding) additionally varies the transmission of data packets over time to minimize time-related effects on the data. Due to the time offset of the packets the recipient has an even better chance of receiving error-free data packets, regardless of the number of antennas.

4.8 Beaconing and Roaming

The default beaconing and roaming settings will usually be appropriate for your wireless LAN. An expert level of skill and understanding of wireless networks is a pre-requisite for changing the default settings.

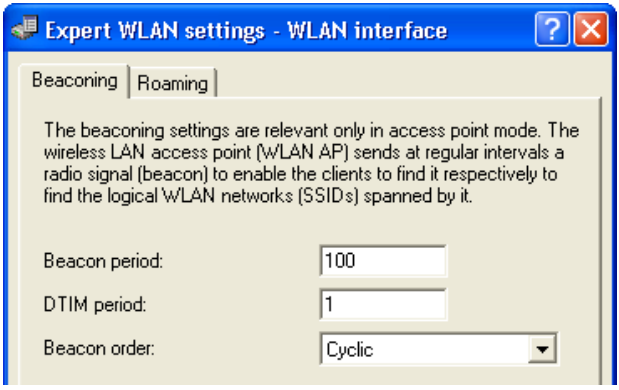
4.8.1 Beaconing

To access the Beaconing dialog:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ Click 'Expert WLAN settings...' and select a WLAN radio interface to open the 'Expert WLAN settings' dialog.

☐ Click on the 'Beaconing' tab to display that dialog.



Configure the beaconing settings to influence the transmission of beacons by the OpenBAT device in its role as Access Point. These settings can influence the roaming behavior of clients, and optimize Multi-SSID operations for older WLAN Clients.

- Beacon period:
  Enter a value, in K?s, to act as the time interval between beacon transmissions. Smaller values result in a shorter beacon time-out period for the client and enable quicker roaming, but also increase the WLAN overhead. The default is 100 K?s.

  Note: 1 K?s corresponds to 1024 microseconds and is the unit of measure for the 802.11 standard. 1 K?s is also known as a Timer Unit (TU).

- DTIM period:
  Input a delivery traffic indication message (DTIM) value to indicate the number of beacon signals that need to be received before sending a broadcast. The default setting is '1', causing broadcasts to be sent without delay. Higher values enable longer client sleep intervals, but increase system latency.

- Beacon order:
  Select the order in which beacons are sent to the multiple WLAN networks (for the following descriptions, assume three wireless networks exist, and the 'Beacon period' is set to 100 K?s):
  - Cyclic (the default): The access point transmits the first beacon transmission at 0 K?s to WLAN-1, followed by WLAN-2 and WLAN-3. For the second beacon transmission (at 100 K?s), WLAN-2 is the first recipient, followed by WLAN-3 and then WLAN-1. For the third beacon transmission (at 200 K?s), the order is WLAN-3, WLAN-1, WLAN-2. At the next transmission period, the process repeats.
  - Staggered: The beacons are not sent together at a particular time, but instead are transmitted separately across the available beacon periods. Beginning at 0 K?s, just WLAN-1 is sent; after 33.3 K?s WLAN- 2, after 66.6 K?s WLAN-3. At the start of a new beacon period, transmission starts again with WLAN-1.
  - Simple burst: The access point transmits the beacons for the wireless networks in the same order. The first beacon transmission (0 K?s) is for WLAN-1, WLAN-2 and WLAN-3; the second transmission is in the same order, and so on.

Note: Some older WLANs cannot process the quick succession of beacons that occurs with simple burst. These clients often recognize just the first beacons and can associate exclusively with this network. Staggered transmission of beacons produces better results, but increases load on the access point's processor. Cyclic transmission is often a good compromise, because all networks are transmitted first in sequence.

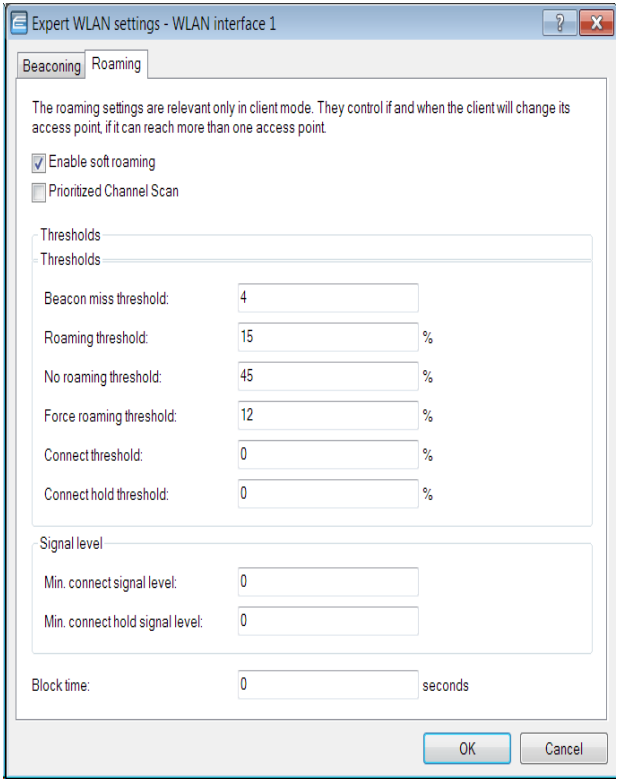
4.8.2 Roaming

The 'Roaming' dialog contains the threshold values that affect the behavior of the OpenBAT device when roaming, while operating in the role of a client station. To access this dialog:

☐ Open the `Configuration : Wireless LAN : General` dialog.

☐ Click 'Expert WLAN settings...' and select a WLAN radio interface to open the 'Expert WLAN settings' dialog.

☐ Click on the 'Roaming' tab to display that dialog.



You can use this dialog to configure the following parameters:

- Enable soft roaming:
  Select this to help provide a seamless transition for a wireless client when it roams between access points.

  Note: If soft roaming is disabled, the client's search for a second access point begins after it can no longer communicate with the current access point, causing interrupted data transmission.

- Prioritized Channel Scan:
  The prioritized channel scan function optimizes roaming by including previous roaming decisions. This is suitable for scenarios with recurring movements of the clients within the WLAN. The prioritized channel scan function selects channels where potential roaming candidates are most likely to be found. This results in accelerated roaming, reduced handover times, and less packet loss.

- Beacon miss threshold:
  Input the number of access point beacon signals the client can miss before it begins to search for another access point.
  – A higher number increases the likelihood that the loss of the connection will go unnoticed, leading to a delay in re-connection.
  – A lower number increases the likelihood that the client will detect a lost connection more often than is necessary.

  The default setting is 4.

- Roaming threshold:
  Input a value representing the percentage difference in signal strength between access points, above which the client will switch to the stronger access point. The percentage difference entered here relates to dB values as follows:
  100% - 64dB
  50% - 32dB
  0% - 0dB
  The default is 15%.

- No roaming threshold:
  Enter a value representing the field strength in percent. Field strengths exceeding the value set here are so strong that no switching to another access point will occur.
  The default is 45%.

- Forced roaming threshold:
  Enter a value representing the field strength in percent. Field strengths below the value set here are so weak that switching to another access point is required. The default is 12%.

- Connect threshold:
  Enter a value representing the minimum field strength in percent that an access point needs to emit for a client to attempt to associate with it. The default is 0%.

- Connect hold threshold:
  Enter a value representing the field strength in percent below which a connection to an access point is deemed to be lost. The default is 0%.
- Min. connect signal level:
  Enter the minimum signal level, in dB, required to establish a connection between the client and an access point. The default is -5dB.
- Min. connect hold signal level:
  Enter the minimum signal level, in dB, required to hold a connection between the client and an access point. The default is 0dB.
- Block time:
  Enter a time period, from 0 to 2147483647 seconds, defining the period of time during which a WLAN Client may not connect to an Access Point after an attempted connection to the Access Point was rejected (Association Reject). The default value is 0 seconds. A connection request sent by the Client will not be rejected.

4.9 Device Authentication

You can configure a OpenBAT device in its role as Access Point to perform authentication of a client device both before the client is granted access to the wireless network and periodically thereafter during the course of an ongoing connection.

4.9.1 Authentication via RADIUS

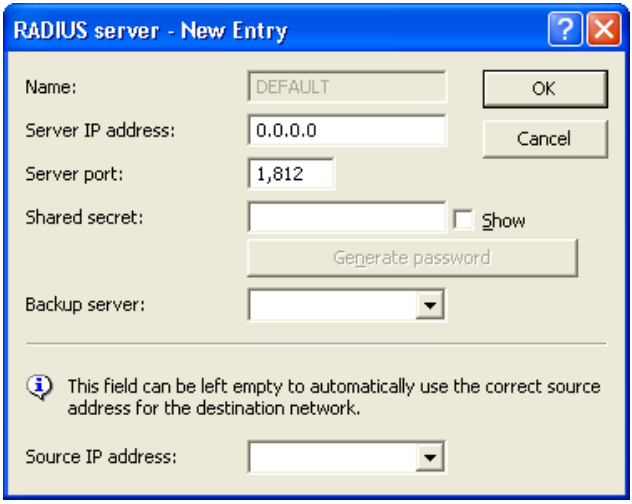
WLAN Clients can use the 802.1x protocol for centralized network registration. The OpenBAT device, in its role as Access Point, can use this protocol to forward the registrations to a remote RADIUS server. The client is identified by its MAC address. This configuration is performed in the 'RADIUS server - New Entry' dialog, which is accessed in the LANconfig software as follows:

☐ Open the `Configuration : Wireless LAN : IEE 802.1x` window.

☐ Click ’RADIUS server...’ to open the ‘Radius server’ list.

☐ In the ‘RADIUS server’ list, click either:
- ’Default server’ to edit the RADIUS server used for all WLAN networks that use an authentication process in line with IEEE 802.1x and that have not specified their own RADIUS server, or
- ’Add...’ to enter settings for an existing RADIUS server.

The ’RADIUS server - New Entry’ window opens for editing:



Display and configure the following parameter in this dialog:

- Name:
  For the default RADIUS server, the read-only value is 'DEFAULT'. For other RADIUS servers, enter a unique name. If you enter the same value also used as the 'Key 1/passphrase' in the 'WPA or Private WEP settings' dialog (see on page 231), each WLAN network using authentication in line with IEEE 802.1x can be assigned its own RADIUS server.
- Server IP address:
  Enter the IP address of your RADIUS server, from which clients are managed centrally.
- Server port:
  Enter the port used for communication to your RADIUS server.
- Shared secret:
  Enter the key to be used for coding data. Also configure the key on the RADIUS server.

- Backup server:
  Select the name of the backup server from the list of RADIUS servers configured so far. The specified RADIUS server has to be unavailable before the backup server will be connected.
- Source IP address:
  Do one of the following:
  – Leave this field blank, and theOpenBAT device will automatically apply the default source IP address for the RADIUS server
  – Select an alternative source address. For example, a loopback address can be used if it has been added to the list of TCP/IP networks.

  Note: The configured source IP address is used unmasked for any remote site.

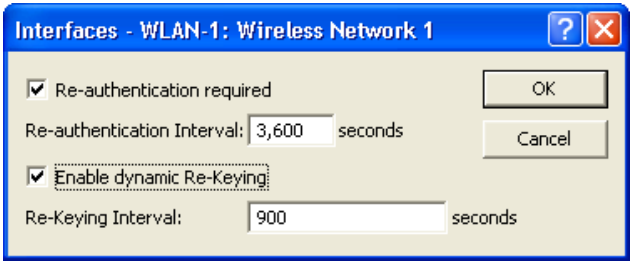
4.9.2 Re-Authentication via IEEE 802.1x and EAP

The international industry standard IEEE 802.1x and the Extensible Authentication Protocol (EAP) enable access points to carry out secure access checks. Access information can be managed centrally on a RADIUS server and can be retrieved by an access point on demand. This technology also enables the secure transmission and the regular automatic changing of WEP keys. In this way, IEEE 802.1x improves the security of WPA2.

Use the ‘Interfaces’ dialog to configure login settings for each wireless network. To access this dialog:

☐ Open the `Configuration : Wireless LAN : IEE 802.1x` dialog.

☐ In the Interface settings section, click ’Interfaces...’, then select a wireless network from the list.



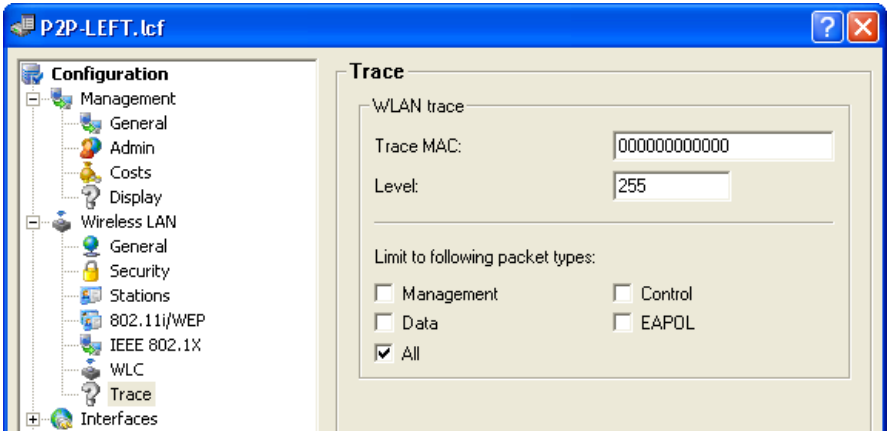
Use this dialog to configure the following settings:

- Re-authentication required:
  Select this to activate periodic re-authentication. When a new authentication starts, the client remains registered during the negotiation.
- Re-authentication interval:
  Enter the frequency, in seconds, for periodic re-authentication. The default is 3600 seconds.
- Enable dynamic Re-Keying:
  Select this to activate the regular generation and transmission of a dynamic WEP key.
- Re-Keying interval:
  Enter the interval, in seconds, for the regular re-generation of the WEP key. The default is 900 seconds.

4.10 Trace

Use the 'Trace' dialog to apply the LANconfig trace function to a specific Access Point, Client or specific WLAN packets. By default, the LANconfig software's trace function collects data of all packets and all OpenBAT devices in the network. Narrowing the trace output can be very helpful in troubleshooting a specific device or packet type. To access this dialog in the LANconfig software, select:

☐ `Configuration : Wireless LAN : Trace`



Note: WLC is not currently supported.

Use this dialog to configure the following settings:

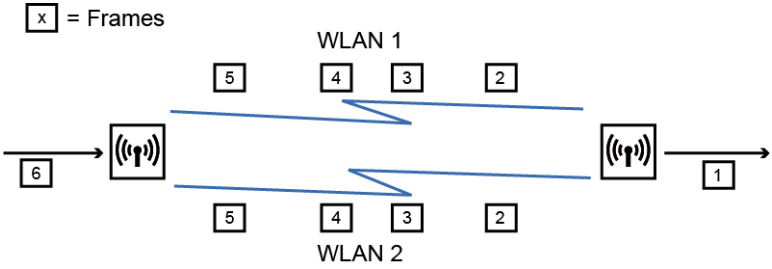
- Trace MAC:
  The MAC address of the device whose activity is to be traced.
- Level:
  Enter a value, from 0 to 255, that limits the trace output to particular content. Particular values include:
  – 0: just the message, if a packet was sent/received at all
  – 1: additionally the physical parameters of the packet (data rate, signal strength...)
  – 2: additionally the MAC header
  – 3: additionally the layer3 header (e.g. IP/IPX)
  – 4: additionally the layer4 header (TCP, UDP...)
  – 5: additionally the TCP/UDP payload
  – 255: (the default) all data without limitation
- Limit to following packet types:
  Select one or more types of packets to be included in the trace, for example:
  – Management: Authenticate, Association, Action, Probe-Request/ Response
  – Control: e.g. Powersave-Poll
  – EAPoL: 802.1x negotiation, WPA key handshake
  The default is 'All'.

4.11 Redundant connections using PRP

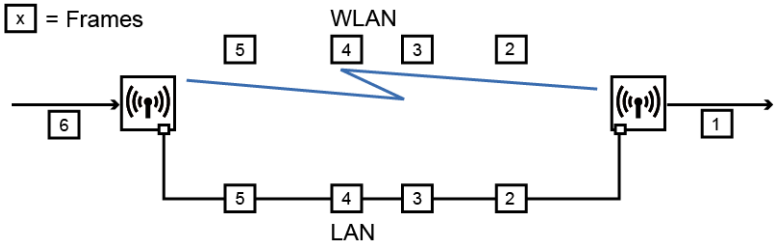
Applications that are sensitive to connection failures require uninterrupted communications. Examples are to be found in automation, transport and mobile applications.

With HiLCOS you have the option of operating redundant connections in your WLAN by means of the parallel redundancy protocol (PRP). Redundant point-to-point links offer you a high level of failover reliability.

PRP achieves high failover reliability by sending 2 identical packets over 2 independent WLANs. While 1 WLAN is active, PRP transports data packets.



You can choose to implement PRP with only WLAN interfaces. Alternatively, you can use one wired and one WLAN interface to implement PRP.



In applications with difficult conditions (moving parts, high temperatures), the wireless link acts as an automatic backup to a wired connection.

4.11.1 Basic function

PRP devices act as the sender and receiver of PRP packets, whereby PRP devices are capable of assuming both roles.

The sender operates as follows:

- It duplicates packets to produce twin pakets, and sends them over 2 independent (W)LANs.
- Each packet is given a redundancy control trailer (RCT).

The RCT provides the following information for the recipient:

- It identifies the packet as a PRP packet.
- It contains a sequence ID.
- It shows which (W)LAN the packet arrived from.
- It contains the packet size.

The sequence ID is a consecutive incremented number. The sequence ID together with the the source MAC address allow the receiver to detect duplicate packets. Duplicate detection causes the packet arriving later to be discarded.

The receiver operates as follows:

- It reads the RCT.
- It forwards the first of the duplicated packets without its RCT.
- Through duplicate detection, the receiver discards the packet that arrives later.

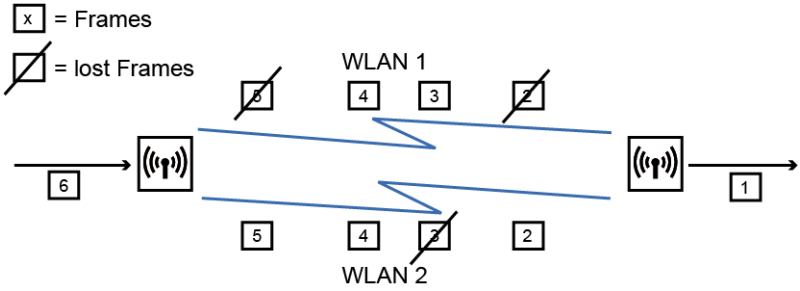
4.11.2 Advantages of WLAN PRP

The functions of PRP offer you significant advantages for your WLAN. In practice, PRP improves the 3 most important quality indicators for a network: Jitter, latency and packet loss.

With PRP, the receivers will accept and forward the first copy of the PRP packets and discard those that arrive later. Because the devices always forward the first incoming packet, latency is reduced. In practice, significant improvements were seen to average and maximum jitter.

Like Ethernet, WLAN is designed to be a shared medium. Within a single WLAN connection, the devices hold back packets if the medium is busy. Because the devices with PRP transport the data via 2 different WLANs, in effect 2 media are available thanks to frequency division.

Because the devices send each packet twice, PRP can to some extent compensate for unsystematic packet loss. As long as the receiver receives one of the packets, then communication was successful. Under certain circumstances there is no need to retransmit lost packets, which also positively affects jitter.



4.11.3 Implementation of PRP in the access points

Any access point (AP) with at least 3 interfaces can be used to setup a PRP network. The AP handles all of the functions necessary for establishing a PRP network.

The devices offer the following options:

- PRP networks can be implemented on any interface; wireless, wired, or mixed
- Each device can implement up to 2 PRP networks
- In addition to a PRP network, connect additional clients to an AP
- Activate smart roaming so that the 2 WLAN modules can roam asynchronously with PRP.
- Comprehensive diagnostic options

4.11.4 Implementing PRP exclusively over WLAN

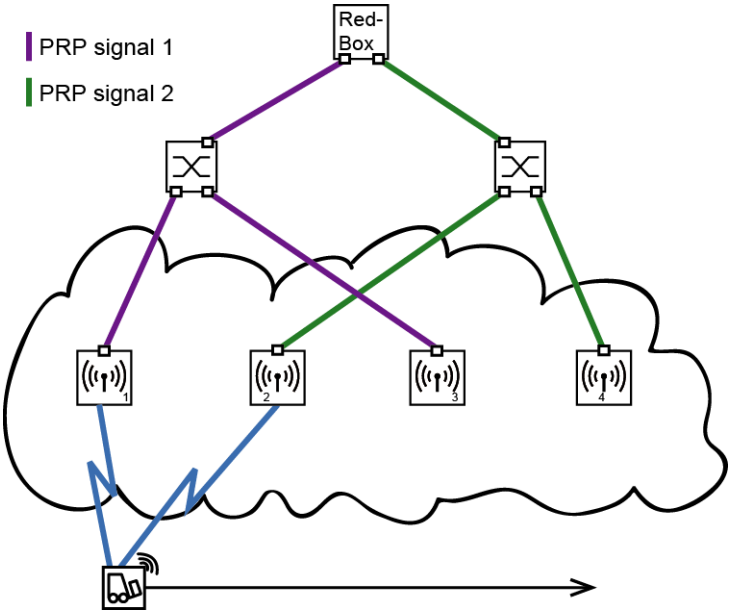
You can optionally setup a PRP network that operates over WLAN only. This is useful if the costs of cabling are high. A WLAN solution is suitable when the application type or environmental conditions demand this.

4.11.5 Smart roaming

A device with just 1 WLAN module will lose its connection to the infrastructure in a handover scenario.

However, a device with 2 WLAN modules can use PRP to reduce interruptions if the corresponding LANconfig setting prevents both WLAN modules from roaming at the same time. This mode is called smart roaming.

A practical example is a client moving past an access point. Due to the design of the network, one WLAN module stays connected and receives PRP packets, while the other WLAN module can already associate with the next AP.



A concrete example would be for materials management, and for the real-time monitoring of inventory flow in particular.

Another example is the railway. An AP in a train connects to the trackside APs throughout the journey.

In addition, you can specify the block time in LANconfig. The block time specifies the minimum time that passes before the different WLAN modules of the same device can perform roaming operations.

4.11.6 Diagnostic options

Recipients of PRP packets discard duplicates during normal operation and remove the RCT from packets that they pass on to their bundled output port.

HiLCOS provides you the following options to assist you in network diagnostics:

- Forwarding packet duplicates without RCT
- Forwarding single packets with RCT
- Forwarding packet duplicates with RCT

HiLCOS also features the following trace options:

- trace # PRP-DATA
- trace # PRP-NODES

PRP-DATA contains information about packets that are sent and received. Information included: Name of the interface group transporting the packet: Direction of transport of the packet (RX|TX): Trailer sequence number: MAC address of the partner device: Interface within the PRP group (A|B) transporting the packet: Treatment of the packet (accept|discard)

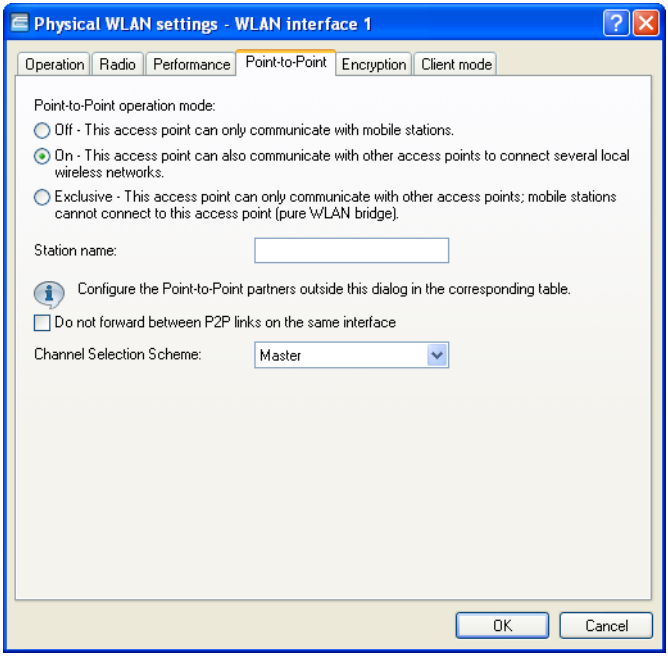
PRP-NODES currently has no function.

4.11.7 Tutorial: Setting up a PRP connection over a point-to-point network (P2P)

Note: The following steps must be conducted for both P2P partners.

Proceed as follows to set up a P2P connection between two PRP-enabled APs:

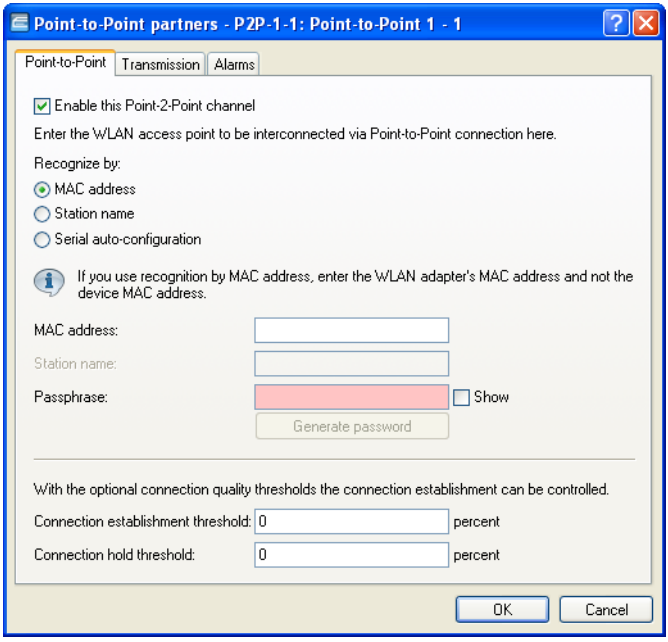
☐ Under `Wireless LAN : General : Physical WLAN settings`, go to the "Operation" tab for each physical WLAN interface (WLAN interface 1, WLAN interface 2) and, on the "Point-to-point" tab, enable the "Point-2-Point operation mode".



☐ In the field "Station name", give each of the physical WLAN interfaces a name that is unique on the WLAN. If the P2P partner can or should identify this interface using the MAC address, leave this field blank.

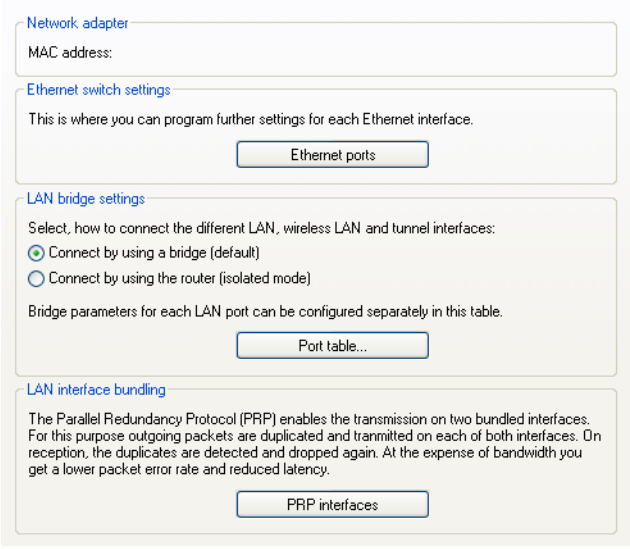
Important: In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

☐ Under `Wireless LAN : General : Point-to-point partners`, enable the point-to-point channels "P2P-1-1" and "P2P-2-1" and specify the interface identifier for each point-to-point partner ("MAC address" or "Station name").

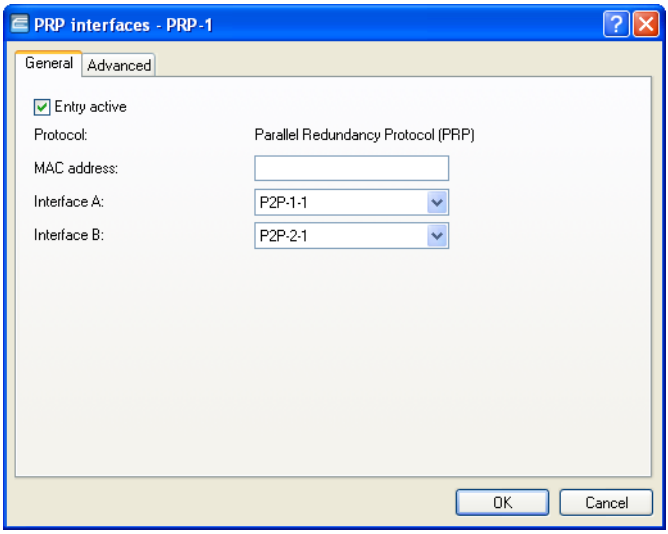


Specify either the MAC address or the station name of the corresponding WLAN interface of the P2P partner. You set these station names in the previous step.

☐ Open the PRP configuration under `Interfaces : LAN` with a click on "PRP interfaces".



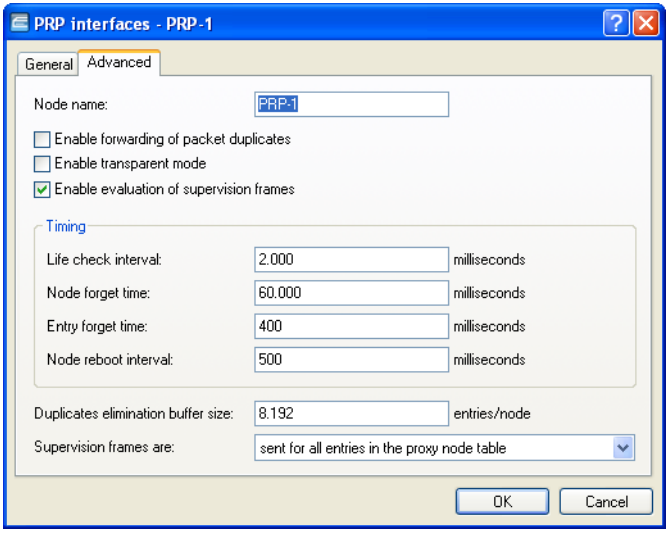
☐ Enable the PRP interfaces and set the interfaces that the AP uses for bundling.



Here you select the previously activated point-to-point interfaces "P2P-1-1" and "P2P-2-1".

Important: In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

☐ You can accept the advanced settings from the default configuration by clicking on "OK".



This completes the setup of a PRP connection over a point-to-point network.

4.11.8 Tutorial: Roaming with a dual-radio client and PRP

A common way to increase the resilience of a WLAN infrastructure is to operate the various APs in different frequency bands. One way to implement this is for the physical WLAN interfaces of the APs to operate SSID-1 on the 2.4-GHz band and SSID-2 on the 5-GHz band, for example. A PRP-capable dual-radio client moving from the radio cell of one physical WLAN interface to a neighboring cell of the same infrastructure can experience uninterrupted cell switching thanks to PRP.

To do this, the dual-radio client using PRP initially connects its physical WLAN interface WLAN-1 to SSID-1 and WLAN-2 to SSID-2. If the reception for SSID-1 deteriorates and another radio cell with better reception is within range, the dual-radio client will perform a cell change. During the cell change the dual-radio client continues to send the data via WLAN-2 on SSID-2, while WLAN-1 already starts sending the same data with better reception on SSID-1. A PRP-enabled switch filters out the duplicate PRP packets before forwarding the data to the LAN.

Note: In this scenario, the APs in the WLAN infrastructure do not have to be configured to operate PRP.

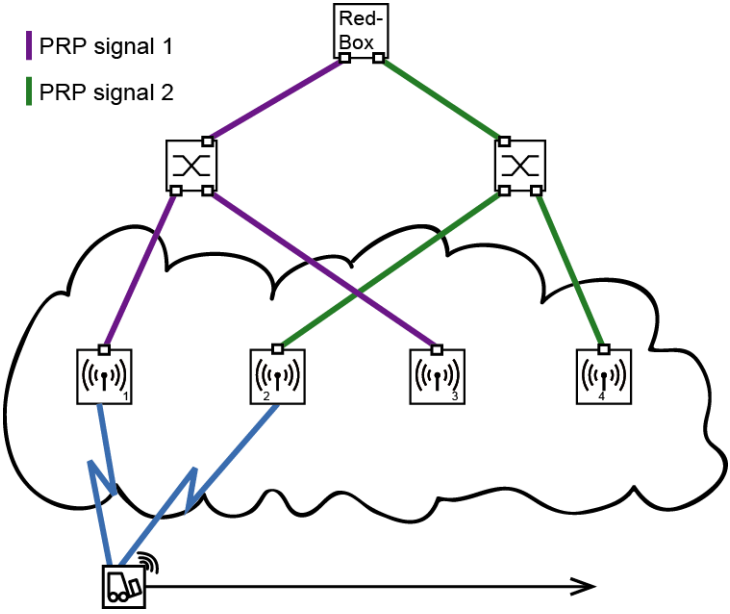
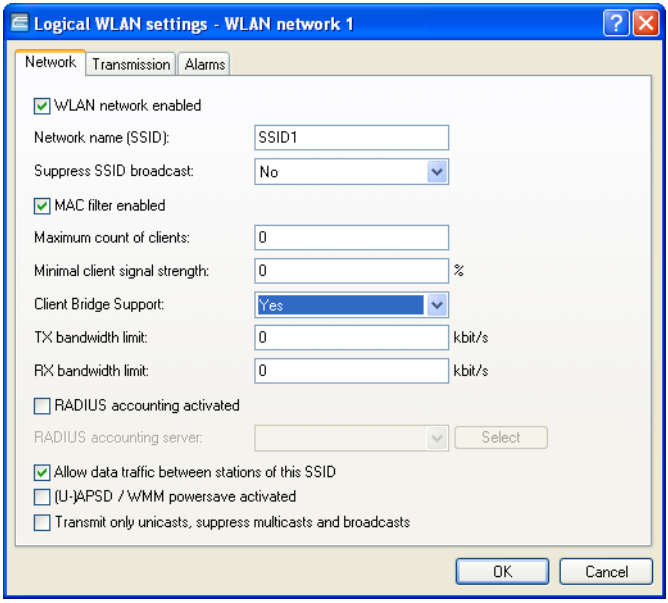


Figure 10: Roaming by a dual-radio client in a PRP-based WLAN infrastructure

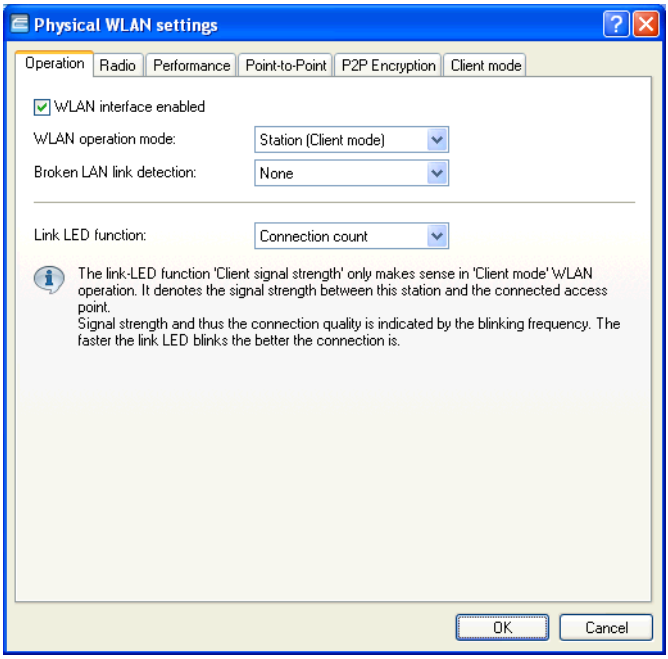
In order for the receiver to detect duplicate data packets, the APs in the WLAN infrastructure must be operating in client-bridge mode. The MAC address of the dual-radio client together with the RCT ensure that the receiver detects the duplicate packets. Without client-bridge support, an AP in the WLAN infrastructure would replace the MAC address of the dual-radio client with its own MAC address, so preventing the detection of duplicates.

Client-bridge support is enabled with LANconfig under `Wireless LAN : General : Logical WLAN settings` on the "Network" tab.


Logical WLAN settings - WLAN network 1
Network
Transmission
Alarms
WLAN network enabled
Network name (SSID):
SSID1
Suppress SSID broadcast:
No
MAC filter enabled
Maximum count of clients:
0
Minimal client signal strength:
0
%
Client Bridge Support:
Yes
TX bandwidth limit:
0
kbit/s
RX bandwidth limit:
0
kbit/s
RADIUS accounting activated
RADIUS accounting server:
Select
Allow data traffic between stations of this SSID
(U-)APSD / WMM powersave activated
Transmit only unicasts, suppress multicasts and broadcasts
OK
Cancel

The PRP configuration of the dual-radio clients involves the following steps:

☐ Under `Wireless LAN : General : Physical WLAN settings`, go to the "Operation" tab for each WLAN interface (WLAN interface 1, WLAN interface 2) and set the "WLAN operation mode" for each one to "Client".

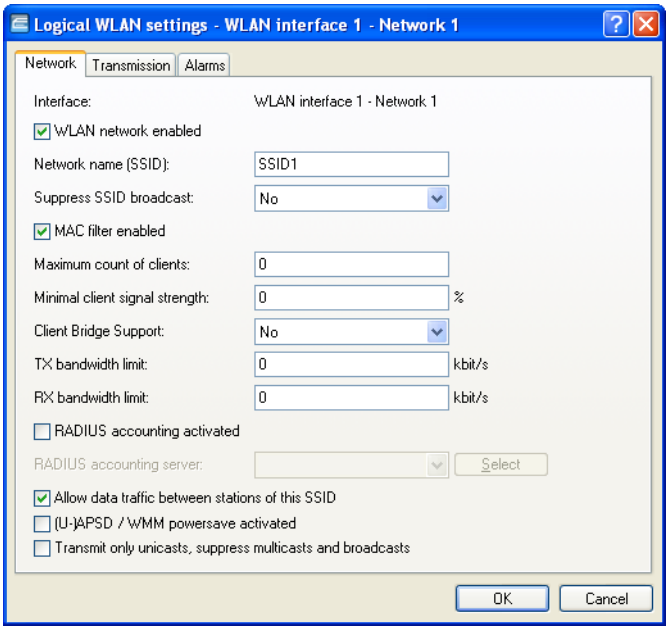


Specify the remaining WLAN parameters under "Radio", "Performance", "Encryption" and "Client mode" according to the requirements of the WLAN radio cells.

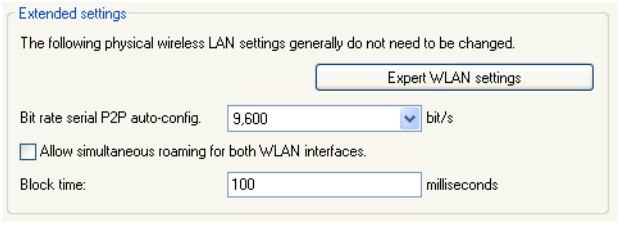
Important: In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

☐ To enter the SSID, switch to the view `Wireless LAN : General`, click "Logical WLAN settings" and, for each WLAN interface, select network 1.

☐ In the field "Network name (SSID)", enter the name of the WLAN which the WLAN interface is to be connected to.



☐ Under `Wireless LAN : General` in the section "Extended settings", disable the option "Allow simultaneous roaming for both WLAN interfaces".



By deactivating the parallel roaming, you prevent the two physical WLAN interfaces from roaming at the same time or performing background scans. The result could be that both could lose connectivity to their radio cell.

When configured in this way, the dual-radio client can move past a line of APs and roam between the individual APs (see fig. 10 on page 297).

4.12 Adjustable rate adaptation algorithm

In contrast to an Ethernet connection, a WLAN connection uses variable bit rates. Higher bit rates provide better throughput, but they also require higher signal quality at the receiver, so that the device decodes it without any errors. WLAN devices adjust the bit rate when properties of the medium change, or when they set up a connection for the first time. They thus ensure that you are using the best available bit rate.
In contrast to the standard algorithm, the familiar minstrel algorithm checks not only the neighboring bit rates, but all of them, and can determine the optimal bit rate faster.

4.12.1 Enhancements in the menu system

`Method`
Here you set the desired rate adaptation algorithm. You must note that the minstrel algorithm in HiLCOS is an experimental implementation.

- **SNMP ID:**
  2.12.51.1
- **Telnet path:**
  `Setup:WLAN:Rate Adaptation`
- **Possible values:**
  Standard
  Minstrel
- **Default:**
  Standard

`Initial Rate`

The initial rate determines the bit rate at which the algorithm starts to determine the optimal bit rate.

- **SNMP ID:**
  2.12.51.2
- **Telnet path:**
  `Setup:WLAN:Rate Adaptation`
- **Possible values:**
  Minimum
  RSSI-dependent
- **Default:**
  Minimum

`Smoothing factor`
The smoothing factor that is applied when the net rates are recalculated for each bit rate.

- **SNMP ID:**
  2.12.51.2
- **Telnet path:**
  `Setup:WLAN:Rate Adaptation`
- **Possible values:**
  0 to 99
- **Default:**
  75

5 Central WLAN Management

In many areas, WLAN systems are suitable substitutes for or additions to wired networks. In some cases, WLANs even provide completely new application options that can enable major progress in organizing the work, or significant resource saving possibilities.

5.1 Application Examples

5.1.1 Managed Mode

The widespread use of wireless Access Points and wireless routers has resulted in a significantly more comfortable and flexible access to networks in companies, universities and other organizations. By employing central WLAN management in managed mode, Access Points are configured in a central instance, the WLAN-Controller.
The WLAN-Controller authenticates the Access Points and transfers a certificate and a matching configuration to the admitted devices. You can thus configure the wireless network comfortably from a central position and the configuration changes simultaneously affect all Access Points.
Using split management, you can separate the WLAN configuration from the remaining router configuration. This is how you can configure e.g. the router and VPN settings in branch offices or home offices. You can define the WLAN configuration via a Hirschmann WLAN Controller in the head office.

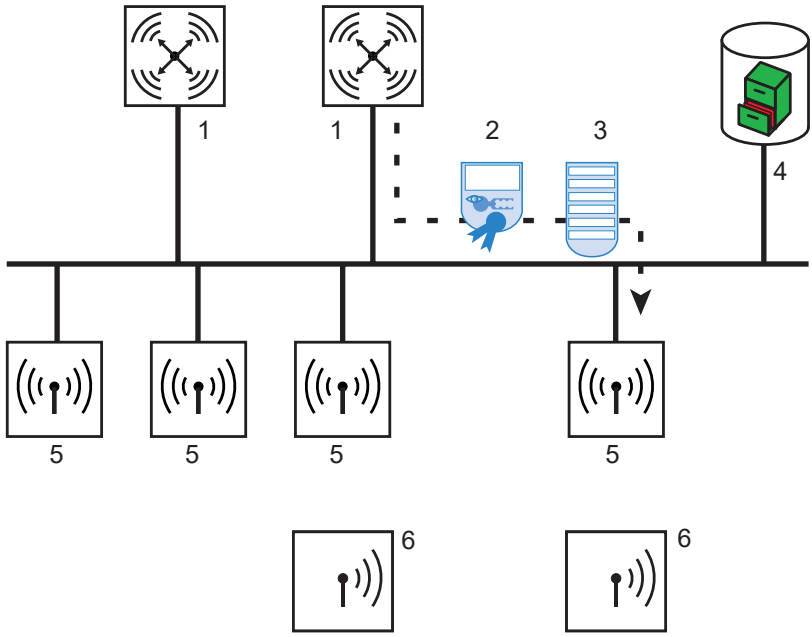


Figure 11: Configuring several Access Points with one WLAN Controller

1: WLAN Controller
2: Certificate
3: Configuration
4: Server
5: Access Point
6: WLAN Client

5.1.2 WLAN Bridge to Access Point – Managed and Unmanaged Mixed

The Access Points managed by a central WLAN Controller are usually directly connected to the wired Ethernet. If a direct connection is not possible, you can also integrate the managed Access Points via a WLAN bridge into the LAN, as far as they have 2 WLAN modules. In this application case, a WLAN module functions as managed Access Point. This WLAN module always retrieves its configuration centrally from the WLAN Controller. The other WLAN module functions as fixed WLAN bridge during this process.

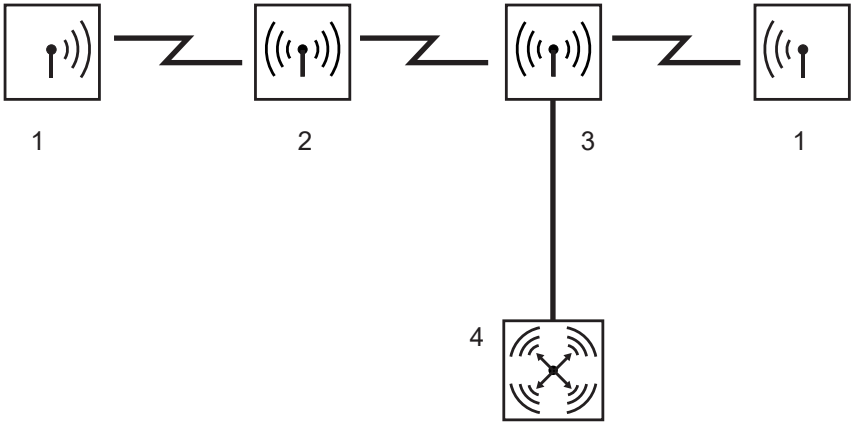


Figure 12: Mixed configuration with WLAN bridge to Access Point

5.2 Introduction

The widespread use of wireless Access Points and wireless routers has resulted in a significantly more comfortable and flexible access to networks in companies, universities and other organizations.
Despite all advantages of WLAN structures, there are still some open aspects to consider:

- ☐ All wireless Access Points must be configured and monitored correspondingly to detect unwanted WLAN Clients, etc. With larger WLAN structures and corresponding security mechanisms, high qualifications are needed for the administration of Access Points. Furthermore, persons in charge must be experienced and significant resources are tied down in IT departments.
- ☐ If the WLAN structure is changed, the manual adjustment of the Access-Point configuration might take a longer period of time. Therefore there will be different configurations in the WLAN at the same time.
- ☐ The joint use of the shared transfer medium (air) requires an effective coordination of the Access Points to avoid frequency overlaps and to optimize the network performance.
- ☐ Access Points in publicly accessible locations represent a potential security risk, as not only the devices, but also the security-relevant data stored in them, such as passwords, are exposed to the risk of theft. Also, third parties may connect external Access Points to the LAN unnoticed and thus bypass the valid security regulations.

A central WLAN management will resolve these problems. The Access Points are configured in a central instance, the WLAN Controller. The WLAN Controller authenticates the Access Points and transfers a matching configuration to the admitted devices. This permits you to configure the wireless network comfortably from a central position. The changes in configuration simultaneously affect all Access Points. The device saves the configuration assigned by the WLAN Controller in the Access Points optionally in the RAM instead of the flash memory. This will ensure that, with particularly security-critical networks, no security-relevant data will get into the hands of unauthorized persons if the devices are stolen. Exclusively in stand-alone operation will the device optionally save the configuration in the flash memory for a defined period of time. There is no possibility of accessing this memory area with LANconfig or other tools.

5.2.1 The CAPWAP Standard

With the Control And Provisioning of Wireless Access Points (CAPWAP protocol), the Internet Engineering Task Force (IETF) presents a draft standard for the central management of large WLAN structures.
CAPWAP uses 2 channels for data transfer:

- ☐ Control channel, DTLS-encrypted. This channel is used to exchange management information between WLAN Controller and Access Point.

  Note: Datagram Transport Layer Security (DTLS) is a TLS-based encryption protocol. It can also be used for transfers via connectionless, unsecured transport protocols, such as UDP. DTLS hence combines the advantages of the high security provided by TLS with the rapid transfer via UDP. Unlike TLS, DTLS is therefore also suitable for the transmission of VoIP packets, as the device can still authenticate the subsequent packets even after the loss of a packet.

- ☐ Data channel, optionally also DTLS-encrypted. The WLAN Controller transfers the WLAN payload data from the Access Point into the LAN - encapsulated in the CAPWAP protocol.

5.2.2 The Smart Controller Technology

A decentralized WLAN structure with autonomous Access Points (stand-alone operation referred to as "Rich Access Points") includes all functions for data transfer on the PHY layer, the control functions on the MAC layer and the management functions in the Access Points. The central WLAN management assigns these tasks to two different devices:

- ☐ The central WLAN Controller assumes the management tasks.
- ☐ The decentralized Access Points handle the data transfer on the PHP layer and the MAC functions.
- ☐ A RADIUS or EAP server may be added as a third component to authenticate the WLAN Clients. This is also possible in stand-alone wireless networks.

CAPWAP describes 3 different scenarios for the relocation of WLAN functions to the central WLAN Controller.

☐ Remote MAC: The device transfers all WLAN functions from the Access Point to the WLAN Controller. In this case, the Access Points serve exclusively as "extended antennas" without own intelligence.

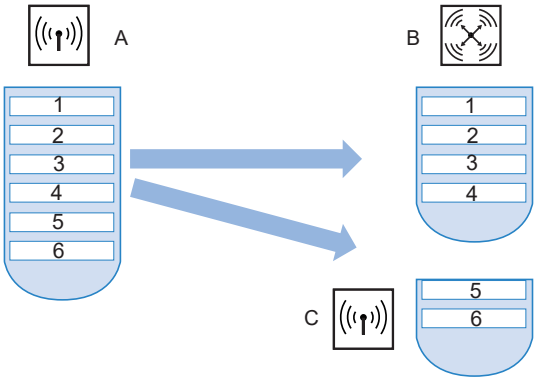


Figure 13: Split MAC in central WLAN management
A: Autonomous Access Point
B: WLAN Controller
C: Decentralized Access Point
1: Management
2: Authentication
3: Realtime MAC
4: Non-realtime MAC
5: PHY layer
6: Antenna

☐ Split MAC: With this variant, the WLAN Controller only obtains some of the WLAN functions. Usually the Access Point continues to perform the time-critical applications (realtime applications) and the applications that are not time-critical (non-realtime applications) will be performed by the central WLAN Controller.

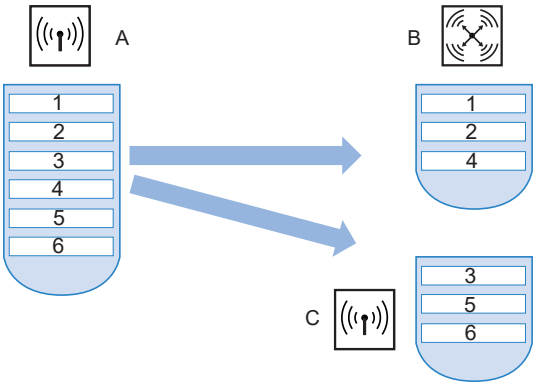


Figure 14: Split MAC in central WLAN management
A: Autonomous Access Point
B: WLAN Controller
C: Decentralized Access Point
1: Management
2: Authentication
3: Realtime MAC
4: Non-realtime MAC
5: PHY layer
6: Antenna

☐ Local MAC: The third option is the complete management and monitoring of the WLAN data traffic directly in the Access Points. The Access Point and the WLAN Controller merely exchange messages on ensuring a uniform configuration of the Access Points and on network management.

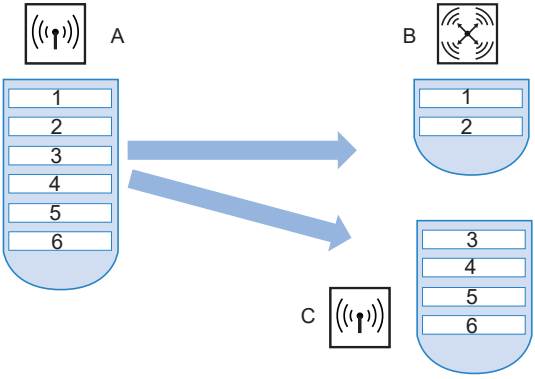


Figure 15: Local MAC with central WLAN management
A: Autonomous Access Point
B: WLAN Controller
C: Decentralized Access Point
1: Management
2: Authentication
3: Realtime MAC
4: Non-realtime MAC
5: PHY layer
6: Antenna

Hirschmann's smart controller technology employs the local MAC procedure. Through the reduction of centralized tasks, these WLAN structures offer optimum scalability. At the same time, such a structure prevents bottlenecks at the WLAN Controller, which processes large parts of the overall data traffic. Remote-MAC and split-MAC architectures always require centralized processing of all payload data in the WLAN Controller. In local-MAC architectures, the Access Points alternatively release the data directly into the LAN, permitting high-performance data transfer. This makes Hirschmann WLAN Controllers suitable for wireless networks complying with the IEEE 802.11n draft standard, offering significantly higher bandwidths than conventional wireless networks. Route the data directly into special VLANs when releasing them to the LAN. This makes it very easy to set up closed networks, e.g. for guest access accounts.

5.2.3 Communication between Access Point and WLAN-Controller

Communication between an Access Point and the WLAN-Controller is always initiated by the Access Point. In the following cases, the devices search for a WLAN-Controller that assigns them a configuration:

- ☐ A Hirschmann Access Point is still set to its factory default settings and has not been configured yet. In this state, the WLAN modules are switched off, the Access Point searches the LAN for a WLAN-Controller.
- ☐ A Hirschmann Access Point has already been configured, at least one WLAN module has been manually set to the operating mode 'managed'. The Access Point searches for a WLAN-Controller for the corresponding WLAN module(s) in the LAN.

At the beginning of the communication, the Access Point sends a "Discovery Request Message" to identify the available WLAN-Controllers. The device sends this request as broadcast. However, because in some structures, the Access Point cannot reach a potential WLAN-Controller via broadcast, define special addresses of additional WLAN-Controllers in the configuration of the Access Points.

Note: The device can also resolve DNS names of WLAN-Controllers. All Access Points with HiLCOS 7.22 or higher have the pre-configured default name 'WLC-Address' so that a DNS server can resolve this name to a Hirschmann WLAN Controller. The same applies to the DNS suffixes learned via DHCP. This also makes it possible to reach WLAN-Controllers that are located in the same network without having to configure the Access Points.

From the available WLAN-Controllers, the Access Point selects the best one and queries it for the structure of the DTLS connection. The "best" WLAN-Controller for the Access Point is the one with the least load, that is the one with the lowest rate of managed Access Points compared to the maximum possible Access Points. In case of 2 or more equally "good" WLAN-Controllers, the Access Point selects the nearest one in the network, i.e. the one with the shortest response time.

The WLAN-Controller then uses an internal random number to determine a unique and secure session key which it uses to protect the connection to the Access Point. The CA in the WLAN-Controller issues a certificate to the Access Point by means of SCEP. The certificate is protected as "challenge" by a password for one-time use only, the Access Point uses this certificate for authentication to the WLAN-Controller to collect the certificate.
The Access Point is provided with the configuration for the integrated SCEP client via the secure DTLS connection – the Access Point is then able to retrieve ts certificate from the SCEP CA via SCEP. Once this is done, the assigned configuration is transferred to the Access Point.

Note: SCEP stands for Simple Certificate Enrollment Protocol; CA for Certification Authority.

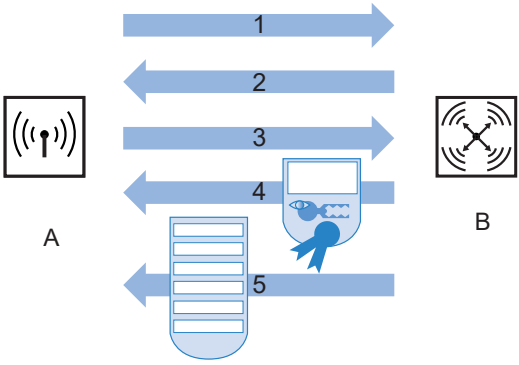


Figure 16: Communication between WLAN Controller and Access Point
A: Access Point
B: WLAN Controller
1: DTLS request
2: SCEP configuration
3: SCEP request
4: Certificate
5: Configuration

Perform the authentication and configuration either automatically or exclusively with a corresponding entry of the Access Point's MAC address in the AP table of the WLAN-Controller. If the Access Point's WLAN modules were deactivated at the beginning of the DTLS communication, the WLAN Controller will activate them after successful transfer of the certificate and configuration.
The management and configuration data will then be transferred via the CAPWAP tunnel. The WLAN Client releases the payload data from the Access Point directly into the LAN and transfers them, for example, to the server.

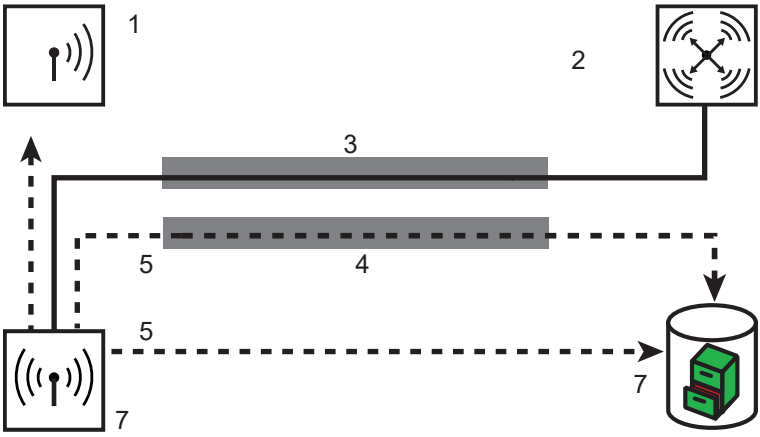


Figure 17: Communication between Access Point and WLAN Controller with CAPWAP tunnel
1: WLAN Client
2: WLAN Controller
3: CAPWAP tunnel
4: CAPWAP tunnel for payload data
5: Payload data
6: Access Point
7: Server

5.2.4 Zero-Touch Management

Hirschmann WLAN Controllers can automatically assign a certificate and configuration to the requesting Access Points. The devices hence implement genuine "zero-touch management". Simply connect new Access Points to the LAN. The Access Points can be operated without special configuration. This simplification to the mere installation of devices reduces the workload of IT departments, especially in decentralized structures. In remote locations, no special IT or WLAN know-how is necessary for the setup.

5.2.5 Split Management

Hirschmann Access Points optionally also locate your WLAN-Controller in remote networks. A simple IP connection, e.g. via a VPN path, is sufficient. As the WLAN-Controllers only influence the WLAN-related part of the configuration in the Access Point, all other functions can be managed separately, if required. Thanks to the distribution of configuration tasks, Hirschmann WLAN Controllers are ideal for setting up a company-wide WLAN infrastructure. The WLAN infrastructure includes the head office and all affiliated branches and home offices.

5.2.6 Inheritance of Parameters

A Hirschmann WLAN-Controller is capable of managing many different Access Points in different locations. The WLAN profile settings are not equally suitable for the managed Access Points. For example, there are differences in the country settings or the device properties.

The logical wireless networks and the physical WLAN parameters can "inherit" specific features from other entries. Even in complex applications, WLAN parameters can thus be managed in common profiles.

- ☐ Initially generate the basic settings that are valid for the majority of managed Access Points.
- ☐ Then generate entries for the more specific values, e.g. country-specific physical settings or a public logical WLAN network.

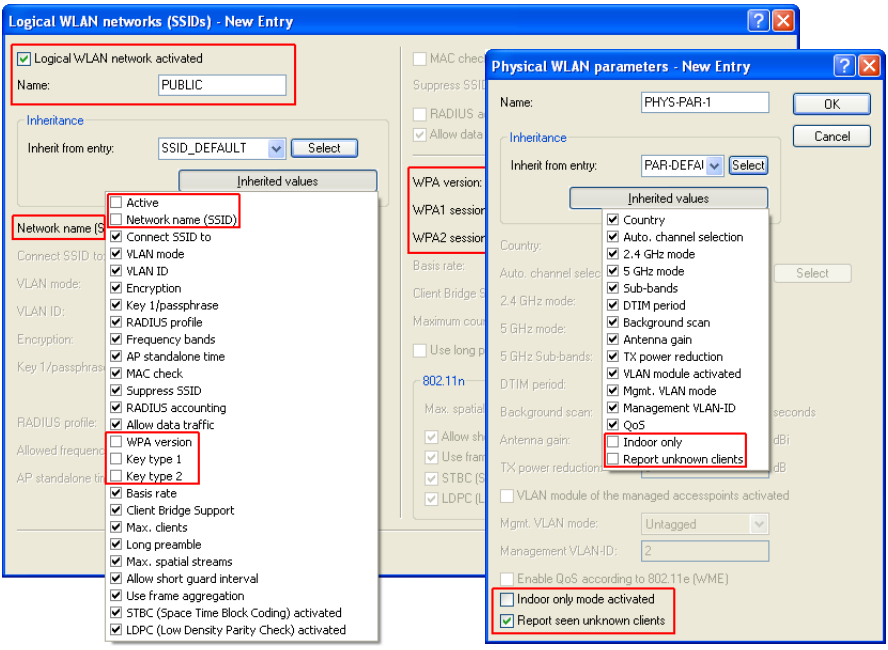


Figure 18: Inheritance of parameters in the case of multiple Access Points

- ☐ Select the entry from which the values are to be inherited and mark the values for inheritance. In the configuration dialog, the inherited parameters will be displayed in gray. You cannot edit these entries.
- ☐ Depending on the application, the edited WLAN settings are then grouped into separate profiles which the device assigns to the respective Access Points.

Note: Inheritance allows chains over multiple stages (cascading). This means that, e.g. country and device-specific parameters can be grouped. Use recursion, if necessary. Profile A then inherits properties from profile B, and at the same time profile B also inherits from profile A. However, the parameters available for inheritance are limited to one "inheritance direction" per parameter.

5.2.7 Opportunistic key caching (OKC)

Authentication of wireless clients using EAP and 802.11X has become standard in corporate networks, and these methods are becoming even more widespread with the integration of the Hotspot 2.0 specification for public Internet access. The disadvantage of 802.11X authentication is the significantly longer time between login and connection, because up to twelve data packets have to be exchanged between the WLAN client and the access point. For most applications, which are all about data exchange, this may not be particularly important. However, for time-critical applications such as Voice over IP, it is important that the authentication at neighboring WLAN radio cells does not affect communication.

To counteract this, authentication strategies such as PMK caching and pre-authentication have become established, although pre-authentication does not fix all of the problems. On the one hand, there is no guarantee that the WLAN client can recognize whether the access point can perform pre-authentication. On the other hand, pre-authentication causes considerable load on the RADIUS server, which needs to handle the authentication of all clients and all access points in the WLAN.

Opportunistic key caching delegates the key management to a WLAN controller, or to a central switch, which manages all of the access points in the network. If a client logs on to an access point, the WLAN controller behind it works as an authenticator to manage the keys and send the PMK to the access point, which is ultimately received by the client. If the client moves to

another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID. It then send this to the new access point in the hope that OKC is enabled there (therefore "opportunistic"). If the access point cannot handle the PMKID, then it negotiates an 802.11X authentication with the client in the usual manner.

An OpenBAT can even perform OKC if the WLAN controller is temporarily unavailable. In this case, it stores the PMK and sends this to the WLAN controller when it becomes available again. Ultimately it sends the PMK to all of the access points in the network, which allows clients to use OKC to login after a change of radio cell.

5.2.8 Fast roaming

The IEEE 802.11r standard ensures that mobile WLAN clients can use a simplified authentication process to roam trouble-free from one access point to the next. Particularly for VoIP, laborious key negotiations while roaming can interfere with the connection, because the wireless client is unable to transfer VoIP data at this time.

Similar to opportunistic key caching (OKC), a centralized key management (preferably by a WLAN controller) supplies the access points connected to it with the credentials of the WLAN clients. In contrast to OKC, the WLAN client during fast roaming can detect whether the access point supports the 802.11r standard.

Access points managed by the WLAN controller transmit the mobility domain information element (MDIE) to inform the WLAN clients about which "mobility group" the access point belongs to, among other things. Based on this information, the WLAN client detects whether it belongs to the same domain and can therefore authenticate without delay. This mobility domain is announced to a WLAN client the first time it authenticates at an access point.

The domain identifier, along with other special keys generated during the initial authentication and transmitted to all managed access points, reduce the stages of negotiation when authenticating at a new access point to just four to six steps.

Note: Older WLAN clients may have trouble establishing a connection to an SSID with enabled 802.11r. Therefore, it is advisable to use two SSIDs here: One SSID for older clients without 802.11r support and another SSID with enabled 802.11r for clients that support 802.11r.

Fast roaming is setup in LANconfig under `Wireless LAN : 802.11i/WEP : WPA or private WEP settings`.

5.2.9 Hirschmann Active Radio Control (ARC)

The intelligent WLAN optimization concept behind **Hirschmann Active Radio Control (ARC)** helps you to sustainably optimize your radio field and proactively avoid sources of interference on the WLAN. Active Radio Control consists of numerous complementary functions in the operating system HiLCOS, which combine to significantly improve the performance of your WLAN. All of the features in Active Radio Control are included for free in the operating system HiLCOS and they are easy to operate with the appropriate management tools.

☐ **RF optimization**

Automatic selection of optimum WLAN channels: WLAN clients benefit from improved throughput thanks to reduced channel overlap. In controller-based WLAN installations, the optimal channels are selected automatically for managed access points.

For more information about RF optimization, see the relevant section on page 365.

☐ **Band steering**

Make optimal use of your WLAN's bandwidth: Automatically controlled by the access point, clients steered to the 5-GHz frequency band can effectively double the WLAN performance because only here are sufficient channels available for channel bundling.

For more information about band steering, see the relevant section on page 207.

☐ **Adaptive noise immunity**

Better WLAN throughput thanks to immunity to interfering signals: WLAN clients benefit from significantly improved data throughput thanks to interference-free signal coverage. Enabling the adaptive noice immunity allows an access point to block out interfering signals and to focus exclusively on WLAN clients with sufficient signal strength.

For more information about adaptive noise immunity, see the relevant section on page 210.

☐ **Spectral scan**

Check your WLAN radio spectrum for sources of interference: With Spectral Scan, you have a professional tool for efficient WLAN troubleshooting. A scan of the entire radio spectrum identifies sources of interference from outside the WLAN and allows a graphical representation.

For more information about spectral scanning, see the relevant section on page 356.

5.3 Configuration of the WLC

5.3.1 General settings

Most parameters for the configuration of the Hirschmann WLAN Controllers correspond to those of the Access Points. This section describes merely those aspects required for the operation of the WLAN-Controller.
This is where you perform the basic settings for your WLAN-Controller.

☐ Automatically accept new APs (auto-accept)
This option enables the WLAN-Controller to assign a configuration to Access Points without valid certificates as well.
It enables the WLAN-Controller to assign a certificate to all new Access Points without such a valid certificate. One of the following conditions must be fulfilled:
- For the Access Point, a configuration must be entered under its MAC address in the AP table.
- The option 'Automatically provide APs with a default configuration' is activated.

☐ Automatically provide APs with a default configuration
This option enables the WLAN-Controller to assign a default configuration to new Access Points without valid certificates. The WLAN-Controller uses the default configuration for all Access Points for which you do not define an explicit configuration. Together with the auto-accept option, this option permits the automatic acceptance of all Access Points found in the LAN. This automatic process ends as soon as the number of logged-in Access Points reaches the maximum number for the WLAN-Controller. Access Points accepted by default will also appear in the MAC list.

Note: This option might also allow unknown Access Points to access your WLAN structure. Therefore only activate this option during the start-up phase when setting up a centrally managed WLAN structure.
The combination of the settings for auto-accept and the default configuration makes it possible to set up and operate Access Points in different situations:

Auto-accept	Default configuration	Suitable for
On	On	Roll-out phase: Use this combination only if unwanted Access Points cannot be connected to the LAN.
On	Off	Controlled roll-out phase: Use this combination if the following conditions apply: You have entered all approved Access Points along with their MAC address into the AP table. You want to accept the entered Access Points automatically into the WLAN structure.
Off	Off	Normal operation: New Access Points require the administrators' approval to access the WLAN structure.

5.3.2 Profiles

In the profiles area, you define the logical WLAN networks, physical WLAN parameters, and the WLAN profiles which represent a combination of these two elements.

WLAN Profiles

The WLAN profiles summarize the settings to be assigned to the Access Points. The WLAN profiles are allocated to the Access Points in the AP table.

For every WLAN profile, define the following parameters:

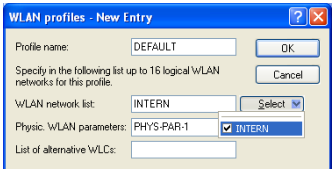


Figure 19: Creating a new WLAN profile

LANconfig: WLAN-Controller > Profiles > WLAN profiles

WEBconfig: HiLCOS-Menu tree > Setup > WLAN management > AP configuration > Common profiles

- ☐ Profile name
  Name of the profile under which the settings are saved.
- ☐ WLAN network list
  List of the logical WLAN networks that are assigned via this profile.
- ☐ Physical WLAN Parameters
  A set of physical parameters that the WLAN modules of the Access Points work with.
- ☐ IP address of alternative WLAN-Controller
  A list of WLAN-Controllers that the Access Point attempts to connect with. The Access Point starts searching for a WLAN-Controller via a broadcast. When the Access Point cannot reach all WLAN-Controllers with such a broadcast, the definition of alternative WLAN-Controllers is advisable. This is the case e.g. when the WLAN-Controller is located in another network.

Logical WLAN Networks

Here you define the logical WLAN networks that the WLAN-Controller assigns to the Access Points. For every logical WLAN network, define the following parameters:

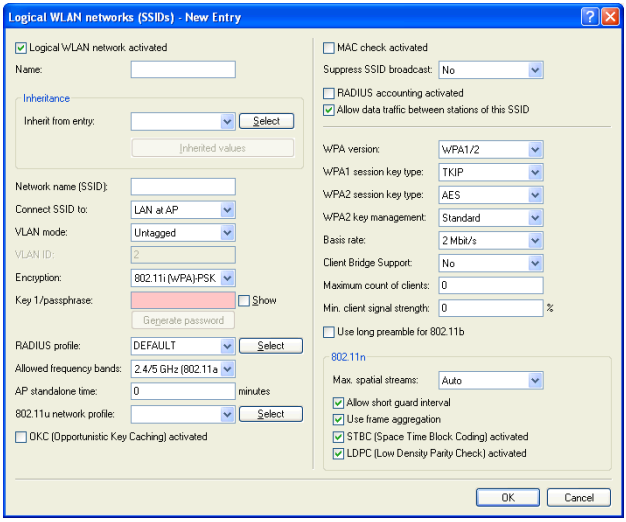


Figure 20: Creating a new entry for a logical WLAN network

LANconfig: WLAN-Controller > Profiles > Logical WLAN networks
WEBconfig: HiLCOS-Menu tree > Setup > WLAN management > AP configuration > Network profiles

☐ "Logical WLAN network activated"

Enable the logical WLAN network by clicking on this option.

☐ "Name"

Here, specify a name which uniquely identifies the logical WLAN network.

☐ "Inheritance"

If you wish to create entries that differ only slightly from existing ones, you can choose a "parent" entry here and select the parameters which are to be applied each time it is used.

Note: A "parent" entry itself can contain inherited entries. Try to ensure that the structure of inherited entries is not too complex, otherwise they may be difficult to understand and configure.

☐ "Network name (SSID)"

Enter the SSID of the WLAN network here. All stations that belong to this WLAN network must use the same SSID.

☐ "SSID connect to"

Here you select which of the access point's logical interfaces is to be associated with the SSID, i.e. where the access point sends the data packets for this SSID.

– "LAN": The access point forwards the data packets locally into the LAN (LAN-1) by default. It must be configured appropriately to do this.

– "WLC-Tunnel-x": The SSID is connected to a WLC bridge layer-3 tunnel. Please note that a maximum of 7 WLC Bridge Layer 3 tunnels are supported. The access point sends all data packets to this tunnel and thus to the WLC. This tunnel must be configured on the WLC.

Note: Note that although forwarding all data packets to the WLC allows you to define routes and filters centrally, this creates a heavy load on the WLAN controller This model demands a correspondingly high bandwidth in order to transfer all of the data traffic of this and any other SSIDs that are connected to this WLAN controller via WLC tunnel.

☐ "VLAN mode"

This item sets the access point VLAN mode for packets belonging to this WLAN network (SSID). VLAN IDs are used if the VLAN module is enabled in the physical WLAN parameters of the access point. Otherwise the access point ignores all VLAN settings in the logical networks. Even with VLAN activated, it is possible to operate the network untagged.

– "Untagged": The access point does not tag data packets from this SSID with a VLAN ID.

– "Tagged": The access point marks the data packets with the VLAN ID specified as follows.

Note: Even with VLAN activated, it is possible to operate a WLAN network untagged. The VLAN ID '1' is reserved internally for this.

☐ "VLAN-ID"

VLAN ID for this logical WLAN network

Note: Please note that to use VLAN IDs in a logical WLAN network, you must set up a management VLAN ID (see physical WLAN parameters).

☐ "Encryption"

This item sets the encryption method or, in the case of WEP, the key length for packet encryption in this WLAN.

☐ "Key 1/passphrase"

You can enter the key or passphrase as an ASCII character string. An option for WEP is to enter a hexadecimal number by adding a leading "0x". The following character string lengths result for the formats used:

– WPA-PSK: 8 to 63 ASCII characters

– WEP128 (104 bit): 13 ASCII or 26 hex characters

– WEP64 (40 bit): 5 ASCII or 10 hex characters

☐ "RADIUS profile"

Specify which RADIUS profile the access point should receive for this network, so that it can connect directly to the RADIUS server if necessary. Leave this field blank if the WLAN controller is to handle RADIUS requests.

Note: You configure the RADIUS profiles in the corresponding table.

☐ "Allowed frequency bands"

Here you set the frequency band used by network participants for transmitting data on the wireless network. You can select the 2.4-GHz band, the 5-GHz band, or both bands.

☐ "AP standalone time"

The time in minutes that a managed-mode access point continues to operate in its current configuration.

The configuration is provided to the access point by the WLAN controller and is optionally stored in flash memory (in an area that is not accessible to LANconfig or other tools). Should the connection to the WLAN controller be interrupted, the access point will continue to operate with the configuration stored in flash for the time period entered here. The access point can also continue to work with this flash configuration after a local power outage.

If there is no connection to the WLAN controller after this time period has expired then the flash configuration is deleted and the access point goes out of operation. As soon as the WLAN controller is available, the WLAN controller transmits the configuration to the access point again.

This represents an effective measure against theft as the access point deletes all security-related configuration parameters after this time has expired.

Note: If the access point establishes a backup connection to a secondary WLAN controller, then the countdown to the expiry of standalone operation is halted. The access point and its WLAN networks remain active as long as it has a connection to a WLAN controller.

Note: Please note that the access point only deletes the configuration in flash memory after the time for standalone operation has expired, and not when the power is lost!

☐ "802.11u network profile"

Select the Hotspot 2.0 profile from the list.

☐ "OKC activated"

This option enables the opportunistic key caching. OKC makes it easy for WLAN clients to quickly and conveniently roam between WLAN cells in wireless environments with WPA2-Enterprise encryption.

☐ "MAC check activated"

The MAC addresses of the clients that are allowed to associate with an access point are stored in the MAC filter list (`Wireless LAN : Stations : Stations`). The "MAC filter enabled" switch allows you to switch off the use of the MAC filter list for individual logical networks.

☐ "Suppress SSID broadcast"

You can operate your wireless LAN either in public or private mode. A wireless LAN in public mode can be contacted by any mobile station in the area. Your wireless LAN is put into private mode by activating the closed network function. In this operation mode, mobile stations that do not know the network name (SSID) are excluded from taking part in the wireless LAN.

With the closed-network mode activated, WLAN clients that use an empty SSID or the SSID "ANY" are prevented from associating with your network.

The option "Suppress SSID broadcast" provides the following settings:

– **No:** The access point publishes the SSID of the cell. When a client sends a probe request with an empty or incorrect SSID, the access point responds with the SSID of the radio cell (public WLAN).

– **Yes:** The access point does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID.

– **Tightened:** The access point does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device does not respond.

Note: Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

☐ "RADIUS accounting activated"

Select this option if you want to enable the RADIUS accounting in this logical WLAN network.

☐ "Allow traffic between stations of this SSID"

Check this option if all stations logged on to this SSID are to be able to communicate with one another.

☐ "WPA version"

Here you select which WPA version the access point is to offer to the WLAN clients for encryption.

- WPA1: WPA2 only
- WPA2: WPA2 only
- WPA1/2: WPA1 and WPA2 in one SSID (radio cell)

☐ "WPA1 session key type"

If you use "802.11i (WPA)-PSK" for encryption, the method for generating a WPA1 session or group key can be selected here:

- AES: The access point uses the AES method.
- TKIP: The access point uses the TKIP method.
- AES/TKIP: The access point uses the AES method. If the client hardware does not support the AES method, the access point will change to the TKIP method.

☐ "WPA2 session key type"

The method for generating a WPA2 session or group key can be selected here.

☐ "Basis rate"

The defined basis rate should allow the slowest clients to connect to the WLAN even under poor reception conditions. A higher value should only be set here if all clients in this logical WLAN can be reached "faster". By setting the transmission rate to auto, the access point collects information about the transmission rates of the various WLAN clients. Clients automatically notify the access point of this rate with each unicast communication. The access point takes the lowest transmission rate from the list of associated clients and applies this to all multicast and broadcast transmissions.

☐ "Client-bridge support."

Enable this option for an access point if you have enabled the client-bridge support for a client station in WLAN client mode ().

Note: The client-bridge mode operates between two HiLCOS devices only.

☐ "Maximum count of clients"

Here you set the maximum number of clients that may associate with this access point. Additional clients wanting to associate will be rejected by the access point.

☐ "Minimum client signal strength"

This value sets the threshold value in percent for the minimum signal strength for clients when logging on. If the client's signal strength is below this value, the access point stops sending probe responses and discards the client's requests.

A client with poor signal strength will not detect the access point and cannot associate with it. This ensures that the client has an optimized list of available access points, as those offering only a weak connection at the client's current position are not listed.

☐ "Use long preamble for 802.11b"

Normally, the clients in 802.11b mode negotiate the length of the preamble with the access point. "Long preamble" should only be set when the clients require this setting to be fixed.

☐ "Max. spatial streams"

The spatial multiplexing function allows the access point to transmit multiple data streams over separate antennas in order to increase the data throughput. The use of this function is only recommended when the remote device can process the data streams with corresponding antennas.

Note: In the 'Auto' setting, the access point uses all of the spatial streams supported by this WLAN module.

☐ "Allow short guard interval"

This option is used to reduce the transmission pause between two signals from 0.8 µs (default) to 0.4 µs (short guard interval). This increases the effective time available for data transmission and thus the data throughput. However, the wireless LAN system becomes more liable to disruption that can be caused by interference between two consecutive signals.

The short guard interval is activated in automatic mode, provided that the remote station supports this. Alternatively the short guard mode can be switched off.

☐ "Use frame aggregation"

Frame aggregation is used to combine several data packets (frames) into one large packet and transmit them together. This procedure reduces the overhead of the packets to increase the throughput.

Frame aggregation is not suitable when working with mobile receivers or time-critical data transmissions such as voice over IP.

☐ "STBC (space time block coding) activated"

Activate the space time block coding here.

The function 'STBC' additionally varies the transmission of data packets over time to minimize time-related effects on the data. Due to the time offset of the packets the recipient has an even better chance of receiving error-free data packets, regardless of the number of antennas.

☐ "LDPC (low density parity check) activated"

Activate the low density parity check here.

Before the sender transmits the data packets, it expands the data stream with checksum bits depending on the modulation rate. These checksum bits allow the receiver to correct transmission errors. By default the 802.11n standard uses 'Convolution Coding' (CC) for error correction, which is well-known from 802.11a and 802.11g; however, the 11n standard also provides for error correction according to the LDPC method (Low Density Parity Check).

In contrast to CC encoding, LDPC encoding uses larger packets to calculate checksums and can also recognize more bit errors. The improved ratio of payload to checksum data enables LDPC encoding to provide a higher data transfer rate.

Note: All other parameters of the WLAN networks correspond to those of the standard Access Point configurations.

Physical WLAN Parameters

Here you define the physical WLAN parameters that the WLAN Controller assigns to the Access Points. For every set of physical WLAN parameters, define the following parameters:

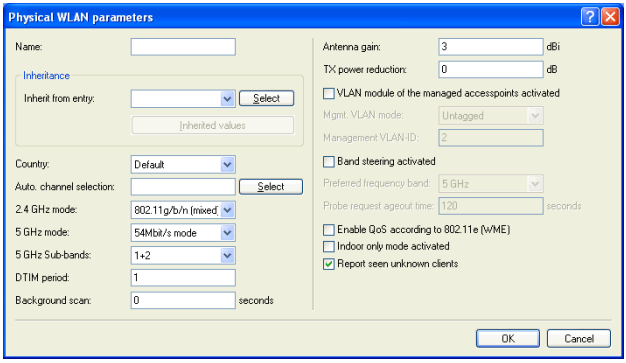


Figure 21: Creating a new entry for a physical WLAN network

LANconfig: WLAN-Controller > Profiles > Physical WLAN parameters
WEBconfig: HiLCOS menu tree > Setup > WLAN management > AP configuration > Radio profiles

☐ Name
Unique name for this combination of physical WLAN parameters.

☐ Inheritance
Selection of a set of physical WLAN parameters defined earlier and from which the entry inherits the settings.

☐ Country
Country in which you operate the Access Points. The device uses this information to define country-specific settings, such as the permitted channels, etc.

☐ Automatic channel selection
By default, the Access Points can use all channels permitted by the country settings. To limit the selection to certain channels, define the desired channels here as a comma-separated list. Ranges can also be defined (e.g. '1,6,11').

☐ Management-VLAN ID
The VLAN ID employed by the management network of the Access Points.

☐ "Band steering activated"
This entry determines whether the access point should enable band steering. In this case, a dual-port access point can forward a WLAN client to a preferred frequency band.

Note: Set the management VLAN ID to a different value than 0 to activate VLANs on the WLAN networks. This also applies when the management network itself is tagged without VLAN IDs (Mgmt-VLAN-ID = 1).
The VLAN activation only applies to those WLAN networks that are connected by means of these physical WLAN parameters.
All other physical WLAN parameters correspond to those for the standard configuration of Access Points.

5.3.3 List of Access Points

Access-point Table

The AP table is a central element for the configuration of WLAN-Controllers. Here the device transmits a WLAN profile to the Access Points based on their MAC addresses, thus a combination of logical and physical WLAN parameters. Furthermore, the mere existence of an entry for a specific Access Point in the AP table enables it to establish a connection to a WLAN-Controller. For every Access Point, define the following parameters:

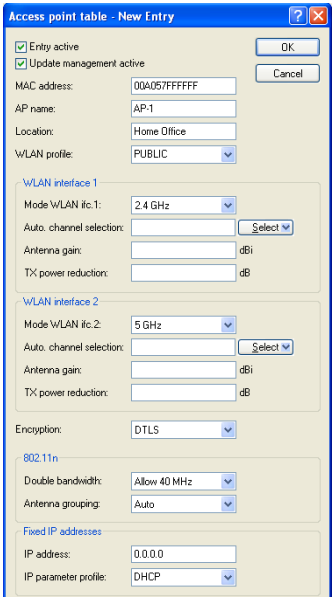


Figure 22: Creating a new Access Point

LANconfig: WLAN-Controller > AP config. > Access-point table
WEBconfig: HiLCOS menu tree > Setup > WLAN management > AP configuration > Access Points

- ☐ Update management active
  Activating update management enables the Access Point to automatically upload the latest firmware or script versions. All other settings are made under AP update.
- ☐ MAC address
  MAC address of the Access Point.
- ☐ Exclusive AP name
  Name of the Access Point in managed mode.
- ☐ Location
  Location of the Access Point in managed mode.
- ☐ WLAN profile
  WLAN profile from the list of defined profiles
- ☐ WLAN interface 1
  Frequency band for the 1st WLAN module. Use this parameter to optionally deactivate the WLAN module.

- ☐ Auto. channel selection Ifc 1
  If no entry is made here, Access Points automatically carry out the channel selection for the frequency band available in the set country of operation.
  Enter the channels to which the automatic selection will be restricted for the first WLAN module. If you enter exactly one channel, the device will use this channel exclusively. In such a case there will be no automatic selection. Therefore when entering a channel number, be certain that it is really valid in the frequency band of the respective country. The device ignores channels that are invalid for the defined frequency band.
- ☐ WLAN interface 1
  Frequency band for the 1st WLAN module. Use this parameter to optionally deactivate the WLAN module.
- ☐ WLAN interface 2
  Frequency band for the 2nd WLAN module.
- ☐ Auto. channel selection Ifc 2
  Automatic channel selection for the 2nd WLAN module.

Note: The device ignores the settings for the second WLAN module, if the managed device has only one WLAN module.

- ☐ Encryption
  Here you define the encryption for the communication over the control channel. Without encryption, the devices exchange the control data as plain text. In both cases authentication is based on certificates.
- ☐ Double bandwidth
  For Hirschmann Access Points according to IEEE 802.11n, activate the use of the double bandwidth here.
- ☐ Antenna grouping
  To optimize the gain through spatial multiplexing, configure the antenna grouping here.
- ☐ IP address
  Specify the static IP address of the Access Point here.
- ☐ IP parameter profile
  Enter the profile name here which the device uses to reference the IP settings for the Access Point. If you retain the default setting DHCP, the Access Point ignores the setting for the static IP address and retrieves its IP address via DHCP.

Default Parameters

You can define central default values for some parameters which the device references as 'default' in other parts of the configuration (for example, using the "Access point table".

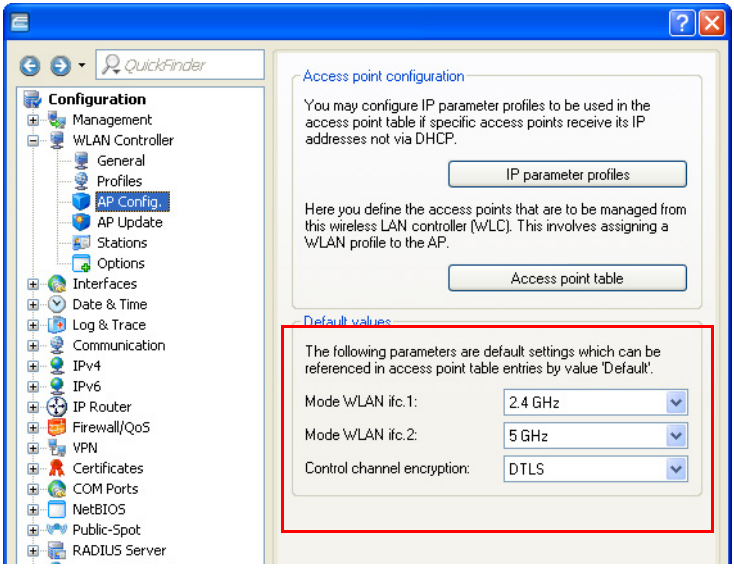


Figure 23: Defining central default values

LANconfig: WLAN-Controller > AP config. > Default values
WEBconfig: HiLCOS-Menu tree > Setup > WLAN management > AP configuration

☐ WLAN interface 1
Frequency band for the 1st WLAN module. Use this parameter to optionally deactivate the WLAN module.

☐ WLAN interface 2
Frequency band for the 2nd WLAN module. Use this parameter to optionally deactivate the WLAN module.

☐ Encryption
Encryption for the communication over the control channel. Without encryption, the devices exchange the control data as plain text. In both cases authentication is based on certificates.

5.3.4 Station Table (ACL Table)

By means of the station table, you define which WLAN Clients can access the WLAN networks of the managed Access Point. Furthermore, the method offers a convenient way to assign an individual authentication passphrase and a VLAN ID to each WLAN Client.
It is imperative that the RADIUS server in the WLAN-Controller is activated in order to use the station table. As an alternative, requests can be forwarded to another RADIUS server.
Activate the MAC check for every logical WLAN network in which WLAN Clients are authenticated by RADIUS.

5.3.5 Options for the WLAN-Controller

In the 'Options' area, you can define notifications in case of events in the WLAN-Controller and set various default values.

Notification can take place via SYSLOG or e-mail. Define the following parameters:

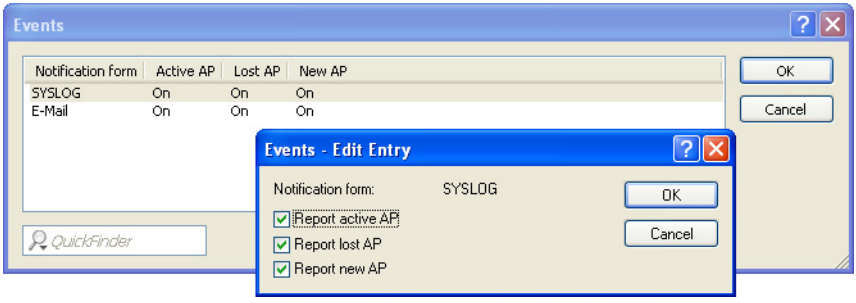


Figure 24: Setting a new event notification

LANconfig: WLAN-Controller > Options > Events
WEBconfig: HiLCOS-Menu tree > Setup > WLAN management > Event notification

- SYSLOG
  Activates notification via SYSLOG.
  Possible values: On/Off.
- E-mail
  Activates notification via e-mail.
  Possible values: On/Off.
- Events
  Selects the events that trigger a notification.
  Possible values:
  - Active Access Point notification
  - Missing Access Point notification
  - New Access Point notification

5.4 Configuring the Access Points

By default, the WLAN modules in the Access Points are set to the operating mode 'Access Point'. In this mode, the devices function as stand-alone Access Points and use a configuration that is stored locally in the device. Switch the operating mode for the WLAN modules in the desired Access Points to 'managed' to integrate them into a centrally managed WLAN structure.

Note: You can define the operating mode separately for every WLAN module. For models with 2 WLAN modules, depending on the application, one module can work with a local configuration, the 2nd module can be part of a centrally managed WLAN structure.

For individual devices, the operating mode of the WLAN modules can be found in LANconfig under Wireless LAN > General > Physical WLAN settings > Operation mode:

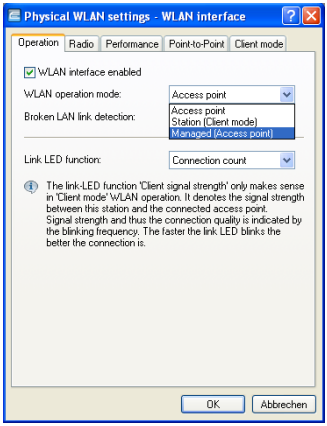


Figure 25: Changing the operating mode of the Access Points to 'managed'

To change the operating mode for multiple devices at the same time, start a simple script for the devices with the following lines:

```
# Script (7.22 / 23.08.2007
lang English
flash 0
cd Setup/Interfaces/WLAN/Operational
set WLAN-1 0 managed-AP 0
# done
exit
```

Note: If the IP address of the Access Point is configured statically, the CAPWAP stack is not aware of a configured default route. Thus it is recommended to use DHCP or the CAPWAP IP profile for a specific IP address assignment to an Access Point.

5.5 Managing the Access Points

5.5.1 Accepting new Access Points manually into the WLAN structure

To integrate the Access Points into the WLAN structure without the automatic (auto-accept) option, accept the Access Points manually.

- **Accepting Access Points via LANmonitor** You can accept new Access Points comfortably via the LANmonitor. Select a configuration that the Access Point uses after transmission of a new certificate.
  In LANmonitor, click the new Access Point with the right-hand mouse button to integrate it into the WLAN structure. From the context menu that pops up, select the configuration for the device.

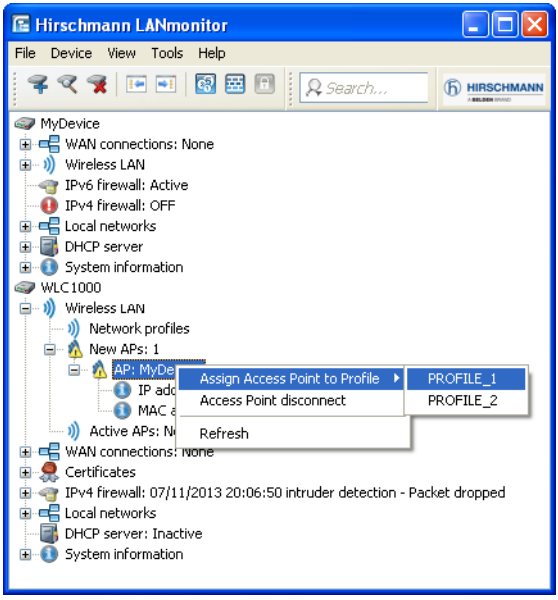


Figure 26: Accepting new Access Point via LANmonitor

Note: This process defines the Access Point in the AP table of the WLAN-Controller. As soon as the Access Point has built up the random, the WLAN-Controller assigns a certificate to the Access Point. Only then will the Access Point become an active element of the central WLAN structure. Until assignment of the certificate is completed, the WLAN-Controller reports the new Access Point with the red Lost-AP LED in the device display and as "Lost AP" in the LANmonitor.

Accepting Access Points via WEBconfig with Assignment of a Certificate

New Access Points with entry in the AP table but without valid certificate can be accepted manually via an action in WEBconfig.

- ☐ Open the configuration of the Hirschmann WLAN-Controller with WEBconfig.
- ☐ Under HiLCOS menu tree>Setup > WLAN management, select the action Accept AP.
- ☐ As parameter for the action, transmit the MAC address of the Access Point that you are integrating into the WLAN structure. Confirm the action with "Execute".

Figure 27: Accepting a new Access Point via WEBconfig with assignment of a certificate

Accepting Access Points via WEBconfig with Assignment of a Certificate and Configuration

New Access Points without entry in the AP table and without valid certificate can be accepted via a new wizard in WEBconfig. Define a configuration that the Access Point uses after transmission of a new certificate.

☐ Open the configuration of the Hirschmann WLAN-Controller with WEBconfig. Among the setup wizards, select the wizard "Assigning new Access Points to profiles".

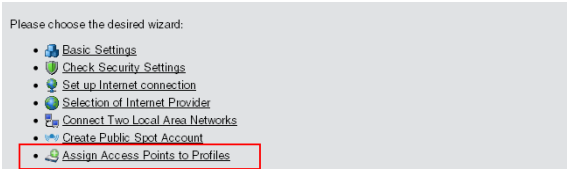


Figure 28: Accepting a new Access Point via WEBconfig with assignment of a certificate and configuration

☐ Click the link to start the wizard. Select the desired Access Point based on its MAC address and enter the WLAN configuration that the device shall assign to the Access Point.

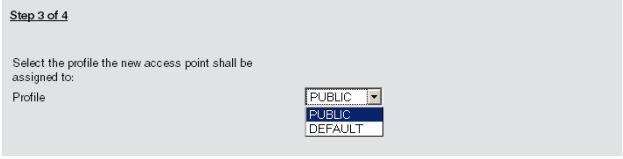


Figure 29: Selecting the WLAN configuration

Note: With the assignment of the configuration, the WLAN-Controller integrates the selected Access Point into the AP table. As soon as the Access Point has built up the random, the WLAN-Controller assigns a certificate to the Access Point. Only then will the Access Point become an active element of the central WLAN structure. Until assignment of the certificate is complete, the WLAN-Controller reports the new Access Point with the red Lost-AP LED in the device display and as "Lost AP" in the LANmonitor.

5.5.2 Removing Access Points manually from the WLAN structure

Perform the following actions to remove a managed Access Point from the WLAN structure:

- ☐ In the Access Point, switch the WLAN operating mode for the WLAN modules from 'managed' to 'client' or 'Access Point'.
- ☐ In the WLAN-Controller, delete the configuration for the Access Point or deactivate the option 'automatic assignment of the default configuration'.
- ☐ Disconnect the Access Point in WEBconfig under HiLCOS menu tree > Setup > WLAN management with the action 'disconnect AP connection' or alternatively in LANmonitor.
- ☐ As parameter for the action, transmit the MAC address of the Access Point that you are removing from the WLAN structure. Confirm the action with "Execute".

Figure 30: Manually removing an Access Point from the WLAN structure

5.5.3 Deactivating or Permanently Removing Access Points from the WLAN Structure

In some cases it is necessary to temporarily deactivate or permanently remove an Access Point managed by the WLAN-Controller.

Deactivating Access Points

To deactivate an Access Point, set the corresponding entry in the AP table to 'inactive' or delete the entry from the table. This process deactivates the WLAN modules in managed mode and deletes the corresponding SSIDs in the Access Point.

Note: This process deactivates the WLAN modules and the WLAN networks (SSIDs) even if stand-alone operation is activated.

An Access Point deactivated like that remains connected to the WLAN-Controller, the certificates are retained. The WLAN-Controller activates the Access Point and its WLAN modules in managed mode, if required. It can do this by activating the existing entry or creating a new entry for the corresponding MAC address in the AP table.

Permanently Removing Access Points from the WLAN Structure

Delete or cancel the certificates in the SCEP client to permanently remove an Access Point from the centrally managed WLAN structure.

- ☐ If you have access to the Access Point, delete the certificates by resetting the device.
- ☐ If a device has been stolen and you want to remove it from the WLAN structure, cancel the certificates in the CA of the WLAN-Controller. In WEBconfig, go to the area Status > Certificates > SCEP-CA > Certificates and access the Certificate status table. Delete the certificate for the MAC address of the respective Access Point here. The certificates are marked as expired, but remain in the device.

Note: In case of a backup solution with redundant WLAN-Controller, cancel the certificates in all WLAN-Controllers.

5.5.4 Managing the Access Points

LANmonitor gives you a quick overview of the Hirschmann WLAN-Controllers in the network and the Access Points within the WLAN structure. LANmonitor LANmonitor displays the following information, among others:

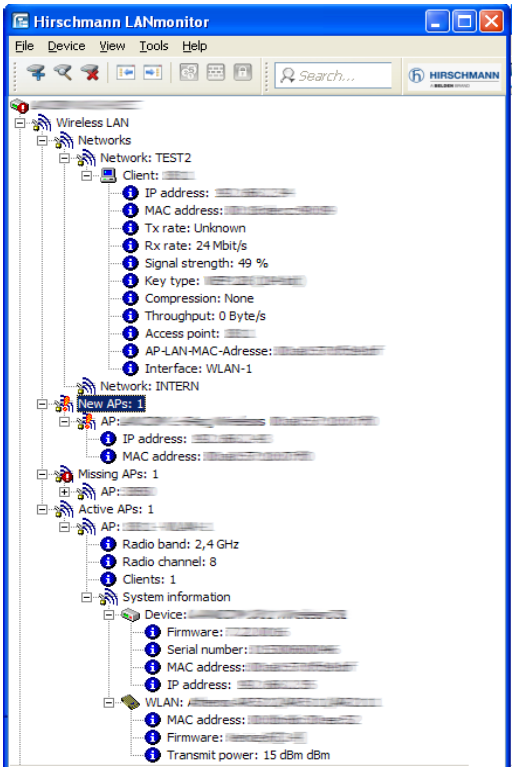


Figure 31: Network in LANmonitor

- ☐ Active WLAN networks with logged-in WLAN Clients and the name of the Access Point where the WLAN Client is logged in.
- ☐ Display of new Access Points with IP and MAC address

- ☐ Display of missing Access Points with IP and MAC address
- ☐ Display of managed Access Points with IP and MAC address, utilized frequency band and channel

Use the right-hand mouse button while pointing at the Access Points to open a context menu with the following actions:

- ☐ Assign new Access Point to profile
  This action assigns a configuration to a new Access Point and integrates it into the WLAN structure.
- ☐ Access Point Disconnect Access Point
  Disconnects Access Point and WLAN-Controller. The Access Point then carries out a new search for the responsible WLAN-Controller. Use this action, e.g., after a backup event to disconnect Access Points from the backup controller and to redirect them to the actual WLAN-Controller.
- ☐ Refresh
  Refreshes the display of the LANmonitor.

5.5.5 Backing up the Certificates

At the first system startup, a Hirschmann WLAN-Controller creates the root certificates for the CA (Certification Authority) and the RA (Registration Authority). Based on these two certificates, the WLAN-Controller generates the device certificates for the Access Points.

Use the same root certificates in the following cases, to ensure smooth operation of the managed Access Points:

- ☐ when you are employing several WLAN-Controllers in parallel within the same WLAN infrastructure (load balancing) or
- ☐ when you are replacing or reconfiguring a device.

Creating Backups of the Certificates

To restore the CA or RA, the device requires the relevant root certificates with the private keys that the WLAN Controller generates automatically at system start. Furthermore back up further files containing information on issued device certificates. To ensure that this confidential information remains protected even when exported from the device, the device initially stores it to a passphrase-protected PCKS12 container.

☐ Open the configuration of the Hirschmann WLAN-Controller with WEBconfig under HiLCOS menu tree > Setup > Certificates > SCEP-CA > CA certificates.

☐ Select the command "create PKCS12 backup files" and enter the passphrase for the PCKS12 container as parameter.

Figure 32: Creating backups of the certificates with PCKS12 container

This action saves the certificates and private keys in PKCS12 files. The files are then available for download from the device.

Downloading Certificate Backups from the Device

☐ Select File management > Download certificate or file

☐ Then, as file type, select the two entries for the SCEP-CA one after the other and confirm with Start download:

- ▶ PKCS12 container with CA backup
- ▶ PKCS12 container with RA backup

Figure 33: Downloading certificate backups from the device

This action saves the backup files to your data carrier. You will not require the passphrase until the backup is uploaded to a Hirschmann WLAN-Controller.

Uploading a Certificate Backup to the Device

- ☐ Select File management > Upload certificate or file
- ☐ Then select the two entries for the SCEP-CA as file type one after the other:
  - ▶ PKCS12 container with CA backup
  - ▶ PKCS12 container with RA backup
- ☐ For each upload, enter the file name with storage location and the corresponding passphrase. Confirm with Start upload:
- ☐ After loading the CA backup, delete the file controller_rootcert in the directory /Status/File-System/Contents. Enter the following commands in the console:
  `cd /Status/File-System/Contentsdel controller_rootcert`
- ☐ Then access the directory /Setup/Certificates/SCEP-Client and execute the command Reinit:
  `cd /Setup/Certificates/SCEP-Clientdo Reinit`

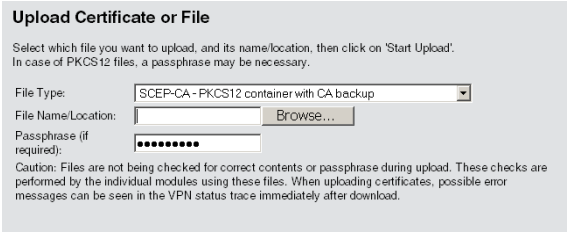


Figure 34: Uploading a certificate backup onto the device

5.5.6 Saving and Restoring more files of the SCEP-CA

To fully restore the SCEP-CA, the information on the device certificates issued by the SCEP-CA for the individual Access Points is also important.

Note: If you back up only the root certificates, there is no possibility to call up the issued device certificates.

For this reason, back up the following files in addition to the certificates:
- ☐ SCEP certificate list: List of all certificates ever issued by the SCEP-CA.
- ☐ SCEP serial numbers: Contains the serial number for the next certificate.
- ☐ Select File management > Download certificate or file.
- ☐ Then, as file type, select the two entries listed above one after the other and confirm with Start download:

Figure 35: Backing up further files of the SCEP-CA

- ☐ To upload these files to the device, go to the start page of WEBconfig and select the command Upload certificate or file.
- ☐ Then, as file type, select the two entries listed above one after the other, enter each file name and the storage location and confirm with Start upload:

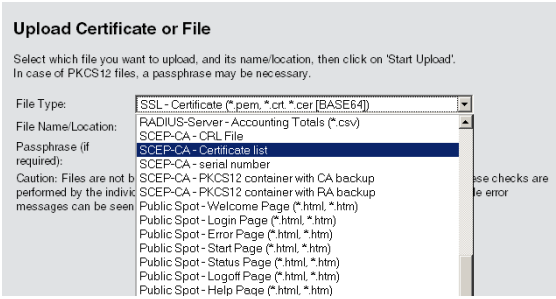


Figure 36: Restoring further files of the SCEP-CA

Note: After a new certificate list has been loaded, the device removes expired certificates and generates a new CRL. Furthermore, the CA reinitializes itself automatically if certificates and keys have been successfully extracted after loading the certificate backup.

5.6 Interference Detection in the Frequency Range (Spectral Scan)

In addition to connecting computers to the Internet, professional users are increasingly using wireless local area networks (WLAN) for business-critical applications. Examples include accessing of patient files, online monitoring of production facilities, and the transmission of video and audio data (ideally without any time lags). The reliability and performance of WLAN systems are thus increasingly important.

The rising significance and usage of WLAN for data transmission is resulting in more and more scenarios where the equipment and systems of various users are crowding the WLAN frequency ranges. These may include, for example, microwave ovens, cordless telephones, Bluetooth devices and video transmitters, with their signals occurring on a continual or intermittent basis. The simultaneous usage of a frequency band or frequency range gives rise to interference that can disrupt or negatively impact the reliability and performance of a WLAN. This type of interference can result in lost data packets or connection failure. If the interference is too strong, the complete failure of the WLAN may result.

It is therefore becoming increasingly important to use targeted analysis to check the frequency ranges. These checks should identify the interference or other interference factors, and introduce countermeasures as required. It can also be used to ensure that the WLAN is working properly and operating interference free.

Targeted analysis can also clarify or identify the following:

- Proper, fault-free operation of the WLAN
- Existence of interference or noise
- Display or identify the bands with interference
- Strength of the interference signal
- Regularity or frequency of the interference signal
- Type, and possibly source, of the interference signal

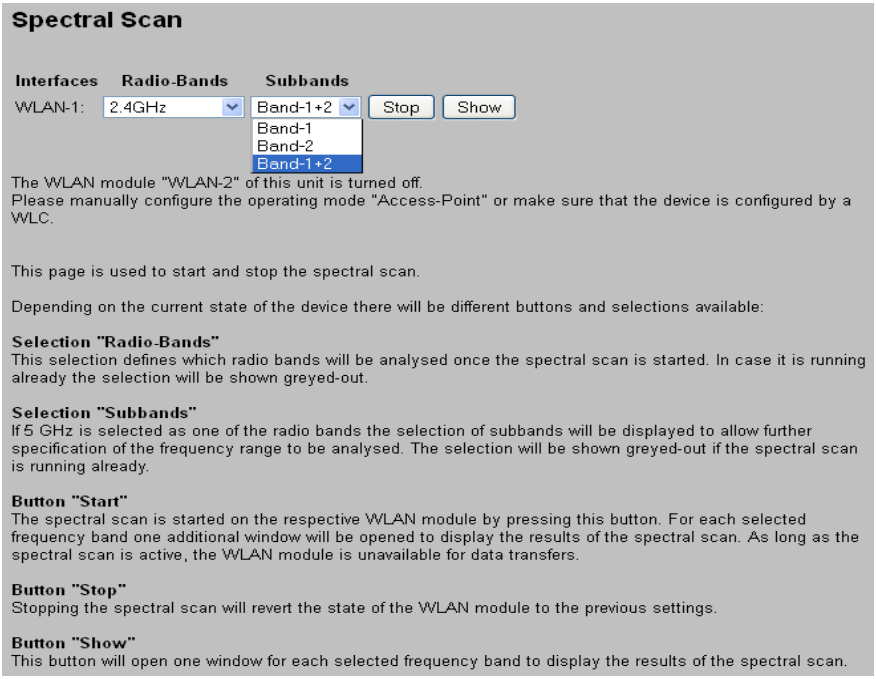
The WLAN-related frequency ranges are subject to spectral analysis. Results are displayed graphically, i.e. in the form of real-time diagrams or real-time overviews of frequencies and interference. However, graphical analyses of a spectral range are open to some freedom of interpretation. Therefore, the following scenario should be fairly commonplace: You ascertain that the frequency currently being used is being subjected to interference that is continual and of constant signal strength. However, you are not able to ascertain unequivocally which room or building the signal is coming from, nor the type of equipment which is transmitting the interfering signal.

5.6.1 Functions of the Software Module

The "Spectral Scan" software module enables you to run a spectral analysis directly on the access point. There is no need to purchase any additional software or hardware as the integrated functionality can be used to analyze the frequency ranges and bands in question. This gives you a graphical overview of the frequency response characteristics within your WLAN at all times, so that you can detect interference and safeguard against it.

5.6.2 Starting a Spectral Scan

Clicking on the menu option `Extras:Spectral scan` in WEBconfig opens the window shown below:



Note: If the WLAN module is disabled (`Setup:Interfaces:WLAN:Operational`), a message is displayed and the spectral scan cannot be started. Configure the access point for "Base station" operation or ensure that a WLAN controller configures the access point.

The following entries, buttons and selection menus are available here:

- "Interfaces": Shows the selected WLAN module for analysis.
- "Radio bands": Use this selection menu to set which frequency band(s) you wish to analyze. The relevant field is grayed out once the spectral scan has started on this module.
- "Subbands": This selection menu is only enabled if '5GHz' or '2.4GHz/5Ghz' is selected in "Radio bands". You are then able to specify which sub-bands of the 5GHz band are included in the analysis.

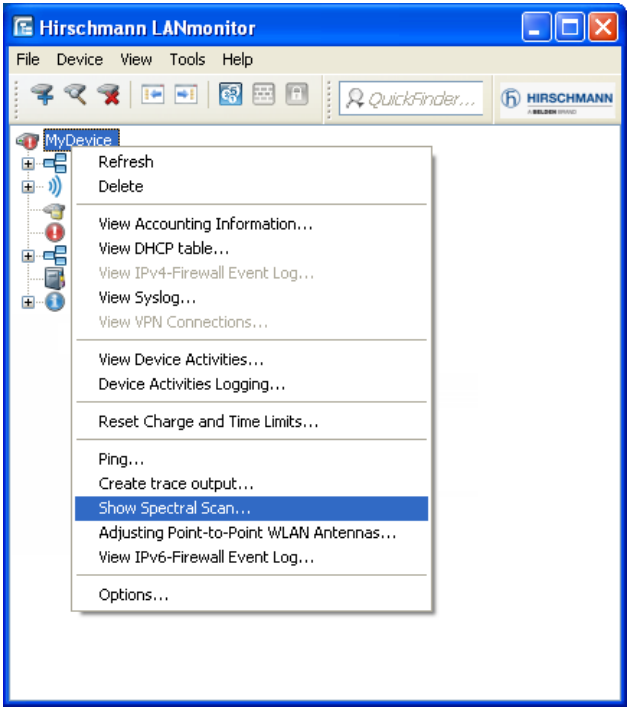
- "Start": Clicking this button starts the spectral scan on the relevant WLAN module. A separate window opens for each of the selected frequency bands.
- "Stop": This buttons ends the analysis. The WLAN module then returns to the previous mode and is available again with its usual functionality.

  Note: This button is only shown once the module has been started.

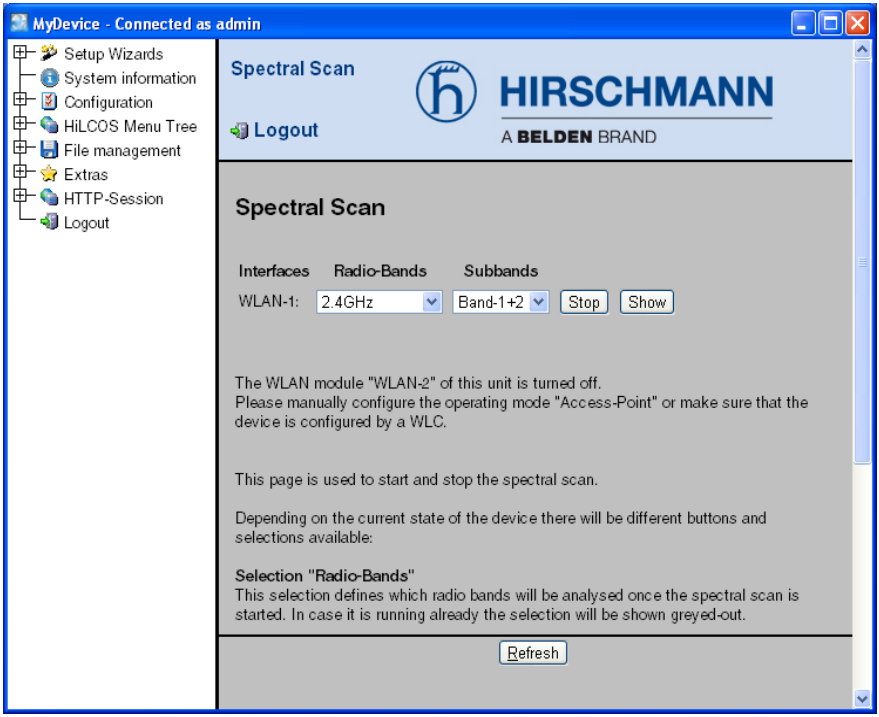
- "Show": Once the spectral scan has started, click this button to open a window for each selected frequency band. Click the button repeatedly to open multiple windows.

Note: During the analysis, the WLAN module being analyzed does not send any data or transmit any SSID.

The spectral scan can also be started from the LANmonitor. To do this, right-click the relevant device in the list and select "Show spectral scan" in the context dialog.



The LANmonitor browser window opens showing you the same entries, buttons and selection menus as those in WEBconfig.



5.6.3 Spectral Scan Analysis Window

Note: The spectral scan is displayed in a browser application. For this to work properly, your browser must support the latest version of WebSockets, and the HTML5 element `<canvas>`. The browser in LANmonitor meets all of these requirements.

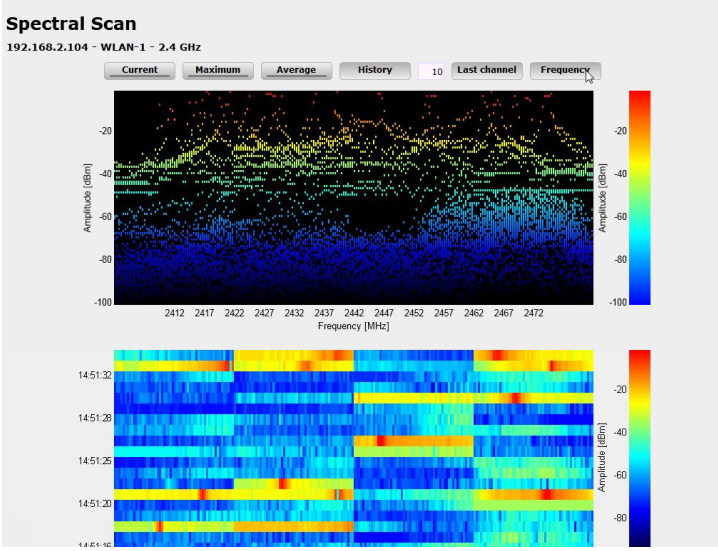
In the separate analysis window of the spectral scan, there are different ways to show the frequencies and frequency ranges together with the potential interference. The following buttons are available at the top of the window:

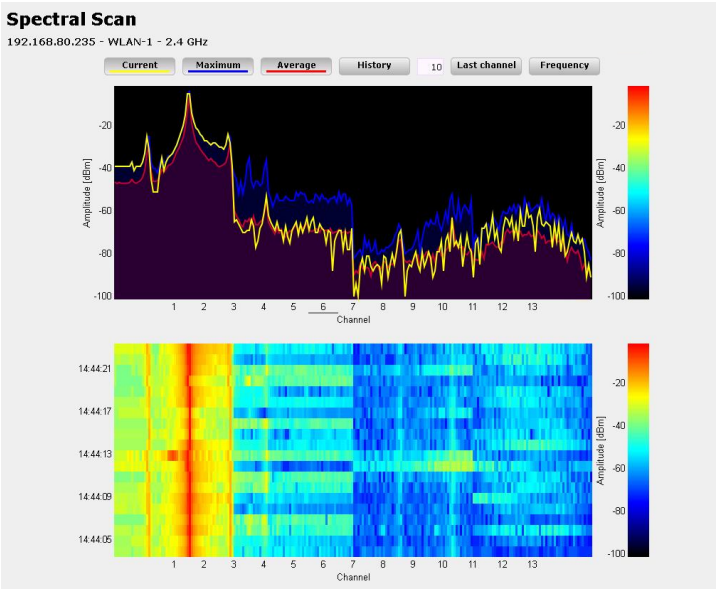
- "Current": Shows or hides the curve of the values being measured.
- "Maximum": Shows or hides the maximum values of the ongoing spectrum scan in relation to the currently set history range.
- "Average": Shows or hides the average values of the ongoing spectral scan in relation to the currently set history range.
- "History": Shows or hides the values last measured.
- "Number of history values": Determines the number of the most recent results to be displayed. You are able to show at least the last 5 and at most the last 50 measuring points for every frequency.
- "Last channel": Shows or hides the channel last used.
- "Frequency": Switches the display on the X-axis between WLAN channel and frequency.

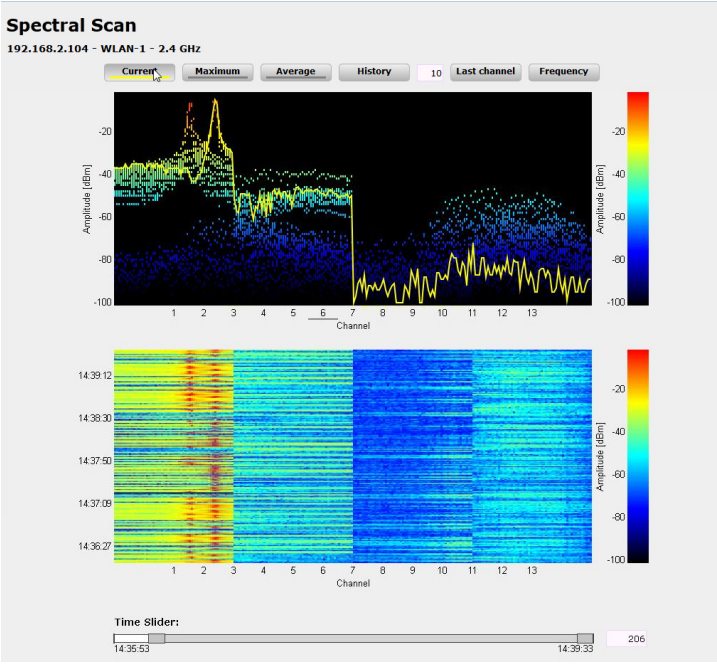
The window contains two graphical views showing the readings in a different manner. The top diagram shows the signal strength in dBm on the Y-axis, and either the WLAN channel or the relevant frequency on the X-axis. The lower diagram contains the analysis progression over time in the form of a waterfall diagram, with the Y-axis showing the time and the X-axis again showing the WLAN channel or the relevant frequency. These view formats depict both continuous and occasional interference on the frequencies, so helping you to take appropriate action to improve the connectivity (e.g. by changing the channel or identifying and eliminating the interference source). For example, certain interference sources such as microwave devices, DECT telephones (working in the 2.4GHz frequency range) and audio-video transmitters exhibit very typical transmit patterns that occur prominently in both diagrams.

On the lower border of the window is a slider denoted "Time slider". This enables you to extend or limit the time period analyzed in the waterfall diagram. Alternatively, you can use the input box to the right of the slider to select how many readings you would like to display in the waterfall diagram. The web application can display up to 300 readings in the waterfall diagram using the time slider. The readings from a maximum of 24 hours can be cached.

Below are some example analysis results showing graphically other settings in a different way:




Spectral Scan
192.168.80.235 - WLAN-1 - 2.4 GHz
Current
Maximum
Average
History
10
Last channel
Frequency
Amplitude [dBm]
-20
-40
-60
-80
-100
1 2 3 4 5 6 7 8 9 10 11 12 13
Channel
14:44:21
14:44:17
14:44:13
14:44:09
14:44:05


Spectral Scan
192.168.2.104 - WLAN-1 - 2.4 GHz
Current
Maximum
Average
History
10
Last channel
Frequency
Amplitude [dBm]
-20
-40
-60
-80
-100
1 2 3 4 5 6 7 8 9 10 11 12 13
Channel
14:39:12
14:38:30
14:37:50
14:37:09
14:36:27
Time Slider:
14:35:53
14:39:33
206

5.7 Extended WLC Functions

5.7.1 Automatic Radio-Field Optimization with Hirschmann WLAN-Controllers

With the selection of the channel from the channel list, you define the part of the frequency band that an Access Point uses for its logical WLANs. All WLAN Clients that connect to an Access Point must use the same channel on the same frequency band. In the 2.4-GHz band, channels 1 to 13 are available (depending on the country), and in the 5-GHz band, channels 36 to 64 are available. At a given point in time, only one Access Point transmits its data on one channel. For a WLAN to reach maximum bandwidth within the radio range of another Access Point, use a separate channel for each Access Point. Otherwise the WLANs share the channel's bandwidth.

Note: With a completely open channel list, the Access Points might automatically select channels that overlap in some areas, resulting in a loss in signal quality. Similarly, the Access Points might select channels which the WLAN Clients cannot use due to the country settings. To direct Access Points towards certain channels, activate e.g. the non-overlapping channels 1, 6, 11 in the channel list.

In larger installations, selecting a suitable channel for every Access Point can be difficult. Automatic radio-field optimization is a method offered by Hirschmann WLAN-Controllers where the optimum channels for the Access Points in the 2.4-GHz band are automatically set.
WEBconfig: Setup > WLAN-Management > Start-automatic-radio-field-optimization

Note: Optionally start the optimization for an individual Access Point by entering the MAC address as parameter for the action.

LANmonitor: Right-click an active Access Point and select "Start automatic RF optimization" from the context menu.

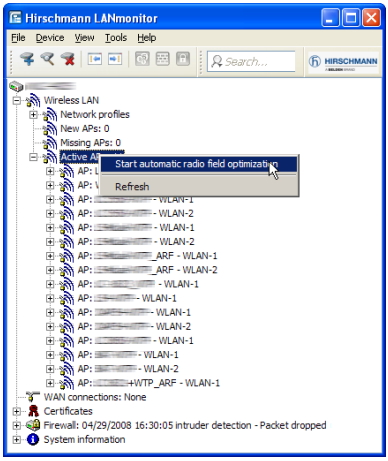


Figure 37: Setting automatic radio-field optimization

Optimization is then carried out in the following steps:

- ☐ The WLAN-Controller deletes the AP channel list of all Access Points in the 2.4-GHz range. As the channel list for the Access Points is then empty, the WLAN-Controller transmits the channel list of its profile by means of a configuration update.
- ☐ The WLAN-Controller switches off all radio modules operating in the 2.4-GHz range.
- ☐ The WLAN-Controller switches on the Access Point one after the other. During this process, the WLAN-Controller observes the sequence in which the Access Points registered.

- ☐ Automatic calibration: After the Access Point is switched on, it selects the optimum channel from the channel list. To determine the optimum channel, the Access Point carries out an interference measurement that considers the signal strengths and channels of all Access Points from the profile channel list in the WLAN-Controller. When the profile channel list is empty, the Access Point selects from all free channels.
- ☐ The Access Point transmits the selected channel to the WLAN-Controller, which saves it in the AP channel list. Therefore the Access Point receives the same channel the next time a connection is established. The AP channel list thus has a higher weighting than the profile channel list.

Note: If an Access Point is equipped with multiple WLAN modules, the Access Point will repeat this process for every WLAN module.

5.7.2 Central Firmware and Script Management

With Hirschmann WLAN-Controller, you can configure multiple Access Points consistently and conveniently from one location. With central firmware and script management, firmware and script uploads can be started automatically on all managed WLAN devices.
For this purpose, store the firmware and script files on a web server (firmware as *.UPX files, scripts as *.LCS files). Once daily or when prompted by a user, the WLAN-Controller compares the available files with the versions in the devices. Alternatively, this procedure can be handled by a cron job . e.g. overnight. The WLAN-Controller downloads files from the web server and uploads them into the corresponding Access Points if one of the following conditions applies:

- ☐ The server contains a newer version of the file.
- ☐ The Access Point runs with another version than the desired one.

With the configuration of firmware and script management, you control the distribution of the files. It is thus possible to limit the use of certain firmware versions e.g. to specific device types or MAC addresses.

The WLAN-Controller starts the update under 2 possible conditions:

- ☐ When a connection is established, the Access Point subsequently restarts automatically.
- ☐ When the Access Point is already connected, the device does not restart automatically. In this case start the Access Point manually via the menu action "/Setup/WLAN-Management/Central-Firmware-Management/Reboot-updated-APs" or via a timed cron job.

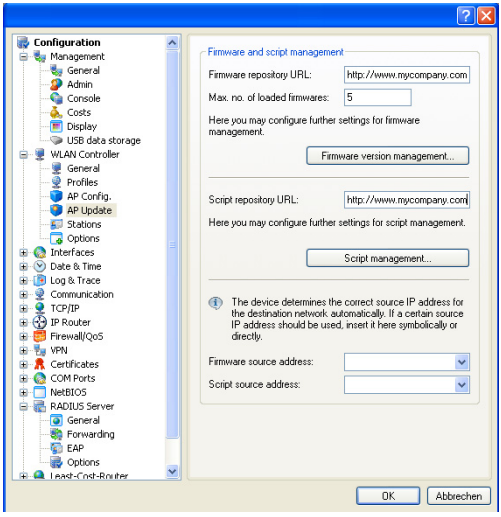


Figure 38: Configuring the firmware and script management

You will find the configuration parameters on the following paths:
LANconfig: WAN Controller > AP Update
WEBconfig: Setup > WLAN Management > Central Firmware Management

General Settings for the Firmware Management

☐ Firmware URL:
Path to the firmware-files directory.
- Possible values: URL in the form `Server/Directory` or `http://Server/Directory`
- Default: blank

☐ Simultaneously loaded FW
The number of firmware versions loaded simultaneously into the main memory of the WLAN-Controller.
- Possible values: 1 to 10
- Default: 5

Note: The WLAN-Controller downloads the firmware versions stored here just once from the server and then uses them for all suitable update processes.

☐ Firmware Sender IP Address
This is where you can configure an optional sender address that the device can use instead of the one automatically selected for the destination address.
Possible values:
- Name of a defined IP network.
- 'INT' for the IP address in the first network with the setting 'Intranet'.
- 'DMZ' for the IP address in the first network with the setting 'DMZ'.
- Name of a loopback address.
- Any other IP address.
- Blank (default):

Note: If the lists of IP networks or loopback addresses contains an entry named 'INT' or 'DMZ', the associated IP address of the IP network or the loopback address named 'INT' or 'DMZ' is used.

Firmware Management Table

Table with device type, MAC address and firmware version for the precise control of the firmware files in use.

☐ Device types
Here select the type of device that the firmware version specified here is to be used for.
- Possible values: Selection from the list of available device types.
- Default: All

- ☐ MAC address
  Here select the device (identified by its MAC address) that the firmware version specified in this entry is to be used for.
  - ▶ Possible values: Valid MAC address.
  - ▶ Default: Blank
- ☐ Version
  Firmware version that is to be used for the devices or device types specified in this entry.
  - ▶ Possible values: Firmware version in the form X.XX
  - ▶ Default: Blank

Load firmware in managed AP

On this page, you have the option of using remote access to manually update the firmware on the access points managed by the WLC. Select an access point based on its MAC address and select the appropriate firmware file. Next click on "Start upload" to load the firmware in the access point.

Note: Please note that this process disables the firmware management for the AP.

In order for the access point to use the loaded firmware, you must subsequently perform a restart. By enabling the setting "Restart AP after updating the firmware" you trigger an automatic restart as soon as the firmware upload is completed.

General Settings for the Script Management

☐ Script URL
Path to the script-files directory.
- Possible values: URL in the form `Server/Directory` or `http://Server/Directory`
- Default: Blank

☐ Script sender IP address
Here you can configure an optional sender address that the device can use instead of the one automatically selected for the destination address.
Possible values:
- Name of a defined IP network.
- 'INT' for the IP address in the first network with the setting 'Intranet'
- 'DMZ' for the IP address in the first network with the setting 'DMZ'
- Name of a loopback address
- Any other IP address.
  Default:
- Blank

Note: If the lists of IP networks or loopback addresses contains an entry named 'INT' or 'DMZ', the associated IP address of the IP network or the loopback address named 'INT' or 'DMZ' is used.

Script Management Table

The table contains the script file names and the assigned WLAN profiles. An Access Point in the operating mode "managed" is configured via WLAN profiles. With a script, you can also set those detailed parameters in managed devices that exceed the pre-defined parameters in a WLAN profile. The assignment is also implemented via the WLAN profiles to ensure that Access Points with the same WLC configuration also use the same script.

As only one script file can be defined for each WLAN profile, versioning is not possible. When a script is assigned to an Access Point, however, the WLAN-Controller saves an MD5 check sum of the script file. This checksum allows the WLAN-Controller to determine whether the script file has to be transmitted again if a new or altered script file has the same file name.

- ☐ Script file name
  Name of the script file to be used.
  - ▶ Possible values: File name in the form *.lcs
  - ▶ Default: blank
- ☐ WLAN profile
  Select here for which WLAN profile the script file specified in this entry is to be used.
  - ▶ Possible values: Selection from the list of defined WLAN profiles.
  - ▶ Default: Blank

Internal Script Memory (Script Management without HTTP Server)

Unlike firmware files, scripts often have small data volumes. The WLAN-Controller's internal script memory can hold 3 scripts of a maximum size of 64 kB each. If this storage capacity is sufficient for your scripts, you do not need to set up an HTTP server for this purpose.
Simply load the script files using WEBconfig to one of the 3 storage locations. After the upload, update the list of available scripts using the action Setup/WLAN Management/Central Firmware Management/ Update Firmware and Script Information.
From the script management table, reference these internal scripts using the relevant names (WLC_Script_1.lcs, WLC_Script_2.lcs or WLC_Script_3.lcs).

Note: Please observe the case sensitivity when entering script names.

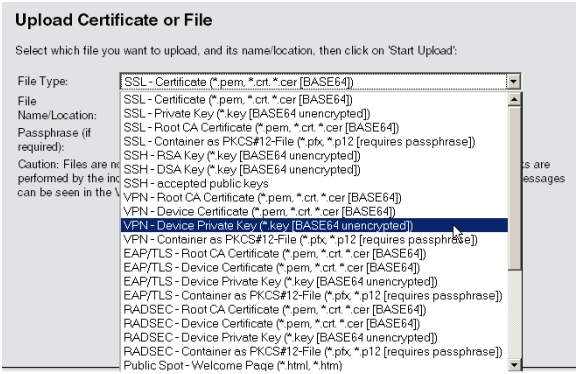


Figure 39: Uploading script files via WEBconfig

5.7.3 Checking WLAN Clients with RADIUS (MAC Filter)

When using RADIUS to authenticate the WLAN Clients, you can use the internal user table of the Hirschmann WLAN-Controller as an alternative to an external RADIUS server. The user table only grants specific WLAN Clients access to the WLAN, based on their MAC address.
Enter the approved MAC addresses in LANconfig into the RADIUS database in the configuration section 'RADIUS servers' on the 'General' tab. Enter the MAC address as 'Name / MAC address' and also as 'Password' and allow all protocols for authentication (no restrictions).

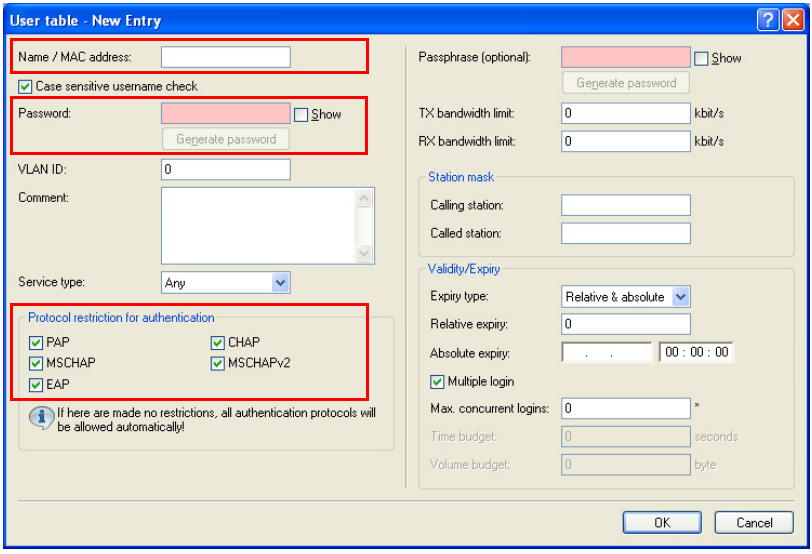


Figure 40: Creating a new user account

Alternatively, enter the approved MAC addresses in WEBconfig under HiLCOS menu tree > Setup > RADIUS > Server > Users.

Note: As 'Name / MAC address' and as 'Password', enter the MAC address in the form 'AABBCC-DDEEFF'.

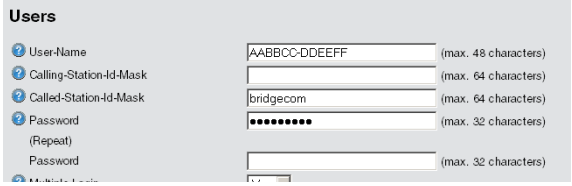


Figure 41: Creating a new user account using WEBconfig

5.7.4 Separate RADIUS Server for Each SSID

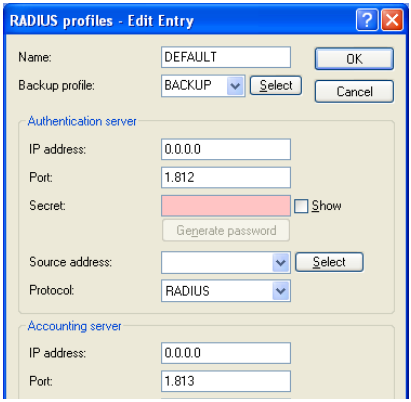
If you operate RADIUS for the central administration of accounts and credentials in your wireless network, then the access point forwards requests for the authorization and accounting to the RADIUS server by default. If you are using a WLAN controller for access point management, then the controller can forward RADIUS requests from all of these access points to the RADIUS server.

In some cases, the operator of access points or WLAN controllers may wish to use a different RADIUS server for each logical wireless network (SSID). This may be the case, for example, when multiple customers share the same technical WLAN infrastructure but use their own authentication systems (e.g. with Wireless as a Service – WaaS).

In these cases, you have the option to choose a separate RADIUS profile for each logical WLAN (i.e. each SSID). The RADIUS profile contains all of the necessary information to use the appropriate RADIUS server, including the optional backup solution.

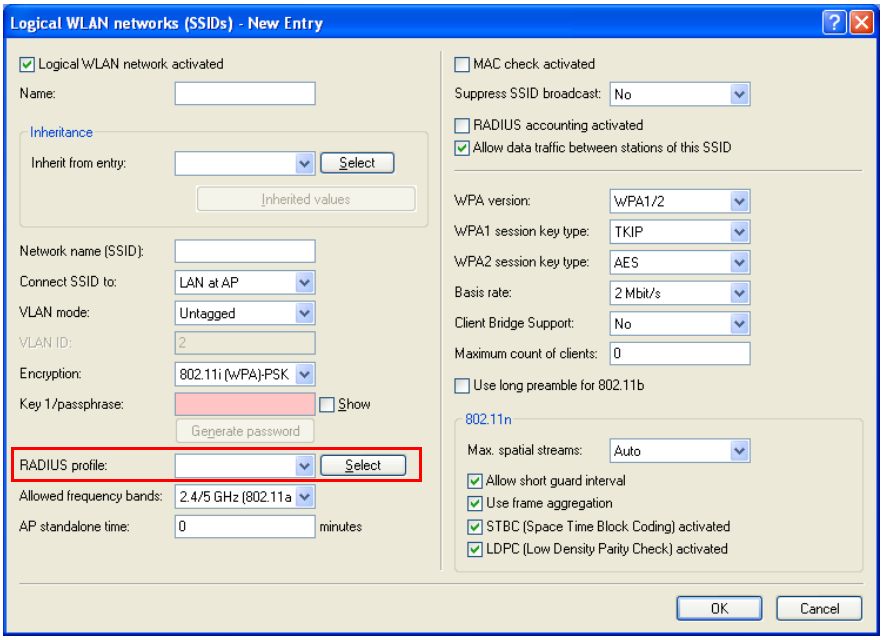
Setting up the RADIUS Profiles

In LANconfig, the settings for the RADIUS profiles in the WLAN controller are to be found under `WLAN Controller:Profiles:RADIUS profiles`.



Selecting a RADIUS Profile for a Logical WLAN

In LANconfig, selecting the RADIUS profile for a logical WLAN in the WLAN Controller is done with the menu item `WLAN Controller:Profiles:Logical WLAN networks`.



5.7.5 IP-dependent auto configuration of APs

The easiest way to manage all of the access points that you add to a managed network is with a flat hierarchy. However, in the largest installations with hundreds of access points across several locations, this type of organization quickly becomes confusing and creates a high level of administrative effort. By setting up "Assignment groups" you have the ability to simplify the management of distributed access points by automatically allowing the WLC to configure new APs based on the associated IP address. Manual assignment of a network configuration and a WLAN profile by an administrator is no longer required.

The following procedure is used to allocate an assignment group to a new remote access point registering with a central WLC: After the AP is installed at the new location (e.g. a company or branch network), it tries to establish a connection to the specified WLC and obtain a configuration via CAPWAP. The WLC recognizes the connection request and checks whether the access point table contains an appropriate profile (e.g., the default profile). If an appropriate profile is present, the WLC checks it for the following states:

- ☐ The AP profile has a group but not a WLAN profile. In this case, the WLC assigns to the AP the WLAN and IP-parameter profile that are defined in the assignment group.
- ☐ The AP profile has a group and a WLAN profile. In this case, the WLC ignores the group configuration and assigns to the AP the settings that are defined in the AP profile.
- ☐ The AP profile has a WLAN profile but not a group. The behavior is the same as point (2).
- ☐ The AP profile has neither a group nor a WLAN profile. In this case, the WLC issues a warning which informs the administrator of the misconfiguration.

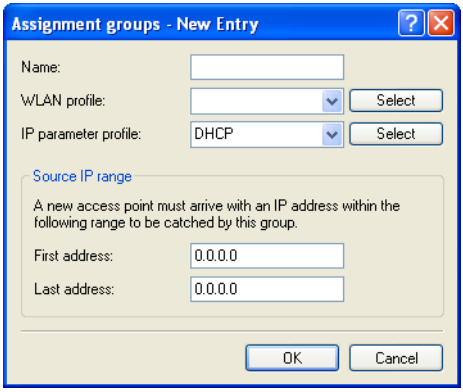
If there is no suitable access point profile (e.g., the default profile), no automatic configuration of the AP occurs.

Setting up assignment groups for IP-dependent configuration

The following tutorial shows you how to use an assignment group to enhance a WLAN controller's default AP configuration. The assignment group enables the WLC to provide different configurations to new remote APs, depending on the address range that they occupy.

☐ Open the configuration dialog for your device and select `WLAN controller : AP configuration : Assignment groups`

☐ Click on "Add" to create a new group.



☐ Enter a unique "Name" for the assignment group, for example, `Berlin branch`.

☐ Select the "WLAN profile" that the WLC should assign to a new AP.

☐ Enter the "IP parameter profile" if the AP should receive a manual network configuration. Otherwise, leave the value as "DHCP", whereby the AP automatically gets a network configuration from the DHCP server.

The DHCP server must be configured to do this.

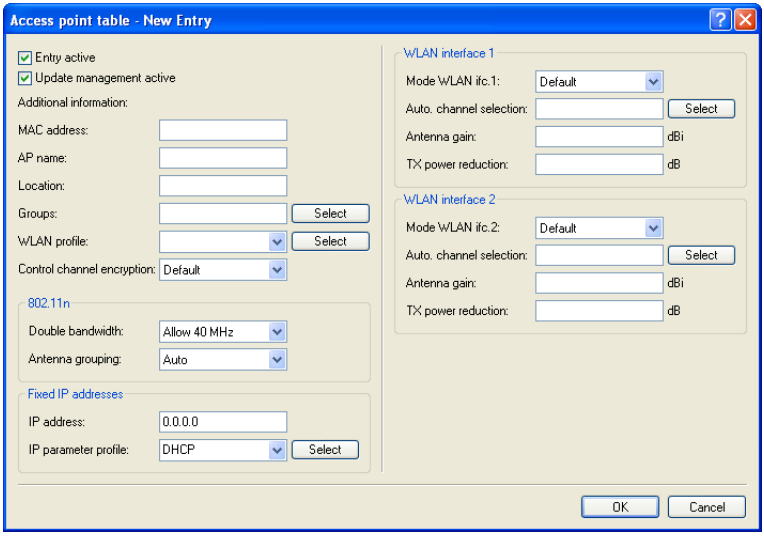
☐ Enter the start and end of the "Source IP range" relevant to the assignment group.

A new access point must register at the WLC with an IP address from this range in order to obtain the configuration for this group.

☐ Save the entry with "OK".

☐ Navigate to the dialog with `WLAN controller : AP configuration : Access point table`.

☐ Click on "Default" to create a new default AP profile. If this type of profile already exists, the select it ("MAC address": "FFFFFFFFFFFF") and click on "Edit".



☐ Under "Groups" select the previously created assignment group(s).

☐ Delete all entries in the input field "WLAN profile".

☐ Close all dialog windows with "OK" and save the configuration to your device.

Once you have defined the corresponding assignment groups and the WLC has assigned these to new APs, the HiLCOS console gives you the option of calling up additional information on the existing categorization, see the Overview of CAPWAP parameters inside the CLI-Reference.

5.7.6 Dynamic VLAN Assignment

In larger WLAN structures, it is often advisable to assign a specific network to the individual WLAN Clients. As long as the WLAN Clients are always within the coverage area of the same Access Point, you can realize this assignment via the SSID in connection with a particular IP network. If the WLAN Clients often change their position, however, and log into different Access Points, they will be in a different IP network, depending on the configuration.
Use dynamically assigned VLANs to direct the WLAN Clients from different WLAN networks to a specific IP network. Unlike it is the case with statically configured VLAN IDs for a specific SSID, the RADIUS server transmits the VLAN ID directly to the WLAN Client.
Example:

- ☐ The WLAN Clients of the employees use an Access Point to log into the WPA-secured wireless network with the SSID 'INTERNAL'. During registration, the RADIUS requests of the WLAN Clients are directed to the Access Point. If the corresponding WLAN interface is in the operating mode 'managed', the RADIUS requests are automatically forwarded to the WLAN-Controller. This in turn forwards the requests to the configured RADIUS server. The RADIUS server checks the access rights of the WLAN Clients. It also transmits, e.g. based on the MAC address, a certain VLAN ID for the respective department. The WLAN Client from Marketing, for example, will receive the VLAN ID '10', and the WLAN Client from Development the VLAN ID '20'. If no VLAN ID is defined for the user, the device transmits the primary VLAN ID of the SSID.
- ☐ The WLAN Clients of the guests use the same Access Point to log into the unsecured wireless network with the SSID 'PUBLIC'. This SSID is statically linked to the VLAN ID '99' and thus directs the guests into a specific network. You can optionally use the static and dynamic VLAN assignment in parallel.

Note: The assignment of the VLAN ID by the RADIUS server can alternatively be controlled by other criteria, such as the combination of user name and password. Thus the RADIUS server will, for example, assign a specific VLAN ID to the unknown MAC addresses of a company's visitors. This VLAN for guest access will, e.g., grant access to the Internet only, but no access to any other network resources.

Note: As an alternative to an external RADIUS server, the internal RADIUS server or the station table in the Hirschmann WLAN-Controller can transmit a VLAN ID to the WLAN Clients.

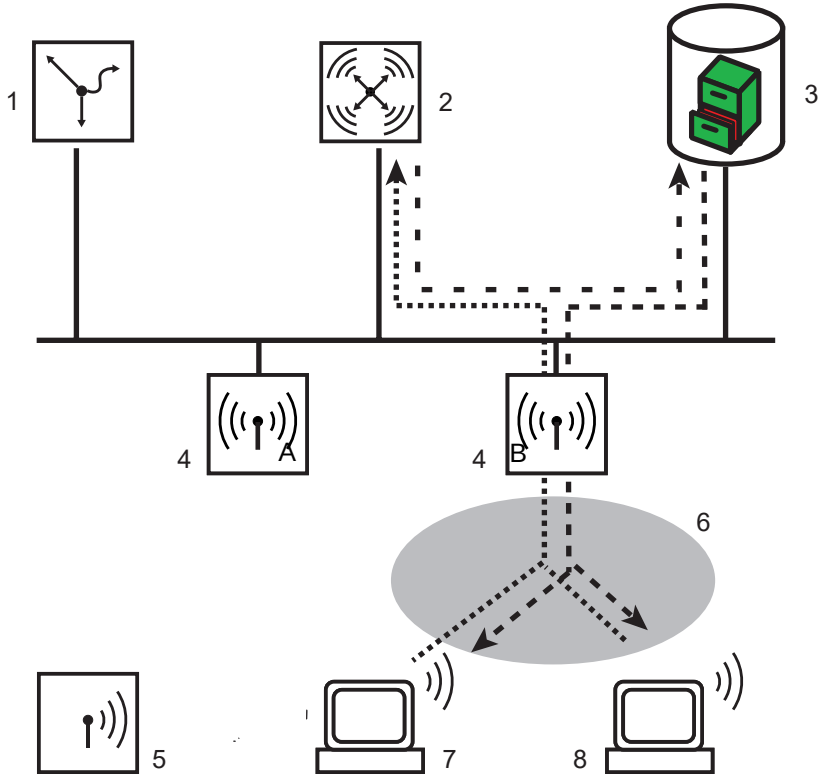


Figure 42: Dynamic VLAN assignment
1: Hirschmann VPN router
2: WLAN Controller
3: RADIUS server
4: Access Point
5: WLAN Clients
6: SSID 'INTERNAL'
7: VLAN-ID '10'
8: VLAN-ID '20'

☐ Activate VLAN tagging for the WLAN-Controller. This is done in the physical parameters of the profile by entering a value greater than '0' as management VLAN ID.
☐ For authentication via 802.1x, go to the encryption settings for the profile's

logical WLAN network and choose a setting that triggers an authentication request.

☐ To check the MAC addresses, activate the MAC check for the profile's logical WLAN network.

Note: For the management of WLAN modules with a WLAN-Controller, a RADIUS server is required both for the authentication via 802.1x and for the MAC-address checks. The WLAN-Controller automatically defines itself as RADIUS server in the Access Points it is managing. The Access Points send all incoming RADIUS requests to the WLAN-Controller, which either processes the requests itself or forwards it to an external RADIUS server.

Note: Further information about RADIUS is available in the documentation for your RADIUS server.

Note: Further information about RADIUS is available in the documentation for your RADIUS server.

5.7.7 Load Balancing between the WLAN-Controllers

If multiple WLAN-Controllers are available in a network, the WLAN-Controllers automatically distribute the Access Points evenly among each other.

At the beginning of the communication, the Access Point sends a "Discovery Request Message" to identify the available WLAN-Controllers.

- ☐ If the Access Point gets responses from primary and secondary WLAN-Controllers, it prefers primary controllers.
- ☐ From the available WLAN-Controllers, the Access Point selects the one with the lowest load. This is the WLAN-Controller with the lowest ratio of managed Access Points to maximum possible Access Points.
- ☐ In case of two or more equally utilized WLAN-Controllers, the Access Point selects the WLAN-Controller with the fastest response time.

So by activating several WLAN-Controllers via automatic assignment of configurations, for example, all WLAN-Controllers are equally filled with configurations for a proportion of the Access Points.

5.7.8 WLAN Layer-3 Tunneling

The CAPWAP standard for centralized WLAN management offers 2 different transmission channels:

- ☐ The obligatory control channel transfers management data between the managed Access Point and the WLAN Controller.
- ☐ The optional data channel transfers the payload data from the respective WLAN networks (SSID) between the managed Access Point and the WLAN Controller.

The optional use of the data channel between the managed Access Point and the WLAN Controller determines the path of the payload data:

☐ If you deactivate the data channel, the Access Point forwards the payload data directly into the LAN. In this case you control the assignment of WLAN Clients to specific LAN segments e.g. via the assignment of VLAN IDs. The advantage of this application is, above all, the low load placed on the controller and the entire network. The Access Point transmits only the management data via the CAPWAP tunnel, the payload data is transmitted over the shortest path.

☐ If you activate the data channel, the Access Point also transmits the payload data to the central WLAN Controller. This approach has the following advantages:

- The Access Points optionally propagate networks that are exclusively available on the Controller, e.g. a central Internet access for a public spot.
- The WLANs (SSIDs) offered by the Access Points are also available separately, without the use of VLAN. Refraining from the use of VLAN reduces the effort for the configuration of other network components, such as switches, etc.
- The WLAN Clients logged into different IP networks at the Access Points are roaming to another Access Point with an uninterrupted IP connection. The controller subsequently manages the connection instead of the Access Point (layer-3 roaming).

With the use of the data channel, additional logical networks, referred to as overlay networks (displayed as dotted lines in the following illustration), are created on the basis of the existing physical network structure.

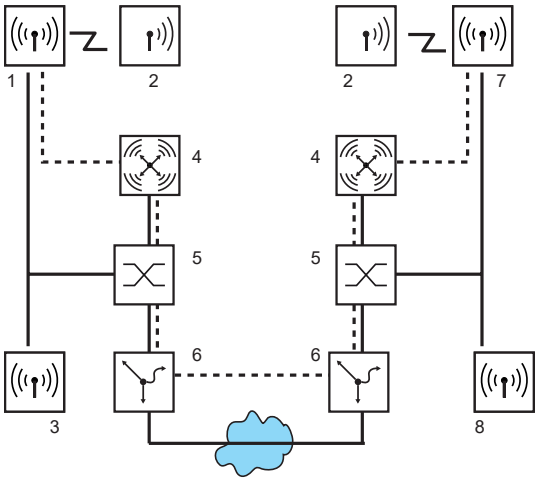


Figure 43: Overlay networks across several IP networks
1: IP network Plant 1 Production
2: WLAN Client
3: IP network Plant 1 Warehouse
4: WLAN Controller
5: Layer-3 switch
6: Gateway
7: IP network Plant 2 Production
8: IP network Plant 2 Warehouse

Via the data channel, you can even establish logical overlay networks across various WLAN Controllers.
Several WLCs that are supporting the same overlay network require separate broadcast domains. The multiple reception of the broadcast news otherwise leads to loops within a broadcast domain. As routers drop the broadcast news, two controllers in separate networks manage the same overlay networks, if necessary.
The Access Points use virtual WLC interfaces (WLC tunnels) to manage the data channels of the respective SSIDs between the Access Point and the WLAN Controller. Depending on the model, every WLAN Controller offers 16 to 32 WLC tunnels that are available for the configuration of the logical WLANs.

Note: The devices contain the virtual WLC interfaces in all dialogs for the selection of logical interfaces (LAN, WLAN, P2P). You can find this selection, e.g. in the port tables of the LAN and VLAN settings or in the definition of IP networks.

5.7.9 Switching off CAPWAP/SCEP in the WLC

In order to operate multiple WLAN controllers in a cluster, they must all have identical configurations. You can define a master controller by disabling CAPWAP/SCEP on all devices except for one. The other WLCs can be synchronized with the master controller's configuration.

`Setup : WLAN-Management : CAPWAP-enabled`

5.8 Application Examples

In the following sections you will find specific scenarios with step-by-step instructions for a range of standard scenarios using WLAN controllers.

5.8.1 "Overlay Network": Separating Networks for Access Points without VLAN

The separation of networks within a common, shared physical infrastructure is mostly based on the use of VLANs. This process requires that the switches used are VLAN-capable, however, and that all switches have the corresponding VLAN configurations. In this example, the administrator distributes the VLAN configuration across the entire network.
With a WLAN Controller, you can also separate the networks with a minimum use of VLANs. Through a CAPWAP data tunnel, the Access Points transmit the payload data of the connected WLAN Clients directly to the Controller, which assigns the data to the corresponding VLANs. Here the VLAN configuration is limited to the Controller and a single central switch. All other switches work without VLAN configuration in this example.

Note: This configuration helps you to reduce the VLAN to the core of the network structure (displayed in blue in the illustration.) In addition, only 3 of the switch ports used require a VLAN configuration.

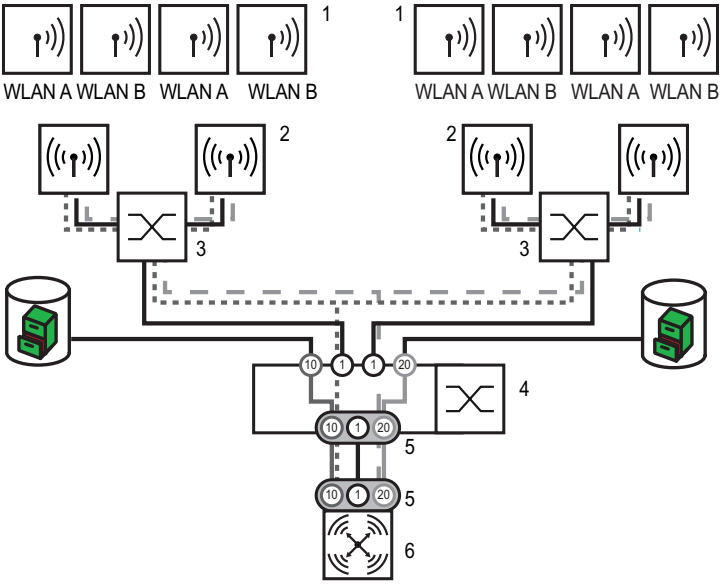


Figure 44: Application example overlay network

1: WLAN Client
2: Access Point
3: Unmanaged switch
4: VLAN switch
5: VLAN trunk, several VLAN IDs
6: WLAN Controller
Black line: No VLAN, in VLAN switches on VLAN-ID 1 displayed as 'native VLAN'
Dark gray dotted line: WCL tunnel group A
Dark gray line: VLAN group A
Light gray dashed line: WCL tunnel group B
Light gray line: VLAN group B
The numbers in circles indicate the VLAN ID

The illustration shows an application example with the following components:

- The network consists of 2 segments, each with its own switch (optionally without VLAN function).
- There are several Access Points in every segment, connected to the respective switch.
- Every Access Point offers 2 SSIDs for the WLAN Clients of different user groups, displayed in green and orange in the illustration.
- Every user group has access to their own server, protected from the access of other user groups. The servers can only be reached via the corresponding VLANs through the access ports configured on the switch.
- A WLAN Controller manages all Access Points in the network.
- A central, VLAN-capable switch connects the switches of the segments, the group-related servers and the WLAN Controller.

The aim of the configuration: A WLAN Client that logs into a specific SSID can access "its" server in every segment.

Note: The following description applies to a WLAN Controller with functional basic configuration. For instructions regarding the configuration of the VLAN switch, please refer to the relevant documentation.

Configuration of the WLAN Settings

- For each SSID, create an entry in the list of logical networks with a suitable name and the corresponding SSID. Connect this SSID to a WLC tunnel, the first SSID e.g. to 'WLC-TUNNEL-1' and the second one to 'WLC-TUNNEL-2'. Set the VLAN operating mode to 'tagged' in both cases, with the VLAN ID '10' for the first logical network and the VLAN ID '20' for the second logical network. In LANconfig, you can find these settings under Configuration/WLAN Controller/Profiles/Logical WLAN networks (SSIDs).

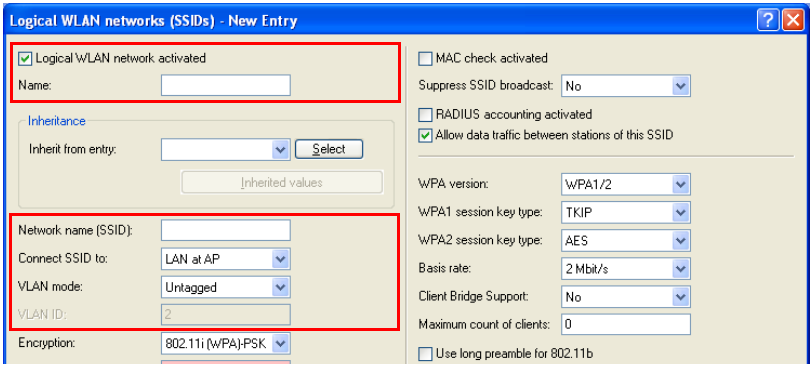


Figure 45: Logical WLAN networks for overlay networks

- Create an entry in the list of physical WLAN parameters. Select the suitable settings for your Access Points, e.g. for the country 'Europe', with channels 1, 6 and 11 in 802.11g/b/n and 802.11a/n mixed mode. For this profile of physical WLAN parameters, activate the option to switch on the VLAN module on the Access Points. Use 'untagged' as operating mode for the management VLAN in the Access Points. In LANconfig, you can find these settings under Configuration/WLAN Controller/Profiles/ Physical WLAN parameters.

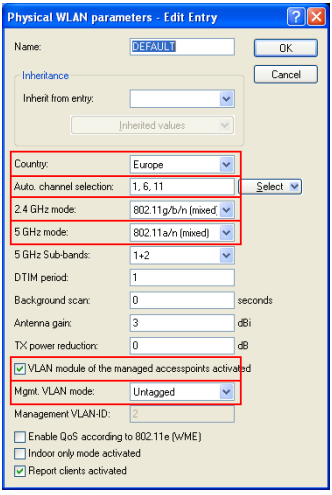


Figure 46: Physical WLAN parameters for overlay networks

- Create a WLAN profile with an appropriate name and select the previously created logical WLAN networks and the physical WLAN parameters for this WLAN profile. In LANconfig, you can find these settings under Configuration/WLAN Controller/Profiles/Physical WLAN profiles.

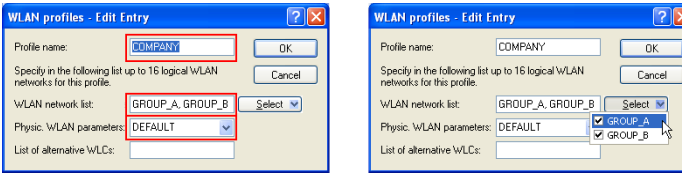


Figure 47: WLAN profiles for overlay networks

- For every managed Access Point, create an entry in the access-point table with an appropriate name and the corresponding MAC address. Select the previously created WLAN profile for this Access Point. In LANconfig, you can find these settings under Configuration/WLAN Controller/AP config/Access-point table.

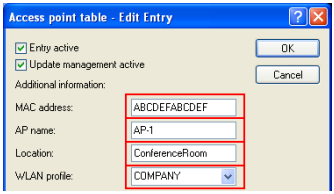


Figure 48: Access-point table for overlay networks

Configuration of the Interfaces on the WLC

- For every physical Ethernet port, select a separate logical LAN interface, e.g. 'LAN-1'. Make sure that further Ethernet ports use other LAN interfaces exclusively. In LANconfig, you can find these settings under Configuration/Interfaces/LAN/Ethernet ports.

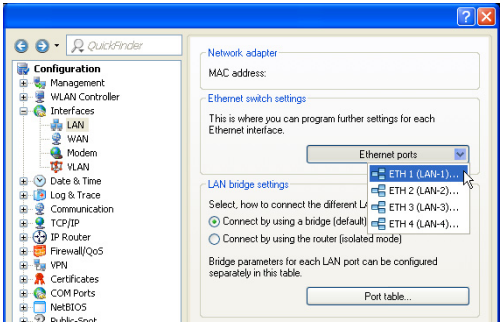


Figure 49: Ethernet settings for overlay networks

- Select the logical LAN interface 'LAN-1' and the WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' for the Bridge group 'BRG-1'. Make sure that the other LAN interfaces use other bridge groups exclusively. In LANconfig, you can find these settings under Configuration/Interfaces/LAN/Port table.

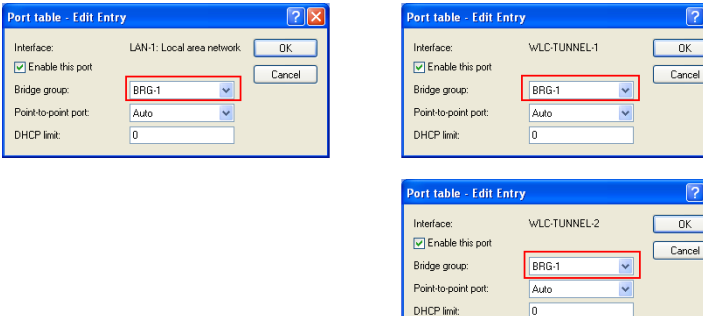


Figure 50: Port settings for overlay networks

Note: By default, the LAN interfaces and the WLC tunnel do not belong to any bridge group. If you assign the LAN interface 'LAN-1' and the two WLC tunnels 'WLC-tunnel-1' and 'WLC-tunnel-2' to the bridge group 'BRG-1', the device transmits all data packets between LAN-1 and the WLC tunnels via the bridge.

- The WLAN Controller can optionally function as DHCP server for the Access Points. To do this, enable the DHCP server for the 'INTRANET'. In LANconfig, you can find these settings under Configuration/IPv4/DHCPv4/DHCP networks.

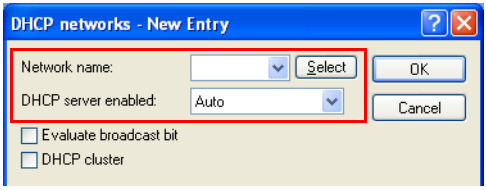


Figure 51: DHCP network for overlay networks

5.8.2 "Layer-3 Roaming"

The forwarding of payload data from the WLANs over WLC tunnels to the Controller permits roaming even beyond the boundaries of broadcast domains. In this application example, a layer-3 switch between the floors prevents the forwarding of broadcasts and thus separates the broadcast domains.
In this example, two user groups, A and B, each have access to their own WLAN (SSID). The Access Points on various floors of the building offer the two SSIDs 'GROUP_A' and 'GROUP_B'.

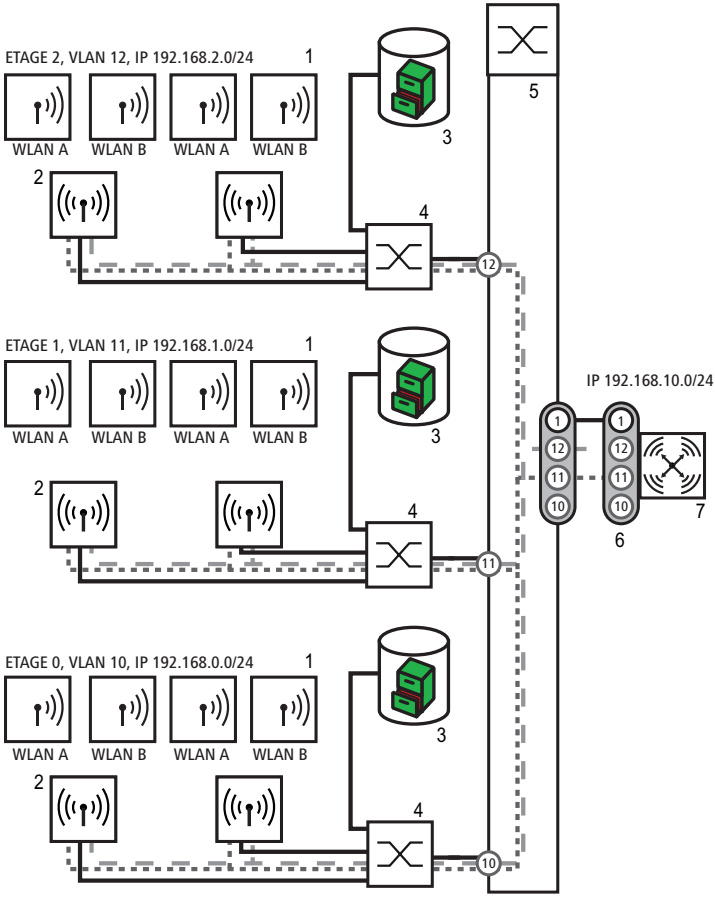


Figure 52: Application example for layer-3 roaming

1: WLAN Client
2: Access Point
3: DHCP Server
4: Unmanaged switch
5: VLAN switch
6: VLAN trunk, several VLAN IDs
7: WLAN Controller
Black line: No VLAN, in VLAN switches on VLAN-ID 1 displayed as 'native VLAN'

Dark gray dotted line: WCL tunnel group A
Dark gray line: VLAN group A
Light gray dashed line: WCL tunnel group B
Light gray line: VLAN group B
The numbers in circles indicate the VLAN ID

The illustration shows an application example with the following components:

- The network consists of three segments on separate floors of the building.
- A central layer-3 switch connects the segments and splits the network into three broadcast domains.
- Each segment uses its own IP address range and its own VLAN.
- In every segment, there is a local DHCP server, transmitting the following information to the Access Points:
  - IP address of the gateway
  - IP address of the DNS server
  - Domain suffix

  Note: The provision of this information enables the Access Points to contact the WLC controller in a different broadcast domain.

The aim of the configuration: A WLAN Client logging into a specific SSID shall have uninterrupted access to "its" WLAN when changing floors - regardless of the Access Point used and regardless of the segment in which it is currently located. As the segments in this example use different IP address ranges, this can only be achieved by managing the Access Points on layer 3 directly via the central WLAN Controller across the VLAN boundaries.

Note: The configuration corresponds to that of the example.

5.8.3 WLAN Controller with Public Spot

This scenario is based on the first scenario (overlay network) and adds specific settings for a user authentication. The forwarding of payload data from the WLANs over WLC tunnels to the controller permits a particularly simple configuration of public spots. Guests, for example, can use these in parallel to an internally used WLAN.
In this example, the employees of a company can access their own WLAN (SSID), guests can also access the Internet via a public spot. The Access Points in all areas of the building offer the two SSIDs 'COMPANY' and 'GUESTS'.

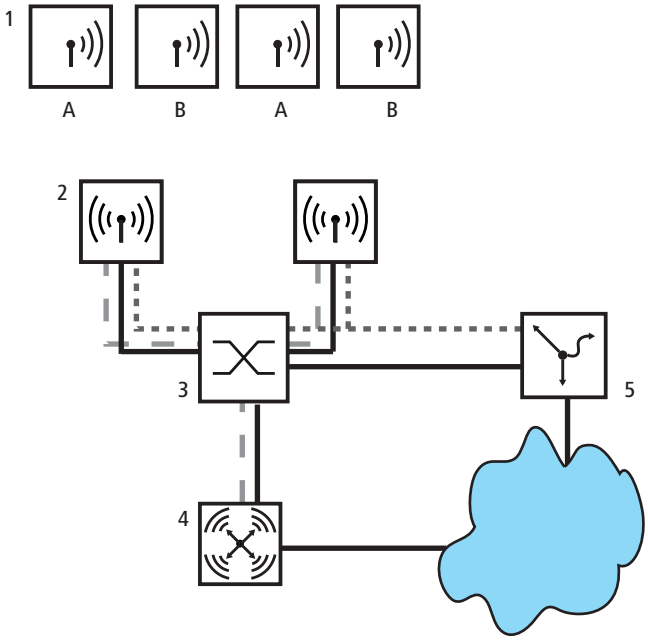


Figure 53: Application example WLAN Controller with public spot
1: WLAN Client
2: Access Point
3: Switch
4: WLAN Controller

5: Gateway
A: Guest access
B: Internal WLAN
Dark gray dotted line: WLC tunnel internal WLAN
Light gray dashed line: WLC tunnel public spot

The aim of the configuration: A WLAN Client logging into the internal SSID shall have access to all internal resources and to the Internet via the central gateway. The Access Points decouple the internal Clients' payload data locally and forward them directly into the LAN. The guests' WLAN Clients log into the public spot. The Access Points forward the guest clients' payload data over a WLC tunnel directly to the WLAN Controller, which provides Internet access via a separate WAN interface.

- Create one entry each for the internal WLAN and the guest WLAN in the list of logical networks, including an appropriate name and the corresponding SSID. Connect the SSID for internal use to the 'LAN on AP', the SSID for the guests to, e.g., 'WLC-TUNNEL-1'. In the SSID for the guest network, deactivate the encryption so that the guests' WLAN Clients can log into the public spot. Inhibit data traffic between the stations for this SSID (interstation traffic). In LANconfig, you can find this setting under Configuration/WLAN Controller/Profiles/Logical WLAN networks (SSIDs).

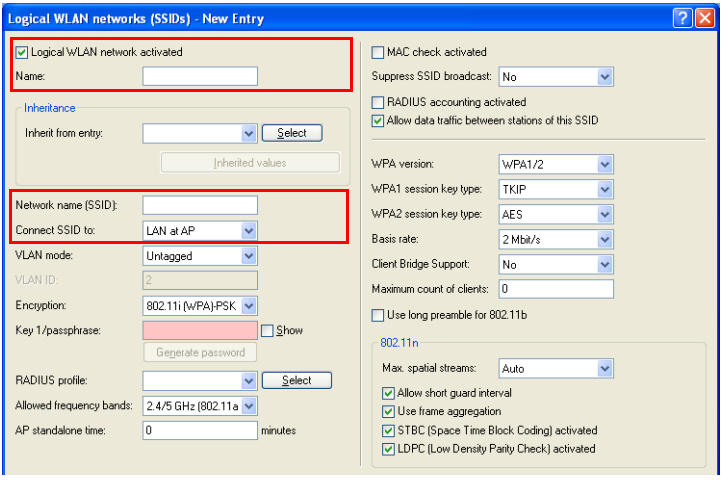


Figure 54: Logical WLAN networks for internal use

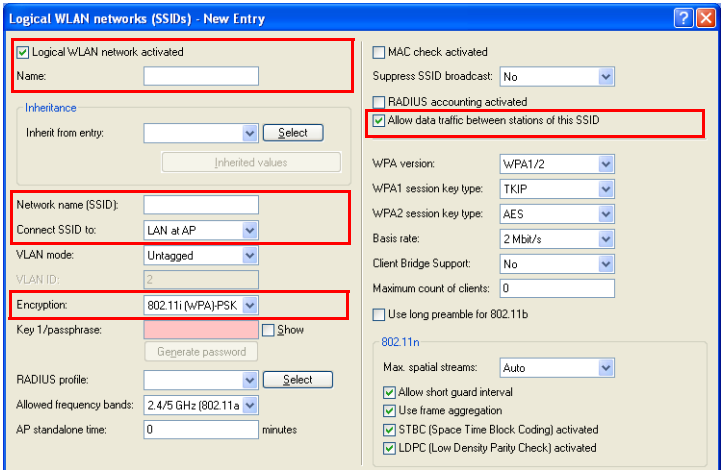


Figure 55: Logical WLAN networks for guest access

- Create an entry in the list of physical WLAN parameters with the suitable settings for your Access Points, e.g. for the country 'Europe', with the channels 1, 6 and 11 in 802.11g/b/n and 802.11a/n mixed mode. In LANconfig, you can find this setting under Configuration/WLAN Controller/Profiles/Physical WLAN parameters.

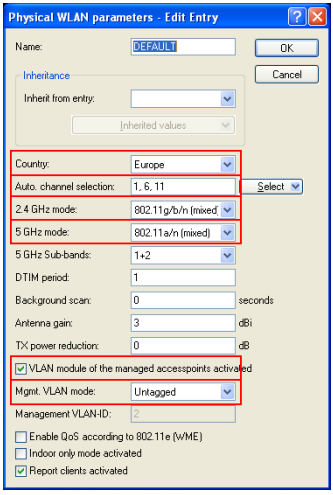


Figure 56: Physical WLAN parameters for public-spot APs

- Create a WLAN profile with an appropriate name and assign the previously created logical WLAN networks and the physical WLAN parameters to this WLAN profile. In LANconfig, you can find this setting under Configuration/WLAN Controller/Profiles/Physical WLAN profiles.

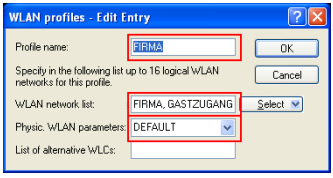


Figure 57: WLAN profiles for public-spot APs

- For every managed Access Point, create an entry in the access-point table with an appropriate name and the corresponding MAC address. Assign the previously created WLAN profile to this Access Point. In LANconfig, you can find this setting under Configuration/WLAN Controller/AP config/Access-point table.

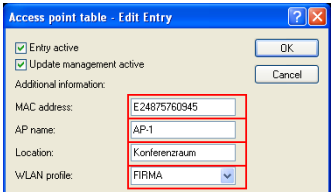


Figure 58: Access-point table for public-spot APs

- Assign a separate logical LAN interface to each physical Ethernet port, e.g. 'LAN-1'. Set the fourth Ethernet port to the logical LAN interface 'DSL-1'. The WLAN Controller uses this LAN interface later for the Internet access of the guest network. In LANconfig, you can find this setting under Configuration/Interfaces/LAN/Ethernet ports.

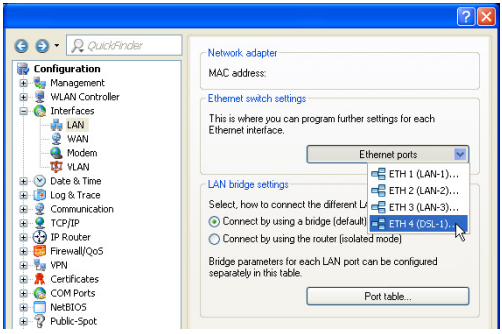


Figure 59: Ethernet settings for public-spot APs

- Check that the logical LAN interface 'WLC-tunnel-1' is not assigned to any bridge group. You thus ensure that the other LAN interfaces do not transmit any data to the public-spot network. In LANconfig, you can find this setting under Configuration/Interfaces/LAN/Port table.

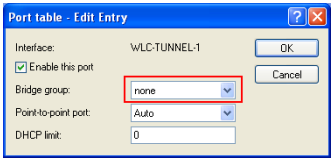


Figure 60: Port settings for public-spot APs

- For the guest Internet access, create an entry in the list of DSL remote terminals with the short hold time ‘9999’ and the pre-defined layer ‘DHCPOE’. The value ‘9999’ sets up a connection immediately without a time restriction. This example requires that a router with activated DHCP server provides the Internet access. In LANconfig, you can find this setting under Configuration/Communication/Remote terminals/Remote terminals (DSL)

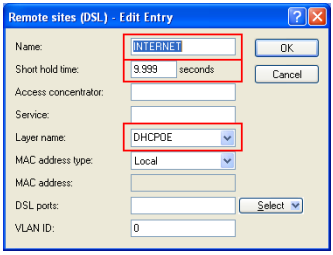


Figure 61: Remote terminal for Internet access

- For internal use, create the IP network 'INTRANET', e.g. with the IP address '192.168.1.100' and the interface tag '1', for guest use, create the IP network 'GUEST ACCESS', e.g. with the IP address '192.168.200.1' and the interface tag '2'. The virtual router in the WLAN Controller uses the interface tags to separate the routes for the two networks. In LANconfig, you can find these settings under Configuration/IPv4/General/IP networks.

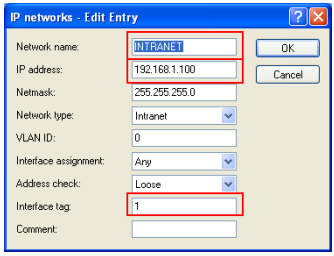


Figure 62: IP network for internal use

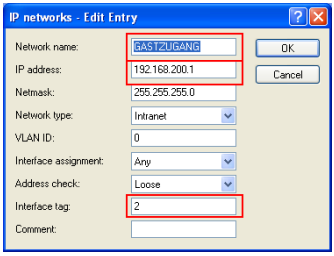


Figure 63: IP network for guest access

- The WLAN Controller can function as DHCP server for the Access Points and the WLAN Clients logged in. For this purpose, enable the DHCP server for the 'INTRANET' and the 'GUEST ACCESS'. In LANconfig, you can find this setting under Configuration/IPv4/DHCPv4/DHCP networks.

  Note: The activation of the DHCP server is obligatory for the guest network, optional for the internal network. You can implement the DHCP server for the internal network differently.

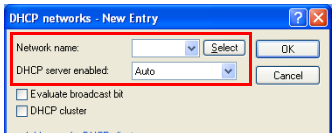


Figure 64: DHCP network for guest access

- Create a new standard route in the routing table which forwards the data from the guest network to the Internet access of the WLAN Controller. Select routing tag '2' and the 'Internet' router. Also activate the option 'Mask Intranet and DMZ (standard)'. In LANconfig, you can find this setting under Configuration/IP router/Routing/IPv4 routing table.

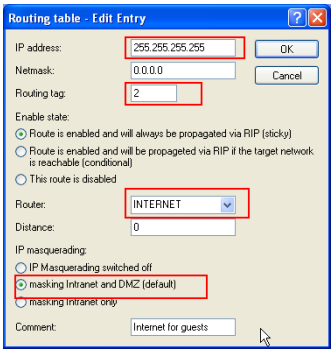


Figure 65: Routing entry for Internet access

- Activate the public-spot login for the logical LAN interface 'WLC-tunnel-1'. In LANconfig, you can find this setting under Configuration/Public spot/Public spot.

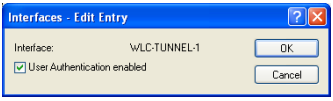


Figure 66: Activating the user login for the WLC tunnel

- As the last step, activate the option "Authenticate with name and password" via the public spot for the WLAN Controller. In LANconfig, you can find this setting under Configuration/Public spot/Login.

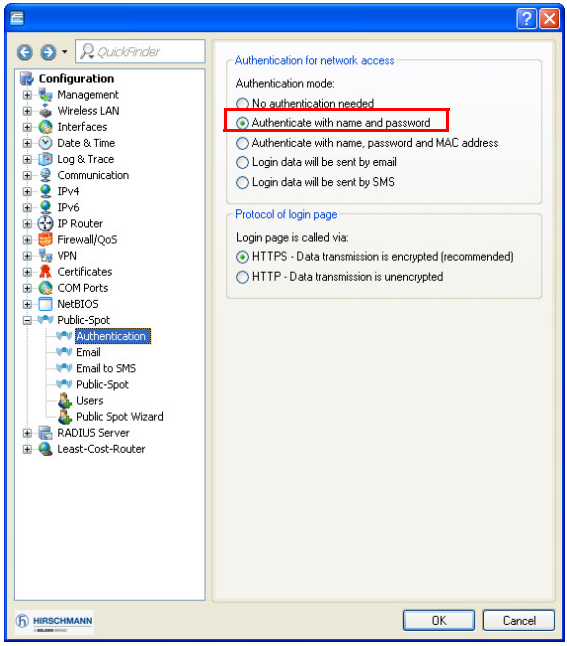


Figure 67: Activating the login via the public spot

Apart from the configuration of the WLAN Controller, you can configure the public spot to meet your requirements, either for the use of an internal or an external RADIUS server.

6 Public Spot

6.1 What is a Public Spot?

Public Spots, also called hotspots, are places where users can connect their terminals – such as smartphones, tablet PCs or laptops – to a publicly accessible network. Normally, these networks provide connections to the Internet; however a Public Spot can also be limited to a local network in order to offer extra information to users visiting a museum or a trade show, for example. The term is usually synonymous to the devices with which the user can connect to the network, which is also why this manual does not differentiate between the location and the device.

Access via wireless LAN is widespread, however, it is also possible to access a Public Spot using a cabled LAN connection. The most popular demand for these services originally came from business travelers at airports, in hotels, or at other locations where their end devices require access to online content. The public rarely has access to modems, ISDN or broadband connections in areas like this. However, the recreational use of Public Spots by private persons has become very popular.

6.1.1 The solution: (W)LAN technology

Public Spot scenarios make use of the widespread (W)LAN technologies based on the internationally established IEEE 802.11/802.3 standards:

- Access via WLANs provides fast, uncomplicated network access by radio. The user only needs a WLAN adapter for their mobile device, which, for modern devices, is usually part of the standard equipment or can be inexpensively added, usually with a USB interface. The bandwidth is sufficient for most applications, even when multiple users are simultaneously logged in to a Public Spot.
- With automatic address allocation via DHCP, access via LAN is similarly uncomplicated: In this case, the user only needs a LAN adapter and a suitable cable for their end device, in order to connect their device to the Public Spot network at a wall socket.

However, when accessing via LAN the user loses mobility and uninterrupted flexibility. However, this access – assuming that a corresponding infrastructure is available – also provides stable network operation with the highest network load (for example, for multimedia content such as video-on-demand) and a higher number of users (for example, in a large hotel), where connections via WLAN may reach their limits sooner. It is also possible to add a Public Spot offering to an existing cable infrastructure (for example, in a college) with the use of a Public Spot via LAN.

Noteworthy issues of access using (W)LAN

It is difficult to employ a standard WLAN access point or LAN router as a Public Spot for two main reasons:

- User authentication is only possible by employing RADIUS/802.11x, so requiring the appropriate infrastructure and configuration.
- There is no facility for billing / accounting.

For this reason, the use of devices without the Public Spot function is not practical, since these devices are not able to separate and log the specific network usage of authorized and unauthorized users of publicly accessible networks.

6.1.2 User authorization and authentication

As soon as an end device moves within range of an access point, the user can spontaneously established a connect to this access point. The same is true for open LAN connections. However, the problem is that access should not be available to the public in general, but only to certain selected users. Setting up restrictions of this type is the task of a Public Spot.

For this purpose, a Public Spot must be in a position to control access to the WLAN on a user basis. For simple Public Spot installations, user data can be locally stored and managed in the router or access point – or alternatively on a WLAN controller. Instead, complex installations employ a direct database connection to a central authentication server in the interests of detailed accounting or direct management. Central servers of this type generally work with RADIUS technology.

6.1.3 Accounting

If the Public Spot operator does not want to offer this service free of charge, connection data has to be collected and billed for each user. Typical methods include: Purchase of a limited amount of online time (pre-paid method), retrospective payment of consumed resources (credit payment), or unrestricted access until a certain time (e.g. checking out of a hotel).

For smaller Public Spot installations, accounting functions should be as simple as possible, and they should be implemented locally in the device. Larger installations offer the facilities for billing via an external RADIUS server. For each application scenario, the connection to an external system can also be implemented using a software interface which has access to the accounting data and can control the user authentication (e.g. hotel reservation systems).

6.1.4 Logging

The operation of commercial telecommunications services is subject to national regulations. Certain information is to be recorded and presented to law enforcement agencies upon request.

The Public Spot module provides suitable functions for recording user data with RADIUS accounting and SYSLOG.

Note: Please note that operating a Public Spot (also referred to as a hotspot) can be subject to legal regulations in your country. Before installing a Public Spot, please inform yourself about any applicable regulations.

6.2 Overview of the Public Spot module

The demands placed on devices operating Public Spots are as varied as the environments they are employed in. A Public Spot offers various functions which are described in more detail in the following sections.

6.2.1 Open User Authentication (OUA)

The Open User Authentication (OUA) provides Web-based authentication by means of an online form and is ideal for Public Spot installations.

Typical procedure for an online session with OUA

☐ The user of a W(LAN)-enabled end device is within reach of an access point or a network outlet in a Public Spot mode.Internet access or the use of chargeable services is not yet possible at this stage.

– WLAN: After system startup, the WLAN adapter automatically logs on to the appropriate access point.

– LAN: After system startup the user connects to the network with a suitable cable and is assigned an address by the DHCP server.

☐ The user starts a web browser. The device offering the Public Spot service automatically directs the user to the login page of the Public Spot. This page provides detailed information on using the services.

Generally, the user purchases a voucher with login data that grants a limited amount of access time. Other login methods are also possible, such as login after confirming the provider's terms of use or independently requesting login data via e-mail or a text message (SMS).

- ☐ In the case of a login using a voucher, the user enters his login data (username and password) on the login page. Depending on the configuration, the RADIUS server on the device (internal) or an external one checks the login data that was entered. If the login is successful, the user gains access to the Public Spot. Otherwise an error message will be displayed. If a prepaid model is employed, i.e. access is to be granted for a limited period of time only, then the RADIUS server additionally informs the Public Spot about the user's time credit.
- ☐ The user can log off from the Public Spot at any time. The Public Spot can terminate a session itself if the time credit has expired, if a specified expiry date is reached, or if contact is lost for an extended period.

  During and at the end of a session the Public Spot provides the user with an overview of the session data. If required, the Public Spot can simultaneously transmit all important accounting information to the RADIUS server. This can be the device's internal server or an external server.

OUA can be employed universally

The big advantage of the OUA method is that it is completely based on standard protocols. This guarantees that OUA can be operated universally. It works with any (W)LAN adapter, can be seamlessly integrated in existing network infrastructures, and makes it possible to implement additional features, for example, when the WLAN is between cells during roaming.

6.2.2 Security in the (W)LAN

Wireless LANs are potentially a significant security risk. Public Spots present similar risks to the operator and users.

Security for the operator

Operators of Public Spots are primarily interested in the security of their own network infrastructure. A Public Spot module provides operators with a range of security technologies and methods:

- **Multi-SSID** (only WLAN)**, VLAN and virtual routers**
  - The safe separation of public access can be achieved using one or more different radio cells for an access point (Multi-SSID).
  - VLAN technology can separate public access from the private network of the operator.
  - Virtual routing technology ARF (Advanced Routing and Forwarding) from Hirschmann supplies one SSID with its own security and QoS settings and only specific destinations are routed on it.

  This ensures that guest access over a Public Spot is securely and effectively separated from the productive network, even though they share the same infrastructure. The device's internal firewall can, for example, limit the available bandwidth in the WAN to max. 50 %, and access can be restricted to web pages (HTTP, port 80) and name resolutions (UDP 53).
- **Traffic limit**

  To avoid denial-of-service (DoS) and brute-force attacks on the Public Spot you can restrict the permissible data transfer for non-authenticated Public Spot participants to a harmless volume.
- **Locking access to the configuration**

  You can lock access from your Public Spot network to device configurations (e.g., your access points, WLAN controllers or routers) so that access to configurations is only possible using other specified management interfaces.

Security for the user

The primary security concern for users of Public Spots is the confidentiality of their data. Users are also interested in security of user data to avoid misuse. Users are protected by the following security technologies:

- **Intra-cell blocking** (WLAN Only)

  Prevent communication between the WLAN clients in your Public Spot network. Along with the user's existing security mechanisms, this measure helps to prevent unauthorized access to the resources of your Public Spot users.

- **Encryption during the login phase**

  If you have a digital certificate, you can load it on your device in order to secure usernames and passwords using an encrypted HTTPS method. The digital certificate should be signed by a recognized public authority so that browsers classify it as trustworthy and do not display security errors to the users. If there is no certificate, data is sent unencrypted.

  Note: The certificate merely secures the login process, as the data within a Public Spot network are normally not encrypted. This is true for LAN as well as WLAN connections. If your users wish to secure their regular data traffic as well, they will have to use their own encryption methods.

  ▶An exception to this are the WLAN connections via HotSpot 2.0: Since the HotSpot 2.0 standard is based on WPA2 (802.1X/802.11i), EAP and 802.11u, data packets are always encrypted for transmission, both for authentication and during the session.

  Hirschmann strongly recommends that sensitive user data should only ever be transferred via encrypted connections, such as the IPSec-based VPN tunnel with the Hirschmann Advanced VPN Client or over normal encrypted data connections based on HTTPS. In addition to this, Public Spot users should ensure that a personal firewall is active on their end devices.

6.2.3 Setup wizard for Public Spots

The "Setup Public Spot" wizard helps you to setup and perform the initial configuration of your Public Spot. You can set up a functional Public Spot network with just a few clicks. The wizard groups the necessary settings together (e.g. assign an interface, choose an IP range, specify the access format and login procedure, logging) and offers you the option to create an administrator with limited rights who can only create and manage Public Spot users.

6.2.4 Wizard for creating and managing users

Using the setup wizard "Create Public Spot account" you can use WEBconfig to create temporary accesses to the Public Spot network with just a few clicks of the mouse. In the simplest case, you only need to enter the duration of access, the wizard assigns the username and password automatically and stores the credentials in the user database of the internal RADIUS server. The user receives a printed, personalized voucher, which the user can use to login to the Public Spot network for the specified period.

Users may not want to access the Public Spot at the moment when the voucher is printed out. For this situation, vouchers can be printed out in advance. The access is set up so that the time budget only starts running when the user logs in for the first time. A maximum period of validity is also defined, after which the access account is automatically deleted, even if the access time budget has not been used up.

The setup wizard "Manage Public Spot account" displays all registered Public-Spot user accounts in a table on a web page. With just one click you have the most important data for your users on one screen, and you can easily view the login status, information about login data and corresponding validity periods, extend a voucher, or delete a user account.

6.3 Basic configuration

The instructions for the basic settings are divided into several separate sections:

- The first section describes the setup of an operational Public Spot using a Wireless Router as an example.

  Note: To set up a Public Spot for a simple application scenario, you can start the corresponding wizard, which assists you in configuring the Public Spot.

- The second section describes the configuration of the default values for the user wizard with which new employees can easily create and manage new Public Spot users without the need for general administrator rights. This also includes creating a limited access account with which your employees can access this wizard only.
- The third section describes user administration on the local RADIUS server, either using the user wizard or manually with LANconfig.

To a certain extent these sections are dependent on one another, and ideally you should work through them in sequence.

6.3.1 Basic installation of a Public Spot for simple scenarios

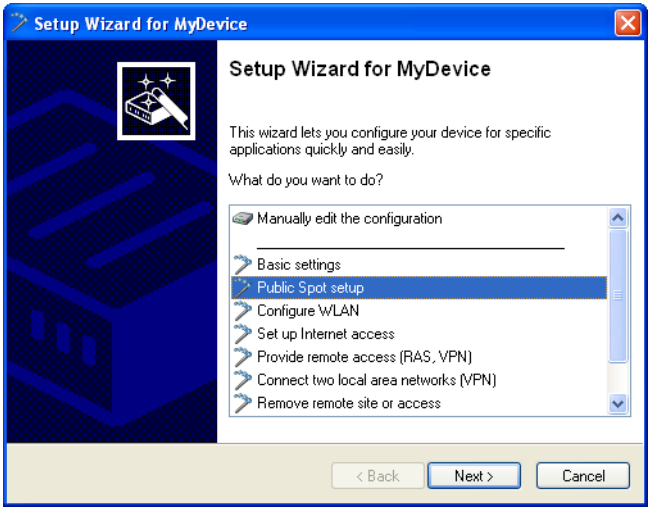
Installation using the setup wizards

The following tutorial describes how to use LANconfig's Public Spot setup wizard to perform a basic Public Spot installation.

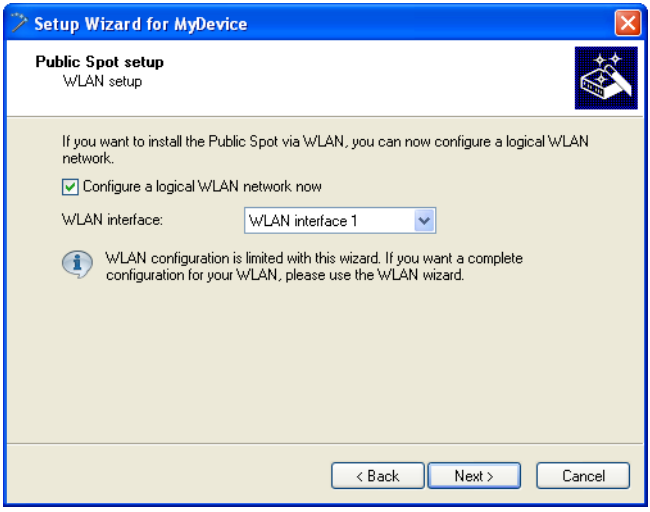
Note: The wizard for the basic configuration of the Public Spot shows different dialogs depending on the device type and your previous choices. This tutorial is only an example.

☐ To do this, start LANconfig and select the device for which you want to set up the Public Spot, for example, a access point.

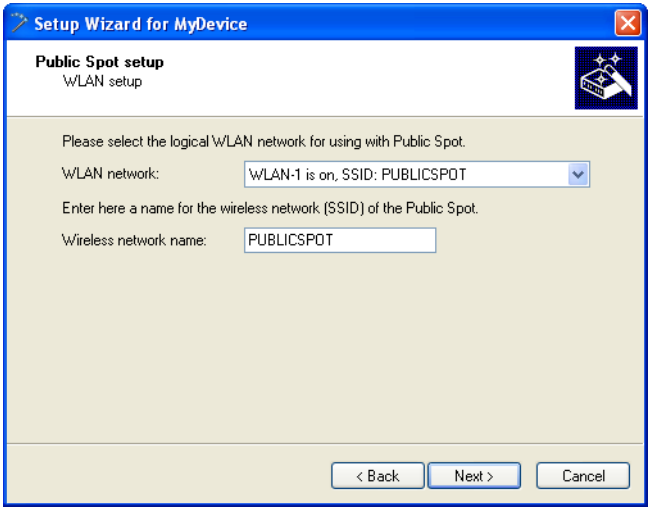
☐ Start the Setup Wizard with `Device : Setup wizard`, select the action "Setup Public Spot" and then click "Next".



☐ If you want the Public Spot to be available over WLAN, enable the corresponding option and then click "Next".



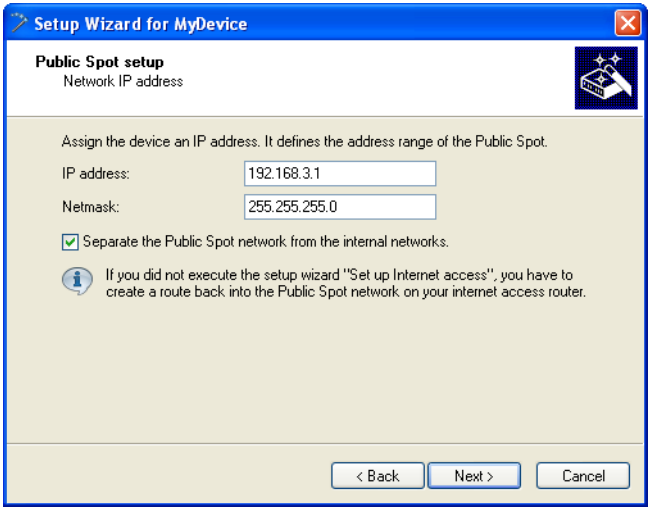
☐ Select the logical interface from the drop-down menu which the Public Spot should offer (e.g., WLAN-1), and enter a descriptive name for the wireless network (SSID). Click on "Next".



☐ Assign the IP address and netmask to the device that your Public Spot network should specify and click "Next".

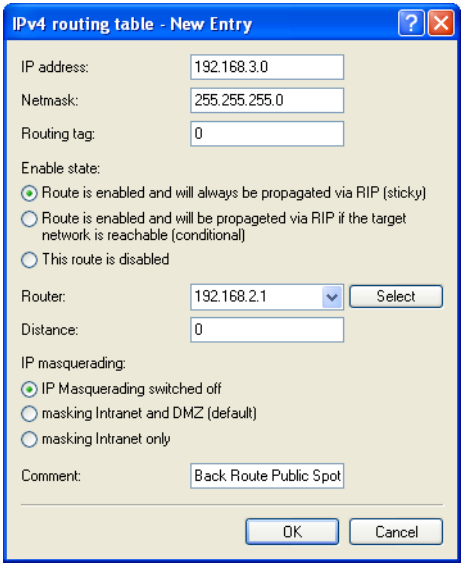
The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set up and your device has the IP address 192.168.2.1, you can assign the IP address `192.168.3.1` and the subnet mask `255.255.255.0`, as long as this IP address has not already been used elsewhere.

If you want to separate the Public Spot network from internal networks for security reasons, make sure that the corresponding option is enabled.



Note: If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you must set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully authenticated.

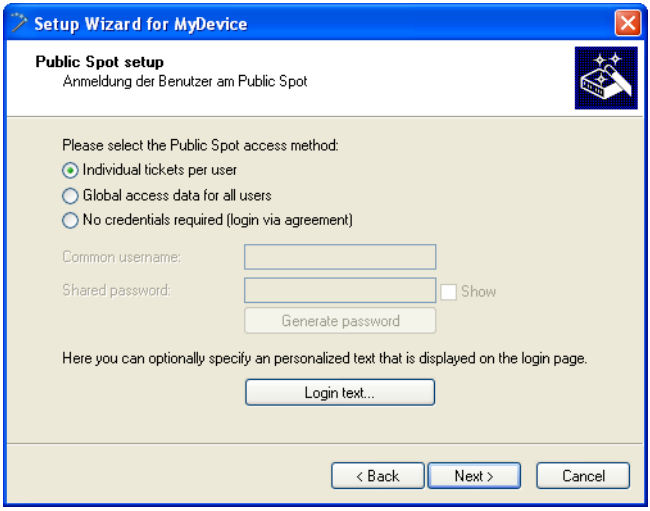
☐Please find the directions on how to set up a return route, in the documentation for your Internet gateway. In LANconfig you can configure it under `IP router : Routing : IPv4 routing table`. To do this, create a new entry and enter the network address of your Public Spot network under "IP Address" and under "Router" enter the address of the Public Spot in your local network.



☐ Specify which login data your users are to use to login to the Public Spot. Also, you can optionally add customized text to the login page. To continue, click on "Next".

You can either give each user their own login data or set up a general account that all users use to access the Public Spot. If you issue vouchers later and would like to set up permanent user accounts, select the option "Individual tickets per guest".

The login text is a customized text entered in HTML format, which appears on the login page inside the box on the registration form. You can manually add or edit this text at a later time (see section “Customized text on the login page” on page 565).

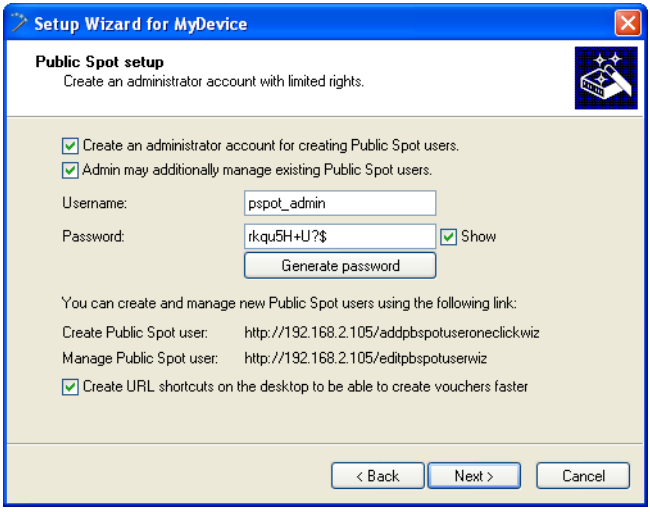


☐ If necessary, create an administrator with limited rights who can use the setup wizards in WEBconfig to create and manage Public Spot users. To continue, click on "Next".

This type of administrator is useful when you want your employees to be able to manage user accounts themselves without the help of a device administrator. The right to create new accounts in WEBconfig enables the Create Public Spot account wizard, and administrator rights enable the Manage Public Spot account wizard.

Using the user creation wizard "Create Public Spot account", the administrator has the option of creating time-limited accounts for Public Spot users and print the corresponding login data on a voucher.

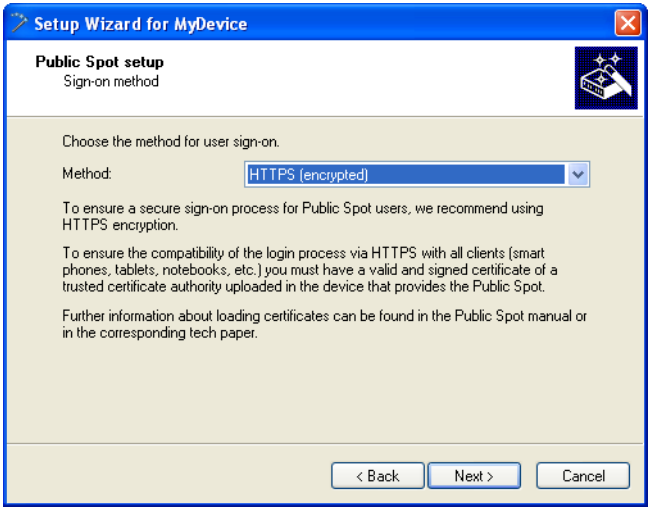
The "Manage Public Spot accounts" wizard enable the administrator to manage the users. The administrator can extend or reduce the validity period of access, or completely delete a specific user account. In addition, the administrator can call up information about the user account using the wizard, such as the password in plain text, the authentication status, the IP address, the sent/received data volume or any restrictions that apply to the account.



Note: Make sure that the password you create is secure. The Setup Wizard will check the quality of the password you enter. For passwords that are not secure the input field appears in red, when it is more secure it changes to yellow, and when it is very secure the background turns green.

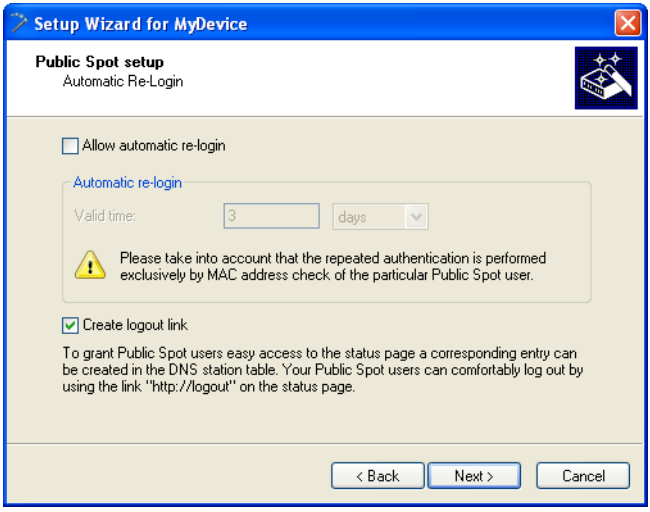
☐ Select the procedure for user login. To continue, click on "Next".

You can select "HTTPS" or "HTTP" in the drop-down list. Using a connection with HTTPS provides a secure connection for Public Spot users.



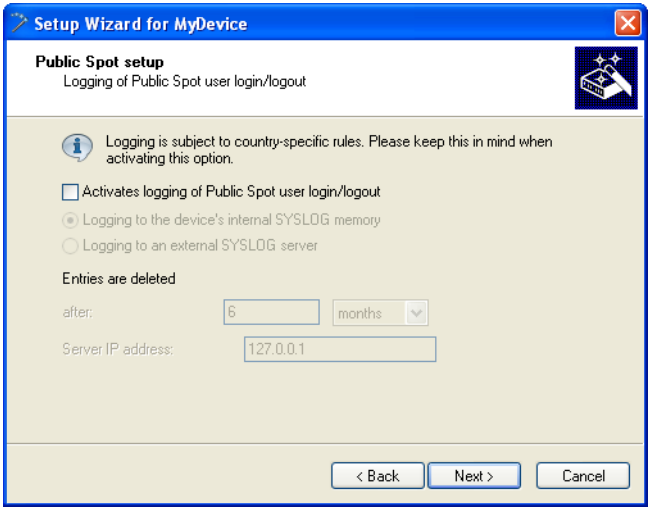
☐ Determine whether automatic re-login is allowed for all Public-Spot users, and the maximum absence that is allowed before the user must login again on the Public Spot webpage. To continue, click on "Next".

The "Automatic re-login" option is a convenience option that allows the Public Spot to automatically authenticate known users or devices. However, if known devices are to be recognized exclusively from the MAC address of the network adapter, the fact that MAC addresses can be falsified represents a potential security risk. For this reason this option is disabled by default.



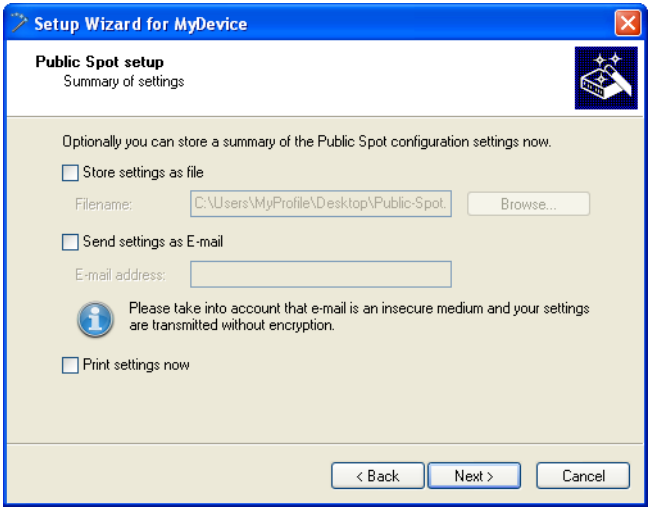
☐ If needed, enable logging of logins and logouts for Public Spot users in the internal SYSLOG storage of your device. To continue, click on "Next".

Since the logs comply with country-specific regulations, this option is disabled by default. Before enabling this function, you need to determine what the data protection regulations are for your country in order to avoid any legal issues.



☐ Save your changes if necessary.

Before you save the configuration to your device, you have the option of saving the configuration locally on your PC, sending it by e-mail, or printing a summary.



☐ The click "Next" and finally "Finish" to complete the basic installation of the Public Spot. The Setup Wizard will now send the settings to the device.

That's it! You have completed configuration of your Public Spot module! Now, if you come within range of a Public Spot with a WLAN-capable device, the device can find the SSID that you set up as a public network and login to it.

Manual installation

The following configuration steps show you how to manually setup a Public Spot for simple scenarios. For the application scenario described here, you enable the Public Spot on an interface over which there is no other data traffic other than the Public Spot traffic – where Public Spot and normal WLAN users do not share the same network (dedicated SSID).

Note: This tutorial is only an example. Depending on the device type (access point, router, WLAN controller, etc.) or complexity of the network configuration (e.g., use of VLAN or ARF), different or additional steps may be required for setting up a Public Spot. Since this type of network configuration can be highly customized, this tutorial concentrates specifically on a simple example, so that you can adapt the steps as needed.

☐ To do this, start LANconfig and select the device for which you want to set up the Public Spot, for example, a access point. Next, open the configuration menu for the device.

☐ Check that the time is correct.

To check the certificates and correctly record and bill session data, it is important for the Public Spot's time setting to be accurate. First make settings such as time zone and time changes (summer and standard time):

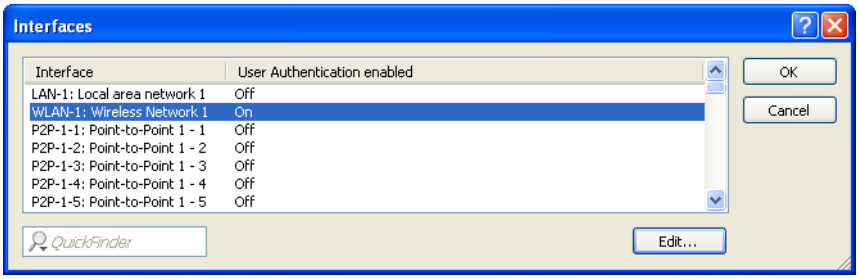
– LANconfig: `Date/time : General`

Note: In order to ensure that the time of the Public Spot remains correct, the device should be set up as an NTP client. Enter the time server that is necessary for that under `Date/Time : Synchronization : Time server`. Open the "Add" window to show a list of possible server addresses.

☐ Select the interfaces for the Public Spot operation.

Here you activate the interfaces which will be available to registered users. Along with the logical WLAN interfaces which Public Spot users directly login to, the logical LAN interfaces (LAN-1, etc.), and the point-to-point connections (P2P-1, etc.) can also be selected. When connected via the LAN or P2P interface, you can integrate additional access points into the Public Spot of another device. For a single access point instead select, for example, the logical WLAN interface "WLAN-1".

– LANconfig: `Public Spot : Server : Interfaces`



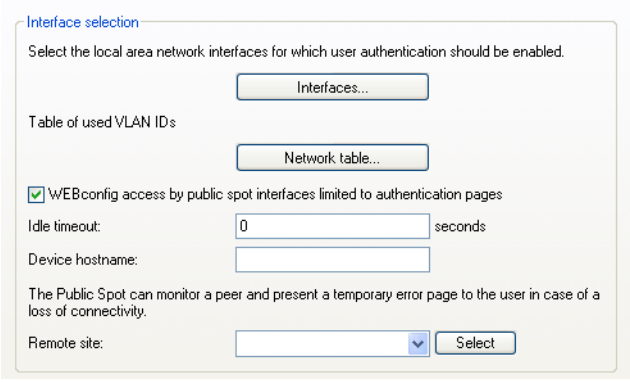
By activating the authentication for a WLAN interface, you automatically release the associated SSID for the Public Spot operation.

Note: On a WLC you can enable certain Ethernet interfaces for the Public Spot. In this manner you can also set up selective restrictions for certain VLANs.

☐ Access to your device from the Public Spot network should be restricted to the authentication pages.

If you do not restrict access, Public Spot users will be able to access the configuration interface of your device (WEBconfig). For security reasons you should not permit this.

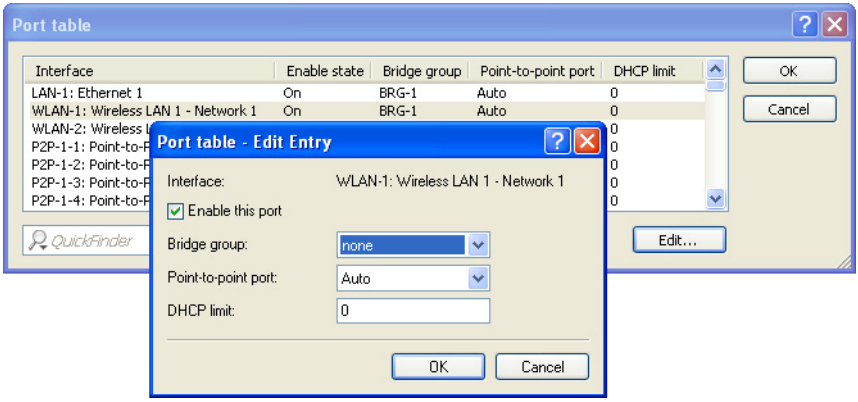
– LANconfig: `Public Spot : Server : WEBconfig access by Public Spot interfaces limited to authentication pages`



☐ Disconnect the interface which is to be used for Public Spot operations from the other network traffic.

In order for end devices to be able to communicate with each other using different interfaces of a Public Spot device (e.g., between LAN-1 and WLAN-1), these interfaces are logically connected to each other (bridged) within your device. However, in a Public Spot scenario this type of bridging may not be desirable for security reasons. In order to disconnect the communication between an interface (e.g., WLAN-1) assigned to a Public Spot and the rest of the network, you have to remove bridging. In the "Port table" set the "Bridge group" for the respective interface to `none`.

– LANconfig: `Interfaces : LAN : Port table`

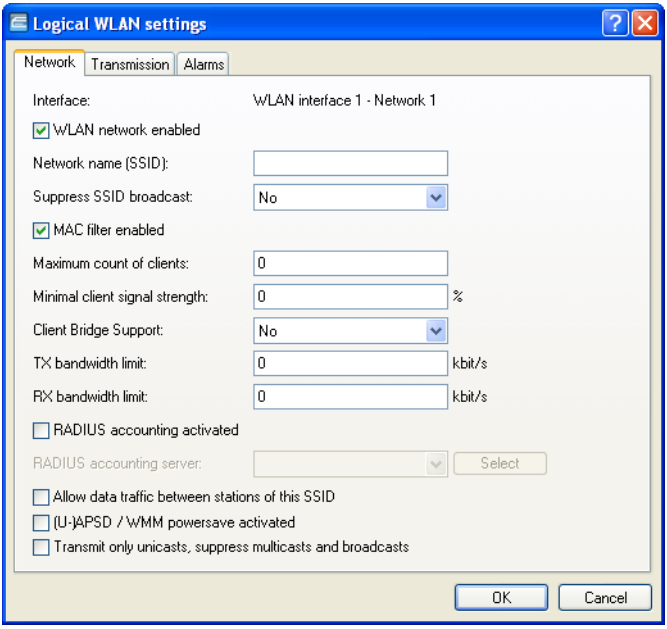


☐ Enable the WLAN for the Public Spot.

This setting does not affect: WLAN controllers.

Activate the logical WLAN which you enabled for the Public Spot login and assign a descriptive name to this network (SSID).

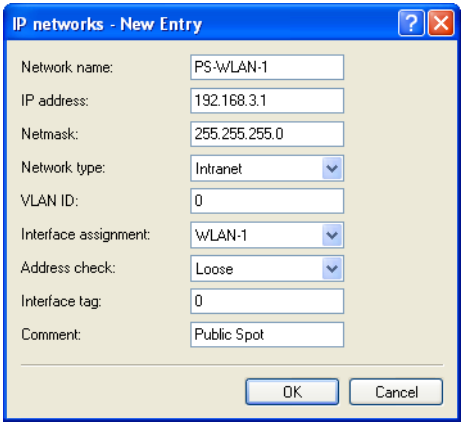
– LANconfig: `Wireless LAN : General : Logical WLAN settings : WLAN network <number> : Network`



☐ Assign the IP address and netmask to the device that your Public Spot network should specify.

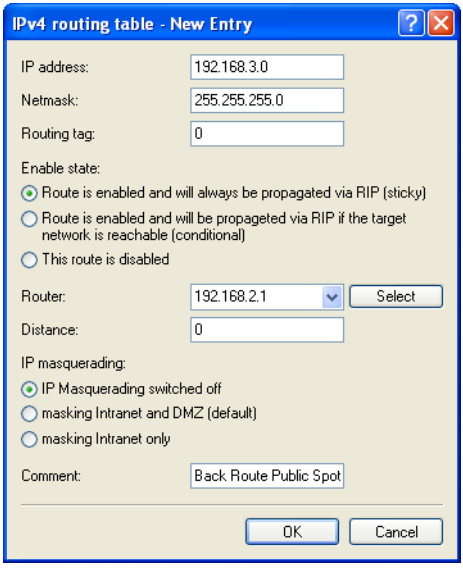
The Public Spot module has its own address on your network, which is independent from the address that you assigned to your device. For example, if you have a 192.168.0.0/24 network set up and your device has the IP address 192.168.2.1, you can assign the IP address `192.168.3.1` and the subnet mask `255.255.255.0`, as long as this IP address has not already been used elsewhere. Select the interface that you chose under "Interface assignment" e.g., `WLAN-1`.

– LANconfig: `IPv4 : General : IP networks`



Note: If your device is not directly connected to the Internet and you have a different address range for your Public Spot, you must set up a return route to your Public Spot network on your Internet gateway. If there is no return route, Public Spot users will see an HTTP error after they have successfully authenticated.

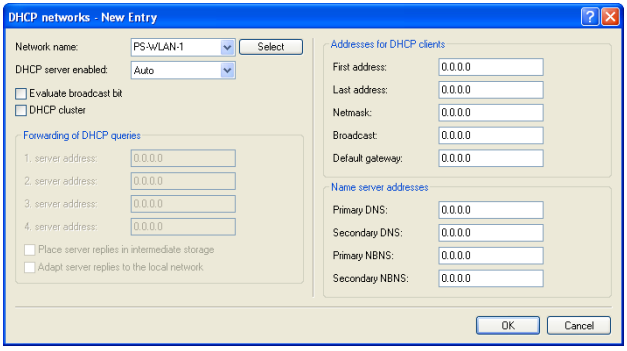
☐Please find the directions on how to set up a return route, in the documentation for your Internet gateway. In LANconfig you can configure it under `IP router : Routing : IPv4 routing table`. To do this, create a new entry and enter the network address of your Public Spot network under "IP Address" and under "Router" enter the address of the Public Spot in your local network.



☐ Configure the DHCP server settings for the Public Spot network.

Since the device has an IP network that is independent from the network where it is located, you must configure a DHCP server for this network. For the previously set up IP network (e.g., `PS-WLAN-1`), set the value for "DHCP server enabled" to `automatic`.

– LANconfig: `IPv4 : DHCPv4 : DHCP networks`

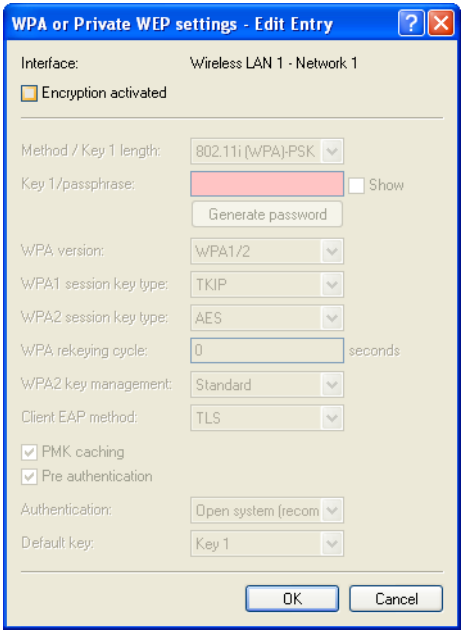


☐ Disable the encryption for the interface that you are using for the Public Spot.

This setting does not affect: WLAN controllers.

Encryption for all logical WLANs is enabled by default. In Public Spot applications, the payload data between the WLAN clients and the access point are usually transmitted unencrypted. For this reason, disable encryption for the logical WLAN which you previously set up for the Public Spot login.

– LANconfig: `Wireless LAN : 802.11i/WEP : WPA or Private WEP settings`

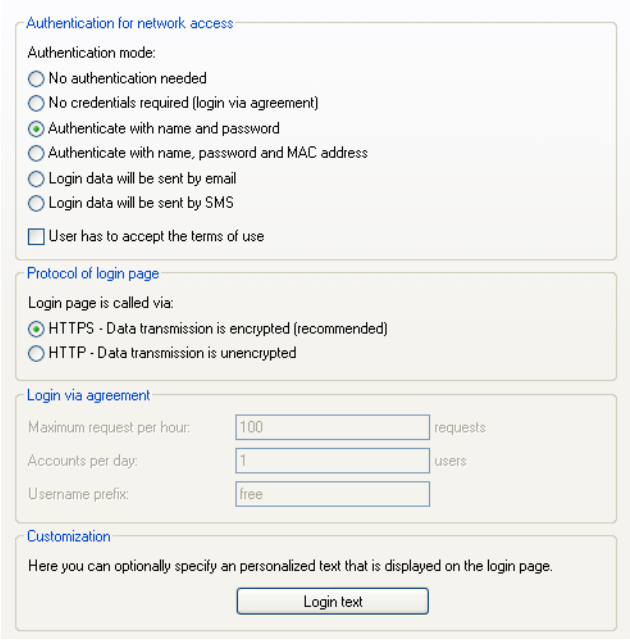


☐ Select the authentication mode and the protocol used for the user login.

The authentication method that you select determines the information which users of the Public Spot WLAN must enter when logging in. Select "Authenticate with name and password" to allow your users the option to login with an individual username and password that you have previously assigned them. This setting also allows you to quickly provide Hotspot access to your guests using vouchers (tickets).

Use "HTTPS" as the protocol in order to be able to send encrypted login data to your users during login.

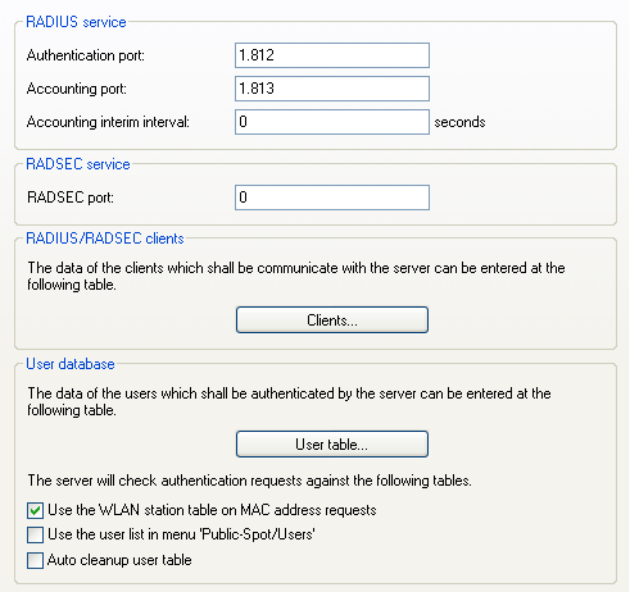
– LANconfig: `Public Spot : Authentication : Authentication mode`



☐ Specify the internal RADIUS server as the server responsible for user administration and accounting. To do this, enter the "Authentication port"`1.812` and "Accounting port"`1.813`.

You store Public Spot access accounts in the user database on the device's own RADIUS server. In order to use Public Spot access accounts, you **must** configure the RADIUS server and the Public Spot module to use the RADIUS server.

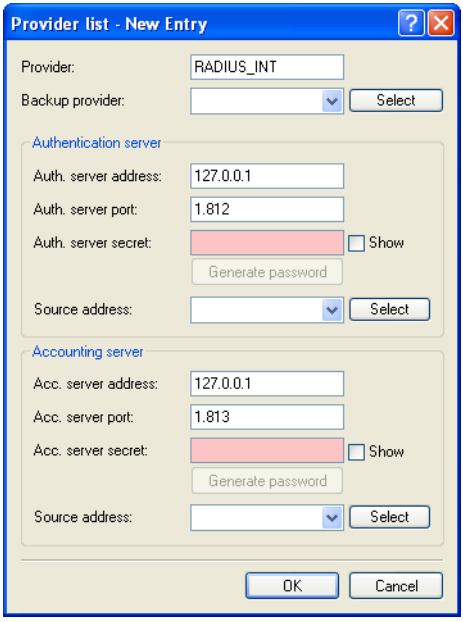
– LANconfig: `RADIUS server : General`



☐ Create an entry for the internal RADIUS server in the list of authentication servers of the Public Spot. Under "Auth. server IP address" and "Acc. server IP address" enter the loopback address `127.0.0.1`. Use the "Auth. server port" and "Acc. server port" used for the authentication port and accounting port in the previous settings.

The list entry is necessary in order for the Public Spot to recognize the address of the RADIUS server and so that it can authenticate Public Spot access on the internal RADIUS server.

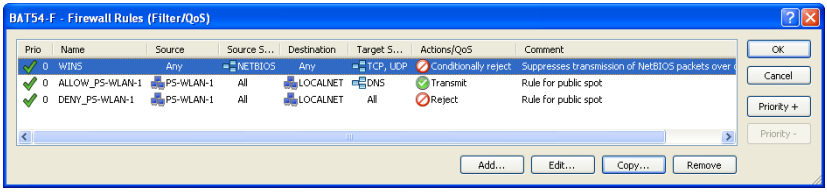
– LANconfig: `Public Spot : Users : Authentication servers`

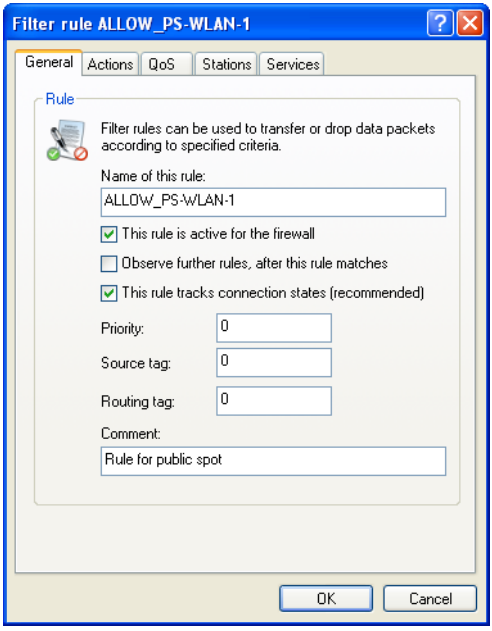


☐ Set up filter rules in the Public Spot's firewall to secure your local network. In each case, create an "accept" rule (for example, `ALLOW_PS-WLAN-1`) and a "reject" rule (for example, `DENY_PS-WLAN-1`).

You use the accept rule when devices are to be able to send DNS requests from the Public Spot network to all local networks, e.g., your local intranet. On the other hand, with a reject rule you generally block all access or requests from the Public Spot network to your local network. The order – accept before reject – is essential, since the firewall applies rules from the top to bottom of the list.

– LANconfig: `Firewall/QoS : IPv4 Rules : Rules…`





– **"Accept" rule settings:**

Enter the name of the rule in "General", for example, `ALLOW_PS-WLAN-1`.

Remove all possible predefined action objects from the list and using `Actions : Add..` add an action object of type "ACCEPT".

In `Stations : Connection source`, enable the option "Connections from the following stations" and select `Add... : Add custom station`.

In the Stations window that opens, select the option "All stations in local network" and for "Network name" select the name of your Public Spot IP network, e.g., `PS-WLAN-1`. "Close the dialog with "OK.

In `Stations : Connection destination`, enable the option "Connections to the following stations" and after selection "Add..." choose "LOCALNET".

In `Services : Protocol/target services` enable the option "Following protocol/target services" and select `Add... : DNS`.

End the filter rule dialog with a final click on "OK".

LANconfig then enters the allow rule into the rule table.

– **"Reject" rule settings**

Enter the name of the rule in "General", for example, `DENY_PS-WLAN-1`.

Remove all possible predefined action objects from the list and using `Actions : Add..` add an action object of type "REJECT".

In `Stations : Connection source`, enable the option "Connections from the following stations" and select `Add... : Add custom station`.

In the Stations window that opens, select the option "All stations in local network" and for "Network name" select the name of your Public Spot IP network, e.g., `PS-WLAN-1`. "Close the dialog with "OK.

In `Stations : Connection destination`, enable the option "Connections to the following stations" and after selection "Add..." choose "LOCALNET".

End the filter rule dialog with a final click on "OK".

LANconfig then enters the rejection rule in the rule table.

☐ Store the configuration on your device.

That's it! You have completed configuration of your Public Spot module! Now, if you come within range of a Public Spot with a WLAN-capable device, the device can find the SSID that you set up as a public network and login to it.

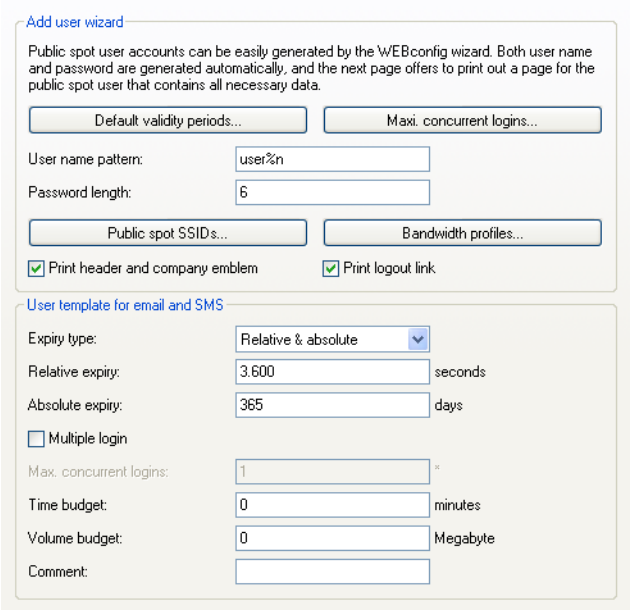
6.3.2 Setting default values for the Public Spot wizard

The following section describes how you define default values for the "New user wizard" (setup wizard "Create Public Spot account") to meet your needs. Public Spot administrators can select the values defined here (e.g. for validity periods, bandwidth profiles, etc.) from selection lists when they are setting up new users and printing out vouchers.

Note: Exceptions to this are the values for User name pattern and Password length shown in the dialog below, which only serve as default values for the device.

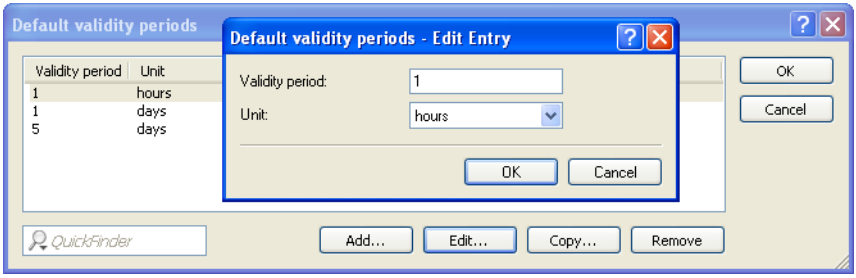
☐ Start LANconfig and open the configuration dialog for the device.

☐ Change the view to `Public Spot : Wizard`.



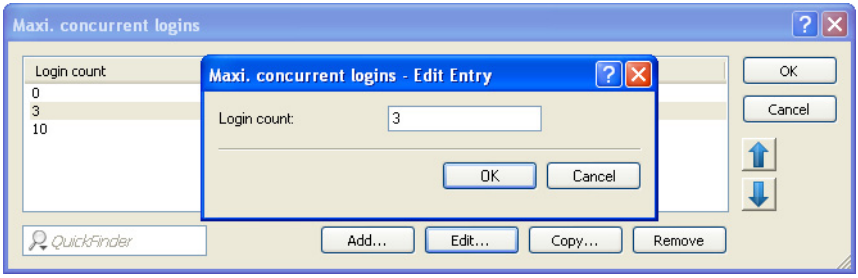
☐ In "Default validity periods", define which default validity periods for user accounts and vouchers are to be available by default.

The new-user wizard takes the shortest validity period as the default.



☐ Under "Max. concurrent logins" you select the maximum number of devices that have access to the user account simultaneously.

The value `0` stands for 'unlimited'. Whether or not it is generally possible for a user to login with the multiple devices at the same time is determined by the Public Spot administrator with a separate setting in the wizard when creating a new user.



☐ In "User name pattern" you specify the pattern used by the new user wizard to create usernames.

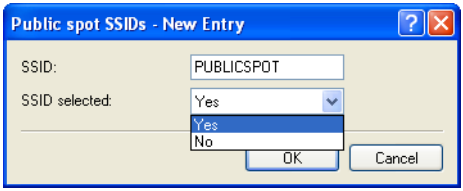
You can enter up to 19 characters, whereby the wizard will automatically create a unique number for every user if you enter "%n". The default description `user%n` will be shown later on the voucher, for example, as `user12345`.

☐ Using "Password length" you specify the length of the passwords that the new user wizard generates for Public Spot access.

The default is 6 characters. If you would like to have longer passwords, keep in mind that guests can make mistakes when entering them, which can cause unnecessary problems and complaints.

☐ Optional: Under "Bandwidth profiles" you set the uplink and downlink limits for each Public Spot user.

☐ Public Spot via WLAN only: Using "Public Spot SSIDs" you specify the names of the Public Spot networks taken by default when you create new user accounts using the Create Public Spot account wizard.



The Create Public Spot account wizard automatically marks the specified network names as "SSID selected" when creating a new Public Spot user. If you employ an access point, WLAN controller or WLAN router, you can select several network names as default values in order to give users access to various different WLANs (e.g., for WLANs in the hotel lobby, the conference room, and floors where their rooms are located). When creating a new user and subsequently printing the voucher, these SSIDs are also printed out on the voucher.

Using the arrow buttons, you can change the order in which the SSIDs are displayed. In this way, the most popular SSIDs can be placed at the top of the list.

That's it! This concludes the configuration of the default values for the Public Spot wizard.

6.3.3 Setting up limited administrator rights for Public Spot managers

In order for employees to be able to manage a Public Spot on the device without further permissions, you can explicitly assign them the function rights to use the Public Spot wizard. This tutorial describes the steps to set up Public Spot function rights for employees without giving them additional administrator rights.

Note: You need to have the "Supervisor" permission to be able to assign Public Spot management to an employee.

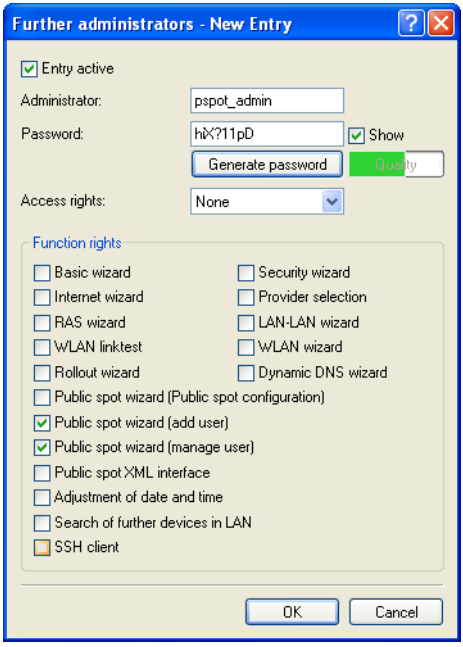
☐ Start LANconfig.

☐ Open the configuration for the device for which you want to register a Public Spot administrator.

The Public Spot option has to be enabled on this device.

☐ Change to the view `Management : Admin`, click in the section "Device configuration" on "Further administrators", and then click on "Add".

If you want to allow an existing user to perform Public Spot management, select the user's entry in the table and click on "Change".



☐ You activate the profile by checking the "Entry enabled" box.

☐ Assign a descriptive name in the field "Administrator".

☐ Enter a "password" and repeat it to be sure.

☐ Set the "Access rights" to "None".

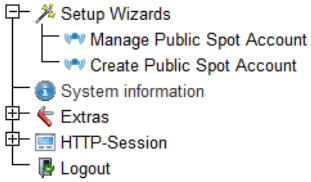
When you modify an existing user, you should not modify existing function rights.

☐ In the section "Function rights" enable the "Public Spot wizard (add user)", and "Public Spot wizard (manage user)".

When you modify an existing user, you should not modify existing function rights.

☐ Save the new or modified profile by clicking on "OK".

The Public Spot administrator is offered the Public-Spot wizards in the navigation when they log on using WEBconfig.



Using the user creation wizard "Create Public Spot account", the administrator has the option of creating time-limited accounts for Public Spot users and print the corresponding login data on a voucher.

Using the user management wizard "Manage Public Spot account", the administrator has the option of managing these users as well as the users that you created as the main administrator using the RADIUS user database. The administrator can extend or reduce the validity period of access, or completely delete a specific user account. In addition, the administrator can call up information about the user account using the wizard, such as the password in plain text, the authentication status, the IP address, the sent/ received data volume or any restrictions that apply to the account.

Note: The function right "Public Spot XML interface" is not needed by a normal Public Spot admin. The right is only relevant if you use the „XML interface“, and should not be combined with the function rights described above for security reasons.

6.3.4 Setting up and managing Public Spot users for simple scenarios

You can set up and manage Public Spot users either manually or by using the setup wizard. Setting up and managing the configuration options manually offers you more extensive options and allows you, for example, to create self-defined users with an unlimited lifetime.

On the other hand, the setup wizard allows you to create generic Public Spot users with automatically generated login data with limited lifetimes. The respective setup wizard is only accessible using WEBconfig, which allows you to quickly create users without requiring administrator permissions for the entire device. The only requirement is an administrator with limited permissions.

You naturally also have the option to initially create generic users with the aid of the setup wizard and then manually adapt them to your needs (e.g., change the usernames).

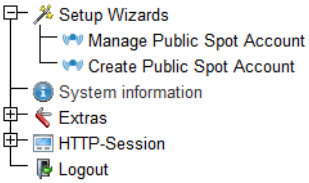
Adding Public Spot users with a single click and voucher printing

The following section describes the setup of a Public Spot user using WEBconfig and then printing a voucher. You can also prepare vouchers in advance.

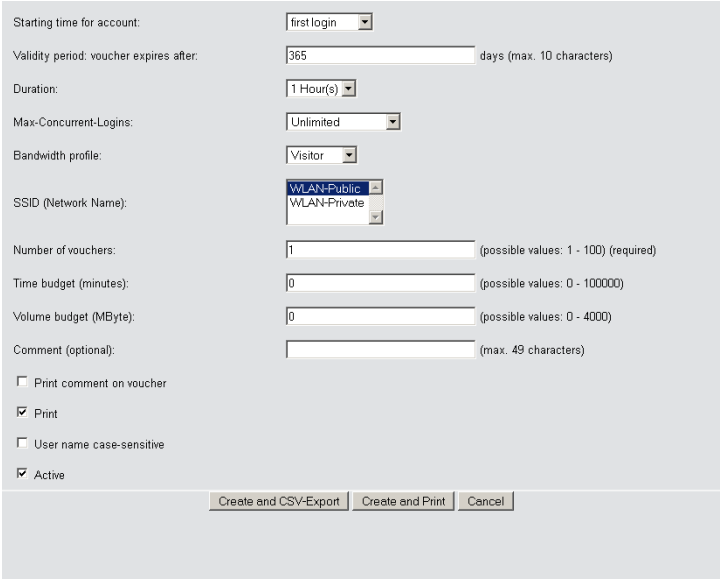
Note: You need the permissions for the "Public Spot Wizard", in order to create a new Public Spot user.

☐ Log on to the WEBconfig home page as an Administrator.

☐ Start the setup wizard by clicking on `Setup wizards : Create Public Spot account`



☐ The new user wizard starts with an input screen. The fields have default values.



The wizard automatically creates a username and a password. In the subsequent printout dialog you can select the voucher printer and print-out the voucher.

☐ If necessary, you can change the default values before you print it.

The following entries affect the appearance as well as the validity of the vouchers:

– "Starting time for account": Sets the time when the voucher becomes valid. Possible values are:

`First login`: Access is valid as of the user's initial login

`Immediately`: Access is valid as of the creation of the user's account

To a supply of vouchers in advance, select `First login` as the validity of the vouchers. That way the vouchers will still be valid even after a longer period.

– "Validity period: Voucher expires after": Enter the overall time period within which the voucher can remain valid.

If the access is to be valid immediately, it is not possible to enter a validity period.

– "Duration": Set how long access is to be available after registration or the first login. The values listed here are managed in the "Default validity periods" table. The pre-defined values are:

  `1 Hour(s)`

  `1 Day(s)`

  `5 Day(s)`

– "Max. concurrent logins": Select the maximum number of concurrent devices that can have access to the user account for the corresponding user. The values listed here are managed in the "Max. concurrent logins table". The pre-defined values are:

  `Unlimited`

  `Only 3 device(s)`

  `Only 10 device(s)`

– "Multiple login": Select this option in order to allow a user to login with several devices using the same login data. The number of devices that can be logged on simultaneously is specified using the drop-down list "Max-concurrent-logins".

– "Bandwidth profile": Select a bandwidth profile from the list in order to selectively restrict the amount of bandwidth available to the user (uplink and downlink). Create a bandwidth profile in the "Bandwidth profile" table.

– "SSID (network name)": Specify which wireless LAN network the access applies to. This SSIDs listed here are managed in the "SSID table". By pressing the "Ctrl" button you have the option of selecting multiple entries. Default entries are already pre-selected. If you have not defined any entries in the table, the wizard conceals this option.

– "Number of vouchers": Specify how many vouchers you want to create at a time. If you set the login time as the access start time, you can print-out a supply of vouchers in advance.

– "Time budget (minutes)": Specify the amount of time after which access to the Public Spot is closed.

Depending on the chosen expiry method, access time is limited either to the time budget (incremental) or to the set voucher validity period (absolute).

- "Volume budget (MByte)": Specify the available data volume after which access is closed.
- "Comment (optional)": Enter a comment here. This comment can contain, for example, additional notes about the access duration or the telephone number of the receptionist in case of access problems.
- "Print comment on voucher": Check this option if the comment is to appear on the voucher.
- "Print:" Check this option to print the vouchers as soon as they are registered.
- "User name case-sensitive": Enable this option if Public Spot users have to pay attention to capitalization when entering their user name at login.

☐ If you want to keep the default values or accept the new values without changing them, you click on "Save and print" at the end.

If the "Print" option is disabled, the wizard displays a summary of the new Public Spot users after they have been registered. You then have the opportunity to print the vouchers again.

Wizard for Public Spot user management

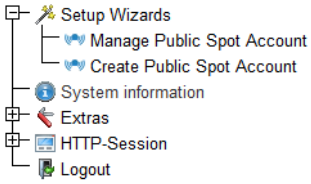
The following section describes how to use WEBconfig to manage the registered Public Spot users.

Note: You need the "Public Spot wizard" permission, in order to manage a Public Spot account.

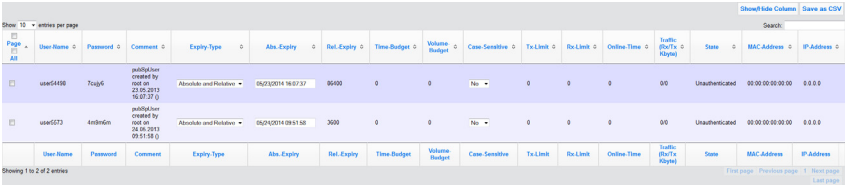
Note: Unsaved changes are lost once you finish this wizard.

☐ Log on to the WEBconfig home page as an Administrator.

☐ Start the setup wizard by clicking on `Setup-Wizards : Manage Public Spot accounts`



☐ The Public Spot wizard starts with a list of registered Public Spot users.



In the "Show... entries per page" drop-down list you set how many entries are displayed per page. The corresponding pages are accessed via the page navigation at the lower right:

– "First page": Shows the page with the first entries.

– "Previous page": Returns to the previous page.

– "Page numbers (1, 2, 3, ...)": Goes directly to the chosen page.

– "Next page": Goes to the next page.

– "Last page": Shows the page with the latest entries.

With "Search" you can filter the displayed entries. The filter immediately searches for entered strings.

You export highlighted entries with "Save as CSV".

The column headers have the following meaning:

– "Page/All": This column is used to select the user for the desired action (print, delete, save). To select all entries on the current page, select "Page". To select all of the entries, select "All".

– "Name": Manually or automatically displays the username generated by the system.

- "Password": Manually or automatically displays the password generated by the system.
- "Comment": Includes the comment entered at registration (in brackets) and any changes to the user data (automatically documented by the system).
- "Expiry type": Indicates whether the validity period of this user account is absolute (e.g. expires on a set date) or relative (expires after the time has elapsed since the first successful login).
- "Abs. expiry": If "absolute" has been selected as the expiry type, the user account becomes invalid at the time defined in this field.
- "Rel. expiry": If "relative" has been selected as the expiry type, the user account becomes invalid after this time period has expired since the user logged in for the first time.
- "Time budget": Specifies the maximum access time for this user account. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.
- "Volume budget": Specifies the maximum data volume for this user account. The user can use this data volume until a relative or absolute expiry time (if set) is reached.
- "Case sensitive": Indicates whether the login page takes capitalization of the user name into account.
- "Tx-Limit": If a bandwidth profile was entered for the user, this entry shows the maximum transmission bandwidth available to that user.
- "Rx-Limit": If a bandwidth profile was entered for the user, this entry shows the maximum receiving bandwidth available to that user.
- "Traffic (Rx/Tx Kbyte)": Indicates the data volume in kilobytes that the user has received (Rx) or sent (Tx) so far.
- "State": Shows the authentication status of the individual users. Possible values are:

  "Unauthenticated": The user is currently not logged on to the Public Spot.

  "Authenticated": The user is currently logged on to the Public Spot.

– "MAC-Address": Indicates the physical address of the network adapter for the device with which the user is currently connected.
– "IP-Address": This shows the IPv4 address that the system currently has allocated to the user.

The buttons at the bottom of the window have the following functions:

– "Print": Print out the voucher for the selected user.
– "Delete": Delete the selected user.
– "Save": Save the changes.
– "Back to main page": Return to the main page; all unsaved changes will be lost.

You can edit the following user information by changing the contents of the corresponding fields:

– "Expiry type"
– "Abs. expiry"
– "Case sensitive"

☐ Select the account that you want to edit in the first column.

☐ Change the corresponding field values and click "Save" to apply the changes. Unsaved changes are lost once you finish this wizard.

☐ If you would like to delete a user, mark the corresponding entry in the first column and click "Delete".

Note: The deletion takes place immediately without confirmation.

Manual set up and management

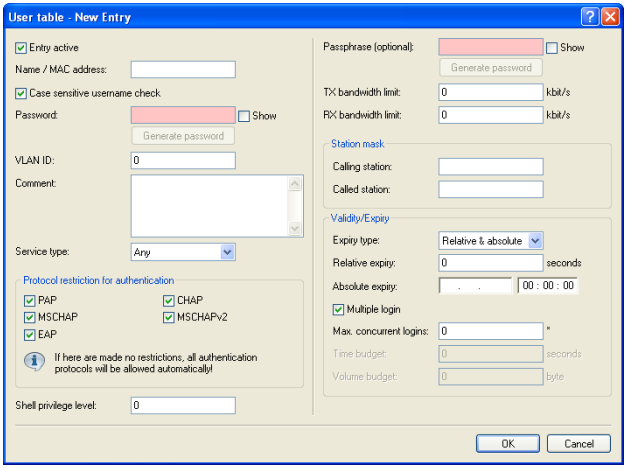
The following configuration steps show you how to use LANconfig to manually setup a Public Spot user for simple scenarios. You create and manage Public Spot users using the "User database" of the device's internal RADIUS server under `RADIUS server : General`. Here you enter all of the users who should have access to the Public Spot – just as the setup wizard does as well.

Note: For user administration, the Public Spot module also has its own internal list (found under `Public Spot : Users : User list`). During technical development, this list was replaced as of HiLCOS 7.70 by the user administration via RADIUS. For compatibility reasons, the device still evaluates the internal user list of the Public Spot module if it is enabled. However, for a new installation you should no longer use this list, since it prevents you from using many features (setup and administration using the wizard, bandwidth restrictions, accounting via RADIUS, VLAN IDs for Public Spot users, etc.).

☐ In "Name" you enter the usernames of future users or the "MAC addresses" of their end devices.

If you selected the authentication mode "Login with name and password", enter the name of the username that the user employs to authenticate on the Public Spot. Entering a "password" is optional, however it is recommended for the authentication mode above.

– LANconfig: `RADIUS server : General : User database`



Note: If the authentication is performed using the MAC address (authentication modus "Authenticate with name, password and MAC address"), you define the MAC address using the field "Calling station" in the format `12:34:56:78:90:AB`.

☐ Set the "Service-Type" to `Login`.

☐ You remove all protocol restrictions by deselecting all check boxes.

Two-phase authentication is not performed in a Public Spot scenario. This only makes sense for direct WLAN connections without Public Spot operations and the associated RADIUS users.

Note: If you do not completely remove the protocol restrictions, a user cannot log in using the login web page of your Public Spot!

☐ Optional: On request, you can also, for example,

- Enter a relative and/or absolute expiry date for the validity of the user account in the section "Validity/Expiry" (relative = validity in seconds after the first login);
- Limit the uplink/downlink under "TX"/"RX bandwidth limit";
- Enable "Multiple login" and enter the "Max. concurrent logins" of end devices

☐ Store the configuration on your device.

That's it! Your Public Spot users can now login with the credentials that you specified.

6.4 Security settings

The Public Spot has two additional safety mechanisms that effectively protect it against abuse.

6.4.1 Traffic limit option

In order for clients to login to the Public Spot via a browser, it must be possible for unauthorized users to transfer data packets (e.g. for DNS requests) to the access point. By default, there is no limit on this data. The following risks are associated with this:

- **Unauthorized use of a Public Spot:** Certain tools enable a user to pack data into a DNS packet (i.e. to establish a DNS tunnel) and to work with the Public Spot without logging in.
- **Denial-of-Service:** The attacker could send large amounts of data to the device and thus try to block the device or Public Spot.
- **Brute force:** The attacker could repeatedly try to access the base station by guessing the login data until successfully breaking in.

The traffic limit option can effectively eliminate these risks.

You enable the traffic limit option by setting a value other than "0". This value determines the maximum data quantity in bytes that can be transmitted between the base station and an unauthorized terminal device.

- LANconfig: `Public Spot : Server : Allow access without authentication : Maximum data volume`

When a terminal device exceeds this traffic volume, the Public Spot locks this device and drops all data received from it without inspection. This lock expires only when the device entry disappears from the station table.

Note: For WLAN devices, this deletion can follow the general idle timeout, for example:Please keep in mind that if station monitoring is active, the lock may be removed earlier. If the mobile station cannot be reached for 60 seconds, the device removes its entry from the station table, and also the block.

- WEBconfig: `HiLCOS menu tree : Setup : WLAN : Idle timeout`

Note: The idle timeout for the Public Spot module has the same purpose as the idle timeout for WLANs, but it applies only to connections via Public Spots. If the idle timeout is set and no further data packages are received from a user, the device automatically logs the device out at the end of the specified time period.

- LANconfig: `Public Spot : Server : Idle timeout`

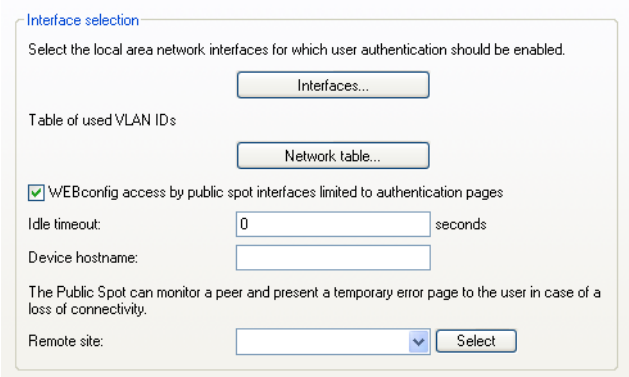
On the one hand the optimal value for traffic limit depends on the data volume of the login page. On the other hand, this value has a significant effect on the potential number of failed login attempts per user. Generally, a traffic limit of 60,000 bytes provides effective protection for a Public Spot but allows a sufficient number of login attempts. You can adjust this value to your individual needs, if necessary. The default value of "0" bytes allows an unlimited volume of data.

Note: The traffic limit option only monitors the traffic before authentication. It does not take into account the traffic to and from a free Web server. This remains unlimited at all times.

6.4.2 Restricting access to the configuration

Public Spot access to a Public Spot network's configuration (WEBconfig) should always be prohibited for security reasons. A special switch allows access via the Public Spot interface to be restricted to the Public Spot authentication pages only. All other configuration protocols are automatically blocked.

- LANconfig: `Public Spot : Server : WEBconfig access by Public Spot interfaces limited to authentication pages`



Note: Note that using permissions under `Management : Admin : Configurations access ways : Access rights` you cannot generally limit the access via HTTP(S) to the device.

6.5 Extended functions and settings

The Public Spot offers a wide range of extended functions, options and parameters, which can be used to adapt it to the specific requirements of the application at hand.

In the following sections you will find information about:

- Multiple logins

  By default, the use of login data is restricted to login with one device. Find out how you increase this limit or completely remove this limit for a user account.

- Open access networks (no login)

  Setup additional networks so that Public Spot users can also reach them without logging in to the Public Spot to provide the user with additional information (e.g., customer web sites inside the company, event calendars in a hotel).

- User administration using the Web API

  Use URLs to create and administrate Public Spot users with file links or scripts.

- Individual bandwidth limitation

  Individually set uplink and downlink restrictions for each Public Spot user.

- Automatic cleanup of user accounts and mobile stations

  Use the device's own functions to automatically delete expired Public Spot user accounts and improperly logged off mobile stations (WLAN only) from the device's internal databases.

- WLAN handover of sessions between devices

  Find out more about the roaming possibilities of mobile stations between access points, and what special configurations are necessary so that your users benefit from the seamless handover of WLAN sessions.

- Authentication via RADIUS

  Find out how you can provide multiple RADIUS servers for authentication and accounting, and how you can chain them, in order to forward the user data to the appropriate backup system in case individual systems are unavailable.

- Accounting for Public Spot connections for commercial operation

  Learn more about the accounting functions provided by the Public Spot for commercial operations. These billing functions can be roughly divided into two models:

  – Retrospective payment for the resources actually used (credit accounting)

  – Service use on a debit payment basis (PrePaid)

- Using multi-level certificates

  Find out how to load certificate chains on your device.

- Individual assignment of VLAN IDs

  Find out how to assign individual VLAN IDs to specific Public Spot users.

6.5.1 Multiple logins

You have the ability to allow Public Spot users to simultaneously sign in using one user account for multiple devices. This can be necessary for a group of people (for example, a family) that has multiple devices, which they would like to use to simultaneously access the Internet.

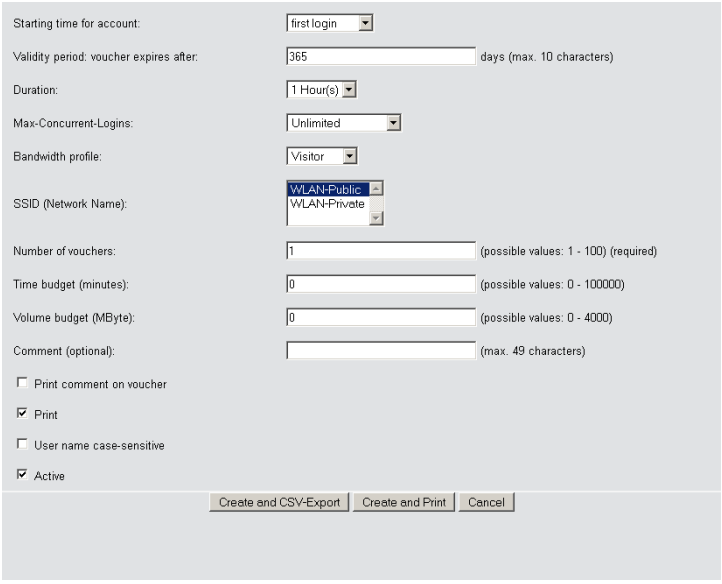
Setting default values

To use this feature, define the number of concurrent devices in the setup menu under `Public Spot module : Add user wizard : Max. concurrent logins table`. Enter the values here that you assigned in the second step with the "Add user wizard". The value `0` stands for "unlimited".

Enabling multiple logins in the new user wizard

When you invoke the Wizard "Create Public Spot account", you will see the menu item "Max concurrent logins". The values shown here correspond to the numbers that you previously entered in the table of the same name. The values are shown within the phrase "Only ... device(s)".

Select the maximum number of concurrent devices that can have access to the user account for the corresponding user. Please note that to enable the feature in the wizard, the option "Allow multiple logins" must also be enabled.



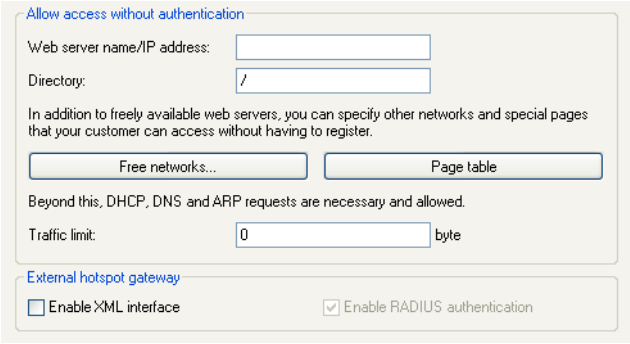
6.5.2 Open access networks (no login)

To provide users with access to important information without them having to login (e.g., important contact information) you can define any publicly available Web server.

- LANconfig: `Public Spot : Server : Web server name/IP Address`

If you do not want to completely release this service, you can optionally define an alternative path to the web server.

- LANconfig: `Public Spot : Server : Directory`

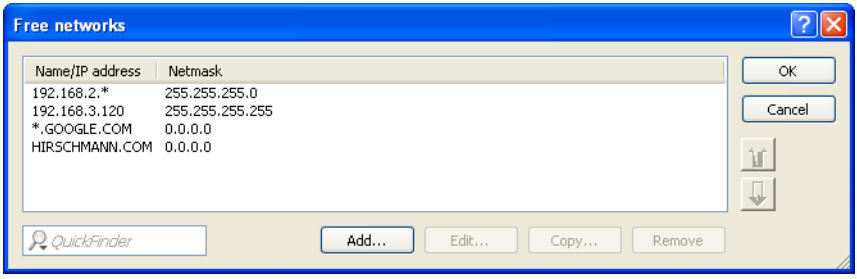


In addition to freely available web servers, you can define other networks and special sites which your customers can access without having to log on.

- LANconfig: `Public Spot : Server : Free networks` or "Page table"
  - "Free networks"

    Enter the IP address of the server or of the network with its netmask, that your Public Spot users are to be given access to. Alternatively, you have the option of entering a domain name (with or without a wildcard "*"). Wildcards can be used, for example, to allow free access to all of the subdomains of a particular domain. The entry `*.google.com` allows the addresses `mail.google.com`, and `maps.google.com`, etc.

    If you wish to authorize a domain or just a single workstation with the address named earlier, set `255.255.255.255` as the netmask here. If you wish to authorize a whole IP network, specify the corresponding netmask. If you do not set a netmask (value `0.0.0.0`), the device ignores the table entry.



  - "Page table"

    Enter the addresses (URLs) of the web pages to be displayed to users on the Public Spot in case of login, error, status display, etc. Read the chapter about “Internal and customized voucher and authentication pages (templates)” on page 559.

DNS snooping

Web services with a high number of users distribute the requests for data to multiple servers for better utilization. This means that two DNS queries for the same hostname (e.g. "www.google.com") can lead to to two different IP addresses. If a Public Spot receives more than one valid IP address for the specified host name from the DNS server, it chooses one of them and stores it for future requests by Public Spot users. If a different IP address for the same host name is allocated to the user by a different server for a subsequent request, the Public Spot blocks this connection because this IP address is not stored as the authenticated one.

In order for Public Spot users to be able to connect to the requested host despite changing IP addresses, the Public Spot analyzes the user's DNS queries and stores the returned IP address with the host name, the valid time to live (TTL), the age and the data source as a free destination address in the table `Status : Public Spot : Free-Hosts` for subsequent use.

The entries in this table will expire after the time period defined in the DNS response (TTL). When the limits are very low (e.g. 5 seconds), you can avoid locking out Public Spot users immediately after a request by setting a minimum validity under `Setup : Public Spot-Module : Free-Hosts-Minimum-TTL`.

6.5.3 Managing Public Spot users via the web API

As an alternative to using the Setup Wizard, entering a special URL in the address bar gives you the option of displaying, creating or deleting Public-Spot users directly.

URL structure

The URL is structured as follows:

```
http://<Device-URL>/cmdpbspotuser/
...?action=actiontodo&parameter1=value1&parameter2=value2
```

The following actions are available:

- **action=addpbspotuser**: Creates one or more new Public Spot users and then prints out the required number of vouchers.
- **action=delpbspotuser**: Deletes the Public Spot user with the specified user ID.
- **action=editpbspotuser**: Displays the Public Spot user with the specified user ID. You can then print out the user's voucher again.

The required parameters and their values depend on the action specified.

Note: The Wizard ignores incorrect parameter information and accepts only the correct parameters. If you omit a required parameter or specify it incorrectly, the wizard displays an input mask. Enter the correct parameter values here.

Adding a Public Spot user

To register a new Public Spot user, simply enter the following URL:

```
http://<Geräte-URL>/cmdpbspotuser/
   ?action=addpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

☐ `comment`

Comment on the registered user

If it is possible to enter multiple comments for a Public Spot user, you can enter the comments and their corresponding comment-field names as follows:

☐ `&comment=<Content1>:<FieldName1>;<Content2>:<FieldName2>;...;<Content5>:<FeildName5>`

If there is just one comment field per user, then the comment is entered as follows:

☐ `&comment=<Comment>`

Note: Special characters such as German umlauts are not supported.

Note: The maximum number of characters for the comment parameter is 191 characters.

- ☐ `print`

  Automatic print-out of the voucher.

  If this parameter is omitted, the wizard displays a button that you can use to print the voucher.

- ☐ `printcomment`

  Print the comment on the voucher.

  If this parameter is omitted, no comment will appear on the voucher (default setting).

- ☐ `nbGuests`

  Number of Public Spot users to be created.

  If this parameter is omitted, the wizard creates one user only (default setting).

- ☐ `defaults`

  Use default values

  The wizard replaces missing or incorrect parameters with default values.

- ☐ `expirytype`

  Combined output of expiry type and, if applicable, the validity period of the voucher.

  Specify this parameter as follows:

- ☐ `&expirytype=<Value1>+validper=<Value2>`

  The parameter values have the following meaning:

  - `Value1`: Expiry type. Possible values are `absolute`, `relative`, `both`, and `none`.
  - `Value2`: Time of the voucher's expiry if `expirytype` has the value `both`. In this case, you use `validper` to specify the voucher's maximum validity period in days for the absolute expiry type. For all other expiry types, the parameter `validper` is not set.

  If a parameter is omitted or set with incorrect values the wizard will apply the default values.

☐ `ssid`

Network name

If this parameter is omitted, the wizard uses the default network name (default setting).

☐ `unit`

Access time

Specify this parameter as follows:

☐ `&unit=<Value1>+runtime=<Value2>`

The parameter values have the following meaning:

– `Value1`: LIfetime units. Possible values are: Minute, hour, day

– `Value2`: Duration

☐ `timebudget`

Time budget

If this parameter is omitted, the wizard uses the default value.

☐ `volumebudget`

Volume budget

If this parameter is omitted, the wizard uses the default value.

☐ `multilogin`

Multiple logins

If you specify this parameter, the user can login multiple times with his/her user account. If this parameter is missing, multiple logins are disabled by default.

☐ `maxconclogin`

Maximum number of concurrent logins

With this parameter you specify with how many different end devices a user can login to a Public Spot. Valid entries are integers such as `0, 1, 2, ...`.

If this parameter is missing or if the parameter has the value `0`, this means that the number of devices is unlimited.

Note: This parameter requires that multiple logins be enabled. Setting this parameter in isolation has no other effects.

☐ `casesensitive`

User name case-sensitive:

If you enter this parameter, the Public Spot user must pay attention to capitalization when entering the user name at login. Valid values are:

– `0`: Case-sensitive username is disabled

– `1`: Case-sensitive username is enabled

If this parameter is omitted, the wizard uses the default value.

☐ `bandwidthprof`

Bandwidth profile

With this parameter you assign a pre-defined bandwidth profile to a Public Spot user. Enter the valid value for this parameter as the line number of an existing profile name under `Setup : Public Spot module : Add user wizard : Bandwidth profiles`, such asto index the first entry in the table.

☐ `&bandwidthprof=1`

If this parameter is missing or the line number is invalid (for example, the table is empty), the wizard does not limit the bandwidth.

Note: If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Modifying a Public Spot user

Modify one or more Public Spot users simply by entering the following URL:

```
http://<device-URL>/cmdpbspotuser/
...?action=editpbspotuser&parameter1=value1&parameter2=value2&...
```

The following parameters are available:

☐ `pbspotuser`

Name of the Public Spot user

Specify multiple users in the form `&=pbspotuser=<User1>+<User2>+....`

If the wizard cannot find the specified user, you have the option to search for a user.

After making your changes, accept these and print them out if necessary.

☐ `expirytype`

Combined output of expiry type and, if applicable, the validity period of the voucher.

Specify this parameter as follows:

☐ `&expirytype=<Value1>+validper=<Value2>`

The parameter values have the following meaning:

– `Value1`: Expiry type. Possible values are `absolute`, `relative`, `both`, and `none`.

– `Value2`: Time of the voucher's expiry if `expirytype` has the value `both`. In this case, you use `validper` to specify the voucher's maximum validity period in days for the absolute expiry type. For all other expiry types, the parameter `validper` is not set.

If a parameter is omitted or set with incorrect values the wizard will apply the default values.

☐ `unit`

Access time

Specify this parameter as follows:

☐ `&unit=<Value1>+runtime=<Value2>`

The parameter values have the following meaning:

– `Value1`: LIfetime units. Possible values are

Minute

Hour

Day

– `Value2`: Duration

☐ `timebudget`

Time budget

If this parameter is omitted, the wizard uses the default value.

☐ `volumebudget`

Volume budget

If this parameter is omitted, the wizard uses the default value.

☐ `print`

Automatic print-out of the voucher.

If this parameter is omitted, the wizard displays a button. Use this to print out the voucher.

☐ `bandwidthprof`

Bandwidth profile

With this parameter you assign a pre-defined bandwidth profile to a Public Spot user. Enter the valid value for this parameter as the line number of an existing profile name under `Setup : Public Spot module : Add user wizard : Bandwidth profiles`, such asto index the first entry in the table.

☐ `&bandwidthprof=1`

If this parameter is missing or the line number is invalid (for example, the table is empty), the wizard does not limit the bandwidth.

Note: If the Public Spot administration contains no default values to replace missing parameters, the wizard opens a dialog. Enter the missing values here.

Deleting a Public Spot user

Delete one or more Public Spot users simply by entering the following URL:

```
http://<deviceURL>/cmdpbspotuser/
...?action=delpbspotuser&pbSpotuser=<User1>+<User2>+...
```

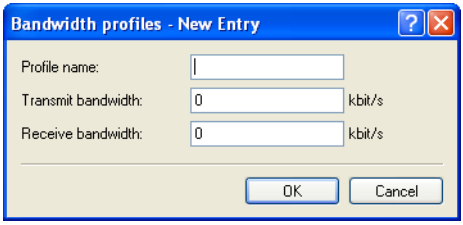
If the wizard finds the specified user in the user list, the user is deleted and the wizard displays a confirming message.

If the wizard cannot find the specified user, it displays a table of registered Public Spot users. Mark the entries for deletion here.

6.5.4 Bandwidth profile

Manage bandwidth profiles

Using the window `Public-Spot : Wizard : Bandwidth profiles`, you have the ability to set up profiles that limit the available bandwidth (uplink and downlink) for Public Spot users. These profiles can be assigned to new users when access is created for the Public Spot by calling the Setup-Wizard "Cerate Public Spot account" in WEBconfig.



In order to edit the entries in the table "Bandwidth profiles", click on the button "Add...". The entries in the edit window have the following meaning:

- "Profile name": Enter the name for the bandwidth profile here.
- "TX bandwidth": Enter the maximum uplink bandwidth (in kbps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value `1024`.
- "RX bandwidth": Enter the maximum downlink bandwidth (in kbps), which should be available to a Public Spot user. To limit the bandwidth, for example, to 1 Mbps, enter the value `1024`.

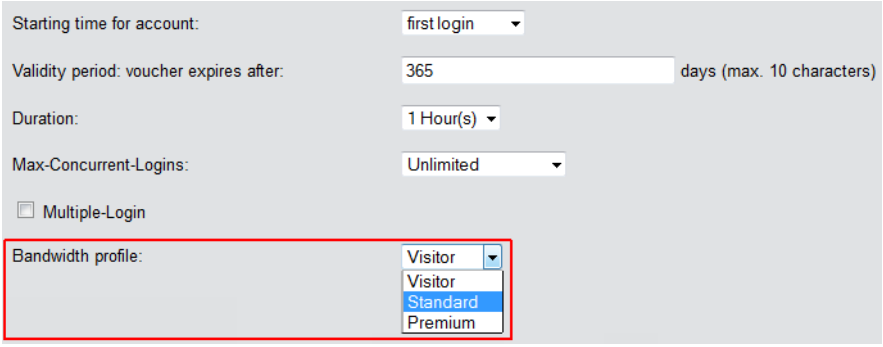
Assigning bandwidth profiles

The following steps describe how you assign the available bandwidth profiles to a Public Spot user.

☐ Open WEBconfig.

☐ Start the add user wizard under `Setup Wizards : Create Public Spot account`.

☐ Assign the new user an appropriate profile from the selection list "Bandwidth profile".



When creating a new user, the RADIUS server automatically assigns the upper and lower boundaries of the bandwidth profile (not the bandwidth profile per se) to the associated account.

6.5.5 Clear user list automatically

The device gives you the option to delete expired accounts for Public Spot users automatically.

Users of the Public Spot Wizard are generally administrators with restricted rights who are often unable to delete user table entries themselves. Because the user table has a limited number of entries, outdated entries could limit the capacity of the Public Spot. We strongly recommend that you activate this option.

If you use the internal RADIUS server for the administration of user accounts, enable automatic clean-up under `RADIUS server : General : Clear user lists automatically`

Note: These settings have no effect on the user table on an external RADIUS server.

6.5.6 Station monitoring

If station monitoring is activated, the Public Spot regularly checks to see if the associated end devices are still available. Lost end devices are automatically deleted from the local user table. If station monitoring is switched off, a user is not logged off until the validity period of the user's authentication expires.

Note: Station monitoring is extremely important for Public Spots operating commercially on a time basis. In installations of this type, users must be assured that they are only paying for the time actually spent using the Public Spot services.

Configuration

Station monitoring for the Public Spot Module is disabled by default. You activate it by entering a value greater than `0` – this value disables the function – under `Public Spot : Server : Interface selection : Idle timeout`. From this point on, all end devices are automatically disconnected from the Public Spot after a specific time.

Note: If your device has WLAN, you also have the option of enabling station monitoring globally for all WLAN interfaces. You can find the corresponding settings under `Wireless LAN : Security : Monitor stations to detect inactive ones`. To do this, the device disconnects mobile stations after 60 seconds (default value). If WLAN station monitoring is disabled, this may take up to an hour.

If you offer Public Spot via WLAN, please note that the station monitoring of the WLAN takes priority over that for the Public Spot, and a disconnection can occur earlier if the idle timeout for WLAN (configurable in the Setup menu under `WLAN : Idle timeout`) is less than that for the Public Spot.

Surveillance

You can monitor the Public Spot during operation using WEBconfig. The station table in the user authentication menu provides an overview of:

- Users currently logged in to the Public Spot and
- End devices in the WLAN which are not logged in.

You can navigate to the Station table in the Status menu under `Public Spot : Station Table`. Using the button "Monitor this table" you automatically refresh the table display at regular intervals.

6.5.7 WLAN handover of sessions between devices

Whenever a site equipped with WLAN hotspots expands, it may be necessary to deploy more than one access point to cover the whole area. One option would be to use a central device as an authentication gateway, enable the Public Spot option on this device only, and require all other access points to redirect requests to the central device. In this way, all other access points act as simple, transparent bridges, which connect to the central gateway using the Ethernet backbone. This allows clients to freely roam among the access points since all session information is kept in the central gateway.

This variant has two drawbacks, however:

- The central gateway is a single point of failure, and is not scalable. You can reduce the risk of failures by using VRRP to create a redundancy solution.

  Note: This solution requires an external RADIUS server, since VRRP cannot synchronize configurations, e.g. the user database. However, this means that certain functions (such as the Public Spot wizards in WEBconfig) are no longer available.

- Roaming is only necessary when the Public Spot module is installed on the access points themselves. Using a WLC, the authentication can be forwarded to the central gateway. In this case, the roaming between access points is transparent to the WLAN controller.

An alternative to this type of centralized setup is to enable the Public Spot module in all of the access points. Authentication and page processing handling is thereby distributed over all devices, and a single point of failure is eliminated.

IAPP (inter access point protocol)

Since the Public Spot module is implemented as a "switchable" transparent bridge, there is no need for clients to acquire a new IP address after they roamed to another access point, so there is no need to terminate open connections. This results in the requirement that an already authenticated client does not have to re-authenticate after roaming to a new access point. Thus the authentication information should be carried over from the old to the new access point.

Access points use the IAPP (inter access point protocol) to share information about roaming clients: Whenever a wireless client decides to change to another access point, it has the option of informing the new AP about which AP it was previously connected to. This information, combined with regular Hello packets on the Ethernet backbone, enable the new access point to inform the old access point. The old access point can then remove the client from its station table and acknowledge the handover.

If a client does not use the corresponding Reassociate packet for connecting to the new access point, the new access point sends a handover request as a multicast on the backbone, instead of a directed packet to the old access point. This means that this handover also works for clients that do not support IAPP.

The main task of the IAPP in a WLAN is to tell the old access point not to send any more packets to the corresponding client in its wireless area, since it will no longer receive them. This type of behavior (based on the definition of the 802.11 frame exchange protocol) could otherwise cause problems with other clients that are connected with it.

In case of an enabled Public Spot module, the communication channel provided by IAPP is used to transport the session information of wireless clients. Whenever an access point receives a handover request for one of its wireless clients, and if a session record for this client is available in its station table, it will append state information about this client to the requesting access point. This information includes:

- The client's current state (authenticated or not authenticated)

  In case the client is authenticated, it also includes:

  – The username used to authenticate
  – The amount of data traffic generated by the client so far
  – The session duration so far
  – The IP address of the client
  – Possible limits on the session duration and data volumes
  – Possible information about idle timeouts

- If RADIUS accounting was used for the session:

  – The entry used for RADIUS accounting in the authentication server list, referenced by name
  – The accounting cycle used for interim updates

After a successful transfer, the old access point terminates the session, which, in the case of RADIUS accounting, means that it sends an accounting stop request to the RADIUS accounting server. This is necessary since a RADIUS server can use the NAS identification to associate requests with specific sessions, and these requests can no longer be associated with the correct sessions once the data packets for a session come from more than one device. If an access point receives this information in a handover reply, it immediately marks the client as authenticated and starts a new RADIUS accounting session, if possible.

Note: Note that the new access point requires a corresponding entry in its "Authentication server" list in order to receive the necessary information. The specific part of the handover reply for the Public Spot module is protected by a shared secret, which is set in the setup menu under `Public-Spot-Module : Roaming-Secret`. These security measures should prevent falsification of handover replies. Without a password configured, the access point does not append the information above on a handover reply, which forces the client to authenticate again.

6.5.8 Authentication via RADIUS

RADIUS is an extensively accepted protocol for providing large groups of users access to a server. Although it was originally developed for dial-in server access over telephone lines, the concept is also useful for the hotspot authentication process. For that reason, it can be used in a more complex provider network, for example, to provide access for the same users via dial-in and hotspots. You configure RADIUS servers and their access parameters in the dialog `Public Spot : Server` under "Authentication servers".

In certain scenarios, it can be feasible to use more than one RADIUS server. In general, a RADIUS server is specified by its IP address, the UDP port the RADIUS service is bound to (typical ports are 1645 or 1812), and a so-called "shared secret". This is a random character string which acts as a password for access to the server. Only clients which know the shared secret can interact with the RADIUS server, since the password for the user account is hashed instead of being sent in plain text.

In theory, the simplest possible RADIUS transaction consists of the device sending the entered account data (user name + password) to the RADIUS server and the RADIUS server responding with either "yes" or "no". However, the RADIUS protocol also allows more complex responses and requests where the communication partners use a list of variables – so-called "attributes" – for requests and responses. In the section “Commonly transmitted RADIUS attributes” on page 595 there is a list of which attributes a device can send to a RADIUS server and which attributes from a RADIUS response are understood by the device.

Multiple authentication servers

As mentioned previously, the list of authentication servers can contain more than one entry. There may be situations where the hotspot provides access to the Internet for customers from different service providers. These providers may have separate user databases and their own RADIUS servers. The device must select which provider corresponds to the user based on the username.

Whenever the device does not find an entry for an authenticated user in its local table, it will first search through the authentication server list to find the provider that corresponds to the user. For example, user account names like `JohnDoe@mydomain.de` contains the authentication server entry named `MYDOMAIN`. If the first allocation does not work, the device attempts to allocate the entry `DEFAULT` to the user. If this entry also does not exist, the device selects the authentication server that is first in the list. If the device does not find an entry (i.e., the list is empty), the user authentication fails.

Depending on the allocation of a user to a authentication server, your device always transmits the complete username to the selected RADIUS server. The selected RADIUS server is stored as the provider for the subsequent session and used for optional RADIUS accounting.

Chaining of backup servers

Internet access providers wish to provide a very high level of availability, and a common method to achieve this relies on redundancy. This redundancy is achieved using the backup servers which are needed when a request times out on the primary server, for example, because the server or another network component along the way was unavailable.

The requirements for backup servers varies widely among the different providers, which is why the list of authentication servers does not have a specific number of input fields. Instead, the device offers you a series of backup servers (backup chaining). Here, two or more entries in the authentication server table may be chained together to form a list of RADIUS servers. The device looks through the list of RADIUS servers one by one until the end of the list is reached (authentication failure due to server unavailability) or a response from a server (either positive or negative) is obtained.

You chain backup servers using the input field "Backup name" in the add/edit dialog under `Public Spot : Server : Authentication server`. Whenever a RADIUS request fails (i.e. times out), the device checks the backup field, and continues to try the RADIUS server specified in the entry that is referenced by the backup name. In general, an unlimited number of servers can be connected this way, which makes it possible for several providers to assign the same fallback server. The chain of backup servers is considered to be terminated if one of the following conditions occurs:

- Querying a RADIUS server failed and the corresponding authentication server table entry has an empty backup field.
- Querying a RADIUS server failed and the corresponding provider table entry has an invalid backup field, i.e. the entry referenced is not present in the authentication server list.
- Querying a RADIUS server failed and the corresponding authentication server list entry refers to an entry that has already been used in the query process. This avoids endless RADIUS requests due to circular references. It is possible to specify two RADIUS servers that reference each other as backups, with the primary server being selected by the user account name.

Note: While the device is sending a RADIUS request, the TCP/HTTP connection to the client still exists. If the runtime of the chaining exceeds the lifetime of the TCP/HTTP connection, the client interrupts the login attempt. Therefore, it may be recommended to reduce the number of request retries to the individual backup servers as well as the time intervals between requests. These settings can be made in `RADIUS server : Options`.

6.5.9 Billing without a RADIUS accounting server

If user administration is performed using the internal user list of the Public Spot module, and you do not want to use a RADIUS accounting server, your only option is to use the expiry date of the user account for accounting purposes.

The use of the internal user list is no longer recommended. Instead, in order to take advantage of all of the options the Public Spot offers, you should use the internal RADIUS server for new installations.

Note: For the purposes of billing by credit payment, the Public Spot can use SYSLOG to output detailed connection information to any computer in the network. Using the appropriate software on the destination computer allows you to precisely bill the resources that were actually used (such as connection times or transfer volumes).

6.5.10 Billing via RADIUS accounting server

For the purposes of billing via a RADIUS server, you can set up the Public Spot so that it regularly supplies the current connection information for every active user to the specified accounting server. Accounting is started when a client is authenticated using RADIUS and a valid "Accounting server" is configured for the relevant "Authentication server" in the list of "Authentication servers". It is possible to use different RADIUS servers for authentication and accounting.

Each of the regular message packets to the accounting server contains information about the resources (time, transferred data volumes, etc.) consumed by the user since the last message. This means that, even in the worst case of a Public Spot failure (e.g., due to a power outage or similar), only a small amount of accounting information will be lost.

Periodic messaging of accounting information to the accounting server (interim updates) is deactivated by default. It is activated by setting a value for the accounting cycle which is greater than 0.

- LANconfig: `Public Spot : Users : Update cycle`

Note: This cycle is defined in seconds. This sets the time interval of when your device regularly sends connection information to the accounting server. Setting the cycle to `0` deactivates this function. If this is the case, your device only sends accounting information at the beginning and end of the session.

When accounting on a prepaid basis, the RADIUS server monitors the restrictions on the users (limits on connection times or transfer volumes, expiry date). As soon as a user has used up the prepaid amount, the RADIUS server locks the user account. Your device rejects future login attempts for the user.

Note: Time limits for prepaid models can be monitored by the Public Spot during active sessions. If a time limit is exceeded, the Public Spot automatically terminates the corresponding session. The monitoring of prepaid amounts is possible if the RADIUS server transmits the user's time credit to the Public Spot as the "Session timeout" attribute at the start of the session.

Request types

Your device is able to send different types of RADIUS requests to an accounting server. These requests differ according to a user's session state:

- An accounting start request is sent after a successful authentication.
- An accounting stop request is sent after a Public Spot session is terminated.
- Optional: Interim updates are sent throughout the session.

There are two types of interim updates: An initial update is sent immediately after the start request since some RADIUS servers need this in order to create a session in the accounting database. All further updates depend on whether an accounting cycle was created for the respective session (see `Public Spot : Users : Accounting update cycle`).

Alternatively, this value may be included in a RADIUS authentication response: The RADIUS server offers the RADIUS client (for example, your Public Spot) an interim accounting interval, which the client will use if it has the appropriate support for this and as long as no interval was set locally on the device itself.

Note: If a local value was set, it will always be given a higher priority than the one received from a RADIUS server, which the RADIUS RFCs require by default!

In the section “Commonly transmitted RADIUS attributes” on page 595 there is a list of which attributes a device can send to a RADIUS server and which attributes from a RADIUS response are understood by the device.

Accounting backup

The backup solution for RADIUS accounting is the same as the one for RADIUS authentication, in that your device goes through the entries in the authentication server list one by one (see chapter “Chaining of backup servers” on page 482). The backup entries for the accounting server should be chosen with the same care as for the authentication server: If you are using multiple backups, you will probably have to reduce the timeout/try values for the requests in order to achieve reasonable response times for the entire system.

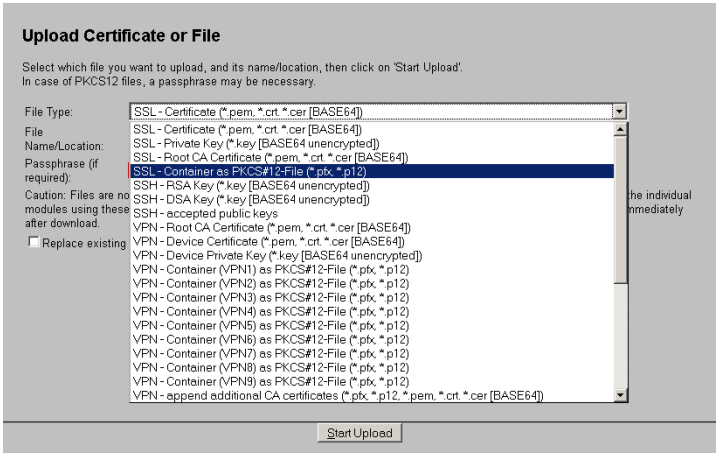
Note: User sessions are not paused while the device sends accounting requests, which consumes additional resources in the device—in contrast to authentication. Please ensure that the time required for the selection of an accounting server* should be less than the length of an accounting cycle for interim update requests. This stops the requests from queuing up, which would result in a stack overflow.

* Number of backups x (idle timeout + number of retries)

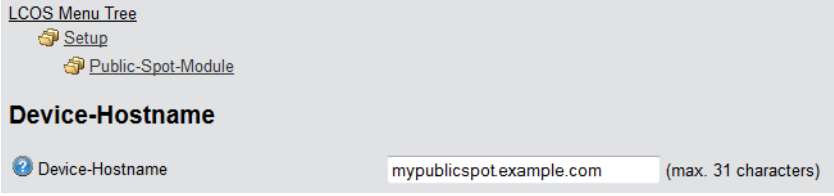
6.5.11 Multi-level certificates for PublicSpots

SSL certificate chains can be loaded into the device as a PKCS#12 container. These certificate chains can be used for Public Spot authentication pages by using the HTTPS server implemented in the device. Certificates from recognized trust centers are normally multi-level. Officially signed certificates in the Public Spot are necessary to avoid certificate-related error messages from the browser when authenticating at a Public Spot.

The certificate is loaded into the device for example by using WEBconfig in File Management to upload the individual files of the root CA certificate or a PKCS#12 container:



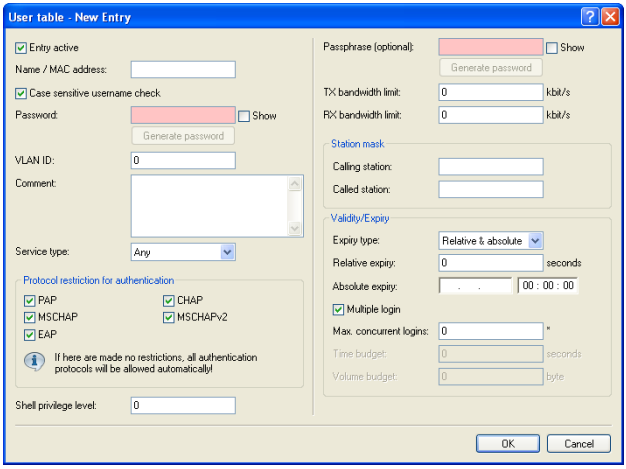
Certificates are normally issued for DNS names, so the Public Spot must specify the certificate's DNS name as the destination and not an internal IP address (enter in `Setup : Public Spot Module : Device Host Name`). This name has to be resolved by the DNS server to provide the corresponding IP address of the Public Spot.



6.5.12 Assigning users to individual VLANs

Regardless of the assignment of a VLAN ID for the entire Public Spot module, the device offers you the option of separately assigning individual VLAN IDs for individual Public Spot users. This ID is automatically assigned by the RADIUS server to your users after successful authentication. In this way it is possible, for example, to classify different Public Spot users in separate networks with different access rights and access options without having them login to separate SSIDs or requiring you to publicize the availability of various networks (e.g., networks for different customer types). The relevant rules can be realized via the firewall by specifying the VLAN ID of the respective user/the relevant user groups as the source tag.

Note: An enabled VLAN module is a prerequisite for the functions described above.



- Open the "User table" in the dialog "RADIUS server ""General" and click "Add..." to create a new user.
- Assign an individual VLAN ID to the new user with the input field "VLAN-ID". After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the interface. The value `0` disables the assignment of an individual VLAN ID.

Note: For technical reasons, the assignment of a VLAN ID requires a new address assignment by the DHCP server. As long as a client is not yet assigned a new address after successful authentication, the client is still in the previous (e.g., untagged) network. In order for the clients to be transferred to the new network as quickly as possible, it is necessary to set the lease time of the DHCP server as low as possible under `IPv4 : DHCPv4`. Possible values (in minutes) include, for example:

- "Maximum lease time:"`2`
- "Default lease time:"`1`

Take into account that a strong reduction in global lease time can flood your network with DHCP messages, and when there is a larger number of users, it leads to an increased network load! Alternatively, you have the option of using an external DHCP server or allowing your users to manually request a new address by using their client. In the Windows command line this is done, for example, using the commands `ipconfig /release` and `ipconfig /renew`.

Note: By assigning a VLAN-ID, the user loses his connection after the initial DHCP lease expires. The connection only remains stable as of the second lease, i.e. after successfully assigning the VLAN-ID.

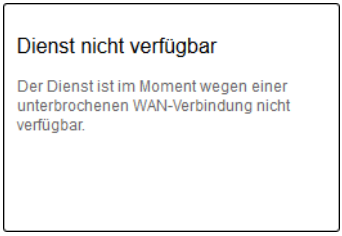
6.5.13 Error page in case of WAN connection failure

In addition to the general login error pages, you can also inform non-authenticated Public Spot users of a WAN connection error. Potential users are informed about the lack of network availability beforehand. This "Error" page is displayed whenever the Public Spot module registers a WAN link failure.

In order for the error page to be displayed properly, a corresponding remote site **must** be named, the connection to which is monitored by the Public Spot module. Make an appropriate entry in the dialog `Public Spot : Server`"Remote site". The "Select" button allows you to assign an existing entry to the input field, or to create a new remote site.

Note: If no remote site is named for monitoring, the Public Spot module disables the display of the connection error page. If the WAN connection fails, unauthenticated will not see an error page and their browsers will timeout instead.

On your custom error page, use the identifier `LOGINERRORMSG` to insert the error message issued by HiLCOS in case of a WAN link failure. In the event of a WAN link failure, the following error message is displayed:



Users who are already authenticated will see an appropriate error message from their browser.

6.6 Alternative login methods

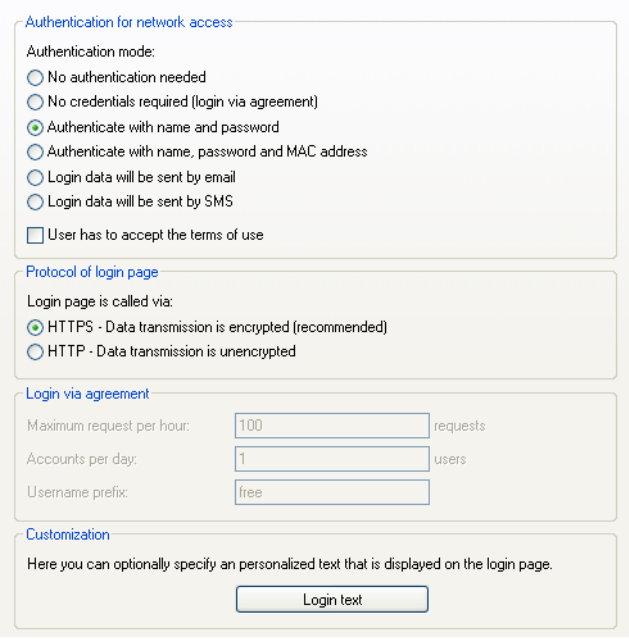
In addition to logging-in with previously provided credentials, your users can also independently request the receipt of login data via e-mail or text message (SMS), or by gaining instant access to the Public Spot by means of Login via agreement. Alternatively, in order to implement more complex or multi-level login scenarios, you can also link your Public Spot to other software systems using the XML or PMS interface (module optionally available).

You can also offer your users additional convenience by allowing, for example, automatic login processes (automatic login as well as re-login using a MAC address, login using WISPr, Hotspot 2.0), and also the related roaming services.

Note: Hotspot 2.0 and roaming features are only available in conjunction with WLAN.

6.6.1 Overview of authentication modes

There are various ways to login to the Public Spot. The network access authentication setting is located in the dialog `Public Spot : Authentication`.



The following authentication modes are available:

- "No authentication required"

  Users get free access to the Public Spot, authentication is not required.

  Note: Do not use this setting if your device has unlimited access to the Internet.

- "No credentials required (login after agreement)"

Users get free access to the Public Spot after they agree to the operator's terms. With a RADIUS server, login is completely transparent for the user. The prerequisite is that you have set up an individual template page (a welcome page with a Login via agreement): In this case, the Public Spot initially forwards a user to the Welcome page. After the user agrees to the terms, the device automatically creates a user account in line with the default values set under `Public Spot : Wizard` and grants access to the connected network.

Once you have select this login mode, the dialog section "Login via agreement" becomes available, where you can set additional conditions for the creation of free user accounts by the RADIUS server:

– "Maximum requests per hour": Specify how many users per hour can automatically create an account on the device. Decrease this value to reduce performance degradation caused by an excessive number of users.

– "Accounts per day": Specify how many accounts a user may create per day. If this value is reached and the user session has expired, a user can not automatically register and get authenticated on the Public Spot for the rest of the day.

– "Username prefix": Enter a prefix which can be used to identify the user in the RADIUS user table that the device created automatically after confirmation of the terms of use. This prefix is placed directly in front of the "User name pattern" specified under `Public Spot : Wizard`.

Note: The terms featured on the Welcome screen are not to be confused with the terms-of-use page itself. The "Terms of use" page is an extra page that becomes available when certain login modes are activated (see “Possible authentication pages” on page 559). If no Welcome page has been set up (see “Configuration of user-defined pages” on page 569), the device displays an error message when accessing the Public Spot.

▶ "Authenticate with name and password"

Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher.

▶ "Authenticate with name, password and MAC address"

Users log on to the Public Spot with their name and their password. Users get their login data from a network administrator as a voucher. For this login mode, the MAC address of the client must also match the one stored in the user list by the administrator.

- "Login data will be sent by e-mail"

  Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent via e-mail. No action by an administrator is necessary. Learn more about this login mode under “Independent user authentication (Smart Ticket)” on page 496.

- "Login data will be sent by SMS (text message)"

  Users log on to the Public Spot with their name and their password. Users generate the credentials themselves, and the data is sent by SMS (text message). No action by an administrator is necessary. Learn more about this login mode under “Independent user authentication (Smart Ticket)” on page 496.

For some login modes, the option "User has to accept the terms of use" allows you to combine the login with an acceptance of the terms and conditions. In this case, the Public Spot login page displays an additional option, which prompts the user to accept the terms of use before registering or logging in. Users who do not explicitly agree to these terms and conditions are unable to login to the Public Spot.

Note: Remember to upload a page with terms and conditions onto the device before you enable this option. Otherwise, the device will only show the user a placeholder instead of the terms and conditions.

6.6.2 Independent user authentication (Smart Ticket)

Devices operating a Public Spot provide users with time-limited access to certain networks, typically the Internet. In many scenarios, a limited administrator account is used for the creation of these accounts: For example, a hotel employee at the front desk can use an account that only has the functional rights to create and manage Public Spot users. With a few mouse clicks the employee can print a voucher for the hotel guests granting them network access.

However, the convenient voucher solution still requires action from an administrator. Alternatively, you can give the users the option to generate their own login data for the wireless network, and send it to themselves by e-mail or SMS (login by "Smart Ticket").

Login via agreement

Alternatively, the device gives you the ability to handle the login for Public Spot users transparently using a RADIUS server. In this case, the user login is preceded by a request to consent to the agreement before the user automatically receives access to the Public Spot. The creation of credentials by the user via e-mail or SMS does not apply for this authentication method. Learn more about this in the section under “Overview of authentication modes” on page 492—the "Login via agreement" is not a part of the Smart Ticket function.

Configuring e-mail authentication

The settings for transmitting the login credentials to the e-mail address specified by the user are adjusted in the dialog `Public Spot : Email`. The following steps show you how to correctly configure e-mail authentication.

Note: In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under `Log & Trace : SMTP account` and `Log & Trace : SMTP options`.

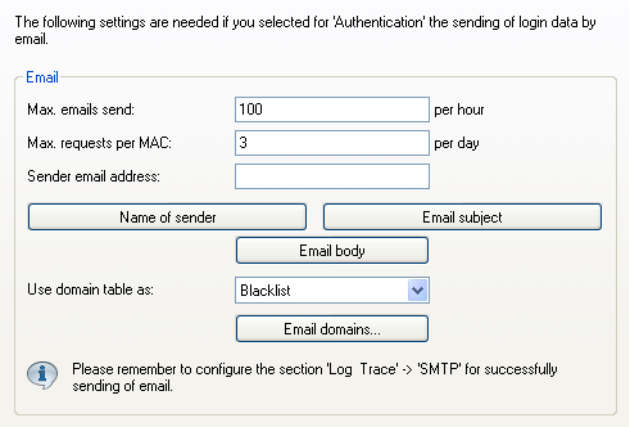
In addition, you can specify individual text blocks used by the device to send the login credentials; see “Customizing text message content” on page 502. By default, the device inserts predefined text modules; for an overview of these see “Standard texts for e-mail sender, subject line and body” on page 504.

☐ Start LANconfig and open the configuration dialog for the device.

☐ Change the view to `Public Spot : Authentication`.

☐ Change the login mode to "Login data will be sent by email".

☐ Change the view to `Public Spot : Email`.



☐ Under "Max. emails send" you enter the maximum number of e-mails that the Public Spot module may send per hour to users authenticating via e-mail. Lower the value to reduce the number of new users per hour.

☐ Under "Max.requests per MAC" you specify how many different sets of credentials the device can provide to a MAC address within one day.

☐ Under "Sender e-mail address" enter the return address that your Public Spot users will see when the e-mail is delivered, e.g. `support@providerX.org`.

☐ Specify whether the device uses the table "Email domains" as a blacklist or whitelist with the selection item "Use domain table as".

This definition sets which e-mail addresses or domains may be entered by your Public Spot users in order to register.

– "Blacklist": Registration is permitted on all e-mail domains except those in this table.

– "Whitelist": Registration is possible only via the e-mail domains that are present in this table.

Note: Please note that a Public Spot operating with an empty whitelist will black-list (reject) all domains.

☐ Use the "Email domains" table to define the e-mail domains that you allow or prohibit in the case of logins by your Public Spot users via e-mail. Enter domains in the format `@web-domain.com`.

☐ You can write the configuration back to the device.

Configuring SMS authentication

The settings for transmitting the login credentials as an SMS text message to the phone number specified by the user are adjusted in the dialog `Public Spot : SMS`. The choices available to you vary according to the device type:

- The credentials are sent as an SMS text message via the 3G/4G WWAN module in another device,
- The access credentials are sent as an e-mail to an external E-Mail2SMS gateway, which then converts the e-mail to SMS.

The following steps show you how to correctly configure the different variants of SMS authentication.

Note: In order to send login data as a text message via a 3G/4G WWAN-capable device, the internal SMS module of this device must be set up under `Log & Trace : SMS messages`.

Note: SMS transmission is suitable for installations with a maximum throughput of 10 SMS per minute.

Note: In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under `Log & Trace : SMTP account` and `Log & Trace : SMTP options`.

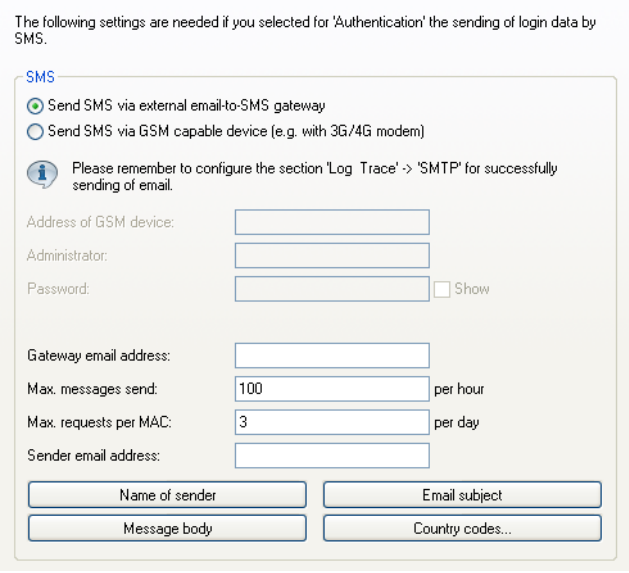
In addition, you can specify individual text blocks used by the device to send the login credentials; see “Customizing text message content” on page 502. By default, the device inserts predefined text modules; for an overview of these see “Standard texts for e-mail sender, subject line and body” on page 504.

☐ Start LANconfig and open the configuration dialog for the device.

☐ Change the view to `Public Spot : Authentication`.

☐ Change the login mode to "Login data will be sent by SMS".

☐ Navigate to the menu item `Public Spot : SMS`.



☐ Specify how the device sends SMS text messages.

– In order to send the login credentials as an SMS text message via the 3G/4G WWAN module of another device, you first carry out the steps in the section “Operating devices with the 3G/4G WWAN module as an SMS gateway” on page 501 and then continue with the next main step in the configuration.

– In order to send the login credentials to an external E-Mail2SMS gateway, select the setting "Send SMS via external e-mail-to-SMS gateway" and then continue with the next main step in the configuration.

Under "Gateway e-mail address" you enter the IP address or the hostname of the gateway server, which converts the e-mail into SMS. If the provider expects to find the mobile phone number in the local part of the e-mail, you can use the variable `$PSpotUserMobileNo`.

Under "Sender e-mail address" enter the return address that your Public Spot users will see when the SMS is delivered, e.g. `support@providerX.org`.

☐ Under "Max. messages send" you enter the maximum number of SMS text messages that the Public Spot module may send per hour to users authenticating via SMS. Lower the value to reduce the number of new users per hour.

☐ Under "Max.requests per MAC" you specify how many different sets of credentials the device can provide to a MAC address within one day.

☐ Under "Country codes" you enter the international code numbers that the Public Spot will accept when sending data via SMS.

Country codes can be entered directly or with a prefixed double-zero, for example for Germany `49` or `0049`.

Note: This table acts as a whitelist. You must define country codes in order for the login data to be delivered.

☐ You can write the configuration back to the device.

Operating devices with the 3G/4G WWAN module as an SMS gateway

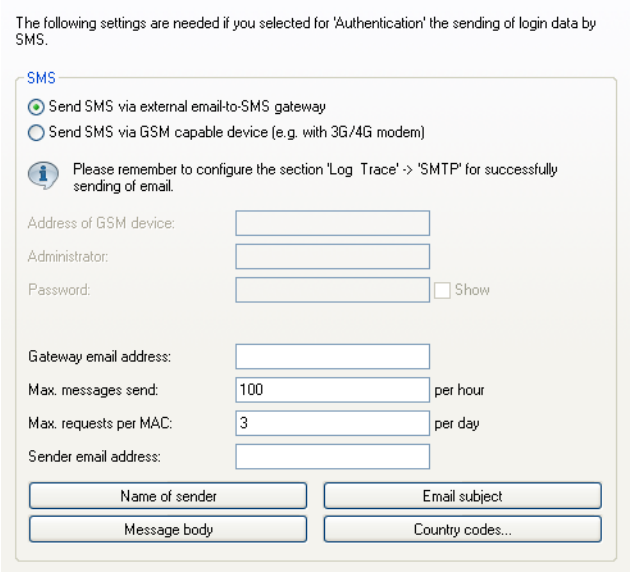
When using Public Spot authentication via SMS (Smart Ticket), you have the option of sending access credentials via the 3G/4G WWAN module in a further device instead of using an external E-Mail2SMS gateway. To use this option, you must store the address and the access credentials for the 3G/4G device on the device that provides the Public Spot. For the purpose of sending the SMS, the Public Spot module uses a URL call to send the credentials and the text message to the external 3G/4G device.

The option is available on devices both with and without their own 3G/4G WWAN module. These options allow you to chain multiple devices together and to set up your own transmitting device if you operate multiple Public Spots or use a device without a 3G/4G WWAN module.

☐ Start LANconfig and set up the SMS module on the 3G/4G device that is to serve as an SMS gateway. In addition, we recommended that you create an administrator without access rights (select "None") and with just one function right, "Send SMS".

☐ Open the configuration dialog for the device that provides the Public Spot.

☐ Navigate to the menu item `Public Spot : SMS`.



☐ Select the setting "Send SMS via GSM-capable device (e.g. with 3G/4G modem)".

☐ Enter the user name and password for the administrator on the other 3G/4G device under "Administrator" and "Password".

☐ In the field "Address of GSM device", enter the IP address where the Public Spot is to reach the other 3G/4G device.

Customizing text message content

By default, the device uses predefined text modules as the content of the e-mails or SMS text messages. An overview of these standard texts is available under “Standard texts for e-mail sender, subject line and body” on page 504. You can also define your own texts.

Note: If you do not specify any text for a language, the device automatically enters the internal default text.

☐ Start LANconfig and open the configuration dialog for the device.

☐ Depending on the selected authentication method, switch to the view `Public Spot : E-mail` or "SMS".

☐ Using the button "Name of sender", enter a customized sender name for the e-mails or SMS text messages sent in the various languages, e.g. `Provider X`.

☐ Use the "E-mail subject" button to enter a subject line for the e-mails sent in the various languages by the Public Spot module. Special control characters are available for this, described in more detail in the section “Variables and control characters” on page 503.

☐ Use the "E-mail body" or "Message body" button to enter the content of the e-mails or SMS text messages sent in the various languages by the Public Spot module. Variables and special control characters are available for this, described in more detail in the section “Variables and control characters” on page 503.

☐ Now write the configuration back to the device.

Variables and control characters

The message texts used for the Smart Ticket function can be customized with the use of variables and control characters. The variables are automatically populated with values when the Public Spot module sends the e-mail to the user or the SMS gateway.

Variables

The following variables are available in the input field "E-mail body":

- `$PSpotPasswd`

  Placeholder for user-specific password for the Public Spot access.

- `$PSpotLogoutLink`

  Placeholder for the logout URL of the Public Spot in the form `http://<IP address of the Public Spot>/authen/logout`. This URL allows users to logout of the Public Spot if, after a successful login, the session window (which also contains this link) was blocked by the browser or closed by the Public Spot user.

Control characters

The following control characters may also be used in the text entered into the fields "E-mail subject" and "E-mail body":

- `\n`

  CRLF (carriage return, line feed)

- `\t`

  Tabulator

- `\<ASCII>`

  ASCII code of the corresponding character

Note: If the e-mail2SMS provider requires a variable which contains a backslash ("\"), you have to prefix this with another "\". This prevents the transformation of the "\" by HiLCOS.

Standard texts for e-mail sender, subject line and body

If you leave the dialogs `Public Spot : Email` or "SMS" blank, then the device automatically reverts to the standard texts in the corresponding language as stored in HiLCOS to generate the e-mail. The language used depends on the language setting of the browser used by the user for registration. If there are no default texts stored internally for a language, the device uses the English texts.

Table 1: Overview of the internal standard texts for authentication via e-mail/SMS

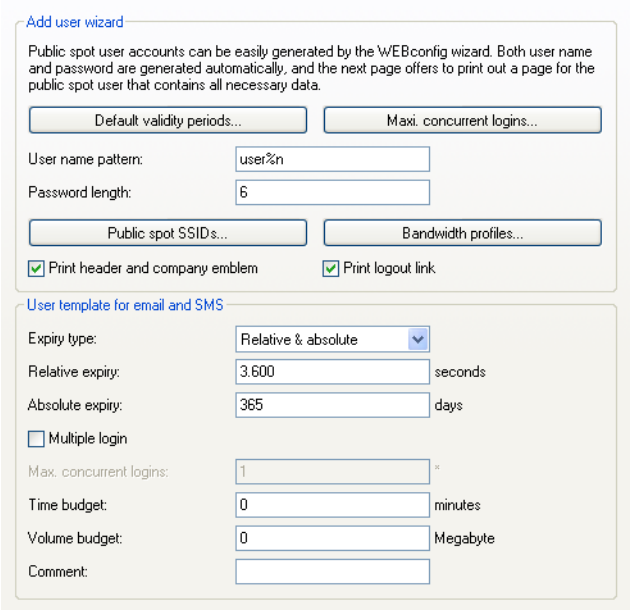
	Name of sender	E-mail subject	E-mail body
Deutsch	Public Spot	Your login credentials for the Public Spot	Your password for the Hirschmann Public Spot: $PSpotPasswd $PSpotLogoutLink
English	Public Spot	Your Public Spot account	Your password for the Hirschmann Public Spot: $PSpotPasswd $PSpotLogoutLink

Setting default values for the user templates

The following section describes how you adjust the default values for the "User templates" to meet your needs. The device uses the values set here as defaults when creating new users in Smart Ticket and when users login after confirming the terms and conditions. If you have so opted to send the login credentials via e-mail/SMS or you have activated the login after confirming the terms and conditions, each new user account is equipped with the permissions and constraints as defined by the user template.

☐ Start LANconfig and open the configuration dialog for the device.

☐ Change the view to `Public Spot : Wizard`.



☐ Complete the input fields in the section "User template" according to your preferences:

– "Expiry type": Using this entry you define how an automatically created Public Spot user account expires. You can specify whether the validity period of a user account is absolute (e.g. expires on a set date) and/or relative (elapsed time since the first successful login). If you select both values, the expiry time depends on which case occurs first.

– "Relative expiry": Using this entry you define the relative expiry time of an automatically created user account (in seconds). The "Expiry-type" that you chose must include `relative` in order for this setting to work. The validity of the account terminates after the time period specified in this field from the time of the first successful login of the user.

- "Absolute expiry": Using this entry you define the absolute expiry time of an automatically created user account (in days). The "Expiry type" that you chose must include `absolute` in order for this setting to work. The validity of the account terminates at the time specified in this field, calculated from the day of the creation of the account.
- "Multiple login": This entry allows you to generally allow or prohibit users with an automatically created account to login to the Public Spot using the same credentials with multiple devices at the same time. The number of devices that can be logged on simultaneously is specified using the input field "Max. concurrent logins".
- "Maximum number": Using this entry you set the maximum number of devices which can concurrently login to an automatically created account. The value `0` stands for "unlimited". In order for this setting to work, the parameter "Multiple login" must be enabled.
- "Time budget": Using this entry you define the time budget which automatically created users are assigned. A value of `0` disables the function.
- "Volume budget": Using this entry you define the volume budget which automatically created users are assigned. A value of `0` disables the function.
- "Comment": Using this entry you specify a comment or informational text which the RADIUS server adds to an automatically created user account.

☐ Optional: If necessary, change the "User name pattern" and the "Password length". In the authentication modes mentioned above, the device uses the relevant New user wizard default values (see “Setting default values for the Public Spot wizard” on page 443) to automatically generate a user name and a password.

☐ You can write the configuration back to the device.

6.6.3 Automatic re-login

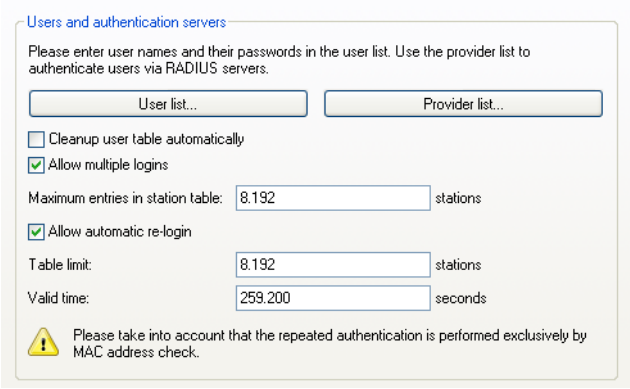
Mobile WLAN clients (e.g., smart phones and tablet PCs) automatically log in to known WLAN networks (SSID) when they reenter the cell. In this case, many apps automatically and directly access web content using the web browser in order to request current data (such as e-mails, social networks, weather reports, etc.) It is similar for mobile LAN clients (e.g., notebooks) which have to be disconnected from the network for a short time for a change of location (e.g., for changes from a lecture hall to a library in a college). In all of these cases, it is impractical to make the user manually log in to the Public Spot again in the browser.

With automatic re-login, the user only has to be identified on the Public Spot once. After a temporary absence, the user can seamlessly use the Public Spot again.

The Public Spot records the manual login and logout as well as a re-login in the SYSLOG. It stores the same login data for a re-login that a user had employed for initial authentication.

Note: The authentication is only performed on the MAC address of the client when re-login is enabled. Since it can lead to security problems, re-login is disabled by default.

The settings for automatic re-login can be found in LANconfig in the device configuration under `Public Spot : Users` in the section "Users and authentication servers".



The selection box "Allow automatic re-login" enables this function.

You specify the number of clients (maximum 65536) in the field "Automatic re-login table limit" that the re-login function may use.

In the field "Automatic re-login valid time" you specify how long the Public Spot stores the credentials of a client in the table for a re-login. After this period expires, the Public Spot user must log in again using the login page of the Public Spot in the browser.

6.6.4 Automatic authentication with the MAC address

After successful authentication, a Public Spot gives the user access to certain services. The Public Spot usually displays a login website to allow users to authenticate themselves. The user enters the authorization credentials into the login page and the Public Spot then redirects the user to the allowed sites.

In some applications, authentication via web site may not be desired or not possible, as the following examples illustrate:

- The end device does not have a browser and therefore cannot open the login page.
- Manually accessing the login page may be undesirable, such as when carrying out a performance test.

Automatic authentication on the Public Spot with a MAC address makes it possible to use the Public Spot without first opening the login page. The administrator enters the MAC addresses of the corresponding end device into the table of permissible MAC addresses under `Public Spot : Users : MAC authenticated users`.

The MAC-address check procedure

When the device receives a request from a client, the Public Spot executes the following steps for the automatic authentication by MAC address:

- If the Public Spot has already authenticated the MAC address of the received data packets, the device forwards the data packets without further delay.
- If the MAC address is in the list of allowed clients, the Public Spot starts a new session for the user and forwards the corresponding data packets.
- If a provider has been defined for verification of the MAC addresses by RADIUS, and a positive, valid MAC address authentication is cached in the Public Spot, then the Public Spot starts a new session for that user and forwards the associated data packets.
- If a provider chooses to check the MAC address with the RADIUS server, but does not have a valid authentication for the MAC address saved in the cache of the Public Spot, the Public Spot starts authentication on the corresponding RADIUS server. After a positive response, the Public Spot starts a new session for that user and forwards the associated packages.
- All of the above checks are unsuccessful, the Public Spot directs the user to the login page.

Authentication of the MAC address by RADIUS

If the MAC address of a WLAN client requesting to associate is not included in the list of permissible addresses, the Public Spot can alternatively authenticate the address via a RADIUS server.

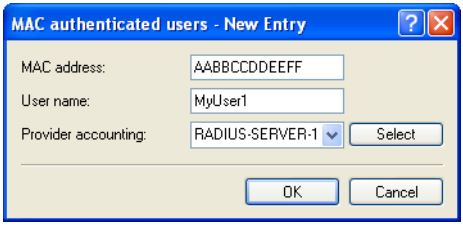
To enable RADIUS authentication, the administrator selects one of the RADIUS servers that has defined in the device and saved to the list of providers.

In addition, the administrator defines a lifetime for the rejected MAC addresses. This lifetime is used by the Public Spot to prevent the RADIUS server from being flooded with repeated requests for MAC addresses which cannot be authenticated (without login) via the RADIUS server or MAC address table.

If a MAC address authentication is rejected by the RADIUS server, the Public Spot saves this rejection for the lifetime defined here. The Public Spot responds to further requests for the same MAC address directly and without forwarding them to the RADIUS server first.

Configuration in LANconfig

For the configuration in LANconfig, you can find the parameters for the authentication of the clients using the MAC address in the dialog `Public Spot : Users : MAC authenticated users`.



6.6.5 Automatic authentication via WISPr

Your device provides an interface for authentication via WISPr. The **WISPr** standard is the technological predecessor of the 802.11u and Hotspot 2.0 specifications. The acronym stands for **Wireless Internet Service Provider roaming** and designates both a process and a protocol that allow users of WLAN enabled devices to roam seamlessly between the WLANs of different operators – and, therefore, between their Internet service providers. The idea behind it is similar to that of 802.11u and Hotspot 2.0; however, it requires more comprehensive support by the respective users.

Using the WISPr protocol, you can provide logins and network usage on your hotspot in a manner similar to Hotspot 2.0, even for end devices that no longer support Hotspot 2.0. The prerequisite is that your service provider provides the necessary infrastructure. Support for the user's device is provided either by the operating system or a suitable app (smart client). This client handles authentication to the hotspot for the user. If no credentials are available for the relevant network, the client queries the user for valid credentials at the system level. In any case, this eliminates the user having to log in via a login web page in the browser.

Because of its age, almost all current end devices with iOS, Android and Windows 8 support the WISPr protocol. In addition, larger WLAN Internet service providers often have their own apps to make the login for their clients easier: These apps include a preconfigured database of the provider's own hotspots and, optionally, those of their roaming partners. The authentication process corresponds to the following schema:

- ☐ A customer installs his provider's hotspot app to act as a client, which provides a database of preconfigured hotspot SSIDs.
- ☐ The client connects automatically with one of the hotspots and sends a HTTP-GET-Request to a random URL to test if direct Internet access is available or the Public Spot requires authentication.
- ☐ In HTTP-Redirect the hotspot sends a WISPr-XML-Tag with the Login-URL.
- ☐ The client sends its login data to the Login-URL in an HTTP-Post.

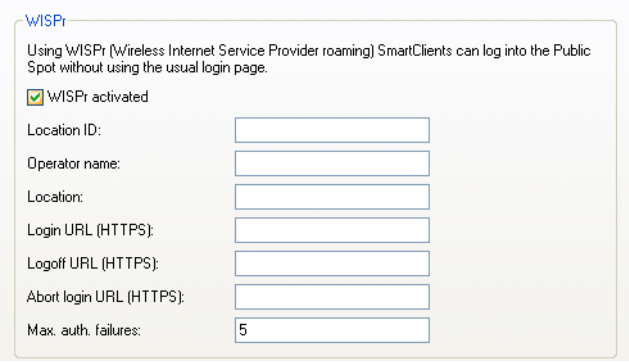
Example for an XML-Tag in redirect:

```
<HTML>
<?xml version="1.0" encoding="UTF-8"?>
  <WISPAccessGatewayParam xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
   xsi:noNamespaceSchemaLocation="http://www.acmewisp.com/WISPAccess
GatewayParam.xsd">
    <Redirect>
      <AccessProcedure>1.0</AccessProcedure>
      <AccessLocation>Hotel Contoso Guest Network</AccessLocation>
      <LocationName>Hotel Contoso</LocationName>
      <LoginURL>https://captiveportal.com/login</LoginURL>
      <MessageType>100</MessageType>
      <ResponseCode>0</ResponseCode>
    </Redirect>
   </WISPAccessGatewayParam>
</HTML>
```

Note: In order to use WISPr, the device must have an SSL certificate and a private key installed. The certificate must either be signed by a trusted authority or – if it is a self-signed certificate – be imported as a trusted certificate on the client. Otherwise the client will reject the login via WISPr.

Configuring WISPr

Configure the WISPr function of your device in the menu `Public Spot : WISPr`.



In this window you have the following options:

- "WISPr activated": Enable or disable the WISPr function for the device.
- "Location ID": Use this ID to assign a unique location number or ID for your device, for example, in the format `isocc=<ISO_Country_Code>,cc=<E.164_Country_Code>,ac=<E.164_Area_Code>, network=<SSID/ZONE>`
- "Operator name": Enter the name of the hotspot operator, e.g., `providerX`. This information helps the user to manually select an Internet service provider.
- "Location": Describe the location of your device, e.g., `CafeX_Market3`. This helps to better identify a user in your hotspot.
- "Login URL (HTTPS)": Enter the HTTPS address, that the WISPr client uses to transfer the credentials to your Internet service provider. Any external URL can be entered or the Public Spot itself. If the Public Spot should authenticate users using WISPr, enter the URL in the format `https://<Device-FQDN>/wisprlogin`. For "wisprlogin" in the example, any freely defined path can be used.
- "Logoff URL (HTTPS)": Enter the HTTPS address that a WISPr client uses for logging off at your Internet service provider. The same rules apply as for the login URL.
- "Abort login URL (HTTPS)": Enter the HTTPS address to which the device forwards a WISPr client if authentication fails. The same rules apply as for the login URL.

Note: The three URLs must be different, if the Public Spot is used in the device domain, for example:

- Login URL: https://<Device-FQDN>/wisprlogin
- Logoff URL: https://<Device-FQDN>/wisprlogoff
- Abort-Login-URL: https://<Device-FQDN>/wisprabort

Finally, for test purposes, you can also configure an URL with IP addresses. In a production system, the client will check the FQDN of the certificate!

- "Max. auth. failures": Enter the maximum number of failed attempts which the login page of your Internet service provider allows. If the Public Spot is used, the Public Spot rejects further login attempts by the specified client after this number of failed attempts.

RADIUS attributes transmitted via WISPr

If you enable WISPr and you use an external RADIUS server, the Public Spot transmits the attributes (access request):

- **Location ID**
- **Location name**
- **Logoff URL**

These attributes are subset of the values configured in the previous section. The provider or roaming broker can use them to identify the location of the client for accounting purposes. Vendor Specific Attributes (VSA) are used with the IANA Private Enterprise Number (PEN) 14122.

The Public Spot processes the attributes (access accept) from an external RADIUS server:

- **Redirection URL**: URL to which a client should be redirected after login. This function is not supported by all smart clients.
- **Bandwidth max up**: Maximum uplink bandwidth available to the client.
- **Bandwidth max down**: Maximum downlink bandwidth available to the client.
- **Session terminate time**: Time when the client should be automatically de-authenticated. According to ISO 8601, the format is `YYYY-MM-DDThh:mm:ssTZD`. If "TZD" is not entered, the client is de-authenticated according to the local time on the Public Spot.
- **Session terminate end of day**: The value of this attribute can be either 0 or 1. It indicates whether the client is de-authenticated on the Public Spot at the end of the accounting day.

For accounting purposes, the Public Spot uses the following attributes:

- **Location ID**
- **Location name**

6.7 IEEE 802.11u and Hotspot 2.0

As of HiLCOS 8.90, your device supports WLAN connections according to the IEEE 802.11u standard and—based on that—the Hotspot 2.0 specification. Using 802.11u you have the option to implement automatic authorization and authentication of your users on a local WLAN network (for example, within your company) or a Public Spot network. The prerequisite for this is that the relevant stations (smartphones, tablet PCs, notebooks, etc.) also support connections for 802.11u and Hotspot 2.0. In detail, the following functions are offered:

- **Automatic network selection**

  In a 802.11u-enabled environment, the user does not have to manually detect and select an SSID. Instead, the client independently searches for and selects a suitable Wi-Fi network by automatically requesting and evaluating the operator and network data of all 802.11u-enabled access points that are in range. A previous login to the access point is not required.

  Hotspot 2.0 stations also have the ability to retrieve information about the services available in a Wi-Fi network. If specific services that are relevant for a user (e.g., connections via HTTP, VPN or VoIP) are not available for a Wi-Fi network, any networks that do not meet the criteria are excluded from further searches. This ensures that users are always connected to the optimal network.

- **Automatic authentication and authorization**

  In 802.11u-enabled environments, the station automatically carries out the user's login if the necessary credentials are available. Authentication can be done, for example, using a SIM card, a username and password, or a digital certificate. Repetitive manual input of the credentials by the user in a login screen is no longer necessary. After successful authentication, the user can immediately use the desired services.

- **Seamless handover**

Connections according to 802.11u and in conjunction with 802.21 facilitate the uninterrupted exchange of data connections between different network types. This enables users to switch their stations seamlessly from a cellular network to a WLAN network as soon as they get within range of a Hotspot 2.0 zone—and vice versa. The same is true for the transfer between two different operators if, for example, the user goes from one homogeneous network to another during a bus trip

- **Automatic roaming**

  Connections as per 802.11u facilitate roaming between different operator networks. If a user is in range of a Hotspot 2.0 zone of an operator for which he does not have any credentials, his station still has the option to switch to its home network. Authentication at a third-party Hotspot 2.0 zone is handled by the operator's roaming partner, which then allows the user to access the third-party Wi-Fi network. This is interesting not only in areas where there are only single network operators with access points, it is also especially attractive for people traveling abroad.

Example: For example, a user who is in transit in the city with his 802.11u-enabled smartphone (station) can enable the WLAN feature to browse the Internet. The station then starts trying to find all available Wi-Fi networks in the area. If any of the access points offer 802.11u, the station selects the one network that best fits the required service based on the operator and network information that was previously obtained, for example, from a hotspot offering Internet access from its own cellular network company. In this case, the subsequent authentication can be performed automatically via the SIM card so that the user does not need to intervene at any time during the process. The encryption method selected for the connection – e.g., WPA2 – is unaffected.

In summary, connections according to 802.11u and with Hotspot 2.0 enabled combine the security features and performance of classic Wi-Fi hotspots with the flexibility and simplicity of data cellular network connections. At the same time, they relieve the cellular networks by redistributing data traffic (and possibly also telephony) to the network connections and frequency bands offered by access points.

6.7.1 Hotspot operators and service providers

The Hotspot 2.0 specification of the Wi-Fi Alliance differentiates between hotspot operators and hotspot service providers: A **hotspot operator** only operates one Wi-Fi network, while a **hotspot service provider** (SP) provides the connection for the user to the Internet or a cellular network. Of course, it is possible for an operator to also be an SP. However, in all other cases, a hotspot operator requires the corresponding roaming agreements with an SP or a group of multiple SPs (called a roaming consortium). Only when an operator has made these agreements are the various roaming partners' customers able to authenticate with the hotspot operator. Each service provider operates its own AAA infrastructure. A hotspot communicates this list of possible roaming partners and the name of the hotspot operator using ANQP (see functional description).

6.7.2 Functional description

The **802.11u** standard is the base standard of IEEE. This standard essentially expands access points or hotspots with the ability to broadcast so-called **ANQP data packets** (Advanced Message Queuing Protocol) in its broadcast signals. ANQP is a query/response protocol that a device can use to request a range of information about the hotspot. This includes both meta-data, such as information about the owner and the venue, as well as information on the underlying network, such as information on operator domains, roaming partners, authentication methods, forwarding addresses, etc. All 802.11u-enabled devices in range have the ability to request these data packets without a prior login to the access point in order to select a network based on the network information.

The Wi-Fi Alliance has added further ANQP elements to the standard, and markets this specification as **Hotspot 2.0**. This Hotspot 2.0 function merely adds additional elements to the standard, which the device can use as criteria for selecting its network. These criteria include, for example, information about the services and WAN metrics available at the hotspot.

The ANQP data packets are the central information element of the 802.11u standard. However, to signal the support for 802.11u and to transmit data packets, further elements are required for the operation of 802.11u:

- The signaling of 802.11u support in the beacons and probes of a hotspot are done by the element known as the **Interworking element**. In this element, the initial basic network information—such as the network classification, Internet availability (Internet bit) and the OI of the roaming consortium and/or of the operator—are already included. At the same time, it is used by 802.11u-enabled devices as an initial screening criterion when detecting a network.
- ANQP data packets are transferred within the so-called GAS containers. **GAS** stands for Generic Advertisement Service, and is the name of generic containers that allow a device to request additional internal and external information for the network selection from the hotspot, in addition to the information in the beacons. The GAS containers are transmitted on layer 2 by what are referred to as public action frames.

Login by an 802.11u-enabled client at a Hotspot 2.0

The following functional description schematically illustrates the selection and login process of an 802.11u-enabled device at a Hotspot 2.0.

Login via username/password or digital certificate

☐ The hotspots reply with an ANQP response, which contains, among other things, the name of the hotspot operator and a list of NAI realms, which list all available roaming partners (service provider, abbreviated SP).

☐ The device loads the locally stored credentials from the WLAN profiles or installed certificates that were set up by the user, and compares the local realms with the NAI realm lists obtained in (2).

– If the device successfully finds one, it knows that it can be authenticated successfully on the relevant Wi-Fi network.

– If the device successfully finds more than one, the selection of a Wi-Fi network is made based on the user's preference list. This list defines the preferred order of operators in conjunction with the potential roaming partners. In this case, the device compares the operator names listed under (2) with the list, and selects the operator with the highest priority.

☐ The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate SP. The access point then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for authentication. The authentication is performed using the authentication method determined by the SP. The authentication via username/password uses EAP-TTLS, and authentication via digital certificate uses EAP-TLS.

Login via (U)SIM

☐ In contrast to the login via username/password or digital certificate, a device with a (U)SIM does not request the list of NAI realms in its ANQP requests, but rather the 3GPP Cellular Network Information. The ANQP responses contain the cellular network information list of all cellular network providers for which the access point offers authentication.

☐ The device loads the parameters for the cellular network from its local (U)SIM card, and compares it with the data retrieved from the cellular network information lists. The list comparison and selection of a preferred provider network is performed analogous to the login via username/password or digital certificate.

☐ The device authenticates itself with its local credentials at the hotspot of the preferred operator for the appropriate cellular network company. The hotspot then transmits this data over its SSPN interface (Subscription Service Provider Network) to an AAA system responsible for the authentication. The presence of a (U)SIM card changes the possible authentication method for the device to EAP-SIM or EAP-AKA.

☐ The AAA system verifies the credentials for authentication via the interface MAP (Mobile Application Part) at the HLR server (Home Location Register) of the cellular network company.

If authentication is successful, the device gets access to the WLAN network either via hotspot (credentials for the operator's network are available) or automatic roaming (credentials for the operator's network are not available).

If there are multiple authentication options available for the device (e.g., SIM card and username/password), it has the option of using the preferred EAP authentication method and, therefore, the preferred credentials based on the NAI realm or cellular network information list.

6.7.3 Recommended general settings

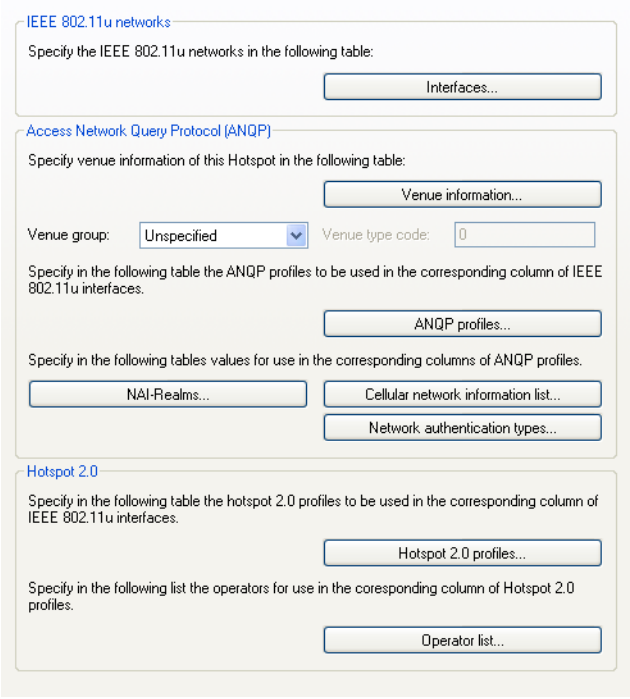
The Hotspot 2.0 specification recommends the following general settings for the 802.11u operator:

- WPA2-Enterprise Security (802.1x) enabled
- Authentication using EAP with the corresponding variant:
  - EAP-SIM/EAP-AKA for authentication with SIM / USIM card
  - EAP-TLS for authentication with a digital certificate
  - EAP-TTLS for authentication with a username and password
- Enabled and properly configured ARP proxy
- Disabled multicasts and broadcast in cellular networks

- Non-approved data traffic between the cellular network devices (Layer 2 traffic inspection and filtering). The corresponding settings can be found in LANconfig under `Wireless LAN : Security`.
- Enabled and implemented firewall on the access router, which provides Internet access

6.7.4 Configuration menu for IEEE 802.11u / Hotspot 2.0

You can find the configuration menu for IEEE 802.11u and Hotspot 2.0 under `Configuration : Wireless LAN : IEEE 802.11u`.



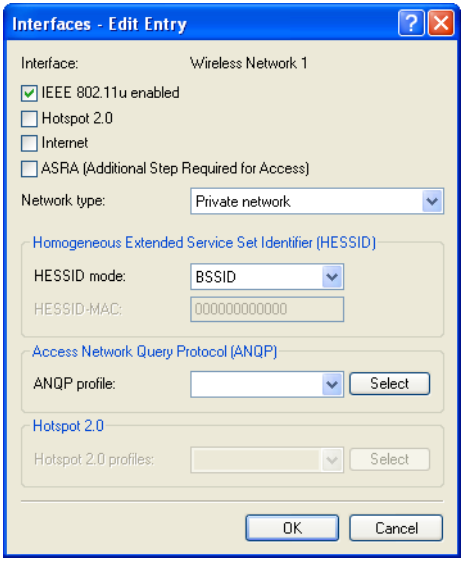
The device offers the ability to individually enable or disable and configure the support the IEEE 802.11u standard as well as the Hotspot 2.0 functionality for each logical WLAN interface using the button "Interfaces".

Some of the parameters that need to be configured are located in so-called "profiles". Using profiles, you can group different rows in lists, which you only have to reference from the other windows. Essentially, these are profiles for ANQP data packets and Hotspot 2.0. The relationships between the profile lists is as follows:

```
|-- Interfaces
  |-- ANQP-Profiles
    |-- NAI-Realms
    |-- Cellular-Network-Information-List
    |-- Network-Authentication-Types
  |-- Hotspot 2.0 Profiles
    |-- Operator-List
```

Activating interfaces

The table "Interfaces" is the highest administrative level for 802.11u and Hotspot 2.0. Here you have the option of enabling or disabling functions for each interface, assigning them different profiles, or modifying general settings.



In order to edit the entries in the table "Interfaces", click on the button "Edit...". The entries in the edit window have the following meaning:

- "Interface": Name of the logical WLAN interface that you are currently editing.
- "IEEE 802.11u enabled": Enable or disable support for connections according to IEEE 802.11u at the appropriate interface. If you enable support, the device sends the interworking element in beacons/probes for the interface or for the associated SSID, respectively. This element is used as an identifying feature for IEEE 802.11u-enabled connections: It includes, for example, the Internet bit, the ASRA bit, the HESSID, and the location group code and the location type code. These individual elements use 802.11u-enabled devices as the first filtering criteria for network detection.

- "Hotspot 2.0": Enable or disable the support for Hotspot 2.0 according to the Wi-Fi Alliance® at the appropriate interface. Hotspot 2.0 extends the IEEE standard 802.11u with additional network information, which stations can request using an ANQP request. These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Using this additional information, stations are in a position to make an even more selective choice of Wi-Fi network.
- "Internet": Select whether the Internet bit is set. Over the Internet-bit, all stations are explicitly informed that the Wi-Fi network allows Internet access. Enable this setting if services other than internal services are accessible via your device.

  Note: Using this function you only communicate the availability of an Internet connection. You configure the corresponding regulations on the firewall, irrespective of this option.

- "ASRA - Additional steps for access required": Select whether the ASRA bit (Additional Step Required for Access) is set. Using the ASRA bit explicitly informs all stations that further authentication steps are needed to access the Wi-Fi network. Enable this setting if you have, for example, set up online registration, additional authentication, or a consent form for your terms of use on your web site.

  Note: Please remember to specify a forwarding address in the "Network authentication types" table for the additional authentication and/or "WISPr" for the Public Spot module if you set the ASRA bit.

- "Network type": Select a network type from the available list which most closely describes the Wi-Fi network behind the selected interface. Based on the setting made here, the user has the option to limit network detection of their devices to specific network types. Possible values include:
  - `Private network`: Describes networks which are blocked to unauthorized users. Select this type, for example, for home networks or corporate networks where access is limited to employees.
  - `Private with guest access`: Similar to `Private network`, but with guest access for unauthorized users. Select this type, for example, for corporate networks where visitors may use the Wi-Fi network in addition to employees.

- `Chargeable public network`: Describes public networks that are accessible to everyone and can be used for a fee. Information about fees may be available through other channels (e.g.: IEEE 802.21, HTTP/HTTPS or DNS forwarding). Select this type, for example, for hotspots in shops or hotels that offer fee-based Internet access.
- `Free public network`: Describes public networks that are accessible to everyone and for which no fee is payable. Select this type, for example, for hotspots in public, local and long-distance transport, or for community networks where Wi-Fi access is an included service.
- `Personal device network`: In general, it describes networks that connect wireless devices. Select this type, for example, for digital cameras that are connected to a printer via WLAN.
- `Emergency services only network`: Describes networks that are intended for, and limited to, emergency services. Select this type, for example, for connected ESS or EBR systems.

  - `Test or experimental`: Describes networks that are set up for testing purposes or are still in the setup stage.
  - `Wildcard`: Placeholder for previously undefined network types.

- "HESSID mode": Specify where the device gets its HESSID for the homogeneous ESS. A homogeneous ESS is defined as a group of a specific number of access points, which all belong to the same network. The MAC address of a connected access point serves as a globally unique identifier (HESSID). The SSID can not be used as an identifier in this case, because different network service providers can have the same SSID assigned in a hotspot zone, e.g., by common names such as "HOTSPOT". Possible values for the HESSID mode include:
  - `BSSID`: Select this item to set the BSSID of the device as the HESSID for your homogeneous ESS.
  - `User`: Select this item to manually assign a HESSID.
  - `None`: Select this item in order to not assign any homogeneous ESS and to isolate it from the device network.
- "HESSID-MAC": If you selected the setting `user` for the "HESSID mode", enter the HESSID of your homogeneous ESS as a 6-octet MAC address. Select the BSSID for the HESSID for any access point in your homogeneous ESS in capital letters and without separators, e.g., `008041AEFD7E` for the MAC address 00:80:41:ae:fd:7e.

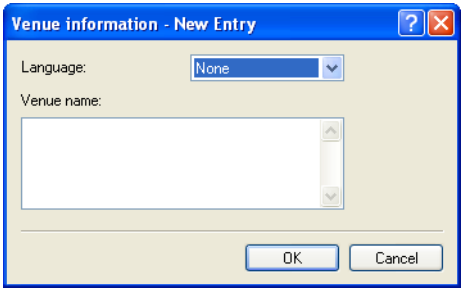
  Note: If your device is not present in multiple homogeneous ESS's, the HESSID is identical for all interfaces
- "ANQP profile": Select an ANQP profile from the list. You create ANQP profiles in the configuration menu using the button of the same name.
- "Hotspot 2.0 profiles": Select the Hotspot 2.0 profile from the list. You create the Hotspot 2.0 profiles in the configuration menu using the button of the same name.

Venue information and group

Using the table "Venue information" and the following dialogs "Venue group" and "Venue type code", you manage the information about the access point's location.

In the event of a manual search, additional details on the "Venue information" help a user to select the correct hotspot. If more than one operator (e.g., multiple cafés) in a single hotspot zone uses the same SSID, the user can clearly identify the appropriate location using the venue information.

You can place your device in a predefined category using the "Venue group" and "Venue type code" – as opposed to the user-defined location information.



In order to edit the entries in the table "Venue information", click on the button "Add...". The entries in the edit window have the following meaning:

- "Language": You have the ability to specify custom information for the location of the access point for each language. The location name that matches your user's language will then be displayed. If a language is not available for a user, its station chooses one based, for example, on the default language.
- "Venue name": Enter a short description of the location of your device for the selected language, for example:
-
```
Ice Café Valencia
123 Street
City, State 12345
```

The "Venue group" describes the environment where you operate the access point. You define them globally for all languages. The possible values, which are set by the venue group code, are specified in the 802.11u standard.

Using the "Venue type code", you have the option to specify the details for the venue group. These values are also specified by the standard. The possible type codes can be found in the following table.

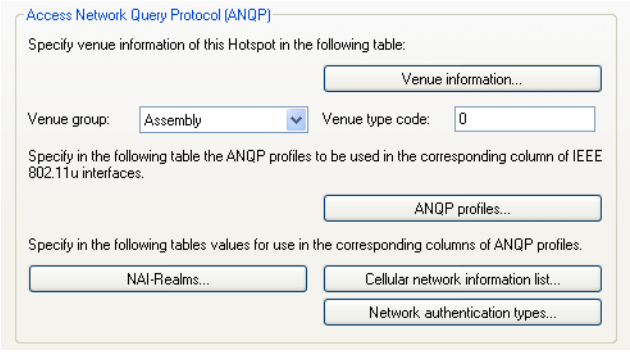


Table 2: Overview of possible values for venue groups and types

Venue group	**Code = Venue type code**
Unspecified Assembly	▶ 0 = unspecified assembly ▶ 1 = stage ▶ 2 = stadium ▶ 3 = passenger terminal (e.g., airport, bus station, ferry terminal, train station) ▶ 4 = amphitheater ▶ 5 = amusement park ▶ 6 = place of worship ▶ 7 = convention center ▶ 8 = library ▶ 9 = museum ▶ 10 = restaurant ▶ 11 = theater ▶ 12 = bar ▶ 13 = café ▶ 14 = zoo, aquarium ▶ 15 = emergency control center

Table 2: Overview of possible values for venue groups and types

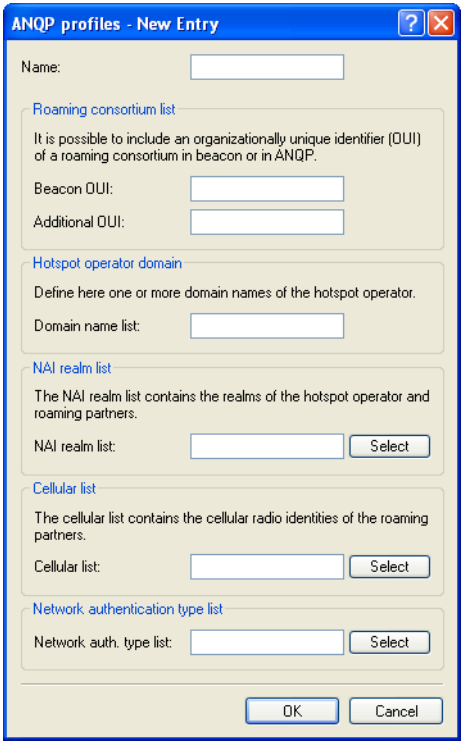
Venue group	Code = Venue type code
Business	0 = unspecified business
	1 = doctor's office
	2 = bank
	3 = fire station
	4 = police station
	6 = post office
	7 = office
	8 = research facility
	9 = law firm
Educational:	0 = unspecified education
	1 = primary school
	2 = secondary school
	3 = college
Factory and industry	0 = unspecified factory and industry
	1 = factory
Institutional	0 = unspecified institution
	1 = hospital
	2 = long-term care facility (e.g., nursing home, hospice)
	3 = rehabilitation clinic
	4 = organizational association
	5 = prison
Commerce	0 = unspecified commerce
	1 = retail store
	2 = food store
	3 = auto repair shop
	4 = shopping center
	5 = gas station
Halls of residence	0 = unspecified residence hall
	1 = private residence
	2 = hotel or motel
	3 = student housing
	4 = guesthouse
Warehouse	0 = unspecified warehouse
Utility and miscellaneous	0 = unspecified service and miscellaneous

Table 2: Overview of possible values for venue groups and types

Venue group	Code = Venue type code
Vehicular	▶ 0 = unspecified vehicle
	▶ 1 = passenger or transport vehicles
	▶ 2 = aircraft
	▶ 3 = bus
	▶ 4 = ferry
	▶ 5 = ship or boat
	▶ 6 = train
	▶ 7 = motorcycle
Outdoor	▶ 0 = unspecified outdoor
	▶ 1 = municipal Wi-Fi network (wireless mesh network)
	▶ 2 = city park
	▶ 3 = rest area
	▶ 4 = traffic control
	▶ 5 = bus stop
	▶ 6 = kiosk

ANQP profiles

Using this table you manage the profile lists for ANQP. "ANQP profiles" offers you the ability to group certain ANQP elements and to independently assign logical WLAN interfaces in the table "Interfaces". These elements include, for example, information about your OIs, domains, roaming partners and their authentication methods. Some of the elements are located in other profile lists.



In order to edit the entries in the table "ANQP profiles", click on the button "Add...". The entries in the edit window have the following meaning:

- "Name": Assign a name for the ANQP 2.0 profile here. This name will appear later in the interfaces table in the selection for ANQP profiles.
- "Beacon OUI": Organizationally Unique Identifier, abbreviated as OUI, simplified as OI. As the hotspot operator, you enter the OI of the roaming partner with whom you have agreed a contract. If you are the hotspot operator as well as the service provider, enter the OI of your roaming consortium or your own OI. A roaming consortium consists of a group of service providers which have entered into mutual agreements regarding roaming. In order to get an OI, this type of consortium – as well as an individual service provider – must register with IEEE.

It is possible to specify up to 3 parallel OIs, in case you, as the operator, have roaming agreements with several partners. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.

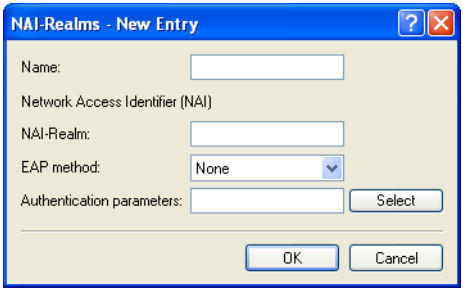
Note: This device transmits the specified OI(s) in its beacons. If a device should transmit more than 3 OIs, these can be configured under "Additional OUI". However, additional OIs are not transferred to a station until after the GAS request. They are not immediately visible to the stations!

- "Additional OUI": Enter the OI(s) that the device also sends to a station after a GAS request. Multiple OIs can be provided in a comma-separated list, such as `00105E,00017D,00501A`.
- "Domain name list": Enter one or more domains that are available to you as a hotspot operator. Multiple domain names are separated by a comma separated list, such as `providerX.org,provx-mobile.com,wifi.mnc410.provX.com`. For subdomains it is sufficient to specify only the highest qualified domain name. If a user configured a home provider on his device, e.g., providerX.org, this domain is also assigned to access points with the domain name wi-fi.providerX.org. When searching for suitable hotspots, a station always prefers a hotspot from his home provider in order to avoid possible roaming costs.
- "NAI realm list": Select an NAI realm profile from the list. You specify profiles for NAI realms in the configuration menu by clicking the button "NAI realms".
- "Cellular list": Select the cellular network identity from the list. You set the identities for cellular networks – similar to profiles – in the configuration menu using the button "Cellular network information list".
- "Network authentication type list": Select an authentication profile from the list. You specify profiles for network authentication in the configuration menu by clicking the button "Network authentication types".

Additionally, using the telnet console or setup menu, you have the option to also display the type of available IP addresses, which they can obtain from the network after a successful authentication. You can access the relevant parameters "IPv4-Addr-Type" and "IPv6-Addr-Type" via the telnet path `Setup : IEEE802.11u : ANQP-General`.

NAI realms

Using this table you manage the profile lists for the NAI realms. With these lists you have the ability to group certain ANQP elements. These include the realms of the hotspot operator and its roaming partners, as well as the associated authentication methods and parameters. Stations use the information stored in this list to determine whether they have the hotspot operator or one of its roaming partners have valid credentials.



In order to edit the entries in the table "NAI realms", click on the button "Add...". The entries in the edit window have the following meaning:

- "Name": Assign a name for the NAI realm profile, such as the name of the service provider or service to which the NAI realm belongs. This name will appear later in the ANQP profile in the selection for "NAI realm list".
- "NAI realm": Enter the realm for the Wi-Fi network. The identification of the NAI realm consists of the username and a domain, which can be extended using regular expressions. The syntax for an NAI realm is defined in IETF RFC 2486 and, in the simplest case, is `<username>@<realm>`, for `user746@providerX.org`, and therefore the corresponding realm is `providerX.org`.

- "EAP method": Select a language for the NAI realm from the list. EAP stands for the authentication profile (Extensible Authentication Protocol), followed by the corresponding authentication method Possible values include:
  - `EAP-TLS`: Authentication using Transport Layer Security (TLS). Select this setting when authentication via the relevant NAI realm is performed by a digital certificate that the user has to install.
  - `EAP-SIM`: Authentication via the Subscriber Identity Module (SIM). Select this setting when authentication via the relevant NAI realm is performed by the GSM Subscriber Identity Module (SIM card) of the station.
  - `EAP-TTLS`: Authentication via Tunneled Transport Layer Security (TTLS). Select this setting when authentication via the relevant NAI real is performed using a username and password. For security reasons, the connection is tunneled for this method.
  - `EAP-AKA`: Authentication using Authentication and Key Agreement (AKA). Select this setting when authentication via the relevant NAI realm is performed by the UMTS Subscriber Identity Module (USIM card) of the station.
  - `None`: Select this setting when the relevant NAI realm does not require authentication.
- "Authentication parameters": In the window that opens when you click the "Select" button, select the appropriate authentication parameters for the EAP method, such as EAP-TTLS `NonEAPAuth.MSCHAPV2,Credential.UserPass` or for EAP-TLS `Credentials.Certificate`. Possible values include:

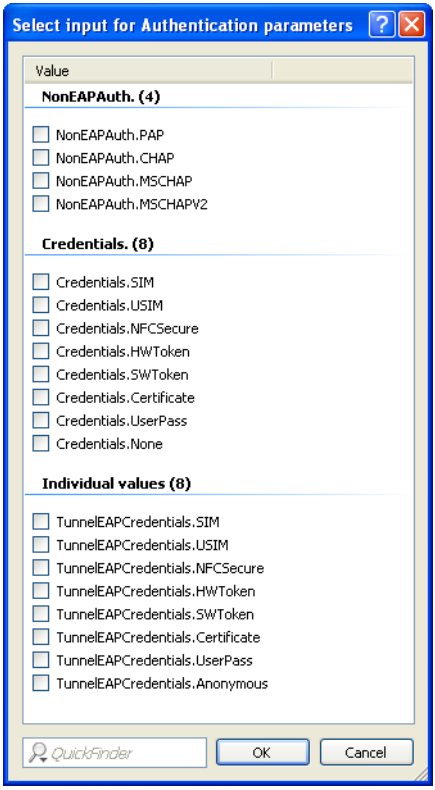


Table 3: Overview of possible authentication parameters

Parameters	Sub-parameters	Comment
NonEAPAuth.		Identifies the protocol that the realm requires for phase 2 authentication:
	PAP	Password Authentication Protocol
	CHAP	Challenge Handshake Authentication Protocol, original CHAP implementation, specified in RFC 1994
	MSCHAP	Implementation of Microsoft CHAP V1, specified in RFC 2433
	MSCHAPV2	Implementation of Microsoft CHAP V2, specified in RFC 2759
Credentials.		Describes the type of authentication that the realm accepts:
	SIM	SIM card
	USIM	USIM card
	NFCSecure	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token

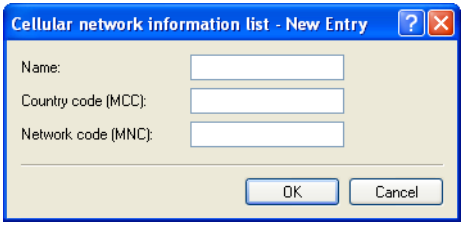
Table 3: Overview of possible authentication parameters

Parameters	Sub-parameters	Comment
	Certificate	Digital certificate
	UserPass	Username and password
	None	No credentials required
TunnelEAPCredentials.*		
	SIM*	SIM card
	USIM*	USIM card
	NFCSecure*	NFC chip
	HWToken*	Hardware token
	SoftToken*	Software token
	Certificate*	Digital certificate
	UserPass*	Username and password
	Anonymous*	Anonymous login

*) The specific parameter or sub-parameter is reserved for future uses within the framework of Passpoint™ certification, but currently is not in use.

Cellular network information list

Using this table you manage the identity lists for cellular networks. With these lists you have the ability to group certain ANQP elements. These include the network and country codes of the hotspot operator and its roaming partners. Based on the information stored here, stations with SIM or USIM cards use this list to determine if the hotspot operator belongs to their cellular network company or has a roaming agreement with their cellular network company.



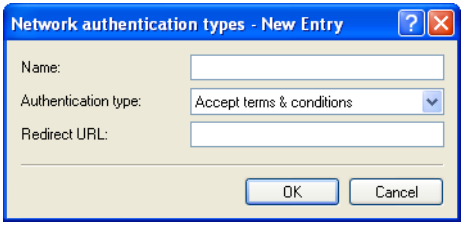
In order to edit the entries in the table "Cellular network information list", click on the button "Add...". The entries in the edit window have the following meaning:

- "Name": Assign a name for the cellular network identity, such as an abbreviation of the network operator in combination with the cellular network standard used. This name will appear later in the ANQP profile in the selection for "Cellular list".
- "Country code (MCC)": Enter the Mobile Country Code (MCC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters, e.g., `262` for Germany.
- "Network code (MNC)": Enter the Mobile Network Code (MNC) of the hotspot operator or its roaming partners, consisting of 2 or 3 characters.

Network authentication types

Using this table, you manage addresses to which the device forwards stations for an additional authentication step after the station has been successfully authenticated by the hotspot operator or any of its roaming partners. Only one forwarding entry is allowed for each authentication type.

Note: Please remember to set the ASRA bit in the "Interfaces" table if you set up an additional authentication step.

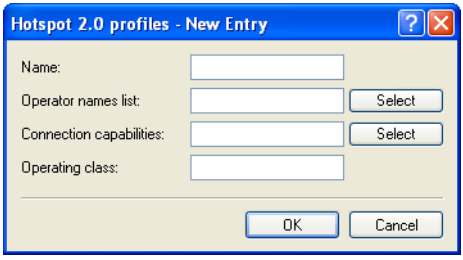


In order to edit the entries in the table "Network authentication types", click on the button "Add...". The entries in the edit window have the following meaning:

- "Name": Assign a name for the table entry, for example, `Accept Terms & Conditions`. This name will appear later in the ANQP profile in the selection for "Network auth. type list".
- "Authentication type": Choose the context from the list, which applies before forwarding. Possible values include:
  - `Accept terms & conditions`: An additional authentication step is set up that requires the user to accept the terms of use.
  - `Online enrollment`: An additional authentication step is set up that requires the user to register online first.
  - `HTTP redirection`: An additional authentication step is set up to which the user is forwarded via HTTP.
  - `DNS redirection`: An additional authentication step is set up to which the user is forwarded via DNS.
- "Redirect URL": Enter the address to which the device forwards stations for additional authentication.

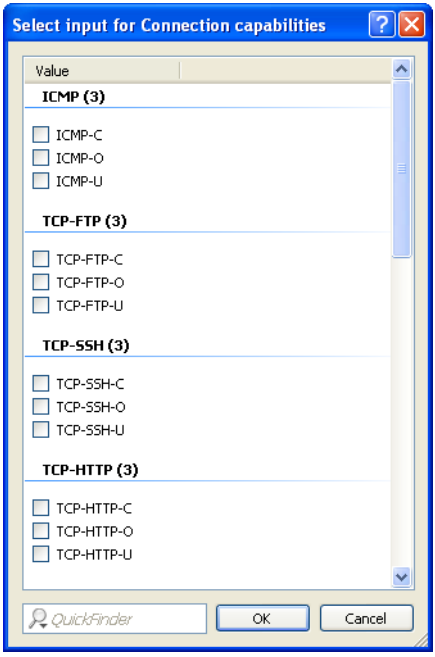
Hotspot 2.0 profiles

Using this table you manage the profile lists for the Hotspot 2.0. "Hotspot 2.0 profiles" offers you the ability to group certain ANQP elements (from the Hotspot 2.0 specification) and to independently assign logical WLAN interfaces in the table "Interfaces". These include, for example, the operator-friendly name, the connection capabilities, operating class and WAN metrics. Some of the elements are located in other profile lists.



In order to edit the entries in the table "Hotspot 2.0 profiles", click on the button "Add...". The entries in the edit window have the following meaning:

- "Name": Assign a name for the Hotspot 2.0 profile here. This name will appear later in the interfaces table in the selection for the Hotspot 2.0 profile.
- "Operator name list": Select the profile of a hotspot operator from the list. You specify profiles for hotspot operators in the configuration menu by clicking the "Operator list".
- "Connection capabilities": Click the "Select" button and enter the connection capabilities for each service in the window that opens. Before joining a network, stations use the information stored in this list to determine whether your hotspot even allows the required services (e.g., Internet access, SSH, VPN). For this reason, the fewest possible entries should be entered with the status "unknown". Possible status values for each of these services are "closed" (`-C`), "Open" (`-O`) or "unknown" (`-U`):



- `ICMP`: Specify whether to allow the exchange of information and error messages via ICMP.
- `TCP-FTP`: Specify whether to allow file transfers via FTP.
- `TCP-SSH`: Specify whether to allow encrypted connections via SSH.
- `TCP-HTTP`: Specify whether to allow Internet connections via HTTP/HTTPS.
- `TCP-TLS`: Specify whether to allow encrypted connections via TLS.
- `TCP-PPTP`: Specify whether to allow the tunneling of VPN connections via PPTP.
- `TCP-VOIP`: Specify whether to allow Internet telephony via VoIP (TCP).
- `UDP-IPSEC-500`: Specify whether to allow IPSec via UDP and port 500.

- UDP-VOIP: Specify whether to allow Internet telephony via VoIP (UDP).
- UDP-IPSEC-4500: Specify whether to allow IPSec via UDP and port 4500.
- ESP: Specify whether to allow ESP (Encapsulating Security Payload) for IPSec.

If you do not know if a service is available and its ports are open or closed on your network, or you consciously do not want to make any entry for the status, select a -U setting.

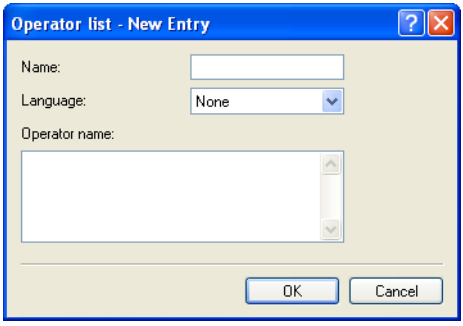
Note: Using this dialog, you do not define permissions! The stations only use the entries to determine whether to join a network via your device. You configure specific access permissions for your network with other device functions, such as the firewall/QoS.

- "Operating class": Enter the code for the global operating class of the access point. Using the operating class, you inform a station on which frequency bands and channels your access point is available. Example:
  - 81: Operation at 2.4 GHz with channels 1-13
  - 116: Operation at 40 MHz with channels 36 and 44

  Please refer to the IEEE standard 802.11-2012, Appendix E, Table E-4, for the operating class that corresponds to your device: Global operating classes, available at standards.ieee.org.

Operator list

Using this table you manage the plain text name of the hotspot operator. An entry in this table offers you the ability to send a user-friendly operator name to the stations, which they can then display instead of the realms. However, whether they actually do that depends on their implementation.



In order to edit the entries in the table "Operator list", click on the button "Add...". The entries in the edit window have the following meaning:

- "Name": Assign a name for the entry, such as an index number or combination of operator-name and language.
- "Language": Select a language for the hotspot operator from the list.
- "Operator name": Enter the plain text name of the hotspot operator.

6.8 XML interface

In order to be able to cover a wide range of Public Spot scenarios, the default authentication method of name and password is not sufficient by itself. Access and accounting models using key cards, dongles or prepaid credit cards often require additional access data, which the Public Spot in this form would be unable to manage.

The implemented XML interface connects the Public Spot and an external gateway. It directs the user data only to the gateway that handles the authentication and accounting, and it only sends information about the duration and limits of the user access to the Public Spot.

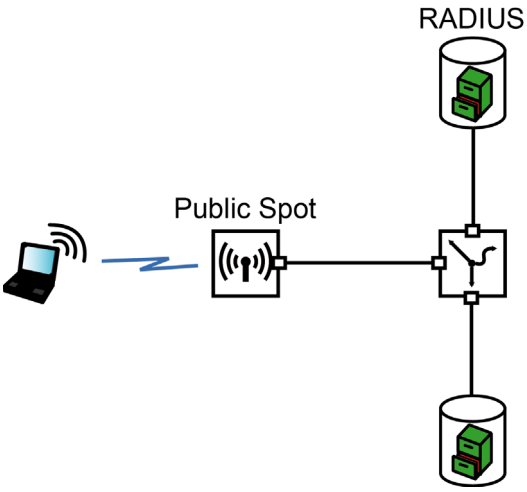
In this case, the Public Spot only performs the following tasks:

- Forward the user requests
- Restrict unauthorized access attempts
- Accept gateway commands to start and stop a session
- Accounting for sessions, if applicable

Since it is not realistic to implement all existing, and at times very specific scenarios with the associated gateway commands on the Public Spot, the XML interface was designed to be flexible and multi-purpose.

6.8.1 Function

The communication between the XML interface and external gateway is processed as follows:



☐ The user connects to the Public Spot's WLAN and sends an HTTP request to the Public Spot.

☐ The Public Spot forwards the login procedure's HTTP request to the external hotspot gateway. The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

The Public Spot forwards the MAC address of the requesting Public Spot client to the external gateway. To implement this, navigate to `Public-Spot-Module : Page-Table`, set the "Type" to "Redirect" and suffix the "URL" with the parameter `?myvar=%m`.

Example: `http://192.168.1.1/?myvar=%m`

In this case, `myvar` is a freely selectable variable. The variable `%m` is vital here, as the Public Spot replaces this with the client's MAC address when forwarding the request.

☐ The hotspot gateway checks the user's credentials and, if applicable, it can contact further systems to charging to credit card, for example.

☐ The hotspot gateway sends an XML file with the user data to the Public Spot's XML interface. The external hotspot gateway contacts the device with the Public Spot XML interface using the URL `http://<Device-URL>/xmlauth`.

The Public Spot's XML interface analyses this file and initiates the corresponding actions. In the case of a login request, the XML interface inserts the user and the corresponding MAC address into the list of logged-on Public Spot users. In the case of a logout request, the XML interface removes the user from this list again. At the same time, the XML interface confirms the request by sending a corresponding XML file to the hotspot gateway.

In order for the Public Spot to be able to process the instructions in the XML file, a special administrator must be set up on the device who has the function right "Public-Spot -XML-interface". This hotspot gateway logs in to the Public Spot with this admin account.

While the user is logged in to the Public Spot, the XML interface and hotspot gateway can exchange status information about the current session in the form of XML files.

If the user has exhausted his online quota, the hotspot gateway will send a stop command to the XML interface, and then the Public Spot locks further access for that user. The XML interface also confirms that the login is blocked by sending the corresponding XML file to the hotspot gateway.

☐ If the additional use of a RADIUS server is enabled, the hotspot gateway optionally creates a user in a RADIUS server.

☐ The Public Spot sends relevant data to the RADIUS server throughout the session, for example to facilitate the accounting of the Public Spot usage. By default, the Public Spot uses its internal RADIUS server for this. If necessary, you can configure the device running the Public Spot to conduct forwarding to an external RADIUS server.

Note: Communications between the Public Spot and a hotspot gateway with the use of XML is not standardized. Configure the hotspot gateway according to the instructions in the „Commands“ section in order for the Public Spot and hotspot gateway exchange the XML messages in the required form. XML messages are exchanged invisibly without a graphical user interface. You can use tools such as cURL (see “Analyzing the XML interface using cURL” on page 550) to test the exchange of messages.

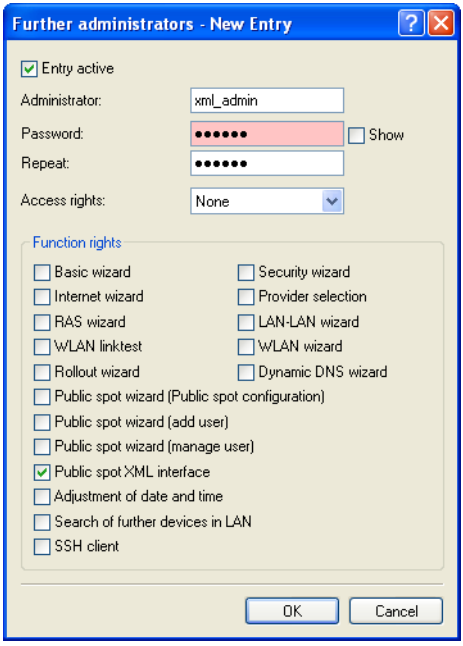
6.8.2 Setting up the XML interface

The following section describes how to set up the XML interface.

Note: You need to have the "Supervisor" permission in order to create another administrator account.

☐ Using `Management : Admin : Further administrators` you create a new administrator with the function right "Public Spot XML interface".

This is the administrator account that the gateway uses to send XML files to the Public Spot XML interface.



Note: The new administrator should not have any further Public Spot function rights, since they represent a potential security risk in combination with the XML interface (e.g., if the communication between XML sender and device is unencrypted).

☐ You enable the XML interface in `Public Spot : Server` in the section "External hotspot gateway" and, if necessary, global RADIUS authentication for your Public Spot.

☐ In the section "Allow access without authentication" click on the button "Free Networks" and add a new network. Enter the "Name/IP address" of the login page. In "Netmask" enter `255.255.255.255`.

When defined as a free network, the user has direct access to the login page of the gateway without having to login to the Public Spot first.

☐ Configure the gateway so that it sends the user's session data to the Public Spot XML interface as an XML file.

For questions about configuring the gateway, please refer to the applicable service provider.

6.8.3 Analyzing the XML interface using cURL

The following section describes the analysis of the XML interface with the open-source software cURL.

Client for URL, or cURL, is a command line application use for transferring files on a network without the use of a Web browser or FTP client. "cURL" is a component of many Linux distributions and is also available for other operating systems.

Note: To analyze the XML interface using cURL, you need an administrator account with the function right "Public Spot XML interface" for the Public Spot.

☐ First download cURL and install or unpack it.

☐ Start cURL with the console command `curl -X POST -H "Content-Type:text/xml" -d @filename http://user:pass@myhost/xmlauth/`

The parameters have the following meaning:

– **@filename**

  Path and name of the local XML file, e.g. the login request from the examples (see “Login” on page 552).

– **user**

  Username with the function right titled "Public Spot XML interface". The XML feature does not work without this authentication.

– **pass**

  User password.

– **myhost**

  IP address or DNS name of the device with the Public Spot XML interface

☐ With Telnet you can use the command `trace # XML-Interface-PbSpot` to activate a trace that verifies whether XML requests were successful or error messages were received.

6.8.4 Commands

The XML interface can process three types of requests and responses:

- Login
- Logout
- Status

An XML file can contain several requests or answers.

Login

If the external gateway sends a "Login" request in an XML file, the Public Spot activates online access for the corresponding user. A "Login" request contains the attribute `COMMAND="RADIUS_LOGIN"`.

If the Public Spot does not use a RADIUS server, a "login" request prompts it to store the user and the associated MAC address directly in the internal Status table. As a result, the user is immediately authenticated in future, and there is no need to display a login page for entering the username and password.

When you operate a RADIUS server, a 'login' request can only be successfully processed if the login data of the corresponding user already exists on the RADIUS server.

Note: The Web API in the Public Spot provides you with a convenient tool for creating new Public Spot users on the device's internal RADIUS server. Further information about this, see “Managing Public Spot users via the web API” on page 467.

The XML interface can process the following XML elements for a request:

- ☐ `SUB_USER_NAME`

  User name

- ☐ `SUB_PASSWORD`

  User password

- ☐ `SUB_MAC_ADDR`

  MAC address of the user's device Possible formats include:

  – 00164115208c
  – 00:16:41:15:20:8c
  – 00-16-41-15-20-8c

The XML interface then sends the gateway a "Login" response, which can contain the following XML elements:

☐ SUB_USER_NAME

User name

☐ SUB_STATUS

The current user status. The following values are possible:

– RADIUS_LOGIN_ACCEPT: Login successful

– RADIUS_LOGIN_REJECT: Login rejected

☐ SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

– 00164115208c

– 00:16:41:15:20:8c

– 00-16-41-15-20-8c

Some examples of XML files are given below:

☐ **Login request**

The external gateway sends the data for the start of a session to the Public Spot:

☐
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGIN">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

The Public Spot enables 'user2350' in the internal Status table.

☐ **Login response:**

The XML interface sends a confirmation about the start of a session to the external gateway:

☐
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_LOGIN_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
```

```
        <TXRATELIMIT>0</TXRATELIMIT>
        <RXRATELIMIT>0</RXRATELIMIT>
        <SECONDSEXPIRE>0</SECONDSEXPIRE>
        <TRAFFICEXPIRE>0</TRAFFICEXPIRE>
        <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
        <IDLETIMEOUT>0</IDLETIMEOUT>
        </ACCESS_CUBE>
    </PUBLICSPOTXMLINTERFACE>
```

Logout

If the external gateway sends a "Logout" request in an XML file, the Public Spot blocks the corresponding user's online access. A "Logout" request contains the attribute `COMMAND="RADIUS_LOGOUT"`.

The XML interface can process the following XML elements for a request:

☐ `SUB_USER_NAME`

User name

If the device receives this request and the Public Spot module discovers that this user is online with the corresponding MAC, then this user is logged out.

☐ `SUB_MAC_ADDR`

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

☐ `TERMINATION_CAUSE`

Reason for the user to log off

The XML interface then sends the gateway a "Logout" response, which can contain the following XML elements:

☐ `SUB_USER_NAME`

User name

☐ `SUB_STATUS`

The current user status. The following values are possible:

- RADIUS_LOGOUT_DONE: Logout successful
- RADIUS_LOGOUT_REJECT: Logout rejected

☐ SUB_MAC_ADDR

MAC address of the user's device Possible formats include:

- 00164115208c
- 00:16:41:15:20:8c
- 00-16-41-15-20-8c

☐ TERMINATION_CAUSE

Reason for blocking access

Some examples of XML files are given below:

☐ **Logout request**

The external gateway sends the command for ending a session to the Public Spot:

☐
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_LOGOUT">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TERMINATION_CAUSE>Check-Out</TERMINATION_CAUSE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

☐ **Logout response:**

The XML interface sends a confirmation about the end of a session to the external gateway:

☐
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_LOGOUT_DONE</SUB_STATUS>
```

```
      <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
      <SUB_USER_NAWLC_PMME>user2350</SUB_USER_NAME>
      <TERMINATION_CAUSE>User logout request</TERMINATION_CAUSE>
     </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

Status

The external gateway queries the current status of a user from the Public Spot with a "Status" request. A "Status" request contains the attribute `COMMAND="RADIUS_Status"`.

The XML interface can process the following XML elements for a request:

☐ `SUB_USER_NAME`

User name

☐ `SUB_MAC_ADDR`

MAC address of the user's device Possible formats include:

– 00164115208c

– 00:16:41:15:20:8c

– 00-16-41-15-20-8c

The XML interface then sends the gateway a "Status" response, which can contain the following XML elements:

☐ `SUB_USER_NAME`

User name

☐ `SUB_MAC_ADDR`

MAC address of the user's device Possible formats include:

– 00164115208c

– 00:16:41:15:20:8c

– 00-16-41-15-20-8c

☐ `SUB_STATUS`

The current user status. The following values are possible:

- RADIUS_STATUS_DONE: Status request successful
- RADIUS_STATUS_REJECT: Status request rejected, e.g. unknown user or MAC address

☐ SESSION_TXBYTES

Current sent data volume

☐ SESSION_RXBYTES

Current received data volume

☐ SESSION_TXPACKETS

Number of data packets sent so far

☐ SESSION_RXPACKETS

Number of data packets received so far

☐ SESSION_STATE

Current status of the session

☐ SESSION_ACTUAL_TIME

Current time

Some examples of XML files are given below:

☐ **Status request**

The external gateway sends the command for a status request to the Public Spot:

☐
```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_STATUS">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

☐ **Status response:**

The XML interface sends a status message to the external gateway:

☐
```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
   <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2"
COMMAND="USER_STATUS">
     <SUB_STATUS>RADIUS_STATUS_DONE</SUB_STATUS>
```

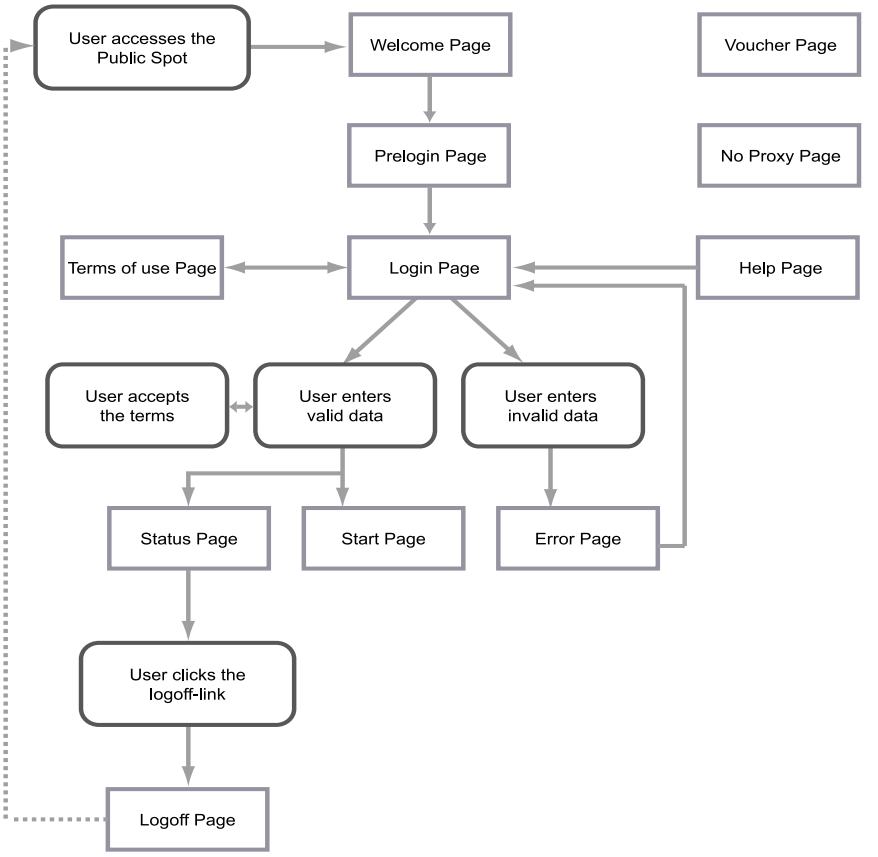
```
      <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
      <SUB_USER_NAME>user2350</SUB_USER_NAME>
      <SESSION_ID>2</SESSION_ID>
      <SESSION_TXBYTES>0</SESSION_TXBYTES>
      <SESSION_RXBYTES>0</SESSION_RXBYTES>
      <SESSION_TXPACKETS>0</SESSION_TXPACKETS>
      <SESSION_RXPACKETS>0</SESSION_RXPACKETS>
      <SESSION_STATE>Authenticated</SESSION_STATE>
      <SESSION_ACTUAL_TIME>0</SESSION_ACTUAL_TIME>
   </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

6.9 Internal and customized voucher and authentication pages (templates)

By default, your device uses pre-installed templates for the login page and all other authentication pages that your user sees before, during and after a Public Spot session. However, you do have the option of adapting the individual web pages to your requirements and changing the design. You need basic HTML knowledge of DIV containers and cascading style sheets (CSS), in order to effectively change the structure and layout of the individual pages.

6.9.1 Possible authentication pages

The following flow-chart shows an overview and interaction of all authentication pages available with the Public Spot module: The chart takes the example of authentication using access credentials. Depending on the authentication mode and errors that can occur, the interaction may vary slightly:


User accesses the Public Spot
Welcome Page
Voucher Page
Prelogin Page
No Proxy Page
Terms of use Page
Login Page
Help Page
User accepts the terms
User enters valid data
User enters invalid data
Status Page
Start Page
Error Page
User clicks the logoff-link
Logoff Page

The "Welcome" or "Login" pages are displayed to users when they access the Internet or the Public Spot for the first time.

- The "Welcome" page precedes the login page and is optional for most authentication modes: You can use this page, for example, to welcome a user, to provide information about the services available, or to provide instructions on how to use the Public Spot before continuing to the Start page with the login form. Only if you have selected the authentication mode "Login via agreement" is it compulsory for a customized Welcome page (containing the agreement) to be displayed, because it takes the place of the login form on the login page.

  Note: The pre-installed default pages on your device do not include a Welcome page. If you set up this type of page without loading a template onto the device or an external server, the user either lands directly to the login page or receives an error message, depending on the login mode.

- "Authentication" includes the login form, assuming that Public Spot authentication requires the use of access credentials and that the latter have to be requested.
- The page with the "Terms of use" is only displayed if you require the confirmation of your terms of use for the selected authentication mode. In this case, a check box is displayed below the login form with an extra link that opens the terms in a pop-up.

Note: The default pages installed on your device only include a placeholder and a generic Terms and Conditions page.

After the user has logged in with his login data (if necessary), the device checks that the information is correct and displays either an "Error" page, which sends the users back to the login page, or shows the "Start" page.

- Here, the "Error" page is only displayed to unauthenticated Public Spot users, which means that it is more or less directly associated with the login process. Typical situations in which a user sees the error page include unauthorized access to the Public Spot, when a user limit is exceeded, failed authentication due to the entry of incorrect credentials,

or in case of failure of the authentication server. If you have set up monitoring of a remote site, the page could also appear whenever the Public Spot module registers a WAN link disconnection, as it provides advance notice to potential users about the lack of network availability (see “Error page in case of WAN connection failure” on page 490).

Users who are already authenticated will see an appropriate error message from their browser.

- If there are no errors during login, the "Start" page verifies the successful login and after a few seconds redirects the user to the Internet page originally requested by user.

Additionally, a successful login is followed by a popup window with the "Status" page.

- The "Status" page shows the user the current information about his session (e.g., time used so far, sent/received data volumes, and validity period for his account). It also offers a link to close the session and stop the accounting. A user clicking on this link is redirected to the "Logout" page.
- The "Logout" page confirms to the user that the logout from the Public Spot was successful.

The remaining "Fallback error", "Help" and "No-proxy" pages are isolated pages not related to the login process.

- The "Fallback error" page appears whenever the device cannot deliver a custom template page and the fallback to the HiLCOS internal default page is missing. Delivery can fail, for example, if you have specified an incorrect file path within the pages table, or if the template page does not exist on the device.
- The "No-proxy" page is displayed whenever a user tries to connect via HTTP on port 8080 instead of port 80. In intranets, port 8080 is typically used for HTTP proxies. Since this proxy is configured with a static IP address in the browser settings, but these cannot be configured via DHCP, the user would not be able to reach this proxy. The purpose of this page is just to instruct the user to disable the proxy before the user can proceed.
- The "Help" page is only a placeholder used to embed and display specific information (e.g., details about the login or where to get vouchers) on the remaining authentication pages (e.g. the Welcome page). The default pages contain neither a help page nor any link pointing to such a page. To use a help page, you must first create a custom template page.

The "Voucher" page is not one of the authentication pages: This is the graphic template for printing the vouchers. By uploading your own template, you can print tickets with the corporate design of your own company.

6.9.2 Pre-installed default pages

Ex-factory, your device comes pre-installed with all of the pages you need to setup an operational Public Spot.

The following table gives you a quick overview of the default pages included with HiLCOS:

Table 4: Overview of installed default pages

Page designation	Pre-installed?
Welcome…	No
Login...	Yes
Error...	Yes
Start…	Yes
Status…	Yes
Logoff...	Yes
Help...	No
No proxy	No
Voucher…	Yes
Terms of use...	No
Fallback error	Yes
Authentication (e-mail)...	Yes
Prelogin (e-mail)...	Yes
Login (e-mail to SMS)...	Yes
Prelogin (e-mail to SMS)...	Yes

These pages were deliberately designed to be simple, not to use any fancy features like dynamic HTML or Java Script, and just to present the necessary elements as-is. The use of plain XHTML and CSS to produce the necessary elements only ensures that the pages appear correctly on a variety of browsers and screen sizes.

As the operator of a hotspot you may want to design more sophisticated pages or display a more neutral page without the manufacturer's logo. For that reason, the Public Spot module gives you the option to customize some of the default pages, or if necessary to replace them with your own design. The latter can be done either by using HTTP redirection or templates that you upload to the device and that the device processes like an intelligent HTML pre-processor. These template pages can be stored directly to the flash memory, so you can do without an external HTTP server.

Additional languages for the authentication pages

With HiLCOS 8.90, the Public Spot module authentication pages now support the languages French, Spanish, Italian and Dutch (i.e. all pre-installed default pages except for the voucher page). This allows you to offer Public Spot access to a broader range of international users. The language displayed is determined by the settings in the Web browser used to access the Public Spot.

Note: Multilingual support refers exclusively to the HiLCOS internal default pages. You can implement multilingual customized template pages with an external server.

6.9.3 Customizing the standard pages

As an alternative to installing complete user-defined Web pages, the device provides the option of customizing the pre-installed default pages to a certain extent. This includes for example the input of a login text that is displayed to your users in the registration form, or replacing the header image (logo). In this way, you can quickly deploy a customized Public Spot without having to deal in-depth with the subject of the Web page authoring.

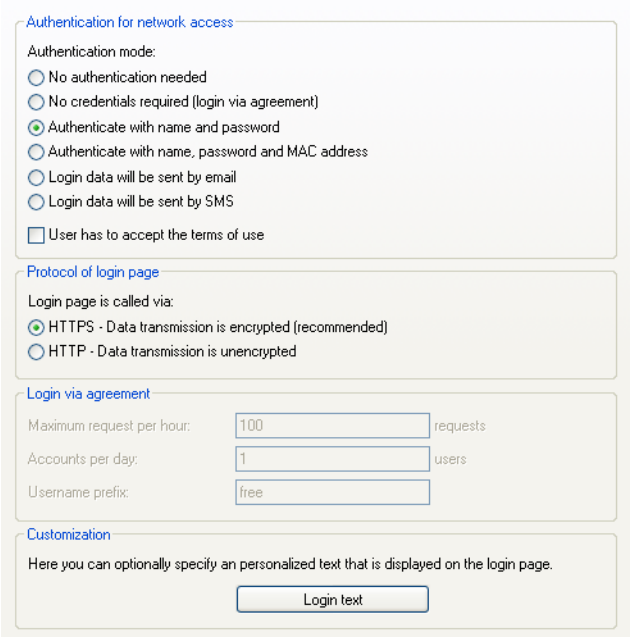
Customized text on the login page

The Public Spot module gives you the option to specify customized text, which appears on the login page inside the box of the login form. This "Login text" can be stored in multiple languages. The language displayed by the device depends on the language settings of the user's Web browser. If no customized login text is specified for a language, then the device falls back to the English login text (if available).

Carry out the following steps to set up customized text on the login page.

☐ In LANconfig, open the configuration dialog for the device.

☐ Navigate to the dialog `Public Spot : Authentication`, click on "Login text" and select a language.



☐ In the dialog that opens, enter the text that your Public Spot should display to users. You can enter an HTML string with max. 254 characters composed of:

☐ `[Leerzeichen][0-9][A-Z[a-z] @{|}~!$%&'()+-,/:;<=>?[\]^_.#*`

LANconfig automatically transforms umlauts into their respective equivalents (ü to `ue`; ß to `ss`; etc.). To type umlauts, use their HTML equivalents (such as `ü` for ü), because the text is directly embedded in the Web page. You can also use HTML tags to structure and format the text. Example:

☐ `Welcome!<br/><i>Please complete this form.</i>)`

☐ Click "OK" to complete your entries and load the configuration back to the device.

Once the configuration has been written successfully, the new login text appears the next time the Public Spot page is called.

Custom header images for variable screen widths

A component of the pre-installed pages in the device is a header image (logo), which is displayed to your users above the login form for the Public Spot. You can change this header image as you please, for example to reflect the application environment or your corporate design. There is no need for an external Web server; you can simply upload the image directly into the device via the file management in WEBconfig or the configuration management in LANconfig.

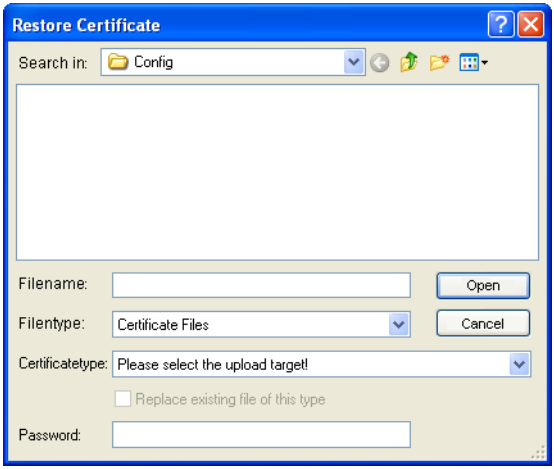
A special feature of the header image is that it is available in the device as two possible variants: One version is for large screens or browser windows with a horizontal resolution exceeding 800 px (normal monitors, laptops, tablet PCs, etc.), and one is a small picture for screens with a lower horizontal resolution (PDAs, mobile phones, etc.). This allows you to provide header images for different target groups and to provide them a login page that is appropriate for their device.

The available resolutions are set by the CSS file of the device. The pre-installed default graphics allow for 800x150 px for the large screen and 258x52 px for the small screen. The file type must be either JPG, GIF, or PNG.

To upload a new header image to the device either as a large or small version, follow the steps below.

☐ Start LANconfig and highlight the device.

☐ In the menu bar, click on `Device : Configuration management : Upload certificate or file`. The "Restore Certificate" dialog opens.



☐ Set the "File type" to "All files" and select the "Certificate type" that you want to upload.

– "Public Spot - Header image of pages": Certificate type for large screens

– "Public Spot - Header image box": Certificate type for small screens

☐ Choose your custom header image and click on "Open". LANconfig then starts the file upload.

After uploading successfully, the new header image appears the next time the Public Spot page is called.

Note: You can check that the large and small header images are displayed by your Public Spot by setting your browser window width to >800 px and then reducing the width of the window. The CSS technology automatically switches between the large and small pictures.

Show/hide manufacturer logo and header on the voucher

In the default settings, the device outputs a voucher with the header image and logo used on the Public Spot start page. The "Print header and company emblem" option under `Public Spot : Wizard` allows you to disable these graphics directly on the device without having to upload a customized version of the voucher template. In this case a neutral text voucher is printed.

6.9.4 Configuration of user-defined pages

If you would like to replace the pre-installed pages with your own webpages, you can either store them directly on the device or on an external HTTP server. Sophisticated HTML pages may require more storage space than the space available on the device. There are additional advantages when using websites from an external server:

- Changes can be applied centrally. This reduces the effort required to change the login pages when using several devices.
- The server can dynamically provide the pages whose appearance is influenced by the information that the device provides. This information is discussed in more detail in the following chapters.

The storage location for the templates is entered in LANconfig in `Public Spot : Server : Page table : <Name of the template> : Page address (URL)`. There are currently three protocols available for the URL:

- `http://...`: Fetch the page via HTTP from an external server. TCP-port overrides and user/password specifications are possible.
- `https://...`: Similar to HTTP, but use HTTP over SSL for an encrypted connection.
- `file://...`: Retrieve the template from the given file in the device's local file system.

You can use any file name. If you decide to store the template pages in the device's local memory, they require the URLs reserved specially for this purpose. An internal standard page will be replaced by a new page loaded into the device by entering the local URL as the "Page address (URL)".

Table 5: Overview of the reserved file names for template pages

Local URL on your device	Page designation
file://pbspot_template_welcome	Welcome…
file://pbspot_template_login	Login...
file://pbspot_template_error	Error...
file://pbspot_template_start	Start…
file://pbspot_template_status	Status…
file://pbspot_template_logoff	Logoff...
file://pbspot_template_help	Help...
file://pbspot_template_noproxy	No proxy
file://pbspot_template_voucher	Voucher…*
file://pbspot_template_agb	Terms of use...
file://pbspot_template_fallback	Fallback error
file://pbspot_template_reg_email	Prelogin (e-mail)...
file://pbspot_template_login_email	Authentication (e-mail)...
file://pbspot_template_reg_sms	Prelogin (e-mail to SMS)...
file://pbspot_template_login_sms	Login (e-mail to SMS)...

*Template for printing vouchers, no authentication page

Note: By uploading user-defined webpages, only the webpages that are pre-installed on the device are replaced, but not overwritten. They can be rolled back to the device's proprietary default pages at any time by deleting the local URL.

Note: To provide the highest possible compatibility with earlier display devices and web browsers, you should avoid using frames, if possible. Also, specialized content such as JavaScript or plug-in elements can lead to an erroneous display.

Login pages depending on the login mode

The following table provides an overview of which login page is displayed by the device in the various authentication modes. If a login mode has no customized page template, the Public Spot module takes the default HiLCOS page:

Table 6: Overview of login pages of each authentication mode

Authentication mode	Page designation
No authentication required	–
No credentials required (login after agreement)	Welcome…
Authenticate with name and password	Login...
Authenticate with name, password and MAC address	Login...
Login data will be sent by e-mail	▶ Prelogin (e-mail)... ▶ Authentication (e-mail)...
Login data will be sent by SMS (text message)	▶ Prelogin (e-mail to SMS)... ▶ Login (e-mail to SMS)...

Special template pages for Smart Ticket

The Public Spot module before HiLCOS version 8.90 used a central login page to for all authentication modes. As of HiLCOS 8.90, you can optionally equip the device with separate template pages for the Smart Ticket function (for self-sufficient user registration via e-mail/SMS). Two pages have to be configured for registration via e-mail/SMS: "Registration(...)" and "Login(...)".

- On the registration page, users enter their personal data (e-mail address or mobile phone number) to register for the Public Spot and to request its login data.
- On the login page, users then enter their credentials in order to authenticate at the Public Spot.

The following table provides an overview of the related dependencies that you need to create your own page templates:

Table 7: Overview of dependencies of the SmartTicket login pages

Authentication mode	Page designation	Local URL on your device	Page template identifiers
Login data will be sent by e-mail	Prelogin (e-mail)...	file://pbspot_template_reg_email	<regemailform>
	Authentication (e-mail)...	file://pbspot_template_login_email	<loginemailform>
Login data will be sent by SMS (text message)	Prelogin (e-mail to SMS)...	file://pbspot_template_reg_sms	<regsmsform>
	Login (e-mail to SMS)...	file://pbspot_template_login_sms	<loginsmsform>

6.9.5 Setting up a customized template page

A custom template page allows you to replace the internal HiLCOS template pages with your own Web pages. This does not overwrite the HiLCOS templates, but just exchanges them for your own pages. If need be, you can fallback to the standard pages.

The steps below use the example of a "Login" page to show you how to set up a custom template page with the help of LANconfig.

☐ You can load your customized error page either onto an external HTTP(S)-server or as the "Public Spot - Login page (* .html, * .htm)" into the memory of the device.

☐ Open the device configuration dialog in LANconfig, navigate to the `Public Spot : Server` dialog and select `Page table : Login`.

☐ Enter the URL of the login page on the external server under "Page address (URL)" or the reference for a file on the local device (`file://pbspot_template_login`).

☐ You can make these additional settings if necessary.

– "Request type": If you are using an external server, you can change the way in which the page is called. By default (in the setting "Template") the device loads an externally stored HTM(L) page from the specified URL for further processing by the internal HTTP server. If you change the setting to "Redirect", the device outsources the processing of the pages to the external server (also see “User-defined pages via HTTP redirect” on page 574).

– "Fallback to implemented page": If you use an external server and chose the template type "Request", the Public Spot module is able to use the internal HiLCOS template in case of HTTP(S) errors (e.g. if the server is unavailable). This enables the Public Spot to continue operating (also see “Auto-fallback” on page 576). If you do not activate this setting, the Public Spot displays the fallback error page instead.

– "Sender address": This setting allows you to specify the loopback address used by the device to connect to the external HTTP(S) server. By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

☐ Close this dialog and also the general configuration dialog each with click on "OK". LANconfig then writes the new settings back to the device.

That's it!

6.9.6 User-defined pages via HTTP redirect

If you implement user-defined pages with redirection (request type: redirect), your device transforms it as follows: Whenever your device must send the respective page to a client, it will expand the URL according to the rules given in the previous chapter and will send an HTTP 307 (temporary redirect) response to the device, with this URL as the new location.

Redirects are particularly meaningful if you use a welcome page and all authentications should be performed on one external gateway. In this case, the clients can be immediately redirected to this gateway. This feature is often used with the external device controller.

6.9.7 User-defined pages via page templates

The device can alternatively act as a client and use the extended URL to download a user-defined page via an HTTP connection. The internal pre-processor takes of the processing of the page and subsequently sends the result to the Public Spot user. This pre-processor makes it possible to process session-specific data, although the server has a static page available. The URL syntax understood by the device's built-in HTTP client is the syntax recognized by web browsers. However, only a subset of what is recognized by browsers is supported:Usage of symbolic names for the server's host instead of plain IP addresses is supported, given that DNS is properly configured. In many aspects, this mechanism can be considered like a proxy, which fetches HTML pages and then sends them to the client. The biggest difference is that the URL of the pages is determined by the device and not by the client of the Public Spot user.

- The user authentication is performed using the form `user:password@host/...`
- The device is incapable of automatically resolving non-fatal HTTP errors such as redirects. Make sure that an access to this page will return the page directly.

Auto-fallback

For every entry in the page table, it is possible to individually define whether a fallback should be used or not. This fallback feature is only meaningful if a page is defined as a template (request type: template), and not as a redirect (request type: redirect). While fetching a page via HTTP, various errors can appear:

- The DNS lookup for a host name may fail.
- The TCP/HTTP connection to the server may fail.
- The HTTP server may respond with an error code (e.g. 404 if an invalid URL was given).

By default, the device passes this type of error on to the user so that the user can start a new request or inform the provider of the Public Spot. Alternatively, the configuration of a fallback feature can ensure that the hotspot continues to function by using the default pages instead. You enable the fallback feature in LANconfig using the setting "Fallback to implemented page".

Passed HTTP attributes

As mentioned above, in some respects the device may be seen as an HTTP proxy that fetches login and status pages for the client. HTTP proxies are obliged to keep certain HTTP attributes intact while forwarding a client request:

- The device forwards cookies between the client and the server. Client cookie values can also be sent transparently to the server and the server can set cookies on the client. Using cookies is necessary if the files that are sent from the server have ASP scripts, since ASP stores the session ID in a cookie.
- The device will forward the `User-Agent` value provided by the client. This allows a server to deliver different pages, based on the browser and system platform on the client side. PDAs and mobile phones for example call for web pages optimised for their small displays.

- The device inserts an `X-Forwarded-For` line into the HTTP request to report the device's IP address.
- WEBconfig generally attempts to use a tag named `Accept-Languages` provided by client browsers to match the request to one of the languages provided by its internal message tables (currently, only German and English). The selected language is communicated to the server via another `Accept-Languages` tag, in the hope that the server will provide a page in the appropriate language. When the server delivers the page, the device will check for a Language tag in the server's response to see if the server was actually capable of delivering a page in the requested language. If not, it will adapt the strings used in template expansion (see next section) to the actual language of the page.

6.9.8 URL placeholder (template variables)

The URLs specified in the page table do not need to be absolute strings. You have the option to integrate template variables in the address which are then filled-out with parameters from a Public Spot session when the device requests the pages from the server. Placeholders have a form similar to C format strings, e.g., a percent sign immediately followed by a single, lowercase character. The following placeholders are defined:

☐ **%a**

Inserts the device's IP address. The placeholder only returns a value if the "Request type" in the "Page table" is set to `Template`.

Note: Note that this placeholder cannot generate a reachable address if the device itself is located behind another router with activated NAT.

☐ **%c**

Inserts the LAN MAC address of the Public Spot device as a 12-character hexadecimal string. The output is in the format 'aa:bb:cc:dd:ee:ff'.

☐ **%e**

Inserts the device serial number.

☐ **%i**

Inserts the NAS port ID. In this context, 'NAS' stands for 'Network Access Server'. This variable contains the interface of the device that the client used to login. For a WLC or router without WLAN this corresponds to a physical interface, such as `LAN-1`, or, for a standalone access point, it is the SSID.

☐ **%l**

Inserts the device host name.

☐ **%m**

Inserts the MAC address of the client as a 12-character hexadecimal string. The individual bytes are separated by colons.

☐ **%n**

Inserts the name of the device the way it is configured in the setup menu under "Name".

☐ **%o**

Inserts the URL of the Internet page which the user initially requested. After successful authentication, the device forwards the user to this URL.

☐ **%p**

Adds the IP address of the Public Spot device to the ARF context of the respective client.

Assuming that your device is active in various IP networks, you can use this variable to specify the IP address used by the device in the network where the client is also located.

☐ **%r**

Inserts the client's IP address.

☐ **%s**

If the client is connected to the device via a WLAN interface, this placeholder will insert the WLAN SSID used in the network that the client is connected to. This feature is particularly interesting when MultiSSID is used, since this gives the server the opportunity to display different pages based on the SSID. If the client is connected via another access point that connects to the device via a Point-2-Point connection, the SSID of the first WLAN will be inserted. If the client is connect via Ethernet, the placeholder remains empty.

☐ **%t**

Inserts the routing tag which is appended to the client's data packets.

☐ **%v**

If the requesting client is assigned an individual VLAN ID, this variable contains the source VLAN ID.

☐ **%0-9**

Inserts a single number between 0 and 9.

☐ **%%**

Inserts a single percent character.

In order to be able to use variables for a template, add the parameters to the "Page address (URL)" in the page table. In the following URLs the variable `%i` is replaced with `LAN-1` as described in the sample above:

Example:`http://192.168.1.1/welcome.php?nas=%i`

Example:`http://192.168.1.1/%i_welcome.html`

6.9.9 Tags and syntax of page templates

After the device receives the page from the server, it performs some transformations to the page template before sending it to the client. These transformations replace pre-defined HTML tag placeholders with data belonging to the client's current session (e.g. the current resource consumption in the status page). An HTML page delivered by the server could therefore better be described as a template for an actual HTML page displayed in the client's browser. HTML syntax was chosen for the placeholders to allow editing of page templates without interfering with syntax sensitive HTML editors.

In total, three placeholder tags are defined:

- `<pblink identifier>text</pblink>`

  Marks **text** as a clickable link to an **identifier**, typically to link to another page. Note that </pblink>is just an alias for , since this symmetrical definition causes less trouble with HTML syntax checkers. For example, the following fragment defines a link to the help page:

- `Please click <pblink helplink>here</pblink>for help.`

- `<pbelem identifier>`

  Insert the item specified by **identifier** at this place. For example, the following line inserts the user's time credit:

- `Session will be ended in <pbelem sesstimeout>.`

- `<pbcond identifier(s)>code</pbcond>`

  Only insert **code** into the page if all the identifiers are TRUE, i.e. numeric values are not equal to zero and string values are not empty. Note that the current implementation does not allow nested conditionals. Continuing from the previous example, the session timeout is only displayed if there is a time limit (a session without timeout internally has a session timeout of zero):

- ```
  <pbcond sesstimeout>Session will be terminated in <pbelem
  sesstimeout>seconds.</pbcond>
  ```
  ```

6.9.10 Page template identifiers

The following identifiers can be used when designing customized template pages. The device does not differentiate between upper and lower case.

Note: Please note that not all identifiers are available for all printouts! Not all identifiers are available on all pages.

☐ **ACCOUNTED**

Valid for:`<pbelem>`

This identifier supplements the voucher with information about the voucher's validity, i.e. from when and until when the created access account is valid.

☐ **APADDR**

Valid for:`<pbelem>`

This identifier contains the Public Spot's IP address, as seen from the client's perspective. Can be used for user-defined login forms when the `LOGINFORM` element is not used.

☐ **AUTOPRINT**

Valid for:`<pbelem>`

This identifier inserts a Java script into the page with the instruction to open the print dialog for printing the displayed page. Please note that in this case you **must** complete the `pbelem` tag with a separate `script`, e.g. `<pbelem autoprint></script>`.

☐ **COMMENT**

Valid for:`<pbelem>`

This identifier adds an optional comment to the voucher, assuming that you have entered an appropriate text into the Setup Wizard.

☐ **HELPLINK**

Valid for:`<pbelem>`

This identifier contains the URL to the help page provided by the device.

☐ **LOGINEMAILFORM**

Valid for:<pbelem>

For authentication via Smart Ticket, this identifier contains the HTML form for authenticating at the Public Spot with credentials provided by e-mail.

☐ **LOGINERRORMSG**

Valid for:<pbelem>

This identifier returns the error message from HiLCOS in the case of a failed authentication or a WAN-connection failure. This identifier is only available on the general error page and the fallback error page.

Note: To retrieve the error message from the RADIUS server in the event of a failed authentication, use the identifier **SERVERMSG**.

☐ **LOGINFORM**

Valid for:<pbelem>

This identifier contains the HTML form for authentication at the Public Spot when authenticating with user name and password (and MAC address, if applicable).

☐ **LOGINLINK**

Valid for:<pbelem>

This identifier contains the URL to the login page provided by the device.

☐ **LOGINSMSFORM**

Valid for:<pbelem>

For authentication via Smart Ticket, this identifier contains the HTML form for authenticating at the Public Spot with credentials provided by SMS.

☐ **LOGOFFLINK**

Valid for:<pbelem>

This identifier contains the URL to the logout page provided by the device.

☐ **ORIGLINK**

Valid for:<pbelem><pblink><pbcond>

This identifier contains the URL originally requested by the user prior to the authentication process. If it is unknown, this value is empty.

☐ **PASSWORD**

Valid for:<pbelem>

On a voucher, this identifier contains the password for Public Spot access.

☐ **REDIRURL**

Valid for:<pbelem><pblink><pbcond>

This identifier holds a possible redirection URL contained in the RADIUS server's authentication response (if there was one). It is only defined for the error and start page.

☐ **REGEMAILFORM**

Valid for:<pbelem>

For authentication via Smart Ticket, this identifier contains the HTML form for requesting the access credentials via e-mail (registration).

☐ **REGSMSFORM**

Valid for:<pbelem>

For authentication via Smart Ticket, this identifier contains the HTML form for requesting the access credentials via SMS (registration).

☐ **RXBYTES**

Valid for:<pbelem>

This identifier contains the amount of data so far received by the device from the client in this session, expressed in bytes. It is zero for a station that is not logged in.

☐ **RXTXBYTES**

Valid for:<pbelem>

This identifier contains the amount of data received by the device from the client so far, or sent to the client in this session, expressed in bytes. This means that it is the sum of TXBYTES and RXBYTES.

☐ **SERVERMSG**

Valid for:<pbelem><pbcond>

This identifier holds the reply message contained in the RADIUS server's authentication response (if there was one). Only applicable for the error and start pages. In the case of a failed authentication, this identifier contains the error message from the RADIUS server.

Note: To retrieve the error message from the HiLCOS server in the event of a failed authentication, use the identifier **LOGINERRORMSG**.

☐ **SESSIONSTATUS**

Valid for:`<pbelem>`

This identifier contains a textual representation of the current status of the client relative to the device (whether authenticated or not).

☐ **SESSIONTIME**

Valid for:`<pbelem>`

This identifier contains the time that has passed since the login on the Public Spot.

☐ **SESSTIMEOUT**

Valid for:`<pbelem>`<pbcond>

This identifier contains the remaining time for the current session. After this time, the device ends the current session automatically. This identifier is zero for a session with no time limit.

☐ **SSID**

Valid for:`<pbelem>`<pbcond>

This identifier on a voucher contains the SSID to be used for Public Spot access.

☐ **STATUSLINK**

Valid for:`<pbelem>`<pbcond>

This identifier contains the URL to the logout page provided by the device. A reference that opens a new browser window is automatically generated within the `<pblink>` element.

☐ **TXBYTES**

Valid for:`<pbelem>`

This identifier contains the amount of data transmitted by the device to the client so far in this session.

☐ **USER NAME**

Valid for:<pbcond>

This identifier allows you to supplement the voucher page with conditional HTML code, which is only printed for certain users or administrators. USER is a prefix and **must** be placed before the user name (NAME) and a space. To generate HTML output specifically for the user 'root' when calling the voucher page, use the following syntax:

☐ `<pbcond USER root>Conditional HTML Code</pbcond>`

When used in larger Public Spot scenarios with central administration, such as with a WLAN controller, this dependency can be used for the purpose of site localization: To do this, you create a Public Spot admin for each of the relevant access points and you specify a conditional voucher text for each administrator.

☐ **USERID**

Valid for:<pbelem>

This identifier contains the user ID (in the form of the username) with which the current session was started. The identifier is not specified if the client is not (yet) logged in.

☐ **VOLLIMIT**

Valid for:<pbelem><pbcond>

This identifier contains the amount of data, expressed in bytes, that the client is still allowed to transfer before the device terminates the current session. This identifier is zero for a session with no data limit.

☐ **VOUCHERIMG**

Valid for:<pbelem>

This identifier inserts the page banner image (in large size) into the page.

6.9.11 Graphics in user-defined pages

All but the simplest web pages contain images, which are fetched by the client's browser independent of the HTML page itself. The graphic files for the pre-installed page are also stored on the device. The device automatically adapts the necessary permissions so that even unauthorized clients have access to the images without problems. However, every access to the referenced (device-external) images for user-defined pages are treated like a normal Internet access, and would automatically send the user back to the welcome or start page.

In order to avoid this behavior, you should make sure that the servers where the graphics are stored are included in the **free servers**. Free servers are addresses that have unlimited access, and are therefore also accessible by unauthenticated clients, and are not billed by the accounting feature in the same way as the rest of the data traffic.

The chapter "Open access networks (no login)" on page 465 contains additional information about configuring free servers. Note that if a user-defined page is defined as a redirect, this of course has to be defined as a free IP address.

6.10 Access to the Public Spot

6.10.1 Requirements for logging in

- Device with network adapter
- Operating systems supporting the TCP/IP protocol (automatic IP-address retrieval by DHCP active)
- Web browser (supporting JavaScript and Frames)
- Direct Internet access (use of proxy deactivated)
- WLAN access information (network name, encryption information)
- Valid user data (user identifier and password)

Information for WLAN access

A maximum of two pieces of information are required to access the WLAN:

- **The network name of the WLAN (SSID)**

  If the Public Spot's base stations are configured for operation as a closed network, the user must know the exact name of the wireless LAN, its SSID.

- **Wireless LAN encryption**

  Although it is possible to provide guest access via encrypted connections using, for example, WPA, Public Spots are not generally operated with WLAN encryption. Protection is provided in this case using authentication with a username and password. Data security when transmitting data on the Public Spot must be provided by the end user (e.g., using a VPN client).

Information for LAN access

If the IP addresses on your network are automatically assigned (for example, via DHCP), your users only need:

- a LAN socket that connects to the Public Spot.
- a LAN cable to connect their LAN adapter to the LAN socket.

Information for authentication

The user needs to have the following information to hand when logging in:

- User identifier
- Password
- MAC address

  If you set the authentication mode for a Public Spot at the base station to "MAC+User+Password", you, as the operator, must know the MAC addresses of the end devices employed by your users. An end device automatically and continuously transmits its MAC address when communicating with a base station. The user does not have to manually enter this information when logging in, but instead it is communicated just once to the operator before attempting to login.

6.10.2 Logging in to the Public Spot

☐ Log in to the WLAN of the Public Spot (for WLAN connections) or connect to the network using an Ethernet cable (for LAN connections).

The different types of mobile devices and WLAN adapters offer various ways of entering the settings required for accessing the WLAN. Many devices require the network name (SSID) of the WLAN to be entered into the configuration program for the WLAN adapter. Some other products also provide an overview of all base stations in the vicinity, from which the user simply chooses the one they want to use.

Depending on the configuration, the user receives the necessary settings for the LAN-adapter connection either automatically from the network or a connected DHCP server, or from the network administrator.

☐ Start your Web browser.

As soon as the Web browser attempts to access any Internet site, the Public Spot automatically intervenes and presents the login page. The login page, or the login form displayed within it, appear differently depending on which firmware version you are using and which login mode you have selected. In the following, we assume a login with a voucher (or by user name and password).

☐ Enter the complete "user ID" and "password" in the corresponding fields and confirm your entries with "Login".

Note: To login, you should use a Web browser with JavaScript support enabled to ensure that session status information can be displayed in a popup window.

If the login to the Public Spot is successful, an additional window pops up with the main information about the current session. This window is also used for the login. This window should be left open throughout the session (e.g., it can be minimized).

If the login fails, an error page opens with a request to return to the login page and to repeat the authentication. The form takes over a portion of the previously entered data as an aid to the user, e.g. in case of typos.

Any number format for Smart Ticket

As of HiLCOS 8.90, Smart Ticket users requesting credentials via SMS can enter their phone number in any format to (0044.../+44.../etc.). The device automatically removes any leading zeros or a leading '+' character and saves the phone number in a standardized format (44...) to the RADIUS user table.

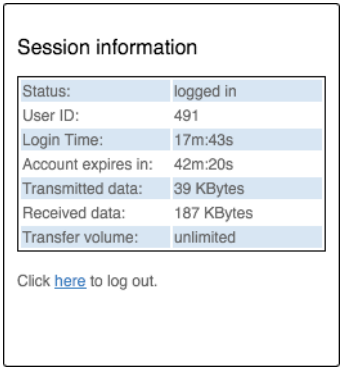
6.10.3 Session information

The window with session information is automatically updated at regular intervals. Along with the status and current user ID, the information displayed includes the connection time and the volume of transferred data.

If the session-information window is not open, you can open it by entering the following in the address line in the browser:

```
http://<IP address of the Public Spot>/authen/status/
```

Alternatively, you can open the session page with the short URL `http://logout`.



6.10.4 Logging out of the Public Spot

The session information window can be used to logout from the Public Spot. Click on "here" in the bottom line of text in the window.

If the session-information window is not open, you can enter the following into the address line in the browser:

`http://<IP address of the Public Spot>/authen/logout`

Alternatively, you can open the session page with the short URL `http://logout` to logout from the Public Spot.

Note: The operator can set up the Public Spot to automatically logoff users if they cannot be reached for 60 seconds. In case of doubt, please ask the Public Spot operator if automatic logoff (“Station monitoring” on page 476) is activated.

6.10.5 Advice and help

The following sections present solutions to the most common problems that may occur when operating a Public Spot.

The Public Spot login page is not displayed

- The Internet access must be set up so that it is directed via the network adapter and not via a dial-up networking connection. To check this, take a look at the connection settings for your Web browser. If you use Microsoft Internet Explorer, you must disable the dial-up configurations in `Tools : Internet Options : Connections`entered there.
- Internet access must be direct, i.e. without going via a proxy server. In Microsoft Internet Explorer, you can disable the use of a proxy server in the menu `Tools : Internet Options : Connections : LAN-Settings...`.
- If you are making the connection with a WLAN adapter: Ensure that your network adapter can in fact find the Public Spot. Your WLAN adapter gives you the option of searching for an access point.
- If you are making the connection with a WLAN adapter: Check if your network adapter has all of the necessary settings to access the Public Spot network:
  - You probably have to enter the network name for the WLAN.
  - When working with an encrypted Public Spots, you are also required to enter the corresponding WPA or WEP key.
- Check that your network adapter is set up for automatic retrieval of an IP address (DHCP). Your device should not have a fixed IP address.

Note: If your network adapter is set up with a fixed IP address, adjusting it for automatic retrieval by DHCP may cause important configuration information to be lost. Ensure that you note all of the values listed in the network settings (IP address, standard gateway, DNS server, etc.).

Login not working

- Ensure that you enter the user data correctly and in full. Ensure that you use the correct capitalization for all entries.
- Is the CAPS-LOCK key activated on your device? This causes the capitalization to be reversed. Deactivate the CAPS-LOCK key and repeat the entry of your login data.
- The Public Spot operator may be checking more than just the user ID and password, but also the MAC address (physical address) of your network adapter as well. In this case, ensure that the Public Spot operator is informed of your correct MAC address.

It is no longer possible to login

If the Public Spot breaks off communications after a number of login attempts have failed, you should deactivate your WLAN adapter for at least 60 seconds (or your entire device) or disconnect the LAN adapter from the network, and then try again.

The session information window is not being displayed

To display the session-information window, enter the following line into the address line of your Web browser:

```
http://<IP address of the Public Spot>/authen/status
```

The Public Spot operator can supply you with the `<Public Spot's IP address>` upon request.

The Public Spot requests a new login for no reason (WLAN)

When moving into the signal coverage area of another access point (roaming), it is necessary to login again. If you are located in the overlap area between two access points, you may even experience a change of connection between the two access points at regular intervals. The task of the roaming secret is to allow Public Spot sessions to be passed between access points without the user having to login again.

- LANconfig: `Public Spot : Users : Roaming Secret`

6.11 Commonly transmitted RADIUS attributes

The RADIUS client module was implemented on the basis of RFCs no. 2865 and no. 2866.

These specifications define various attributes, some of which are an absolute necessity and some of which are optional. The following overview shows which attributes are transmitted/processed in messages between RADIUS servers and base stations.

6.11.1 Messages to/from the authentication server

Transferred attributes

As previously mentioned, your device transmits far more than just the username and password in a RADIUS request. RADIUS servers might choose to completely ignore these additional attributes, or only use a subset of these attributes. Many of these attributes are used for access to the server using dial-in, and are defined as standard attributes in the RADIUS RFCs. However, some important information for hotspot operation can not be represented with standard attributes. For this reason Hirschmann has chosen to provide these values as vendor-specific attributes, marked with the enterprise ID 2356.

Overview of the RADIUS attributes transmitted by the device to the authentication server

☐ **1**

User name

The name entered by the user.

☐ **2**

User-Password

The password entered by the user.

☐ **4**

NAS-IP-Address

IP address of your device

☐ **6**

Service-Type Id 1

Type of service that the user requested. The value `1` stands for **Login**.

☐ **8**

Framed-IP-Address

IP address that was assigned to the client

☐ **26**

Vendor 2356(LCS) ID 2

MAC address of the client if authentication using the MAC address is enabled. In contrast to the Calling-Station-Id, this value is transmitted as a 6-byte binary string. This attribute only exists for the login mode "Authenticate with name, password and MAC address".

☐ **30**

Called-Station-Id

MAC address of your device

☐ **31**

Calling-Station-Id

MAC address of the client The address is given byte-wise in hexadecimal notation with separators (nn:nn:nn:nn:nn:nn).

☐ **32**

NAS-identifier

Name of your device, if configured.

☐ **61**

NAS-Port-Type

Type of physical port over which a user had requested authentication.

– **ID 19** denotes clients from WLAN

– **ID 15** denotes clients from Ethernet

☐ **87**

NAS-Port-Id

Description of the interface over which the client is connected to your device. This can be a physical as well as a logical interface, such as `LAN-1`, `WLAN-1-5` or `WLC-TUNNEL-27`.

Note: Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.

Processed attributes

Your device evaluates the authentication response of a RADIUS server for attributes that it may possibly process further. Most attributes however only have a meaning if the authentication response was positive, so that they influence the subsequent session:

Overview of the RADIUS attributes processed by the device

☐ **18**

Reply-Message

An arbitrary string from the RADIUS server that may transport either a login failure reason or a user welcome message. This message may be integrated into user-defined start or error pages via the `SEVERMSG` element.

☐ **25**

Class

An arbitrary octet string that may contain data provided by the authentication/accounting backend. Whenever the device sends RADIUS accounting requests, they will contain this attribute as-is. Within an authentication response, this attribute can occur multiple times in order, for example, to transmit a string that is longer than 255 bytes. The device processes all occurrences in accounting requests in the order they appeared in the authentication response.

☐ **26**

Vendor 2356(LCS) ID 1

Trafficlimit

Defines the data volume in bytes after which the device automatically ends the session. This value is useful for volume-limited accounts. If this attribute is missing in the authentication response, it is assumed that no volume limit applies. A traffic limit of 0 is interpreted as an account which is principally valid, however with a used-up volume budget. The device does not start a session in this case.

☐ **26**

Vendor 2356(LCS) ID 3

LCS-Redirection-URL

This can contain any URL that is offered as an additional link on the start page. This can be the start page of the user or a page with additional information about the user account.

☐ **26**

Vendor 2356(LCS) ID 5

LCS-Account-End

Defines an absolute point in time (measured in seconds since January 1, 1970 0:00:00) after which the account becomes invalid. If this attribute is missing, an unlimited account is assumed. The device does not start a session if its internal clock has not been set, or the given point in time is in the past.

☐ **26**

Vendor 2356(LCS) ID 8

LCS-Public Spot-Username

Contains the name of a Public Spot user for auto-login. Auto-login refers to the table of MAC authenticated users who are automatically assigned usernames by the server.

☐ **26**

Vendor 2356(LCS) ID 8

LCS-TxRateLimit

Defines the maximum downstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.

☐ **26**

Vendor 2356(LCS) ID 9

LCS-RxRateLimit

Defines the maximum upstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.

☐ **27**

Session-Timeout

Defines an optional maximum duration of the session, measured in seconds. If this attribute is missing in the response, an unlimited account is assumed. A Session timeout of zero seconds is interpreted as an account which is principally valid, however with a used-up time budget. The device does not start a session in this case.

☐ **28**

Idle timeout

Defines a time period in seconds after which the device will terminate the session if no packets were received from the client. This value overwrites in the locally defined idle timeout under `Public Spot : Server : Idle timeout`.

☐ **64**

Tunnel-Type

Defines the tunneling protocol which will be used for the session.

☐ **65**

Tunnel-Medium-Type

Defines the transport medium over which the tunneled session will be established.

☐ **81**

Tunnel-Private-Group-ID

Defines the group ID if the session is tunneled.

☐ **85**

Acct-Interim-Interval

Defines the amount of time between subsequent RADIUS accounting updates. This value is only evaluated if the RADIUS client does not have a local accounting interval defined, i.e. if you have not set an "Accounting update cycle" for the Public Spot module.

Note: Note that the LCS-Account-End and Session-Timeout attributes are mutually exclusive, and it therefore does not make sense to include both in the response. If both attributes are included in a response, the attribute that appears as the last one in the attribute list will define the session's time limit.

6.11.2 Messages to/from the accounting server

Transferred attributes

The set of RADIUS attributes transmitted to a RADIUS server in an accounting request is similar to the set of attributes transmitted in an authentication request. However, additional attributes specific to accounting will be added. The following attributes are present in all RADIUS accounting requests:

Overview of the RADIUS attributes transmitted by the device to the accounting server

☐ **1**

User name

Name of the account that was used for authentication.

☐ **4**

NAS-IP-Address

IP address of your device

☐ **8**

Framed-IP-Address

IP address that was assigned to the client

☐ **25**

Class

All class attributes that the RADIUS authentication server sent in its authentication response.

☐ **30**

Called-Station-Id

MAC address of your device

☐ **31**

Calling-Station-Id

MAC address of the client The address is given byte-wise in hexadecimal notation with separators (nn:nn:nn:nn:nn:nn).

☐ **32**

NAS-identifier

Name of your device, if configured.

☐ **40**

Acct-Status-Type

Request type which signals the start or stop of accounting, or an interim update. Please refer to the section “Request types” on page 485 for further information.

☐ **44**

Acct-Session-Id

A series of characters that uniquely identify the client. It consists of the MAC address of the network adapter, the login timestamp (measured in seconds since January 1, 1970 0:00:00), and the session counter that your device manages locally.

☐ **61**

NAS-Port-Type

Type of physical port over which a user had requested authentication.

– **ID 19** denotes clients from WLAN

– **ID 15** denotes clients from Ethernet

☐ **87**

NAS-Port-Id

Description of the interface over which the client is connected to your device. This can be a physical as well as a logical interface, such as `LAN-1`, `WLAN-1-5` or `WLC-TUNNEL-27`.

Note: Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.

In the case of an accounting stop request or an interim update, the request contains the following additional attribute:

☐ **42**

Acct-Input-Octets

The sum of all data bytes received from the client in this session, modulo 2^{32}.

☐ **43**

Acct-Output-Octets

The sum of all data bytes sent to the client in this session, modulo 2^{32}.

☐ **46**

Acct-Session-Time

The total duration of the client's session in seconds.

Note: If the session was ended due to an idle timeout, this value is reduced by the idle time.

☐ **47**

Acct-Input-Packets

The number of data packets that your device received from the client during the session.

☐ **48**

Acct-Output-Packets

The number of data packets that your device sent to the client during the session.

☐ **49**

Acct-Terminate-Cause

The reason for termination or the end of the accounting session. This is sent if **Acct-Status-Type** has the value `Start` or `Stop`.

☐ **52**

Acct-Input-Gigawords

The upper 32 bits of the sum of all data bytes received from the client during this session.

☐ **53**

Acct-Output-Gigawords

The upper 32 bits of the sum of all data bytes sent to the client during this session.

☐ **55**

Event-Timestamp

The elapsed time since this accounting request was submitted by the device, measured in seconds since January 1, 1970 0:00:00. This attribute is only present if your device's real time clock contains a valid value.

Note: Note that the RADIUS accounting only starts accounting after a client successfully logs in, i.e. the time needed for authentication is not recorded. Using „Traffic limit option“ you can limit the data traffic during the authentication phase. The final accounting stop request also contains the termination cause attribute (49).

Processed attributes

Your device currently does not process any attributes in responses sent by a RADIUS accounting server.

6.12 Tutorials for setting up and using Public Spots

The following tutorials describe examples of how the Public Spot option can be implemented.

6.12.1 Setting up an external RADIUS server for user administration

Some applications user data is not stored on the device, but on an external, centralized RADIUS server. In this case, the Public Spot must communicate with the external RADIUS server to check the user data.

Note: Please note that specific functions (such as the Public Spot wizards in WEBconfig) are not available to you if you use an external RADIUS server for user administration!

Note: The following instructions assume that you know the IP address of a functional RADIUS server in the network.

The following configuration steps are used to set up a Public Spot that will be used with an external RADIUS server:

☐ Follow the steps in the section “Manual installation” on page 429.

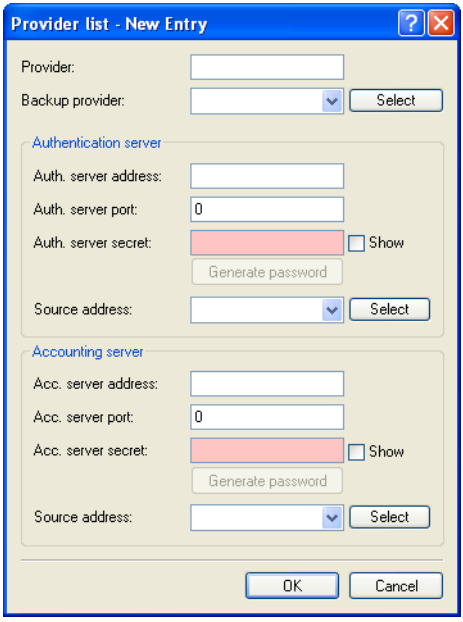
Among other things, the exact time on the device is necessary for the proper control of time-limited access.

Note: If authentication with an additional check of the physical address (MAC address) is enabled, the Public Spot transmits the MAC address of the end device to the RADIUS server. In this manner the Public Spot does not see whether the MAC address was actually checked or not. For MAC address checks to work without problem, the RADIUS server must be configured accordingly.

☐ Enter the settings for the RADIUS server.

– LANconfig: `Public Spot : Users : Authentication servers`

When configuring a Public Spot, user registration data can be forwarded to one or more RADIUS servers. These servers are configured under `Public Spot : Users : Authentication servers`. The registration data that individual RADIUS servers require from the clients is not important to the device that provides the Public Spot, since this data is transparently passed on to the RADIUS server.



Note: IP addresses specified here must be static. The Public Spot must be able to contact the specified destination addresses. For IP addresses outside of your own network, a router that has contact to the destination network must be specified as a gateway in the DHCP settings for the Public Spot. You have to define this gateway as the default route in the routing table.

Note: In order for the RADIUS server to record the connection data, the information on the accounting server must be specified in full. As an alternative to using a RADIUS accounting server, the connection information from the Public Spot can also be output by the SYSLOG function.

☐ That's it!

Your Public Spot is now ready for operation. All users with a valid account on the RADIUS server can use the Web interface to login to the Public Spot.

6.12.2 Internal and external RADIUS servers combined

Some companies use an external RADIUS server to authenticate users with IEEE801.1x. For applications with a WLAN controller and multiple access points, the access points initially address the WLAN controller as their RADIUS server. You define how the RADIUS requests are forwarded to the external RADIUS server on the WLAN controller.

Note: The settings described below are only necessary if you are operating an external RADIUS server on your device in addition to the Public Spot in the external RADIUS server.

A Public Spot providing guest-access accounts requires the following settings:

- Authentication requests from internal employees are to be forwarded to an external RADIUS server.
- The authentication requests for Public Spot access accounts are to be handled by the internal RADIUS server.

Realm tagging for RADIUS forwarding

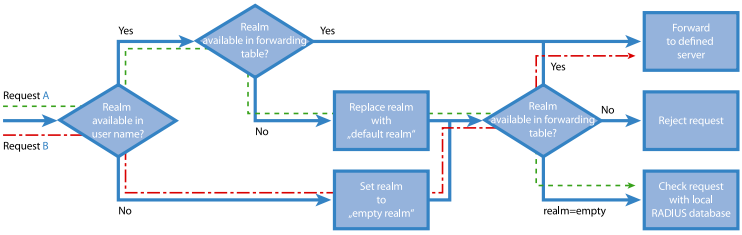
Authentication requests from the two user groups are to be handled separately. The WLAN controller uses what are known as "realms" to differentiate between these two groups. The purpose of realms is to address domains within which user accounts are valid. The WLAN controller can transmit the realms with authentication requests to the RADIUS server. Alternatively, the RADIUS server can change the realms in the user names for the purpose of RADIUS forwarding:

- The value defined for "Standard realm" replaces an existing realm of an incoming request if no forwarding is defined for that existing realm.
- The value defined under "Empty realm" is **only** used by the RADIUS server if the incoming user name **still does not** have a realm.

An entry in the forwarding table causes all authentication requests with a certain realm to be forwarded to a RADIUS server. If no matching entry exists in the forwarding table, the request is refused.

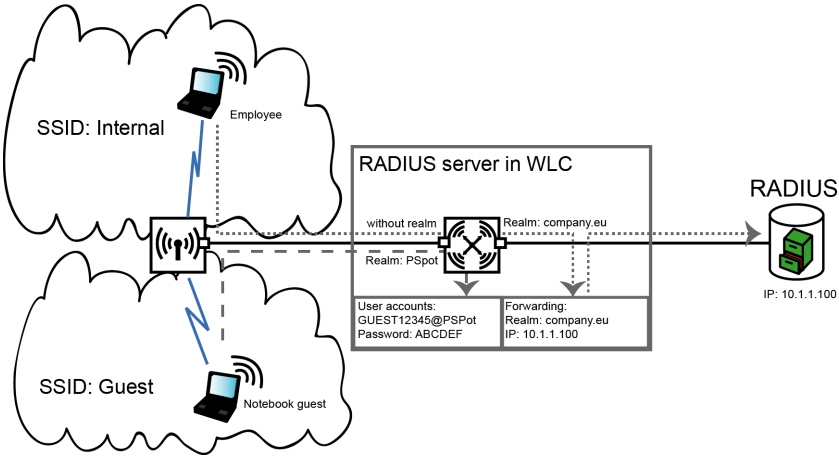
Note: If the WLAN controller checks the realm and finds that it is empty, it **always** checks the authentication request with the internal RADIUS database.

The following flow diagram illustrates the method used by the RADIUS server to process realms:



Using different realm tags allows different RADIUS servers to be targeted with requests. The way in which device's RADIUS server makes decisions for the two requests is shown in the diagram:

- ☐ Because the user names for guest access accounts are generated automatically, they are suffixed with an appropriate realm, such as "PSpot". Because the forwarding table does not contain this entry and the standard realm is empty, the WLAN controller forwards all authentication requests with this realm to the internal RADIUS server.
- ☐ To limit the amount of work required for the configuration, internal users are listed without a realm. The RADIUS server in the device can automatically replace an empty realm with another realm in order to identify internal users. In this example, the empty realm is replaced by the domain of the company "company.eu". The information specified in the forwarding table allows all authentication requests with this realm to be forwarded to the external RADIUS server.



Configuring RADIUS forwarding

The following configuration steps allow you to specify the different manners in which internal users and guests are processed.

☐ In the Public Spot, adapt the pattern of user names such that a unique realm can be suffixed.

For example, if the pattern is "user%n@PSpot", the Public Spot generates usernames with the format "user12345@PSpot".

– **LANconfig:** `Public Spot : Wizard : Add user wizard`

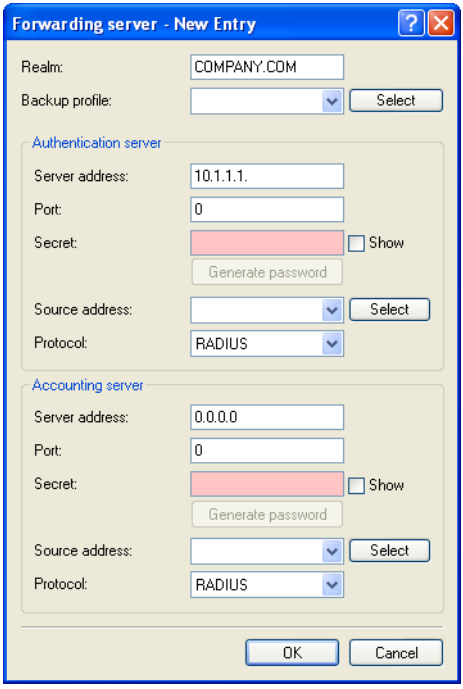
☐ In the WLAN controller's RADIUS server, define an "empty realm" (e.g., "COMPANY.EU").

This realm is attached to all user names which request authentication from the WLAN controller and which do not already have a realm. In this application, the internal users have no realm defined. In order to prevent the WLAN controller's RADIUS server from attaching a realm, you must leave the "Default realm" field blank.

– **LANconfig:** `RADIUS Server : Forwarding : Forwarding server`

☐ In order for the WLAN controller to forward authentication requests from internal users to the external RADIUS server, suitable entries must be made in the forwarding settings.

All incoming RADIUS requests which have the realm "COMPANY.EU" will be forwarded to the specified IP address.



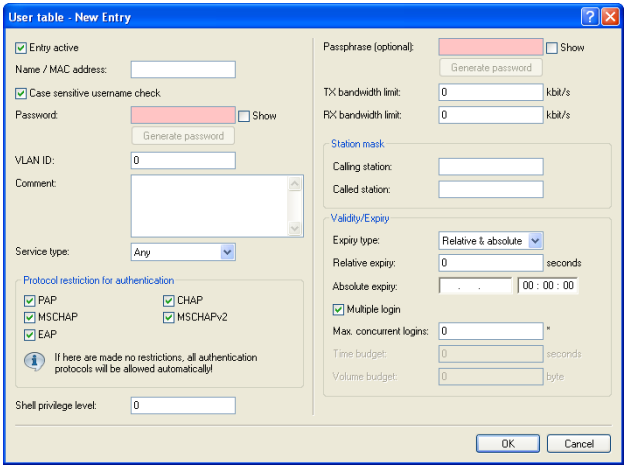
☐ Authentication requests from Public Spot users have the realm "@PSpot" and are received by the WLAN Controller. With no forwarding defined for this realm, the usernames are automatically checked with the internal RADIUS database. Because the Public Spot access accounts created with the Wizard are stored in this database, these requests can be authenticated as required.

6.12.3 Checking WLAN clients with RADIUS (MAC filter)

To use RADIUS to only authenticate specific WLAN clients and grant them WLAN access based on their MAC address, an external RADIUS server can be used, as can the internal RADIUS user database of the WLAN controller.

Enter the MAC addresses in the RADIUS database using LANconfig, and enable all authentication methods. For "Name/MAC address" and "Password" select the corresponding MAC address in the format "AABBCC-DDEEFF".

- LANconfig: `RADIUS server : General : User database`



6.12.4 Setting up an external SYSLOG server

Depending on the use case, storage of the usage data is required for the operation of a Public Spot. This data can be stored to a SYSLOG server, for example. Some SYSLOG servers are available as free software.

To save user data from a Public Spot by means of SYSLOG, the external SYSLOG server has to be configured in the respective Public Spot. Once this is done, messages are sent for logging to the SYSLOG server whenever Public Spot user accounts are created or deleted, and at the beginning and end of Public Spot sessions. The message issued at the end of a session—with the source "Login" and the priority "Information"—also includes information on the transferred data volumes and the IP address used.

Configuring an external SYSLOG server

Your device is capable of logging the creation and deletion of Public Spot users, as well as their login and logout activities. You can also transfer this internally stored information to an external SYSLOG server. The following steps show you how you can set up logging with a program installed on an external SYSLOG server (in this example, "Kiwi").

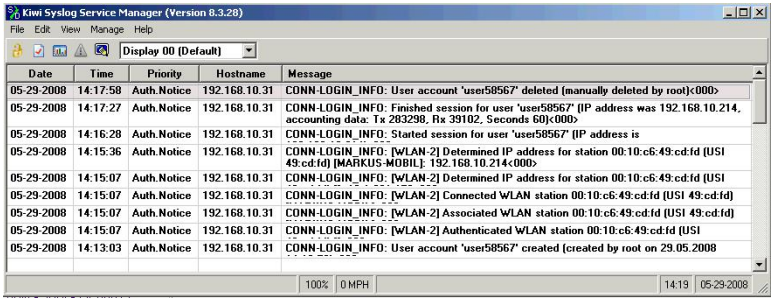
☐ Start LANconfig and open the configuration dialog for your device.

☐ Change to the dialog `Log & Trace : General` and open the table "SYSLOG servers".

☐ Add a new entry. Specifiy the "IP address" of the computer where the SYSLOG client is installed (e.g., `192.168.10.237`), and enter the "Source" (`Login`, `Accounting`) and the "Priority" (`Information`).

☐ Close the dialog and store the configuration on your device.

☐ Start the analysis program on your SYSLOG server (e.g., "Kiwi"). As soon as the program has started, it logs the creation and deletion of Public Spot accounts and also the user logins and logouts.



7 Virtual Private Networks – VPN

7.1 What are the Benefits of VPN?

A VPN (Virtual Private Network) via IPSec enables you to establish secure connections from a remote PC to a OpenBAT device over the Internet (Remote Access Service - RAS).

Connection via the Internet

When the Internet is used instead of direct connections, the following structure results:

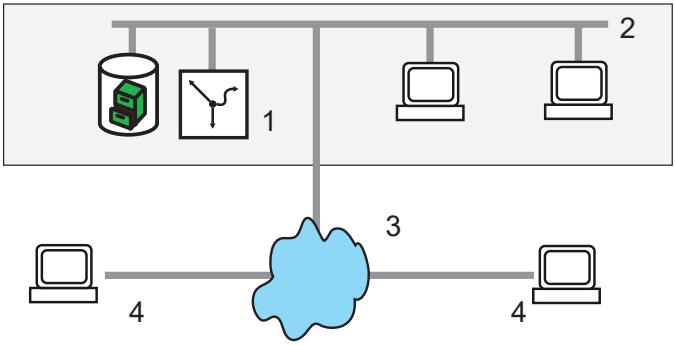


Figure 68: Connection via the Internet
1: OpenBAT device
2: LAN
3: Internet
4: Computer with remote-access connection

All participants are connected to the Internet (fixed or dial-in connection). There are no longer expensive dedicated lines between the participants.

- ☐ Only the Internet connection of the head office's LAN is necessary. Special dial-in devices or routers for dedicated lines to individual participants can be omitted.
- ☐ The RAS computers dial into the head office's LAN via the Internet.

There are no longer any direct physical connections between 2 participants, but each participant has direct access to the Internet. The access technology does not play a role here: Ideally, broad-band technologies, such as DSL (Digital Subscriber Line) in connection with flat rates are used.
It is not necessary that the technologies used by the individual participants are compatible, as is the case with conventional direct connections. Via a single Internet access you can establish several simultaneous logical connections to various remote stations.
Low connection costs and high flexibility make the Internet (or any other IP network) an excellent transfer medium for a corporate network.
Two technical characteristics of the IP standard, however, are detrimental to the use of the Internet as part of corporate networks:
☐ The necessity of public IP addresses for all participants.
☐ Insufficient data security due to unprotected data transmission.

7.1.1 Private IP Addresses on the Internet?

The IP standard defines two types of IP addresses: public and private addresses. A public IP address is valid worldwide, while a private IP address is only valid in an isolated LAN.
It is necessary that public IP addresses are unique worldwide. Private IP addresses can occur any number of times worldwide, but only once within an isolated LAN.
Usually, computers in the LAN only have private IP addresses, only the router that is connected to the Internet also has a public IP address. The computers behind this router access the Internet via its public IP address (IP masquerading). In such a case, solely the router itself is addressed via the Internet. There is no possibility to address computers behind the router without intervention by the router.

7.1.2 Security of Data Traffic on the Internet?

The skepticism towards the idea of handling parts of corporate communication over the Internet is based on the fact that the Internet is no longer within a company's direct sphere of influence. Unlike with dedicated connections, the data is transmitted through external network structures whose owners are unknown to the company.
In addition, the Internet is based on a simple form of data transmission using unencrypted data packets. Further participants through whose networks the packets are transmitted might read them or even manipulate them. Anyone can access the Internet. This entails the risk that additional participants also try to gain unauthorized access to the transmitted data.

- **VPN – Security based on Encryption**
  To resolve this security problem, encrypt the data traffic between two participants. While the data is transmitted in the VPN, it is unreadable to other participants.
  The latest and most secure cryptographic procedures are used for encryption. For this reason, the transmission security in the VPN exceeds the security level of dedicated lines by far.
  The participants agree on data-encryption codes which are referred to as "keys". These keys are only known to the persons involved in the VPN connection. Without a valid key, the data packets cannot be decrypted. The data is inaccessible to other participants, it remains 'private'. A direct connection between two remote terminals within the IPSec VPN is referred to as "transport mode".

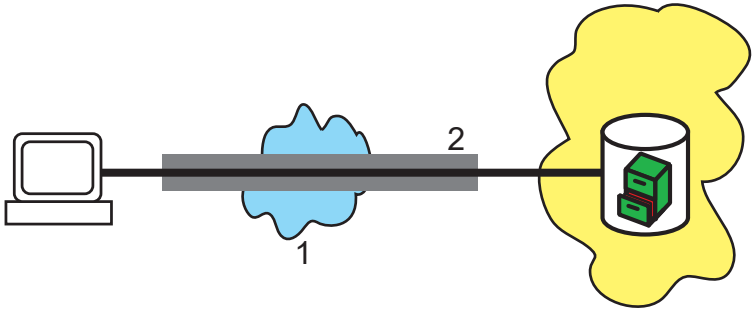


Figure 69: VPN data transmission in IPSec transport mode
1: Internet
2: VPN tunnel

- **Send your Data into the Tunnel – for Security Reasons**
  It now becomes clear why VPN creates a virtual private network: the devices never establish a fixed physical connection between each other. The data moreover follows suitable routes through the Internet. It is still harmless, however, if additional participants intercept and record the transmitted data during transmission. As the devices have encrypted the data by VPN, the actual content remains inaccessible. Experts compare this status to a tunnel: Open at the beginning and the end, but perfectly shielded in between. The most secure connections within a public IP network are therefore referred to as "tunnels". A connection between two networks within the IPSec VPN is referred to as "tunnel mode".

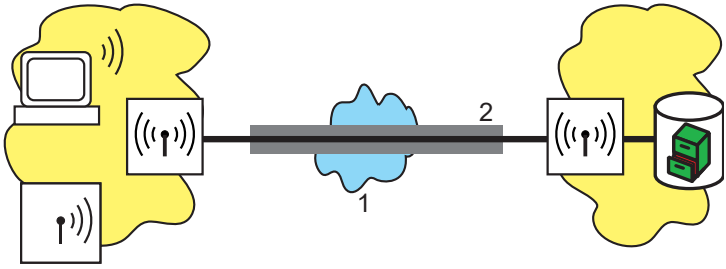


Figure 70: VPN data transmission in IPSec tunnel mode
1: Internet
2: VPN tunnel

The aim of modern network structures has thus been achieved: Provide secure connections over the largest and cheapest of all public IP networks: the Internet.

7.2 VPN at a Glance

7.2.1 VPN Application Example

You can use VPN connections in various different areas of application. Different transmission technologies for data and also audio are used, which VPN unites to an integrated network. The following example shows a typical application, which can often be found in practice in identical or similar form.

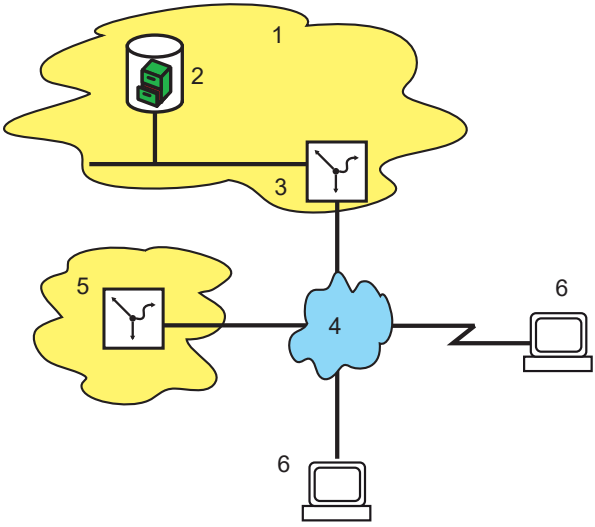


Figure 71: Application example of a VPN connection

1: Head office
2: Server in the DMZ
3: VPN gateway
4: Internet
5: Branch office
6: Computer with remote access connection

The essential components and characteristics of these applications:

- ☐ Coupling of networks, e.g. between the head office and the branch office
- ☐ Connection of branch offices without fixed IP addresses via the VPN router
- ☐ Connection of home offices without fixed IP, possibly via ISDN or analog modems
- ☐ Connection to Voice-over-IP telephone systems
- ☐ Connection of mobile users, e.g. via public WLAN access

7.2.2 Functions of VPN

This section lists all of the functions and properties of VPN. Experts in the VPN sector are offered a highly compressed summary of the performance of the function. Understanding the terminology requires a sound knowledge of the technical fundamentals of VPN. However, for commissioning and normal operation of the VPN, this information is not required.

- VPN according to IPSec standard
- VPN tunnel via leased lines, switched connections and IP networks
- IKE Main and Aggressive mode
- Dynamic VPN: Public IP addresses can be static or dynamic (establishing a connection with remote sites using dynamic IP addresses requires ISDN)
- IPSec protocols ESP, AH and IPCOMP in transport and Tunnel mode
- Hash algorithms:
  - HMAC-MD5-96, hash length 128 bits
  - HMAC-SHA-1-96, hash length 160 bits
  - HMAC-SHA-2-256, hash length 256 bits
- Symmetrical encryption methods
  - AES, key lengths of 128, 192 and 256 bits
  - Triple DES, Key length 168 bits
  - Blowfish, key length 128 - 448 bits
  - CAST, key length 128 bits
  - DES, key length 56 bits
- Compression with "Deflate“ (ZLIB) and LZS
- IKE config mode
- IKE with preshared keys
- IKE with RSA signature and digital certificates (X.509)
- Key exchange via Oakley, Diffie-Hellman algorithm with a key length of 768 bits, 1024 bits, 1536 bits and 2048 bits (well known groups 1, 2, 5 und 14)
- Key management according to ISAKMP

7.3 Configuration of VPN Connections

The following three questions come up when VPN connections are configured:

- ☐ Between which VPN gateways (remote terminals) is the connection established?
- ☐ Which security parameters secure the VPN tunnel between both gateways?
- ☐ Which networks and computers communicate via this tunnel?

Note: This section describes the basic considerations for the configuration of VPN connections. First, a simple connection between two local networks is described. Descriptions of special cases, e.g. dialing into LANs using individual computers (RAS) or connecting structured networks can be found further down.

7.3.1 VPN Tunnel: Connection between VPN Remote Terminals

In virtual private networks (VPNs), you can connect local networks over the Internet. The device routes the private IP addresses from the LANs via an Internet connection between 2 VPN remote terminals with public IP addresses.
To enable secured routing of the private IP address ranges via the Internet connection, establish a VPN connection between the two LANs. This connection is also referred to as VPN tunnel.

The VPN tunnel has two important tasks:

- ☐ It shields transmitted data from unwanted access by unauthorized persons
- ☐ It forwards private IP addresses via an Internet connection over which only public IP addresses can be routed.

The following parameters define the VPN connection between the two gateways:

- ☐ The end points of the tunnel, the VPN gateways, which a device reaches via a public IP address (static or dynamic)
- ☐ The IP connection between the two gateways
- ☐ The private IP address ranges that the two VPN gateways are routing.
- ☐ Security-relevant settings, such as passwords, IPSec keys, etc. for shielding the VPN tunnel

This information can be found in the VPN rules.

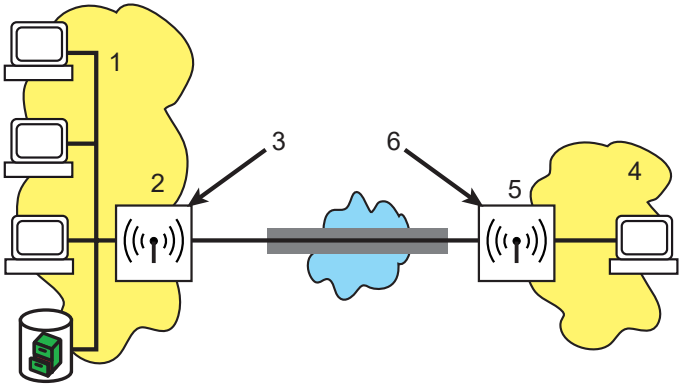


Figure 72: VPN tunnel between gateways

1: Private IP network: 10.1.0.0 Network mask: 255.255.0.0
2: Public IP address: 80.146.81,251
3: IP connection
4: Computer with remote access and dynamic IP address
5: VPN tunnel

7.3.2 1-Click VPN for Hirschmann Advanced VPN Client

VPN access for employees who dial into a network by means of the Hirschmann Advanced VPN Client can easily be created using the setup wizard. You can export them into a file which the Hirschmann Advanced VPN Client imports as a profile. During this process, the client retrieves the required information for the current configuration from the Hirschmann VPN Router and adds randomly generated values (e.g. for the pre-shared key).

☐ Start the setup wizard 'Set up access' via LANconfig and select the 'VPN connection'.

☐ Activate the options 'Hirschmann Advanced VPN Client' and 'Accelerate configuration with 1-click VPN'.

☐ Enter the name for this access and select under which address the router can be reached from the Internet.

☐ In a last step, select how the device outputs the new access data:

- Save profile as import file for the Hirschmann Advanced VPN Client
- Send profile via e-mail
- Print profile

Note: Sending the profile file via e-mail represents a security risk because someone could intercept the e-mail.

To send the profile file via e-mail, the device must be configured with an SMTP account including the necessary access data. Furthermore, the configuration computer must include an e-mail program that is set up as standard e-mail application and that other applications can also access for sending e-mails. When generating the VPN access, the device uses settings that are optimally configured for use in the Hirschmann Advanced VPN Client, among them, e.g..: ☐ Gateway: If defined in the BAT VPN Gateway, a DynDNS name is used,

otherwise the IP address

☐ FQDN (Full Quality Domain Name): Combination of the name of the connection, a sequential number and the internal domain in the BAT VPN Gateway

☐ Domain: If defined in the BAT VPN Gateway, the internal domain is used, otherwise a DynDNS name or the IP address.

- ☐ VPN IP networks: All IP networks of the ‘Intranet’ type defined in the device.
- ☐ Pre-shared key: Randomly generated key with a length of 16 ASCII characters.
- ☐ Connection medium: The LAN serves to establish connections.
- ☐ VoIP prioritization: The VoIP prioritization is activated by default.
- ☐ Exchange mode: As exchange mode, the ‘aggressive mode’ is employed.
- ☐ IKE config. mode: The IKE config mode is activated, the IP address information for the Hirschmann Advanced VPN Client is automatically assigned by the BAT VPN Gateway.

7.3.3 VPN remote access wizard in WEBconfig:

You have the option of using WEBconfig to create VPN-client dial-in accounts for the Advanced VPN Client and myVPN. The setup steps are the same as those for LANconfig.

Note: The 1-Click VPN configuration is not available in WEBconfig due to restrictions on browser access.

7.3.4 Viewing VPN Rules

As the VPN rules are always a combination of various pieces of information, you define these rules indirectly in a device. You do this by compiling them from different sources.
You can call up information on the current VPN rules in the device using the Telnet console. To do this, establish a Telnet connection to the VPN gateway and enter the following command in the console:

```
show vpn
```

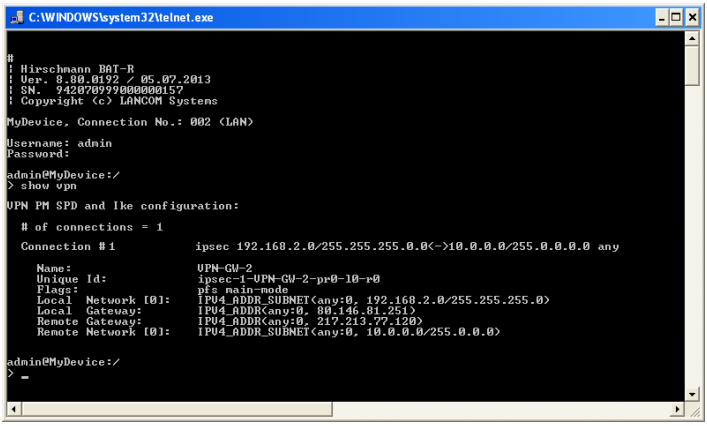


Figure 73: Calling up VPN rules using Telnet

The output contains information on the network relationships that are relevant for setting up VPN connections to other networks.
In this case, the local network of a branch office (network 192.168.2.0 with network mask 255.255.255.0) is connected to the network of the head office (network 10.0.0.0 with network mask 255.0.0.0). The public IP address of your own gateway is 80.146.81.251, the one of the remote VPN gateway is 217.213.77.120.
The following command shows the protocols and ports permitted over the connection:

```
any:0
```

An extended output can be requested using the command "show vpn long". In addition to the network relationships, this output also includes information on security-relevant parameters, such as IKE and IPSec proposals.

7.3.5 Manually Setting up VPN Connections

Manually setting up VPN connections involves the tasks previously described:

- ☐ Defining tunnel end points
- ☐ Defining security-relevant parameters (IKE and IPSec)
- ☐ Defining the VPN network relationships, meaning the IP address ranges to be connected. In case of overlapping IP network ranges on both sides of the connection, please also observe the section 'N:N mapping'.
- ☐ When coupling Windows networks (NetBIOS/IP): Without WINS servers on both sides of the VPN connection (e.g. when connecting home offices), the device assumes the corresponding NetBIOS proxy functions. This requires the activation of the NetBIOS module in the device and the entry of the corresponding VPN remote terminal as remote terminal in the NetBIOS module. If, however, both networks have their own WINS servers in the case of site-to-site connections, deactivate the NetBIOS module, so that the device no longer performs any NetBIOS proxy functions.

Note: To use the device's NetBIOS proxy, enter the IP address of the remote terminal (Intranet address) as primary NBNS in the IP parameter list. You will find the settings under LANconfig: Communication / Protocols.

Apart from your own, local VPN gateway, enter one VPN remote terminal each in the VPN connection list.

Manually configuring the VPN connections involve the following steps:

- ☐ Create an entry for the remote VPN gateway in the connection list and enter the public IP address.
- ☐ The device takes the security parameters for the VPN connection from the prepared lists. Apart from the definition of an IKE key, there is no further need for action.

- ☐ For a dynamic VPN connection, create a new entry in the PPP list with the name of the remote VPN gateway as remote terminal, the name of the local VPN gateway as user name and a suitable password. For this PPP connection, definitely activate the IP routing and, if required, also the routing of "NetBIOS over IP". Define the remaining PPP parameters, such as the procedure for checking the remote terminal, as with other PPP connections.
- ☐ The main task in setting up VPN connections is the definition of network relationships: Which IP address ranges on both sides of the VPN tunnel will you integrate into the secured connection?

7.3.6 IKE Config Mode

When configuring VPN dial-in access options, you can, as an alternative to the fixed assignment of IP addresses, also enter a pool of IP addresses for the remote terminals logging in. To do this, select the "IKE-CFG" mode in the entries of the connection list. It can take the following values:

- ▶ Server: With this setting, the device functions as server for this VPN connection. There are 2 possibilities for assigning the IP address to the client:
  - ▶ If there is an entry for the remote terminal in the routing table, the device assigns it the IP address configured there.
  - ▶ If there is no entry for the remote terminal in the routing table, the device takes a free IP address from the IP pool of the dial-in access options.

Note: Here it is necessary that you configure the remote terminal as IKE-CFG client and it thus requests an IP address for the connection from the server.

- Client: With this setting, the device functions as client for this VPN connection and requests an IP address for the connection from the remote terminal (server). The device thus behaves similar to a VPN client.
- Off: If the IKE-CFG mode is switched off, the device does not assign IP addresses for the connection. In this case it is necessary that you configure fixed IP addresses to be used for this connection on both sides of the VPN path.

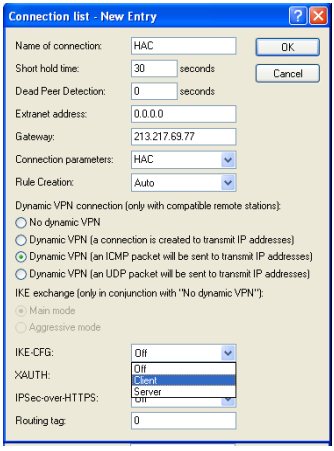


Figure 74: Editing an entry in the connection table

LANconfig: VPN / General / Connection list
WEBconfig: HiLCOS menu tree / Setup / VPN / Name list

7.3.7 Establishing VPN Network Relationships

With the integrated firewall, Hirschmann Routers include a powerful instrument for the definition of source and target address ranges. For this purpose, you can allow or deny data transmission (if required, with further limitations). Use this function also for setting up the network relationships for the VPN rules.

In the best case, the firewall generates the VPN rules automatically.

- As source network, the firewall uses the local Intranet, meaning the private IP address range which includes the local VPN gateway itself.
- As destination networks for the automatically generated VPN rules, the network areas from the IP routing table are used, with a remote VPN gateway as specified router.

To activate this automatic generation of rules, it is sufficient that you activate the corresponding option in the firewall. This is done automatically when the VPN installation wizard in LANconfig is used. When two simple local networks are coupled, the automatic VPN function derives the network relationship from the IP address range of its own LAN and from the entry for the remote LAN in the IP routing table.

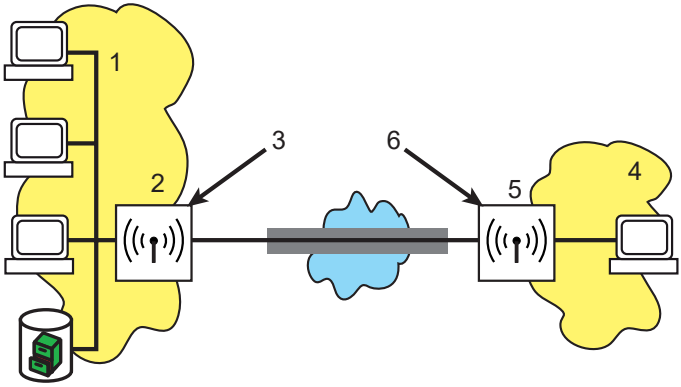


Figure 75: Automatic VPN function with coupled LANs
1: IP network: 10.1.0.0 Network mask: 255.255.0.0
2: VPN-GW-1: 80.146.81,251
3: IP routing table: 10.2.0.0/16 > VPN-GW-2
4: IP network: 10.2.0.0 Network mask: 255.255.0.0
5: VPN-GW-2: 217.213.77,120
6: IP routing table: 10.1.0.0/16 > VPN-GW-1

The description of the network relationships becomes more complex when the source and destination networks exceed the respective Intranet address range of the connected LANs.
If one part of the entire local Intranet connects to the remote network, the automatic function releases an IP address range for the VPN connection that is too large.
As they are connected to the local Intranet via additional routers, many network structures are connected to other network sections with their own IP address ranges. Include these address ranges in the network relationship using additional entries.
In these cases it is necessary that you manually enter the network relationships to describe the source and destination networks. Depending on the situation, this leads to an extension of the automatically generated VPN rules. It might be necessary to switch off the automatic VPN function completely in order to avoid unwanted network relationships.

Define the required network relationships using corresponding firewall rules under the following conditions:

- ☐ For the firewall rule, activate the option "This rule is used for generating VPN rules".
- ☐ As firewall action, select the option "transmit" in any case.
- ☐ You can enter individual stations, specific IP address ranges or entire IP networks as source and target for the connection.

Note: The firewall rules for the generation of VPN rules are active even when you do not require a firewall function in the device and have therefore deactivated it.

Note: Define the destination networks in the IP routing table, so that the router forwards the corresponding data packets in the devices to the other network. Use the already available entries and enter a higher-level network as target. The intersecting portion of the destination-network entry in the firewall and the subordinate entries in the IP routing table will be integrated into the network relationships for the VPN rules.

Example: The IP routing table contains the destination networks 10.2.1.0/24, 10.2.2.0/24 and 10.2.3.0/24, which are all connected via the VPN-GW-2 router. One entry for the destination network 10.2.0.0/16 in the firewall is sufficient to include the three desired subnetworks in the VPN rules.

Note: Define identical source and destination networks on both sides of the VPN connection. This is required if you map a larger target-address range onto a smaller source-address range at the remote terminal. Decisive are the IP address ranges allowed by the VPN rules, and not the networks specified in the firewall rules. These may deviate from the network relationships in the VPN rules because of intersecting ranges.

Depending on your requirements, you can additionally limit the VPN connection to specific services or protocols. This will permit you to e.g. reduce the VPN connection to use with a Windows network only.

Note: For this limitation, use separate rules that apply exclusively to the firewall and are not used for the generation of VPN rules. Firewall/VPN rules can quickly become complex and difficult to manage.

7.3.8 Collective Establishment of Security Associations

"Security Associations" (SAs) form the basis for establishing a VPN tunnel between two VPN remote terminals. An SA defines, among others, the following parameters:

- IP addresses of source and destination network
- Encryption, integrity check and authentication methods
- The key for the connection
- The period of validity of the keys used

The Security Associations are defined by automatically or manually generated VPN rules (see also 'Establishing VPN Network Relationships' in the reference manual).

Usually, an IP packet transmitted from the source network to the destination network triggers the establishment of Security Associations. In the case of keep-alive connections, this is an ICMP packet that the device sends to the remote terminal by an entry in the polling table.

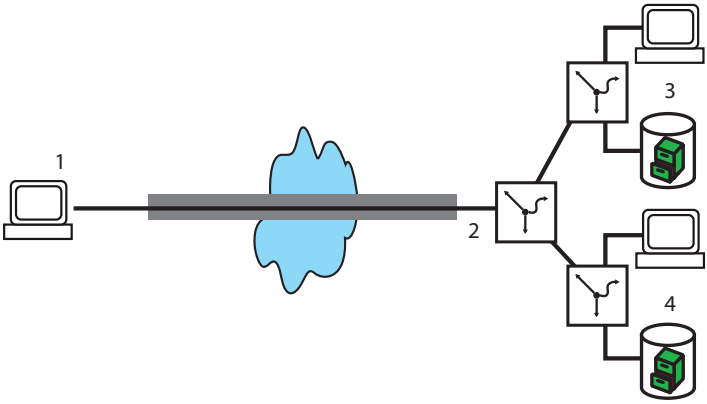


Figure 76: Various connected IP networks
1: Computer with remote access
2: IP network: 10.2.x.x
3: IP network: 192.x.x.x
4: IP network: 172.x.x.x

In complex network scenarios, various network relationships are possible between two VPN remote terminals. If the device transfers a single IP packet, this leads to the establishment of SAs for precisely this one network relationship which matches this packet. For the establishment of the other SAs, the device requires IP packets matching the other network relationships.
The establishment of SAs based on data packets requires time and leads to packet losses as long as the SAs are not yet installed. This is often an unwanted effect, especially with keep-alive connections. Instead, all SAs matching the network relationships defined in the remote terminal are established immediately. As the negotiation of all SAs requires substantial CPU performance particularly in complex scenarios, you can define the behavior with the parameter "Establish SAs collectively".

- Establish SAs collectively
  - Yes: The device establishes all defined SAs.
  - No [default]: The device only establishes the SAs explicitly addressed by a packet to be transmitted.
  - Only with keep alive: The device establishes all defined SAs for remote terminals with a hold time of '9999' (keep alive) in the VPN connection list.

WEBconfig: HiLCOS menu tree > Setup > VPN

Note: In most cases, the default setting for the exclusive establishment of explicitly addressed SAs is sufficient, especially if you are only using automatically generated VPN rules. The currently available SAs are listed under HiLCOS menu tree/Status/VPN.

7.3.9 VPN Connection Diagnostics

If the VPN connections fail to work after the relevant parameters have been configured, the following diagnostic methods are available:

- ☐ Use the command `show vpn spd` on the Telnet console to call up the "Security Policy Definitions".
- ☐ Use the command `show vpn sadb` to call up information about the negotiated "Security Associations" (SAs).
- ☐ Use the command `trace + vpn` to call up the status and error messages for the current VPN negotiation.
  - ▶ The error message `No proposal chosen` indicates a configuration error at the remote terminal.
  - ▶ The error message `No rule matched`, on the other hand, indicates a configuration error in the local gateway.

7.4 IPSec over HTTPS

7.4.1 Introduction

In some environments, it is impossible to establish a secured VPN connection over an existing Internet connection because the ports used by IPSec are blocked in the settings of an upstream firewall. To permit the establishment of an IPSec-secured VPN connection even under these conditions, the VPN routers support the 'IPSec over HTTPS' technology. The device initially tries to transmit data via standard IPSec. If the connection fails to be established (e.g. because IKE port 500 is blocked by a mobile phone network), an automatic attempt to set up a connection is made. For this attempt, the device encapsulates the IPSec VPN with an additional SSL header (port 443, as with https).
Please note that the 'IPSec over HTTPS technology' is only available when both remote terminals support this function and when the relevant options are activated. IPSec over HTTPS is available in VPN routers with HiLCOS 8.0.

7.4.2 Configuring the IPSec over HTTPS Technology

To actively establish a connection from a VPN device to another remote terminal using the IPSec over HTTPS technology, activate the option in the relevant entry for the remote terminal in the VPN name list.
LANconfig: VPN / General / Connection list
WEBconfig: Menu tree / Setup / VPN / VPN remote terminal

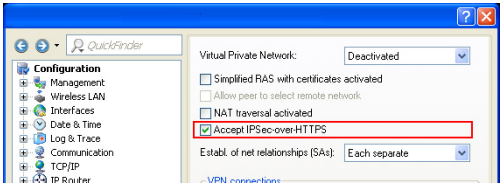


Figure 77: Configuring active IPSec over HTTPS

☐ IPsec-over-HTTPS: With this option, you activate the IPSec over HTTPS technology when actively establishing a connection to this remote terminal.

- Possible values: On, Off
- Default: Off

Note: With activated IPSec over HTTPS option, the VPN connection is only available when the remote terminal also supports this technology and when the acceptance of passive VPN connections with IPSec over HTTPS has been activated in the remote terminal.

For the passive establishment of a connection to a VPN device from another VPN remote terminal using the IPSec over HTTPS technology (e.g. Hirschmann Advanced VPN Client), activate the option in the general VPN settings.
LANconfig: VPN / General
WEBconfig: Menu tree / Setup / VPN

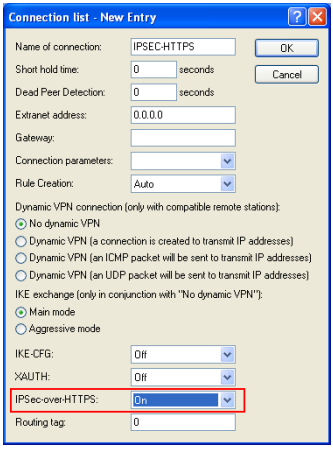


Figure 78: Configuring passive IPSec over HTTPS

☐ Accept SSL-IPsec: With this option, you activate the acceptance of passive connection setups when the remote terminal supports the IPSec over HTTPS technology.
- Possible values: On, Off
- Default: Off

Note: The Hirschmann Advanced VPN Client supports automatic fallback to IPSec over HTTPS. With this setting, the VPN client first tries to establish a connection without additional SSL encapsulation. If the device fails to establish a connection, it then tries to establish a connection with the additional SSL encapsulation.

7.4.3 Status Displays for IPSec over HTTPS Technology

The status displays for every active VPN connection indicate whether the IPSec over HTTPS technology (SSL encaps.) is activated for the respective connection.
WEBconfig:Hirschmann Menu tree / Status / VPN / Connections

7.5 Use of Digital Certificates

The security of communications via VPN fulfills three core requirements:
- Confidentiality: No unauthorized person can read the transmitted data (via encryption).
- Integrity: No unauthorized person can change the data while it is being transmitted (via authentication – hash).
- Authenticity: The recipient ensures that the data received has really been sent by the supposed sender (via authentication).

A number of procedures are available for the encryption and authentication of data, providing satisfactory solutions for the first two aspects – confidentiality and integrity. The use of digital certificates aims at also ensuring the authenticity of the communication partners.

7.5.1 Basics

Encryption methods can be divided into 2 categories: Symmetrical and asymmetrical encryption.

Symmetrical Encryption

Symmetrical encryption has been known for thousands of years and is based on the fact that both the sender and the recipient of a message have a shared secret key. This key can take on various forms. The Romans used a stick of a certain diameter for encryption and decryption. In today's digital communication, the key is usually a specific password. Using this password and an encryption algorithm, the sender modifies the data to be sent. The recipient uses the same key and the relevant decryption algorithm to render the data readable again. Any other person who does not know the key cannot read the data. A common symmetrical encryption method is 3DES, for example.

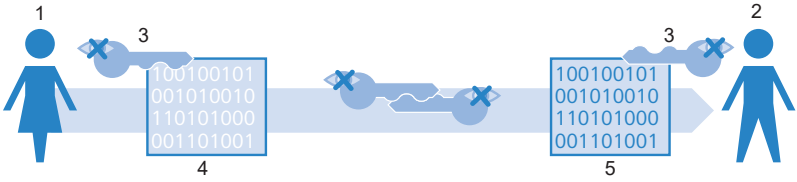


Figure 79: Symmetrical encryption method

1: Alice
2: Bob
3: Secret key
4: Encrypted message
5: Message in plain text

Example:

- ☐ Alice wants to send a confidential message to Bob. To do this, she encrypts the message with a secret key and a secret procedure, such as 3DES. She sends the encrypted message to Bob, informing him of the encryption method she has used.
- ☐ Bob has the same key as Alice. As he also knows the encryption method Alice used, he can decrypt the message and transform it back into plain text.

Symmetrical encryption is very simple and efficient, but has two significant disadvantages:

- ☐ Each secret communication relationship requires a separate key. If Carol joins Alice and Bob, three keys are necessary to secure the data communication between all partners, with four participants, six keys are required, with 12 participants, 66 and with 1000 participants, almost 500,000. In a worldwide network with ever increasing requirements for the secure communication of numerous participants, this becomes a serious problem.
- ☐ While this first disadvantage could be solved with technological means, the second problem remains the core problem for symmetrical encryption. On both sides of the data transmission, the secret key must be known and protected from unauthorized persons. If Alice simply e-mails the key to Bob, this method is not secure enough. The prerequisite is that the data connection is sufficiently secured, which is achieved precisely with this key. She must hand over the key to Bob in person or transmit it using an 'interception-proof' method. This task is difficult to handle in times of worldwide dynamic data communication.

Asymmetrical Encryption

Asymmetrical encryption was developed in the 70ies as a fundamentally new approach. Instead of one secret key that is known to both sides, this variant employs a pair of keys.

- The key owner uses the first part of the key pair to encrypt the data he is going to transmit. This key, subsequently referred to as public key, can be made publicly available to anyone worldwide.
- The second part of the key pair is the private key, which is only used for decrypting the messages received. Protect this secret key from access by unauthorized persons.

The main difference to symmetrical encryption methods: A publicly known key is used, resulting in the name "public-key method". A common asymmetrical encryption method is RSA, for example.
Let's take another look at the example of Alice and Bob:

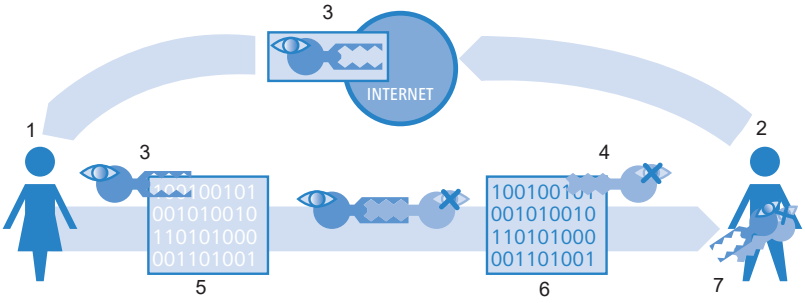


Figure 80: Asymmetrical encryption method

1: Alice
2: Bob
3: Bob's public key
4: Bob's private key
5: Encrypted message
6: Message in plain text
7: Bob's key pair, containing private and public key

- ☐ For secured communication, Bob first generates a key pair with a private key and public key that are uniquely matched. When generating these keys, Bob employs a procedure that makes it impossible to derive the private key from the public key. Bob can now distribute the public key without worries. He can e-mail it to Alice or simply store it on his web server.
- ☐ Alice now encrypts her message to Bob using his public key. Now Bob is the only one to decrypt this unreadable message with his private key. Even if unauthorized persons intercept the data on its way from Alice to Bob, no one but Bob can decrypt the plain text.

The asymmetrical encryption offers the following advantages over the symmetrical variant:

- A single key pair is required for each participant, and not for each communication relationship (as with synchronous encryption). With 1000 participants, every participant only requires his or her personal key pair, of which the public key is made publicly available. Instead of 500,000 secret keys, only 1000 key pairs are thus required with the public-key method.
- The unsecured transmission of the secret key to the communication partners is no longer necessary, as the public key is known on the other side of the communication relationship. This resolves an essential problem in the dynamic encryption of data between various participants.

Combination of Symmetrical and Asymmetrical Encryption

Asymmetrical encryption methods have quickly become established due to their security. However, security has its price: Asymmetrical encryption methods are slow. The mathematical procedures for encrypting and decrypting messages are much more complex than those of symmetrical encryption methods and therefore require more computing time. This is an exclusion criterion for the transmission of large data quantities.
The advantages of symmetrical and asymmetrical encryption can be enjoyed by suitably combining the methods. The secure asymmetrical encryption method is used to protect the transmission of the secret key. The connection's actual payload data is then encrypted using the quicker symmetrical encryption method.

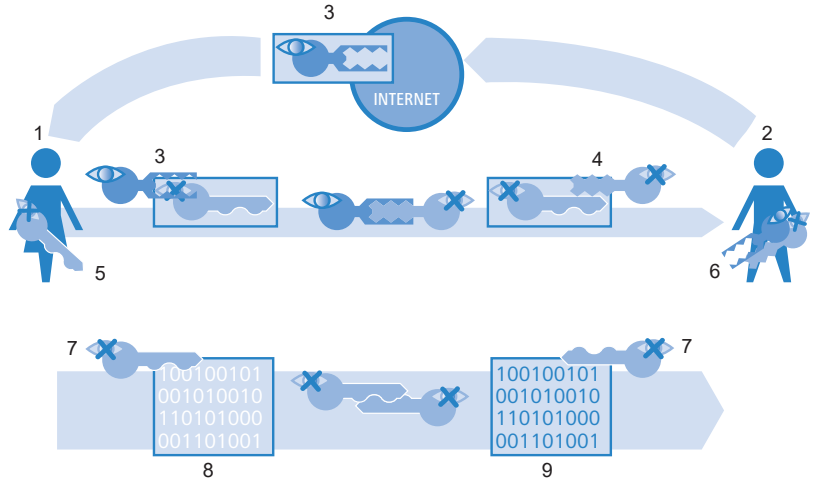


Figure 81: Combination of symmetrical and asymmetrical encryption

1: Alice
2: Bob
3: Bob's public key
4: Bob's private key
5: Alice's secret key
6: Bob's key pair, containing private and public key
7: Secret key
8: Encrypted message
9: Message in plain text

- ☐ In a first step, Bob creates his key pair and makes his public key publicly available.
- ☐ Alice uses the public key to encrypt a secret symmetrical key and sends it to Bob. This secret key is randomly generated for each transmission.
- ☐ Only Bob is able to decrypt the secret key with the aid of his private key.
- ☐ Alice and Bob then use the secret key for encrypting and decrypting the considerably larger payload data volumes.

Public Key Infrastructure

The combination of symmetric and asymmetric encryption methods make it possible to set up a secure data communication even via initially unsecured connections. Now we will shed some light on the aspect of authenticity: How does Alice know that the public key in use is actually from Bob? That is to say, the use of public keys depends on trust in the authenticity of the communication partner.
In order to secure this trust, publicly recognized credible offices confirm the key pairs of the asymmetric encoding that are being used In Germany, for example, the Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways is the highest credible authority for confirming digital keys. It in turn issues accreditations to suitable service providers who have likewise proved to be trustworthy.

Note: You can always find updated lists with accredited certification service providers, as well as references to revoked accreditations, on the website of the Federal Network Agency (www.bundesnetzagentur.de). A number of tax consultants and attorneys offices are included among the accredited service providers, for example.

The task of these authorities is to assign exactly one public key to one person or organization. This assignment is in a certificate and is publicly known. Therefore these providers are also called "certification authorities" or CA for short. The highest certification authority is considered the root/ master CA.
Bob turns to such a CA when he wants to have his public key certified for himself. To do this, he submits his public key to the CA, which confirms the association of the key with Bob.
The CA issues a certificate of this confirmation, which also contains data about Bob in addition to the public key, for example, his identity.

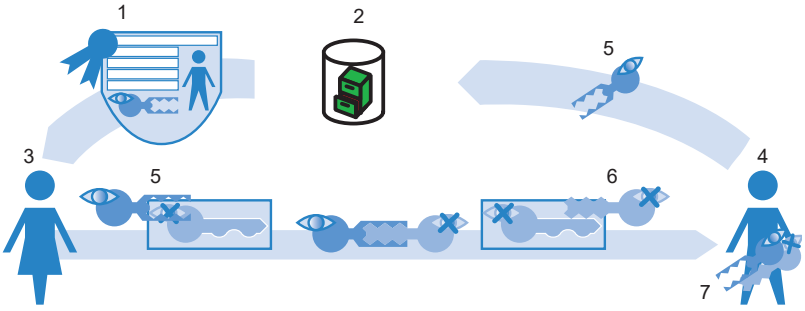


Figure 82: Method for issuing certificates for authorization

1: Certificate with public key from Bob, information on identity, signature of the CA
2: Certification authority (CA)
3: Alice
4: Bob
5: Bob's public key
6: Bob's private key
7: Bob's key pair with private and public key

The CA again signs the certificate, so that no one doubts the confirmation. Since the certificate consists only of a small amount of data, an asymmetric method is used for it. The asymmetric method operates in the opposite direction for the signature, however.

- The CA also has the key pair consisting of private and public key. As a trustworthy authority, its own key pair is considered reliable.
- The CIA calculates the hash value for the certificate, encrypts it and signs Bob's certificate with it. The CA therefore verifies the association of Bob's public key with his identity
  This process behaves in exactly the opposite manner as that for normal asymmetric encryption. Instead of protecting the data from unauthorized persons, encryption here has the purpose of confirming the CA's signature.
- With the public key of the CA, every participant in a data communication around the world is able to check the certificate signed with that key.
  Only the CA produces signatures with its private key, which it again encrypts with the CA's public key. This signature ensures that the certificate actually originates from the issuing CA.

7.5.2 Advantages of certificates

In some cases, the use of certificates for securing VPN connections is an alternative to the pre-shared key (PSK) method that is otherwise used.

- Secure VPN-client connections (with IKE main mode):
  When setting up PSK connections for peers with dynamic IP addresses, there is no possibility of using main mode. Instead of that, use aggressive mode with lower security. Using certificates enables usage of the main mode,and therefore an increase of security, even for peers with dynamic IP addresses.
- Higher security of the keys and passwords used:
  Pre-shared keys are just as susceptible as all other passwords. How the users handle these passwords ("human factor") thus has a considerable influence on the security of the connections. In a certificate-based VPN structure, the keys used in the certificates are automatically created with the desired key length. In addition, the random keys generated by computers, even with an identical key length, are more secure against attacks (e.g., dictionary attacks) than the pre-shared keys invented by human beings.
- Checking the authenticity of the counterparty is possible:
  In the VPN connection setup via certificates, it is necessary that the two opposing sides authenticate themselves. The certificates possibly contain additional information elements that help to check the remote terminals. The time limitation of certificates provides additional protection, e.g., for issuance to users who obtain temporary access to a network.
- Support of tokens and smart cards:
  Offloading the certificates onto external data media also allows them to be successfully integrated into "strong security" environments; reading passwords from computers or notebooks is out of the question.

The advantages of certificates contrast, however, with the higher expense for introducing and maintain a public key infrastructure (PKI).

7.5.3 Structure of certificates

Contents

In order to fulfill its tasks, a certificate contains a variety of information. Some parts of it are obligatory, others are optional. There are various formats in which a certificate is stored. A certificate according to the X.509 standard contains the following information, for example:

- Version: This entry contains the version of the X.509 standard. The current version (06/2005) is "v3."
- Serial number: An unambiguous serial number for identification of the certificate.
- Signature algorithm: Identifies the algorithm with which the issuer signed the certificate. The digital signature of the issuer is also located there.
- Validity: Certificates are valid for a limited period of time. Validity contains information on the duration.
- Issuer: Data for identifying the issuer, e.g., name, e-mail address, nationality, etc.
- Subject: Data for identifying the owner of the certificate, e.g., name, institution, e-mail address, nationality, city, etc.
- Subject public key: Information as to the method that the issuer used in generating the public key of the certificate holder. The public key of the owner is likewise located in this item.

Target application

When creating the certificates, select the purpose for which the certificates are available. Some certificates are conceived specifically and only for web browsers and e-mail transmission, while others are generally usable for any purposes.

Note: When creating the certificates, take care that you issue them for the desired purpose.

Formats

The ITU X.509 standard is a widely disseminated form for the certificates In a text representation, such a certificate resembles the following, for example:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial number: 1 (0x1)
        Signature algorithm: md5WithRSAEncryption
      Issuer: CN=CA/Email=ca@trustme.dom, OU=Certificate Authority,
O=TrustMe Ltd, ST=Austria, L=Graz, C=XY,
        Validity:
            Not Before: Oct 29 17:39:10 2000 GMT
            Not After: Oct 29 17:39:10 2001 GMT
       Subject: CN=anywhere.com/Email=xyz@anywhere.com, OU=Web Lab,
O=Home, L=Vienna, ST=Austria, C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (1024 bit)
                Modulus (1024 bit):
                    00:c4:40:4c:6e:14:1b:61:36:84:24:b2:61:c0:b5:
                    d7:e4:7a:a5:4b:94:ef:d9:5e:43:7f:c1:64:80:fd:
                    9f:50:41:6b:70:73:80:48:90:f3:58:bf:f0:4c:b9:
                    90:32:81:59:18:16:3f:19:f4:5f:11:68:36:85:f6:
                    1c:a9:af:fa:a9:a8:7b:44:85:79:b5:f1:20:d3:25:
                    7d:1c:de:68:15:0c:b6:bc:59:46:0a:d8:99:4e:07:
                    50:0a:5d:83:61:d4:db:c9:7d:c3:2e:eb:0a:8f:62:
                    8f:7e:00:e1:37:67:3f:36:d5:04:38:44:44:77:e9:
                    f0:b4:95:f5:f9:34:9f:f8:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
                email:xyz@anywhere.com
            Netscape Comment:
                mod_ssl generated test server certificate
            Netscape Cert Type:
                SSL Server
    Signature algorithm: md5WithRSAEncryption
        12:ed:f7:b3:5e:a0:93:3f:a0:1d:60:cb:47:19:7d:15:59:9b:
        3b:2c:a8:a3:6a:03:43:d0:85:d3:86:86:2f:e3:aa:79:39:e7:
        82:20:ed:f4:11:85:a3:41:5e:5c:8d:36:a2:71:b6:6a:08:f9:
        cc:1e:da:c4:78:05:75:8f:9b:10:f0:15:f0:9e:67:a0:4e:a1:
        4d:3f:16:4c:9b:19:56:6a:f2:af:89:54:52:4a:06:34:42:0d:
        d5:40:25:6b:b0:c0:a2:03:18:cd:d1:07:20:b6:e5:c5:1e:21:
        44:e7:c5:09:d2:d5:94:9d:6c:13:07:2f:3b:7c:4c:64:90:bf:
        ff:8e
```

File types

Digital certificates and private keys have different file extensions, depending on the issuer. The following endings are typical, for example:

- ☐ *.pfx and *.p12: PKCS#12 files
- ☐ *.pem, *.cer and *.crt: BASE 64-coded certificates
- ☐ *.cer, *.crt and *.der: DER-coded certificates
- ☐ *.key: BASE64- or DER-coded keys
- ☐ *.pvk: Microsoft-specific key format

In the context of certificate-secured VPN connections, another file type is very important in addition to pure certificates: the PCKS#12 files, which may contain several components, including a certificate and private key among others. Processing the PCKS#12 files requires a password, which you define when exporting the certificates.

Note: BASE64-coded certificates contain the following line in the header:

```
----- BEGIN CERTIFICATE -----
```

Validity

A reference to a so-called certificate revocation list (CRL) is also optionally included. Certificates that have become invalid, for example, because an employee left the company and the company therefore withdrew his certificate, are listed in the CRLs. With this information, the proper CRL is used in checking the certificates.

7.5.4 Security

Observe the following safety aspects in handling certificates:

- ☐ Transmit the private keys only via secure connections, for example, HTTPS.
- ☐ Use sufficiently long and secure passphrases as keywords for the key or the PKCS#12 files.

7.5.5 Certificates in VPN connection setup

In addition to the fundamental information on the topic of certificates, we will consider the specific application for VPN connection setup in this section. For such a connection setup with certificate support, there must be certain information available on both sides of the connection:

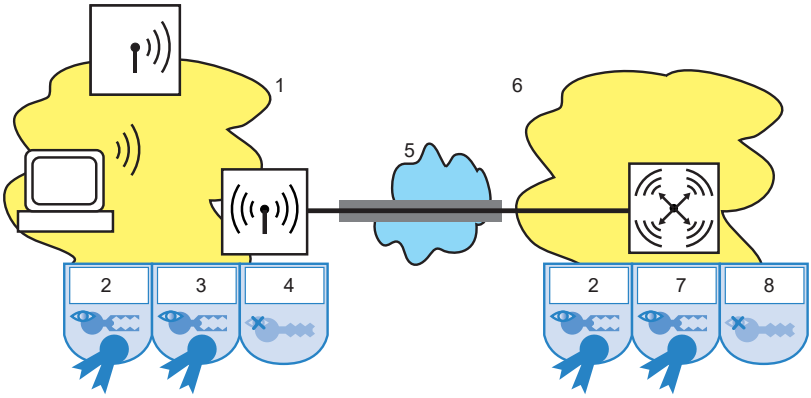


Figure 83: Usage of certificates for a VPN connection between headquarters and a branch office
1: Branch office
2: Root CA certificate
3: Branch office certificate

4: Branch office private key
5: Internet
6: Headquarters
7: Headquarters certificate
8: Headquarters private key

- The branch office has the following components:
  - Root CA certificate with the CA's public key
  - Its own device certificate with its own public key and the confirmation of identity. The checksum of the certificate is signed with the CA's private key.
  - Own private key
- The headquarters has the following components:
  - Root CA certificate with the CA's public key
  - Its own device certificate with its own public key and the confirmation of identity. The checksum of the certificate is signed with the CA's private key.
  - Own private key

The following processes, shown in main mode for simplicity, take place in the VPN connection setup (symmetrically in both directions):

- In a first packet exchange, the peers negotiate the encryption methods to be used in the authentication processes, for example. In this phase, both sides do not have any certain knowledge of whom they are currently negotiating with. That is insignificant up to this point, however.
- In the next step, the connected devices negotiate a shared key material for further use, containing symmetric keys and asymmetric key pairs, among others. In this state as well, both sides are still uncertain of whom they have negotiated the keys with.
- With the aid of the certificates, the device checks in the next step whether the peer from the negotiation of the key material is in fact the intended communication partner:
  - From the key material of the current negotiation, the branch office calculates a checksum (hash), which only the two involved peers (branch office and headquarters) calculate during this connection.
  - The branch office encrypts this hash with its own private key and thus creates a signature.
  - The branch office transmits the signature together with its own certificate to the peer in headquarters.

- Headquarters then checks the signature for the received certificate from the branch office. It does this with the aid of the public key in the root CA, which is available identically in both peers. If the peer at headquarters decrypts the signature from the branch office certificate created by the private key of the CA with the public key of the CA, then the signature is valid and the peer trusts the certificate.
- In the next step, headquarters then checks the signature of the encrypted checksum. It has already found that the branch office's public key from the corresponding certificate is valid in the previous step. Headquarters therefore checks whether it can decrypt the signed checksum with the branch office's public key. Headquarters calculates the same checksum from the key material of the current connection as did the branch office. If this check is successful, headquarters considers the peer "branch office" to be authenticated.

7.5.6 Certificates from certificate service providers

The certificates offered by public certification authorities are generally requested in different security classes. As security increases, the effort and expense for the applicant to authenticate its identity to the CA rises. Trustcenter AG in Hamburg uses the following classes, for example:

- Class 0: Trustcenter issues these certificates without checking the identity and uses them for test purposes for business clients.
- Class 1: In this level, Trustcenter checks the existence of an e-mail address. This level is suitable for private users who sign their e-mail, for example.
- Class 2: In this level as well there is no personal identity check. Transmitting an application with a copy of a commercial register entry, for example, is sufficient. This level is suitable for communication between companies that are known to one another.
- Class 3: In this level Trustcenter checks the person or company personally. Trustcenter checks the information in the issued certificates against a passport or an extract from the commercial registry. This level is suitable for advanced applications, for example, in e-business or online banking.

If you work together with a public certificate service provider, carefully check the security levels offered for the identity check. That way you can determine whether the certificates used actually meet your security needs.

7.5.7 Structure of one's own CA

Using public CAs is recommended for secure enterprise communication only to a certain extent:

- The issuance of new certificates is expensive and sometimes too slow.
- Public CAs transmit the keys that are used over poorly secured connections.
- Communication is based on trust of the CA.

Construction of a CA of one's own is therefore a suitable alternative for enterprise communication. The Microsoft CA on the Microsoft Windows 2003 Server, or OpenSSL as an open source version, are suitable for this. Create and manage all required certificates for securing data exchange yourself with a CA of your own, without dependency on outside authorities.

The use of a CA of their own is certainly more advisable to companies than using public providers for certification services. There are some important items already in the planning stage for the CA, however. Already when a Windows CA is installed, for example, the program establishes validity times for the root CAs that cannot be subsequently changed. Further aspects of planning include:

- The certificate policy, i.e., the security level which you seek with the aid of the certificates
- The namespace to be used
- The key lengths
- The lifetime of the certificates
- The management of blacklists

Precise planning pays off in every case, since later corrections can sometimes only be achieved at great expense.

7.5.8 Requesting a certificate with the standalone Windows CA

Note: A combination of a PKCS#12 file with a root certificate, a certificate of one's own devices and the public key of the device provide the best service for use in a device.

☐ Open the starting page of the Microsoft certificate service in your browser.
☐ Choose "Extended certificate request" as the certificate type.
☐ In the next step, choose the option "Create and submit a request to this certificate authority."

Note: Choose the option "BASE64" only if the root certificate is already present in a separate file.

☐ Enter the data for identification in the next step.

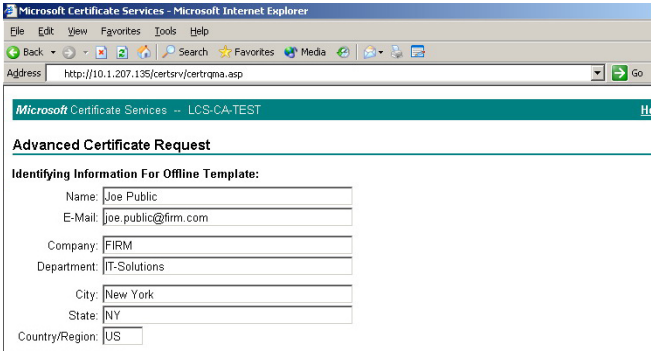


Figure 84: Request for extended certificate – entering data for identification

☐ In the same dialogue, select the option "Other ..." as the type of certificate and delete the value for "Object identifier" that then appears.

Figure 85: Extended certificate request – selecting the type of certificate

☐ Highlight "Automatic key generation." Thereby the CA automatically generates the public and private key for the current user.

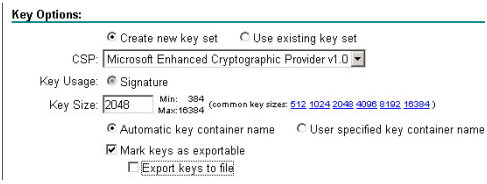


Figure 86: Extended certificate request – defining key options

☐ Select a suitable key length (matching the certificate policy). Activate the option for exportable keys.

Note: Since no export of the key is necessary at this point, you indeed not specify any filenames. While exporting, the program would create a file in the Microsoft-specific *.pvk format, which is worthless for further processing in a Hirschmann device.

☐ Finally choose the "SHA-1" algorithm and submit the certificate request by clicking the "Submit" button.

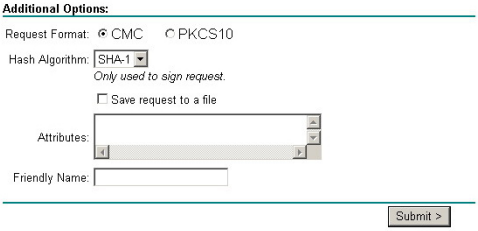


Figure 87: Extended certificate request – selecting hash algorithm

Note: You can view the status of the submitted certificate requests at any time via the homepage of the Windows CA. However you are only able to view the certificate requests from the same computer with which you submitted the request.

☐ Install the certificate on your computer as soon as the administrator of the CA has checked the certificate request and created the certificate

Note: You are only able to view the certificates from the same computer with which you submitted the request.

7.5.9 Exporting the certificate to a PKCS#12 file

When the certificate is installed, the device stores it in your operating system, but it does not yet exist as a separate file. You need one for installation in the Hirschmann device, however. To obtain a certificate in file form, it is necessary to first export it.

Export via the Windows console tree:

☐ To do this, open the management console with the MMC command at the prompt, and select the menu item File > Snap-in add/remove.

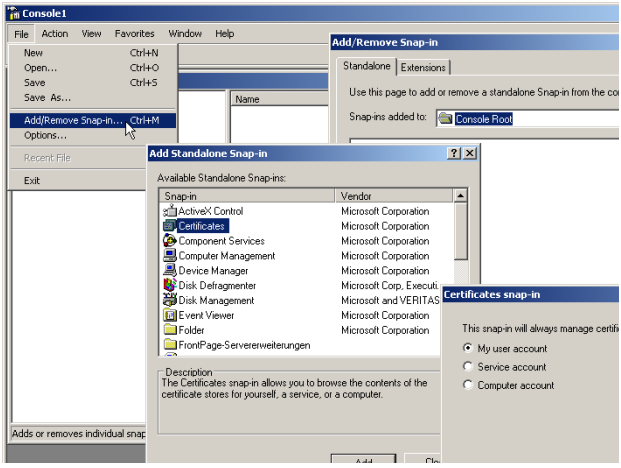


Figure 88: Adding certificates with Windows Management Console

☐ Click on Add.. and select the "Certificates" entry. Confirm with Add, then highlight "Own user account" and click on "Finish."

☐ In order to export the desired certificate into a file, click in the management console in the group Certificates – Current User > Own Certificates > Certificates with the right mouse button and select the entry All Tasks > Export in the context menu.

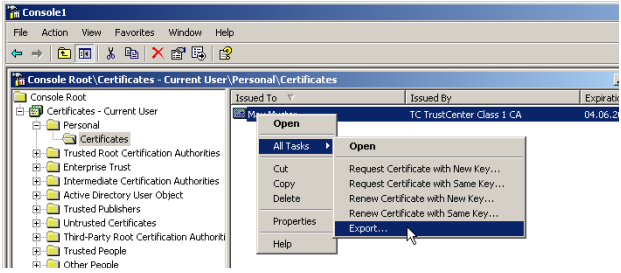


Figure 89: Exporting certificates with Windows Management Console

☐ In the process for the Certificate Export Wizard, activate the option for exporting the private key. Optionally delete the private key from the system after the export.

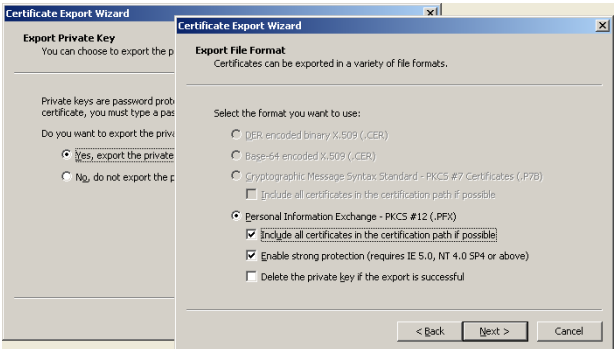


Figure 90: Certificate Export Wizard

Note: It is necessary to activate the option "Include all Certificates in the Certification Path." In this case, the program also exports the root certificate into the PKCS#12 file.

☐ During export the device prompts you to input a password for protecting the private key. Select a secure passphrase of sufficient length. You will again require this passphrase for the installation of the certificates in the Hirschmann device.

Note: Different environments also use the synonymous terms "password" or "PIN" for passphrase.

Export via the system controller

Alternatively you can open the certificates installed on the system via the system controller.

☐ To do this, select Start > System Controller > Internet Options and click the Certificates button on the "Contents" tab.

☐ Select the desired certificate and click on Export

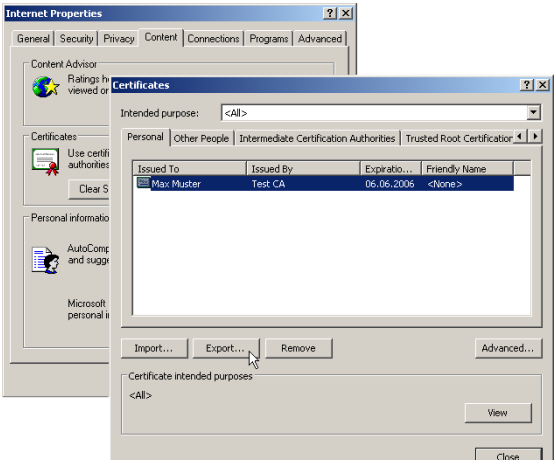


Figure 91: Exporting certificates via the system controller

Note: The subsequent Certificate Export Wizard behaves exactly as described in "Exporting certificates with Windows Management Console."

7.5.10 Creating certificates with OpenSSL

OpenSSL provides another possibility for creating certificates of your own and testing certificate connections. OpenSSL is available free as an open source project for Linux and Windows but as a command-line tool, it is less user-friendly than other CA versions.

Note: It is also necessary that you adapt the configuration file openssl.cnf to your specific needs. Further information can be found in the documentation for OpenSSL.

Installing OpenSSL

- ☐ Download a current version of OpenSSL from http://www.slproweb.com/products/Win32OpenSSL.
- ☐ Install the package and in the `./bin/PEM/demoCA` directory, also create the subdirectories:
  - `/certs`
  - `/newcerts`
  - `/cerl`.
- ☐ In the file openssl.cnf, change the path in the group [CA_default] to: `dir= ./PEM/demoCA`
- ☐ Start OpenSSL by double-clicking on openssl.exe in the `./bin` directory.

Issuing certificate for the root CA

- ☐ Create a key for the CA with the command:
  `genrsa -des3 -out ca.key 2048`

  Note: Note the passphrase that you input after the prompt for the CA key. You will need it again later.

  This command creates the file "ca.key" in the current directory.
- ☐ Create a certificate request for the CA with the command:
  `req -key ca.key -new -subj /CN=”Test_CA” -out ca.req`

  Note: Again input the passphrase for the CA key here.

  This command creates the file "ca.req" in the current directory.
- ☐ Create a certificate from the certificate request with the command:
  `x509 -req -in ca.req -signkey ca.key -days 365 -out ca.crt`
  This command signs the certificate request "ca.req" with the key "ca.key" and thus issues the certificate "ca.crt."

  Note: Again input the passphrase for the CA key here as well.

Issuing a certificate for users or devices

☐ Create a key for the device or the user with the command:
`genrsa -out device.key 2048`
This command creates the file "device.key" in the current directory.

☐ Create a certificate request for the device or the user with the command:
`req -key device.key -new -subj /CN=DEVICE -out device.req`
This command creates the file "device.req" in the current directory.

Note: In addition to this command, additional changes in the file "openssl.cnf" are necessary for definition of an extension.

☐ Create a certificate from the certificate request with the command:
`x509 -extfile openssl.cnf -req -in device.req -CAkey ca.key -CA ca.crt -CAcreateserial -days 90 -out device.crt`
This command signs the certificate request "device.req" with the key "ca.key" and thus issues the certificate "device.crt." The device also uses the configuration file openssl.cnf here.

☐ Export the certificate for the device or the user with the command:
`pkcs12 -export -inkey device.key -in device.crt -certfile ca.crt -out device.p12`
This command combines the key "device.key," the device certificate "device.crt," and the root certificate "ca.crt" and stores them jointly in the file "device.p12." Load this PKCS#12 file directly into the desired device.

7.5.11 Loading certificates into the Hirschmann device

It is necessary for the following components to be present in the Hirschmann device for the certificate-secured VPN connection setup:

- Root CA certificate with the CA's public key
- Its own device certificate with its own public key and the confirmation of identity. The checksum of the certificate is signed with the CA's private key.
- Own private key

If you have followed the instructions for issuing and exporting a certificate via a Windows CA, this information is now available in the form of a shared PKCS#12 file. Alternatively, you have used a different method and the individual components are present in separate files.

☐ Log onto the desired device with administrator rights via WEBconfig.
☐ Select the entry Upload Certificate or File.

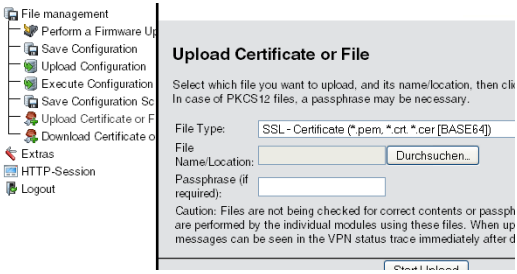


Figure 92: Load certificate into the Hirschmann device via WEBconfig.

☐ Select the components you will load into the device:
  ☐ Root certificate
  ☐ Device certificate
  ☐ Private key of the device
  ☐ PKCS#12 with a combination of root certificate, device certificate and private key

Note: Depending on the type of uploaded file, it may be necessary for you to input the respective passphrase.

You have the possibility of subsequently viewing the uploaded files in a list under HiLCOS Menu Tree > Status > File System > Content.

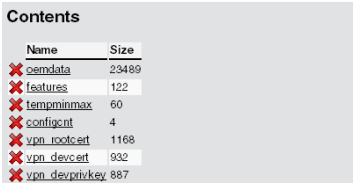


Figure 93: List of uploaded files in WEBconfig

Note: In the upload, the device breaks a combined PKCS#12 file down into the required parts automatically.

7.5.12 Backing up and uploading certificates with LANconfig

Use different certificates for decrypting defined services in a Hirschmann device. Load the certificates into the devices via LANconfig. You also have the possibility of reading out the certificates stored in a device via LANconfig and saving them in a file.

☐ Select the device into which you load a certificate or from which you back up a certificate.

☐ Click the selection with the right mouse button and select Configuration Management > Backup Certificate as File/Load Certificate as File in the context menu.

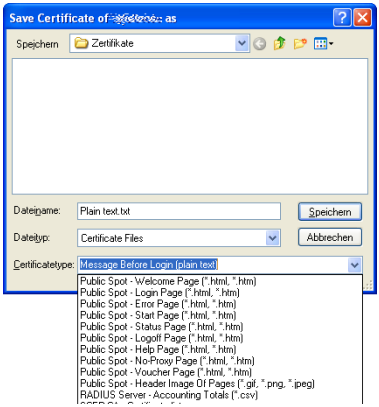


Figure 94: Saving or reading out certificates with LANconfig

☐ Select the storage location and type of the certificate that you are backing up or uploading and confirm the selection with Save/Open.

Note: By selecting several devices you upload a certificate file into several devices at the same time. Simultaneously backing up certificates from several devices is excluded, however. Depending on the type of certificate file, a passphrase may be necessary for uploading.

7.5.13 Adjusting VPN connections to certificate support

Note: The device sets up VPN connections with certificate support only if the Hirschmann device has the correct time of day. If the device has no up-to-date time of day, it also has no possibility of correctly assessing the validity of the certificates. The device then rejects the certificates and no connection is created.

Prepare different parts of the configuration in order to adjust VPN connections to support certificates:

- IKE proposals
- IKE proposal lists
- IKE keys
- VPN parameters
- Connection parameters

Note: Depending on the firmware status, your device already contains some of the required values. In this case, simply check the values for correct settings.

Note: If you are converting a remote device to certificate support via VPN, then by all means convert the remote device first. Do this before you change the connection of the local device. Otherwise, if you change the local configuration you cannot set up a connection to the remote device.

☐ Two new proposals with the exact designations "RSA-AES-MD5" and "RSA-AES-SHA" appear in the lists of proposals. They both use "AES-CBC" as their encryption and the "RSA signature" authentication mode, and differ only in their hash method (MD5 or SHA1)

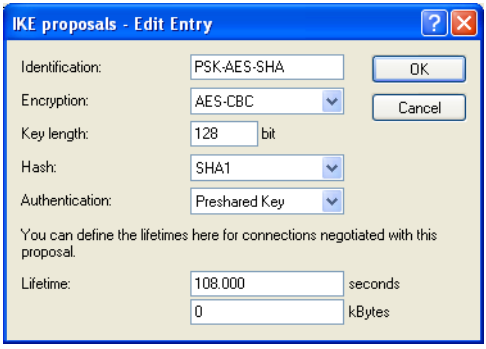


Figure 95: Entries into the IKE proposals

LANconfig: VPN > IKE-Param. > IKE proposals
WEBconfig: HiLCOS Menu Tree > Setup > VPN > Proposals > IKE

☐ A new list with the exact designation "IKE_RSA_SIG," which contains the two new proposals "RSA-AES-MD5" and "RSA-AES-SHA," is required in the proposal lists.

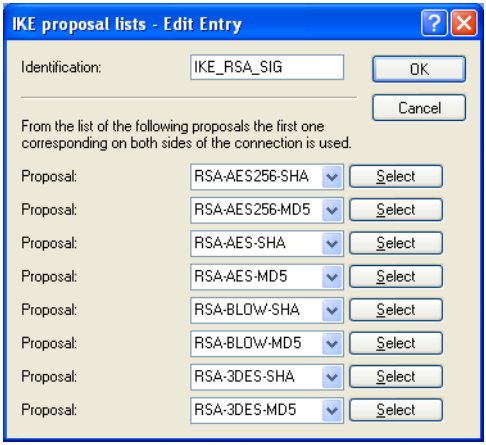


Figure 96: New list in the IKE proposals

LANconfig: VPN > IKE-Param. > IKE Proposal Lists
WEBconfig: HiLCOS Menu Tree > Setup > VPN > Proposals > IKE Proposal Lists

☐ Insert the appropriate identities in the list of IKE keys for all certificate connections.

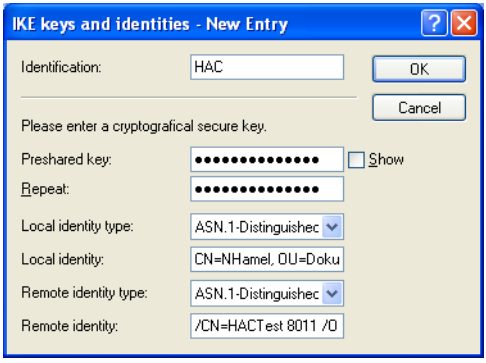


Figure 97: IKE keys in LANconfig

LANconfig: VPN > IKE Auth. > IKE keys and identities

- Delete the pre-shared key when it finally has no more use.
- Adjust the type of the identities to "ASN.1 Distinguished Names" (local and remote).
- Enter the identities exactly as in the certificates. Separate the individual values for "CN," "O" or "OU" by commas or slashes.
  It is required that you list all the values entered in the certificates in the same order. Check the contents of the certificates via the system controller if necessary. To do this, select Start > System Controller > Internet Options and click the Certificates button on the "Contents" tab. Open the desired certificate and select the appropriate value on the "Details" tab. Here you will find the required ASN.1 Distinguished Names with the associated abbreviations for the requester, for example.. Enter the values in the certificates from top to bottom into the IKE key from left to right. Please note the case-sensitivity here.

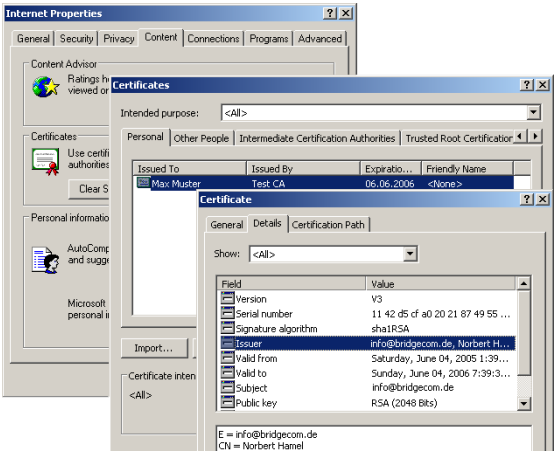


Figure 98: Certificates in the Internet options

Note: The display of certificates under Microsoft Windows shows older abbreviated forms for some values. These include, for example, "S" in place of "ST" for "stateOrProvinceName" or "G" in place of "GN" for "givenName." For these, use only the current abbreviated forms "ST" and "GN."

Note: You can enter special characters in the ASN.1 Distinguished Names by inputting the ASCII code in hexadecimal representation with a preceding backslash. For example, "\61" corresponds to a lowercase "a."

You can find the IKE key under WEBconfig or Telnet at the following places:

Configuration tool	Call
WEBconfig	HiLCOS Menu Tree > Setup > VPN > Certificate Keys > IKE Keys
Terminal/Telnet	/Setup/VPN/Certificate keys/IKE keys

☐ In the IKE connection parameters, place the default IKE proposal lists for incoming aggressive mode and main mode connections on the proposal list "IKE_RSA_SIG." Also note the setting of the default IKE group, the adjustment of which may be required by the next step.
The default IKE proposal lists and default IKE groups are found under LANconfig in the "VPN" configuration area on the "Defaults" tab.

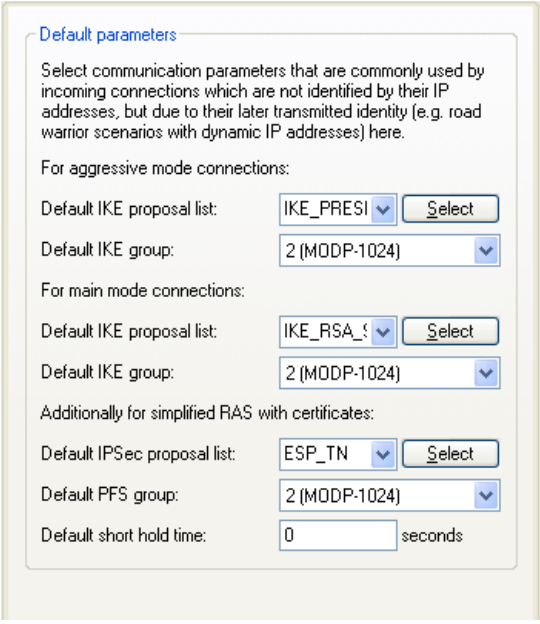


Figure 99: Editing IKE connection parameters

You can find the IKE proposal lists and the default IKE groups under WEBconfig or Telnet at the following places:

Configuration tool	Call
WEBconfig	HiLCOS Menu tree > Setup > VPN
Terminal/Telnet	/Setup/VPN

☐ Finally adjust the VPN connections in the APN connection parameters to the use of the correct IKE proposals ("'IKE_RSA_SIG"). It is necessary that the values for "PFS group" and "IKE group" match the values set in the IKE correction parameters.
The VPN correction parameters are found under LANconfig in the "VPN" configuration area on the tab "General" with a click on the Connection Parameters button.

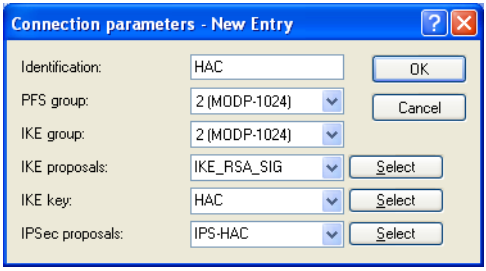


Figure 100:Checking the connection parameters in LANconfig

You can find the VPN connection parameters under WEBconfig or Telnet at the following places:

Configuration tool	Call
WEBconfig	HiLCOS Menu tree > Setup > VPN > VPN Layer
Terminal/Telnet	/Setup/VPN/VPN-Layer

7.5.14 Creating certificate-based VPN connections for LAN coupling using the Setup Wizard

With the Setup Wizard from LANconfig you have the possibility of setting up LAN couplings via VPN quickly and conveniently.

Note: Setting up VPN connections with certificate support is possible only if the Hirschmann device has the correct time of day and you have loaded the appropriate certificates into the device.

- ☐ Select the Wizard for connecting networks via VPN. Then select the VPN connection authentication via certificates (RSA signature) in the appropriate dialog.
- ☐ Enter the identities from the local and remote device certificate. Transfer the complete data from the respective certificates in the correct order: Enter the ASN.1 Distinguished Names listed under Windows in the certificates from top to bottom into LANconfig from left to right.

Note: The display of certificates under Microsoft Windows shows older abbreviated forms for some values. These include, for example, "S" in place of "ST" for "stateOrProvinceName" or "G" in place of "GN" for "givenName." For these, use only the current abbreviated forms "ST" and "GN."

Note: The Telnet command `show vpn cert` shows the contents of the device certificate in a Hirschmann device, including the input relative distinguished names (RDN) under "subject."

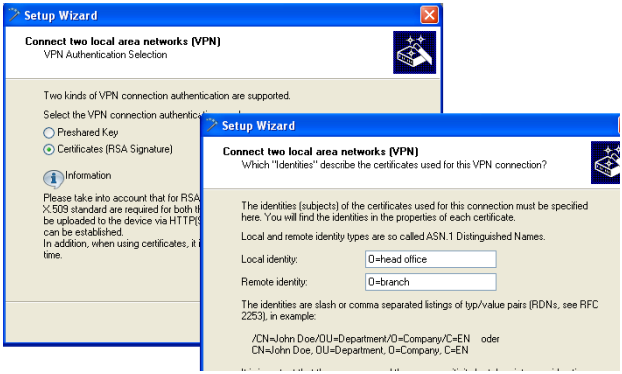


Figure 101:Setup Wizard for LAN-LAN coupling

☐ Select the optimized connection setup with IKE and PFS group 2 if possible. Select group 5 for IKE and PFS only if the remote terminal demands it.

☐ Enter the names of the VPN remote terminal, the IP address and the network mask of the remote network as well as a domain for the DNS relay, if appropriate. Activate the "Extranet" function and "netBIOS Routing" as needed.

7.5.15 Simplified network connection with certificates – pro-adaptive VPN

For VPN-coupling of large network structures, it is advantageous if the configuration effort for the setup of the new subnetwork is limited to the VPN router there and the configuration of the central dial-in router remains untouched. In order to achieve this simplified network connection, the devices dialing in transfer their identity with the aid of a certificate.

If you have activated the simplified dial-in with certificates for the Hirschmann router in the central station, then the remote routers themselves specify a network during the IKE negotiation in Phase 2. The routers then use it for the connection. This network is used, for example, when setting up the VPN connection in the remote router. The Hirschmann router in the central station accepts the opposed network if you have activated the option "Allow remote terminal selection of the remote network." It is also necessary that the parameters used by the client in the dial-in match the default values of the VPN router.

Note: In the configuration of the remote terminals that dial in, see to it that each remote terminal requests a special network. In that way there will be no conflicts between the network addresses.

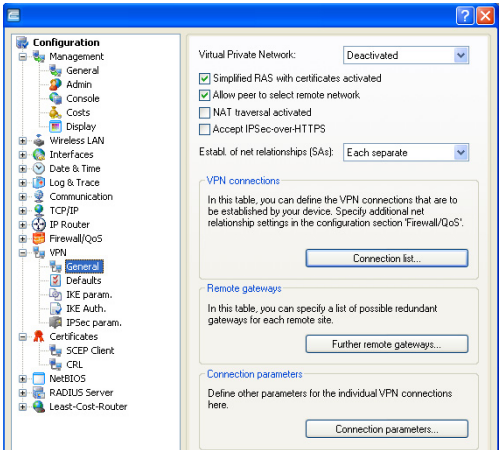


Figure 102:Simplified network connection with certificates

Configuration tool	Call
LANconfig	VPN/General and VPN > General > Defaults
WEBconfig, Telnet	HiLCOS Menu tree > Setup > VPN

Note: By activating the simplified certificate dial-in, all remote routers have the possibility of dialing in to the respective network with a valid certificate that bears the signature of the issuer of the root certificate located in the device. The router does not need any further configuration. You present undesired dialing-in exclusively by blocking certificates and using a certificate revocation list (CRL).
Simplified connection of networks with certificates is therefore limited to Hirschmann routers that support CRL.

7.5.16 Requesting certificates by means of CERTREQ

Some VPN gateways expect that the remote terminal will request certificates to be transmitted via a "certificate request" (CERTREQ) in an IPSec mediation authenticated by means of an RSA signature. Among other things, this allows a selection of the certificate to be used, as long as the gateway trusts multiple CAs.
In order to allow the setup for such VPN gateways, Hirschmann routers send a corresponding CERTREQ during the connection setup. It contains the issuer of the root certificate stored in the Hirschmann router.

7.5.17 Certificate revocation list - CRL

Certificates for VPN connections contained a validity period in the form of starting and ending dates. Set up a VPN connection during this time via this certificate. If an employee who uses such a certificate for mobile VPN access, for example, leaves the company, it may be desirable to prematurely declare the certificate invalid. This is done so that there is no longer a possibility for access to the company network even with an unchanged configuration of the VPN routers.

Since the certificate itself is with the employee, and the latter cannot make any changes to the certificate, the device uses a certificate blocking list. The invalid certificates are entered in such a certificate blocking list, which is supported by Microsoft CA or OpenSSL, for instance. The CRL is available on a suitable server. The VPN router itself enters the URL from which a router loads the CRL into its memory into the root certificate and/or its configuration. This CA updates the CRL regularly, so that VPN routers promptly recognize changes in the CRL due to withdrawn certificates. When the CA is imposed, there is usually a time span after which the CRL is regularly updated. After the update of the CRL and the storage of the CRL on the server (manually or automatically) the VPN router updates this new information. To do this, the router reads out the validity period of the CRL and attempts to load the current CRL shortly before expiration. Alternatively you find a regular update – independently of the validity period of the CRL – in a Hirschmann router. In the connection setup, the VPN router checks whether the current CRL contains a certificate of the remote terminal. In that way, the device refuses connections to remote terminals with invalid certificates.

Configuration of the CRL function

In addition to the path of the CRL, specify additional parameters such as the update interval for the configuration of the CRL function.

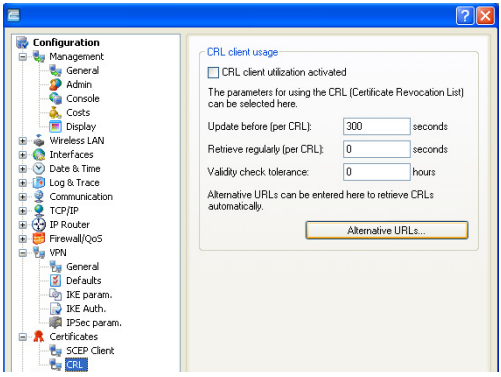


Figure 103:Configuration of the CRL function

Configuration tool	Call
LANconfig	Certificates > CRL client
WEBconfig, Telnet	HiLCOS Menu tree > Setup > Certificates > CRLs

- CRL functionality [default: off]
  Activated: When checking a certificate, the device also consults the CRL (if available).

  Note: If you have activated this option and the device does not find a valid CRL because, for example, there is no connection to the server, then the router refuses all connections and interrupts existing connections.

- Retrieval before expiration [default: 300 seconds]
  The point in time before expiration of the CRL from which the device attempts to load a new CRL. This value is increased by adding a random component in order to avoid excessively many requests to the server. When this point in time is reached, a regular update that may be activated stops.

  Note: If the loading of the CRL is unsuccessful in the first attempt, then the device starts new attempts in short intervals of time.

- Retrieval regular [default: 0 seconds]
  The length of the period of time after which the device periodically attempts to obtain a new CRL. With this, you can download CRLs published out of sequence early. With an entry of "0" you deactivate the regular retrieval.

  Note: If loading of the CRL is unsuccessful for regular updates, then the device will not start any attempts until the next regular date.

- Validity tolerance
  The device allows certificate-based connections even after the expiration of the CRL validity within the period of time entered here. With this tolerance time, you can prevent the device from refusing or disconnecting conditions in case of a short-term interruption of connection to the CRL server.

Note: Within the period of time set here, you can keep a connection in existence or set up a new connection with the aid of the certificates already blocked in the CRL.

- Alternative URLs
  The certificates usually contain the address from which the device retrieves a certificate revocation list (CRL) as crlDistributionPoint. Specify alternative URLs in this table. After system startup, the device loads the corresponding CRLs automatically from these URLs and uses them in addition to the lists specified in the certificates.

Display of the CRL status in LANmonitor

Information on the validity period and the publisher of the current CRL in the Hirschmann router can be found in LANmonitor.

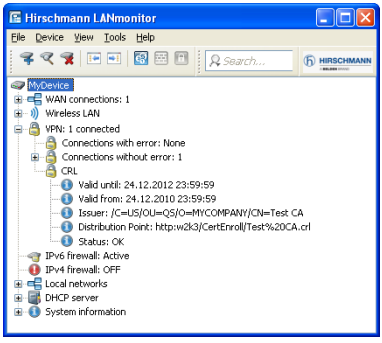


Figure 104:CRL status in LANmonitor

7.5.18 Diagnosis of the VPN certificate connections

The following commands at the console provide helpful information in case the device has no possibility of setting up a functional connection:

- ☐ `trace + vpn-status`
  Shows a trace of the current VPN connections.
- ☐ `show vpn long`
  Shows the contents of the VPN configuration, among other things, the distinguished names (DN) that are registered.
- ☐ `show vpn ca`
  Shows the content of the root certificate.
- ☐ `show vpn cert`
  Shows the content of the device's own certificate.

7.6 Multilevel certificates for SSL/TLS

7.6.1 Introduction

For large or spatially distributed organizations, multilevel certificate hierarchies are used, in which one or more intermediate CAs issue final certificates. The intermediate CAs are themselves certified by a root CA.

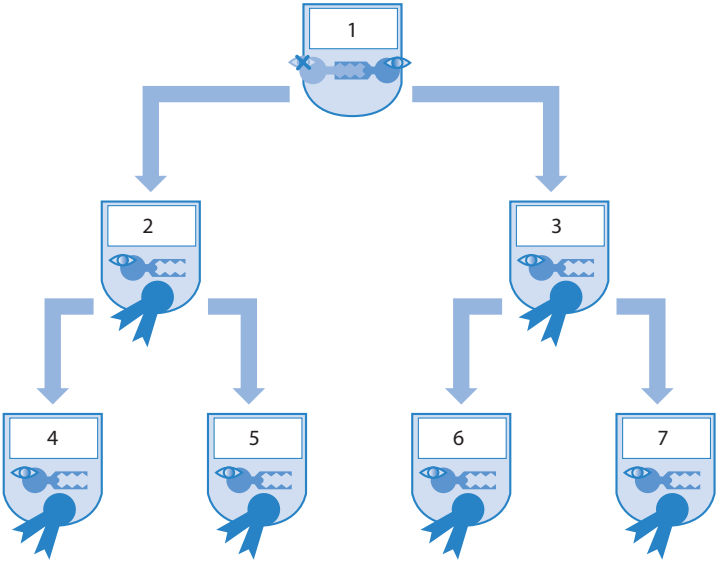


Figure 105:Multilevel certificates for SSL/TLS

1: Root CA
2: CA Europe
3: CA America
4: User 01
5: User 02
6: User 03
7: User 04

Checking the entire certificate hierarchy is necessary for authenticating the final certificates.

7.6.2 SSL/TLS with multilevel certificates

Applications that are based on SSL/TLS, (e.g. EAP/802.1x, HTTPS or RADSEC) load the SSL (server) certificate, together with its private key and the CA certificate(s) of the intermediate levels, as PKCS#12 containers into the device.
The remote terminals then send only their own device certificate to the device during connection setup. The Hirschmann router checks the certificate chain for validity.

7.6.3 VPN with multilevel certificates

To set up certificate-based VPN connections, the device stores a private key, a device certificate and the certificate of the CA in the file system. Use either the individual files or a PKCS#12 file for single-layer certificate solutions. After uploading and the input of the passphrase, the router breaks such a container down into the three above-mentioned components.
For a multilevel certificate hierarchy, however, the device uses a PKCS#12 container with the certificates of the CAs of all levels in the certificate chain. After uploading and the input of the passphrase, the device unpacks the certificate of the next CA "above" the device, in addition to the private key and the device certificate. The remaining certificates remain in the PKCS#12 container. For updating the VPN configuration, the router reads the unpacked certificates and the certificates from the container. When setting up a VPN connection, the remote terminal then transmits only its own device certificate. The device then checks the certificate against the existing hierarchy.

Note: It is necessary for the certificate structures to match for both remote terminals. That means that the hierarchy of the requesting VPN device requires only certificates that likewise occur in the hierarchy of the other VPN device.

7.7 Certificate enrollment via SCEP

To secure communication over publicly accessible networks, certificate-based VPN connections are being used more and more. The high-security demand of the digital certificates is countered by a considerable extra expense for managing and distributing the certificates. This expense primarily arises in the branch offices or home offices of a distributed network structure.
In order to set up a certificate-based VPN connection from a remote terminal to the network of a central system, a Hirschmann VPN router requires the following components:

- ☐ Certificate of the root CA with the public key of the CA. It is necessary that a certificate issued by the same CA likewise be present in the central station.
- ☐ Device's own certificate with its own public key. This certificate contains the signature with the private key of the CA and creates the confirmation of identity.
- ☐ Its own private key.

Note: The SCEP client supports one certificate for each purpose of use (VPN, WLAN controller). For the CAs, you have the opportunities to select the setting "general" in addition to the concrete purpose of use. If you enter a general CA then the router uses this CA for all certificates.

For a conventional structure of the VPN with certificates, it is necessary to enter the keys and certificates manually into the individual devices and change them promptly before expiration. The Simple Certificate Enrollment Protocol (SCEP) permits secure and automated distribution of certificates via an appropriate server. This reduces the expense for the rollout and the maintenance of certificate-based network structures. The router itself

generates the key pair for the device directly. The private part of the key thus never leaves the device, which represents a considerable increase in security. A Hirschmann VPN router has the possibility of calling up both the root certificate of the CA and its own device certificate via SCEP automatically from a central location.

7.7.1 SCEP server and SCEP client

An SCEP server takes over the provision and maintenance of the certificates. In addition to the function of an ordinary certification authority (CA) the server also has the SCEP functionality. Implement this server, e.g., as a Windows 2000 Server CA with a special plug-in (mscep.dll). There are also a number of CA solutions that support SCEP, for example the open-source solution OpenCA (www.openca.org).
The SCEP extension, i.e. mscep.dll, creates an additional instance on the server that processes the SCEP clients and hands them over to the actual CA. This instance is known as a registration authority (RA).
The VPN devices, (that is, the Hirschmann VPN routers) appear as SCEP clients, which automatically retrieve the required certificates from the central server. The device also requires the certificates signed by the CA from the RA (registration authority) for the SCEP process. For the actual VPN operation, the Hirschmann VPN routers primarily require valid system certificates (device certificates). The other certificates that are used are necessary solely for the SCEP process.

7.7.2 The process sequence of a certificate distribution

In overview, the distribution of certificates via SCEP runs according to the following diagram:

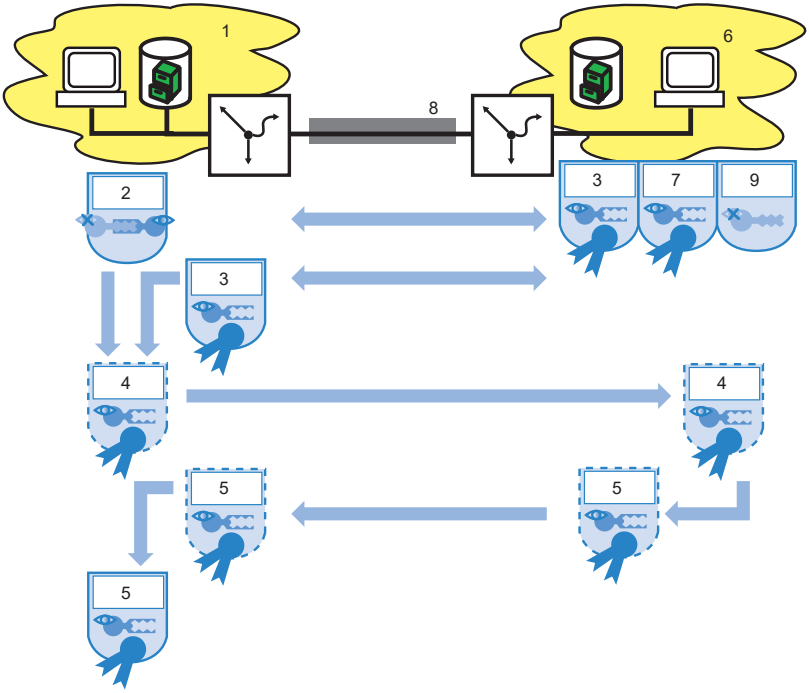


Figure 106:Process sequence of the certificate distribution

1: Branch office
2: Branch office key pair
3: Root CA certificate
4: Certificate request

5: Device certificate
6: Headquarters
7: Headquarters certificate
8: Internet
9: Headquarters private key

- Generating key pair in the Hirschmann VPN router:
  You have the possibility to generate a key pair in the Hirschmann VPN router. The device later transmits the public part of this key pair together with the request to the SCEP server. The private part of the key pair remains in the SCEP client (Hirschmann VPN router). The fact that the private key never leaves the device at any time represents an increase in security compared to manual certificate distribution, for example via PKCS#12 containers.
- Retrieving CA and RA certificates:
  In order to communicate with RA/CA, the relevant RA and CA certificates are necessary in the Hirschmann VPN router. In a retrieval of the CA certificate via SCEP, the router automatically checks the fingerprint configured in advance as to whether the retrieved certificates actually originate from the desired CA. SCEP itself does not offer a mechanism for automatic authentication of the CA certificates on the SCEP client side. If the administrator of the Hirschmann VPN router has no access to the CA himself, then he can check the fingerprint by telephone with the CA admin, for example.
- Creating and encrypting a request for a device certificate
  The SCEP client gathers the configured information for the request for a system or device certificate. These include the identity of the requesting device (requester), the "challenge phrase" and the passphrase for the automatic processing of the request on the SCEP server. This request bears the signature of the private part of the key pair.
- Transmitting request to the SCEP server:
  The SCEP client subsequently transmits the request together with its public key to the SCEP server.

- Checking the certificate request on the SCEP server and issuance of the device certificate:
  The SCEP server decrypts the received request and then issues a system or device certificate for the requester. SCEP distinguishes the following methods for processing the requests:
  - Ensure the authenticity of the requester in the automatic processing via the challenge phrase. Mscep.dll creates the challenge phrase automatically on a Windows CA server. The CA is valid for one hour. If the challenge phrase in the certificate request coincides with the currently valid value on the server, then the device automatically issues the system certificate.
  - In the manual case, the SCEP server puts the certificate request into a wait state until the acceptance or denial of the CA administrator is certain. During this waiting time, the SCEP client regularly checks whether the SCEP server has issued the required system certificate in the meantime.
  - With RA-AutoApprove the device identifies the client via a certificate validly issued by the CA.
- Retrieving the device certificate from the SCEP server:
  As soon as the certificate is ready, the client determines by regular polling that it is possible to retrieve the certificate.
- Checking device certificate and providing it for VPN operation

7.7.3 Configuration of SCEP

For configuration of SCEP, define global parameters for the SCEP operation and the CAs from which the device retrieves the certificates.

Note: In addition to the configuration of the SCEP parameter, an adjustment of the VPN configurations may be necessary.

Configuration tool	Call
WEBconfig, Telnet	HiLCOS Menu tree > Setup > Certificates > SCEP Client

Global SCEP parameters

- Active:
  Turns the usage of SCEP on or off.
  Possible values: Yes, No
  Default: No
- Repeat-after-error interval:
  The interval in sections for repetitions after any type of error.
  Default: 22
- Check-pending-request interval
  Interval in seconds for checking pending certificate request.
  Default: 101
- Update system certificates before process:
  Lead time in days for timely request of new system certificates (device certificates).
  Default: 2
- Update CA certificates before process:
  Lead time in days for timely retrieval of new RA/CA certificate.
  Default: 1

Actions

- Reinit:
  Starts the manual re-initialization of the SCEP parameters. As in ordinary SCEP initialization, the device retrieves the necessary RA and CA certificates from the CA and stores them in the file system of the Hirschmann VPN router in such a manner that usage in VPN operation is not yet possible.
  - If the available system certificate matches the retrieved CA certificate, the router uses the system certificate, the CA certificate and the private device key for the VPN operation.
  - If the existing system certificates do not match the retrieved CA certificate, a new certificate request to the SCEP server is first required. The router can use the system certificate, the CA certificate and the private device key for VPN operation only if the device has issued and retrieved a new system certificate matching the CA certificate.
- Updating:
  Manually starts the request for a new system certificate independently of the remaining period of validity. The device generates a new key pair.
- Cleaning SCEP file system:
  Starts the cleaning of the SCEP file system.
  - Deleted: RA certificates, pending certificate requests, new and inactive CA certificates, new and inactive private keys.
  - Retained: system certificates currently used in the VPN operation, private keys for them and the CA certificates currently used in the VPN operation.

Configuration of the CAs

- Name:
  configuration name of the CA
- URL
  URL of the CA.
- DN:
  Distinguished Name of the device. Firstly, CAs are associated with system certificates (and conversely) via this parameter. Secondly, this parameter also plays a part in assessing whether received or existing certificates correspond to the configuration.

- Enc-Alg:
  The device encrypts the payload of the certificate request with this algorithm.
  Possible values: DES, 3-DES, Blowfish
  Default: DES
- Identifier:
  CA identifier. Some Web servers require this to assign the CA.
- RA-Autoapprove:
  Some CAs offer the possibility of using a certificate already issued by this CA as verification of the authenticity for subsequent requests. You determine with this option whether the device signs new requests with the existing system certificate if a system certificate already exists.
  Possible values: Yes, No
  Default: No
- CA signature algorithm
  The router signs the certificate request with this algorithm.
  Possible values: MD5, SHA1
  Default: MD5
- CA fingerprint algorithm:
  Algorithm for signing the fingerprint. Determines whether the device undertakes a check of the CA certificates based on the fingerprint, and with what algorithm. It is necessary that the CA fingerprint agrees with the checksum that results when the algorithm is used.
  Possible values: Off, MD5, SHA1
  Default: Off
- CA fingerprint:
  Based on the checksum (fingerprint) registered here, you check the authenticity of the obtained CA certificate (according to the set CA fingerprint algorithm).
- Usage:
  Indicates the purpose of use of the registered CA. The device retrieves the CA registered here solely for the corresponding purpose of use.
  Possible values: VPN, WLAN controller, general
  Special values: General If a general CA is present, an additional one cannot be configured, because otherwise the choice of the CA is unclear.

Configuration of the system certificates

- Name:
  Configuration name of the certificate
- CADN:
  Distinguished Name of the CA. Firstly, CAs are associated with system certificates (and conversely) via this parameter. Secondly, this parameter also plays a part in assessing whether received or existing certificates correspond to the configuration.

  The SCEP client can also use these internal HiLCOS variables:

  – %% inserts a percent sign.

  – %f inserts the version and the date of the firmware currently active in the device.

  – %r inserts the hardware release of the device.

  – %v inserts the version of the loader currently active in the device.

  – %m inserts the MAC address of the device.

  – %s inserts the serial number of the device.

  – %n inserts the name of the device.

  – %l inserts the location of the device.

  – %d inserts the type of the device.
- Subject:
  Distinguished Name of the subject of the requester.
- ChallengePwd:
  Passphrase for the automatic issuance of the device certificates on the SCEP server.
- SubjectAltName:
  Further information on the requester, e.g., domain or IP address.
- KeyUsage:
  Arbitrary, comma-delimited combination of:
  - digitalSignature
  - nonRepudiation
  - keyEncipherment
  - dataEncipherment
  - keyAgreement
  - keyCertSign
  - cRLSign
  - encipherOnly

- decipherOnly
- critical (possible, but not a recommendation)

- extended Key Usage:
  Arbitrary, comma-delimited combination of:
  - critical
  - serverAuth
  - clientAuth
  - codeSigning
  - emailProtection
  - timeStamping
  - msCodeInd
  - msCodeCom
  - msCTLSign
  - msSGC
  - msEFS
  - nsSGC
  - 1.3.6.1.5.5.7.3.18 for WLAN controller
  - 1.3.6.1.5.5.7.3.19 for access points in managed mode
- System certificate key length.
  Length of the key that the device generates for itself.
  Possible values: 31 or greater
- Usage:
  Indicates the purpose of use of the registered certificates. The device retrieves the certificates registered here solely for the corresponding purpose of use.
  Possible values: VPN, WLAN controller

7.8 Extended Authentication Protocol (XAUTH)

7.8.1 Introduction

When remote terminals dial in via WAN connections (e.g., via PPP) RADIUS servers are often used to authenticate the users. Over time the more secure (encrypted) and inexpensive VPN connections displaced the previously customary WAN connections. Setting up VPN connections via IPSec with IKE, however, does not allow one-directional authentication of users via RADIUS or the like.
The Extended Authentication Protocol (XAUTH) offers the possibility of expanding the authentication in negotiating IPSec connections with an additional level. This is used for authenticating the user data. For this purpose, the device carries out an additional authentication with XAUTH username and XAUTH password, protected by the previously negotiated encryption, between the first and second IKE negotiation phase. This authentication uses a RADIUS server and thus allows continued use of RADIUS databases in the migration to VPN connections for dial-in clients. The authentication alternatively uses an internal user table in the device.

Note: In order to design the use of XAUTH to be particularly secure, use dial-in via RSA-SIG (certificates) in place of the pre-shared key method (PSK) if possible. Ensure that the VPN gateway accesses only the certificate of the respective correct remote terminal and not all certificates issued by the same CA.

7.8.2 XAUTH in HiLCOS

In the Hirschmann router, the XAUTH protocol uses the entries in the PPP table to authenticate the remote terminal. The use of entries in the PPP table is dependent on the direction of the connection setup, i.e., the XAUTH operating mode:

XAUTH operating mode	Server	Client
XAUTH user name	Remote terminal from the PPP table Here the device uses the entry from the PPP table in which the PPP remote terminal corresponds to the transmitted XAUTH username. The PPP remote terminal is also required to correspond to the VPN remote terminal in use.	Username from the PPP table Here the device selects the entry from the PPP table in which the PPP remote terminal corresponds to the VPN remote terminal in use.
XAUTH passphrase	Passphrase from the PPP table	Passphrase from the PPP table

7.8.3 Configuration of XAUTH

Use the XAUTH protocol separately for each VPN remote terminal Only define the XAUTH operating mode.

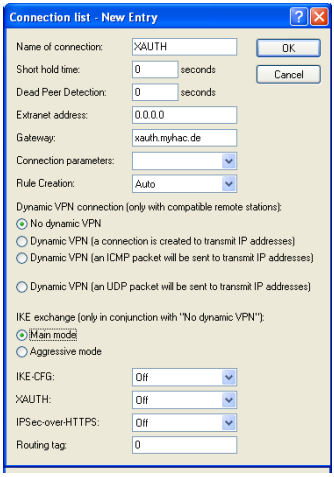


Figure 107:New entry in the connection list

LANconfig: VPN > General > Connection List

WEBconfig: Setup > VPN > VPN Remote Terminal

- XAUTH:
  Activates the use of XAUTH for the selected VPN remote terminal.
- Possible values:
  - Client: In the operating mode as XAUTH client, the device starts the first phase of the IKE negotiation (main mode or aggressive mode) and then waits for the authentication request from the XAUTH server. The XAUTH client responds to this request with the username and the passphrase from the entry of the PPP table in which the PPP remote terminal corresponds to the VPN remote terminal defined here. It is therefore necessary that there is a PPP remote terminal with the same name as the VPN remote terminal. The username defined in the PPP table typically deviates from the remote terminal name.
  - Server: In the operating mode as a server, the device starts the authentication, after the negotiation of the first IKE has been successful, with a request to the XAUTH client, which then responds with its username and passphrase. The server searches for the transmitted username in the remote terminal names of the PPP table and, if there is a match, checks the passphrase. The username for this entry in the PPP table is not used here.
  - Off: The devices not perform an XAUTH authentication for the connection to this remote terminal.
- Default:
  Off

Note: Set the IKE-CFG option to the same value if you activate the XAUTH authentication for a VPN remote terminal.

7.9 How does VPN operate?

In practice, it is necessary for the VPN to meet a number of demands:
- ☐ Unauthorized third parties are forbidden from reading the data (encryption)
- ☐ Exclusion of data manipulation (data integrity)
- ☐ Indubitable determination of the sender of data (authenticity)
- ☐ Easy handling of keys
- ☐ Compatibility with VPN devices from different manufacturers

VPN achieves these five important goals by using the widely disseminated IPSec standard.

7.9.1 IPSec – the basis for VPN

The original IP protocol does not contain any kind of security precautions. A further complication is that the sender has no possibility for transmitting packets directly to the recipient. Instead, all computers connected to the entire network segment receive these packets. Anyone who wishes to do so can read the packets. That makes abuse of data possible.
Therefore researchers further developed the IP protocol. There is now a secure version: IPsec. VPN is based on IPSec
IPSec stands for "IP Security Protocol" and is originally the name of a working group inside the IETF interest Association, the Internet Engineering Task Force. Over the years, this working group developed a framework for a secure IP protocol, which is now known under the name IPSec.
The important point is that IPSec itself is not a protocol but only the standard for a protocol framework. IPSec consists in fact of a wide variety of protocols and algorithms for encryption, authentication and key management. The following section introduces the standards.

Security in IP clothing

IPSec is implemented (almost) completely inside layer III of the OSI model, i.e. in the network layer. In IP networks, the traffic of data packets based on the IP protocol takes place in layer 3.

Thus IPSec replaces the IP protocol. The internal structure of packets under IPSec is different than for IP packets. At the same time, their external structure remains completely compatible with IP. The transport of IPSec packets inside existing IP networks is therefore largely problem-free. The devices in the network responsible for the transport of the packets have no possibility of distinguishing IPSec packets from IP packets by looking at their exterior.

Certain firewalls and proxy servers that also access the contents of the packets are exceptions. The problems result from (partially functionally-induced) incompatibilities of these devices with the prevailing IP standard. For these devices, an appropriate adaptation to IPSec is necessary.

The next generation of the IP standard (IPv6) has implemented IPSec. Therefore the assumption has been that IPSec will continue to be the most important standard for virtual private networks in the future as well.

7.9.2 Alternatives to IPSec

IPSec is an open standard. It is independent of individual manufacturers, and the IETF developed IPSec with the inclusion of the interested public. The IETF is open to everyone and does not have any economic interests. The wide recognition of IPSec results from the open design for combining a variety of technical approaches.

There nevertheless were and are different approaches for implementing VPNs. Only the two most important ones will be mentioned here. In contrast to IPSec, which operates on the network layer, they act on the connection and application layer.

Security on the connection layer – PPTP, L2F, L2TPthe

The possibility of forming tunnels already exists on the connection layer (layer 2 of the OSI model). Microsoft and Ascend developed the Point-to-Point Tunneling Protocol (PPTP) early on. Cisco introduced a similar protocol with Layer 2 Forwarding (L2F). Both manufacturers agreed on a common procedure and the Layer 2 Tunnel Protocol (L2TP) resulted from it in the IETF.

The advantage of these protocols versus IPSec is primarily that there is a possibility of constructing any desired network protocol on such a secure network connection, in particular NetBEUI and IPX.

An essential disadvantage of the above described protocols is the lack of security on the packet level. Moreover, these particles were specifically developed for dial-in connections.

Security on a higher level – SSL, S/MIME, PGP

Communication can be secured by encryption on higher layers of the OSI model as well. Well-known examples for protocols of this type are SSL (Secure Socket Layer), primarily for Web browser connections, S/MIME (Secure Multipurpose Internet Mail Extensions) for e-mail and PGP (Pretty Good Privacy) for e-mail and files.

In all these protocols an application takes over the encryption of the transmitted data, for example, the web browser on one side and the HTTP server on the other.

One disadvantage of these protocols is a limitation to certain applications. Additionally, different keys are generally needed for different applications. You therefore manage the configuration on each individual computer. A convenient configuration only at the gateways, as with IPSec, is impossible. To be sure, security protocols on the application layer are more intelligent; after all they know the meaning of the transmitted data. But they are generally also markedly more complex

All these layer 2 protocols allow only end-to-end connections and are therefore (without extensions) unsuitable for coupling entire networks. On the other hand, these mechanisms do not require any changes to the network devices or the access software. They also have the capability, differently from protocols and other network layers, of being effective even if the data contents have already reached the computer.

Combination is possible

All the above mentioned alternatives are compatible with IPSec and therefore also applicable in parallel. In this manner there is the possibility of increasing the security level. Thus there is the possibility of dialing into the Internet with an L2TP connection, constructing an IPSec tunnel to a Web server and also exchanging the HTTP data between the Web server and the browser in the secure SSL mode.

However, each additional encryption impairs the data rate. The user will decide in the individual case whether security over IPSec alone is sufficient. In rare cases, a higher security will in fact be necessary. Particularly since the degree of security to be used can still be adjusted inside IPSec.

7.10 The standards behind IPSec

IPSec Is based on different protocols for different subfunctions. The protocols build on and supplement one another. The modularity achieved by this concept is an important advantage of IPSec over other standards. Since IPSec is not restricted to certain protocols, supplementation with future developments is possible at any time. The protocols so far integrated also offer such a high degree of flexibility that there is a possibility of adapting IPSec perfectly to almost any need.

7.10.1 Modules of IPSec and their tasks

IPSec has a number of tasks to perform. One or more protocols are defined for each of these tasks.

- ☐ Securing the authenticity of the packets
- ☐ Encryption of the packets
- ☐ Transmission and management of the keys

7.10.2 Security Associations – numbered tunnels

A logical connection (tunnel) between two IPSec devices is called an SA (Security Association). The IPSec device manages these SAs independently. An SA consists of 3 values:

- ☐ Security parameter Index (SPI)
  Code number for distinguishing us several logical connections to the same target device with the same protocols.
- ☐ IP target address
- ☐ Security protocol used
  characterizes the security protocol used for the connection: AH or ESP (more on these protocols in the following sections)

Characterizes the security protocol used for the connection: AH or ESP (more on these protocols in the following sections)
An SA applies solely to one communication direction of the connection (simplex). For a full-fledged transmission and reception connection, two SAs are required. An SA also only applies to one protocol in use. If AH and ESP are used, then 2 separate SAs are likewise necessary, i.e., 2 for each communication direction.
The SAs are managed in the IPSec device in an internal database, in which the extended connection parameters are also present. These parameters include, for example, the algorithms and keys that are used.

7.10.3 Encryption of the packets – the ESP protocol

The ESP (Encapsulating Security Payload) protocol encrypts the packets for protection from unauthorized access. The protocol now has additional possibilities for protecting integrity and determining authenticity. ESP also now has effective protection against packet replay. ESP thus offers all the functions of AH.

Mode of operation of ESP

The structure of ESB is more complicated than that of AH. ESP likewise adds a header behind the IP header, but also a trailer of its own and a block with ESP authentication data.

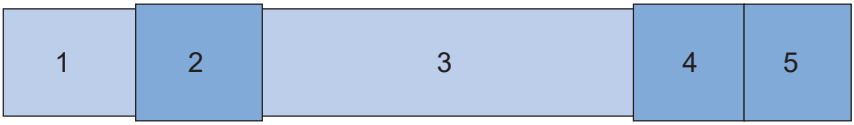


Figure 108:ESP packet

1: IP header
2: ESP header
3: Data
4: ESP trailer
5: ESP auth. data

Transport and tunnel mode

ESP (like AH as well) offers 2 modes Transport mode and tunnel mode. In transport mode, the IP header of the original packet remains identical and the ESP header, the encrypted data and the two trailers are inserted. The IP header contains the constant IP address. Transport mode is therefore suitable only for usage between 2 endpoints, e.g., for remote configuration of a router. If you want to connect networks via the Internet, then transport mode is unsuitable. Here you need a new IP header with the public IP address of the opposite party. In these cases, ESP is used in tunnel mode.

Tunnel mode encrypts the entire packet, including the original IP header, at the tunnel entry, authenticates it and provides it with an ESP header and trailers. This new packet contains a new prefixed IP header, this time with the public IP address of the recipient at the end of the tunnel.

Encryption algorithms

As a higher-level protocol, IPSec does not presume any specific encryption algorithms. The manufacturers of IPSec products are free to choose the methods applied. The following standards are typical:

- ☐ AES – Advanced Encryption Standard.
  AES Is the official encryption standard for use in United States government agencies, and therefore the most important encryption technique globally. Following a global competition between numerous encryption logarithms, the National Institute of Standards and Technology (NIST) chose the Rijndael algorithm (pronunciation: "Rine doll") and declared it the AES in 2001.
  The Rijndael algorithm is asymmetrical encryption method that operates with variable block and key lengths. Two Belgian cryptographers, Joan Daemen and Vincent Rijmen, developed this method, which is distinguished by high security, high flexibility and outstanding efficiency.
- ☐ DES – Data Encryption Standard
  IBM developed DES in the early 1970s for the NSA (National Security Agency). For many years it was the global encryption standard. The key length of this symmetrical method is 56 bits. Because of its short key length, this method is considered insecure today and thus NIST replaced it in 2000 with AES (Rijndael algorithm). Continuing to use it is discouraged.
- ☐ Triple-DES (also called 3-DES)
  Is a refinement of DES. This standard applies the conventional DES algorithm three times in succession. Two different keys with 56 bits each are used, with the key of the first pass being used again in the third pass. This results in a nominal key length of 168 bits and an effective key length of 112 bits.
  Triple DES combines the clever technique of DES with a sufficiently long key and is therefore considered very secure. Triple DES operates more slowly than other methods, however.
- ☐ Blowfish
  This development of the prominent cryptographer Bruce Schneier encrypts symmetrically. Blowfish achieves an outstanding data throughput and is considered very secure.
- ☐ CAST (named for its authors, Carlisle Adams and Stafford Tavares)
  Is a symmetrical method with a key length of 128 bits CAST allows a variable change of parts of the algorithm during runtime.

Note: You have the possibility of adjusting the encryption under LANconfig. Interventions of this type are usually necessary only if you are setting up VPN connections between devices of different manufacturers. By default, Hirschmann gateways offer encryption either according to AES (128 bits), Blowfish (128 bits) or Triple DES (168 bits).

7.10.4 Authentication – the AH protocol

The AH (Authentication Header) protocol guarantees the integrity and authenticity of the data. We will consider integrity as a separate problem below that the AH protocol solves (not a component of authenticity). In addition to integrity and authenticity, AH also offers effective protection against third-party resending of received packets (replay protection).
AH adds its own header to IP packets directly after the original IP header. The most important component of this AH header is a field with authentication data, also referred to as an integrity check value (ICV).

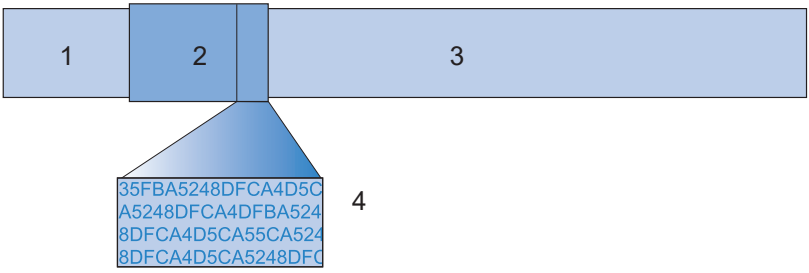


Figure 109:AH header with authentication data
1: IP header
2: AH header
3: Data
4: Authentication data, ICV

The process sequence of AH in the transmitter

The creation of the authentication data in the packet transmitter runs in 3 steps.

- ☐ A checksum is calculated from the total packet by means of hash algorithms.
- ☐ A hash algorithm calculates a new checksum from this checksum, together with a key known to the transmitter and receiver.
- ☐ This results in the sought-for authentication data, which is in the AH header.

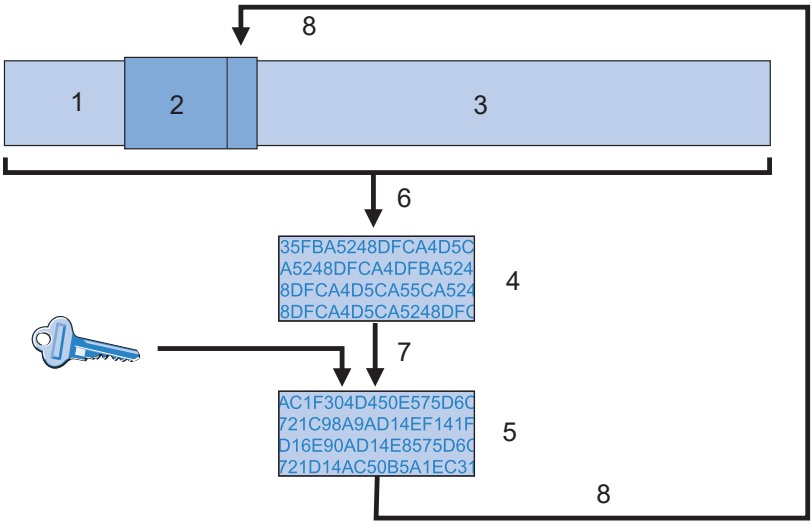


Figure 110:Creation of the authentication data in 3 steps

1: IP header
2: AH header
3: Data
4: Check sum (hash code)
5: Authentication data, ICV
6: Checksum of the entire packet by means of hash algorithm
7: New checksum from old checksum and key
8: Authentication data for AH header

Checking integrity and authenticity in the receiver

The AH protocol runs very similarly in the receiver. The receiver also first calculates the authentication data for the received packet with its key. The comparison to the transmitted ICV of the packet indicates whether the integrity and authenticity of the packet have been preserved.

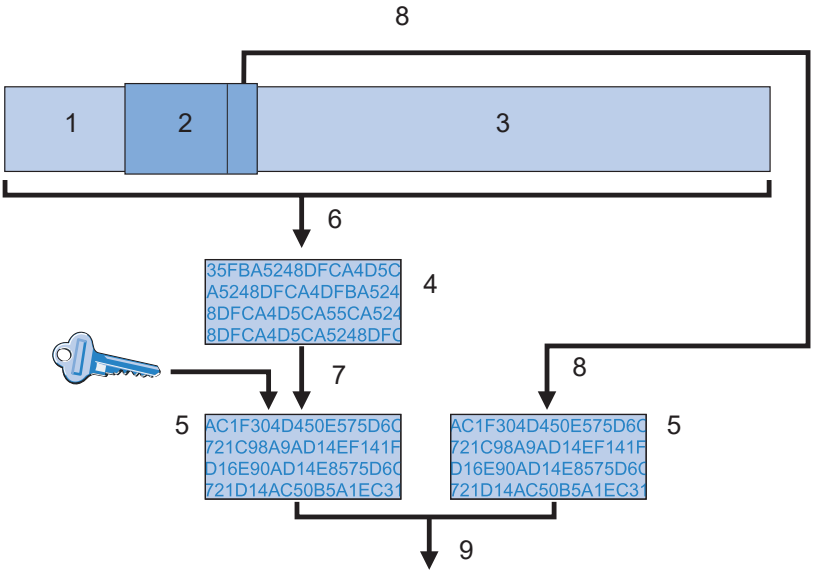


Figure 111:Checking integrity and authenticity in the receiver

1: IP header
2: AH header
3: Data
4: Checksum (hash code)
5: Authentication data, ICV
6: Checksum of the entire packet by means of hash algorithm
7: New checksum from old checksum and key
8: Authentication data of the AH header
9: Check for equality

Forming the checksum for the integrity check

In order to guarantee the integrity, i.e., the correctness of the transferred packets, AH furnishes each packet with a checksum when it is transmitted. In the receiver, AH checks whether the checksum matches the content of the packet. If it does not match, then there was either a transmission error or someone deliberately changed the data. AH immediately rejects such packets so that they do not reach any higher protocol level.

Various so-called hash algorithms are available for calculating the checksum. Hash algorithms are distinguished by the fact that the results (the hash code) are characteristic of the input data ("fingerprint"). Conversely, it is impossible to infer the input data from the hash code. With a high-quality hash algorithm, even the slightest changes of the input value result in a completely different hash code. This makes systematic analyses of several hash codes difficult.

VPN supports the two most common hash algorithms: MD5 and SHA-1. Both methods operate without keys, i.e., solely on the basis of fixed algorithms. Keys come into play only in a later step of AH: in the final calculation of the authentication data. The integrity checksum is only a necessary interim result on the way to the calculation.

Calculation of the authentication data

In this second step, AH forms a new hash code, the final authentication data, from the checksum and a key. For this process as well, there are different standards that can be selected under IPSec. VPN supports HMAC (Hash-based Message Authentication Code). The hash functions MD5 and SHA-1 are available as hash algorithms. The HMAC versions are accordingly called HMAC-MD5-96 and HMAC-SHA-1-96.

It now becomes clear that AH itself leaves the packet unencrypted. Only the checksum of the packet and one's own key are encrypted together into the ICV, the authentication data and added to the packet as the check criterion.

Replay protection – protection from repeated packets

In addition to the labeling with the ICV, AH marks each package with an unambiguous sequence number. Thereby the receiver has the possibility to recognize those packets that a third party has received and is now sending again. This type of attack is called "packet replay."

Note: Masking of IPSec tunnels is not possible with AH unless additional measures such as NAT traversal or an external layer 2 tunneling (e.g., PPPT/LPT2) again provide a "changeable" external IP header.

7.10.5 Management of the keys – IKE

The Internet Key Exchange Protocol (IKE) is a protocol with which there is the possibility of incorporating subprotocols for constructing SAs and for key management.
VPN uses 2 subprotocols inside of IKE: Oakley for the authentication of the partners and the key exchange, as well as ISAKMP for managing the SAs.

Construction of the SA with ISAKMP/Oakley

Every construction of an SA takes place in several steps. For dynamic Internet connections, these steps take place after the transmission of the public IP address. The steps are:

- ☐ The initiator sends a message via ISAKMP to the remote terminal in clear text with the request to set up an SA and proposals for the security parameters of this SA.
- ☐ The remote terminal accepts this proposal.
- ☐ Both devices now generate number pairs (consisting of a public and a private numerical value) for the Diffie-Hellman method.
- ☐ The two devices exchange their public numerical values for Diffie-Hellman in 2 additional messages.
- ☐ From transmitted numerical material (according to the Diffie-Hellman method) and the shared secret, the two sides generate a common secret key with which they encrypt further communication. The two sides additional mutually authenticate themselves using hash codes of their shared secret. The so-called phase 1 of the SA construction is thus ended.
- ☐ Phase 2 is based on the encrypted and authenticated connection that was set up by the devices in phase 1. In phase 2 they generate and transmit the session keys for the authentication and symmetric encryption of the actual data transfer.

Note: Use symmetric methods for encrypting the actual data transfer. Asymmetric methods (also known as public-key encryption) are more secure, since the devices do not transmit any secret keys, but require expensive calculations and are therefore markedly slower than symmetric methods. In practice, public-key encryption is usually used on only for exchanging key material. The actual data encryption then takes place with fast symmetric methods.

The regular exchange of new keys

ISAKMP ensures during the existence of the SA that the devices exchange new key material with one another on a regular basis. This process takes place automatically. You have the possibility of controlling this process via the setting for "lifetime" in the extended configuration of LANconfig.

7.11 Improved phase 1 rekeying

During a VPN connection, the participating stations continually check whether the communication is always performed according to a previously agreed security association (SA). If the framework conditions change (e.g. change of IP address of client due to change of location to different radio cell), you set up this security association again by what is known as “rekeying”.
From version 2.30 on, the Hirschmann Advanced VPN Client transmits a special identification number (ID) during the phase 1 rekeying. Using this ID, a Hirschmann VPN gateway detects the rekeying and connects the previously negotiated security association with the logged in client. Therefore, the re-authentication, usually compulsory, is not required.

7.12 Intelligent Precalculation of DH Keys

The negotiation of a VPN connection is based on the creation of keys according to the Diffie-Hellman method. Depending on the key length, however, calculating a DH key can take some time. If a VPN gateway temporarily loses its Internet connection, the recalculation of all the DH keys may incur a delay before all of the VPN clients can reconnect to the VPN gateway.

With the precalculation of DH keys, the device can accelerate the renegotiation of VPN connections. The precalculation and the number of keys to be generated are set up in WEBconfig:

`HiLCOS Menu Tree:Setup:VPN:Isakmp:Groups`

The precalculation of keys has a low priority. When the CPU of the device is not busy with other, higher priority tasks, it builds up a stock of public DH keys.

7.13 MPPE encryption for PPTP tunnel

The MPPE encryption protocol (Microsoft Point-To-Point Encryption) secures the data transmission via PPP and VPN connections with key lengths of up to 128 bits.
For the encryption, MPPE uses what is known as the “Stateless Mode” to ensure the synchronization of the two communication partners. In this mode, the session key changes with every transmitted data packet. Additionally, each time the two stations synchronize their encryption tables, in which the keys for the data encryption are stored.
VPN-capable Hirschmann devices use MPPE as a means of encrypting the data transmission via PPTP tunnels.
In LANconfig, you will find this setting under `Communication:Protocols:PPTP List`.
If you have activated the MPPE encryption protocol, the device only sets up connections with clients under the following conditions:

- The client wants to set up an MPPE-secured connection. With other protocols, the router rejects a connection.
- The client uses a minimum of the key length specified in the router. If the key length is smaller, the router rejects a connection, and if the encryption is stronger, the router switches to the corresponding key length.

7.13.1 Enhancements in the menu system

Encryption
Here you enter the key length.

- **SNMP ID:**
  2.2.21.7
- **Telnet path:**
  `Setup:WAN:PPTP Remote Devices`

- **Possible values:**
  Off
  40 bit
  56 bit
  128 bit
- **Default:**
  Off

8 Security

Security is an important topic in the configuration of an OpenBAT device.

8.1 A WLAN Security Overview

8.1.1 Basic Considerations

The following elements should be considered when developing a security plan for your wireless network:

- **Authentication**

  Authentication is used to grant network access to authorized network users.

  Authentication can be implemented, for example, using certificates or passwords.

- **Authenticity**

  Authenticity encompasses the proof of authorship and originality of data content. Authentication is the process of establishing this proof.

- **Integrity**

  After access has been granted, data packets need to reach the target without any falsification.

- **Confidentiality**

  Confidentiality involves shielding data traffic from unauthorized third parties. This is achieved by encrypting the data.

8.1.2 IEEE 802.11i /WPA2

The IEEE standard 802.11i—WiFi Protected Access 2 (WPA2)— provides a heightened standard of security for WLANs. WPA2 enables IEEE 802.1X authentication and authorization of users. It also supports AES encryption, which is a far more secure technique than WEP or WPA.

8.1.3 TKIP and WPA

The original WPA standard specifies TKIP/Michael as an encryption method. With the further development of the 802.11i standard, the AES/CCM method was added. In a WPA network it is possible for some clients to communicate with the access point using TKIP, while other clients use AES.

8.1.4 WEP

WEP offers far lower security than IEEE 802.1x/WPA2. OpenBAT devices continue to support this encryption method in order to be compatible with older client devices that exclusively support the WEP protocol. However, Hirschmann expressly recommends use of a better method for securing the WLAN (e.g., IEEE 802.1X/ WPA2).

8.1.5 LEPS: Hirschmann Enhanced Passphrase Security

LEPS increases global passphrase security

WPA and IEEE 802.11i encryption provide WLAN data traffic with greater security against eavesdropping than the older WEP method.

LEPS provides an efficient method that makes use of the simple configuration of IEEE 802.11i. LEPS uses an additional column in the access control list (ACL) to assign an individual passphrase to each MAC address. The connection to the access point and the subsequent encryption with IEEE 802.11i or WPA is achieved by using the correct combination of passphrase and MAC address.

Configuring LEPS

To configure a WLAN client for LEPS, do the following:

- ☐ Enable MAC filtering for the access point:
  - ☐ In the `Configuration : Wireless LAN : General` dialog click 'Logical WLAN settings...' and select a wireless network.
  - ☐ In the `Logical WLAN settings : Network` dialog, select 'MAC filter enabled'.
- ☐ Add a unique passphrase to each client station:
  - ☐ In the `Configuration : Wireless LAN : Stations` dialog, click 'Stations...'.
  - ☐ In the `Stations` window, select a station and click 'Edit...'
  - ☐ In the `Stations : Edit Entry` dialog, enter a unique 'Passphrase' for the client station.

8.1.6 Background WLAN Scanning

A OpenBAT device in the role of access point actively scans the available wireless channels (just as a WLAN client does when searching for an available access point). If the OpenBAT device detects another active access point, that device's relevant information is recorded in the scan table. Because this scan/record process occurs in the background during the normal radio activity of the access point, it is called a background scan.

Background scanning is primarily used to detect:

- rogue access points
- fast roaming clients

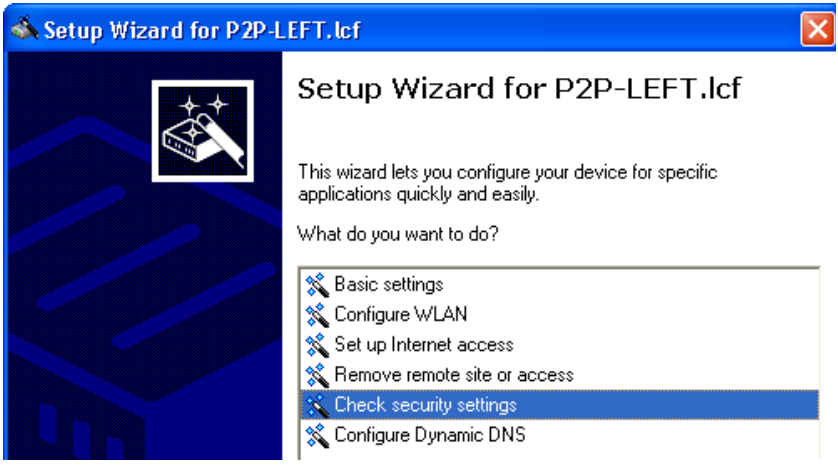
Evaluating the Background Scan

Use LANmonitor to view the results of background scanning. You can use the tools within LANmonitor to group detected access points, and provide e-mail notification whenever a new WLAN access point or client is detected.

8.2 Securing the Configuration

Many parameters for the security of your network and the authorizations for individual network users are established in the configuration of the device. These parameter settings should not be changed by unauthorized persons. These security-related settings can be configured individually, or by means of the 'Check security settings' wizard.

8.2.1 Using the Check Security Settings Wizard



Use the ’Check Security Settings’ wizard to step through the process of securing your OpenBAT device configuration, including:

- Passwords (see on page 727)
- Login barring (see on page 729)
- Selection and configuration of an encryption method:
  - WPA, or
  - WEP
- SSID assignment
- Controlling access to the configuration settings from (see on page 730):
  - remote networks
  - the wireless network (WLAN)
  - the local area network (LAN)
- Controlling access to the configuration settings by IP address (see on page 732)
- Activating the following firewall features:
  - stateful inspection firewall
  - ping blocking
  - stealth mode

Many of these settings can also be set by the ’Basic settings’ and ’Configure WLAN’ wizards. These settings can be independently configured in the LANconfig or the WEBconfig software.

8.2.2 Passwords

The simplest way to help secure the configuration is to assign a password.

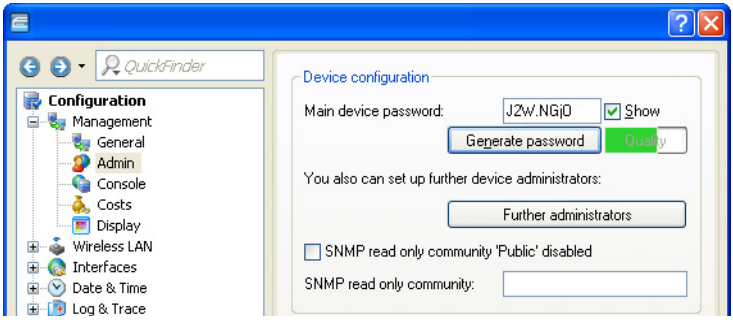
Note: If a password has not been set:

- Anyone can access and change the configuration of the device.
- The LED flashes at regular intervals until the device has been configured correctly.

Note: The combination of user and password can also be used for both Telnet and HyperTerminal access.

Configuring the Password

The 'Main device password' can be set in the 'Device configuration' section of the `Configuration : Management : Admin` dialog. The default password setting is 'private'.



Requiring a Password for SNMP Read Access

When you set the password, you should also select the 'Password required for SNMP read permission' setting in the same dialog.

Password protection for WLAN keys

As of HiLCOS 8.90 the system no longer displays WPA and WEP group keys in plain text on the console, but masked (********). As a result, it is no longer possible to read these keys via SNMP, for example.

8.2.3 Login Barring

The OpenBAT device can be configured to frustrate brute force attacks. A brute-force attack is the attempt by an unauthorized person or device to decipher a password and gain access to a network. A brute force attack involves multiple login attempts, using all possible combinations of letters and numbers until the right password is found. To guard against brute force attacks, configure the following settings in the "Configuration Login Lock" section of the `Configuration :, Management : Admin`:

- ☐ Lock configuration after: Type in the number of login attempts that will lock the device configuration.
- ☐ Lock configuration for: Type in the duration of the device configuration lockdown, in minutes.

Note: If barring is activated on any one port, all other ports are also barred.

8.2.4 Restricting Configuration Access Rights

Access to the internal functions of the devices can be restricted separately for each access source, as follows:

- local area network (LAN)
- wireless LAN (WLAN)
- remote networks

For network-based configuration access, further restrictions can be made—for example, specified IP addresses or dedicated LANcapi clients are exclusively allowed access.

The following internal functions are separately selectable:

- LANconfig
- WEBconfig
- SNMP
- Terminal/Telnet

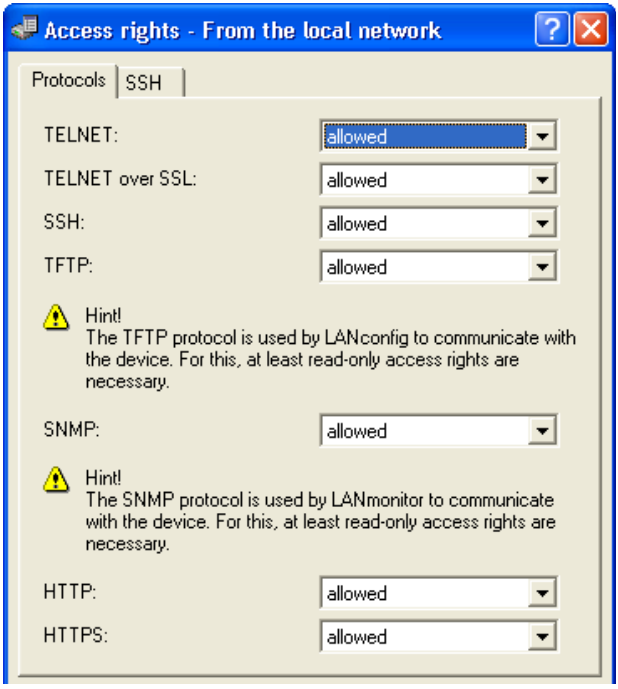
Limiting Configuration Access by Access Source

Access to internal device functions can be controlled based on the access source—LAN, WLAN or remote networks—for individual configuration services. Configuration access can be allowed, denied, or read-only. To configure these access rights:

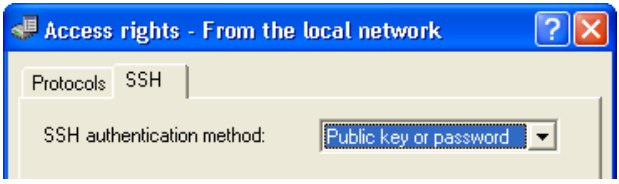
☐ Open the `Configuration : Management : Admin` dialog.

☐ In the 'Configuration access ways' section, click 'Access rights' and then also select an access source:
- from the local network
- from the wireless LAN
- from remote networks

☐ In the 'Access rights' dialog, click on the Protocols tab to display that dialog (below):



- ☐ Use this dialog to grant or deny access rights from the selected access source.
- ☐ Click on the SSH tab to display a dialog where you can select an authentication method for secure shell (SSH) transmissions:



Limiting Configuration Access by IP Address

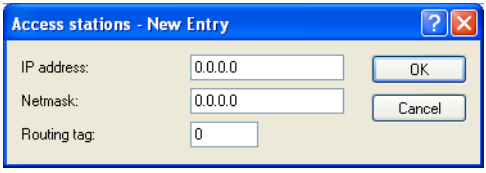
Access to the configuration can also be controlled by creating an IP address filter list. Stations with an IP address included in this list exclusively can access the configuration. To create a station filtering list:

☐ Navigate to the following dialog:`Configuration : Management`. Click the 'Access stations' button.

☐ In the ’Access stations’ window, click ’Add...’.

☐ In the ’Access stations - New Entry’ dialog, enter the following information for each station:
- IP address
- Netmask
- Routing tag

Note: If you specify a routing tag for this access station, it will accept exclusively those packets that were marked with the same tag in the firewall or which arrived via a network with a suitable interface tag. If the routing tag is 0, any access with a suitable IP address is allowed. The use of routing tags is advisable when combined with the corresponding accessory rules in the firewall or tagged network interfaces.



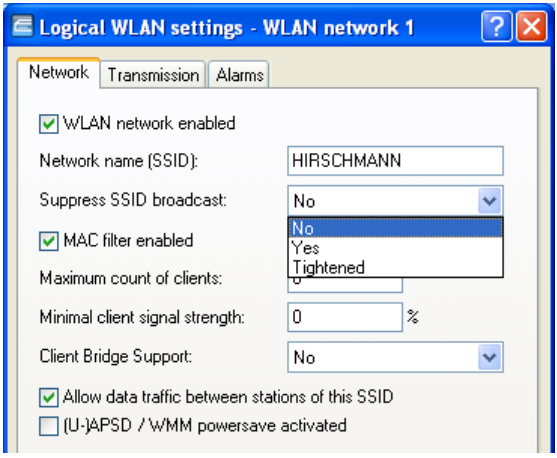
By default, this table does not contain entries. Thus the device can be accessed over TCP/IP from computers with any IP addresses. With the first entry of an IP address (as well as the associated net mask) the filter is activated, and solely the IP addresses contained in this entry are entitled to use the internal functions then. With further entries, the number of the entitled ones can be extended. The filter entries can designate both individual computers and whole networks.

8.2.5 Closed-network Function: Suppress SSID broadcast

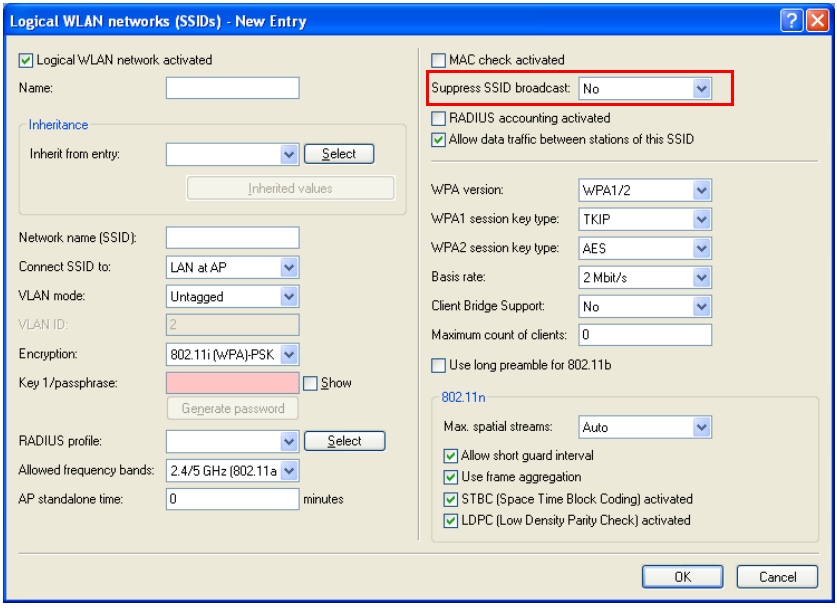
A WLAN client can only connect to a wireless network if it is informed of the corresponding SSID. The state on delivery for many wireless networks allow the use of a blank SSID or the SSID "any", and continuing to use this means that potential intruders do not need to know the SSID of the wireless LAN. The closed network function prevents unauthorized WLAN clients from logging into the WLAN. The access point rejects any attempt to log on with a blank SSID or the SSID "any". Any user wanting to logon to the WLAN must know the correct SSID.

Note: Simply suppressing the SSID broadcast does not provide adequate protection: When legitimate WLAN clients associate with the access point, this transmits the SSID in plain text so that it is briefly visible to all clients in the WLAN network.

LANconfig: `Wireless LAN:General:Interfaces:Logical WLAN settings:Network`.



LANconfig: `WLAN Controller:Profiles:Logical WLAN networks (SSIDs)`



The option "Suppress SSID broadcast" provides the following settings:

- **No**: The access point publishes the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device responds with the SSID of the radio cell (publicly visible WLAN).
- **Yes**: The access point does not publish the SSID of the cell. When a client sends a probe request with an empty SSID, the device similarly responds with an empty SSID. The client cannot log on to the radio cell.
- **Tightened:** The access point does not publish the SSID of the cell. When a client sends a probe request with a blank or incorrect SSID, the device does not respond. The client cannot log on to the radio cell. This setting also reduces the network load if there is a large number of WLAN clients in the radio cell.

8.2.6 Post-Initial-Password Security Hardening

Immediately after the administrator sets a device password, HiLCOS automatically enforces a stricter security posture to mitigate clear-text and unauthenticated attack vectors. For details, see here.

8.3 Automatic generation of device-specific SSH keys

Ex-factory, all HiLCOS-based devices with an HiLCOS version earlier than 8.90 are equipped with a default set of cryptographic keys that are represented by the following fingerprints:

```
ssh-dss 27:c5:1d:9f:be:27:3d:50:d7:bf:c1:68:0b:18:97:d7
ssh-rsa 03:56:e6:52:ee:d2:da:f0:73:b5:df:3d:09:08:54:b7
```

If you have a device with HiLCOS 8.90 or later and you have not uploaded an individual key to the device, the internal SSH server will try to compile its own device-specific SSH keys after a configuration reset followed directly by a system restart. These include

- an SSH-2 RSA key of 2048-bit length and
- an SSH-2 DSS key of 1024-bit length (as defined in FIPS 186-2),

which the device stores as "ssh_rsakey" and "ssh_dsakey" in its internal file system.

If key generation is successful, the entry "SSH: ... host key generated" is entered as a "note" in the SYSLOG; if it fails, an entry "SSH: host key generation failed, try later again with '...'" is made as an "alarm". If key generation fails (e.g. insufficient entropy), the device falls back to its factory cryptographic key.

Note: If you perform an update from an older version of HiLCOS to 8.90 or higher without a subsequent configuration reset, the device does not generate a device-specific SSH key. This is to maintain compatibility with existing installations. However, you can manually initiate the key generation. Enter the following commands in the console:

```
sshkeygen -t rsa -b 2048 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
```

8.4 Suppress security confirmations during SSH key generation

As of HiLCOS 8.90, you have the option of suppressing any security prompts during the SSH key generation with HiLCOS:

```
sshkeygen [-?|-h] [-t (dsa|rsa)] [-b <bits>] -f <OutputFile> [-q]
```

- **-q**
  This parameter enables the 'quiet' mode for the key generation. If you set this parameter, HiLCOS overwrites any existing RSA or DSA keys without asking for confirmation, and there is no output about the progress of the operation. You can use this parameter in a script, for example, to suppress security confirmations by the user.

9 Virtual LANs

9.1 What is a Virtual LAN?

The increasing availability of inexpensive layer 2 switches makes it possible to design LANs that are much larger than in the past. Until now, smaller parts of a network were connected using hubs. These individual segments—collision domains—had been connected via routers to the wider network. Because a router constitutes the border between two LANs, several LANs with their own IP address ranges arose using this design.

By using switches, you can combine many more stations to one large LAN. By confining the flow data to individual switch ports, the available bandwidth can be utilized more efficiently than with hubs; the need to configure and maintain routers within the network is avoided.

However, a network structure based on switches also presents certain disadvantages:

- Broadcasts are sent over the entire LAN, even if the broadcast data packets relate to just a small segment of the LAN. The increased number of network stations transmitting broadcasts leads to a reduction of available LAN bandwidth.
- All data traffic on the physical LAN is public. Even if individual segments are using different IP address ranges, each station on the LAN is theoretically able to tap into data traffic from all logical networks on the Ethernet segment. The need to secure individual LAN segments using firewalls or routers increases the amount of network administration.

One approach to this situation is the use of virtual LANs (VLANs), as described in IEEE 802.1p/q. Several VLANs can be configured for a single physical LAN. No VLAN obstructs another VLAN, and no VLAN receives or taps into the data traffic of another VLAN on the physical Ethernet segment.

9.2 Configuring VLANs

Adding a OpenBAT device to a VLAN involves the following configuration tasks:

- Defining the VLAN by assigning it a name, giving it a VLAN ID, and identifying the interfaces over which the VLAN operates.
- Defining for each VLAN interface how to handle data packets with and without VLAN tags.

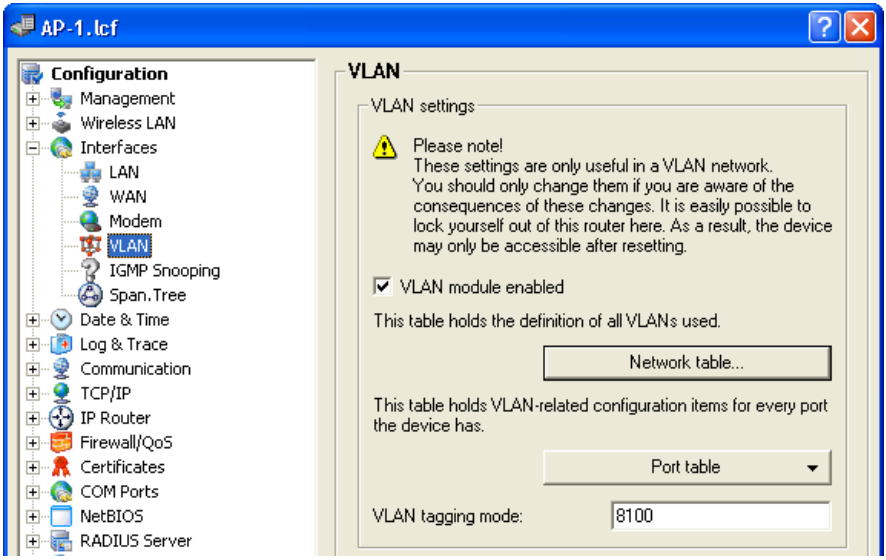
9.2.1 VLAN and ARF

In some cases it is sufficient to configure VLAN settings on the basis of the IP network, using a technique called advanced routing and forwarding (ARF). Using ARF, a VLAN ID is defined for an IP network. All outbound packets from this network are tagged with this VLAN ID. Incoming packets need to be tagged with this VLAN ID in order to be assigned to the network. Details are contained in section on ARF "Advanced Routing and Forwarding." Please observe the information there (see on page 780).

9.2.2 General VLAN Settings

To enter general VLAN settings, follow these steps:

☐ Navigate to the following dialog:`Configuration : Interfaces`. Open the `VLAN` dialog:



☐ Configure the following VLAN settings:

Note: These settings should be edited only by persons with expert level understanding of VLAN operation. Mistaken editing of these VLAN settings can result in the inability to access the OpenBAT device. In such a case, you need to reset the device to regain access.

- VLAN module enabled:
  Select this to activate VLAN support for the OpenBAT device.
- VLAN tagging mode:
  Enter a 16 bit hexadecimal value for the VLAN tag (Ethernet II type). The default value is 8100 (representing 802.1p/q VLAN tagging). Other values for VLAN tagging include 9100 and 9901.

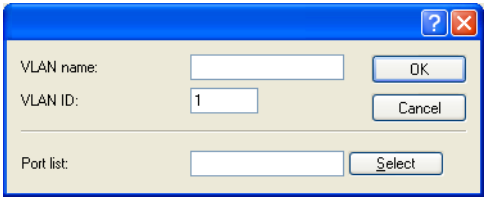
Note: When operating VLAN tagged networks over provider networks that use additional VLANs themselves, providers often use special VLAN tagging IDs, which are entered here as the ‘VLAN tagging mode’.

9.2.3 The Network Table

Use the Network table to define VLANs for the OpenBAT device as follows

☐ Open the `Configuration : Interfaces : VLAN` dialog and click ‘Network table...’

☐ In the ‘Network table’, click ‘Add...” to open the ‘New Entry’ dialog:



☐ Configure the following settings for each VLAN:

- VLAN name:
  The VLAN name serves as a description during configuration. This name is not used in any other place.
- VLAN ID:
  An integer, from 1 to 4094, that serves as a unique identifier for the VLAN.
- Port list:
  Enter every OpenBAT device interface that belongs to this VLAN.

  For a device with a LAN interface and a WLAN port, this setting might contain the entry ‘LAN-1, WLAN-1’.

  To add a port range, enter the beginning and ending port separated by a tilde: ‘P2P-1~P2P-4’.

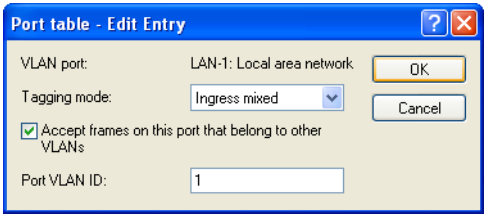
Note: The first SSID of the first WLAN module is named WLAN-1, the other SSIDs are WLAN-1-2 up to WLAN-1-8. If the device has two WLAN modules the SSIDs are WLAN-2, WLAN-2-2 up to WLAN-2-8.

9.2.4 The Port Table

Use the port table to configure each port that is used by the VLAN, as follows:

☐ Navigate to the following dialog:`Configuration : Interfaces: VLAN` dialog:

☐ Click ‘Port table’, then select a port from the list to open the following dialog for that port:



☐ Configure the following settings for each VLAN port:

- Tagging mode:
  Specify how VLAN tags will be assigned and processed over this port. Selections include:

  Never: Outbound packets are not given a VLAN tag at this port. Incoming packets are treated as though they have no VLAN tag. If incoming packets have a VLAN tag, it is ignored and treated as though it were part of the packet's payload. Incoming packets are assigned to the VLAN defined for this port.

  Ingress mixed: Incoming packets may or may not have a tag, but outgoing packets do not obtain a tag. This mode is mainly required for configuration conversion (see below).

  Mixed: Allows mixed operation of packets with and without VLAN tags at the port. Packets without a VLAN tag are assigned to the VLAN defined for this port. Outgoing packets are given a VLAN tag unless they belong to the VLAN defined for this port.

  Always: Outgoing packets obtain a tag, regardless of whether they belong to the port VLAN or not. Incoming packets need to contain a tag—untagged packets are discarded.
- Accept frames on this port that belong to other VLANs:
  This option defines whether tagged data packets with any VLAN ID should be accepted, even if the port is not a ‘member’ of the VLAN.
- Port VLAN ID:
  This setting has two functions:

  Untagged packets received at this port in 'Mixed' or 'Ingress-mixed' mode are assigned to this VLAN, as are all ingress packets received in 'Never' mode.

In the 'Mixed' mode, this value determines whether outgoing packets receive a VLAN tag or not: Packets assigned to the VLAN defined for this port are not given a VLAN tag; all others are given a VLAN tag.

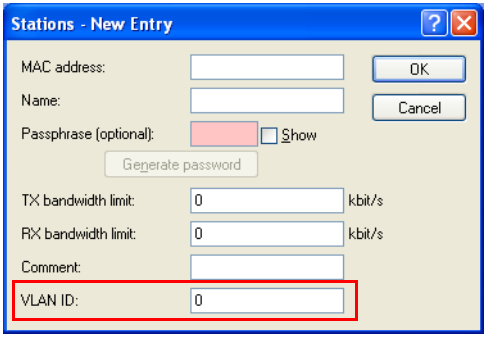
9.3 Configuring VLAN IDs

9.3.1 Assigning Different VLAN IDs to WLAN Clients

VLANs are usually connected to a LAN interface on the OpenBAT device. Therefore, all packets that pass through this interface receive the same VLAN ID when the VLAN module is enabled. However, in some cases, you may want to assign individual WLAN stations to different VLANs. To assign an individual WLAN client station to a specific VLAN:

☐ Navigate to the following dialog:`Configuration : Wireless LAN`. Open the `Stations` dialog and click ‘Stations’.

☐ In the ‘Stations’ dialog, select a station and click ‘Edit’:

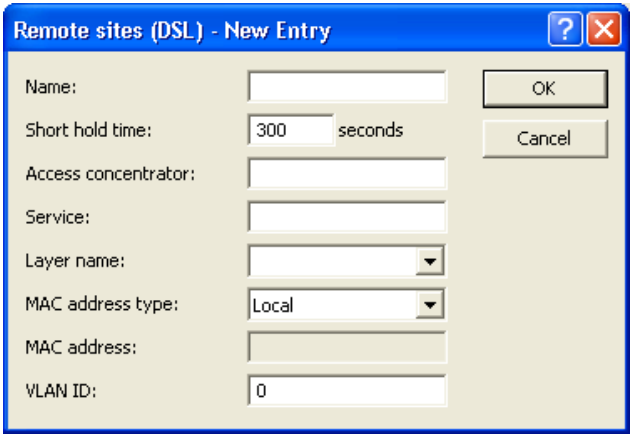


☐ In the ’VLAN ID’ field, enter the identifier that applies to this station.

9.3.2 Special VLAN ID for DSL Interfaces

In order to better separate the data traffic on a DLS interface from other traffic, 'VLAN ID' can be set up independently for a DSL interface in the LANconfig software as follows:

- ☐ Open `Configuration : Communication : Remote Sites` and click ‘Remote sites (DSL)...’
- ☐ In the ‘Remote sites (DSL)’ window, click ‘Add...
- ☐ In the ‘Remote sites (DSL) - New Entry’ dialog, in the ‘VLAN ID’ field, enter the specific ID of the VLAN so that it can be uniquely identified over the DSL connection.



9.4 VLAN Tagging on Ethernet Layers 2 and 3

9.4.1 Introduction

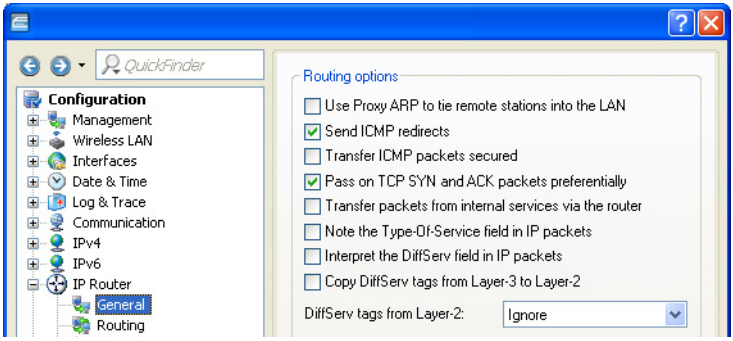
VLANs operate on the Data Link Layer (layer 2) of the OSI model. However, you can configure the OpenBAT device to transfer VLAN tags to the DSCP fields (Differentiated Services Code Point - DiffServ) and/or the priority setting in the TOS field (Type of Service), both of which operate on the Network Layer (layer 3). The processing of VLAN tagged packets requires that packets in the receive direction are regarded differently from packets in the send direction.

Note: When a tagged packet is received, the tag is saved to the associated entry in the connection list. If a packet is to be sent with a priority setting, the VLAN ID recorded earlier is entered into the packet together with the priority to form a VLAN tag. Where a connection causes other connections to be opened—e.g. with ftp or H.323—the tag is inherited by the new entries.

9.4.2 Configuration of VLAN tagging on layer 2/3

Configuration of the transfer of VLAN tags between layer 2 and layer 3 elements of the IP data packet is accomplished by entering routing settings as follows:

☐ Navigate to the following dialog:`Configuration : IP-Router:` Open the `General` dialog.



☐ Specify how TOS/DiffServ tags will be routed:

– Select "Note the Type-Of-Service field in IP packets" to enable ToS checking. The OpenBAT device checks the bits for particularly fast or secured transmission.

– Select "Interpret the DiffServ field in IP packets" to enable DiffServ checking. The OpenBAT device checks the bits for Class Selector, Assured Forwarding, and Expedited Forwarding settings.

– De-select both of these settings (the default setting), and the device will not transfer VLAN tags between layers 2 and 3.

Note: De-selecting both of these fields will also disable QoS for the device.

☐ Use the ‘Copy DiffServ tags from Layer-3 to Layer-2’ settings to regulate device behavior when it transmits a data packet. If this option is selected, VLAN tags with priority bits originating from the DSCP precedence will be generated if the recipient has previously sent at least one tagged packet.

☐ Use the ‘DiffServ tags from Layer-2’ setting to regulate device behavior when it receives a data packet:

- Ignore: Turns off layer-2 to layer-3 VLAN tag transfer.
- Copy to Layer-3: Priority bits in the VLAN tag are copied to the precedence of the DSCP.
- Copy automatically: Priority bits in the VLAN tag are copied exclusively to the DSCP precedence if this is '000'.

10 LLDP

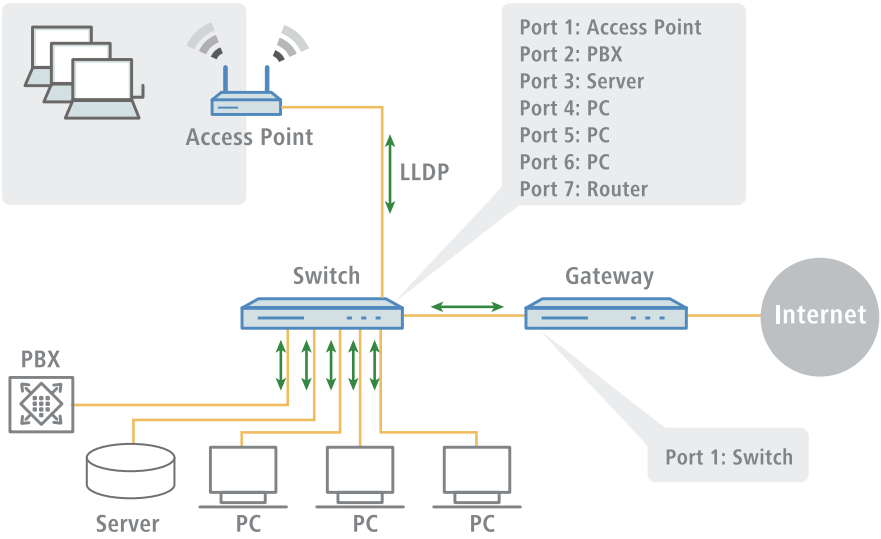
The Link Layer Discovery Protocol (LLDP) provides a simple and reliable way to exchange information between neighboring devices on the network and for determining the topology of networks. LLDP provides discovery functions to identify individual devices and entire network structures using the procedures defined in the IEEE 802.1AB standard. Since the protocol works on Layer 2 (security level) of the OSI layer model and it is, therefore, used for physically addressing devices, its functionality is not limited to logical networks such as IP networks. In principle, LLDP covers all physically accessible devices on the network.

In particular, the vendor-independent LLDP protocol offers many advantages in complex networks:

- It enables the automatic detection of components attached to a network such as routers, switches, and WLAN access points.
- It simplifies the integration of a wide range of different devices, which support the LLDP standard, into an existing network: Using central network management software, and automatic testing and diagnostic processes, the time required for setup, operation and maintenance of a network is reduced.
- The information sent by the individual devices provides an overview of the topology (i.e., structure and arrangement) of the entire network. Central management software provides the administrator with a virtual image of the network, which is automatically updated when there are changes in the topology.
- With the help of management software, the administrator can also easily monitor and manage complex networks. Using this software, he can determine which components and devices are interconnected and can easily locate any faults.
- LLDP can reduce the costs of buying, building or restructuring a network, since companies are no longer dependent on specific manufacturers because of this open standard. Individual network components can be selected based on which one is best for your implementation. This was previously not possible when proprietary protocols were in use.

10.1 How it works

LLDP works on a simple principle: The so-called LLDP agent runs on all devices with LLDP support. On the one hand, this software component sends information to all interfaces of the device at regular intervals. This is done using either Unicast or Multicast, depending on the destination addresses, which you can configure as required. On the other hand, the LLDP agent is continuously receiving information from neighboring devices. The transmission and reception of the respective data packets is handled independently from each other.



The data packets being sent and received contain information such as the name and the description of the device, the ID and description of ports, the IP address or MAC address of the device, the specific capabilities of the device (e.g., in terms of switching and routing), VLAN identifiers and vendor-specific details. In this case, LLDP defines basic information that a data packet must always include, as well as optional additional information.

The individual devices store the information received locally in a data structure, the so-called MIB (Management Information Base). An MIB therefore contains data from its own LLDP agent and of the detected, direct neighbor agent.

The information exchange provides a continuing identification of the devices within the network, because the devices normally send packets cyclically (i.e. in configurable intervals). Furthermore, the devices also inform their network neighbors when changes occur on the device or in its network connection.

For the actual device identification process it is crucial that each connection point in the topology is clearly identified as a "Media Service Access Point" (MSAP). An MSAP is composed of a device ID (Chassis ID) and a port identification (Port ID). The unique identification or assignment of devices is therefore based on the fact that each MSAP in the monitored network topology may occur only once.

The Administrator can query and capture the data reported by the devices via a central network management software on his computer, where the query of the individual MIBs is performed using the SNMP protocol. The management software thus documents the entire topology of the network and allows automatic display of this topology along with a graphic representation of the current diagnostic data.

10.2 Structure of LLDP Messages

Information is exchanged using specific units of data known as LLDP Data Units (LLDPDU). These data unit consists of TLVs (Type-Length-Values), and each TLV field corresponds to a certain type and has a certain length.

In accordance with the LLDP standard IEEE 802.1AB three TLVs are mandatory at the beginning of an LLDPU in the following order:

- Type 1 = Chassis ID
- Type 2 = Chassis ID
- Type 3 = Time to live

Following these mandatory TLVs, an LLDPDU can include additional, optional TLVs:

- Type 4 = Port description
- Type 5 = System name
- Type 6 = System description
- Type 7 = System capabilities
- Type 8 = Management address

At the end of an LLDPDU the following TLV is mandatory:

- Type 0 = End of LLDPDU

Table 8: Tabular overview of the TLVs

TLV	Usage	Name	Example	Function
Type 1	Required	Chassis ID	0018.2fa6.b28c	Identifies the device
Type 2	Required	Port ID	Fi-0/12	Identifies the port
Type 3	Required	Time to live	60 sec	Signals to the receiving device how long the received information should remain valid
Type 4	Optional	Port description	GigabitEthernet0/12	Displays details about the port such as the hardware version
Type 5	Optional	System Name	PN-I/O 3	Displays the name given to the device by the administrator

Table 8: Tabular overview of the TLVs

TLV	Usage	Name	Example	Function
Type 6	Optional	System description	HiLCOS software, version 8.9.1 SE	Displays details about the device such as the version of the networking software
Type 7	Optional	System capabilities	Router	Displays the primary function and capabilities of the device.
Type 8	Optional	Management address	192.168.0.1	Shows the IP or MAC address of the device
Type 0	Required	End of LLDPDU	----------	Signals the end of the data unit

10.3 Supported Operating Systems

In principle, LLDP works on all popular systems, provided that LLDP agents or an appropriate software for evaluation of the LLDP packets is available. For Linux there are various open source projects, such as "LLDPD", "Open-LLDP" (with hyphen) or "ladvd", which deploy an LLDP agent.

The project "OpenLLDP" aims to achieve a further dissemination and acceptance of the LLDP protocol (802.1AB). The software supports the transmission and reception of LLDP messages on the Linux, Mac OS X, FreeBSD, and NetBSD platforms. Currently, however, this development seems to be stalled.

Microsoft Windows Vista and Windows 7 contain a proprietary protocol called LLTD (Link Layer Topology Discovery), which is essentially the same functionality as LLDP. On Windows XP, the LLTD component can be installed later as a patch. However, the patch is limited compared to the features implemented in Vista and Windows 7 because the "LLTD Responder" only reports IPv4 addresses, and not IPv6 addresses.

If you want to install LLDP on Windows systems, you can use a shareware called "haneWIN LLDP Agent". Using this, LLDP works on all Windows systems as of Windows 2000, i.e., on both 32-bit and 64-bit systems.

The most widely used free software for evaluation and analysis is Wireshark. The basic version of Wireshark is free of charge and now well-established as a standard. The software supports a wide variety of operating systems and can read and evaluate a wide variety of protocols (including LLDP). However, the focus of the basic version of Wireshark is the analysis of problems within the network. If you need more features (such as the visualization of network traffic in the form of colored graphs), you can purchase add-on modules.

10.4 Configuration

LLDP configuration via WEBconfig. For further information, see the CLI reference material.

HiLCOS menu tree : Setup : LLDP

11 Routing and WAN Connections

This chapter describes WAN protocols, and shows you how to configure and optimize WAN connections.

11.1 General aspects of WAN connections

WAN connections are used for the following applications:

- Internet access
- LAN to LAN coupling
- Remote access

11.1.1 Bridges for Standard Protocols

WAN connections differ from direct connections in that the data in the WAN are transmitted via standardized network protocols also used in the LAN. Direct connections, on the other hand, operate with proprietary processes that have been specially developed for point-to-point connections.

WAN connections extend a LAN. WAN connections form a kind of bridge for the communication between networks (or for connecting individual computers to the LAN). By contrast, a direct connection establishes just a single connection from one individual PC to another PC.

WAN Connection Protocols

WAN connections over high speed ports (e.g. DSL connections) use the IP standard for transmitting packets.

WAN Connections and the Router

WAN connections characteristically interact with the router modules in the OpenBAT device. The router modules (IP and IPX) provide the connection to LAN and WAN. They use the WAN connections to respond to requests for external resources, made by PCs within the LAN.

11.2 IP Routing

An IP router operates between networks that use TCP/IP as the network protocol. This allows data transmissions exclusively to destination addresses that are entered in the routing table. This section explains the structure of the IP routing table in a router, as well as the additional functions available to support IP routing.

11.2.1 The Routing Table

The IP routing table informs the router to which remote station (other router or computer) the router should send the data for a particular IP address or an IP address range. This type of entry is known as a ‘route’ because it is used to describe the path of the data packet.

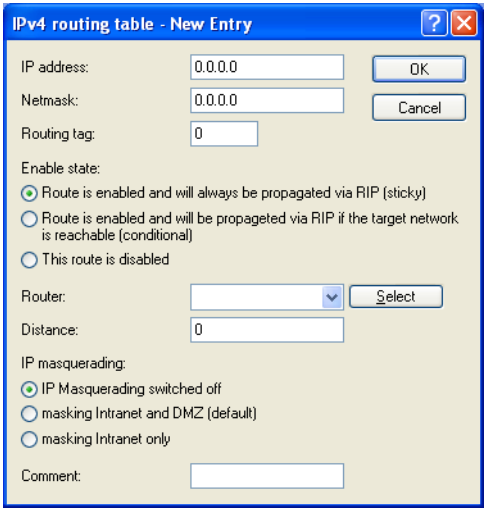
In ‘static routing’, you manually make these entries; they remain unchanged until you either change or delete them yourself. In ‘dynamic routing’, the routers discover existing routes by exchanging data between themselves, then continuously and automatically update this information. The IP router uses the static and the dynamic routing table when the IP Routing Information Protocol (RIP) is activated.

The IP routing table also determines the length of a route's path, so that the router can select the most suitable route—from among several existing routes—to the destination. The default setting for the distance to another router is 0, indicating that the other router can be reached directly. All devices that can be reached locally—including other routers in the same LAN or workstation computers connected via proxy ARP—are assigned the distance 0. The ‘quality level’ of this route is reduced if the entry addressed has a higher distance (up to 14). ‘Unfavorable’ routes with higher distance values are used if no other route to a particular remote station can be found.

Configuring the Routing Table

To access the routing table for editing:

☐ Navigate to the following dialog:`Configuration : IP Router: Routing`, and click ‘IPv4 routing table...’.



In the Routing table, you can edit an existing entry by selecting it then clicking ‘Edit...’ or create a new entry by clicking ‘Add...’

A routing table entry can include settings for the following parameters:

- IP addresses and Netmask:
  This is the address of the destination network to which data packets may be sent and its associated network mask. The router uses the network mask and the destination IP address of the incoming data packets to check whether the packet belongs to the destination network.

  The route with the IP address '255.255.255.255' and the network mask '0.0.0.0' is the default route. All data packets that cannot be routed by other routing entries are sent over this route.

- Routing tag:
  This permits more precise control of the selection of the target route. The target IP address for the selected route is detected, as well as other information that is joined to the data packets by the firewall. The routing tag ’0’ indicates the routing entry is valid for all packets.

- Enable state:
  Indicates if the route is enabled or disabled, and how the route will be propagated for RIP. For enabled networks, RIP propagation can be either:
  – ‘Sticky’: always propagated
  – ‘Conditional’: propagated exclusively if the target network is reachable
  – ‘Off’: never propagated

- Router:
  The router transmits the appropriate data packets to the IP address and network mask to this remote station.
  – If the remote station is a router in another network or an individual workstation computer, this is the name of the remote station.
  – If the router on the network cannot address the remote station itself, then the IP address of another router which knows the path to the destination network is entered.

  The router name indicates what should happen with the data packets that match the IP address and network mask:
  – Routes with the entry '0.0.0.0' identify exclusion routes. Data packets for this ‘zero route’ are rejected and are not routed any further. That way routes which are inaccessible on the Internet (private address spaces, e.g., '10.0.0.0'), for example, are excluded from transmission.
  – If an IP address is input as router name, this is a locally available router, which is responsible for transfer of the relevant data packets.

- Distance:
  The number of routers between this router and the destination router. This value is often equated with the cost of the transmission and used to distinguish between inexpensive and expensive call paths for wide-area connections. The distance values entered are propagated as follows:
  – All networks which can be reached while a connection exists to a destination network are propagated with a distance of 1.
  – All non-connected networks are propagated with the distance entered in the routing table (but with a minimum distance of 2) as long as a free transmitting channel is still available.

  - The remaining networks are propagated with a distance of 16 (= unreachable) if there are no longer any channels available.
  - Remote stations connected using proxy ARP are an exception to this. These ‘proxy hosts’ are not propagated.

- Masquerading:
  IP masquerading can be used to hide a logical IP network behind a single address – namely, that of the router. For example, if you have Internet access, you can use this functionality to connect your entire network to the Internet. When IP Masquerading is turned on, its scope can extend to:
  - Interfaces (Intranet) and DMZ
  - Intranet only

11.2.2 Policy Based Routing

Policy-based routing uses other criteria along with the destination IP address to define the destination route (meaning the remote device that is to be used to transfer the data). Additional information can be employed—including the service or the protocol used, sender addresses or the destination for the data packets—for selection of the destination route. Policy-based routing can be used to achieve a more finely controlled routing behavior, as in the following application scenarios:

- The LAN's entire Internet traffic is diverted to a proxy without entering the proxy address into the browsers. As the users do not notice the proxy routing, the scenario is named ‘transparent’ proxy:

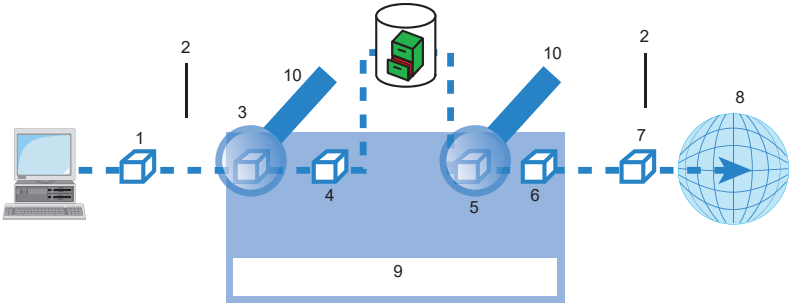


Figure 112:Policy-based routing

1: Data packet with destination address in Internet			
2: Firewall			
3: Source: Local network all port 80			
4: Data packet with destination address and IP routing tag ‘1’			
5: Source: Proxy destination: all port 80			
6: Data packet with destination address and IP			
7: Data packet routed to the Internet			
8: Internet			
9: Table: Extract of IP routing tables:			
IP Address	Net mask	RT tag	Router
255.255.255.255	0.0.0.0	1	Proxy
255.255.255.255	0.0.0.0	0	Internet
10: Firewall rules			

- With load balancing, the data traffic for selected protocols is diverted over a specified DSL port that uses an additional external ADSL modem.
- A server in the local network is supposed to be accessible exclusively from the WAN via a fixed IP address; this is routed via a specified WAN interface.

Appropriate settings can be made causing the firewall to select channels according to information other than just the destination IP address. These entries are supplemented with a special routing tag that is used to control the channel selection with the routing table. For example, a rule can add the routing tag '2' to all data traffic for a local group of computers (defined by an IP address range). Alternatively, data traffic based on specified protocols can be configured to receive a different supplementary routing tag.

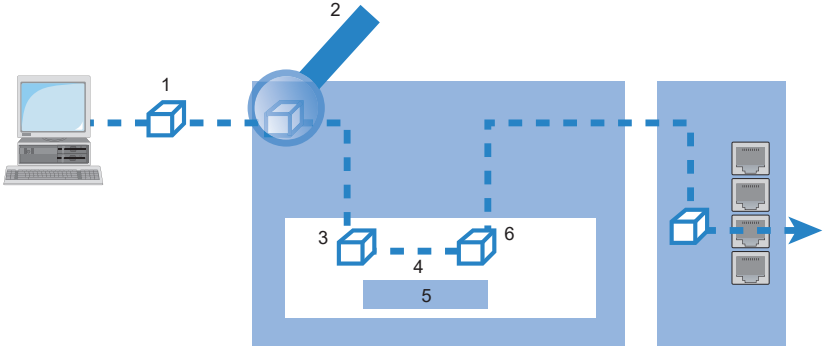


Figure 113:Application of policy-based routing with load balancing

1: Data packet with IP destination address
2: Firewall rules
3: Data packet with IP destination address, IP routing tag
4: IP router
5: Chart:
IP routing table IP address -> Routing tag ->Remote station
6: Data packet with IP destination address, IP routing tag, and DSL port

- When establishing a connection, the firewall initially checks if the packets for transmission fit a rule that applies a routing tag. If so, the routing tag is entered into the data packet.
- The IP routing table combines the routing tag and destination IP address to determine the appropriate remote station. The IP routing table is processed from top down in the usual fashion.
- If an entry is found that corresponds to the remote network, then the router checks the routing tag. The required remote station can be found with the help of the appropriate routing tag.

Note: If the routing tag has a value of ‘0’ (default) then the routing entry applies to all packets.

- Internal services implicitly use the default tag. Using the appropriate firewall rule, you can configure the transfer all services from all source stations to all destination stations with routing tag ‘1’.
- Routing tags and RIP: The routing tag is also transmitted in RIP packets for processing upon reception, so that, for example, the distance setting of the proper route can be changed.

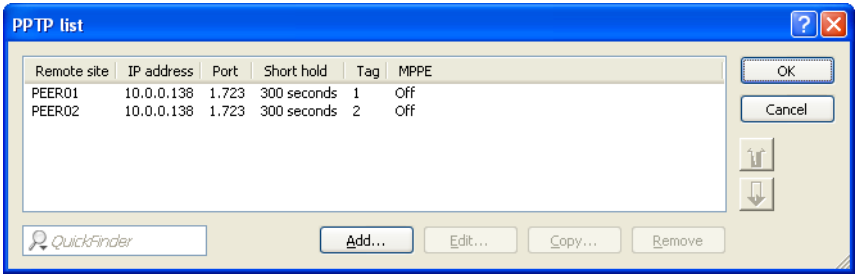
Routing Tags for PPTP Connections

Routing tags are used by the OpenBAT device to evaluate criteria relevant to the selection of the target route, in addition to the IP address. In general, routing tags are added to the data packets using special firewall rules. However, in some cases, it is desirable to assign the tags directly.

In the PPTP table, a routing tag can be entered in addition to the IP address of the PPTP server. Using this routing tag, two or more DSL modems that use a single IP address can be operated on different DSL ports. To configure the PPTP list:

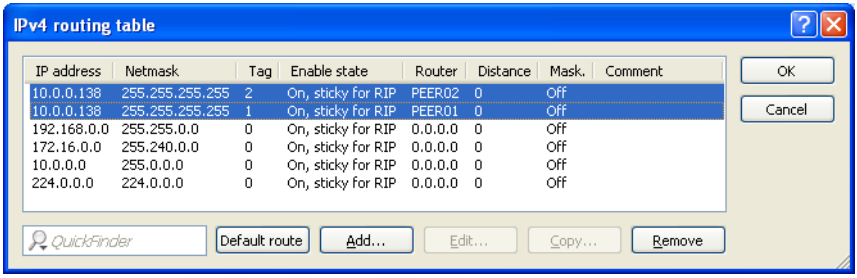
☐ Use the `Configuration : Communication : Protocols` dialog to open the "PPTP list" and click "Add".

☐ Set up the PPT peers as instructed on page 798 „Configuring Remote Stations“. Give each remote terminal its own routing tag.



In the IP routing table, two appropriately tagged routes are required. To access the IP routing table:

☐ In the `Configuration : IP Router : Routing` dialog, click "IPv4 routing table".



11.2.3 Local Routing

When a workstation within a local network attempts to transmit a data packet to an IP address that is outside its own LAN, it searches for a router. Typically, the router is identified in the workstation configuration by means of an entry identifying it as a standard router or standard gateway. It is frequently the case that the workstation can be configured with just a single default router—which is presumed to be able to reach all IP addresses that are unknown to the workstation—even in cases where there are multiple routers on the local network. Sometimes the default router is unable to reach the destination network itself, but does know of another router that can find this destination.

ICMP Redirects

In this case, the designated router sends the computer a response—known as an ICMP redirect—that identifies the address of the router that knows the route to the destination network. The workstation computer then accepts this address and sends the data packet straight to the other router.

However, some workstations cannot handle ICMP redirects. To deliver data packets in this case, use local routing. By means of local routing, the default router sends the data packet directly to other routers. Local routing is enabled by disabling the ICMP redirect function:

☐ Open the `Configuration : IP Router : General` dialog and de-select ‘Send ICMP redirects’.

Note: Local routing should be used sparingly, because it doubles the network load of transmitted data packets. Data is first sent by a workstation to the default router, which then re-sends the data over the same network to a second router that can forward it to the target remote network.

11.2.4 Dynamic Routing with IP RIP

In addition to the static routing table, Hirschmann routers also include a dynamic routing table. Unlike the static table, you do not propagate this yourself, but instead leave this task to the router. The router uses the Routing Information Protocol (RIP) for this purpose. Devices that support RIP use this protocol to exchange information on the available routes.

Information Propagated by IP RIP

A router uses IP RIP to inform other network routers of the routes entered in its own static routing table, except for the following routes:

- Rejected routes with the '0.0.0.0' router setting
- Routes referring to other routers in the local network
- Routes linking individual computers to the LAN by proxy ARP

Although the entries in the static routing table are set manually, both this information—and the transmitted RIP packets based on it—changes according to the connection status of the router:

- If the router has established a connection to a remote station, it propagates all the networks that can be reached via this route in the RIPs with the distance '1'. This informs other routers in the LAN that a connection to the remote station has been established on this router. This means that other routers do not need to establish additional connections, thereby reducing connection costs.
- If this router cannot establish a connection to another remote station, all other routes are propagated with the distance '16' in the RIP. The '16' indicates the route is not currently available.

Information Received in IP RIP Packets

When the router receives IP RIP packets, it incorporates them in its dynamic routing table, which looks something like this:

IP address	IP netmask	Time	Distance	Router
192.168.120.0	255.255.255.0	1	2	192.168.110.1
192.168.130.0	255.255.255.0	5	3	192.168.110.2
192.168.140.0	255.255.255.0	1	5	192.168.110.3

Time-Based Structure of the Dynamic Routing Table

Each route entered in the dynamic routing table includes a value for the following fields:

- IP address and IP netmask:
  Together, these identify the destination network.
- Distance:
  Indicates the number of routers between the transmitter and receiver.
- Router:
  identifies the specific router that has revealed the route.
- Time:
  This parameter acts as a multiplier, and indicates how long the route has been in the table. A newly added route is assigned the value of 1 and is automatically incremented when the corresponding amount of time—about 30 seconds—has elapsed. Thus, a value of 5 indicates the entry has existed for about 2.5 minutes, and so on. After about 3.5 minutes, the Distance value is set to 16 (route not reachable). After about 5.5 minutes, the route is deleted from the table.

When the router receives an IP RIP packet, it needs to decide whether or not to add the contained route to its dynamic table, as follows:

- The route is incorporated if it is not yet listed in the table (as long as there is enough space in the table).
- The route exists in the table with a time of '5' or '6'. The new route is then used if it indicates the same or a better distance.
- The route exists in the table with a time of '7' to '10' and thus has the distance '16'. The new route will be used.
- The route exists in the table. The new route comes from the same router that discovered the route, but has a worse distance than the previous entry. When a device reports the degradation of its own static routing table (e.g. releasing a connection increases the distance from 1 to 2), the router adds the poorer entry to its dynamic table.

Note: RIP packets from the WAN will be ignored and will be rejected immediately. RIP packets from the LAN will be evaluated and will not be propagated in the LAN.

The interaction between static and dynamic tables

The router uses the static and dynamic tables to calculate the actual IP routing table it uses to determine the path for data packets. In doing so, it includes the routes from the dynamic table that it did not itself detect—or which indicate a shorter distance than the same route in its own static table—with the routes from its own static table.

Scaling with IP RIP

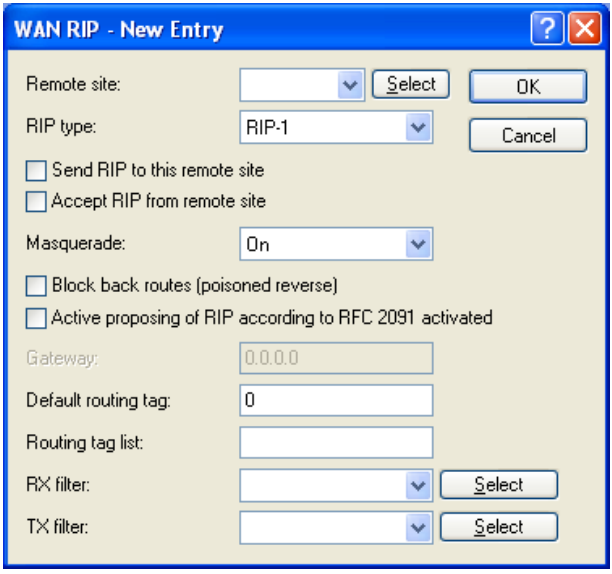
If you use several routers in a local network with IP RIP, you can represent the routers outwardly as a single large router. This procedure is known as ‘scaling’. By constantly exchanging information among the routers, the outwardly projected ‘single router’ theoretically has no limits to the transmission options available to it.

Configuring IP RIP

You can add remote sites to the RIP table, and indicate if the router will send RIP packets to the remote site, or receive RIP packets from the remote site, or both. To configure the RIP table:

☐ Open the `Configuration : IP Router : General` dialog and click ‘WAN RIP...’.

☐ In the ‘WAN RIP’ table, click ‘Add...’ to open the ‘New Entry‘ dialog:



☐ Refer to the topic ‘WAN RIP’ (see on page 864) for a description of this dialog.

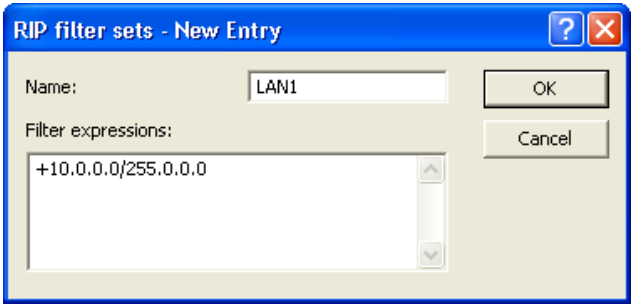
Note: Routers with RIP capabilities dispatch the RIP packets approximately every 30 seconds.The router is set up to send and receive RIPs if it has a unique IP address.The IP RIP module is deselected in the default setting using the IP address xxx.xxx.xxx.254

Configuring the RIP Filter

Routes learned from RIP can be filtered by their routing tag according to the settings for LAN and WAN RIP. Routes can additionally be filtered by specifying network addresses. RIP filters are contained in a central table, and can be applied against entries in the LAN and WAN RIP tables. To create a RIP filter:

☐ Open the `Configuration : IP Router : General` dialog and select ‘RIP filter sets...’.

☐ In the ‘RIP filter sets’ table, click ‘Add...’ to open the New Entry dialog:

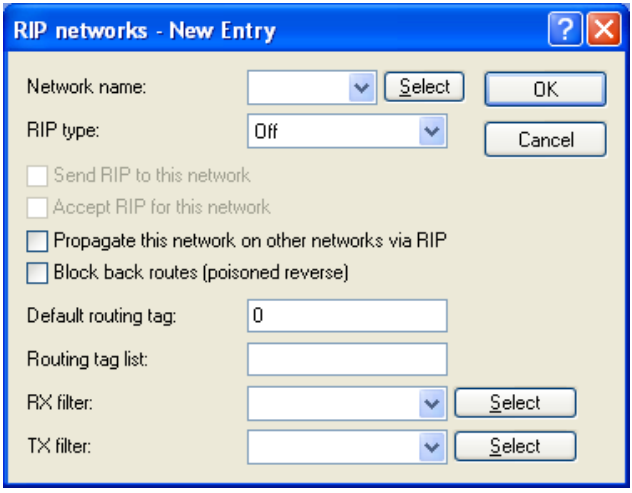


Configure RIP for Separate Networks

It is often not desirable to propagate routing table data equally to all networks. For example, it usually makes little sense to propagate the local route structure via RIP to the DMZ. Similarly, while it may be necessary to propagate the known routes to certain networks, it is not necessary for the router to learn routes from the network (e.g. in the WAN). For these reasons, the router lets you separately configure RIP functionality for every network. To configure RIP for separate networks:

☐ Open the `Configuration : IP Router : General` dialog and select ‘RIP networks...’.

☐ In the ‘RIP networks’ table, click ‘Add...’ to open the New Entry dialog:



Timer Settings

The Routing Information Protocol (RIP) regularly provides neighboring routers with updates on the available networks and the associated metrics (hops). RIP uses various timers to control the exchange of routing information. These timers include the following:

- Update Delay
- Update

They can be viewed and configured in WEBconfig in the Hirschmann Menu Tree at

`Setup : IP Router : RIP : Preferences`

Triggered Update in the LAN

With a triggered update, changes to the metrics are immediately reported to the neighboring router. The system does not wait until the next regular update. An update delay helps prevent imperfect configurations from causing excessive update messages.

- Update delay:
  The delay begins when the routing table, or parts of it, are propagated. While this delay is active, new routing information is accepted and entered into the table, but it is not reported any further. The router actively reports its current entries after expiration of this delay.

  This setting establishes the upper limit for the delay. The actual delay is a random value between one second and this setting.

Triggered Update in the WAN

WAN bandwidth limitations may make regular updates every 30 seconds undesirable. For this reason, RFC 2091 requires that routes are transmitted to the WAN when the connection is established. After this, just updates are transmitted.

Because updates are explicitly requested, broadcasts or multicasts should not be used for delivering RIP messages. Instead, the subsidiary device needs to be statically configured with the IP address of the next available router at the central location. Due to these requests, the central router knows which subsidiary routers it has received update requests from; it sends any messages on route changes directly to the subsidiary device.

To configure a triggered update for a WAN:

- ☐ Navigate to the following dialog:`Configuration : IP Router:General` dialog and click ‘WAN RIP...’.
- ☐ In the ‘WAN RIP’ table, select the WAN and click ‘Edit...’.
- ☐ In the ‘Edit Entry’ dialog, select ‘Active proposing of RIP according to RFC 2091 activated’, then input the target Gateway address.

Poisoned Reverse

Poisoned reverse stops the formation of routing loops. An update is sent back to the router that propagated the route to inform it that the network is unreachable at the associated interface.

This has a significant disadvantage over WAN connections: The central location transmits a high number of routes, which then suffer from route poisoning, leading to a heavy load on the bandwidth. For this reason, poisoned reverse can be manually activated for a LAN/WAN interface.

To enable poison reverse for a LAN:

☐ Open the `Configuration : IP Router : General` dialog and select ‘RIP networks...’.

☐ In the ‘RIP networks’ table, select the network and click ‘Edit...’.

☐ In the ‘Edit Entry’ dialog, select ‘Block back routes (poison reverse)’.

To enable poison reverse for a WAN:

☐ Navigate to the following dialog:`Configuration : IP Router :General` dialog and click ‘WAN RIP...’.

☐ In the ‘WAN RIP’ table, select the WAN and click ‘Edit...’.

☐ In the ‘Edit Entry’ dialog, select ‘Block back routes (poison reverse)’.

Static Routes for Constant Propagation

Routers use RIP to propagate both dynamic routes and statically configured routes as well. Some of these static routes may not be constantly available, for example, when an Internet connection or dial-up access is temporarily unavailable. For a static route, the ‘Active’ setting in the routing table indicates if it should be propagated constantly or exclusively when it is actually reachable. You can edit this setting using WEBconfig in the Hirschmann Menu Tree at:

`Setup : IP-Router : IP-Routing-Table`

11.2.5 SYN/ACK Speedup

SYN/ACK speedup is used to accelerate IP data traffic. The IP check characters (SYN for synchronization and ACK for acknowledge) are given preference within the transmission buffer over simple data packets. Check characters are not delayed in the transmission queue causing the remote station to stop sending data.

The effect of SYN/ACK speedup is most apparent for fast connections (e.g. ADSL) when data quantities are simultaneously transferred in both directions at high speed.

SYN/ACK speedup is enabled by default.

Disabling SYN/ACK Speedup

SYN/ACK speedup changes the order of packet delivery. In some cases, where a protocol assumes a certain packet delivery sequence, this may be undesirable. In this case the SYN/ACK speedup can be deactivated.

To de-activate SYN/ACK speedup:

☐ Open the `Configuration : IP Router : General` dialog and de-select ‘Pass on TCP SYN and ACK packets preferentially’.

11.3 Advanced Routing and Forwarding

11.3.1 Introduction

For some applications, it may be desirable to operate more than one intranet and one DMZ with a OpenBAT device—for example, in order to provide multiple IP networks with Internet access via a central router. OpenBAT devices support up to 64 different IP networks.

Various scenarios are possible when operating multiple IP networks:

- One network per interface
- Multiple networks per interface
- Multiple VLANs per interface; one or more networks per VLAN (a combination of the first two scenarios)

The implementation of these scenarios is facilitated by advanced routing and forwarding (ARF), which provides very flexible options in the definition of IP networks and the assignment of these networks to the interfaces. The diagram below illustrates the network/interface assignment at various levels. The configuration options applied here are described in the following chapters:

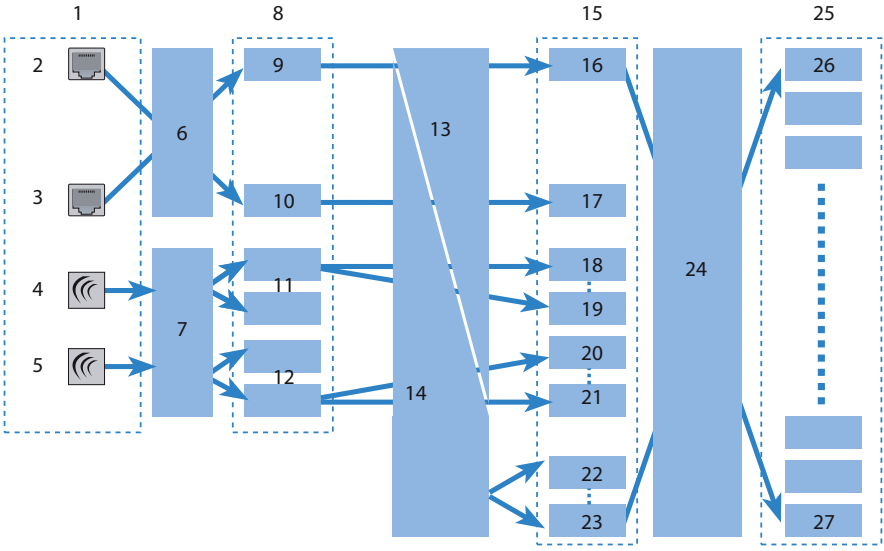


Figure 114:Network/interface assignment at various levels

1: Physical interfaces	8: Logical interfaces	15: Logical interfaces with VLAN tags, bridge groups	24: Advanced Routing and Forwarding
2: ETH - 1	9: LAN - 1	16: LAN-1, VLAN ID 1	25: IP networks
3: ETH - 2	10: LAN - 2	17: LAN-2, VLAN ID 9	26: Network 1
4: WLAN - 1	11: WLAN-1-1 to P2P-1-16	18: WLAN-1-1, VLAN ID 10	27: Network 64
5: WLAN - 2	12: WLAN-2-1 to P2P-2-16	19: P2P-1-6, VLAN ID 18	
6: Ethernet port mapping	13: VLANs	20: WLAN-1-1, VLAN ID 19	
7: Multi-SSID, P2P	14: LAN bridge	21: P2P-1-6, VLAN ID 25	
		22: BRG-1	
		23: BRG-8	

The assignment of IP networks to interfaces proceeds as follows:

- Different models of the OpenBAT devices present varying numbers of physical interfaces—i.e. Ethernet (LAN) ports or WLAN radio modules.
- Each logical interface is assigned to a physical interface:
  - For Ethernet ports, port mapping assigns the physical ETH-1 and ETH-2 ports to the logical LAN-1 and LAN-2 ports.

    For some but not all models, the number of logical LAN interfaces corresponds to the number of physically available Ethernet ports.
  - For WLAN modules, the establishment of point-to-point connections (P2P), or the use of Multi-SSID—or both—can mean that multiple WLAN interfaces are assigned to each physical WLAN module. This can include up to eight WLAN networks and up to sixteen P2P connections for each physical WLAN module.
- These logical interfaces are further specified and grouped in the next stage:
  - For devices supporting VLAN, multiple VLANs can be defined for each logical interface simply by using VLAN-IDs. Although the data traffic for the various VLANs flows via a common logical interface, the VLAN-ID keeps the different VLANs strictly separated. From the perspective of the OpenBAT device, the VLANs are completely separate interfaces. This means that a single logical interface becomes multiple logical interfaces for the OpenBAT device, and each of these interfaces can be addressed individually.
  - For devices with WLAN modules, the individual logical interfaces can be grouped together. This is handled by the LAN bridge which regulates data transfer between the LAN and WLAN interfaces. The formation of bridge groups (BRG) allows multiple logical interfaces to be addresses at once; they appear as a single interface to the OpenBAT device—in effect achieving the opposite of the VLAN method.
- In the final stage, the ARF forms a connection between the logical interfaces with VLAN tags and the bridge groups on the one side, and the IP networks on the other. For this reason, an IP network is configured with a reference to a logical network (with VLAN-ID, if applicable) or to a bridge group. Furthermore, an interface tag can be set for each IP network, by means of which the IP network can be separated from other networks without having to use firewall rules.

The definition of routing tags for IP networks as described above is one of the main advantages of ARF. This option allows "virtual routers" to be implemented. A virtual router takes up only a portion of the routing table by using interface tags for an IP-network, and therefore configures routing individually for that particular IP-network. This method allows, for example, several default routes to be defined in the routing table, each of which is given a routing tag. Virtual routers in the IP networks use the tags to select the default route that applies to the IP network with the appropriate interface tag. The separation of IP networks via virtual routers even permits multiple IP networks with one and the same address range to be operated in parallel in just one OpenBAT device without conflict.

One example: Consider the case of an office building that houses several different companies, which need to be connected to the Internet via a central OpenBAT device, even though each of these companies has its own Internet provider. All of the companies want to use the popular IP network '10.0.0.0' with the netmask '255.255.255.0'. To implement these requirements, each company is given an IP network '10.0.0.0/255.255.255.0' with a unique name and a unique interface tag. In the routing table, a default route with the corresponding routing tag is created for each Internet provider. This allows the clients in the different company networks, all of which use the same IP addresses, to access the Internet via their own provider. Employing VLANs enables logical networks to be separated from one another even though they use the same physical medium (Ethernet).

Routing Tags Versus Interface Tags

Routing tags (assigned by the firewall) and interface tags (defined by the IP networks) have a great deal in common, but also some significant differences:

- The router interprets both tags in the same way. Packets with the interface tag '2' are valid for routes with the routing tag set to '2' in the routing table (and all routes with the default route tag '0'). The same routes apply for packets which the firewall has assigned with the routing tag '2'. Thus the interface tag is used in the same way as a routing tag.
- Interface tags have the additional ability to delimit the visibility (or accessibility) between different networks:
  - In principle, networks that are visible to one another, and thus able to interconnect, are those networks that share the same interface tag.
  - Networks with the interface tag '0' have a special significance; they are in effect supervisor networks. The networks can see all of the other networks and can connect to them. Networks with an interface tag not equal to '0' cannot make connections to supervisor networks.
  - Networks of the DMZ type can be seen by all other networks independently of their interface tag—which makes sense, because the DMZ often contains servers that are open to the public, like web servers etc. The DMZ-networks exclusively see networks with the same interface tag (and of course all other DMZ-networks).
  - Networks of the DMZ type with the interface tag '0' have a special significance: As ‘supervisor networks’ they can see all other networks, and they are also visible to all other networks.

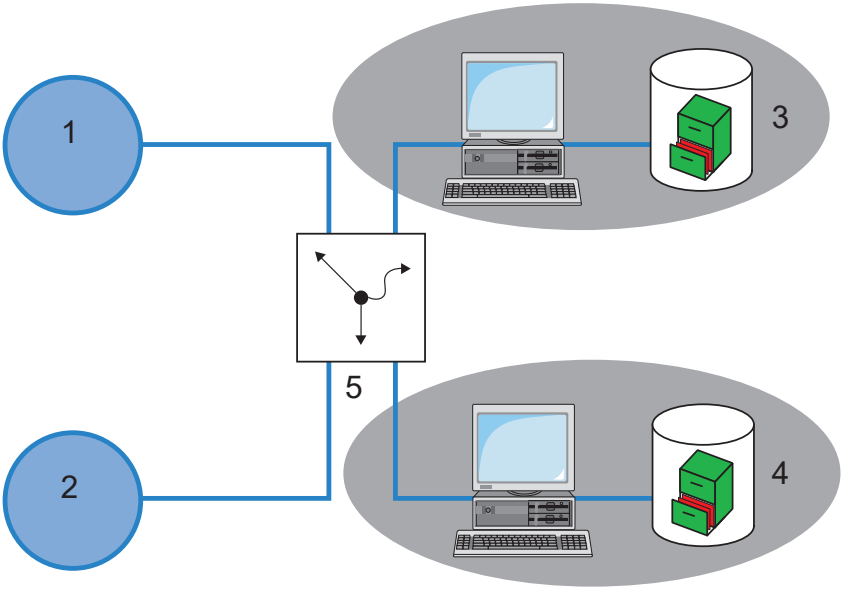


Figure 115:Creating a default route with the corresponding routing tag in the routing table

1: Provider A			
2: Provider B			
3: IP network Company A 10.0.0.0/255.255.255.0, interface tag 1			
4: IP network Company B 10.0.0.0/255.255.255.0, interface tag 2			
5: Routing table:			
IP address	Netmask	Interface tag	Router
255,255,255,255	0.0.0.0	1	Provider A
255,255,255,255	0.0.0.0	2	Provider B

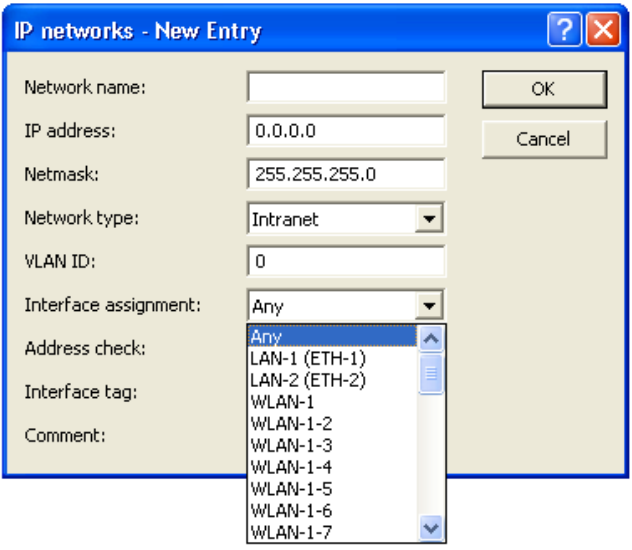
Note: For cases which do not allow IP addresses to be uniquely assigned by interface tags, ARF can be supported by firewall rules. In the above example, this would be the case if each of the networks were to support a public web or mail server, all of which use the same IP address.

11.3.2 Definition of networks and Assignment of Interfaces

When defining a network, the first setting is for the IP-address, which is to be valid for a certain local interface on the OpenBAT device. "Local interfaces" are logical interfaces that are assigned either to a physical Ethernet port (LAN) or a wireless port (WLAN). It is possible for several networks to be active on one interface in order to implement the scenarios above. Conversely, a network can also be active on multiple interfaces (via bridge groups or with the interface assignment "Any"). To define a new network:

☐ Navigate to the following dialog:`Configuration : IPv4 : General` dialog and click "IP networks".

☐ Click "Add" to open the following dialog:



In this dialog, enter values for at least the following fields:

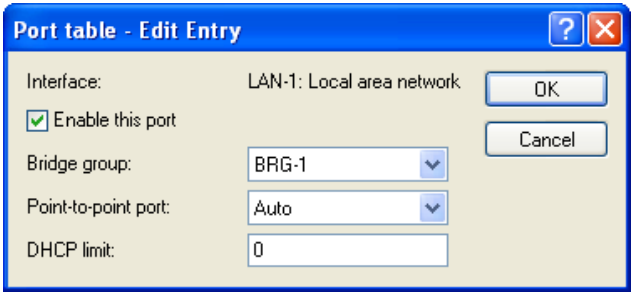
- Network Name: A unique network name allows the identification of networks in other modules (DHCP server, RIP, NetBIOS, etc.) and enables control over which services are available in which networks.
- IP address and Netmask
- Network type: Intranet or DMZ

11.3.3 Assigning Logical Interfaces to Bridge Groups

Particular properties of the logical interfaces are defined in the port table. To configure an interface:

☐ Navigate to the following dialog:`Configuration :Interfaces : LAN` dialog and click "Port table".

☐ Select an interface to open the port table configuration dialog:



In this dialog, enter values for the following fields:

- Enable this port:
  This option activates or deactivates the logical interfaces.
- Bridge group:
  Assigns the logical interface to a bridge group to enable bridging from/to this logical interface via the LAN bridge. If assigned to a common bridge group, several logical interfaces can be addressed at once and they appear to the OpenBAT device to be a single interface. This can then be used for ARF.

  If you remove the interface from all bridge groups via the setting "none," then there is no transmission via the LAN bridge between LAN and WLAN (isolated mode). In this setting, a data transfer between LAN and WLAN for this interface is possible only via the router.

- Point-to-point port:
  Sets the priority for the logical interface when the spanning-tree protocol is enabled. If multiple connections are available, the interface with the highest priority is used. The smaller the value, the higher the priority. If priorities are the same then the interface with lower transmission fees is used or, alternatively, the interface that appears in the highest position in the table.
- DHCP limit:
  Number of clients that can be handled by DHCP. If the limit is exceeded, the oldest entry is dropped. This feature can be used in combination with the protocol filter table to limit access to just one logical interface.

11.3.4 Interface Tags for Remote Sites

By defining interface tags, you can configure virtual routers to be used as part of ARF in a way that uses just a part of the overall routing table. For inbound data packets from the WAN, the assignment of interface tags can be regulated in several different ways, including:

- appropriate firewall rules that capture data packets from particular remote sites, IP addresses, or ports
- entries in the routing table
- the explicit assignment of tags to remote sites

The assignment of tags to the remote sites to separate ARF networks can also be conveniently used for packets received at the WAN-side (which by default contain Tag 0). Without controlling the assignment of tags explicitly with the firewall, the virtual router can be identified directly from the remote site or source route by the form of the interface tag. Inbound and outbound communication can thus be easily divided bi-directionally between virtual routers.

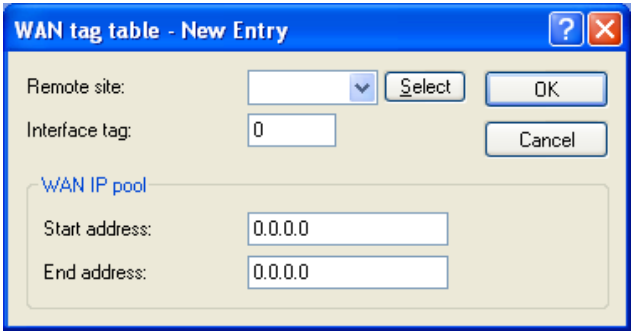
Note: The interface tags determined via the tag table, on the basis of the routing table, can be overwritten with an appropriate entry in the firewall.

Assigning Interface Tags in the WAN Tag Table

To access the dialog where you can add interface tags using the WAN tag table:

☐ Open `Configuration : Communication : Remote Sites` and click 'WAN tag table...'.

☐ In the 'WAN tag table' click 'Add...' to open the 'New Entry' dialog.



WAN Tag Generation

WAN tag generation defines the source for the assignment of interface tags. Besides assignment via the firewall or direct assignment via the tag table, the interface tag can also be selected based on the source route in the effective routing table (static routing entries plus routes learned via RIP). The router compares the source IP and the name of the remote site used to establish the IP connection to the routing information. The routing tag of this source route is assigned for further processing to the packets received at the WAN-side of this connection. If the effective routing table contains more than one entry for a remote site with the same network, the smallest tag is used.

For example, the following ARF networks have been defined:

Network	IP address	Routing tag	Port
PRIVATE	192.168.1.1/24	1	LAN-1:
FACTORY	192.168.10.1/24	10	LAN-2

PRIVATE is to be limited to Internet access; FACTORY is to be limited to the remote site FACTORY. The corresponding effective routing table appears as follows:

IP address	IP netmask	Routing tag	Remote site	Distance	Masking
192.168.10.0	255.255.255.0	10	FACTORY	0	No
255,255,255,255	0.0.0.0	1	INTERNET	0	No

- Data packet coming from network 192.168.10.x: Tag = 10
- Data packet coming from network 192.168.1.x: Tag = 1
- Data packet coming from any other network: Tag = 0

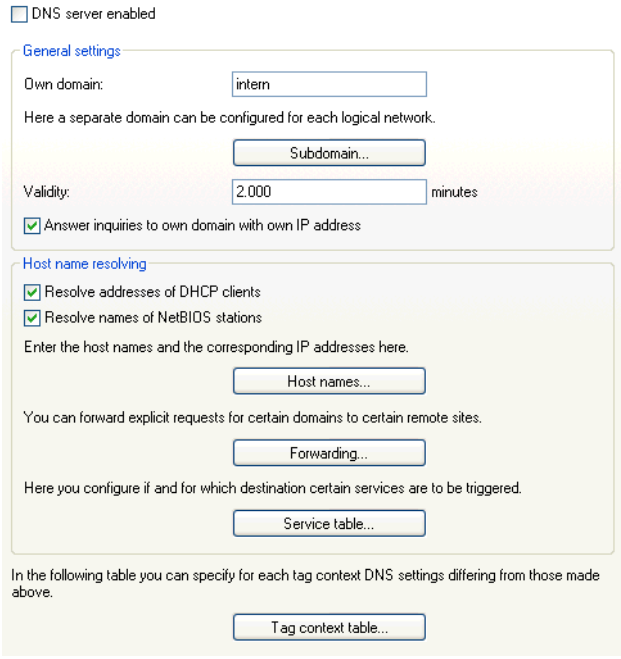
Possible values:

- Manual: With this setting, the interface tags are determined solely by an entry in the tag table. The routing table has no significance in the assignment of interface tags.
- Auto: With this setting, the interface tags are determined initially by an entry in the tag table. If no matching entry is located there, the tag is determined based on the routing table.

Note: The interface tags determined via the tag table and on the basis of the routing table can be overwritten with an appropriate entry in the firewall.

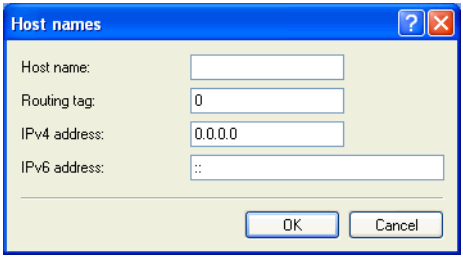
11.3.5 Routing tags for DNS forwarding

For DNS forwarding, multiple independent forwarding definitions (especially general wildcard definitions with "*") are possible for DNS forwarding by identifying them with unique routing tags. Depending on the routing context of the requesting client, the router considers only the forwarding entries that are identified accordingly and the general entries marked with "0".



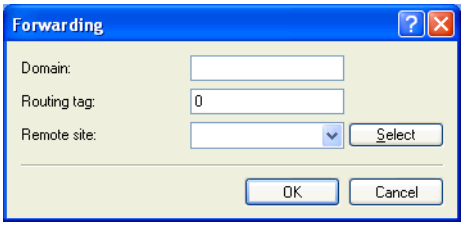
Host names

The item `Configuration:IPv4:DNS:Host names` is used to define the tag context and IP number used by the device to resolve the station names.



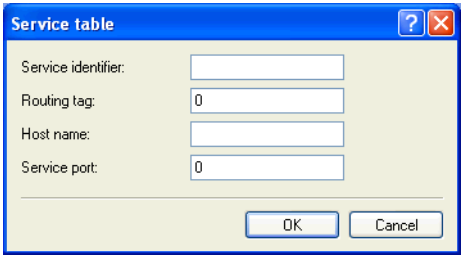
DNS forwarding

The item `Configuration:IPv4:DNS:Forwarding` is used to set the routing tags for the forwarding rules, so ensuring they only apply when the correct routing tags are used.



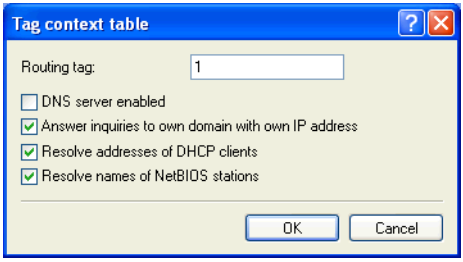
Service table

The item `Configuration:IPv4:DNS:Service table` is used to assign routing tags to the services, so ensuring that they are only available when the correct routing tags are used.



Tag context table

It is possible to define tag contexts in LANconfig under `Configuration:IPv4:DNS:Tag context table`, which override the global settings of the DNS server for specific interface and routing tags (routing context):



If an entry for a tag context exists, then only the DNS settings in this table apply for this context. However, if there is no entry in this table, then the global settings of the DNS server apply.

The following options are possible for each tag context:

- "Routing tag": Unique interface or routing tag in the range of 1 to 65535, the subsequent settings will override the global settings of the DNS server.
- "DNS server enabled": Enables the DNS server of the device.
- "Answer inquiries to own domain with own IP address": If enabled, DNS requests relating to the router's own domain will be answered with the router's IP address.
- "Resolve addresses of DHCP clients": Enables resolution of station names that have requested an IP address through DHCP.
- "Resolve names of NetBIOS stations": Enables resolution of station names that are known to the NetBIOS router.

11.3.6 Virtual Routers

By means of interface-dependent filtering, in combination with policy-based routing, virtual routers can be defined for every interface. For example:

Two separate IP networks are used by the Development and Sales departments. Both networks are connected to different switch ports although they use the same network "10.1.1.0/255.255.255.0". Sales should be restricted to accessing the Internet, whereas Development should also have access to a partner company's network ('192.168.1.0/255.255.255.0').

The result is the following routing table (where the Development department has tag 2, Sales has tag 1):

IP address	IP netmask	Rtg tag	Peer or IP	Distance	Masking	Enabled
192.168.1.0	255.255.255.0	2	PARTNER	0	No	Yes
192.168.0.0	255.255.0.0	0	0.0.0.0	0	No	Yes
255,255,255,255	0.0.0.0	2	INTERNET	2	Yes	Yes
255,255,255,255	0.0.0.0	1	INTERNET	2	Yes	Yes

If Development and Sales were in IP networks with different address ranges, then it would be possible to assign the routing tags with firewall rules. But because both departments are in the same IP network, the only available method of assignment is with network names.

Tag assignment can be carried out directly in the network definition:

"Name"	IP address	Netmask	VLAN-ID	Interface	Source check	Type	Rtg tag
DEVELOPMENT	10.1.1.1	255.255.255.0	0	LAN-1:	strict	Intranet	2
Sales	10.1.1.1	255.255.255.0	0	LAN-2	strict	Intranet	1

Alternatively the assignment of tags can be carried out with a combination of network definitions and firewall rules. The networks are defined as follows:

"Name"	IP address	Netmask	VLAN-ID	Interface	Source check	Type	Rtg tag
DEVELOPMENT	10.1.1.1	255.255.255.0	0	LAN-1:	strict	Intranet	0
Sales	10.1.1.1	255.255.255.0	0	LAN-2	strict	Intranet	0

Routing tags can be used to define the following firewall rules:

"Name"	Protocol	Source	Destination	Action	Linked	Prio	(...)	Rtg tag
DEVELOPMENT	ANY	%Ldevelopment	ANYHOST	%a	Yes	255		2
Sales	ANY	%Lsales	ANYHOST	%a	Yes	255		1

Set these rules to the maximum priority (255), so that they are checked first. Because filtering is still possible by services, set the option "Linked" in the firewall rule.

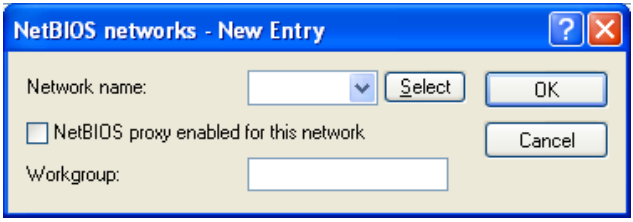
11.3.7 NetBIOS Proxy

Configure the behavior of the NetBIOS proxy separately for each network for which it is relevant—for example, the NetBIOS proxy normally is not active within the DMZ.

To configure the NetBIOS proxy:

☐ Navigate to the following dialog:`Configuration : NetBIOS : General` dialog and click "NetBIOS networks".

☐ Click "Add" to open the following dialog:



In this dialog, enter values for the following fields:

- network name:
  Name of the network for which the NetBIOS proxy is to be activated.
- NetBIOS proxy enabled for this network:
  Select this to activate the NetBIOS-proxy for the selected network.
- Workgroup:
  Enter the name of the workgroup or domain used by the network clients. If multiple workgroups exist within the network, enter just one workgroup name.

Note: By default, networks 'Intranet' and 'DMZ' are entered into the list of NetBIOS networks. The NetBIOS proxy is activated for intranet and deactivated for DMZ.

As soon as a network is assigned to an interface tag, then the names (hosts and groups) that are visible from this network are those in a network with the same tag, or which are accessible via a suitably tagged (with the same tag) WAN route. An untagged network sees all names. Similarly, all names learned from untagged networks are visible to all networks.

The DNS server considers the interface tags when resolving names, i.e. the names resolved by DNS are those learned from a network with the same tag. The special role played by untagged networks applies here too.

The workgroup/domain enables networks to be scanned for NetBIOS names when a device is started. The workgroup is different for every network and has to be defined everywhere. In networks without domains, the name of the largest workgroup should be defined here.

11.4 Source tags for firewall rules

The source tag (the expected interface- or routing tag) is used to identify the ARF context from which a packet was received. This can be used to restrict firewall rules to certain ARF contexts.

Hirschmann Menu tree : Setup : IP-Router : Firewall : Rules : Src-Tag

11.5 Configuring Remote Stations

Remote stations are configured in two tables:

- In the remote site (peer) table all information is input that applies exclusively to a single remote station.
- Parameters for the lower protocol levels (below IP or IPX) are defined in the communication layer table.

Note: The configuration of the authentication (protocol, user name, password) is not covered in this section. Information on authentication is contained in the section ‘Establishing connection with PPP’ (see on page 824).

11.5.1 Remote Site (Peer) List

The available remote stations are created in the peer list with a suitable name and additional parameters. For every WAN interface exists a separate peer list. There are two separate input dialogs for the peer list: one for DSL connections, one for serial connections. To add new remote stations to the peer list:

☐ Navigate to the following dialog:`Configuration : Communication Remote Sites` and click either the button

  – "Remote sites (DSL)..." or

  – "Remote sites (Serial)..."

The following parameters can be configured for each remote station:

Preferences	Used where (in which peer list)	Description
Name	DSL/Serial	Enter the name of the remote station.
Phone number	Serial	The dialup telephone number for the remote station. A number is required if phone calls need to be made to the remote station. This field can remain empty if just incoming calls should be accepted. Several phone numbers for the same remote station can be entered in the RoundRobin list.
Short hold time	DSL/Serial	The time, in seconds, after which the connection should be closed if no data has been transferred.
Short hold time (bundle)	Serial	If a second channel has been opened to the remote station (bundling), it will be closed after the time specified here if no data has been transferred.
Access concentrator	DSL	Used, with the Service parameter, to identify your Internet provider. Contact your Internet provider for this information.
Service	DSL	Used, with the Access concentrator parameter, to identify your Internet provider. Contact your Internet provider for this information.
Layer name	DSL/Serial	Select the layer name for the connection. The configuration of this layer is described in the following section (see on page 800).
MAC address type	DSL	Select which MAC address should be used: ▶ Local: Additional virtual addresses are generated for each WAN connection, based on the device MAC address. ▶ Global: The device MAC address will be used for all connections. ▶ User-defined: Input a MAC address for the remote gateway in the “MAC address” field.
MAC address	DSL	The MAC address for user defined types.

Preferences	Used where (in which peer list)	Description
VLAN ID	DSL	The VLAN identifier if the remote station connection is part of a VLAN.
Automatic callback	Serial	When automatic callback is enabled, a call from the remote station will not be accepted, but the remote station will be called back. This is useful to provide a secure connection, and reduce the connect charges for the remote site. **Note:** ▶ If you select the “fast procedure” option, callback may take one or two seconds. However, on the remote device, be sure the remote site supports this option and “wait for callback” is enabled. ▶ Select “Call back the remote site after name verification” to force the remote site to be authenticated before calling back.

When editing the remote site peers list, note the following:

- If a remote site appears on the two lists, the OpenBAT device uses the faster interface to connect to the remote site. The other interface is used as a backup.
- If neither the access concentrator nor the service is specified, the router connects to the first access concentrator that answers the query.

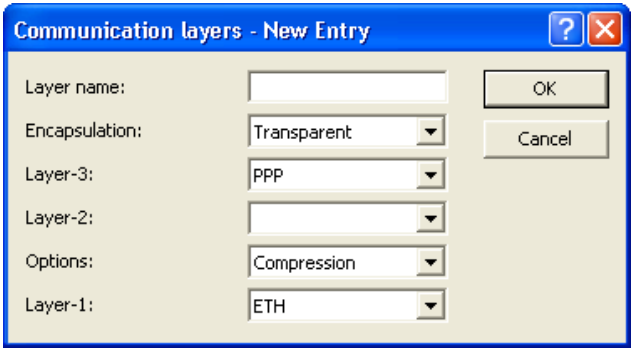
11.5.2 Communication Layers List

A communication layer is a collection of protocol settings that are used when connecting to specific remote stations. By default, the communication layers list includes layer entries with common combinations of protocols. Changes or additions to this list should be made if remote stations are incompatible with all of the existing layer entries.

To access the communication layers list:

☐ Navigate to the following dialog:`Configuration : Communication General` dialog, and click "Communication layers".

☐ Click "Add" to open the following dialog:



A layer entry can contain combinations of the following options.

Note: The available selection possibilities in a given OpenBAT device depend on the device model. Some devices offer the options described below.

Parameter	Description	
Layer name	The layer is selected in the peer list under this name.	
Encapsulation	Additional encapsulations can be set for data packets.	
	Transparent	No additional encapsulations.
	Ethernet	Encapsulation in the form of Ethernet frames.
Layer 3	The following options are available for the switching layer or network layer.	
	Transparent	No additional header is inserted
	PPP	The connection is established according to the PPP protocol (in the synchronous mode, i.e. bit-oriented). The configuration data is taken from the PPP table
	AsyncPPP	Like "PPP" only in asynchronous mode. This means that PPP functions character-oriented.
	... with script	All options can be run with their own script if desired. The script is specified in the script list.
	DHCP	Assignment of the network parameters via DHCP

Parameter	Description	
Layer 2	In this field the upper section of the security layer (Data Link Layer) is configured. The following options are available:	
	Transparent	No additional header is inserted
	PPPoE	The PPP negotiation runs via Ethernet. The PPP packets are encapsulated in Ethernet frames for this purpose. This process is frequently used for DSL connections.
Option	Here you can activate the compression of the data to be transmitted and the bundling of channels. The selected option becomes active when it is supported by both the ports used and the selected Layer-2 and Layer-3 protocols.	
Layer 1	In this field the lower section of the security layer (Data Link Layer) is configured. The following options are available:	
	ETH	Transparent Ethernet as per IEEE 802.3
	Serial	Transmission via the serial interface

11.6 IP Masquerading

One of the most common tasks for a router is to connect LAN workstations to the Internet. For security reasons, hide the IP address of each LAN workstation to the entire internet. IP masquerading can hide the IP addresses of LAN workstations. IP masquerading operates in a router that has been configured with two IP addresses:

- an intranet IP address—typically a private IP address—which the router uses to communicate with computers in the LAN, and
- a public IP address, which the router uses to communicate with remote stations in the Internet

The computers in the LAN use the router as a gateway but are not recognizable themselves. The router divides the intranet from the Internet.

11.6.1 Simple Masquerading

How IP Masquerading Works

Masquerading uses a feature of TCP/IP data transmission—source and destination port numbers—in addition to the source and destination addresses. When the router receives a data packet for transfer, it records the IP address and the sender's port in an internal table. It next assigns the packet the router’s public IP address and a new port number, which could be any number. The router enters this new data in its internal table, and forwards the packet.

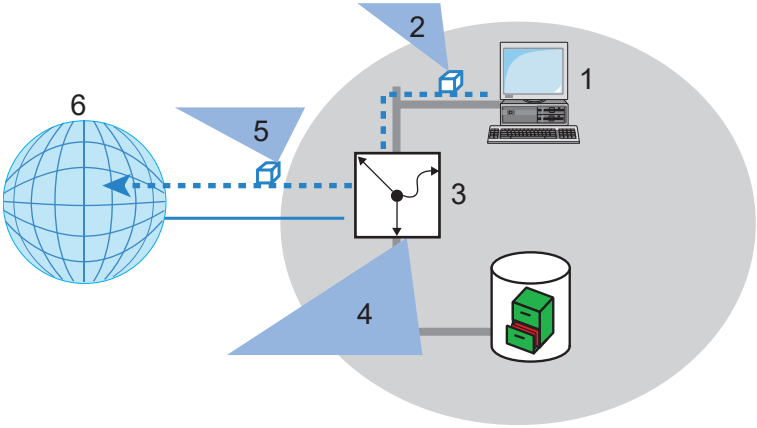


Figure 116:IP masquerading: forwarding data packet with new information

1: Internal workstation: IP address 10.0.0.100
2: Data packet - Source: 10.0.0.100, Target: 80.123.123.123
3: Router - Internal IP address: 10.0.0.1, Public IP address: 80.146.74.146
4: Internal router table entry - Source IP: 10.0.0.100, Port: 3456
5: Data packet - Source: 80.146.74.146, Port 3456, Target: 80.123.123.123
6: Internet

The response to this new packet is now sent to the IP address of the router with the new sender port number. The entry in the internal table allows the router to assign this response to the original sender again:

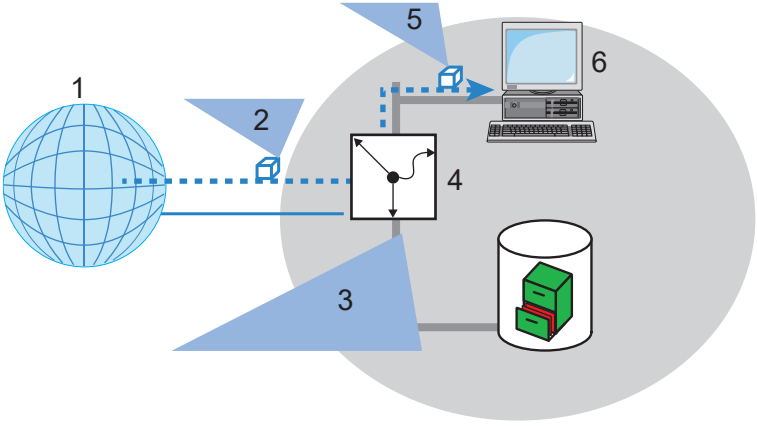


Figure 117:IP masquerading: assigning the response to the original sender

1: Internet
2: Data packet - Source: 80.123.123.123, target: 80.146.74.146
3: Internal router table entry - Source IP: 10.0.0.100, Port: 3456
4: Router - Internal IP address: 10.0.0.1, Public IP address: 80.146.74.146
5: Data packet - Source: 80.123.123.123, target: 10.0.0.100
6: Internal workstation: IP address 10.0.0.100

Protocols that can be Transmitted via IP Masquerading

IP masquerading can transmit IP protocols that are based on TCP, UDP, or ICMP and communicate exclusively through ports. One example of this type of uncomplicated protocol is the one on which the World Wide Web is based: HTTP.

Individual IP protocols do use TCP or UDP, but do not, however communicate exclusively through ports. This type of protocol calls for a corresponding special procedure for IP masquerading. Among the group of protocols supported by IP masquerading in the OpenBAT device are:

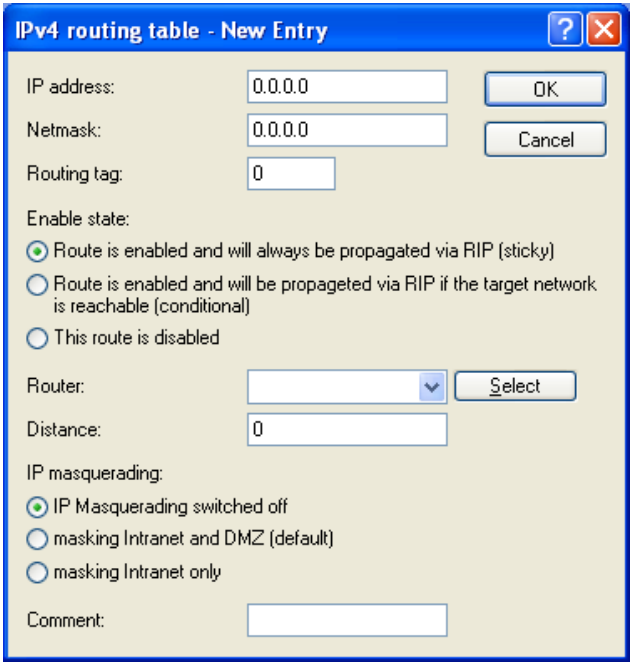
- ftp (using the standard ports)
- H.323 (to the same extent as used by Microsoft Netmeeting)
- Point-to-Point Tunneling Protocol (PPTP)
- Internet Protocol Security (IPSec)
- Internet Relay chat (IRC)

Configuring IP Masquerading

IP Masquerading can be configured for each entry in the routing table:

☐ Open `Configuration : IP Router. Routing` dialog and click ‘IPv4 routing table...’.

☐ Inside the 'IPv4 routing table', select an entry and click 'Edit...', or click 'Add...' for creating a new entry. The following dialog opens:



You can apply IP masquerading to devices in the Intranet, or in both the Intranet and DMZ.

11.6.2 Inverse Masquerading

Simple masquerading hides internal LAN IP addresses behind the public IP address of the router. However, if a certain device on the LAN—for example an ftp server—is supposed to be available to stations on the internet, simple masquerading would also hide its IP address from Internet devices. A connection to this ftp server from the internet is not possible.

To enable the access to such a server (’exposed host’) in the LAN, the IP address of the ftp server needs to be entered with all services that are accessible from outside the LAN. If a remote device sends a packet from the Internet to the ftp server on the LAN, from the point of view of this remote device, the router appears to be the ftp server. The router reads the IP address of the ftp server in the LAN from the entry in the service table. The packet is forwarded to this computer. Packets that come from the ftp server in the LAN (responses from the server) are hidden behind the IP address of the router.

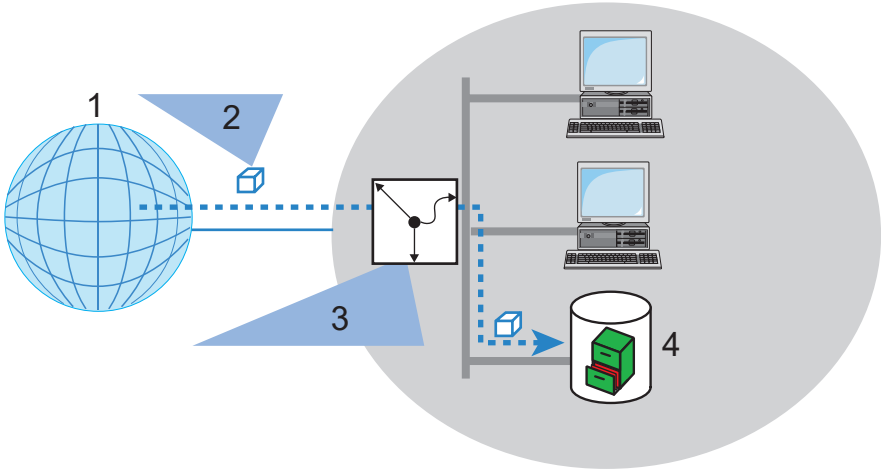


Figure 118:Inverse masquerading

1: Internet
2: Data packet - Source: 80.123.123.123, target: 80.146.74.146, port 21
3: Internal router table entry: Source IP: 10.0.0.100, Port: 3456
4: ftp server - IP address: 10.0.0.10

The difference between simple masquerading and inverse masquerading is that:

- Access to a service (port) in the intranet from outside needs to be defined in advance by specifying a port number. This is achieved by associating the destination port with the intranet address of, for example, the ftp server, in a service table.
- When accessing the Internet from the LAN, the router itself makes the entry in the port and IP address information table.

Note: The table can hold up to 2048 entries, thereby allowing 2048 simultaneous transmissions between the masked and the unmasked network. After a specified period of time, the router assumes that an entry is no longer required and deletes it automatically from the table.

Stateful Inspection and Inverse Masquerading

If the masquerading module exposes a port (for example, packets received on this port are forwarded to a server in the LAN), then this should be implemented with both a Deny All firewall strategy plus an additional entry in the Stateful Inspection firewall, which enables the access by all stations to the respective server.

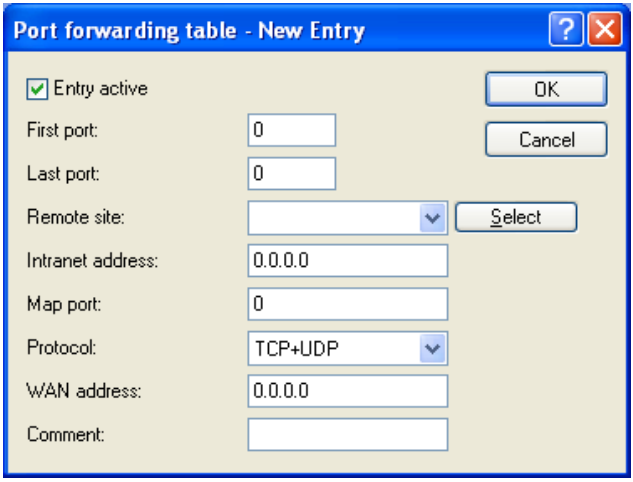
Configuring Port Mapping

On occasion it is desirable for the exposed host not to be contacted over this standard port, e.g. when security reasons demand the use of another port. In this case, both the mapping of ports to an IP address, and the mapping of ports to other ports (port mapping) are necessary. Another use for this port mapping is the assignment of several ports of the WAN to a shared port in the LAN, which can be assigned to different IP addresses.

The configuration of port mapping involves the assignment of a port or port range (first port to last port) to a target IP address from the LAN, and the port (map port) to be used in the LAN. Port mapping is performed in the Port Forwarding table:

☐ Navigate to the following dialog:`Configuration : IP Router : Masq.` and click "Port forwarding table".

☐ Click "Add" to open the following dialog:



Configure the following parameters:

- Entry active:
  Toggles the port mapping entry on and off.
- First port / Last port:
  Defines the port, or range of ports, over which service requests will be received.
- Remote site:
  Select the remote site to which this entry applies. If this is left empty, the entry applies to all remote sites.
- Internet address:
  The intranet (LAN) address of the device providing the service, to which packets will be forwarded.
- Map port:
  The port over which requests will be forwarded. If ‘0’ is entered for the map port, the ports used in the LAN will be the same as those used in the WAN. If a port range is to be mapped, then the map port identifies the first LAN port to be used. For example, mapping the port range '1200' to '1205' to the internal map port '1000' means that the ports 1000 to 1005 will be used for data transfer in the LAN.
  Port mapping is static, meaning that two ports or port ranges cannot be mapped to the same port in a target LAN computer. The same port mapping can be used for different target computers

- Protocol:
  The protocol to which this entry applies.
- WAN address:
  WAN address which applies for this entry. If the device has more than one static IP address, then this allows port forwarding to be limited to certain connections.

11.7 Demilitarized Zone (DMZ)

A demilitarized zone (DMZ) renders certain stations in a network accessible from the Internet. These computers in the DMZ are generally used to offer Internet services such as e-mail or http. The rest of the network should of course be inaccessible from the Internet.

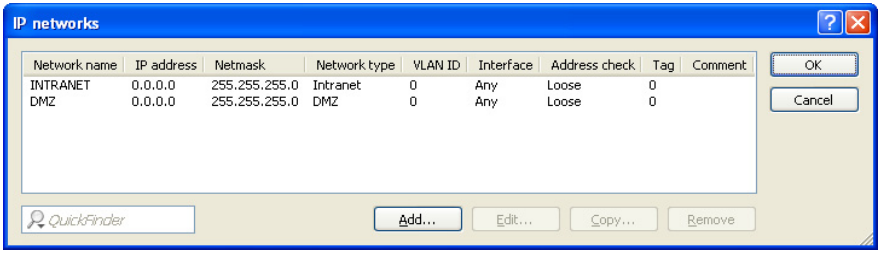
In order to allow this architecture, data traffic between the three zones—Internet, DMZ and LAN—need to be analyzed by a firewall. The firewall's tasks can also be consolidated in a single device (the router). In this design, the router needs to include three separate interfaces that can be monitored independently by the firewall:

- LAN interface
- WAN interface
- DMZ interface

11.7.1 Assigning Networks to the DMZ

In its factory configuration the OpenBAT device is preconfigured with only one logical DMZ network zone. You can access this in LANconfig at the following position. Carry out the following steps to access the present DMZ network zone

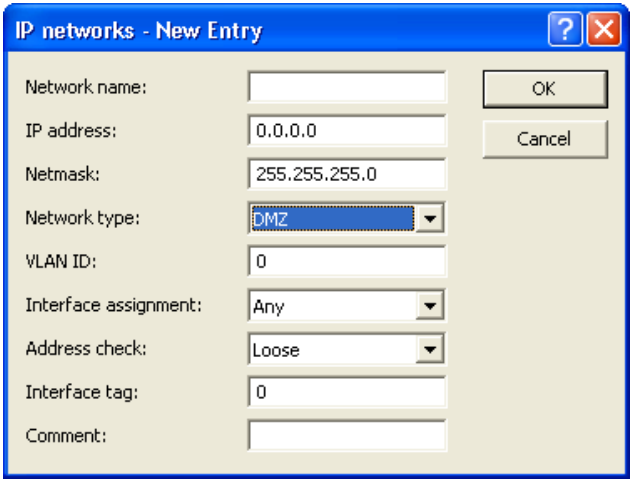
☐ Navigate to the following dialog:`Configuration : IPv4 : General` dialog and click "IP networks".



The DMZ network can be selected and edited from the "IP networks" window.

New additional networks can be added and assigned to the DMZ. To do so:

☐ In the ‘IP networks’ window, click ‘Add...’ to open the ‘New Entry‘ dialog:



☐ In this dialog, set the ‘Network type’ parameter to ‘DMZ’.

11.7.2 Address Checking

To shield the DMZ (demilitarized zone) and the Intranet from unauthorized attacks, you can activate an additional address check for each interface using the firewall's Intrusion Detection System, or IDS (see on page 960).

To configure address checking, do the following:

☐ In the "IP Networks - New Entry" dialog, select a setting for the "Address Check" parameter. Possible values:

- Loose: The OpenBAT device accepts any source address if the OpenBAT is directly addressed.
- Strict: The OpenBAT device requires that a return route has to be explicitly available so that no IDS notification is triggered. This is usually the case if the data packet contains a sender address to which the relevant interface can also route data. Sender addresses from other networks, to which the interface cannot route, or sender addresses from the local address range will therefore trigger an IDS-notification.

11.7.3 Unmasked Internet Access for a Server in the DMZ

While the inverse masquerading allows the (see on page 806) OpenBAT device to expose at least one service of each type (e.g. one Web, Mail and ftp server), this approach includes some restrictions:

- The masquerading module should support and "understand" the particular server service of the "exposed host." For instance, several VoIP servers use proprietary, non-standard ports for extended signaling. Such a server could be used exclusively on unmasked connections.
- Keep in mind that the "exposed host" resides within the LAN. When the host is under control of an attacker, it could be misused as a starting point for further attacks against machines in the local network.

Two Local Networks Operating Servers in a DMZ

This feature requires an Internet access with multiple static IP addresses.

Note: Please contact your ISP for an appropriate offer.

One example: For example: your ISP assigns you the IP network address 123.45.67.0 with the netmask 255.255.255.248. In this case, you can assign the following IP addresses:

DMZ IP address	Description
123.45.67.0	Network address
123.45.67.1	The OpenBAT device as a gateway for the Intranet
123.45.67.2	Device in the LAN which is to receive unmasked access to the Internet, e.g. web server connected at the DMZ port
123.45.67.7	Broadcast address

Computers and devices in the Intranet have no public IP address, and therefore appear with the IP address of the OpenBAT device (123.45.67.1) on the Internet.

Separation of Intranet and DMZ

Although Intranet and DMZ may already be separated at the Ethernet level by distinct interfaces, an appropriate firewall rule needs to be set up in all cases. In this way, the DMZ is also separated from the LAN at the IP level.

In this way, server service is available from both the Internet and the Intranet. However, IP traffic from the DMZ to the Intranet is not permitted. Extending the previous example:

- With an 'Allow All' strategy (default): Deny access from 123.45.67.2 to 'All stations in local network'.
- With a 'Deny All' strategy (see on page 923): Allow access from 'All stations in local network' to 123.45.67.2.

11.8 N:N Mapping

Network Address Translation (NAT) can be used to achieve several different goals:

- N:1 mapping:
  In N:1 NAT (also known as IP masquerading (see on page 803)), all addresses (‘N’) of the local network are mapped to just one (‘1’) public address. This clear assignment of data streams to the respective internal PCs is generally made available by the ports of the TCP and UDP protocols. For this reason, N:1 mapping is sometimes referred to as NAT/PAT (Network Address Translation/Port Address Translation).

  Due to the dynamic assignment of ports, N:1 masquerading enables exclusively those connections that have been initiated by the internal network. Exception: ‘inverse masquerading’ (see on page 806) where an internal IP address is statically exposed on a certain port.
- Network coupling:
  N:N mapping is used to couple networks with identical address ranges. This transforms unambiguously multiple addresses (“N”) of the local network to multiple (“N”) addresses of another network. This helps resolve address conflicts. Rules for address translation are defined in a static table in the OpenBAT device. Thereby new addresses are assigned to single stations, parts of the network, or the entire LAN, by means of which the stations can contact other networks.
- Remote monitoring and control:
  Some protocols (ftp, H.323) exchange parameters during their protocol negotiation, which can influence the address translation for the N:N mapping. For a correct functioning of the address translation, the connection information of these protocols is tracked appropriately by functions of the firewall in a dynamic table, and is additionally considered to the entries of the static table.

Note: The address translation is made ‘outbound’, i.e. the source address is translated for outgoing data packets and the destination address for incoming data packets, as long as the addresses are located within the defined translation range. An ‘inbound’ address mapping, whereby the source address is translated (instead of the destination address), needs to be realized by an appropriate ‘outbound’ address translation on the remote side.

11.8.1 Application Examples

The following examples of network coupling, and remote monitoring and control represent typical applications of N:N mapping.

Network Coupling

It is often desirable to couple the networks of two different companies that internally use the same private address range (e.g. 10.0.0.x). This occurs when one company needs to gain access to one (or more) servers of the other.

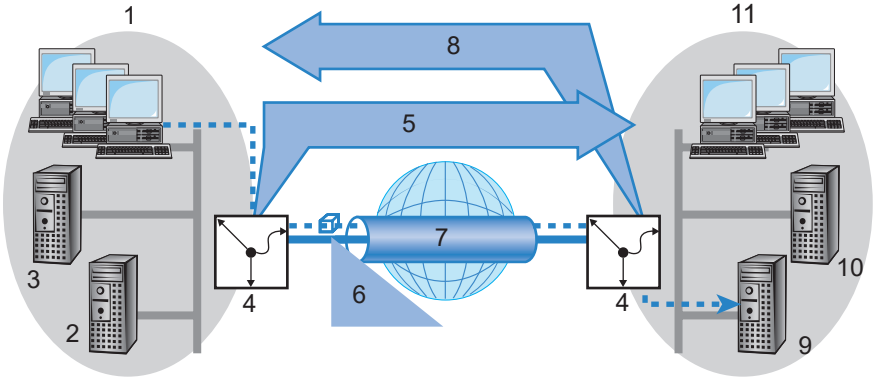


Figure 119:Network coupling

1: Network of company A	7: VPN tunnel
2: Server_A1: 10.0.0.1	8: N:N mapping to 192.168.2.x
3: Server_A2: 10.0.0.2	9: Server_B1: 10.0.0.1
4: Gateway	10: Server_B2: 10.0.0.2
5: N:N mapping to 192.168.1.x	11: Network of company B
6: Data packet - target: 192.168.2.1	–

In this example, network servers of company A and B need to gain access via a VPN tunnel to the other company's network. All stations of each LAN require access to the servers of the remote network. Initially, access to the other network is not possible, because each network uses the same address range. If a workstation on the company A network attempts to access server 1 of company B, the request (with an address from the 10.0.0.x network) will be routed exclusively within company A's local network; the inquiry will not even reach the gateway.

With the help of N:N mapping, all addresses of each LAN can be translated to a new address range for coupling with the other network. The network of company A is translated to 192.168.1.x. The network of company B is translated to 192.168.2.x. Using these new addresses, each LAN can now be reached from the other network. The station from the network of company A is now addressing server 1 of company B under the address 192.168.2.1. The addressee no longer resides within the network of company A. The inquiry is now passed on to the gateway, and is routed to the other network.

Remote Monitoring and Remote Control of Networks

Remote maintenance and control of networks is easier to accomplish by means of VPN. Using the nearly ubiquitous broadband Internet connections, a network administrator is not captive to multiple data communication technologies or expensive leased lines.

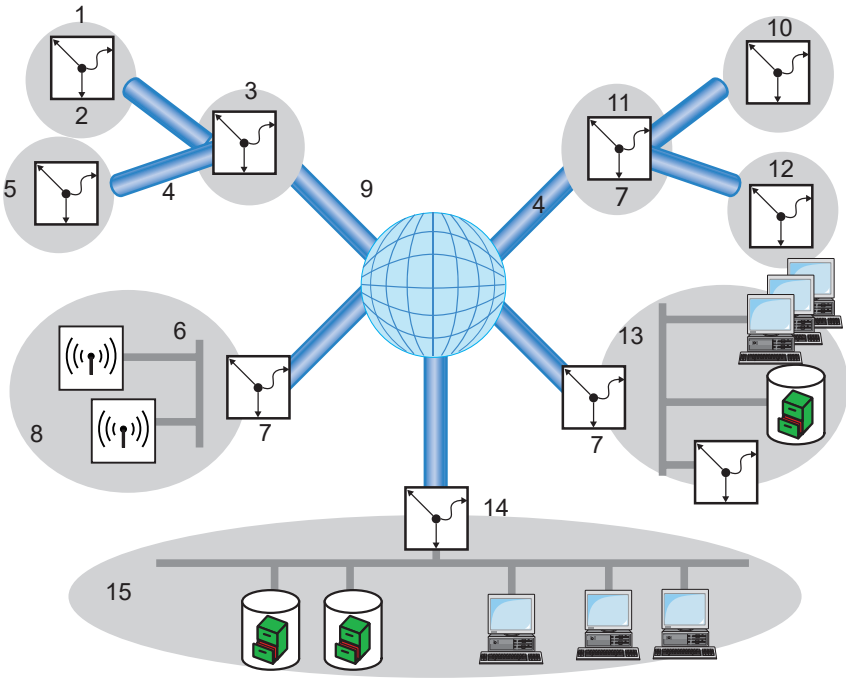


Figure 120:Centralized monitoring and control of networks for different clients

1: Customer A, office 1: 10.1.2.x, 255.255.255.0	9: Internet
2: Gateway, e.g. 10.1.2.1	10: Customer B, office 1: 10.1.2.x
3: Customer A, headquarters: 10.1.x.x, 255.255.0.0	11: Customer B, headquarters: 10.1.x.x, 255.255.0.0
4: VPN tunnel	12: Customer B, office 2: 10.1.3.x, 255.255.255.0
5: Customer A, office 2: 10.1.3.x, 255.255.255.	13: Customer D: 172.16.10.x, 255.255.255.0
6: WLAN, e.g. 172.16.10.11	14: Gateway, e.g. 80.123.123.123 (public) and 172.16.10.11 (intern)
7: Gateway	
8: Customer C: 172.16.10.x, 255.255.255.0	15: Service provider: 172.16.10.x, 255.255.255.0

In this example, a service provider monitors the networks of different clients out of a central control location. For this purpose, SNMP-capable devices should automatically send the respective trap notices of important events to the SNMP trap addressee (e.g. LANmonitor) of the network of the service provider. In this way, the LAN administrator of the service provider can dynamically view the current of the state of the devices at any time.

The individual networks can be structured very differently:

- Clients A and B integrate their branches with their own networks via VPN connections to each company LAN.
- Client C operates a network with several public WLAN base stations as hot spots.
- Client D includes an additional router for dial-up accesses in his LAN.

Note: The networks of client A and B use different address ranges in the respective head office and the connected branches. A standard network coupling via VPN is therefore possible between these networks.

In order to avoid the effort of creating its own VPN tunnel to each individual subnetwork clients A and B, the service provider makes just one VPN connection to the head office, and uses the existing VPN lines between head office and branches for communication with the branches.

Traps from the networks report to the service provider whether, e.g., a VPN tunnel is backed-up or lost, if a user has tried to log in three times with an incorrect password, if a user has attempted to establish a wireless connection, or if a LAN cable has been detached from a switch.

Routing of these different networks quickly reaches their address limits, if two or more clients use same address ranges. Additionally, if some clients use the same address range as the service provider, additional address conflicts are added. In this example, one of the hot spots of client C has the same address as the gateway of the service provider.

Here are two different approaches to resolve these address conflicts:

- Loopback decentralized 1:1 mapping:
  in the decentralized version, alternative IP addresses for communicating with the SNMP addressee are assigned to each of the monitored devices by means of 1:1 mapping. This address is in also known as a loopback address, and the method as the loopback method.

  Note: Loopback addresses are valid exclusively for communication with certain remote stations on the connections belonging to them. A OpenBAT device is thus not generally reachable at this IP address.

- Central N:N mapping:
  Instead of separately configuring each individual gateway in the branch networks, a better solution is for the administrator to configure a single central address translation in the gateway of the head office. At the same time, all subnetworks located behind the head office are also assigned the required new IP addresses.

In this example, the administrator of the service provider selects 10.2.x.x as central address translation for the network of client B, so that both networks configured with the same address range look like two different networks to the gateway of the service provider.

The administrator selects the address ranges 192.168.2.x and 192.168.3.x for client C and D, so that the addresses of these networks differ from the network of the service provider.

In order to enable the gateway of the provider to monitor the networks of clients C and D, the administrator also configures an address translation to 192.168.1.x for its own network.

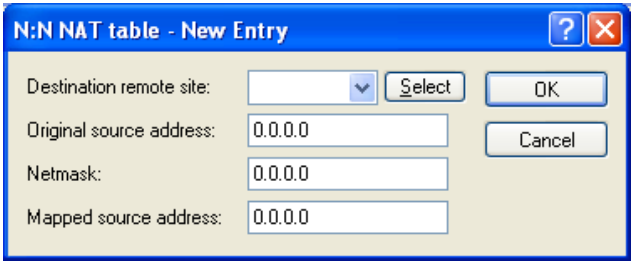
11.8.2 Configuring Address Translation

Configuration of N:N mapping requires very little information. Because a LAN can be coupled with several other networks via N:N mapping, different destinations can also have different address translations for a source IP range. The NAT table can contain a maximum of 64 entries.

To enter an item into the N:N NAT table:

☐ Navigate to the following dialog:`Configuration : IP-Router : N:N-Mapping` and click "N:N NAT table".

☐ Click "Add" to open the following dialog:



In this dialog, enter values for the following fields:

- Destination remote site:
  The name of the remote station to which this mapping rule will apply.
- Original source address:
  The IP address of the network to be mapped to a different address range for the specified remote station. This can be the address of a single station or of the router itself.
- Netmask:
  The netmask associated with the specified IP addresses. The netmask applies to both IP address ranges (original and mapped) because, for N:N address mapping, the original and the mapped IP networks need to be the same size. If you want to map just a single IP address, enter 255.255.255.255 for the netmask.
- Mapped source address:
  The IP address of the network to which the original addresses should be mapped for the specified remote station. The size of the mapped IP network depends on the specified netmask and is identical for the original and the mapped IP range.

When entering original and mapped source addresses, note the following:

- Original and mapped address can be assigned arbitrarily for the translation of single addresses. For example, it is possible to assign the mapping address 192.168.1.88 to a LAN server with the IP address 10.1.1.99.
- For translation of entire address ranges, the station-related part of the IP address will be taken directly, appended to the network-related part of the mapping address. Therefore, in an assignment of 10.0.0.0/255.255.255.0 to **192.168.1**.0, a server of the LAN with IP address 10.1.1.99 will get assigned the mapping address 192.168.**1.99**.

Note: The mapped address range should be at least as large as the source address range.

Note: N:N mapping functions are effective provided that the firewall has been activated.

Advanced Configuration Considerations

By setting up address translation in the NAT table, the networks and workstations become initially visible exclusively under the mapped address to devices in other networks. For seamless routing of data between networks, some further settings are still necessary:

- Entries in the routing tables for the new addresses so packets can find the way to their destination.
- DNS forwarding entries, in order that inquiries about certain devices in the other network can be resolved into mapped IP addresses (see on page 1113).
- The firewall rules of the gateways need to be adjusted so that authorized stations in external networks can set up connections.

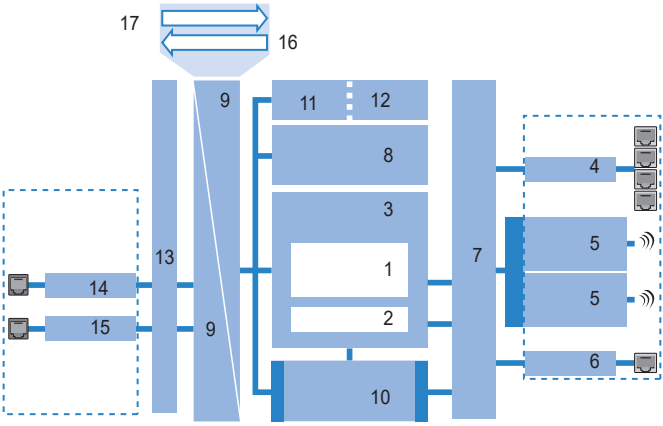


Figure 121:Address translation

1: IP router	10: Configuration & management
2: IP redirect	11: OpenBAT User administration
3: Firewall	12: RADIUS client / server
4: LAN interface or an integrated switch	13: DHCP client / PPP
5: Wireless modules	14: ADS
6: DMZ	15: DSL
7: LAN bridge	16: Source address
8: IP modules (NetBIOS, DNS, DHCP server, RADIUS, RIP, NTP, SNMP, SYSLOG, SMTP)	17: Destination address
9: IP masquerading and N:N mapping	

11.9 Establishing Connection with PPP

This routers also supports the point-to-point protocol (PPP). PPP is a generic term for a whole series of WAN protocols, which enable the interaction of routers made by different manufacturers. Because of the increasing importance of this family of protocols, and the fact that PPP is not associated with any specific routing operating mode, the following sections separately describe the device functions that are associated with PPP.

11.9.1 The Point-to-Point Protocol (PPP)

What is PPP?

The point-to-point protocol was developed specifically for network connections via serial channels and has become the standard for connections between routers. It implements the following functions:

- Password protection according to Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP) or the Microsoft version of CHAP (MS CHAP)
- Callback functions
- Negotiation of the network protocol to be used over the established connection (IP or IPX, for example). Included in this are any parameters necessary for these protocols, for example IP addresses. This process is carried out using IPCP (IP Control Protocol).
- Negotiation of the connection parameters, e.g. the MTU (Maximum Transmission Unit (see on page 862).

- Verification of the connection through LCP (Link Control Protocol).
- Combining several DSL channels (MultiLink PPP, MultiLink PPPoE)

PPP is the standard used by router connections for communication between devices, or by the WAN connection software of different manufacturers. Connection parameters are negotiated and common settings are agreed using standardized control protocols (e.g., LCP, IPCP, CCP) that are contained in PPP.

PPP Application Scenarios

The point-to-point protocol is used in the following applications:

- for reasons of compatibility, for example, when communicating with external routers
- remote access from distant workstations
- Internet access (when sending addresses)

The PPP that is implemented by the OpenBAT device can be used synchronously or asynchronously, by either a transparent HDLC connection or an X.75 connection.

The Phases of PPP Negotiation

Establishing a connection using PPP begins with a negotiation of the parameters to be used for the connection. This negotiation is carried out in four phases which should be understood for the sake of configuration and troubleshooting:

- Establish phase:
  After a connection has been initiated at the data communication level, negotiation of the connection parameters begins through the LCP. This ascertains whether the remote site is also ready to use PPP. The packet sizes and the authentication protocol (PAP, CHAP, MS-CHAP or none) are determined. The LCP then switches to the opened state.
- Authenticate phase:
  Passwords are exchanged, if necessary. The password is sent just once if PAP is used for the authentication process. An encrypted password is sent periodically at adjustable intervals if CHAP or MS CHAP is used. A callback may also be negotiated in this phase via CBCP (Callback Control Protocol).
- Network phase:
  The OpenBAT device supports the protocols IPCP and IPXCP. After the password has been successfully transmitted, the IPCP and/or IPXCP network layer can be established. IP and/or IPS packets can be transferred from the router modules to the opened line if the negotiation of parameters is successful for at least one of the network layers.
- Terminate phase:
  In the final phase the line is cleared, when the logical connections for all protocols are cleared.

The PPP negotiation in the OpenBAT device

The progress of a PPP negotiation is logged in the devices' PPP statistics. The protocol packets listed in detail there can be used for checking purposes in the event of unusual system events. The PPP trace outputs offer a further method of analysis. You can use the command line interface command:

```
trace + ppp
```

to begin output of the PPP protocol frames exchanged during a terminal session. You can perform a detailed analysis once the connection has been broken if this terminal session has been logged in a log file.

11.9.2 Checking the Connection with LCP

The devices involved in the establishment of a connection through PPP negotiate a common behavior during data transfer. For example, they first decide whether a connection can be made using the specified security procedure, names and passwords.

The reliability of the connection can be constantly monitored using the link control protocol (LCP) after the connection has been established. This is achieved within the protocol by the LCP echo request and the associated LCP echo reply. The LCP echo request is a query in the form of a data packet which is transferred to the remote station along with the data. The connection is stable if a valid response to this request for information is returned (LCP echo reply). This request is repeated at defined intervals so that the connection can be continually monitored.

What happens if there is no reply? Initially, a few retries are initiated to exclude the possibility of any short-term line interference. The connection will be dropped and an alternative route sought if all the retries remain unanswered.

Note:

- During remote access of individual workstations with Windows operating systems, you may wish to switch off the regular LCP requests because these operating systems do not reply to LCP echo requests.
- The LCP request behavior is configured in the PPP list for each individual connection. Entries made in the ‘Time' and ‘Retries' fields set the intervals at which LCP requests should be made, and the number of retries that should be initiated without a response before the line can be considered lost. Setting both the ‘Time’ and the ‘Retries’ to ‘0’ turns off LCP requests (see on page 830).

11.9.3 Assignment of IP Addresses via PPP

In order to connect computers using TCP/IP as the network protocol, all participating computers require a valid and unique IP address. If a remote station does not have its own IP address (such as the individual workstation of a telecomputer), the OpenBAT device assigns it an IP address for the duration of the connection, enabling communications to take place.

This type of address assignment is carried out during PPP negotiation and implemented exclusively for connections via WAN. In contrast, the assignment of addresses via DHCP is (normally) used within a local network.

Note: Assignment of an IP address is possible provided that the OpenBAT device can identify the remote station by its call number or name when the call arrives, i.e. when the authentication process has been successful.

- Remote Access example:
  Address assignment is made possible by a special entry in the IP routing table. 255.255.255.255 is specified as the network mask, in addition to the IP address to be assigned to the remote site in the "Router-name" field. In this case, the router name is the name with which the remote site needs to identify itself to the OpenBAT device.

  In addition to the IP address, the addresses of the DNS and NBNS servers (Domain Name Server and NetBIOS Name Server) including the backup server from the entries in the TCP/IP module are transmitted to the remote station during this configuration.

  So that everything functions properly, the remote site also needs to be adjusted in such a way that it can obtain the IP address and the name server from the OpenBAT device. This can be accomplished with Windows dial-up networking through the settings in the "TCP settings" under "IP address" and "DNS configuration." This is where the options "IP address assigned by server" and "Specify name server addresses" are activated.
- Internet Access Example:
  If Internet access for a local network is accessed via the OpenBAT device, the assignment of IP addresses can occur in a reverse manner. In this case, configurations are possible in which the OpenBAT device itself has no valid IP address in the Internet and can be assigned one by the Internet provider for the duration of the connection. In addition to the IP address, the OpenBAT device also receives information about the DNS server from the provider during the PPP negotiation. In the local network, the OpenBAT device is known exclusively by its internal valid intranet address. Workstations in the local network can then access the same Internet account and also reach e.g. the DNS server.

Windows users are able to view the assigned addresses via LANmonitor. In addition to the name of the remote station, the current IP address as well as the addresses of DNS and NBNS servers can be found there. Options such as channel bundling or the duration of the connection are also displayed.

11.9.4 Configuring PPP Negotiation Settings

Use the PPP list to specify your own definition of PPP negotiation for each remote site contacting your network.

The authentication of point-to-point connections in the WAN commonly relies on one of the protocols PAP, CHAP, MS-CHAP or MS-CHAPv2. There exists a hierarchy among these protocols: MS-CHAPv2 is a "higher-level" protocol than MS-CHAP, CHAP or PAP. Higher-level protocols provide greater security. Many dial-in routers at Internet providers allow up-front authentication using a higher-level protocol such as CHAP, but support the use of PAP further down the line. If the setting for the protocol for authentication is fixed in the OpenBAT device, the connection may be lost because no common authentication protocol can be negotiated.

Note: In principle, authentication can be repeated during connection negotiation. Another protocol can be selected if, for example, it can be initially recognized from the username. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, the OpenBAT device needs to explicitly refuse the provider's request for CHAP in order to be able to provide PAP user data for requests to be forwarded by the provider.

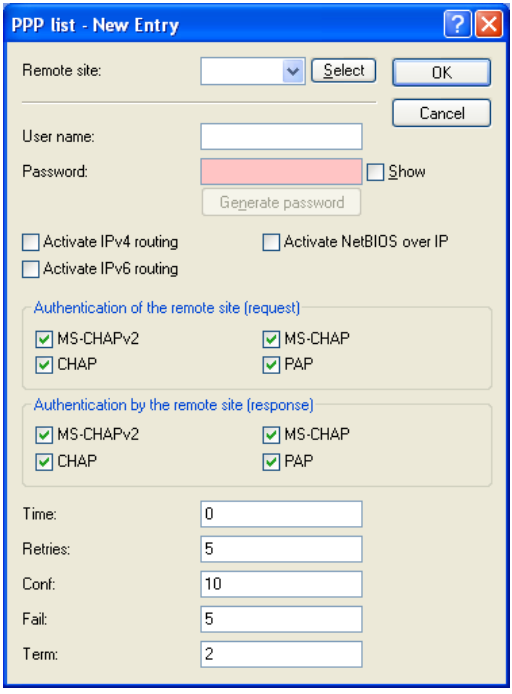
A flexible setting for the authentication protocols in the OpenBAT device establishes the PPP connection as required. In addition, one or more protocols can be defined that are accepted for authentication of remote sites in the OpenBAT device (inbound connections) and on login of the OpenBAT device into other remote sites (outbound connections).

- When establishing inbound connections, the OpenBAT device requires the lowest of the permitted protocols, but where possible it also permits the remote site to use one of the higher-level protocols.
- When establishing outbound connections, the OpenBAT device offers all enabled protocols, but permits just those that are selected. It is not possible to negotiate one of the disabled, possibly higher-level, protocols.

To access the PPP List, follow these steps:

☐ Open the `Configuration : Communication : Protocols` window, and click ‘PPP list...’.

☐ In the ‘PPP list’, click ‘Add...’ to open the ‘New Entry’ dialog:



PPP negotiation is configured using the following parameters:

- Remote site:
  The name of the remote station, which needs to correspond to an entry in the list of remote sites (see on page 798).
- User name:
  The name under which the router should log in to the remote station. The router will use its own name if you leave this field blank.
- Password:
  The PPP password for the remote station. If your router has to log in to the remote station (e.g. an Internet provider), enter the log-in password here. If the remote station has to call your router, enter the log-in password with which the remote station will authenticate itself.

- Activate IPv4/IPv6 routing / Activate NetBIOS over IP:
  Select the protocols that are to be routed to the remote site.
- Authentication of the remote site (request):
  Specify the security measures that apply to the remote site when a connection is established. At least one of the selected measures needs to be responded to by the remote site. This is required by the local dial-in, for example. If the remote site is an Internet provider, select none of them. If more than one method is selected, a fallback to the next protocol is performed until the remote site successfully responds.
- Authentication by the remote side (response):
  Specify the security measures which are allowed for the local station when performing an authentication response. If the remote site is an Internet provider, select all of them. If none of the methods are selected, no local authentication is accepted from the remote site.
- Time:
  This parameter establishes the intervals at which cyclical checks should be performed for the remote station. For Windows remote stations, set this parameter to ‘0’.
- Retries:
  The number of attempted repetitions.
- Conf. / Fail / Term:
  These parameters affect the way PPP works. Please refer to RFC 1661 for detailed information. Normally, you can accept the default settings.

11.9.5 The DEFAULT Remote Site

During the PPP negotiation, the remote station dialing in logs into the OpenBAT device with its name. The OpenBAT device can derive the permissible values for authentication from the PPP table based on the name. At the start of the negotiation, the remote site occasionally cannot be identified by call number (dial-in), IP address (PPTP dial-in) or MAC address (PPPoE dial-in). It is thus not possible to determine the permitted protocols

in this first step. In these cases, authentication is performed first with those protocols enabled for the remote site with name DEFAULT. If the remote site is authenticated successfully with these settings, the protocols permitted for the remote site can also be determined.

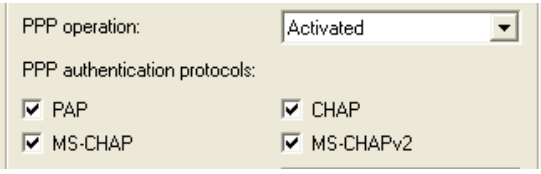
If authentication uses a protocol entered under DEFAULT, but which is not permitted for the remote site, then authentication is repeated with the permitted protocols.

11.9.6 RADIUS authentication of PPP connections

PPP connections can also be authenticated by an external RADIUS server. However, these external RADIUS servers do not necessarily support all available protocols. For this reason, the permitted protocols can also be selected in the configuration of the RADIUS authentication. LCP negotiation is restarted with the permitted protocols if the RADIUS server does not support the negotiated protocol.

To access the PPP List, follow these steps:

☐ Open the `Configuration : Communication : RADIUS` dialog. The PPP parameters are located in the middle of the dialog:



Configure the following parameters:

- PPP operation:
  Enable PPP authentication by the RADIUS server. In order to accomplish this, switch the PP. Select either:
  – Exclusive: the internal user authentication is ignored and the configured RADIUS server performs authentication.
  – Activated: the internal user authentication is the default authentication method.
- PPP authentication protocols:
  Specify the security measures which apply when authenticating a remote station. If the remote station is an Internet provider, which needs to be called by the router, de-select all choices. If all are selected, the next method will be used for authentication, if the previous did not achieve authentication. If none are selected, no authentication is required from the remote station.

11.10PPPoE Servers

11.10.1Introduction

As the availability of DSL has become widespread, point-to-point protocol over Ethernet (PPPoE) clients have been extensively integrated into device operating systems. PPPoE clients can be used to ‘log on to the network’ as well as to manage access rights to services such as the Internet, e-mail or remote stations.

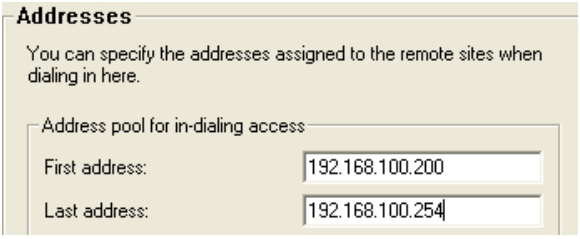
PPPoE: PPOE can only be used on one network segment

Because it is a layer 2 technology, PPPoE can be used exclusively within a network segment—i.e. it cannot be used across IP subnets. PPPoE connections cannot be established across network segment limits, such as via a router.

11.10.2Example Application

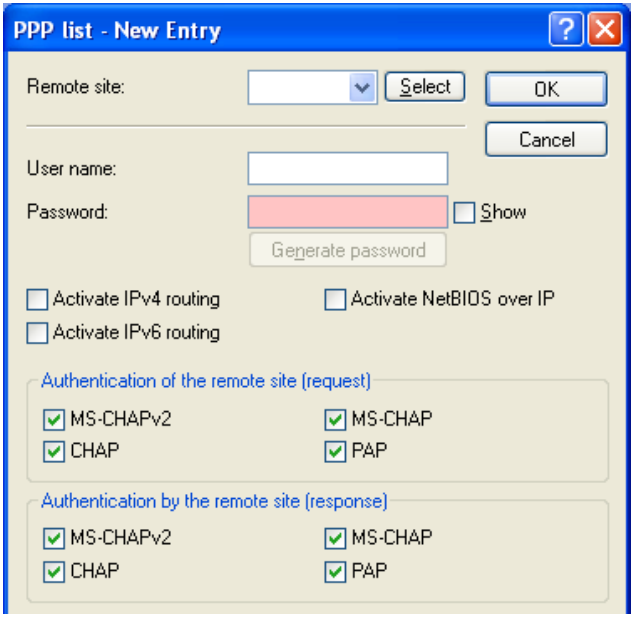
The following example illustrates the use of PPPoE:

- All employees in the Purchasing department need to first authenticate themselves to the OpenBAT device using PPoE (IP routing, PAP check) in order to access the Internet.
- All users in the LAN can directly access the OpenBAT device in its capacity as a router, firewall and gateway—i.e. there are no other routers between them. The computers in Purchasing are assigned an IP address from the address pool for dial-in addresses (192.168.100.200 - 192.168.100.254). This address range is configured in LANconfig in following dialog: `Configuration : TCP/IP :Addresses`.

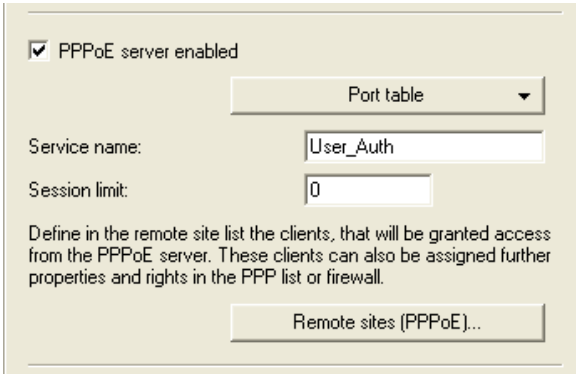


Note: The OpenBAT device itself is in a different IP Address range.

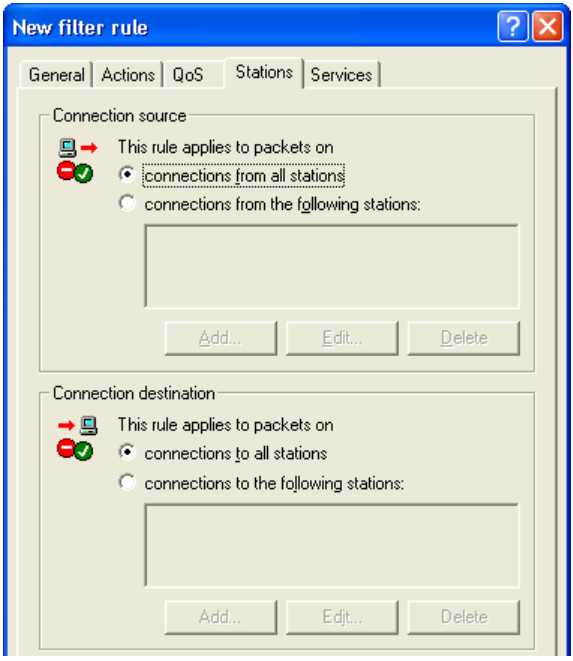
- To stop users from bypassing the authentication, a DENY ALL rule is defined in the firewall to stop local connections from being established.
- The user 'Purchasing' is then entered into the PPP list without a user name but with a password which is to be used by all staff members in the department, and authentication (encrypted) is set up as CHAP. Both IP routing and NetBIOS (Windows Networking) are to be activated for this PPP user. The "PPP list" can be accessed in LANconfig at: `Configuration : Communication : Protocols`.



- The PPPoe server is activated at: `Configuration : Communication : General` via the option "PPPoE server enabled".



- Additional limitations (e.g. permissible MAC addresses) are also defined in the PPPoE server. This example uses the existing entry 'DEFAULT' with the MAC address '00.00.00.00.00.00', thereby permitting all MAC addresses. Refer to the section ‘Configuring PPPoE’ (see on page 839).
- Finally, firewall rules are created to control the services that are made available to the employees in Purchasing (e.g. release of http and e-mail exclusively). The firewall rules table can be accessed in LANconfig in the `Configuration : Firewall/QoS : Rules` dialog by clicking ‘Rules...’:

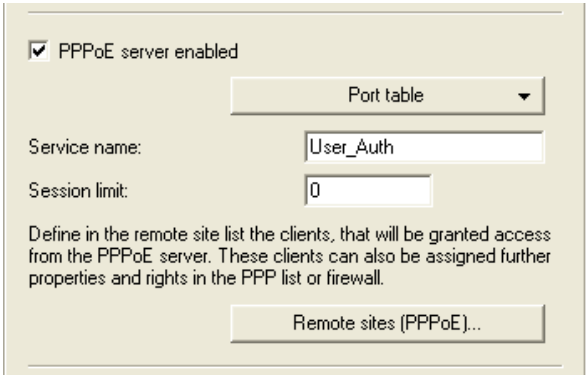


11.10.3Configuring PPPoE

To configure PPPoE, follow these steps:

General PPPoE Settings

☐ Navigate to the following dialog:`Configuration : Communication : General`.



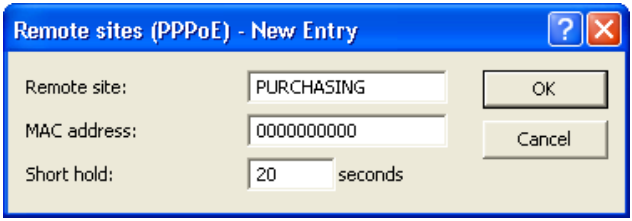
Enter settings for the following parameters:

- PPPoE server enabled:
  This selection enables and disables the PPPoE server.
- Service name:
  The name of the service offered. This enables a PPPoE client to select a certain PPPoE server that is entered for the client.
- Session limit:
  Indicate how often a client can be logged on simultaneously with the same MAC address. After the limit has been reached, the server stops responding to the client queries that are received. Default value is '1', maximum value '99'. A Session limit of '0' permits an unlimited number of sessions.

Adding Remote Sites (PPPoE)

☐ Navigate to the following dialog:`Configuration : Communication : General` and click "Remote sites (PPPoE)".

☐ In the ‘Remote sites (PPPoE)’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following parameters:

- Remote site: The remote client’s PPP username.
- MAC address:
  If you specify a MAC address, the negotiation is terminated if the client logs on from a different MAC address. A MAC address of '000000000000' means that the client may log on with any MAC address.
- Short hold:
  The user's short hold time is set after the logon. If no entry exists, then the time belonging to user 'DEFAULT' is applied.

Note: In addition to this table, make an entry in the PPP table in which you enter the password, the rights (IP, IPX, NetBIOS) and other PPP parameters (LCP polling). The user can therefore also be authenticated using a RADIUS server. The "PPP list" can be accessed in LANconfig at: `Configuration : Communication : Protocols`.

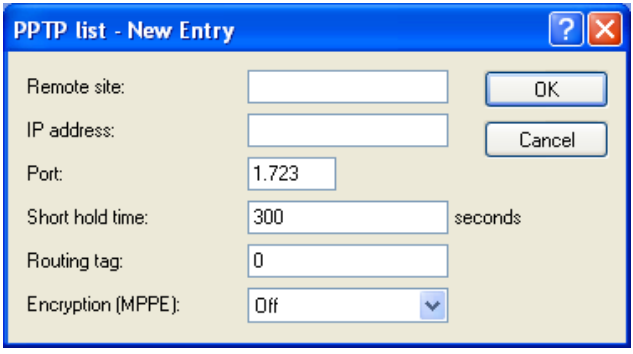
11.11DSL Dial-in over PPTP

Some DSL providers enable dial-in using the Point-to-Point Tunnelling Protocol (PPTP) instead of PPPoE. PPTP is an extension of PPP, partly developed by Microsoft. With PPTP it is possible to build up a ‘tunnel’ over IP networks to a remote station. A tunnel is a logical, shielded connection that secures the transferred data from unauthorized access, using the RC4 encoding algorithm.

The OpenBAT device can be configured for PPTP using the Setup Wizard, by selecting "Set up Internet access" and following the steps in that wizard. You can also manually configure PPTP, as follows:

☐ Navigate to the following dialog:`Configuration : Communication : Protocols` and click "PPTP list".

☐ In the "PPTP list", click "Add" to open the following dialog.



PPTP negotiation is configured using the following parameters:

- Remote site:
  The name of the remote station, which corresponds to an entry in the list of remote sites (see on page 798).
- IP address:
  The IP address of the PPTP gateway, often the address of the DSL modem.

- Port:
  The port the PPTP protocol runs on. For conformity with the protocol standard enter the port '1,723'.
- Short hold time:
  The time, in seconds, after which the connection should be closed if no data has been transferred. The value 9999 is used to establish an immediate connection of unlimited duration.
- Routing tag:
  This is used to evaluate the route of the respective PPTP server. This can be useful when running some PPTP ADSL modems, for example, those with the same IP address on different DSL ports.
- Encryption (MPPE):
  If you intend to secure the PPTP negotiation using the Microsoft Point-To-Point Encryption (MPPE) protocol (which also must be supported by the remote station), enter here the strength of the encryption.

11.12 Keep Alive: Extended Connections for Flat Rates

Flat rates refer to connection fees that are not charged according to connection time but at a fixed price for fixed periods. Setting up a new connection is not worthwhile for flat rates

The keep-alive function of the OpenBAT device can be configured so that connections are re-established when the remote station has disconnected them.

The keep-alive function is activated by setting the "Short hold time" parameter for remote sites (peers) (see on page 798) Do one of the following:

- 0 seconds: The OpenBAT device will not independently break the connection However, connections interrupted by the remote site are not automatically re-established if this value is used.
- 9999 seconds: The OpenBAT device automatically reestablishes the connection after every disconnection. In addition, the connection is reestablished after a reboot of the OpenBAT device.

11.13Revised flow control

The flow control can be configured in the Setup menu and viewed in the Status section of the mode (symmetrical, asymmetrical).

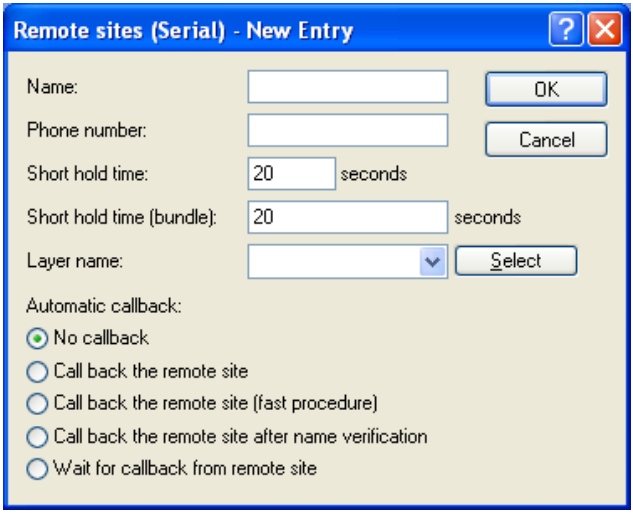
```
Setup : Interfaces : Ethernet-ports : Flow control
Setup : Interfaces : LAN-Interfaces : Flow control
```

11.14Callback Functions

Callback functions can be configured in LANconfig in the ‘Remote sites (Serial)’ dialog. To access this dialog:

☐ Navigate to the following dialog:`Configuration : Communication :Remote Sites` and click "Remote sites (Serial)".

☐ In the "Remote sites (Serial)" window, either add a new entry, or select and edit an existing entry:



11.14.1 Callback for Microsoft CBCP

For the Microsoft callback control protocol (CBCP), there can be various callback responses:

- the device called does not call back
- the device called allows the caller to specify the callback number
- the device called knows the callback numbers and calls these numbers exclusively

Via CBCP, it is possible to establish a connection to a OpenBAT device from a PC running the Windows operating system and to be called back by this PC. Three possible settings are selected in the remote sites list via the callback entry as well as the calling number entry.

No Callback

Automatic callback is set to ‘No callback’ (or set to ‘Off’ in WEBconfig or in the console).

Callback Number Specified by Caller

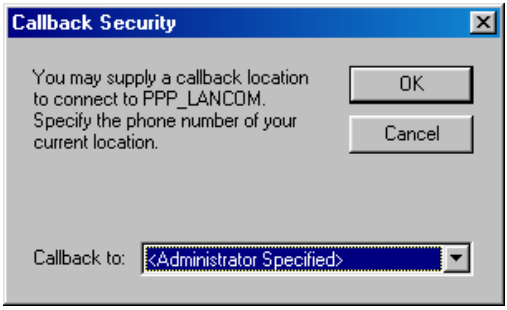
- ☐ ‘Automatic callback’ is set to 'Call back the remote site after name verification', or needs to have the value 'Name' in WEBconfig or in the console.
- ☐ No ‘Phone number’ setting may be specified.

After the authentication, an input dialog appears on the caller's screen in Windows that requests the telephone number of the PC.

The OpenBAT device determines the callback number.

- ☐ "Automatic callback" must be set to "Call back the remote site after name verification" (or needs to have the value "Name" in WEBconfig or in the console).
- ☐ One ‘Phone number’ value needs to be specified.

Some Windows versions (especially Windows 98) prompt the user to confirm the callback to the telephone number stored in the OpenBAT device ("Administrator Specified") with an input dialog. Other Windows versions inform the user that the PC is waiting for the callback from the OpenBAT device.



The callback to a Windows workstation occurs approximately 15 seconds after the first connection has been dropped. This time setting cannot be decreased since it is a Windows default setting.

11.14.2Fast Callback

Fast callback is ideal if two OpenBAT devices are to communicate with one another via callback.

In the device that is to be called back:

☐ Set "Automatic callback" to "Wait for callback from remote site" (or "Looser" when configuring via WEBconfig, terminal program or Telnet).

In the remote site (i.e., the callback party):

☐ Set "Automatic callback" to "Call back the remote site (fast procedure)" (or "fast" when configuring via WEBconfig, terminal program or Telnet).

☐ Specify one "Phone number" value.

Note: For fast callback using this method, keep up to date the number list for answering calls at both ends.

11.14.3 Callback via RFC 1570 (PPP LCP Extensions)

Callback via 1570 is the standard method for calling back routers from other manufacturers. This protocol extension describes five possibilities for requesting a call back. All versions are accepted by the OpenBAT device. The procedure is always the same: The OpenBAT device drops the connection after authenticating the remote station and then calls back the station a few seconds later.

To configure this version of callback, set "Automatic callback" to "Call back the remote site" (or select "Auto" in WEBconfig, the terminal program, or Telnet).

Note: For callback as per PPP, keep up to date the number list for answering calls in the OpenBAT device.

11.14.4 Overview of WEBconfig, Terminalprogram and Telnet

The following options are available in the peer list under WEBconfig and terminal program/telnet for the callback function:

Setting	Description
"Off"	No callback occurs.
"Auto"	The remote station will be called back if so specified in the peer list. Initially, the call is denied; as soon as the channel is clear again, the remote station is called back (duration is approximately 8 seconds). If the remote station is not found in the numerical list, it is first accepted as the DEFAULT remote station, and the callback is negotiated during the protocol negotiation. A charge of one unit is incurred.
"Name"	Before a callback occurs, a protocol negotiation is performed—even when the remote station was found in the numerical list (e.g. for computers with Windows having direct dialing on the device). Here minor charges result.
"fast"	When the remote station is found in the numerical list, a quick callback is carried out, i.e., the OpenBAT device sends a special signal to the remote station and calls back immediately when the channel is clear again. After approximately 2 seconds, the connection is established. If the remote station does not take back the call immediately after the signal, then after 2 seconds the situation reverts back to normal callback procedures (duration is once again approximately 8 seconds). This process is exclusively available for DSS1 connections.
Looser	Use this option when a callback is expected from the remote station. This setting carries out two functions simultaneously. First, it takes back a custom connection setup when there is an incoming call from the called remote station. Second, the function is activated with this setting to be able to react to the rapid callback procedure. Thus, in order to be able to use rapid callback, the caller needs to be in the "Looser" mode while the party being called needs to discontinue callback with "fast".

Note:

- The setting "Name" offers heightened security when an entry is made into the number list as well as the PPP list. The setting "fast" discovers the fastest callback method between two Hirschmann routers.
- With Windows remote stations, the "Name" setting needs to be selected.

11.15Operating a modem over the serial interface

Internationally, analog telephone connections are common in the business world. The operation of international networks places particular demands on remote maintenance options and for high-availability of the gateways. Apart from conventional analog telephone lines, mobile telephone networks such as GSM or GPRS may, in certain cases, represent the single way of providing remote maintenance without broadband or other cabled access.

In response to these requirements, OpenBATs with a serial interface can present an additional WAN interface, that is accessible via analog modems, GSM or GPRS. The following functions are available with a suitable modem in combination with a modem adapter:

- Internet access via modem with all of the router functions such as firewall, automatic connection establishment and termination, etc.
- Remote maintenance (e.g. dial-in to international sites)
- Backup connection (e.g. high-availability through GSM/GPRS modem connection)

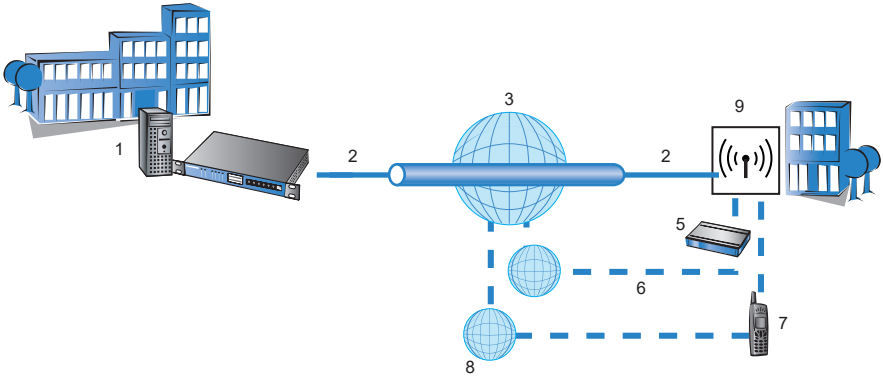


Figure 122:Operating a modem over the serial interface

1: Headquarters	6: Analog phone line
2: DSL	7: Modem (Global System for Mobile Communications (GSM)/General Packet Radio Service (GPRS))

3: Internet provider	8: GSM/GPRS
4: Secure connection	9: OpenBAT Device
5: Modem (analog)	–

11.15.1System Requirements

The following are required to set up a backup connection over the serial interface:

- A OpenBAT device with serial configuration interface and support for the modem adapter kit.
- LANconfig software (alternatively a web browser or CLI program)
- Serial configuration cable (supplied with the device)
- Analog modem, Hayes compatible, with access to a suitable analog telephone connection (D-sub9 or D-sub25 connector)
- Modem adapter to connect the modem over the serial configuration cable

11.15.2Installation

Perform the installation by connecting the modem to the serial configuration interface of the OpenBAT device, using a modem adapter.

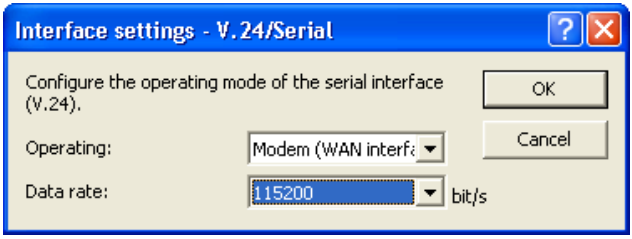
Note: Familiarize yourself with the contact assignments of the OpenBAT device (see on page 861).

11.15.3 Configuring the serial interface for modem operation

The operation of the serial interface requires the operating mode and bit rate to be set. To access these serial interface parameters:

☐ Navigate to the following dialog: `Configuration : Interfaces : WAN`.

☐ Click "Interface settings" and select "V.24/Serial".



In the 'Interface settings -V2.4/Serial' dialog, configure the following settings:

- Operating mode:
  Select one of the following settings:
  – Outband: the serial interface is used exclusively for configuration with a terminal program.
  – Modem: the device attempts to find a modem connected to the serial interface. If this is successful then the modem can be used as an additional WAN interface. If a computer running a terminal program is detected, then the device automatically switches the interface to outband mode.
- Data rate:
  the maximum bitrate supported by the modem. The serial interfaces of OpenBAT devices support data rates of 19,200 bps, 38,400 bps, 57,600 bps up to a maximum of 115,200 bps.

Note: While a OpenBAT device is set to "Modem" operating mode, a terminal program operating over the serial interface will display the AT commands that the OpenBAT device transmits while attempting to identify a connected modem. In the terminal program, press the return key repeatedly until the modem identification is interrupted, and start the configuration session.

11.15.4 Configuring Modem Parameters

The operation of a modem at the serial interface is configured using the following WAN and Modem interface settings.

☐ Navigate to the following dialog: `Configuration : Interfaces : WAN`, to configure the following parameters:

- Request modem ID (default = 16)
- Reset command (default = &F)
- Initialize command (default = L0X1M1S0=0)
  - L0: Loudspeaker quiet
  - X1: Operation at an extension
  - M1: Loudspeaker on while connecting
  S0=0: Disable auto answering
- Deactivate modem echo (default = E0)

☐ Navigate to the following dialog: `Configuration : Interfaces : Modem`, to configure the following parameters:

- AT polling cycle time (default = 1 second)
- AT polling count (default = 5)
- Ring count (default = 1)
- Initialize answer command
- Answer command (default = A)
- Initialize dial command
- Dial command (default = DT)
- Escape sequence—to terminate data phase response to return to command phase (default = +++)
- Wait after escape sequence (default = 1000 ms)
- Disconnect command (Default = H)

Note: The modem parameters are set with values that should suit most modems. Changes are usually not necessary. Refer to the documentation for your modem for settings that vary from these.

Configuring a GPRS Backup Connection

If the connection is to use a GPRS-capable modem at the serial interface, you will need the APN name and the dial-up telephone number. The following init-strings for the configuration apply to T-Mobile and Vodafone:

- T-Mobile:

Init-string:

```
L0X1M1S0=0+CGDCONT=1, "IP", "internet.t-d1.de"
```

Dial-up number:

```
*99#
```

- Vodaphone:

Init-string:

```
L0X1M1S0=0+CGDCONT=1, "IP", "web.vodafone.de"
```

Dial-up number:

`*99#` or `*99***1#`

Entering Special Characters in the Console

For a GPRS dial-up, the initialization strings require the entry of inverted commas and equal signs. Certain special characters can be correspondingly marked with a leading backslash:

- *
- "
- =
- space

Example:

```
+cgdcont\=1,\"IP\",\"internet.t-d1.de\"
```

As an alternative, the entire command sequence can be enclosed within inverted commas. In this case, those inverted commas which are inside the surrounding inverted commas needs to be preceded by a backslash:

Example:

```
”+cgdcont=1,\”IP\”,\”internet.t-d1.de\””
```

11.15.5Direct Entry of AT Commands

The following command allows you to use Telnet to send a character string directly to a modem that is connected to the OpenBAT device:

```
sendserial "AT..."
```

This function allows you to send any AT commands to the modem.

Note: Sending AT commands is possible exclusively in the internal modem state "idle" or "Modem ready." The responses can be found in the serial trace.

11.15.6Statistics

Statistics about activities of the serial interface can be accessed with a terminal program or Telnet under:

```
Status/Modem-Status
```

The statistics show the following states:

- the type of modem identified
- the status of its last connection, e.g. the transfer rate, the transfer protocol used or the exception-detection method used
- internal state of modem management, for example:
  - Discovery
  - interface deactivated
  - modem initialization
  - modem ready
  - Connection setup
  - modem in data mode

  These messages may be very helpful for debugging purposes.

11.15.7Trace Output

The following command allows you to start the trace output for the serial interface in a Telnet session when a OpenBAT device has a modem connected:

```
trace + serial
```

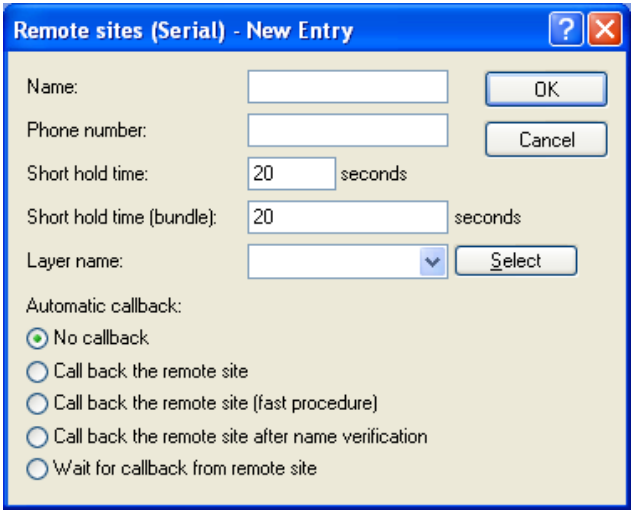
The output shows all messages exchanged up until the establishment of data transfer between the modem and the OpenBAT device.

11.15.8 Configuring Remote Sites for V.24 WAN Interfaces

To establish a connection to a remote station via the modem connected to the serial interface, create a corresponding entry in the remote sites (serial) list (see on page 798). To create a remote site list entry for a serial connection, follow these steps:

☐ Navigate to the following dialog: `Configuration : Communication :Remote Sites` and click "Remote sites (Serial)".

☐ In the 'Remote sites (Serial)' window, click 'Add...' to open the 'New Entry' dialog:



Configure the following settings for a serial connection:

- Name:
  Name of the remote site.
- Telephone number:
  The telephone number that reaches the remote site. The field can be left empty if calls are to be received exclusively.

- Short Hold time:
  This time defines how long a connection is kept active even if no more data is being transferred. If a zero is entered, the connection will not be interrupted automatically. A short hold time of ’9999’ means that the connection is held open indefinitely. If it is interrupted, then the connection will be actively opened up again. This behavior is known as keep alive.
- Short hold time (bundle): This is ignored
- Layer name:
  Select 'V.24_DEF' for the connection over the serial WAN interface. The layer is preset and does not need further configuration. The layer 'V.24_DEF' uses the following settings:
  – Encapsulation: Transparent
  – Layer 3: APPP (asynchronous PPP)
  – Layer 2: Transparent
  – Options: none

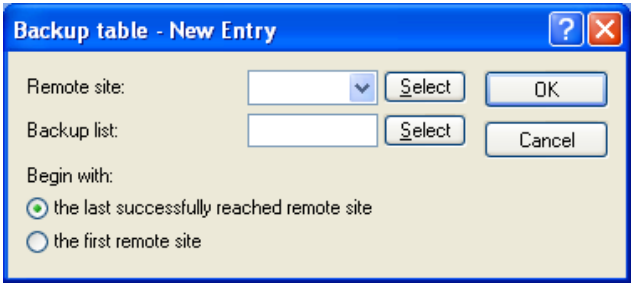
After an entry in the remote site (serial) list has been generated for the WAN interface, this remote station can be used just like any other for routing and WAN connections.

11.15.9 Configuring a Backup Connection on the Serial Interface

The configuration of a backup connection via a modem at the serial interface includes the following configuration entries:

☐ a dial-up peer station in the ‘Remote sites (Serial)’ table (see on page 798)

☐ a backup remote station entry in the "Backup table". Access this table at `Configuration : Communication : Call Management`.

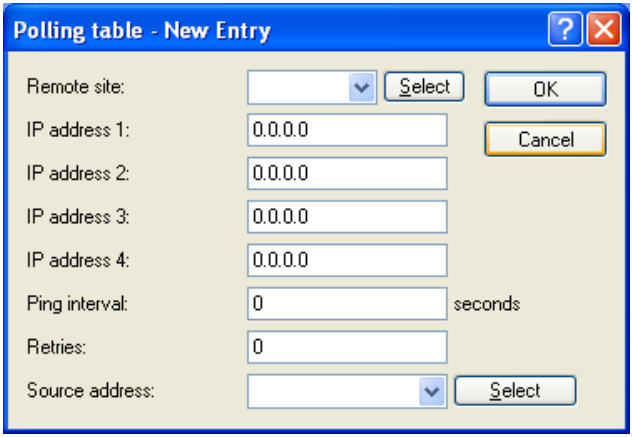


For each entry, configure the following parameters:

- Remote site:
  The remote site that is to be called by the modem at the serial interface.
- Backup list:
  The backup remote stations. Use exactly the same names that have been entered in the list of remote sites. Separate the individual remote stations with semicolons.
- Begin with:
  The order in which remote stations in the backup list are called.

☐ an entry in the ‘Polling table’ may be needed if the link to the remote station to be backed up cannot be checked by LCP polling (with PPP exclusively). This involves assigning the remote site with an IP address that can be regularly tested with a ping command. The IP address should typically be a computer directly at the opposite end of the connection being tested, e.g. a DNS server in your provider's network.

In the `Configuration : Communication : Remote Sites` dialog, click "Polling table".



For each entry, configure the following parameters:

- Remote site:
  The remote site that is to be called by the modem at the serial interface.
- IP address 1...4:
  A list of up to 4 IP addresses that will be pinged in sequence to check the connection state of the remote site. The connection is evaluated as intact as long as at least one specified IP address can be reached successfully. Select IP addresses that are continuously reachable. Otherwise, there will be needless and possibly costly backup connections.
- Ping interval:
  The interval, in seconds, between pings. If you set the ping interval and the number of retries to 0, defaults will be used to check the connection.

- Retries:
  The number of retries in case there is no response to a ping. Retries are sent once per second. The connection will be terminated if no response is received. If you set this value and the ping interval to 0, defaults will be used to check the connection.
- Source IP address:
  An optional source address that can be used instead of the source address, which is otherwise obtained automatically for the respective destination address. When loopback addresses are configured, they can be used as source address here.

11.15.10 Contact Assignment of Modem Connectors

Device signal	D-Sub9 plug	Device or modem signal	D-Sub9 plug
TxD	3	RxD	2
RxD	2	TxD	3
RTS	7	CTS	8
CTS	8	RTS	7
DTR	4	DCD	1
DCD	1	DTR	4
GND	5	GND	5

11.16 Manual Definition of the MTU

Many Internet providers operate their own backbone, but their customers dial in to the network over the access nodes of third-party telecommunications providers. This "two-stage" dial-in procedure can lead to problems with the resulting data rate:

- When dialing into the nodes of Deutsche Telekom, for example, a OpenBAT device negotiates a permissible maximum transmission unit (MTU), which defines the greatest possible size of unfragmented data packet. This MTU is then also used by the OpenBAT device.
- When the data packets are forwarded to the actual provider, an additional header is added that again increases the size of the data packets. For the data packets to meet maximum size limits, they need to be fragmented into smaller units. This additional fragmentation can cause reduction in data-transfer speeds.

This situation can be avoided by entering a fixed MTU for each remote site.

11.16.1 Configuring the MTU

Enter an MTU setting for remote sites using WEBconfig as follows:

☐ Navigate to the following dialog:

`Hirschmann Menu tree : Setup : WAN : MTU-List`

Configure the following parameters for each MTU entry:

- Remote site: the name of the device in the remote sites list.
- MTU: the maximum size, in bytes, of a data packet that can be transmitted over the connection to the remote site.

11.16.2Statistics

To view MTU statistics in WEBconfig, navigate to the following location:

`Hirschmann Menu tree : Status : WAN : MTU`

The table is partially dynamic and begins with 16 entries. It includes two columns in which the device name and the MTU are stored.

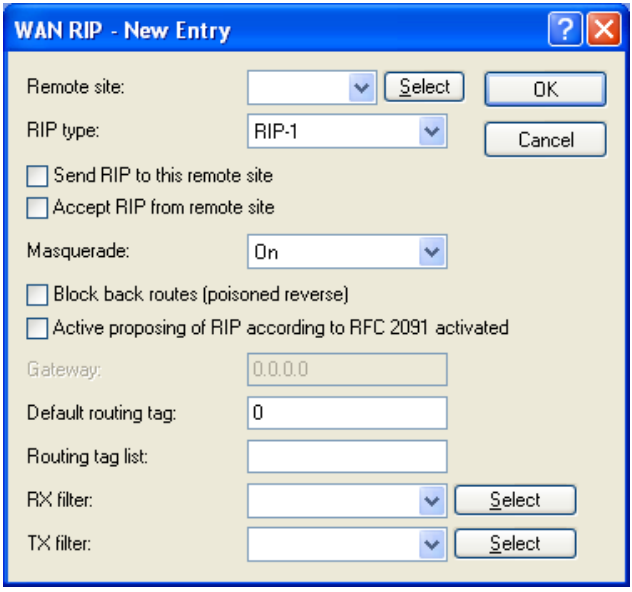
Note: MTU lists and MTU statistics are available exclusively for devices with a DSL or ADSL interface.

11.17WAN RIP

To enable routes learned from RIP to be broadcast across the WAN, enter the respective remote sites into the WAN RIP table. To make an entry into the WAN RIP table, follow these steps:

☐ Open the `Configuration : IP Router : General` dialog and click ‘WAN RIP...’.

☐ In the ‘WAN RIP’ table, click ‘Add...’ to open the ‘New Entry‘ dialog:



Configure the following settings for each entry:

- Remote site:
  The name of the remote site.
- RIP type:
  The version of RIP used to propagate local routes.
- Send RIP to this remote site:
  Select this to enable the sending of RIP route data to the selected remote site.

- Accept RIP from remote site:
  Select this to enable the receipt of RIP route data from the selected remote site.
- Masquerade:
  This indicates whether or not masquerading is enabled on the connection and how it is implemented. This entry makes it possible to start WAN RIP even with an empty routing table. Settings include:
  – Auto: The masquerade type is taken from the routing table (value: 0). If there is no routing entry for the remote site, then masquerading is not performed.
  – On: All connections are masqueraded (value: 1).
  – Intranet: IP masquerading is used for connections from the intranet, connections from the DMZ pass through transparently (value: 2)
- Block back routes (poisoned reverse):
  When you select this, routes learned/received via this interface are marked as 'not reachable' and sent back with the hop count directly set to 16, the maximum count (see on page 778).
- Active proposing of RIP according to RFC 2091 activated:
  For active connections (according to RFC 2091), there is a fallback to 'normal' RIP according to RFC 2453: the fallback is initiated if the remote site does not answer after 10 retries of the first packet (10 retries last approximately 30 seconds).
- Gateway:
  If ‘Active proposing of RIP...’ is selected, the IP address of the RIP partner on the remote side of the WAN connection has to be entered as gateway. It is possible to enter 0.0.0.0 here if a PPP negotiation is established on the WAN connection and thereby the IP address of the remote site is transferred.
- Default routing tag:
  The column Default tag lists the valid ’Default routing tag’ for the WAN connection. All untagged routes are tagged with this tag when sent on the WAN.

- Routing tag list:
  A comma-separated list of the tags that are accepted on the interface. If this list is empty, then all tags are accepted. If at least one tag is in the list, then just the tags in this list are accepted. When sending tagged routes on the WAN, exclusively routes with valid tags are propagated. All learned routes from the WAN are treated internally as untagged routes and propagated on the LAN with the default tag (0). In the WAN, they are propagated with the tag with which they were learned.
- Rx/Tx filter:
  Select the filters to be used on receiving (RX) and transmitting (TX) RIP packets. Items in this list are taken from the ‘RIP Filter’ list (see on page 774).

11.18 The Rapid Spanning Tree Protocol

In networks with numerous switches and bridges, multiple physical connections can exist between two stations that are connected to the network. These redundant data paths are desirable because they can offer alternative paths to the desired destination if one network path ceases to operate. However, multiple connections can also create loops or cause network stations to receive duplicate frames. Both of these events negatively impact network performance.

The spanning tree protocol (STP) enables an analysis of the network at the layer 2 level and offers solutions for intelligent path selection between two network stations below the routing layer. By discovering redundant paths between network stations, STP builds a unique structure in which loops and duplicate packets can be avoided. STP sends Bridge Protocol Data Units (BPDUs) as a multicast to a specific MAC address. The BPDUs let STP discover redundant paths, as well as the distance and the data rate available on each connection. Using these values, STP calculates a priority (also called route or path costs) for each connection. Low-priority connections are disabled and thereby made unavailable to clients. By disabling all but the non-redundant connections between clients, the protocol builds a tree which unambiguously defines all of the connections that arise from a central switch (root bridge).

BPDUs are regularly transmitted over the network to check the availability of the connections. If a connection ceases to function, network analysis is triggered again, and network paths and their priorities are redefined. After initialization, all ports are initially in the “blocking” state, in which just BPDUs are transmitted. The ports subsequently switch to the states of ’listening’ and then ’learning’ before reaching ’forwarding’ which allows payload data to be exchanged via the ports.

11.18.1 Classic and Rapid Spanning Tree

The early version of the spanning-tree protocol (compliant with IEEE 802.1D)—here referred to as classic spanning tree—implemented topology changes very slowly after a connection break was detected. Depending on the complexity of the network, classic spanning tree protocol requires from 20 seconds to a minute to establish new routes. For many network services, a delay of this duration is unacceptable.

The spanning tree protocol was improved and published as the "rapid spanning tree protocol" (RSTP), initially as the IEE 802.1t/w standard and later as a part of the newly published IEEE 802.1D. The OpenBAT device supports both the classic and rapid versions of STP.

11.18.2RSTP Improvements

The primary aim of RSTP is to accelerate the activation of network paths after an active connection is lost. RSTP achieves this by dispensing with the states 'blocking' and 'listening' to reduce the time required to update the network paths to just a few seconds. In case of a network path disconnection, not all of the links are blocked until the new topology has been calculated. Instead, just the lost connections are unavailable for use. RSTP also allows a network administrator to edit network topology settings.

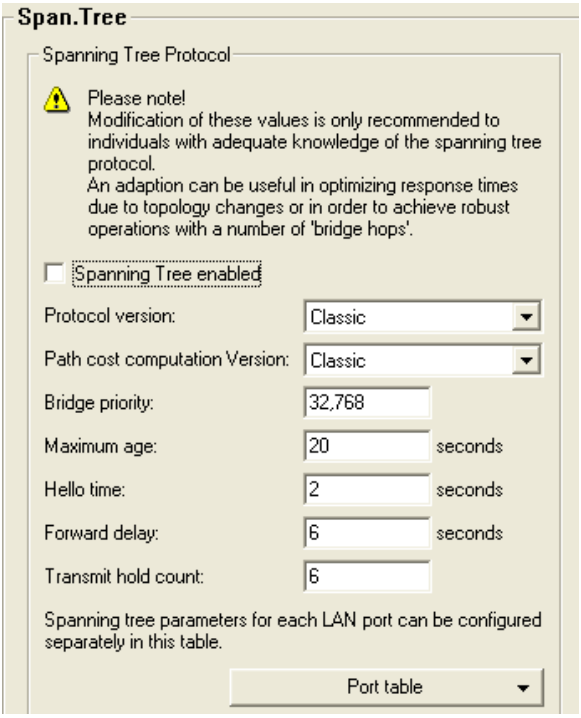
- A bridge port can be defined as an edge port. An edge port is the exclusive bridge port leading to the connected LAN segment. No additional bridges can be connected to the LAN segment, just workstations, servers, etc. Because these ports cannot lead to loops, they change immediately into the forwarding state without waiting for the network topology to be determined. However, RSTP continues to monitor these ports. If BPDUs are unexpectedly received at an edge port due to another bridge being connected to the LAN, the port automatically returns to its normal state.
- A bridge port can also operate as a point-to-point link. In this case the port is directly connected with an additional bridge. Since no additional stations can be positioned between the two bridges, the change into the forwarding state can take place faster.

In the ideal case, RSTP immediately resorts to familiar alternative network paths in case of connection loss.

11.18.3Configuring the Spanning Tree Protocol

To configure parameters for RSTP or STP functionality, make edits to both the general RSTP parameters and the port table, as follows:

☐ Navigate to the following dialog:`Configuration :Interfaces : Span.Tree`.

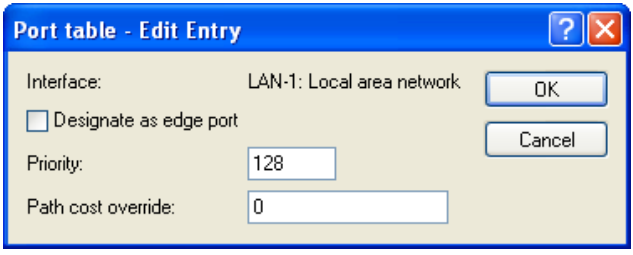


General STP settings:

- Spanning tree activated
  Toggles STP support on and off. When STP is turned off, a OpenBAT device does not send any spanning tree packets, and forwards received packets instead of processing them.
- Protocol version:
  Either the classic or RSTP version of the protocol.

- Path cost computation version:
  The version of spanning tree used to compute path costs, either the classic or RSTP version of the protocol.
- Bridge priority:
  The priority of the bridge in the LAN. This can influence which bridge should preferably be made root bridge by the protocol. To maintain compatibility with RSTP, this value should be adjusted in multiples of 4096, because RSTP uses the lower 12-bits of this 16-bit value for other purposes.
- Maximum age:
  This value defines the time (in seconds) after which a bridge drops messages received through Spanning Tree as "outdated." This parameter defines how quickly the Spanning Tree algorithm reacts to changes.
- Hello time:
  This parameter defines (in seconds) the intervals a device—selected to be the root bridge—sends Spanning Tree information into the LAN.
- Forwarding delay
  This time (in seconds) determines how much time needs to pass at a minimum before a Spanning Tree port can change the status (listening, learning, forwarding). When using RSTP the forwarding delay often has no effect, because RSTP has suitable mechanisms of its own to prompt a rapid switching into the forwarding state.
- Transmit hold count:
  The number of BPDUs which can be transmitted by RSTP before a one second pause commences. When using classical STP the transmit-hold count has no effect.

To make edits to Port table settings, click ‘Port table’ and select an available port (LAN, wireless LAN, point-to-point connections):



Configure the following parameters for each selected port:

- Designate as edge port:
  Marks the port as an edge port that is not connected to any other bridges, but exclusively to workstations or servers. Edge ports switch immediately into the forwarding state. Edge ports continue to be monitored by RSTP. If a port of this type receives BPDUs, then its status as an edge port is removed.
- Priority:
  The priority of the port. In the case of multiple network paths with identical path costs, the priority value decides which port is used. If priority values are identical, the port to be used is the first in the list. To maintain compatibility with RSTP, this value may be adjusted in steps of 16 because RSTP uses just the upper 4-bits of this 16-bit value.
- Path cost override:
  This setting controls the priority of paths with equal value. The value set here is used to make the selection instead of the computed path costs. A value of ‘0’ turns off this override.

11.18.4Status Reports for Spanning Tree

Current spanning tree values can be monitored via Telnet or WEBconfig. To view the status of spanning tree parameters, navigate to the following location in WEBconfig:

```
Hirschmann Menu tree : Status : LAN-Bridge-
Statistics : Spanning-Tree
```

General Status Information

The following spanning tree parameters are displayed:

- Bridge ID:
  The ID for the device that is being used by the spanning tree algorithm. It is composed of the user-defined priority (upper 16 bits) and the device MAC address (lower 48 bits).
- Bridge Priority:
  The priority of the LAN bridge within the root bridge detection process.
- Operating:
  Operating status of the port.
- Path Cost Computation:
  The protocol version currently set for computing path cost.
- Protocol Version:
  The protocol version currently set for determining network topology.
- Root Bridge:
  The ID for the device that is currently elected root bridge.
- Root Path Cost:
  The path costs of all hops added together in order to reach the root bridge from this device.
- Root Port:
  The port that can be used to reach the root bridge from this device. If the device itself is the root bridge, it is displayed with the special value '255'.

Port Table Information

The port table can be used to inspect the following values for all available ports (LAN, wireless LAN, point-to-point connections):

- Priority:
  The priority of this port taken from the port configuration.
- Status:
  The current status of the port:
  - disabled: no packets can be sent or received through this port. This occurs when the port has either been disabled manually or when it has a negative link status.
  - Listening: Intermediate state on the way to enabling. Only spanning tree packets are listened to, data packets are ignored and are also not forwarded to this port.
  - Learning: Further intermediate state. As opposed to "listening" additional MAC addresses from data packets entering this port are learned but data packets are still not forwarded.
  - Forwarding: Forwarding: the port is completely active, data packets are received and forwarded in both directions.
  - Blocking: Spanning tree has identified this port to be redundant and disabled it for data traffic.
- Root:
  The ID of the root bridge that can be reached through this port.
- Bridge:
  This is the ID of the bridge through which the root bridge can be reached.
- Path cost:
  The value is determined by the port technology (Ethernet, WLAN, etc.) and the bandwidth. Examples of values used are:

Transfer technology	Costs of Classic STP	Costs of RSTP
Ethernet 10 MBit	100	2000000
Ethernet 100 MBit	19	200000
Ethernet 1000 MBit	4	200000
WLAN 2 MBit	500	12500000
WLAN 11 MBit	140	4000000
WLAN 54 MBit	35	900000
WLAN 108 MBit	25	450000

Note: If path costs for a port were manually entered, then the configured value appears in this column.

RSTP Port Statistics Information

The RSTP port table can be used to inspect the following values for all available ports (LAN, wireless LAN, point-to-point connections):

- Role: Root or Non-root bridge.
- Learning: Port in learning state.
- Forwarding: Port in forwarding state.
- Edge Port: Port defined as an edge port.
- Protocol Version: Classic or Rapid.
- Costs: Setting for this port's cost

11.19The Action Table

The action table controls actions triggered when there is a change in the status of WAN connections. WAN connections include direct connections to an Internet provider. Every action is linked with a condition that describes the change in status of the WAN connection (establishment, termination, failure or establish failure). Actions include any of the commands available at the Telnet console. Furthermore, actions can transmit messages by e-mail or SYSLOG, send an http request, or transmit a DNS request. Variables allow information—for example, the current IP address, the name of the device, or an exception response—to be integrated into the action.

11.19.1Actions for Dynamic DNS

Systems with dynamic IP addresses can be made available for access via the WAN, for example via the Internet, by using the services of commercially available dynamic DNS servers. Servers offering these services can assign the current IP address of a device to its FQDN name (Fully Qualified Domain Name, e. g. “http://MyDevice.dynDNS.org”).

The advantage is obvious: If you wish to carry out remote maintenance via WEBconfig/http, for example, you need just the dynamic DNS name.

In order for the current IP address to match the DynDNS name at all times, the IP address recorded on the DynDNS server needs to be constantly updated. This change is triggered by a dynamic DNS client.

- The DynDNS server, maintained by a DynDNS service provider on the Internet, is in contact with the Internet DNS servers.
- The Dynamic DNS client can run on a workstation as a separate client program. Alternatively, a Dynamic DNS server is integrated into the OpenBAT device. It can make contact to any one of a number of dynamic-DNS service providers and, assuming that a user account has been set up, automatically update its current IP address for the DNS name translation.

Dynamic DNS Client on the Workstation

Dynamic DNS providers support a range of PC client programs that use various methods to determine the IP address currently assigned to a OpenBAT device. A change in IP address is communicated to the appropriate dynamic DNS server.

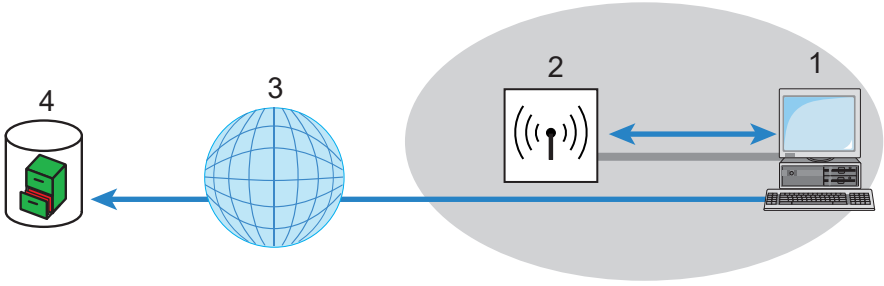
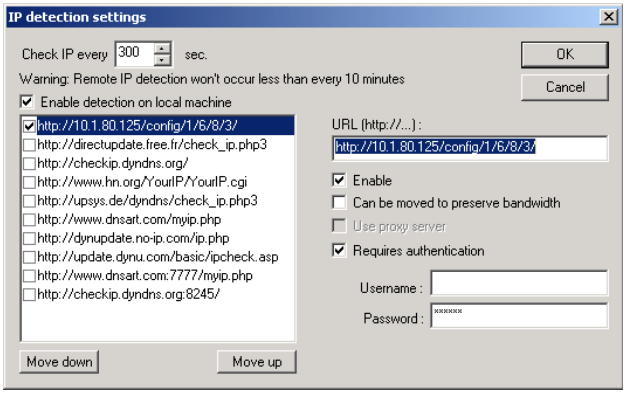


Figure 123:Dynamic DNS client on the workstation

1: PC with DynDNS client	3: Internet
2: OpenBAT Device	4: Server at DynDNS provider

The current WAN-side IP address of a device can be read from the following address and entered into a client program:

```
http://<Address of the Device>/config/1/6/8/3/
```



Note: The above screenshot illustrates how to access the WAN IP address on the WEB interface from an external application.

Dynamic DNS client in the OpenBATvia HTTP

Alternatively the OpenBAT device can directly transmit the present WAN IP to the DynDNS provider:

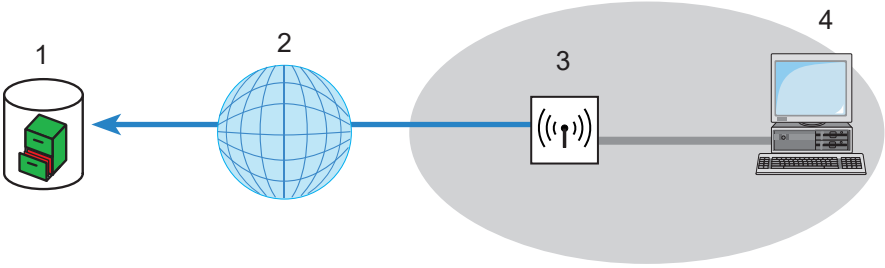


Figure 124:Transmitting the current WAN IP to the DynDNS provider directly

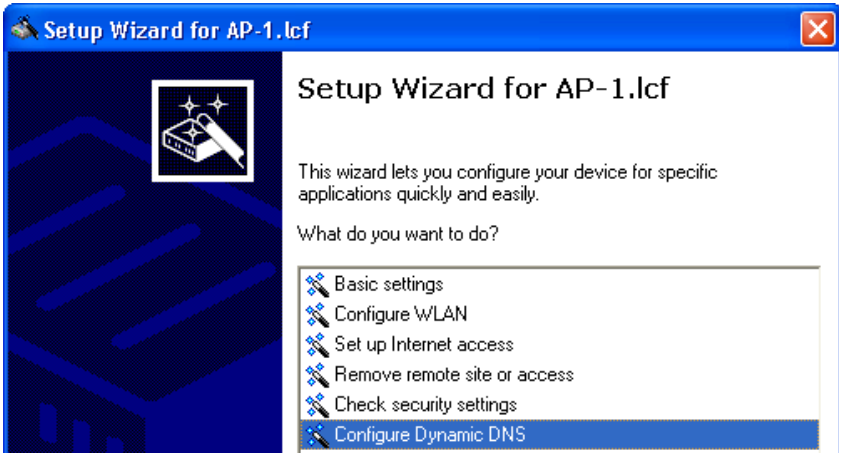
1: Server at DynDNS provider	3: OpenBAT Device
2: Internet	4: Client

An action is defined for this which, for example, automatically sends an http request to the DynDNS server each time a connection is established. The necessary information is transferred via the DynDNS account, thereby triggering an update of the registration. An http request of this type from DynDNS.org appears as follows:

```
http://Username:Password@members.dyndns.org/nic/
update?system=dyndns&hostname=%h&myip=%a
```

The host name of the action and the OpenBAT device's current IP address are sent to an account at DynDNS.org as specified by a username and password, and the appropriate entry is updated.

The settings necessary for this can be adjusted easily by using the Setup Wizard in LANconfig:



The Setup Wizard supplements the basic action with further provider-specific parameters, which are not described here. Apart from that, the Setup Wizard creates additional actions that control the OpenBAT device in case the update does not succeed the first time.

Dynamic DNS client in the OpenBAT device via HTTP

As an alternative to using a simple http request to update DynDNS information, some services make use of the GnuDIP protocol. The GnuDIP protocol is based on a challenge-response mechanism, as follows:

- The client opens the connection to the GnuDIP server.
- The server responds with a random value calculated for the session.

- The client uses the random value and the password to create a hash value, and returns it to the server.
- The server checks this hash value and reports its result by sending a number back to the client.

The GnuDIP protocol can exchange messages between the client and server either via a simple TCP connection (standard port 3495) or as a CGI script running on an Internet server. The version using an http request from a CGI script has two advantages: no additional ports on the server need to be opened for GnuDIP, and HTTPS helps protect against passive interception and offline dictionary attacks.

Requests to a GnuDIP server are triggered by the OpenBAT device with an action in the following form:

```
gnudip://<srv>[:port][/path]?<parameter>
```

The elements of the GnuDIP request include:

- <srv> – The GnuDIP server address.
- [:port] – Specifying the port is optional. If it is not defined, default values are taken instead (3945 for TCP, 80 or 443 for http/https).
- [/path] – Path information alone is required by http/https to define the location where the CGI script is stored.

The following parameters are extensions to the request:

- method=<tcp|http|https> – Selects the protocol to be used for the transmission between the GnuDIP server and client. Just one protocol can be selected here.
- user=<username> – Specifies the user name for the account on the GnuDIP server.
- pass=<password> – Specifies the password for the account on the GnuDIP server.
- domn=<domain> – Specifies the DNS domain containing the DynDNS entry.

- reqc=<0|1|2> – Defines the action that is triggered by the request. Action <0> sends the server a dedicated IP address that is to be used for the update. Action <1> deletes a DynDNS entry. Action <2> triggers an update, although no IP address is transmitted to the server. Instead, the server carries out the update with the IP address of the GnuDIP client.
- addr=<address> – Specifies the IP address that an action with the parameter <0> is to use for updating the DynDNS entry. If this is unspecified in a <0> action, the request is treated as a <2> action.

With the GnuDIP protocol, the host name that is to be registered corresponds to the user name sent to the server. If, for example, the username is "myserver" and the DNS domain is "mydomain.org," then the DNS name "myserver.mydomain.org' is registered.

For example, the following action executed via the GnuDIP protocol updates the DynDNS entry at a DynDNS provider with the current IP address of the OpenBAT device (%a) as soon as a connection is established:

```
gnudip://gnudipsrv?method=tcp
&user=myserver&domn=mydomain.org
&pass=password&reqc=0&addr=%a
```

Use the following action to delete a DynDNS entry, for example once the connection has been terminated:

```
gnudip://gnudipsrv?method=tcp
&user=myserver&domn=mydomain.org
&pass=password&reqc=1&addr=%a
```

In response to the request, the GnuDIP server returns one of the following values to the GnuDIP client (assuming that the connection between server and client was established):

- 0 – The DynDNS entry was updated successfully.
- 0:address – The DynDNS entry was successfully updated with the specified address
- 1 – Authentication at the GnuDIP server was unsuccessful.
- 2 – The DynDNS entry was deleted successfully.

These responses can be evaluated by the OpenBAT device's actions to trigger further actions if necessary.

11.19.2Action Examples

Broken Connection Alert as an SMS to a Mobile Telephone

The placeholder %t allows the current time of an event to be incorporated into a message. For example, an alert about the interruption of a WLAN connection can be sent by e-mail or as an SMS to a system administrator's mobile telephone.

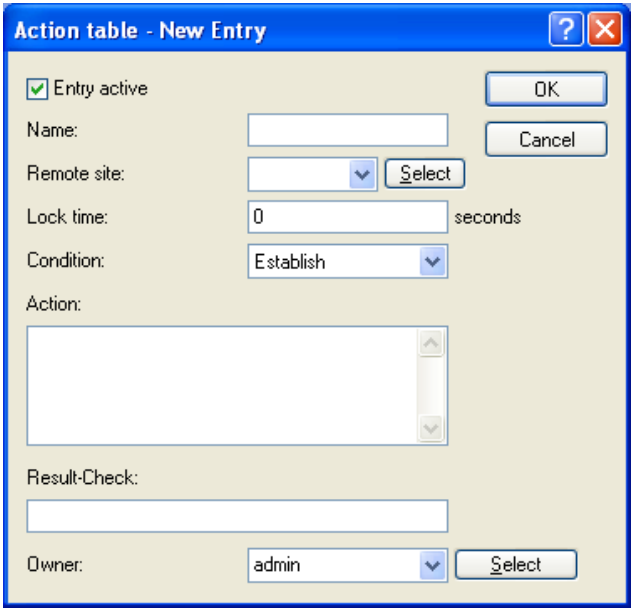
The following pre-conditions have to be met for messaging:

- The status of the WLAN connection is monitored, for example by means of "dead-peer-detection" (DPD).
- The OpenBAT device has to be configured as an NTP client in order to have the current system time.
- An SMTP account needs to be set up for transmitting e-mails.

After these requirements are met, messaging can be set up in the LANconfig software (for this example) by following these steps:

☐ Navigate to the following dialog:`Configuration : Communication : General` and click "Action table".

☐ Click "Add" to open the following dialog:



Configure the parameters in this dialog as follows:

- Name:
  Enter a name for the action.
- Remote site:
  Select the remote site.
- Lock time:
  Define an optional lock time to prevent the recurrence of this action for the specified time.
- Condition:
  Select ‘Broken’.
- Action:
  Configure the e-mail transmission, as follows:
  mailto:admin@mycompany.com?subject=WLAN connection broken at %t?body=WLAN
  connection to Subsidiary 1 was broken.

If the connection is broken, this action sends an e-mail to the administrator with the time of the event in the subject line.

Note:

- If the mail is sent to an appropriate Mail2SMS gateway the alert can be sent directly to a mobile telephone.
- For complex scenarios with several subsidiaries, each of the remote sites is given a corresponding entry in the central OpenBAT device. For monitoring the headquarters itself, an action is entered into a device at one of the branch offices. In this way the administrator receives an alert even if the WLAN gateway at the central location ceases to function.

Suppress Messaging in case of Re-connects with a DSL Connection

Some providers interrupt the DSL connection once every 24 hours. To avoid informing the administrator of these regular interruptions, messaging can be disabled at the time when the re-connect occurs.

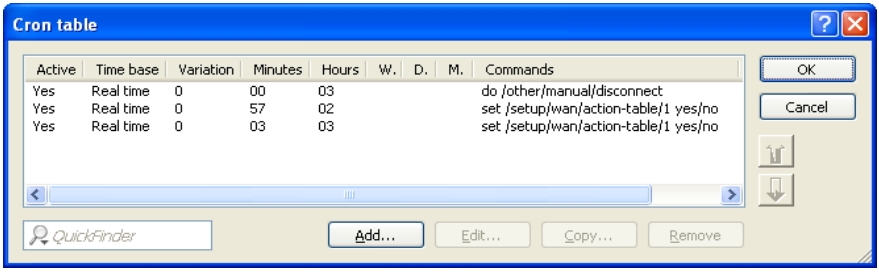
First of all an action is required to force the re-connect to occur at a fixed time; generally at night when the Internet connection is not in use. The entry defines, for example, 03:00h and the Internet connection is broken with the command:

```
do other/manual/disconnect internet
```

With two more Cron commands

```
set /setup/wan/action-table/1 yes/no
```

the corresponding entry in the action table is switched off three minutes before 03:00h and switched on again three minutes after 03:00h. The number 1 following the path to the action table is an index that stands for the first entry in the table.

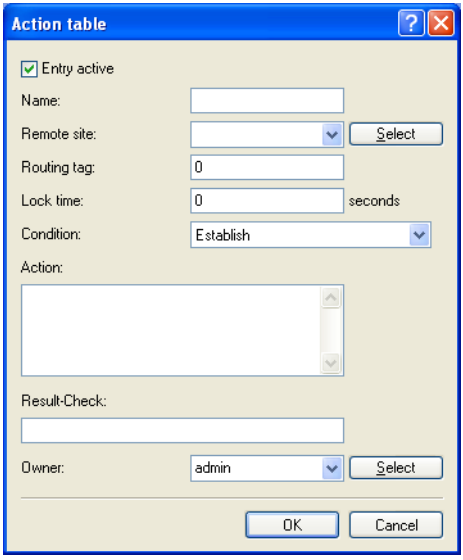


11.19.3Configuring action table entries

To configure entries for the Action table, follow these steps:

☐ Navigate to the following dialog:`Configuration : Communication : General` and click "Action table".

☐ Click "Add" to open the following dialog:



Configure the parameters in this dialog as follows:

- "Entry active": Activates or deactivates this entry.
- "Name": Action name. This name can be referenced with the wildcard `%h` (hostname) in the fields "Action" and "Result check".
- "Remote site": A change in status of this remote site triggers the action defined in this entry.
- "Routing tag": You can use the routing tag to specify which remote site is used when the action is applied. Of course, this site must be equipped with the appropriate routing tag.
- "Lock time": Prevents this action from being repeated within the period defined here in seconds (max. 10 characters).

- "Condition": Various changes in WAN-connection status can be set here, and the action is triggered when this condition occurs. Possible values are:
  - Establish – the action triggers if the device has successfully established the connection.
  - Disconnect without failure – the action triggers if the device itself terminates the connection (e.g. through manual disconnection or expiry of a holding time).
  - End (disconnect or broken) – the action triggers as soon as the connection terminates (regardless of the reason).
  - Broken with failure – this action is triggered on disconnects that were not initiated or expected by the device.
  - Establish failure – the action triggers if connection establishment was unsuccessful.
  - Volume budget exhausted – this action executes when the specified volume is reached.
  - Volume budget released – this action occurs after a state change from 'Volume exceeded' to 'Volume no longer exceeded', e.g. when you reset an exceeded volume or when the device enters a new billing period. If the volume has not been exceeded at the time of the reset, no action takes place.
- "Action": This item describes the action to be executed by the device when there is a change in the status of the WAN connection. You can specify only one action per entry (max. 250 characters). For each of the following values, the colon (:) is part of the action value. Possible values are:
  - `exec:` – This prefix initiates any command as you would enter it at the Telnet console. For example, the action `exec:do /o/m/d` terminates all current connections.
  - `dnscheck:` – This prefix initiates an IPv4 DSN name resolution. For example, the action `dnscheck:myserver.dyndns.org` requests the IPv4 address of the indicated server.
  - `dnscheck6:` – This prefix initiates an IPv6 DSN name resolution. For example, the action `dnscheck6:myserver.dyndns.org` requests the IPv6 address of the indicated server.

- `http:` – This prefix initiates an HTTP-get request. For example, you can use the following action to execute a DynDNS update at dyndns.org: The meaning of the place holders `%h` and `%a` is described below.

```
http://username:password@members.dyndns.org/nic/update?system=dyndns&hostname=%h&myip=%a
```

- `https:` – Like `http:`, except that the connection is encrypted.
- `gnudip:` – This prefix initiates a request to the corresponding DynDNS server via the GnuDIP protocol. For example, you can use the following action to use the GnuDIP protocol to execute a DynDNS update at a DynDNS provider: `gnudip://gnudipsrv?method=tcp&user=myserver&domn=mydomain.org&pass=password&reqc=0&addr=%a`. The meaning of the place holder `%a` is described below.
- `repeat:` – This prefix together with a time in seconds repeats all actions with the condition "Establish" as soon as the connection has been established. For example, the action `repeat 300` causes all of the establish actions to be repeated every 5 minutes.
- `mailto:` – This prefix causes an e-mail to be sent. For example, you can use the following action to send an e-mail to the system administrator as soon as a connection is terminated: `mailto:admin@mycompany.com?subject=VPN connection broken at %t?body=VPN connection to branch office 1 was broken`.

Optional variables for the actions:

- `%a` – WAN IPv4 address of the WAN connection relating to the action.
- `%z` – WAN IPv6 address of the WAN connection relating to the action.
- `%H` – Host name of the WAN connection relating to the action.
- `%h` – Like %H, except the hostname is in small letters.
- `%c` – Connection name of the WAN connection relating to the action.
- `%n` – Device name
- `%s` – Device serial number
- `%m` – Device MAC address (as in Sysinfo)

- `%t` – Time and date in the format `YYYY-MM-DD hh:mm:ss`
- `%e` – Description of the error that was reported when connection establishment failed.

Note: Using the variable `%z` requires that you specify the IPv6 address. If you do not supply an address, the device will not execute the script.

You can inspect the outcome of the actions in the field "Result check".

- "Result check": You can evaluate the result of the action here to determine the number of lines to be skipped in the processing of the action table. Possible values for the actions (max. 50 characters):
  - `contains=` – This prefix checks if the result of the action contains the defined string.
  - `isequal=` – This prefix checks if the result of the action is exactly equal to the defined string.
  - `?skipiftrue=` – This suffix skips the defined number of lines in the list of actions if the result of the "contains" or "isequal" query is TRUE.
  - `?skipiffalse=` – This suffix skips the defined number of lines in the list of actions if the result of the "contains" or "isequal" query is FALSE.

  The optional variables for the actions are the same as for the actions above.

  Example: A DNS check queries the IP address of an address in the form "myserver.dyndns.org". The check `contains=%a?skipiftrue=2` allows you to skip the two following entries in the action table if the IP address found by the DNS check agrees with the current IP address (%a) of the device.
- "Owner": Owner of the action. The exec actions are executed with the rights of the owner. If the owner does not have the necessary rights (e.g. administrators with write access) then the device cannot execute the action.

11.20 Using the LAN Serial Interface

In the IT field, COM port servers—also known as serial port servers—are devices that transport data between TCP and serial connections. There are many applications:

- Networking of devices with a serial interface but without a network interface.
- Remote maintenance of devices that can be configured only a a serial interface.
- Virtual extension of a serial connection between two devices with serial interfaces over a network.

Most OpenBAT devices feature a serial interface that can be used to carry out configurations or to connect to a modem. In some cases the interface is used for neither of these purposes, yet a COM port server is required in the vicinity of the device. In this case, the OpenBAT device can use its serial interface as a COM port server, thereby saving the cost of an external COM port server. If the OpenBAT device is used in an application that focuses on the serial configuration interfaces of other devices, additional serial interfaces can be provided by some models by employing suitable CardBus or USB adapters. This design enables multiple instances of the COM port server to operate in a single OpenBAT device.

11.20.1 Operating Modes

A COM port server has two operating modes:

- Server mode: The COM port server waits for requests from a defined TCP port to establish TCP connections. The mode can be used for remote maintenance, for example.
- Client mode: As soon as a device connected to the serial interface becomes active, the COM port client opens a TCP connection to a preset remote site. This operating mode is used, for example, for devices that have just one serial interface but require network access.

In both of these cases, a transparent connection is established between the serial interface and the TCP connection. Data packets received at the serial interface are forwarded to the TCP connection, and vice versa.

A common server-mode application is to install a virtual COM port driver at the remote site that connects to the COM port server. Drivers of this type allow applications running at the remote site to use the TCP connection as if it were an additional COM port. The IETF RFC 2217 standard describes the Telnet WILL/DO protocol extensions, which transmit the negotiations for the serial connection (bitrate, data and stop bits, handshake) to the COM port server. The use of this protocol is optional, so practical default values can be set in the COM port server.

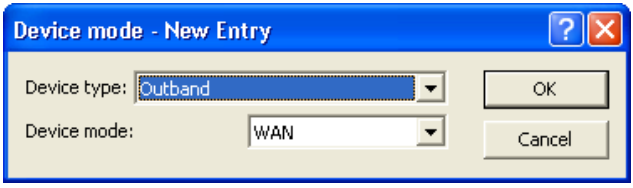
11.20.2 Configuring the Serial Interface

The "Device mode" table allows individual serial devices to be assigned to specific applications. When the device recognizes a hot-pluggable USB adapter, the device automatically creates a new entry for provided serial interfaces in this table. This automatic operation facilitates the configuration of the serial devices The built-in serial interface of the OpenBAT device is an exception; you must configure it manually.

To manually configure an entry for the Devices table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : Devices` and click "Device mode".

☐ In the ‘Device mode’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Select settings for the following parameters:

- Device type:
  The serial interface from the list of those available in the device.
- Device mode:
  The operating mode for the device. Values include:
  - WAN: The device ports can be used for operating a modem. The operating mode sets the device ports to serial interfaces.
  - COM port server: The outband interface can be used for device management.

  Note: Some devices support ‘COM port server’ device operating mode.

11.20.3Configuring the COM Port Server

Configuring the COM port server involves making entries in three tables:

- Device ports table
- Serial interface table
- Network interface table

What all three tables have in common is that a certain port at a serial interface is identified by the values for device type and port number. Because some serial devices such as a CardBus card have multiple ports, the port to be used needs to be specified explicitly. For a device with just one port, for example, a single serial configuration interface, the port number is set to zero.

Device Ports Table: Operational Settings

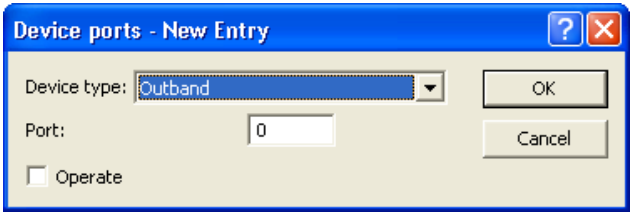
This table activates the COM port server at a port of a specified serial interface. Add an entry to this table to start a new instance of the COM port server. Delete an entry to delete the corresponding server instance. The switch Operating can be used to deactivate a server instance in the table.

When a server instance is created or activated, the other tables in the COM port configuration are searched for matching device type and port number values. If no suitable entry is found, the server instance takes workable default values.

To manually configure an entry for the Device Ports table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : Server` and click "Device ports".

☐ In the ‘Device ports’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following parameters:

- Device type:
  The serial interface from the list of those available in the device.
- Port:
  Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.
- Operate:
  Enables and disables the COM port server on the selected port of the selected interface.

Serial interface table: COM port settings

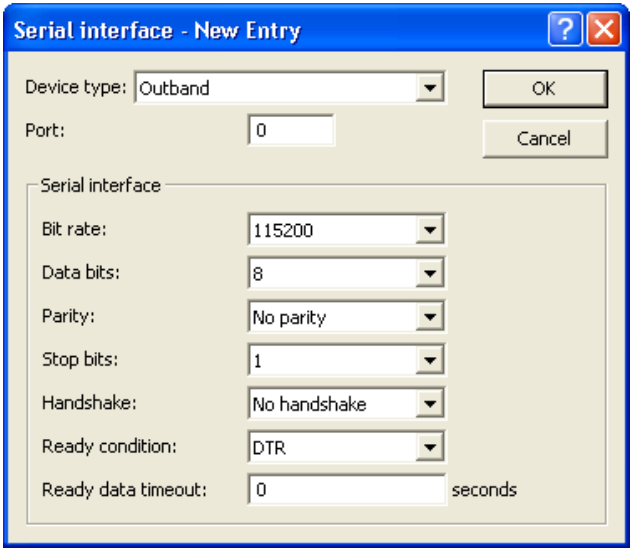
This table contains the settings for data transmission over the serial interface.

Note: All of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu in WEBconfig.

To manually configure an entry for the Serial Interface table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : Server` and click "Serial interface".

☐ In the ‘Serial interface’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following parameters:

- Device type:
  The serial interface from the list of those available in the device.
- Port:
  Some serial devices such as the CardBus have more than one serial port. Enter the number of the port on the serial interface that is to be used for the COM-port server.
- Bit rate:
  Bitrate used on the COM port. Values range from 110 to 230400 Bps.
- Data bits:
  Number of data bits—7 or 8.
- Parity:
  The checking technique used on the COM port. Values include no parity, odd or even.
- Stop bits:
  The number of stop bits—1 or 2.
- Handshake:
  The data-flow control used on the COM port—RTS/CTS (flow control) or no handshake.

- Ready conditions:
  A characteristic of a serial interface is the ready state. The COM port server does not forward data from serial to network side, unless it is in ready state. Furthermore the change-over from ready- to not-ready state in operating mode 'client' (which has to be set in the network table), is used for establishing/terminating a TCP connection. Currently there are two alternatives to recognize the ready state of the serial interface. This can be set using the parameter Ready condition.
  - DTR mode (default): The handshake line is monitored. The serial interface is regarded as ready, as long the DTR line is active.
  - Data mode: The ready state is expected after characters are received on the serial interface.

  If there are no characters received for the period of time set in Ready data timeout, the state falls back to 'not ready'. This mechanism can be switched off by setting the timeout value to 0. The serial interface is ready, if the ready condition option is set to ‘data’ and the timeout is set to ‘zero’.
- Ready data timeout:
  The timeout switches the port back to the not-ready status if data is not received within this time period. This function is deactivated when timeout is set to zero. In this case the port is ready if the data mode is selected.

Network interface table: Network settings

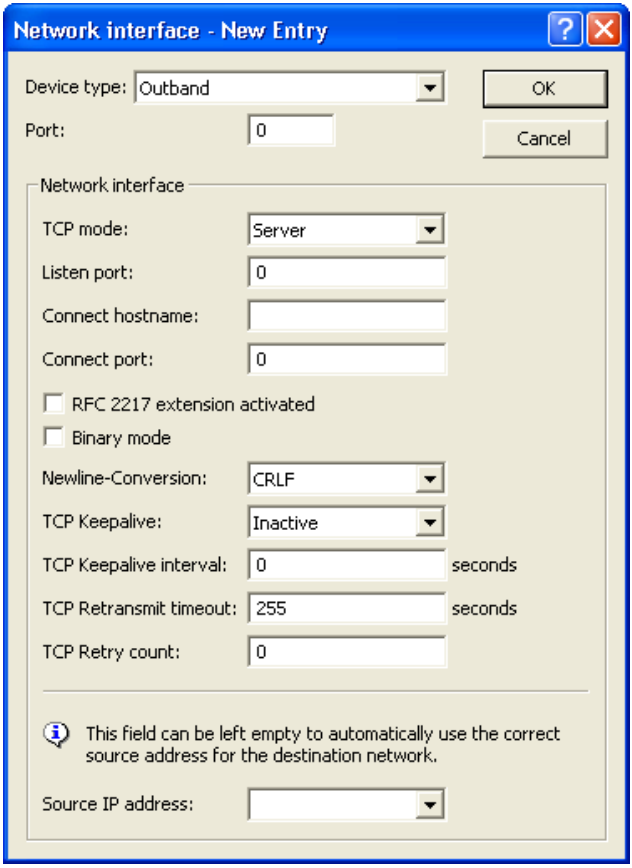
This table contains all settings that define the behavior of the COM port in the network.

Note: All of these parameters can be overwritten by the remote site if the RFC2217 negotiation is active. Current settings can be viewed in the status menu in WEBconfig.

To manually configure an entry for the Network Interface table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : Server` and click "Network interface".

☐ In the ‘Network interface’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following parameters:

- Device type:
  The serial interface from the list of those available in the device.
- Port:
  some serial devices such as a CardBus have more than one serial port. In this case, enter the number of the port that the COM port server uses on the serial interface

- TCP mode:
  Select a mode:
  - Server mode: Each instance of the COM port monitors the specified listen port for incoming TCP connections. Just one active connection is permitted per instance. All other connection requests are refused.
  - Client Mode: The instance attempts to establish a TCP connection via a defined port to the specified remote site, as soon as the port is ready. The TCP connection is closed again as soon as the port becomes unavailable.

  In each case, a OpenBAT device closes any open connections when the device is restarted.
- Listen port:
  The TCP port where the COM port in TCP server mode expects incoming connections.
- Connect hostname:
  The COM port in TCP client mode establishes a connection to this host as soon as the port is in "Ready" status.
- Connect port:
  The COM port in TCP client mode uses this TCP port to establish a connection as soon as the port is in "Ready" state.
- RFC 2217 extension activated:
  The RFC2217 extensions can be activated for both TCP modes. With these extensions activated, the OpenBAT device uses the IAC DO COM-PORT-OPTION sequence to signal that it will accept Telnet control sequences. The COM port subsequently works with the corresponding options; the configured default values are overwritten. The port also attempts to negotiate the local echo and line mode for Telnet. Using the RFC2217 extensions with incompatible remote sites is not recommended. Unexpected characters may be displayed at the remote site. A side effect of using the RFC2217 extensions may be that the port regularly carries out an alive check as Telnet NOPs are transmitted to the remote site.
- Binary mode:
  Serial data will be forwarded as binary. Thereby no CR/LF (Carriage Return / Line Feed) conversion occurs.

- Newline conversion:
  This defines which character sequence is sent to the serial port if a newline character is received in non-binary mode. The default setting (CRLF) will reproduce what was received over the TCP connection, but it is not necessarily the correct setting for all applications. For instance, some Unix serial consoles will interpret this sequence as an undesirable double linefeed, so a single linefeed or carriage return is more appropriate. If another LANconfig device's outbound port is attached to the serial port, either CRLF or CR will do, but not LF because carriage return characters are expected by a LANconfig for its auto-bauding feature.
- TCP Keepalive:
  When active, the TCP implementation will regularly send certain dummy packets to the remote site. These packets contain no payload data, but hinder firewalls and NAT gateways from discarding this connection since the connection still looks alive. In extension to RFC 1122, the TCP keepalive offers three modes of operation:
  - Inactive: No packets are sent during idle periods.
  - Active: Packets are regularly sent, but the lack of answers to these packets has no further effect. Connection entries in firewalls or NAT gateways will be kept alive, but the complete loss of the TCP connection will not be detected. This mode of operation is recommended for server operation.
  - Proactive: The TCP stack additionally expects answers to its keepalive packets and will report a broken TCP connection in case no answer is received after several attempts. The number of tries is the same as the "TCP Retry count" for data packets (see below).
- TCP Keepalive interval:
  Defines how often the TCP stack will transmit keepalive packets. A setting of 0 results in the internal default of 7200 seconds.
- TCP Retransmit timeout:
  Specifies the time after which a single retransmission is started. A value of 0 is equal to the default value (60 seconds). Note that the actual time until a connection is detected as broken is the sum of all retransmissions.

- TCP Retry count:
  This limits the total number of retransmits. A retry count of zero is equal to setting the default value of 5 retries.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination address. When loopback addresses are configured, they can be input here.

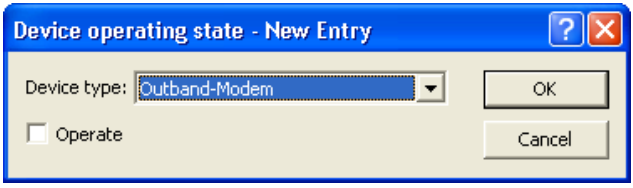
11.20.4WAN Device Configuration

The table with WAN devices is a status table. All HotPlug devices (connected via USB or CardBus) are automatically entered into this table.

To manually configure an entry for the Devices table, follow these steps:

☐ Navigate to the following dialog:`Configuration : COM Ports : WAN` and click "Device operating state".

☐ In the ‘Device operating state’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Select settings for the following parameters:

- **Device type:**
  The serial interface from the list of those available in the device.
- **Operate:**
  Enabled/disabled status of the device.

11.20.5Serial Connection Status Information

Various statistics and status values are recorded for every instance of the COM-port server. This includes data relating to:

- Network status
- COM port status
- Byte counters
- Serial port errors
- Connections

In addition, you can clear the content of all status tables.

All this data is available in Telnet. Navigate in WEBconfig to the following place:


```
HiLCOS Menu tree: Status : COM Ports
```

Network Status

This table contains information on current and recent TCP connections. Field values include:

- Device type:
  List of serial interfaces available in the device.
- Port number:
  The port number used for the COM port server on the serial interface.
- Connection status:
  Possible values include:
  - Connected: An active connection exists (server or client mode).
  - Listening: This instance is working in server mode; no TCP connection is currently active.
  - Not listening: In server mode, the specified TCP port could not be reserved for inbound connections, e.g. because it is already occupied by another application.

  - Blank: This instance is working in client mode and the port is not ready. No TCP connection will be established now.
  - Transfer: The port has reached the 'ready' state; a connection is being established.

- Last error:
  In client mode this displays the reason for the last unsuccessful connection attempt. In server mode this value has no significance.
- Remote address:
  Displays the IP address of the remote site for a successful TCP connection.
- Local port:
  Displays the local TCP port used for a successful TCP connection.
- Remote port:
  Displays the remote TCP port used for a successful TCP connection.

COM Port Status

This table displays the serial port status and the settings currently used by this port.

- Device type: List of serial interfaces available in the device.
- Port number: The port number used for the COM port server on the serial interface.
- Port status: Possible values:
  - Not available: The serial port is currently not available to the COM port server, for example because the USB or CardBus adapter has been removed or because it is being used by other functions in the OpenBAT device.
  - Not ready: The serial port is available to the COM port server but is currently not ready for data transfer, for example because the DTR line is inactive. In the client state, no attempt is made to establish a connection as long as the port is in this state.
  - Ready: The serial port is available and ready for data transfer. In the client state, no attempt is made to establish a connection as long as the port is in this state.

Note: The port status is relevant in server mode, too. All TCP connection requests are accepted, although the COM port instance transfers data exclusively between the serial port and the network when the serial port has reached the "ready" state. The following columns display the settings that are currently in use on the serial port. These are either the values as configured or as set by the negotiations via the RFC2217 extensions.

- Bit rate: Bit rate used on the COM port.
- Data bits: Number of data bits.
- Parity: The checking technique used on the COM port.
- Stop bits: Number of stop bits.
- Handshake: The data-flow control used on the COM port.

Byte Counters

This table displays the inbound and outbound data packets at the serial port and on the network side.

Note: These values are not reset when the connection is opened or closed.

- Device type: List of serial interfaces available in the device.
- Port number: The port number used for the COM port server on the serial interface.
- Serial-Tx: Number of bytes sent over the serial interface.
- Serial-Rx: Number of bytes received over the serial interface.
- Network-Tx: Number of bytes sent to the network.
- Network-Rx: Number of bytes received from the network.

COM Port Errors

This table displays the anomalies on the serial port. These messages may indicate a broken cable or incorrect parameter settings in the configuration.

- Device type: List of serial interfaces available in the device.
- Port number: The port number used for the COM port server on the serial interface.
- Parity errors: A count of events caused by a checksum mismatch.
- Framing errors: Number of corrupted data packets.
- Rx Lost errors: The number of lost transmissions.

Connections

This table displays successful and unsuccessful TCP connections in both server mode and client mode.

- Device type: List of serial interfaces available in the device.
- Port number: The port number used for the COM port server on the serial interface.
- Server granted: Number of connections granted by the COM port server.
- Server rejected: Number of connections rejected by the COM port server.
- Client succeeded: Number of connections successfully established by the COM port client.
- Client DNS error: Number of connections that the COM port client could not establish due to DNS reasons.
- Client TCP error: Number of connections that the COM port client could not establish due to TCP reasons.
- Client remote disconnects: Number of connections where the COM port was disconnected from the remote site.

Delete Values

This action deletes all values in the status tables.

11.20.6CPM Port Adapters

Devices with serial interfaces can be connected to a OpenBAT device in the following ways:

Adapters	OpenBATs
COM-port adapters	All those with a serial configuration interface
USB serial adapter	All those with a USB interface
CardBus serial adapter	All those with a CardBus slot
Modem adapter	All those with a serial configuration interface

The COM port adapter needs to be a two-way D-sub plug with the following PIN assignment:

Pin	Signal	Signal	Pin
2	RxD	TxD	3
3	TxD	RxD	2
4	DTR	DSR	6
5	GND	GND	5
6	DSR	DTR	4
7	RTS	CTS	8
8	CTS	RTS	7

11.21IGMP Snooping

11.21.1Introduction

All OpenBAT devices feature a "LAN bridge," a software mechanism for transferring data between the Ethernet ports and the WLAN interfaces. In many ways the LAN bridge works like a switch. The core task of a switch, as opposed to a hub, is to forward packets to the specific port to which the relevant user is connected. Based on the incoming data packets, the switch automatically creates a table listing the senders' MAC addresses and their ports.

If the table contains the destination address for an incoming packet, the switch forwards the packet to the corresponding port. If the destination address is not in the table, the switch forwards the packet to all ports. That is to say, a switch can deliver a packet precisely provided that the destination address appeared earlier in a packet arriving at a certain port from the sender's address. However, broadcast or multicast packets can never be entered as a sender address into a packet, and so these packets end up being flooded to all ports.

This may be the correct action for broadcasts that are supposed to reach all available recipients, but it may not be the case for multicasts. Multicasts are usually aimed at a targeted group of recipients within a network, but not all of them. Example:

- Video streams are frequently transmitted as multicasts, but not all of the network stations are intended to receive that stream.
- Various applications in the medical field use multicasts to send data to certain terminal devices, but this data should not be available to all stations.

A LAN bridge in the OpenBAT device will have ports to which no multicast recipients are connected. While this "unnecessary" transmission of multicasts to ports without any receivers is not an error, it can impact overall performance:

- Many stations are unable to reject the unwanted multicasts in their hardware. Instead, the packets are forwarded to higher protocol layers, which leads to an increase in CPU load.
- WLANs are particularly susceptible to bandwidth restrictions due to multicasts if none of the associated WLAN clients want to receive the multicast.

The TCP/IP protocol suite defines the Internet Group Management Protocol (IGMP) that network stations can use to notify their router of their intention to receive certain IP multicasts. Stations carry out a multicast registration with their router to subscribe to certain multicast groups which deliver the relevant packets. IGMP makes use of "Join" messages and "Leave" messages to register and un-register as a multicast group member.

Note: Information describing which multicast groups a station can or should join is available from protocols other than IGMP.

As a layer-3 protocol, IGMP performs multicast guiding/routing for entire IP subnets. However, network devices such as bridges, switches or WLAN access points forward the packets exclusively via layer 2, meaning that IGMP itself does not help to further guide multicast traffic through this substructure. For this reason, the bridges use the multicast registrations between stations and routers to receive additional information for targeting the distribution of multicasts. IP multicasts merely need to be forwarded to an interface where a router is located that is capable of multicast routing, and therefore of forwarding multicasts to other IP subnets. This method is called IGMP snooping. The bridges, which normally use the MAC on layer 2 for packet forwarding, thus additionally use the layer 3 information in the IP multicast packets.

For more detailed description of the functions of IGMP snooping in a OpenBAT device, understand the following terms:

- A port is a "member" of a multicast group if at least one station connected to it wishes to receive the packets for a certain multicast address. Multicast registration can be dynamic via IGMP snooping or configured manually.
- A port is a "router port' if it is connected to a router that is capable of multicast routing and therefore of forwarding multicasts to other IP subnets.
- A multicast group is "unregistered" if none of the interfaces attached to the bridge is a member of this multicast group.

11.21.2IGMP Snooping Operation

Whenever a packet is received, the bridge initially determines whether it is a unicast, broadcast, or multicast packet. For broadcast and unicast packets, the bridge operates in the usual way, i.e. it floods to all ports or sends to a specific port based on the MAC table entry for the recipient.

Two types of IP multicast packet are differentiated (whereby packets which are truncated or contain an invalid checksum are discarded entirely):

- IGMP messages are handled in different ways depending on their content:
  - A 'Join' message results in the incoming port becoming a member of the respective multicast group. This message is forwarded to router ports exclusively.
  - Similarly, a 'Leave message' results in the incoming port being removed from the multicast group's member list. This message is also forwarded to router ports exclusively.

- An incoming IGMP query results in the port being marked as a router port. These messages are flooded to all interfaces.
- All other messages are flooded to all interfaces—no ports experience a change of state.

- If an IP multicast packet does not contain an IGMP message, the IP destination address is examined. Packets for the destination address ‘224.0.0.x’ are flooded to all ports because this is a ‘reserved’ range. For all other packets the destination address is looked up in the IGMP membership table:
  - If the address is found, the packet is forwarded according to the membership stored in the table.
  - If the address is not found, the packet may either be discarded, flooded to all ports, or forwarded exclusively to all router ports (depending on the configuration).

11.21.3IGMP snooping through multiple bridges

As described, IGMP snooping forwards incoming ‘Join’ or ‘Leave’ messages via router ports. In a structure with multiple bridges, initially none of the ports are router ports or members of a multicast group. If a station connected to the bridge registers with a multicast group, the port automatically becomes a member of this group. However, none of the ports are router ports at this point, so the ‘Join’ messages are not forwarded anywhere. Other bridges thus receive no information about the port's membership with the multicast group.

Consequently, bridges need to be equipped with router ports in order for membership information to be propagated. Because the ports of a bridge become router ports only in the case of IGMP queries, one of the multicast-capable routers in the network needs to take over the task of distributing the necessary IGMP queries throughout the network. This router is referred to as the IGMP querier. If the network does not contain a multicast router, the

OpenBAT access points are capable of simulating a querier. To avoid parallel queries arriving from various queriers, a querier will deactivate itself if it discovers another querier with a lower IP number. The distribution of IGMP information by the querier can be explained with the following example:

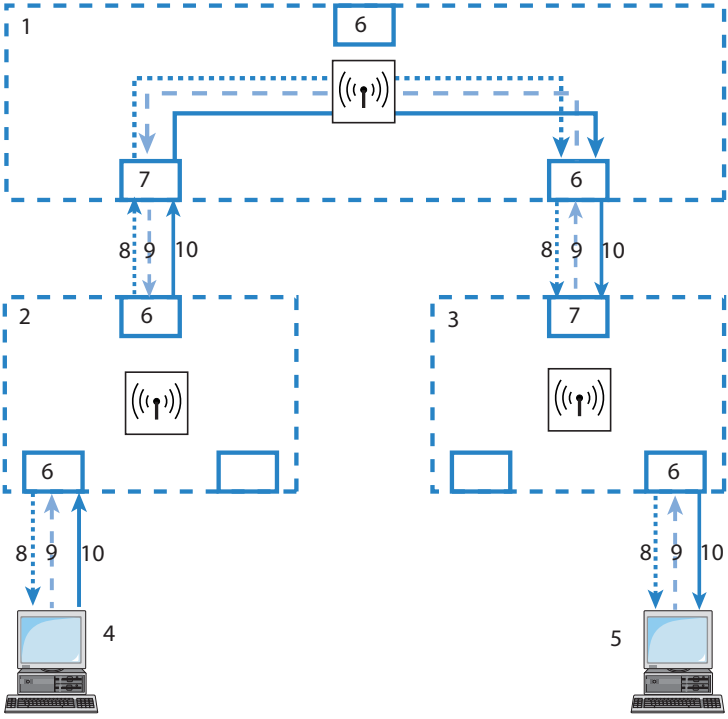


Figure 125:IGMP snooping through multiple bridges

1: Bridge 1	6: Member port
2: Bridge 2	7: Router port
3: Bridge 3	8: Query
4: PC-1	9: Join
5: PC-2	10: Data

- The querier (Bridge 2 in this example) regularly sends out IGMP queries on all ports of bridge 2 (dotted lines). The next bridge (Bridge 1) receives the query on a port which is then marked as a router port (R). PC 1 responds to this query with a Join message for all multicast groups (light dashed lines) that it wishes to join. The port connecting PC 1 to Bridge 2 then becomes a member of the multicasting group(s).
- In addition to this, Bridge 1 sends the queries on all other ports to the bridges and stations lower down in the structure. In Bridge 3 the port receiving the query becomes a router port (R).
- The station (PC 2) connected to bridge 3 responds to this query with a Join message for all registered multicast groups. The port connecting PC 2 to Bridge 3 then becomes a member of the multicasting group(s).
- Bridge 3 forwards this Join message to Bridge 1 over the router port. The receiving port on Bridge 1 thus also takes on membership of the multicast groups that PC 2 has registered for.
- In the final step, Bridge 1 forwards the Join message from PC 2 via the router port to Bridge 2, where the receiving port also takes on membership of PC 2's multicast groups.

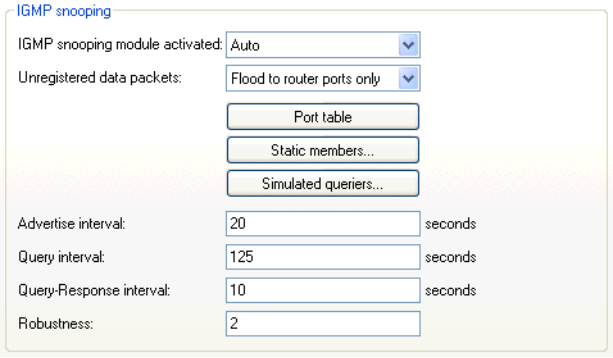
If PC 1 now transmits a multicast for which PC 2 has registered, all of the bridges (2, 1 and then 3) forward the packets to PC 2 via the member port.

11.21.4 Configuring IGMP Snooping

General Settings

To configure general IGMP settings in LANconfig, follow these steps:

☐ Open `Configuration : Interfaces : IGMP Snooping`:



Enter settings for the following IGMP general properties:

- IGMP snooping module activated:
  This enables or disables the IGMP snooping function, plus any configured IGMP querier entities that might have been defined.
  - If enabled: the LAN bridge will track any IGMP traffic and sort ports for IGMP relevance.
  - If disabled: the LAN bridge will behave like a 'dumb switch' and flood all IP multicasts to all ports.
  - With the setting "Auto", the bridge only activates the IGMP snooping when there are also queriers in the network.

  Note: If this function is deactivated, the bridge sends all IP multicast packets on all ports. If there is a change of operating state, the bridge completely resets the IGMP snooping function, i.e. it clears all dynamically learned values (memberships, router port properties).

- Unregistered data packets:
  This setting defines the handling of multicast data packets with a destination address outside the 224.0.0.x range and no defined memberships (i.e. no static members were defined, and no dynamic memberships were learned by the reception of IGMP join messages). Values include:
  - Router ports only (default): Sends these packets to all router ports.
  - Flood: Sends these packets to all ports.
  - Discard: Drops these packets.
- Advertise interval:
  The interval during which devices send packets advertising themselves as multicast routers. This information makes it quicker for other IGMP-snooping devices to find which of their ports are to operate as router ports. When activating its ports, a switch (for example) can query for multicast routers, and the router can respond to this query with an advertisement of this type. Under some circumstances this method can be much quicker than the alternative IGMP queries. Values are in seconds, and range from 4 to 180. The default is 20 seconds.
- Query interval:
  Interval in seconds during which a multicast-capable router (or a simulated querier) sends IGMP queries to the multicast address 224.0.0.1, prompting the stations to transmit return messages regarding multicast group memberships. These regular queries influence the time in which memberships age, expire, and are then deleted, as follows:
  - After the startup phase, the querier sends IGMP queries in this interval.
  - A querier returns to the querier status after a time equal to: Robustness * Query Interval + ((Query-Response Interval) / 2).
  - A port loses its router-port status after a time equal to: Robustness * Query Interval + ((Query-Response Interval) / 2).

  Values: a 10-figure number greater than 0. Default = 125.

  Note: The query interval must be greater than the query response interval.

- Query-Response interval:
  This Interval, in seconds.
  - influences the timing between IGMP queries and router-port aging and/or memberships.
  - is the time period during which a multicast-capable router (or a simulated querier) expects to receive responses to its IGMP queries. These regular queries influence the time in which memberships age, expire, and are then deleted.

  Values: a 10-figure number greater than 0. Default = 10.

  Note: The query response interval must be less than the query interval.

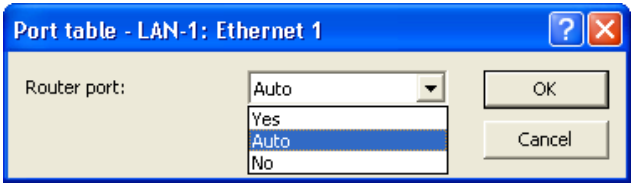
- Robustness:
  This setting tolerates packet losses of IGMP queries with respect to 'Join' messages. Possible values include a 10-figure number greater than 0. A value of 1 is not recommended. Default = 2.

Port Settings

To configure IGMP port settings in LANconfig, follow these steps:

☐ Open `Configuration : Interfaces : IGMP Snooping`.

☐ Click 'Port table', then select a port from the list to open the following dialog:



Enter settings for the following IGMP port properties:

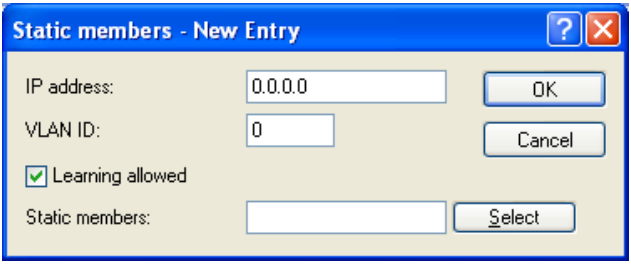
- **Router port:**
  This option defines the port's behavior. Selections include:
  - Yes: This port will always work as a router port, irrespective of IGMP queries or router messages that the bridge receives at this port.
  - No: This port will never work as a router port, irrespective of IGMP queries or router messages that the bridge receives at this port.
  - Auto (Default): This port will work as a router port if IGMP queries or router messages are received. The port loses this status if the bridge receives no packets for the duration of "Robustness*Query-Interval+(Query-Response-Interval/2)".

Static Members

To configure IGMP static member settings in LANconfig, follow these steps:

☐ Open `Configuration : Interfaces : IGMP Snooping` and click ‘Static members’.

☐ In the ‘Static members’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following IGMP static members properties:

- IP address:
  The IP address of the manually defined multicast group.
- VLAN ID:
  The VLAN ID to which the bridge applies this static membership. You can enter multiple entries with different VLAN IDs for each IP multicast address. Possible values: 0 to 4096 default = 0.

  Note: If ‘0’ is selected, the IGMP queries are sent without a VLAN tag. For this reason, this value makes sense when VLAN is deactivated in general.
- Learning allowed:
  This option activates the automatic learning of memberships in this multicast group. If automatic learning is deactivated, the bridge only sends packets via the ports which have been manually defined for the multicast group.
- Static members:
  The bridge will always send packets with the corresponding IP multicast address to these ports, irrespective of any Join messages received. Enter values in the form of a comma-separated list of the desired ports, up to a maximum of 215 alphanumerical characters.

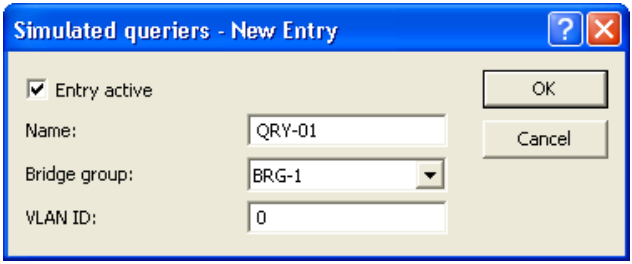
Simulated Queriers

This table contains all of the simulated queriers defined in the device. These units are employed if IGMP functions are required but there is no multicast router in the network. The querier can be limited to certain bridge groups or VLANs by defining multiple independent queriers to support the corresponding VLAN IDs.

To configure IGMP simulated queriers in LANconfig, follow these steps:

☐ Open `Configuration : Interfaces : IGMP Snooping` and click ‘Simulated queriers’.

☐ In the ‘Simulated queriers’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter settings for the following IGMP simulated querier properties:

- Entry active:
  Activates or deactivates the querier instance.
- Name:
  Name of the querier instance, containing up to 8 alpha-numeric characters.
- Bridge group:
  Limits the querier instance to a certain bridge group. If bridge group is set to ‘none’, the IGMP queries will be sent via all bridge groups.
- VLAN ID:
  An entry limits the querier instance to the specified VLAN. Because this parameter is also an index field, it is possible to make definitions that differ in the VLAN ID. A valid VLAN ID is in the range of 0...4094. The value 0 is meaningful if the VLAN module is turned off and then refers to untagged frames.

11.21.5IGMP Status

IGMP snooping status messages can be viewed in WEBconfig for the following:

- General status
- Groups status

- Port Status
- Simulated queriers

In addition, you can clear the content of all status tables.

These messages are presented in WEBconfig at:

```
HiLCOS Menu Tree : Status : LAN
BridgeStatistics : IGMP Snooping
```

General Statistics

This table contains information on IGMP packets. Field values include:

- Bad packets:
  The number of damaged data or IGMP packets received at all ports. Possible causes for damage to packets may be IP checksum events or truncated packets.

  Note: For performance reasons, IP checksums are evaluated just for IGMP packets, and not for the data portion of multicast packets. Hence, packets with an inaccurate checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

- Control packets:
  The number of intact IGMP packets received at all ports.
- Data packets:
  The number of intact IPv4 multicast packets received at all ports that are not IGMP packets.
- IPv4 Packets:
  The number of IPv4 multicast packets received at all ports, whether they were IGMP packets or not.
- Operating:
  Indicates whether IGMP snooping is activated or deactivated.

Groups Status

This table displays all the multicast group memberships known to the device, irrespective of whether they were configured statically or learned dynamically. If both static and dynamic memberships exist for a multicast group, these are shown in separate entries. Field values include:

- Address: The group's IP multicast address.
- VLAN ID: The VLAN ID to which this entry applies.
- Allow learning:
  Indicates whether new memberships for this group can be learned dynamically.
- Static members:
  The list of statically defined members for this group.
- Dynamic members:
  The list of dynamically learned members for this group.

Port Status

This table displays all port related statistics. Field values include:

- Router port:
  Indicates whether the port is currently in use as a router port, irrespective of whether this status was configured statically or learned dynamically.
- IPv4 packets:
  The number of IPv4 multicast packets received at this port, whether they were IGMP packets or not.
- Data packets:
  The number of intact IPv4 multicast packets received at this port that are other than IGMP packets.
- Control packets:
  The number of intact IGMP packets received at this port.
- Bad packets:
  The number of damaged data or IGMP packets received at this port. Possible causes for damage to packets may be IP checksum events or truncated packets.

Note: For performance reasons, IP checksums are evaluated just for IGMP packets, and not for the data portion of multicast packets. Hence, packets with an inaccurate checksum in the TCP/UDP or IP header are not detected. These packets are counted as data packets.

Simulated Queriers

This table shows the status of all defined and active IGMP querier instances. Field values include:

- Name:The name of the multicast group.
- Bridge group: The bridge to which this entry applies.
- VLAN ID: The VLAN to which this entry applies.
- Status: The current status of the entry:
  - Initial: The querier instance has just started and is sending IGMP queries in short intervals (four-times faster than the query interval defined).
  - Querier: The querier instance considers itself to be the active querier and is sending IGMP queries in the defined query interval.
  - Non-Querier: Another querier instance with a lower IP address has been detected, and the instance listed here is not sending any IGMP queries.

12 Configuring the Firewall

In an industrial environment, a firewall is indispensable for the separation of subnets, or for securing the LAN if the Internet access is also provided. But each connection from a workstation on the local network to the Internet represents a potential entry point for unauthorized users, who may attempt to access and edit your data, and manipulate your device configurations.

12.1 The Device Firewall

This chapter introduces the firewall embedded in the OpenBAT device.

The default value for IPv4 firewall is enabled for BAT devices.

Note: For ease of understanding, this chapter uses IPv4 as a basis for explanation and is mainly confined to the general firewall settings and the IPv4-specific configuration. Detailed documentation and background information on the IPv6 firewall is available separately in the chapter IPv6 (see on page 986).

12.1.1 Tips for Configuring the Firewall

The firewall in the OpenBATdevice is an extremely flexible and powerful tool. The following advice is offered to help you create rules for your firewall.

Default Firewall Settings

On delivery there is exactly one entry in the Firewall rule table: 'WINS'. This rule inhibits unwanted connection set-ups on the default route (usually to the Internet) by the NetBIOS protocol. Windows networks send inquiries in regular intervals into the network to find out if known stations are still available. This leads, in the case of a time-based account of network coupling, to unwanted connection set-ups.

Note: The OpenBAT device can prevent this, using the integrated NETBIOS proxy for network couplings, by simulating an answer for the concerned resource, until a real access takes place.

Security by NAT and Stateful Inspection

If no further firewall rule will be entered, the local area network benefits from the interaction of Network Address Translation (NAT) and stateful inspection. Only connections from the local area network produce an entry in the NAT table, whereupon the OpenBAT device opens a communication port. The stateful inspection monitors the communication via this port. Packets that belong to this connection may communicate via this port. For attempted access from the outside to the local network, this results in an implicit "Deny All" strategy.

Note: If you operate a web server in your LAN, which has been permitted access to this service from the outside (see on page 803), stations from the Internet can establish connections to this server. The inverse masquerading has priority over the firewall in this case, as long as no explicit 'Deny All' rule has been set.

Setting up an explicit 'Deny All' Strategy

The 'Deny All' rule is by far the most important rule to help protect local networks. By this rule the firewall operates according to the principle: All actions that are not explicitly allowed remain forbidden. By means of this strategy, the administrator can be sure not to have forgotten an access method, because the means of access that exist are the ones that have been opened explicitly.

Hirschmann recommends that you set up the "Deny All" rule before connecting the LAN to the Internet via an OpenBAT device. In this way, you can analyze in the logging table (e.g. via LANmonitor) which connection attempts have been blocked by the firewall. With the help of this information, you can gradually extend the "Allow" rules of the firewall.

To increase protection and control of the data traffic, you should first guard against any data transfer by the firewall. Then, the necessary functions and communication paths are selectively allowed. This approach guards against so-called Trojan horses or e-mail viruses, which actively set up an outgoing connection on certain ports.

Typical examples of firewall settings include the following:

Rule Name	Source	Destination	Action	Service (target ports)
ALLOW_HTTP	Local network	All stations	transmit	http, https
ALLOW_FTP	Local network	All stations	transmit	ftp
ALLOW_EMAIL	Local network	All stations	transmit	MAIL, NEWS
ALLOW_DNS_FORWARDING	Local network	IP address of device (or local network)	transmit	DNS
DENY_ALL	All stations	reject	reject	ANY

- Sample configuration: ‘Basic Internet’

- For a network coupling you permit additionally the communication between the involved networks:

Rule Name	Source	Destination	Action	Service
ALLOW_LAN1_TO_LAN2	LAN1	LAN2	transmit	ANY
ALLOW_LAN2_TO_LAN1	LAN2	LAN1	transmit	ANY

- If you operate e.g. an own web server, you selectively allow access to the server:

Rule Name	Source	Destination	Action	Service (target ports)
ALLOW_WEBSERVER	ANY	Webserver	transmit	http, https

- For diagnostic purposes it is helpful to allow ICMP protocols (e.g. ping):

Rule Name	Source	Destination	Action	Service (target ports
ALLOW_PING	Local network	ANY	transmit	ICMP

These rules can now be refined as needed - e.g. by the indication of minimum and maximum bandwidths for the server access, or by a finer restriction on certain services, stations or remote sites.

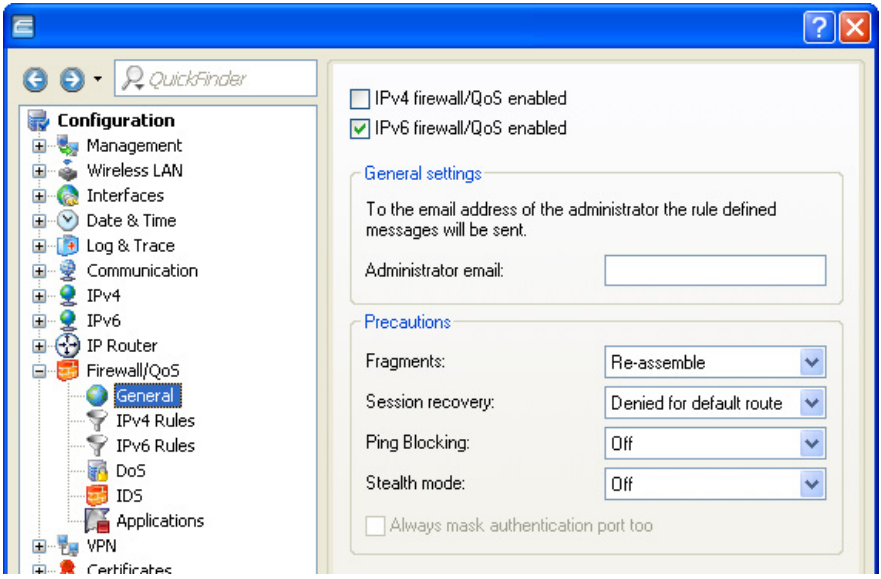
Note: The OpenBAT device automatically sorts firewall rules when creating the filter list. Thereby, the rules are sorted into the filter list on the basis of their level of detail. First, each specific rule is considered, then the general ones (e.g. Deny All). Examine the filter list in case of complex rule sets.

12.2 Firewall Configuration: LANconfig

The firewall can be configured using LANconfig, WEBconfig, and Telnet. The easiest way to configure the firewall is with LANconfig software.

12.2.1 General Firewall Parameters

Apart from individual firewall rules, the following general settings can be set for firewall. To access these general settings open the following dialog in the LANconfig software: `Configuration : Firewall/QoS : General`.



IPv4- bzw. IPv6 firewall/QoS enabled

This option switches on or off the entire firewall, including Quality of Service functions for IPv4 and/or IPv6.

Administrator e-mail

The firewall can trigger the alerting of a network administrator via e-mail. The 'administrator email' parameter contains the e-mail address to which the alerting mails are sent.

Fragments

Some attacks from the Internet try to outsmart the firewall by fragmenting packets into several small units. One of the main features of stateful inspections the ability to re-assemble fragments into entire packets, then check them against firewall rules. You can configure the firewall to treat fragmented packets as follows:

- Filter:
  The firewall discards packet fragments.
- Route:
  The firewall allows packet fragments to pass without further checking, provided the packet fragments are otherwise permitted by filter settings.
- Re-assemble:
  Fragmented packets are buffered and re-assembled into complete IP packets. The re-assembled packets are checked and treated according to filter settings.

Session recovery

The firewall adds the permitted connections into the connection list. Entries are automatically removed from the list after a timeout period, during which no data has been transmitted over this connection.

General TCP aging settings can close a connection before data packets requested by a remote station have been received. In this case it is possible for a connection entry that has been closed to continue to appear in the connection list.

Use this parameter to specify firewall behavior when it receives packets for a closed connection:

- Always allowed:
  The firewall re-establishes the connection if the packet belongs to a previously listed connection.
- Always denied:
  The firewall does not re-establish the session and discards the packet.
- Denied for WAN:
  The firewall re-establishes the session if the packet source was an interface other than a WAN interface.
- Denied for default route:
  The firewall re-establishes the session if the packet wasn't received from the default route (e.g. Internet).

Note: Because the virtual router takes action based on its analysis of the interface-tag, routes other than the untagged default route can be treated as the default route:

– When a packet is received at a WAN interface, then the WAN interface is considered by the firewall to be a default route if either a tagged or an untagged default route refers to this WAN interface.

– If a packet is received at a LAN interface and is to be routed to a WAN interface, then the WAN interface is considered to be a default route if either the untagged default route or a default route tagged with the interface tag refers to this WAN interface.

Default route filters are also effective if the default route is in the LAN. In this case, the filter takes effect when:

– A packet received over a tagged LAN interface is to be sent over a default route tagged with the interface, or

– A packet from another router was received at a tagged LAN interface and there is a default route with the interface tag to the packet's source address, or

– A packet was received from the WAN and is to be sent to the LAN via a default route with any tag.

Ping blocking

Hiding the router increases security. Many attacks start with a search for workstations or open ports by making harmless inquiries via the "ping" command or a port scan. Each response—even the answer "I'm not here"—indicates that the attacker has found a potential target. To help avoid these attacks, the OpenBAT device can be configured to suppress responses to these inquiries.

To achieve this, the OpenBAT device can be configured not to answer ICMP echo requests. At the same time TTL-exceeded messages of a trace route are also suppressed. The possible settings are:

- Off:
  ICMP responses are not blocked.
- Always:
  ICMP responses are always blocked.
- WAN only:
  ICMP responses are blocked on WAN connections.
- Default route only:
  ICMP responses are blocked on default route (usually Internet).

Stealth mode

The behavior of the OpenBAT device with respect to TCP and UDP connections can inform attackers of its existence. Depending on the surrounding network, it may make sense to silently reject TCP and UDP packets instead of answering with a TCP RESET or an ICMP message (port unreachable), if no listener for the respective port exists.

Note: If ports without listeners are hidden, this will create a challenge for masked connections. In this case, such a port can be separately configured.

Stealth mode settings include:

- Off:
  All ports are closed and TCP packets are answered with a TCP reset.
- Always:
  All ports are hidden and TCP packets are silently discarded.

- WAN only:
  On the WAN side all ports are hidden; on the LAN side all ports are closed.
- Default route only:
  Ports are hidden on the default route (usually Internet) and closed on all other routes.

Always mask authentication port too

Hiding TCP or UDP ports creates challenges for masked connections. If, for example, the so called 'Authenticate' or 'Ident' inquiries from special mail or news servers are returned to receive further user data and your device does not reject them, the corresponding connections will deliver a timeout. This can slow down mail or news delivery significantly.

To overcome this challenge, stealth mode is temporarily disabled for the specific port. The firewall recognizes that the internal stations intend to establish connections to a mail (SMTP, POP3, IMAP2) or news (NNTP) server, and opens the port for 20 seconds.

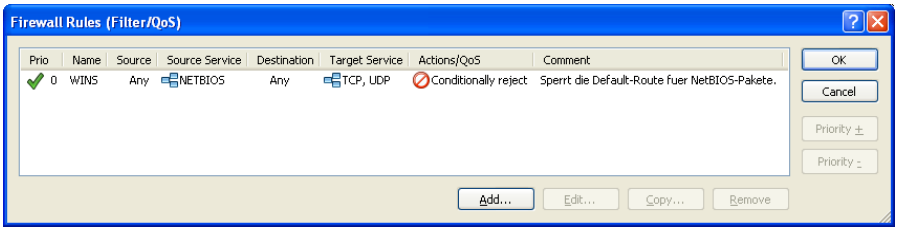
De-select this parameter to suppress the short-term cancellation of the stealth mode for the authentication port.

Note: Selecting this option significantly slows news and mail delivery.

12.2.2 Creating a New IPv4 Firewall Filter Rule

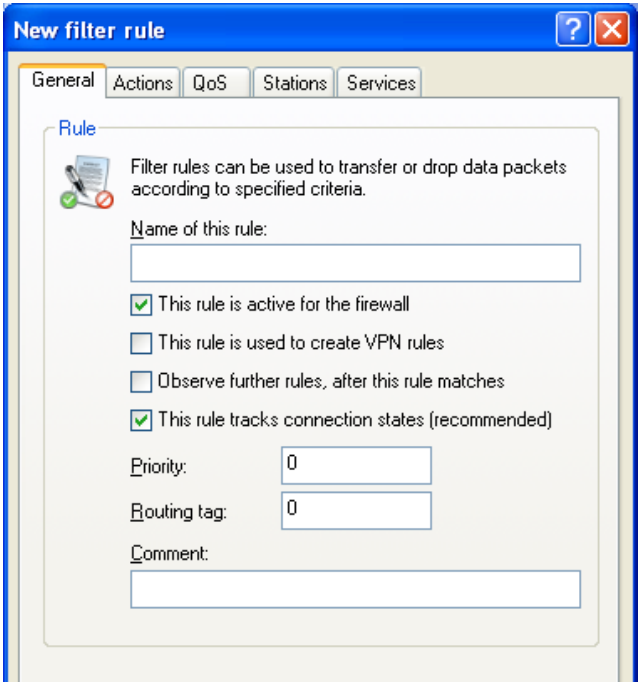
A new IPv4 firewall filter rule can be created in the ‘New filter rule’ dialog. To open this dialog:

☐ In the `Configuration : Firewall/QoS : IPv4 Rules` window, click "Rules" to open the rules list:



☐ In the ’Firewall Rules’ window (above,) click ’Add...’ to open the ‘New filter rule’ dialog (below).

☐ In the ’New filter rule’ dialog, click the ’General’ tab.



The settings in this dialog are described, below.

Activate the Rule

Activate the firewall rule by selecting the corresponding checkbox. If you uncheck this box, you can temporarily disable the rule without deleting it.

Use the Rule to Create VPN Rules

A VPN rule takes the details of the source and destination networks from the firewall rules, among others. By enabling this option, a VPN rule is derived from this firewall rule. For more information on this subject see the VPN chapter about creating rules (see on page 634 „Establishing VPN Network Relationships“).

Observe Further Rules

Some filters cannot be implemented using a single rule. For example, a company with three departments might want to limit bandwidth to each department to 512kbps, while at the same time limiting bandwidth to all three departments collectively to 1024 kbps. This can be accomplished by multi-level checking of multiple firewall rules. In this example:

– Step 1 checks to see if the data rate of the individual department exceeds the limit of 512 kbps.

– Step 2 checks to see if the data rates of all departments together exceed the overall limit of 1024 kbps.

If the ‘Observe further rules...’ option is not selected, a packet is checked until the first filter rule applies. The first time a filter applies, the firewall takes the appropriate action. The packet is not checked to see if additional rules apply to the packet.

But if the ‘Observe further rules...’ option is selected for the first rule applied to the packet, the firewall continues to apply other rules against the packet. This process continues until either:

– a rule applies to the packet, for which the ‘Observe further rules...’ option is not activated, or

– all remaining rules in the list have been applied to the packet.

Track Connection States

If selected, the firewall performs stateful inspections on data packets entering the firewall.

Priority

The OpenBAT device applies firewall rules according to a pre-defined priority. General rules (e.g. Deny All) are applied first, followed by special rules. It is possible to manually change the prioritization of rules. The higher the priority of the firewall rule—beginning with 1—the earlier it will be placed in the associated filter list. A value of 0 places no special priority on the rule.

Note: For complex rule types, please refer to the description of the filter list (see on page 954).

Routing tag

The routing tag is used by the device to identify the ARF context from which a packet was received. Using this tag restricts the use of firewall rules to certain ARF contexts.

12.2.3 Firewall filter rule settings and actions

This section shows you how to configure the parameters that determine:

- Connection:
  To which stations and protocols does the filter rule apply?
- Conditions:
  Is the effectiveness of the rule limited by other conditions?
- Trigger:
  What threshold values trigger the rule?

- Action:
  How should the firewall handle data packets to which the rule applies when the threshold trigger is reached?
- Further measures:
  Should further measures be initiated in addition to the packet action?
- Quality of Service (QoS):
  Do certain data packets enjoy prioritized treatment by virtue of their QoS tags?

All of these settings and actions can be configured in dialogs in, or linked to, the ‘New filter rule’ dialog.

Note: The settings conditions, trigger, action and further measures together constitute a so-called ’action set’. Each firewall rule can contain a number of action sets. If the same trigger is used for several action sets, the sequence of action sets can be adjusted.

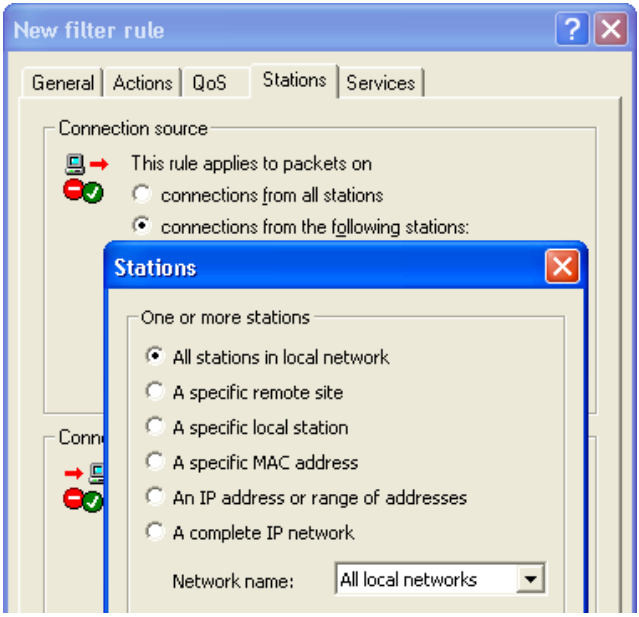
Connection

The connection element of a firewall rule defines the data packets to which the firewall filter rule applies. A connection is defined by its source and destination stations, and the services or protocols it requires.

To specify the source and destination stations for a rule:

☐ In the ‘New filter rule’ dialog, click the ‘Stations’ tab.

☐ If you select ‘connections from the following stations’, you can click ‘Add...’ to include less than all stations in the rule.



You can add the following connection source and destination station selections to the rule:

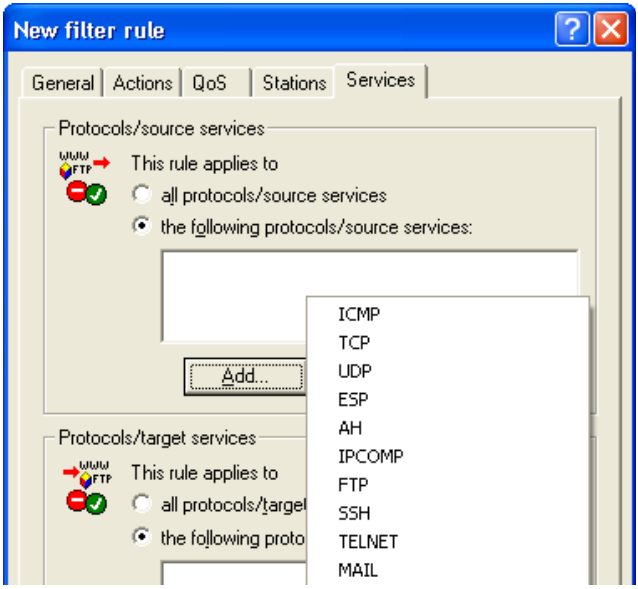
– all stations
– all stations in the LAN
– a specific remote site
– a specific local station
– a specific MAC address
– an IP address or range of addresses
– a complete IP network

You can operate with host names only if the OpenBAT device can transform their names into IP addresses. For that purpose the device needs to have learned the names via DHCP or NetBIOS, or you need to enter the assignment statically in the DNS or IP routing table. An entry in the IP routing table can therefore assign a name to a whole network.

Similarly, you can configure the rule to apply to all or some protocols and services. To do so:

☐ In the ‘New filter rule’ dialog, click the ‘Services’ tab.

☐ If you select ‘the following protocols/source services’ you can click ‘Add...’and apply less than all services or protocols to the rule.



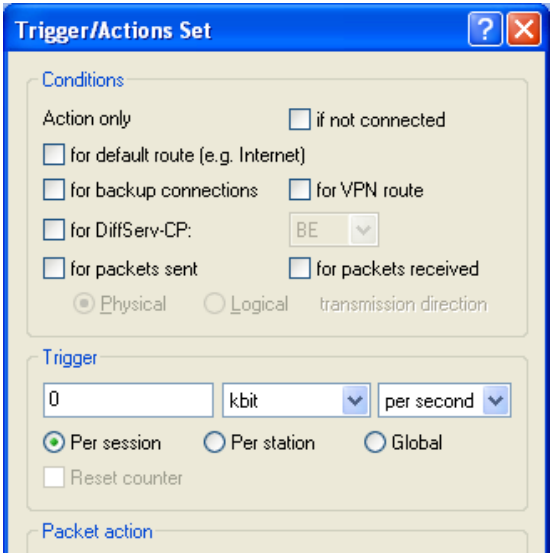
The service is determined by the combination of an IP protocol with respective source and/or destination port. For frequently used services (www, mail, etc.) the appropriate combinations are already predefined in the OpenBAT device.

Trigger

The trigger—or limit—describes a quantified threshold value that needs to be exceeded on the defined connection before the filter action is applied to a data packet. To set a trigger:

☐ In the ‘New filter rule’ dialog, click the ‘Actions’ tab.

☐ Click ‘Add...’ and select ‘Add custom action...’ to open the ‘Trigger/ Actions Set’ dialog.



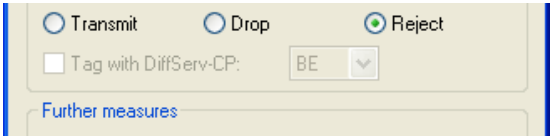
A trigger is set using the following parameters:

- Value: the measure of the trigger. This field accepts SI prefixes (k, Ki, M, Mi, G, Gi) as well as the SI unit bit, which divides the value by 8 when the entry field is exited.
- Unit: kbit, kByte, packets, sessions, %bandwidth
- Periodic reference: absolute, per hour, per minute, per second
- Scope: per session, per station, or global

If the rule applies, different counters are started. Either all packets or bytes that match this rule are counted globally or a specific counter will be started separately for every station (local host) or session (logical connection). The specific counter will either reset after the specified period of time (second, minute or hour) or it will count infinitely (absolute). An absolute counter can be reset if it exceeds its trigger value.

Packet Action

When a packet triggers a rule, the firewall acts in response. The specified action is also configured in the 'Trigger/Actions Set' dialog (just below the Trigger settings):



The firewall can take any of three packet actions:

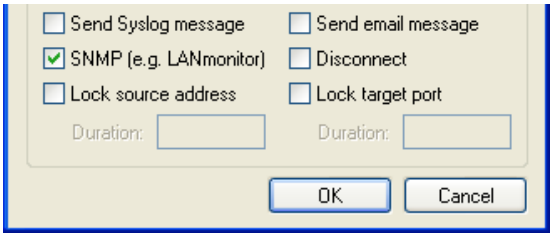
- Reject:
  The packet is not accepted; an ICMP reject notice is sent to the sender.
- Drop:
  The packet is silently rejected; no message is sent to the sender.
- Transmit:
  The packet is sent to its destination.

Note: A DiffServe codepoint (DSCP) tag can optionally be added to each transmitted packet. DSCP tags include:

– BE: Best Effort Normal packet (corresponds CS0)
– CS: 0 - 7 Class Selector Is compatible to the TOS field of the IPv4 header and corresponds to the precedence of unset TOS bits.
– AF: 0 - 4 / 0 - 3 Assured Forwarding The first digit represents the process priority and the second one represents the drop probability. The higher the priority and the lower the drop probability, the less frequently a packet will actually be dropped.
– EF: Expedited Forwarding Self declaring
– Value: An arbitrary tag—from 0 to 63—can be added.

Further Measures

In addition to discarding or accepting the filtered data packets, the firewall can also take additional measures when a data packet has been registered by the filter. These further measures are also configured in the 'Trigger/Actions Set' dialog (just below the 'Packet action settings'):



One or more of the following further measures can be set:

- Send Syslog message:
  Sends a message via the SYSLOG module to a SYSLOG client, that has been defined in the following page: `Configuration : Log & Trace : General : Syslog servers`.
- Send e-mail message:
  Sends an e-mail message to the designated administrator. To configure e-mail:
  – configure the administrator's e-mail address in the `Configuration : Firewall/QoS : General` dialog
  – properly set up the SMTP e-mail account in the `Configuration : Log & Trace : SMTP Account` dialog
- SNMP (e.g. LANmonitor):
  Sends an SNMP trap that will be analyzed, e.g., by LANmonitor.

  Note: A message sent by any of the above three methods causes an entry to be made in the firewall event table.

- Disconnect:
  Cuts both the physical and logical connections over which the filtered packet has been received.

- Lock source address:
  Temporarily blocks packets that are received from a specific address.
- Lock target port:
  Temporarily blocks packets that are transmitted over a specific port.

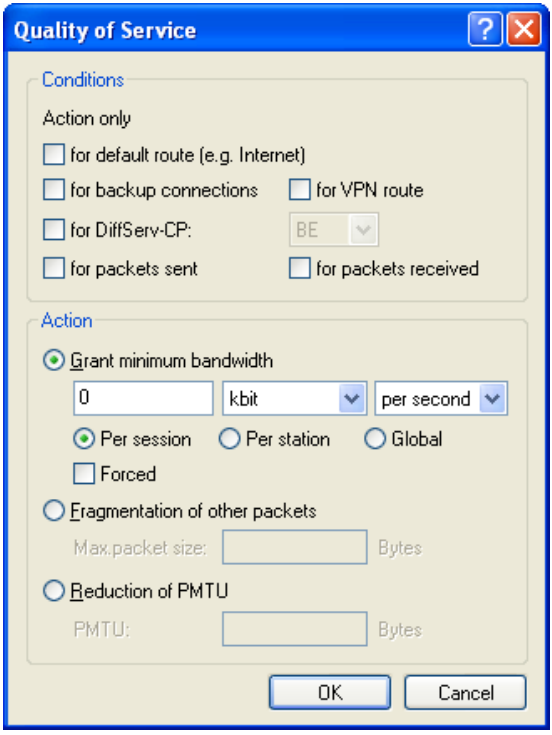
  Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can be released on the device exclusively by using a Telnet console or WEBconfig.

QoS

You can also configure Quality of Service (QoS) settings for the rule, which assigns a relative priority to the handling of the packet. To access the QoS firewall rule configuration dialog:

☐ In the ‘New filter rule’ dialog, click the ‘QoS’ tab.

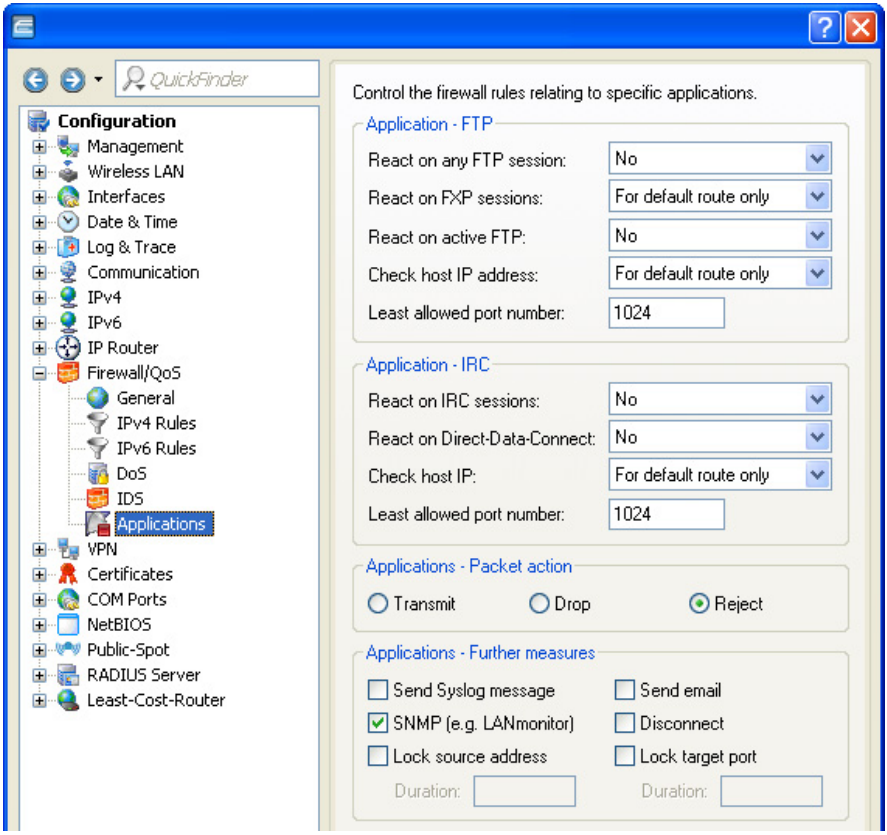
☐ Click ‘Add...’ and select ‘Add custom QoS...’ to open the ‘Quality of Service’ dialog.


Quality of Service
Conditions
Action only
for default route (e.g. Internet)
for backup connections
for VPN route
for DiffServ-CP:
BE
for packets sent
for packets received
Action
Grant minimum bandwidth
0
kbit
per second
Per session
Per station
Global
Forced
Fragmentation of other packets
Max.packet size:
Bytes
Reduction of PMTU
PMTU:
Bytes
OK
Cancel

12.2.4 Applying firewall rules to FTP and IRC connections

Special firewall rules can be configured and applied to file transfer protocol (ftp) and internet relay chat (IRC) connections, because of the unique threats presented by these two means of access to the local area network. To access the configuration dialog for these settings:

☐ Open the `Configuration : Firewall/Qos : Applications` dialog:



Use the settings described below to configure special handling for packets sent to the firewall over ftp and IRC connections:

- ftp applications:
  If an ftp session is recognized on any port, the countermeasures specified below apply:
  - React on Any FTP session: Indicate if, and over which routes, an ftp transmission should receive special handling. Default setting is 'Off'.
  - React on FXP sessions: Indicate if, and on which routes, a Site-To-Site transfer—via the file exchange protocol (FXP)—should receive special handling. Default setting is 'For default route only'.
  - React on active FTP: Indicate if, and on which routes, an ftp transmission in active mode should receive special handling. Default setting is 'Off'.
  - Check host IP address: Indicate if, and on which routes, the address transferred in the ftp command channel should be checked against the source address of the ftp client. If it does not match, the firewall performs packet action specified below.
  - Least allowed port number: The lower boundary for active ftp. Default setting is port '1024'.
- IRC applications:
  If an IRC session is recognized on any port, the countermeasures specified beneath apply:
  - React on IRC sessions: Indicate if, and over which routes, an IRC transmission should receive special handling. Default setting is 'Off'.
  - React on Direct-Data-Connect: Indicate if, and on which routes, Direct-Data-Connect (DDC - private chats and file transfers) should receive special handling. Default setting is 'Off'.
  - Check host IP address: Indicate if, and on which routes, the address transferred in the DDC command channel should be checked against the source address of the IRC client. If it does not match, the firewall performs packet action specified below. This check is skipped if a Site-To-Site transfer takes place and is already allowed. Default setting is 'For default route only'.
  - Least allowed port number: The lower boundary for active DDC. Default setting is port '1024'.

- Packet action:
  Indicate the action the firewall should take with respect to packets that are responsible for triggering an action or exceeding a limit:
  - Transmit: the packet is forwarded according to its address.
  - Drop: no notice to the addressor is sent.
  - Reject: an ICMP reject notice is sent to the packet source.
- Further measures:
  One or more of the following further measures can be set:
  - Send Syslog message: Sends a message via the SYSLOG module to a SYSLOG client, that has been defined in the following page:
    `Configuration : Log & Trace : General : Syslog servers`
  - Send e-mail message: Sends an e-mail message to the designated administrator. Both the administrator's e-mail address and the SMTP e-mail account need to be properly configured.
  - SNMP (e.g. LANmonitor): Sends a SNMP trap, that will be analyzed e.g. by LANmonitor.
  - Disconnect: Cuts both the physical and logical connections over which the filtered packet has been received.
  - Lock source address: Temporarily blocks packets that are received from a specific address.
  - Lock target port: Temporarily blocks packets that are transmitted over a specific port.

  Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can be released on the device exclusively by using a Telnet console or WEBconfig.

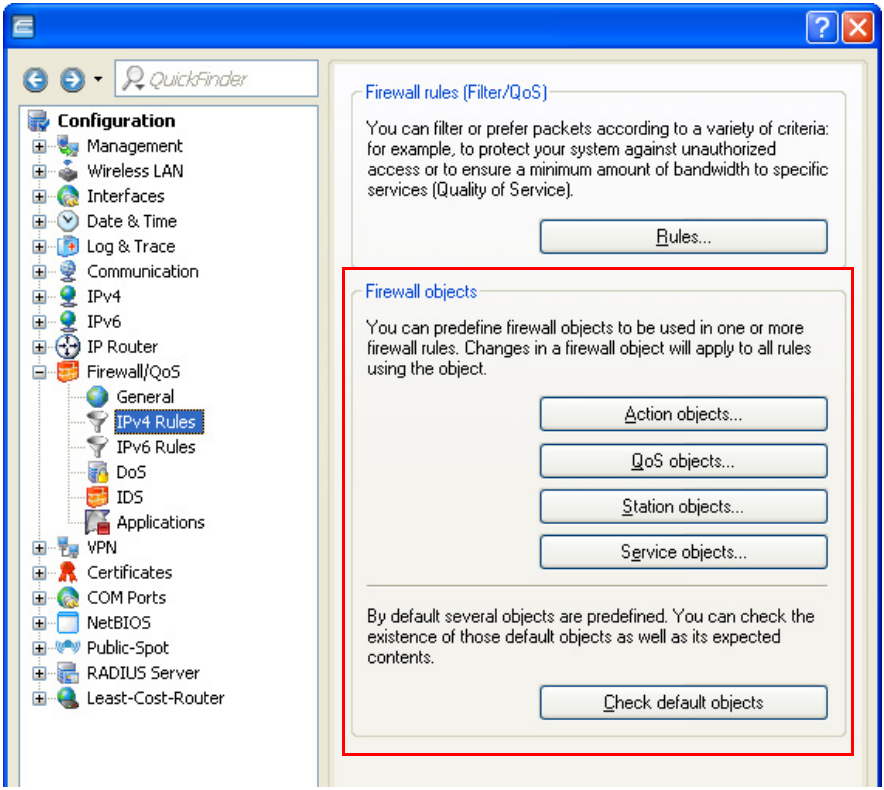
12.2.5 Defining Firewall Objects

When configuring the firewall with LANconfig, various objects can be defined that are used in the firewall rules. This means that frequently used definitions (such as a particular action) do not need to be re-entered for every rule. Instead they can be stored once at a central location.

Note:

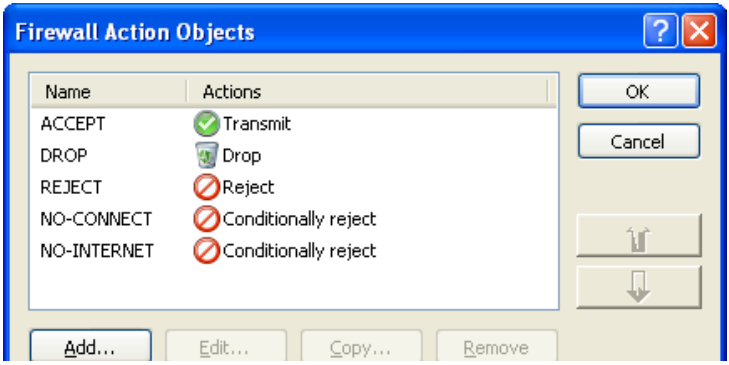
- Be aware that a change to a firewall object affects all of the firewall rules that use this object. For this reason, all firewall rules that also use these objects are displayed when you make changes to firewall objects.
- Existing firewalls (in the % notation) are not automatically converted to the object-orientated form when the configuration is opened in LANconfig. The KnowledgeBase contains the pre-defined firewall settings used by the new objects.

New firewall objects can be defined in LANconfig at the following dialog:
`Configuration : Firewall/QoS : IPv4 Rules`.


QuickFinder
Configuration
Management
Wireless LAN
Interfaces
Date & Time
Log & Trace
Communication
IPv4
IPv6
IP Router
Firewall/QoS
General
IPv4 Rules
IPv6 Rules
DoS
IDS
Applications
VPN
Certificates
COM Ports
NetBIOS
Public-Spot
RADIUS Server
Least-Cost-Router
Firewall rules (Filter/QoS)
You can filter or prefer packets according to a variety of criteria: for example, to protect your system against unauthorized access or to ensure a minimum amount of bandwidth to specific services (Quality of Service).
Rules...
Firewall objects
You can predefine firewall objects to be used in one or more firewall rules. Changes in a firewall object will apply to all rules using the object.
Action objects...
QoS objects...
Station objects...
Service objects...
By default several objects are predefined. You can check the existence of those default objects as well as its expected contents.
Check default objects

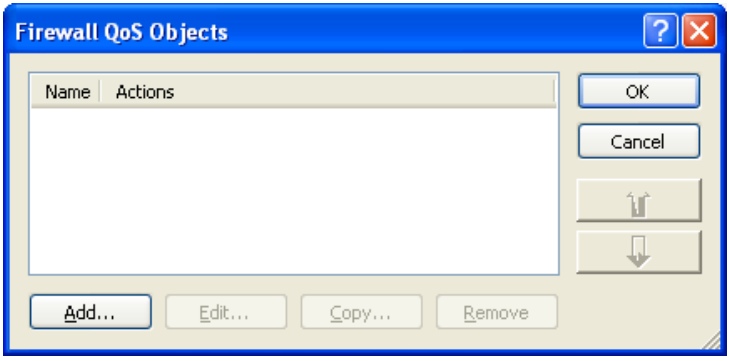
Action Objects

Use the ‘Firewall Action objects’ configuration dialogs to create firewall actions, each of which is a unique collection of condition, limit trigger, packet action and other measures to be used by the firewall rules.



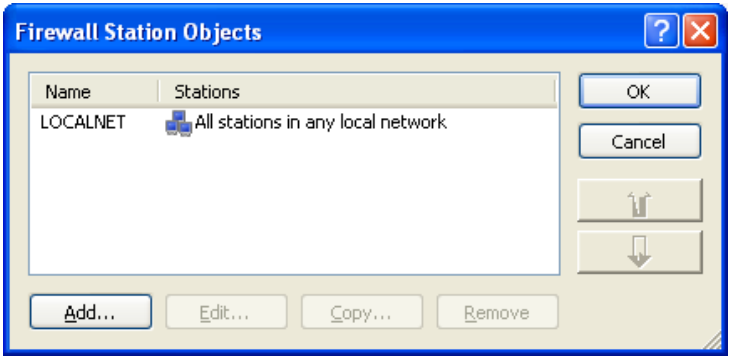
QoS Objects

Use the ‘Firewall QoS objects’ configuration dialog to set the minimum bandwidths that the firewall rules allocate to data packets.



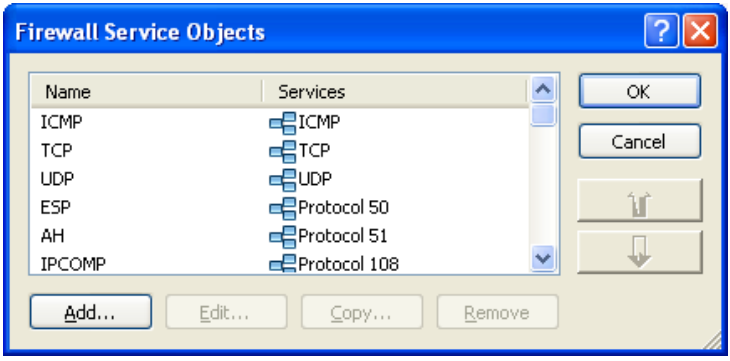
Station Objects

Use the ‘Firewall Station Objects’ configuration dialogs to define stations that the firewall rules can use as packet source or destination. The station objects are not restricted to any particular source or destination, but can be used as required by the firewall rules. In the context of Advanced Routing and Forwarding (ARF) you can specify a certain IP network as station object:



Service Objects

The IP protocols and the source/destination ports to be used by the firewall rules are defined here.



12.3 Configuring the IPv4 Firewall: WEBconfig and Telnet

12.3.1 Rules Table

The Rules table links various pieces of information of a firewall rule. The rule contains the protocol to be filtered, the source, the destination and the firewall action to be executed. For every firewall rule there is also an on/off switch, a priority, the option to link with other rules.

Just as with LANconfig, WEBconfig can be used to configure the firewall with the help of objects. The % notation described as follows is necessary for defining objects or actions.

To access the IPv4 rules table, follow these steps:

`Configuration : Firewall/QoS :IPv4 rules: Rule table`

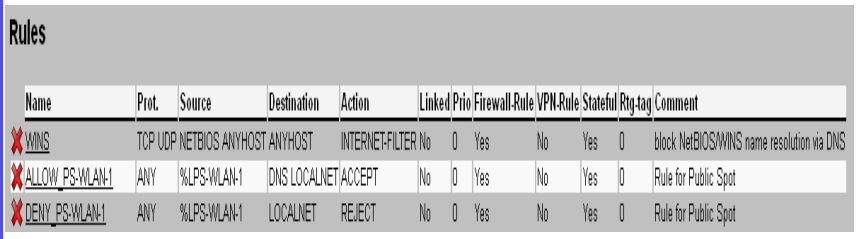


Figure 126:IPv4 Firewall Rules Table in WEBconfig

Note: Existing firewalls in the % notation are not automatically converted to the object-orientated form. However, the KnowledgeBase contains the pre-defined firewall settings used by the new objects.

The operating system of the OpenBAT device uses a special syntax for the firewall rules. This syntax enables the representation of complex interrelationships for the testing and handling of data packets in the firewall with just a few characters. The rules are defined in the rules table. Pre-defined objects can be stored in two further tables so that frequently used objects do not have to be entered into the operating system syntax every time:

- Firewall actions are stored in the Action table.
- Stations and service references are stored in the Object table.

Note: You can use the objects from in these tables to define rules, although this is not compulsory. These tables are designed to simplify the use of frequently used objects.

The definition of firewall rules can contain entries in the object table for protocols, services, stations and the action table for firewall actions, and also direct definitions in the appropriate operating system syntax (e.g. %P6 for TCP).

Note: For direct input of level parameters in the operating system syntax, the same rules apply as specified in the following sections for protocols, source/destination and firewall actions.

12.3.2 Objects Table

Elements/objects that are to be used in the firewall rules table are defined in the Objects table.
To access the IPv4 objects table, follow these steps:

```
Configuration : Firewall/QoS :IPv4 rules: Object table
```

Objects

	Name	Description
✖	ANYHOST	%A0.0.0.0 %M0.0.0.0
✖	LOCALNET	%L
✖	ANY	
✖	ICMP	%P1
✖	TCP	%P6
✖	UDP	%P17
✖	ESP	%P50
✖	AH	%P51
✖	IPCOMP	%P108
✖	FTP	TCP %S21
✖	MAIL	TCP %S25,110,143
✖	SECURE-MAIL	TCP %S993,995
✖	HTTP	TCP %S80
✖	HTTPS	TCP %S443
✖	WEB	TCP %S80,443
✖	NEWS	TCP %S119
✖	TFTP	UDP %S69
✖	IPSEC	UDP %S500,4500
✖	SSH	TCP %S22
✖	TELNET	TCP %S23
✖	DNS	TCP UDP %S53
✖	NETBIOS	TCP UDP %S137-139

Figure 127:IPv4 Firewall Objects Table in WEBconfig

Objects can be:

- Individual computers (MAC or IP address, hostname)
- Complete networks
- Protocols
- Services (ports or port areas, e.g. http, Mail&News, ftp, ...)

These elements can be combined and hierarchically structured in any way. For example, objects for the TCP and UDP protocols can be defined first. Building upon this, objects can subsequently be created, for example, for ftp (= TCP + ports 20 and 21), http (= TCP + port 80) and DNS (= TCP, UDP + port 53). These can in turn be combined into one object that contains the definitions of every individual object.

12.3.3 Action Table

A firewall action comprises of a condition, a limit, a packet action and other measures. As with the elements of the object table, firewall actions can be given a name and be combined with each other in any way recursively. The maximum recursion depth is limited to 16. They can also be entered into the actions field of the rules table directly.

To access the IPv4 actions table, follow these steps:

```
Configuration : Firewall/QoS :IPv4 rules: Action table
```

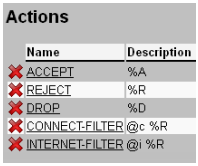


Figure 128:Firewall Action Table in WEBconfig

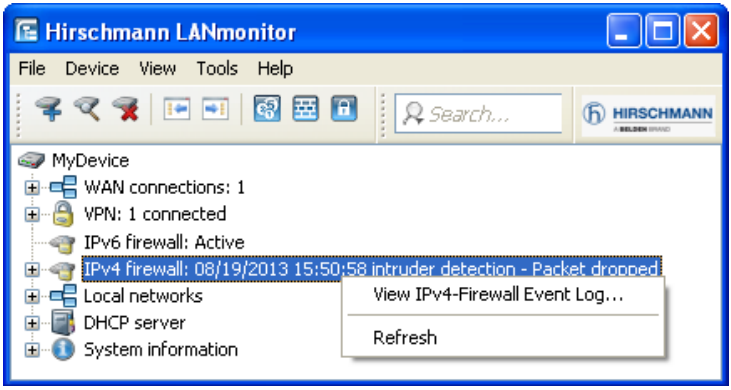
12.4 Firewall Diagnosis

All events, conditions and connections of the firewall can be logged and monitored in detail using either LANmonitor software or WEBconfig. The examples in this section are presented using LANmonitor software. However, all dialog and lists presented here can also be accessed at the following location:

`HiLCOS Menu Tree : Status : IP Router`

12.4.1 The Firewall Log Table

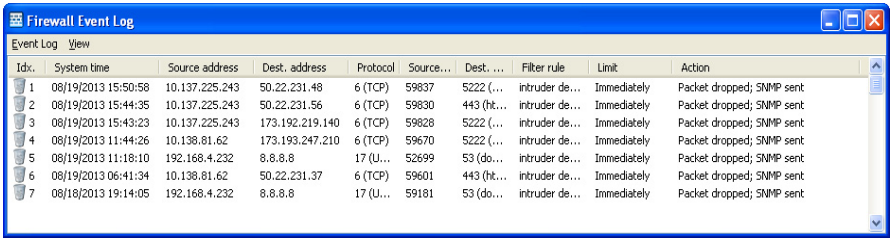
The easiest way to inspect firewall performance is by opening the ‘Log table’ from LANmonitor.



To open the log table in LANmonitor:

☐ Select the firewall and click on the right mouse button.

☐ In the pop-up menu, select ‘Firewall Event Log’:



The table contains the following fields:

Element	Description
Idx	Current index (so that the table can be polled also via SNMP)
Timestamp	System time in UTC codification (will be transformed on displaying of the table into clear text)
Src address	Source address of the filtered packet
Dst address	Destination address of the filtered packet
Protocol	Protocol (TCP, UDP etc.) of the filtered packet
Src port	Source port of the filtered packet (exclusively with port-related protocols)
Dst port	Destination port of the filtered packet (exclusively with port-related protocols)
Firewall rule	Name of the rule, which has raised the entry
Limit	Bit field, which describes the crossed limit, which has filtered the packet. There following values are currently defined: 0x01 Absolute amount, 0x02 Number per second 0x04 Number per minute 0x08 Number per hour: 0X10 Global limit 0x20 Byte limit (if not set, it is a packet limit) 0x40 Limit only applies in the inbound direction 0x80 Limit only applies in the outbound direction
Action	Bit field which lists all the actions performed. Currently, the following values are defined: 0x00000001 Accept 0x00000100 Reject 0x00000200 Dial-up filter 0x00000400 Internet (Default Route) filter 0x00000800 Drop 0x00001000 Disconnect 0x00004000 Lock source address 0x00020000 Lock destination address and port 0x20000000 Send SYSLOG notification message 0x40000000 Send SNMP trap 0x80000000 Send e-mail

Note: All Firewall actions are likewise displayed by the IP router trace function, and some OpenBAT devices have a Firewall LED that signals each filtered packet.

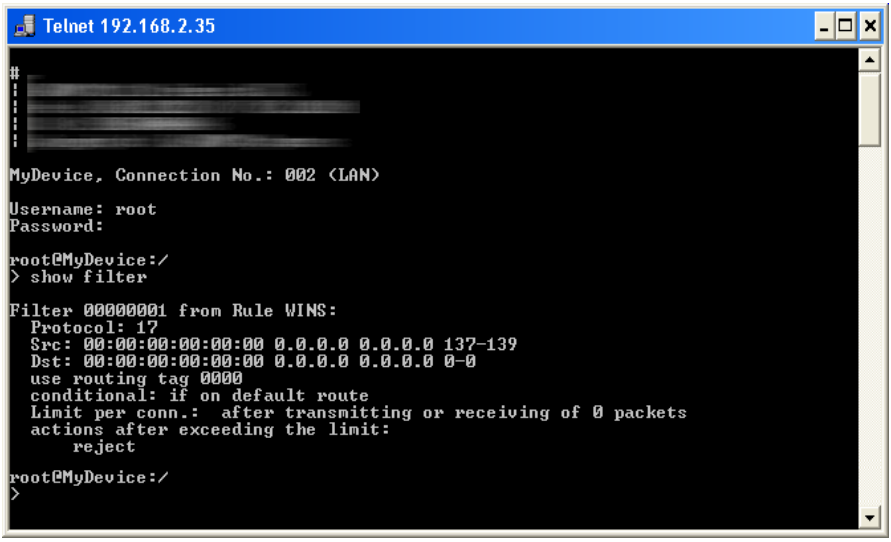
12.4.2 The Filter List

The filter list displays filters generated by rules defined in the action, object and rules tables.

Note: Manually entered filter rules do not indicate potential anomalies or generate exception response messages. If you configure filters manually, you should examine each entry in the filter list on a case by case basis to determine whether that filter is performing as intended.

You can view the contents of the filter list using Telnet by issuing the following command:

```
show filter
```



The firewall table contains the following fields

Element	Description
Idx	Current index (so that the table can be polled also via SNMP)
Prot	Protocol to be filtered, e.g. 6 for TCP or 17 for UDP
Src MAC	Ethernet source address of the packet to be filtered or 000000000000, if the filter should apply to all packets
Src address	Source IP address or 0.0.0.0, if the filter should apply to all packets
Source mask	Source network mask, which determinates the source network together with the source IP address, or 0.0.0.0, if the filter should apply to packets from all networks
S start	Start source port of the packets to be filtered.
S end	End source port of the packets to be filtered. Makes up the port range together with the start source port, in which the filter takes effect. If start and end port are 0, then the filter is valid for all source ports.
Dst-MAC	Ethernet destination address of the packet to be filtered or 000000000000, if the filter should apply to all packets.
Dst address	Destination address or 0.0.0.0, if the filter should apply to all packets.
Dst mask	Destination network mask, which determinates the destination network together with the destination IP address, or 0.0.0.0, if the filter should apply to packets to all networks.
D start	Start destination port of the packets to be filtered.
end	End destination port of the packets to be filtered. Makes up the port range together with the start destination port, in which the filter takes effect. If start and end port are 0, then the filter is valid for all destination ports.

Element	Description
Action	Into this column, the main action is unveiled as a text, which will be executed when the first limit has been exceeded. The first limit can be also an implicit limit, e.g. if exclusively one limit for the restriction of the throughput was configured. Then an implicit limit - linked with an accept action - is inserted. In this case, accept is unveiled as main action. You can see the complete actions under the command show filter.
Linked	Specifies if this rule is a “first match rule” (linked = no). The device appraises further rules only if a linked rule matches.
Prio	Priority of the rule having generated the entry.
Rtg tag	Routing tag including the data packets which are captured by this entry

12.4.3 The Connection List

The connection table files source address, destination address, protocol, source port, destination port, etc. of a connection, as well as possible actions. This table is sorted according to source address, destination address, protocol, source port and destination port of the packet, which caused the entry in the table.

The connection list contains these fields:

Element	Description
Src address	Source address of the connection
Dst address	Destination address of the connection
Protocol	Used protocol (TCP/UDP etc.) The device refers to the protocol with its decimal value.
Src port	Source port of the connection. The port is exclusively indicated with port-related protocols (TCP/UDP) or protocols, which own a comparable field (ICMP/GRE)
Dst port	Destination port of the connection (with UDP connections, this one is occupied exclusively with the first answer)
Rtg tag	Routing tag of the connection
Timeout	Each entry ages out with the time of this table, thus the table does not overflow with died connections.
Flags	Flags save the state of a connection and further (internal) information into a bitfield. The following values are possible for a state: new, establish, open, closing, closed, rejected (according to the TCP flags: SYN, SYN ACK, ACK, FIN, FIN ACK and RST).UDP connections know the conditions new, open and closing (the last one exclusively, if the UDP connection is linked with a condition-afflicted control path. This is e.g. the case with protocol H.323.)

Element	Description
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.
Src route	Name of the remote station, over which the first packet has been received.
Dst route	Name of the remote station, where the first packet will be sent to.

Flags of the connection list include:

Element	Description
00000001	TCP: SYN sent
00000002	TCP: SYN/ACK received
00000004	TCP: waiting for ACK of the server
00000008	All: Connection opened
00000010	TCP: FIN received
00000020	TCP: FIN sent
00000040	TCP: RST sent or received
00000080	TCP: session will be re-established
00000100	ftp: passive ftp connection will be established
00000400	H.323: belonging to T.120 connection
00000800	connection via loopback interface
00001000	checking concatenated rules
00002000	rule is catenated
00010000	destination is on local route
00020000	destination is on default route
00040000	destination is on VPN route
00080000	physical connection is not established
00100000	source is on default route
00200000	source is on VPN route
00800000	no route for destination
01000000	contains global actions with condition

12.4.4 Port Block List

Address, protocol and port of a destination station are filed in the port block list, if blocking of the destination port on the destination station was selected as a filter's packet action. This table is likewise a sorted semi-dynamic table. Sorting is done according to address, protocol and port. The table contains the following elements:

Element	Description
Address	Address of the station, to which the blocking should apply.
Protocol	Used protocol (TCP/UDP etc.). The device refers to the protocol with its decimal value.
Port	Port to close at the station. If the respective protocol is not port related, then the entire protocol for this station becomes closed.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

12.4.5 Host Block List

The address of a station is filed in the host block list, if blocking of the sender was selected in a filter's packet action. This table is a sender address sorted semi-dynamic table and contains the following elements:

Element	Description
Address	Address of the station, to which the blocking should apply.
Timeout	Duration of the blocking in minutes.
Filter rule	Name of the rule, which has generated the entry (determines also the actions to be executed), when a suitable packet is received.

12.5 Firewall Limitations

In addition to understanding how the firewall works, be aware of its limitations, and how to supplement the firewall if necessary. The firewall does not guard against malicious content entering the network through a permitted path. Although a firewall may stop some viruses and worms from entering the network, that is because the packets containing them were blocked from entering a port. However, no firewall alone provides comprehensive security against viruses.

A firewall does not hinder lurkers, who wish to read unencrypted communications sent beyond the firewall.

12.6 Combating intrusion attempts Intrusion detection

A firewall examines data traffic that attempts to pass between networks, and rejects those packets that lack permission to access the network. In addition to attempts to access directly a computer in the protected network, intruders also mount attacks against the firewall itself, or attempt to outwit a firewall with falsified data packets.

The Intrusion Detection System (IDS) is designed to recognize, repel and keep a record of these attacks. When an intruding packet is detected, the IDS can provide notice of the event, via e-mail notification, SNMP traps or SYSLOG alarms. IDS checks the certain properties of the data traffic looking for conspicuous patterns, which indicate an attempted attack upon the network.

12.6.1 Examples of Break-in Attempts

Spoofing

In a spoofing attack, the sender of a packet poses as a different computer. This approach is taken either to trick the firewall, which trusts packets from the own network more than packets from untrusted networks, or to hide the source of an attack.

The firewall guards itself against spoofing by route examination—it determines whether a packet is permitted over the specific interface over which it was received.

Port Scan Detection

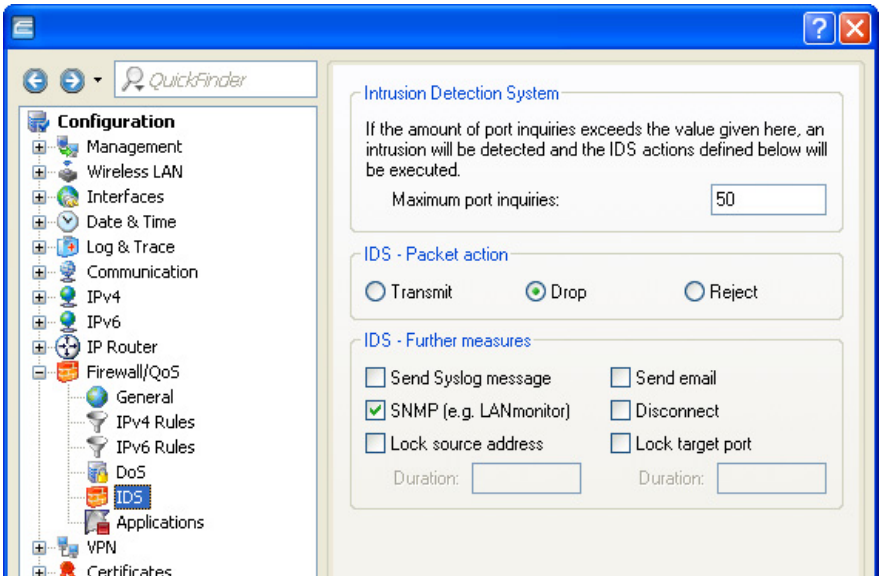
The IDS attempts to detect port scans as they occur, then to report and react appropriately to this form of attack. The response is similar to the recognition of a 'SYN Flooding' attack: Any 'half-open' connections are also checked (the product of a TCP RESET sent by the scanned computer that lease a connection 'half-open').

If a certain number of half-open connections between the scanned and the scanning computer exist, then this is reported as a port scan. In addition, the receipt of empty UDP packets is interpreted as an attempted port scan.

12.6.2 Configuring the IDS

To configure the firewall for intrusion detection:

☐ Open the `Configuration : Firewall/Qos : IDS` dialog:



The following parameters can be configured for the IDS:

- IDS: Use this section of the dialog to define an intrusion:
  - Maximum port inquiries: A number of intrusion attempts above this number trigger IDS responsive action.
- Packet action: Indicate the action the firewall should take with respect to an IDS attack:
  - Transmit: the packet is forwarded according to its address.
  - Drop: no notice to the addressor is sent.
  - Reject: an ICMP reject notice is sent to the packet source.
- Further measures:
  One or more of the following further measures can be set:
  - Send Syslog message: Sends a message via the SYSLOG module to a SYSLOG client, that has been defined in the following page:
    `Configuration : Log & Trace : General : Syslog servers`
  - Send e-mail message: Sends an e-mail message to the designated administrator. Both the administrator's e-mail address and the SMTP e-mail account need to be properly configured.
  - SNMP (e.g. LANmonitor): Sends a SNMP trap, that will be analyzed e.g. by LANmonitor.
  - Disconnect: Cuts both the physical and logical connections over which the filtered packet has been received.
  - Lock source address: Temporarily blocks packets that are received from a specific address.
  - Lock target port: Temporarily blocks packets that are transmitted over a specific port.

  Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can be released on the device exclusively by using a Telnet console or WEBconfig.

12.7 Protection from denial of service attacks

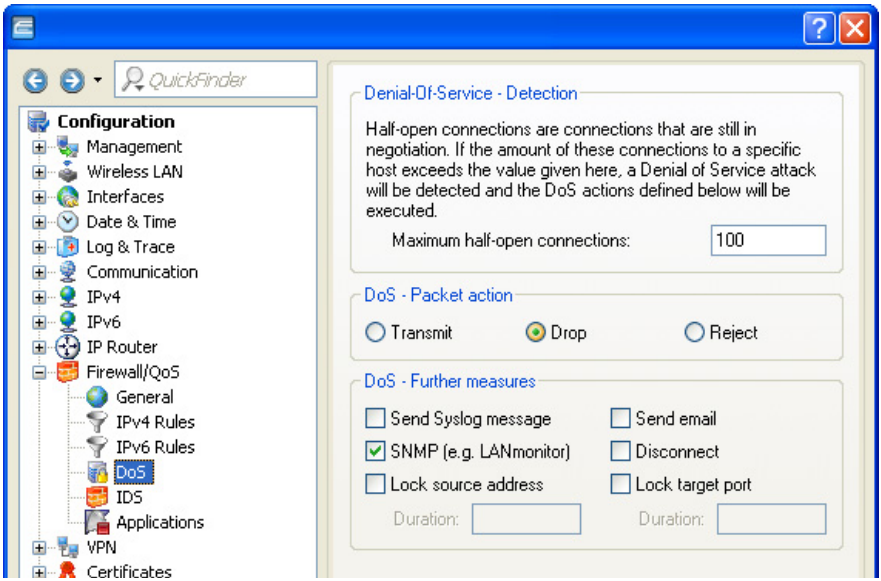
Some external attacks aim to block access to, and the functioning of, LAN services. Each OpenBAT device includes mechanisms that are designed to recognize well-known hacker attacks and continue to provide functionality in the face of such attacks.

12.7.1 Configuring DoS Blocking

In order to drastically reduce the susceptibility of the network to denial of service (DoS) attacks, packets from distant networks may be accepted exclusively if a connection has been initiated from the internal network, or the incoming packets have been accepted by an explicit filter entry (source: distant network, destination: local area network). The firewall tracks the connection state, source addresses and correctness of fragments for all explicitly permitted connections. This is performed with respect to both incoming and outgoing packets, since an attack could also be initiated from within the local area network. Address examination (against IP spoofing) and blocking of broadcasts into the LAN are continuously performed.

To configure the firewall to respond to denial of service attacks:

☐ Open the `Configuration : Firewall/Qos : DoS` dialog:



The following parameters can be configured for the IDS:

- DoS: Use this section of the dialog to define a DoS attack:
  - Maximum half-open connections: A number of half-open connections that triggers a responsive action.
- Packet action: Indicate the action the firewall should take with respect to an DoS attack:
  - Transmit: the packet is forwarded according to its address.
  - Drop: no notice to the addressor is sent.
  - Reject: an ICMP reject notice is sent to the packet source.
- Further measures:
  One or more of the following further measures can be set:
  - Send Syslog message: Sends a message via the SYSLOG module to a SYSLOG client, that has been defined in the following page:
    `Configuration : Log & Trace : General : Syslog servers`
  - Send e-mail message: Sends an e-mail message to the designated administrator. Both the administrator's e-mail address and the SMTP e-mail account need to be properly configured.
  - SNMP (e.g. LANmonitor): Sends a SNMP trap, that will be analyzed e.g. by LANmonitor.
  - Disconnect: Cuts both the physical and logical connections over which the filtered packet has been received.
  - Lock source address: Temporarily blocks packets that are received from a specific address.
  - Lock target port: Temporarily blocks packets that are transmitted over a specific port.

  Note: The duration of the source host or target port lock should be specified. Otherwise the respective addresses or ports will be permanently locked. These locks can be released on the device exclusively by using a Telnet console or WEBconfig.

13 IPv6

13.1 IPv6 basics

IPv4 (Internet Protocol version 4) is a protocol for unique addressing of nodes in a network and, at the time of writing, it has defined all of the IP addresses assigned globally. The limited availability of address space required the development of IPv6 (Internet Protocol version 6), which is to replace the former standard. With a different IP-address structure, IPv6 provides for a greater range of IP addresses and thus increases the possible number of participants in networks worldwide.

13.1.1 Why Use IPv6-standard IP Addresses?

The new IPv6 standard was developed for the following reasons:

- IPv4 address space allows for approximately four billion IP addresses for unique identities in networks. When the IPv4 standard was implemented in the '80s this address space was considered to be sufficient. Due to the enormous growth of the World Wide Web and the unexpectedly large number of computers and network devices, an address shortage has arisen that the IPv6 standard is intended to bridge.
- The increase in address space with IPv6 hampers the scanning of IP addresses by viruses and Trojans. The broader spectrum provides greater protection against attacks.
- IPv6 has been implemented with a view to the security requirements. For this reason it uses the security protocol IPSec (IP Security). This provides secure network communications on layer 3 whereas many of IPv4 security mechanisms only operate on higher layers.
- Simplified, fixed descriptors for data packets save on router processing power and thus accelerate the available throughput.

- IPv6 allows for easier and faster transmission of data in real time, making it suitable for multimedia applications such as Internet telephony and Internet TV.
- So-called mobile IPs allow you to use a fixed IP address to login to different networks. This allows you to log on with your laptop using the same IP address, whether you are in your home network, in a café or at work.

13.1.2 IP Address Structure According to the IPv6 Standard

The new IPv6 addresses are 128 bits long and the range of possible addresses can cater for about 340 sextillion network participants. IPv6 addresses consist of eight blocks of 16 bits and are written as hexadecimal numbers. The following is an example of a possible IPv6 address:

2001:0db8:0000:0000:0000:54f3:dd6b:0001/64

To improve the legibility of these IP addresses, zeros at the beginning of a block of numbers are omitted. It is also possible to omit one group of blocks that consist entirely of zeros. For the above example, one possible representation would be as follows:

2001:db8::54f3:dd6b:1/64

An IPv6 address consists of two components: A prefix and an interface identifier. The prefix denotes the membership of the IP address to a network, while the interface identifier (e.g. in the case of auto-configuration) is generated from a link-layer address, and thus belongs to a particular network card. The device can also generate interface identifiers from random numbers. This improves security. In this way, multiple IPv6 addresses can be assigned to a single component.

The prefix describes the first part of the IP address. The length of the prefix is ??shown as a decimal number after a slash. For the example given here the prefix is:

2001:db8::/64

The remainder of the IP address is the interface identifier. In our example, this is:

::54f3:ddb6:1

Compared with the IP addresses for the IPv4 standard, a number of changes have resulted in the structure of the new IPv6 addresses:

- While IPv4 addresses cater for an address space of 32 bits, the new length of 128 bits results in a significantly larger address space with IPv6. IPv6 addresses are four times longer than IPv4 addresses.
- An interface can have multiple IPv6 addresses due to the potential assignment of multiple prefixes to a single interface identifier. With the IPv4 standard, an interface has only one IP address.
- The automatic assignment of IPv4 addresses is always handled by a DHCP server. However, IPv6 can operate an auto-configuration, which makes the use of a DHCP server unnecessary. However, it is still possible to employ a DHCP server or to configure the IP addresses statically.

13.1.3 Stages of Migration

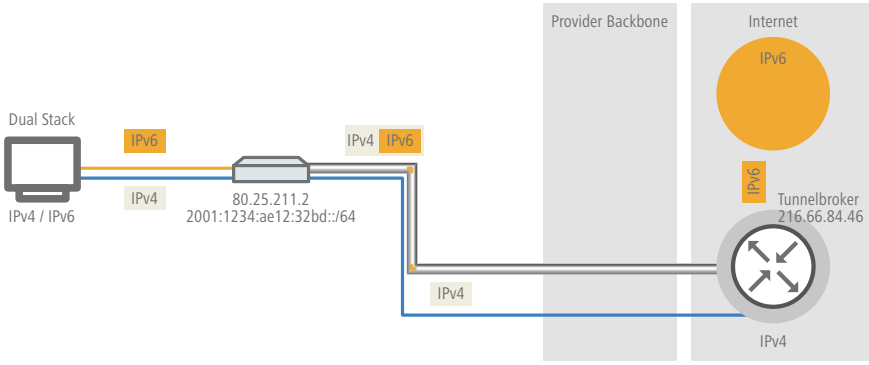
IPv6 is available to networks in a variety of ways. We make a distinction between environments with native IPv6 and those which provide IPv6 through a tunnel.

- **Native IPv6:** Native IPv6 describes a network that communicates to the outside only via IPv6. Users with IPv4 Internet can only gain access to this if the router uses one of the tunnel technologies described below.
- **IPv6 via dual stack:** Dual stack refers to the parallel operation of IPv4 and IPv6 in a network.
- **IPv6 tunneling:** If a router does not have native IPv6 Internet access, it can still access IPv6 networks by means of a tunnel.

13.2 IPv6 Tunneling Technologies

13.2.1 6in4 Tunneling

6in4 tunnels are used to connect two hosts, routers, or to interconnect a host and router. This means that 6in4 tunnels can connect two IPv6 networks via an IPv4 network. The diagram shows a static 6in4 tunnel between the local router and a 6in4 gateway belonging to a tunnel broker.



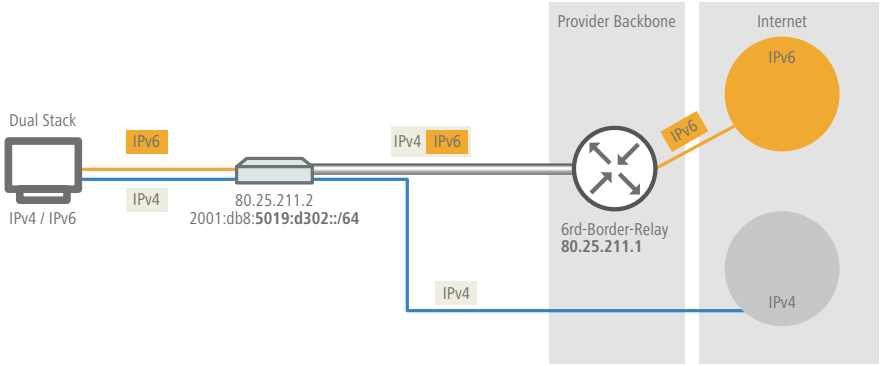
Unlike 6to4, these are dedicated services operated by a known provider. The end-points are fixed and the tunnel broker assigns a static prefix. The advantages of a 6in4 solution are that the gateways are fixed and the operator is known. The fixed prefix from the tunnel broker also determines the number of possible subnets that can be used. A 64-bit prefix (e.g. 2001:db8::/64) allows one subnet to be used. If a 48-bit prefix is used, 16 bits of the 64-bit prefix are available for use. This allows the implementation of up to 65,536 subnets.

The disadvantage of the 6in4 technology is the higher administrative effort. You must be registered with and login to the tunnel broker. In addition, the tunnel endpoints must be statically configured. Where a dynamic IPv4 address is used, the relevant data must be updated regularly. This can be automated by running a script on a router.

6in4 is a relatively secure and stable technology for providing IPv6 Internet access. This technology is thus suitable for operating web servers that are to be accessed over IPv6. The only drawback is the increased effort in administration. This technology is also suitable for professional use.

13.2.2 6rd Tunneling

6rd (rapid deployment) is a development of 6to4. The underlying function is identical. The difference is that just one particular relay is used, as operated by a provider. This solves the two basic problems of the 6to4 technology—the lack of security and stability. The prefix with 6rd is ??either configured manually or sent via DHCP (IPv4), which further reduces the effort involved with configuration. The diagram is a schematic representation of a 6rd scenario.

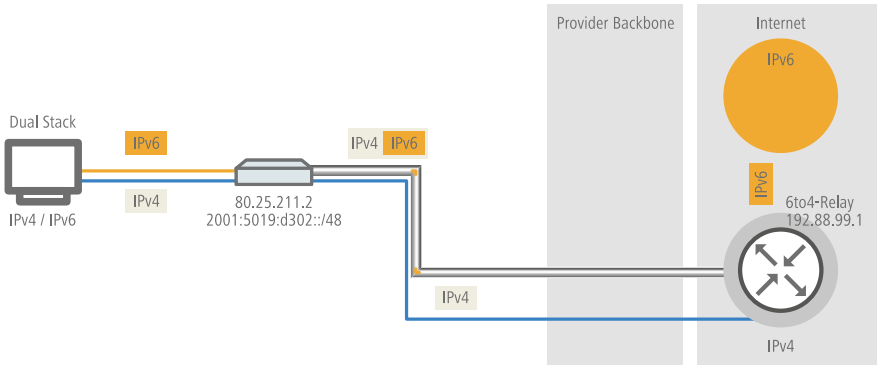


The provider assigns the router with a prefix (2001:db8::/32), which the router then supplements with its own IPv4 address. The IPv6 address generated in this way has the form: 2001:db8:5019:d302::/64. This makes 6rd interesting from two perspectives. The provider has a simple way to give its customers access to the IPv6 Internet. In addition, customers benefit from greatly simplified usage. They do not have to accept the security risks of 6to4, nor do they have to handle the complicated configuration of 6in4.

13.2.3 6to4 Tunneling

6to4 tunneling offers you an easy way to set up a data connection between two IPv6 networks via an IPv4 network. To this end, what is known as a 6to4 tunnel is set up:

- A router between a local IPv6 network and an IPv4 network serves to mediate between the networks.
- The router has both a public IPv4 address and an IPv6 address. The IPv6 address consists of an IPv6 prefix and the IPv4 address in hexadecimal notation. If a router has the IPv4 address 80.25.211.2, this will first be converted into hexadecimal notation: 5019:d302. Supplementing this is an IPv6 prefix (e.g. 2002::/16), so that the IPv6 address for the router appears as follows: 2002:5019:d302::/48.
- If a device in the IPv6 network sends data packets via the router to an IPv4 destination address, then the router first of all repacks the IPv6 packets and encapsulates them into a package with an IPv4 header. The router then forwards the encapsulated package to a 6to4 relay. The 6to4 relay unpacks the packet and forwards it to the desired destination. The following illustration shows the operating principle of 6to4 tunneling:



6to4 tunnels provide a dynamic data connection between IPv6 and IPv4 networks: The reply packets could be routed back using a different 6to4 relay as the one used on the way out. 6to4 tunnels are not a point-to-point connection. For every new data connection, the router always looks for the "nearest" public 6to4 relay. This is done using the anycast address 192.88.99.1. This aspect is an advantage of 6to4 tunneling on the one hand, but it also presents a disadvantage on the other. Public 6to4 relays do not require registration and are freely accessible. What's more, the dynamic data connection is easily configured. In this way it is possible for any user to create a 6to4 tunnel over a public relay, quickly and easily.

On the other hand, the dynamic data connection means that the user has no influence on the choice of the 6to4 relay. The provider of the relay is able to intercept or manipulate data.

13.3 DHCPv6

Compared to IPv4, clients in an IPv6 network do not require automatic address assignment from a DHCP server because they use auto-configuration. However, because certain information such as DNS server addresses are not transmitted during auto-configuration, certain application scenarios can benefit from a DHCP service on the IPv6 network.

13.3.1 DHCPv6 Server

The use of a DHCPv6 server is optional for IPv6. In principle, a DHCPv6 server supports two modes:

- **Stateless**: The DHCPv6 server does not distribute addresses but only information, such as DNS server addresses. Using this method, clients generate their own IPv6 addresses by 'stateless address auto-configuration (SLAAC)'. This method is particularly attractive e.g., for small networks in order to keep administration efforts to a minimum.
- **Stateful**: The DHCPv6 server distributes IPv6 addresses, similar to IPv4. This method is more complicated, since a DHCPv6 server has to assign and manage the addresses.

A DHCPv6 server distributes only the options that are explicitly requested by an IPv6 client, i.e. the server only assigns an address to a client if it explicitly requests one.

Additionally, the DHCPv6 server can pass on prefixes to routers for further distribution. This method is referred to as 'prefix delegation'. A DHCPv6 client must have explicitly requested this prefix, however.

13.3.2 DHCPv6 Client

The auto-configuration available with IPv6 networks makes it very easy and convenient to configure the clients.

However, in order for a client to receive additional information, such as a DNS server address, you must configure the device so that it can activate the DHCPv6 client when necessary.

The settings for the DHCPv6 client ensure that a device receiving certain flags in the router advertisement will start the DHCPv6 client, which can then send requests to the DHCPv6 server:

- **M flag**: If an appropriately configured device receives a router advertisement with the 'M flag' set, the DHCPv6 client will request an IPv6 address from the DHCPv6 server along with other information such as DNS server, SIP server and NTP server.
- **O flag**: With an 'O flag', the DHCPv6 client requests the DHCPv6 server for information such as a DNS server, SIP server and NTP server only, but not an IPv6 address.

  Note: If the 'M-flag' is set, the 'O-flag' does not necessarily have to be set as well.

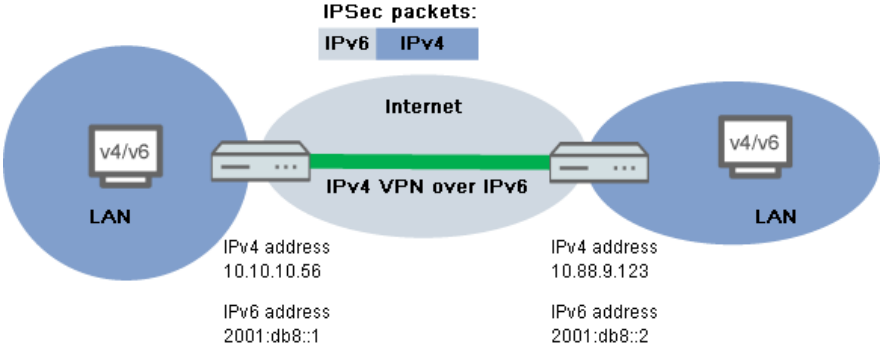
Note: With IPv6, the default route is distributed via router advertisements and not via DHCPv6.

13.4 IPv4 VPN Tunnel via IPv6

Until now it was not possible to set up a VPN between two remote stations using private IPv4 addresses to access the Internet (e.g. 3G/4G networking).

This restriction no longer exists with IPv6, because every IPv6 device receives a public IPv6 address. Thus IPv6 can be used to set up an IPv4 VPN tunnel to interconnect two remote IPv4 networks, regardless of the IPv4 WAN addresses used at each site.

In the example shown, two local IPv4 networks are connected via an IPv4 VPN tunnel, which is established over an IPv6 Internet connection. The IPv4 VPN packets are given IPv6 headers and sent to the remote site via the IPv6 Internet connection (either native or via tunnel broker).



13.4.1 Setup Wizard: IPv4 VPN Tunnel via IPv6 Setup

The Setup Wizard option "Connect two local area networks" helps you to set up a VPN connection.

☐ Start the Hirschmann LANconfig.

LANconfig now automatically searches the local network for devices. As soon as LANconfig has completed its search, it presents a list of all the devices it found, if possible with a brief description, the IP address and the status.

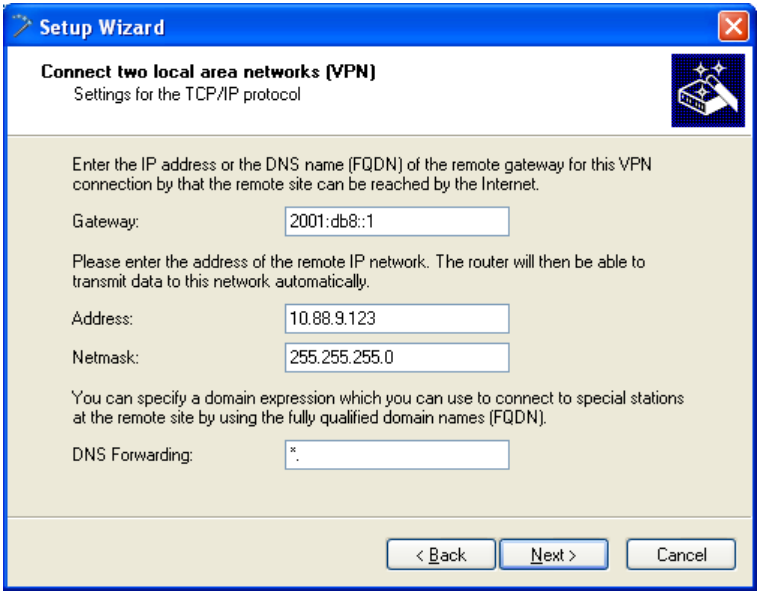
☐ Choose your device from the selection window in LANconfig and select the "Setup Wizard "button or use the menu under `Tools:Setup Wizard`.

LANconfig first reads out the device configuration and then displays the selection window with the optional applications.

☐ Launch the action "Connect two local area networks".

☐ Follow the Wizard’s instructions and enter the necessary data.

☐ As the gateway address, enter the IPv6 address of the gateway.



☐ You can then close the Wizard with "Finish".

The Setup Wizard writes the configuration to the device.

13.5 Dual-Stack Lite (DS-Lite)

Dual-Stack Lite, abbreviated DS-Lite, is used so that Internet providers can supply their customers with access to IPv4 servers over an IPv6 connection. That is necessary, for example, if an Internet provider is forced to supply its customer with an IPv6 address due to the limited availability of IPv4 addresses. In contrast to the other three IPv6 tunnel methods "6in4", "6rd" and "6to4", DS-Lite is also used to transmit IPv4 packets on an IPv6 connection (IPv4 viaIPv6 tunnel).

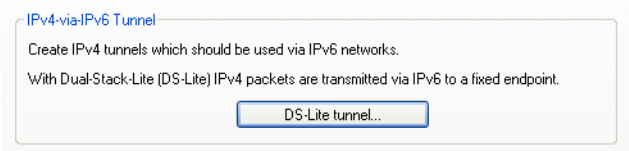
For this, the router packages the IPv4 packets in an IPv4-in-IPv6 tunnel and transmits them unmasked to the provider, who then performs a NAT with one of their own remaining IPv4 addresses.

To define a DS-Lite tunnel, the router only needs the IPv6 address of the tunnel endpoint and the routing tag with which it can reach this address.

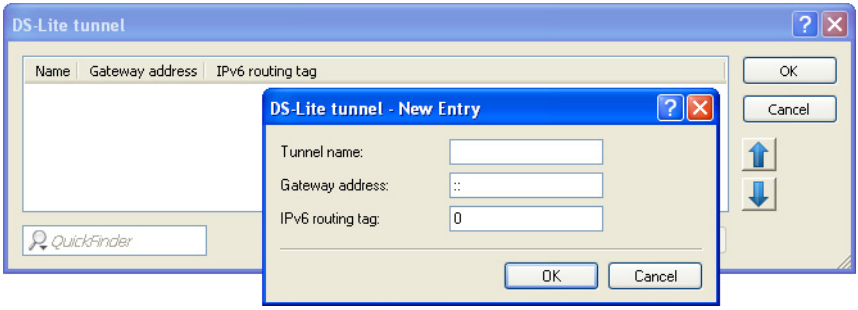
By default, the router uses the IPv4 address of the corresponding internal network, e.g., from "INTRANET". If you would like to define a different IP address instead (e.g., 192.0.0.2), it must be entered in the IP parameter list along with the remote site name of the DS-Lite tunnel.

Entering an IPv4 DNS server is not recommended for a DS-Lite tunnel, since its entries would unnecessarily fill the NAT table of the Internet provider.

You set up a DS-Lite tunnel in LANconfig via `IPv4 : Tunnel` by clicking on "DS-Lite tunnel".



Then click on the "Add" button and enter the designation of the tunnel, the IPv6 address of the gateway, and the routing tag.



☐ **Name of the tunnel**

This entry determines the name of the IPv4-over-IPv6 tunnel.

☐ **Gateway address**

This entry defines the address of the DS-Lite gateway, the so-called Address Family Transition Router (AFTR).

The following values are possible:

– One IPv6 address (e.g. 2001:db8::1)

– An FQDN (Fully Qualified Domain Name) that can be resolved by DNS, e.g., aftr.example.com

– The IPv6 unspecified address "::" determines that the device should retrieve the address of the AFTRs via DHCPv6 (default setting).

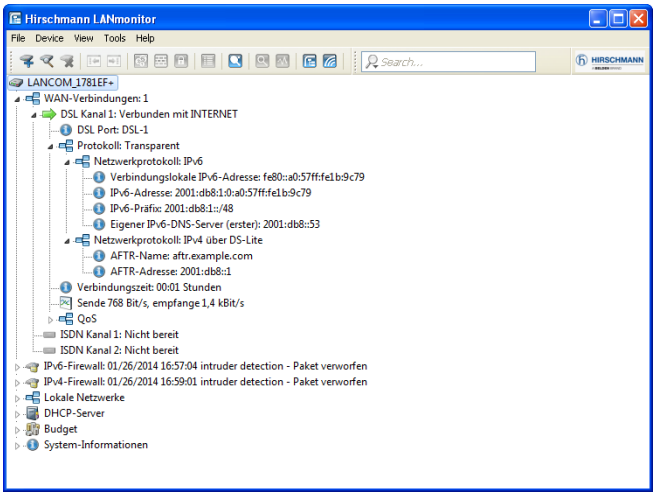
– An empty field behaves the same as the entry "::".

☐ **IPv6 routing tag**

The routing tag uniquely specifies the route to the DS-Lite gateway.

Note: With DS-Lite, since the NAT is performed by the provider, the function of many applications depends on the settings of the NAT provider (e.g., SIP, H.323, IRC or IPSec). PPTP does not work via DS-Lite at all. If the provider does not operate port forwarding, the IPv4 server services do not function.

The status table and the number of current DS-Lite connections can be shown using LANmonitor:

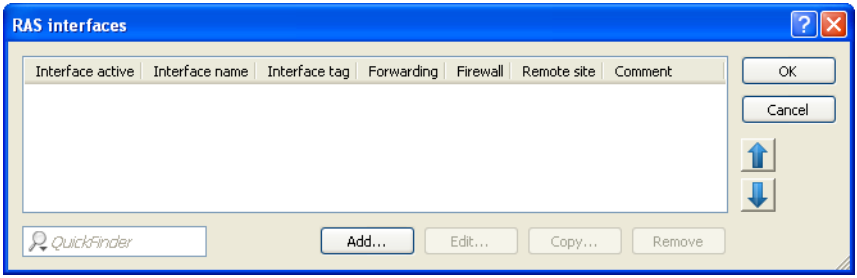


13.6 IPv6 support for RAS services

As of HiLCOS 8.90, RAS remote stations are able login via IPv6. The configuration is done in LANconfig under `IPv6 : General` and the setup of prefix pools under `IPv6 : Router advertisement`.

RAS interfaces

For RAS access via IPv6, you must also set up the corresponding "RAS interface".



Entries in the "RAS interfaces" table have the following meaning:

- "Interface active": Enable or disable this interface here.
- "Interface name": Here you define the name of the RAS interface that the IPv6 remote sites use for access.
- "Interface tag": The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

- "Forwarding": Enables or disables the forwarding of data packets to other interfaces.
- "Firewall": If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for each interface individually here. To globally enable the firewall for all interfaces, navigate to `Firewall/QoS : General` and check the option "IPv6 firewall/QoS enabled".

  Note: If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

- "Remote site": Specify the remote site or a list of remote sites for RAS dial-in users.

  The following values are possible:

  – An individual remote site from the table under `Setup : WAN : PPTP-Peers` or `Setup : PPPoE-Server : Name-List`.

  – The wildcard "*" makes the interface valid for all PPTP and PPPoE peers.

  – The "*" wildcard as a suffix or prefix of the peer, such as "COMPANY*" or "*TUNNEL" .

  By using wildcards you can implement template interfaces, which apply to peers which are named accordingly. In this manner, the name of the IPv6 RAS interface can be used many places in the IPv6 configuration.

- "Comment": Enter a descriptive comment for this entry.

Prefix pools

This table contains the pools of prefixes which RAS users receive when they connect remotely via IPv6. The following settings are possible:

☐ **Interface name**

Specifies the name of the RAS interface that is valid for this prefix pool.

☐ **First prefix**

Specifies the first prefix in the pool that is assigned to remote users by the router advertisement, e.g., "2001:db8::". Each user is assigned precisely one /64 prefix from the pool.

☐ **Last prefix**

Specifies the last prefix in the pool that is assigned to remote users by the router advertisement, e.g. '2001:db9:FFFF::'. Each user is assigned precisely one /64 prefix from the pool.

☐ **Prefix length**

Specifies the length of the prefix that the remote user is assigned by the router advertisement here. The size of the dial-in pool depends directly on the first and last prefix. Each user is assigned precisely one /64 prefix from the pool.

Note: In order for a client to be able to form an IPv6 address from the auto-configuration prefix, the prefix length must always be 64 bits.

☐ **SLAAC**

Specifies whether the prefix can be used for a stateless address auto-configuration (SLAAC).

13.7 IPv6 Firewall

13.7.1 Function

While the IPv4 firewall only controls the forwarding of IP data, the IPv6 firewall also regulates the functions of the access lists for all IPv6 server services. Therefore, the IPv6 firewall is similar to a classic firewall design, which separately supports the inbound and outbound communications, as well as forwarding. Since the HiLCOS device configuration specifically controls communication, HiLCOS does not require an outbound firewall.

13.7.2 Configuration

The configuration of the IPv6 firewall is practically the same as the IPv4 firewall; however, it is performed separately.

The inbound and forwarding firewalls each have their own rule tables, which are similar in scope and structure to the IPv4 firewall.

The rules are sorted with decreasing priority, i.e. the rule with the highest priority is at the top of the list. Rules of the same priority are sorted by their precision, analogous to the IPv4 procedure. If a rule requires further actions, these are also performed by firewall in sequence. Otherwise, firewall filtering is terminated after the current rule has been applied.

13.7.3 Default Entries for the IPv6 Firewall Rules

By default, IPv6 firewall has a number of filter rules that are applied on incoming data streams.

Default Entries for the Inbound Rules

This table contains the rules that the firewall will apply to inbound connections. The factory settings provide the following rules for the most important applications:

- **ALLOW-ICMP, ACCEPT**:
  Allow all connections using ICMPV6.
- **ALLOW-DHCP-CLIENT, ACCEPT**:
  Allow communication with the DHCPv6 client.
- **ALLOW-DHCP-SERVER, ACCEPT**:
  Allow communication with the DHCPv6 server.
- **ALLOW-CONFIG-LOCALNET, ACCEPT**:
  Allow configuration in the local network via HTTP, HTTPS, SNMP, SSH, TELNET, TFTP.
- **ALLOW-VPN-CONFIG, ACCEPT-VPN**:
  Allow HTTP, HTTPS, SNMP, SSH, TELNET, and TFTP communication via VPN.
- **ALLOW-DNS-SERVER, ACCEPT**:
  Allow communication with the internal DNS server from the local network.
- **ALLOW-DNS-SERVER-VPN, ACCEPT-VPN**:
  Allow communication with the internal DNS server via VPN.
- **DENY-ALL, REJECT-SNMP**:
  Block all communication and inform the admin via SNMP.
- **ALLOW-CONFIG-WAN, ACCEPT**:
  Allow communication via the WAN interface via HTTPS, SSH. (disabled)

- **ALLOW-IPSEC, ACCEPT**:
  Allow all VPN communication over IPSec. (disabled)
- **ALLOW-IPSEC-HTTPS-ENCAPSULTION, ACCEPT**:
  Allow the use of IPSec over HTTPS. (disabled)

Default Entries for the Forwarding Rules

This table contains the rules that the firewall will apply for forwarding data. The factory settings provide the following rules for the most important applications:

- **ALLOW-VPN, ACCEPT-VPN**:
  Allow all data connections using IPSec.
- **DENY-ALL, REJECT-SNMP**:
  Block all communication via SNMP.
- **ALLOW-OUTBOUND, ACCEPT-VPN**:
  Allow all outbound communication.

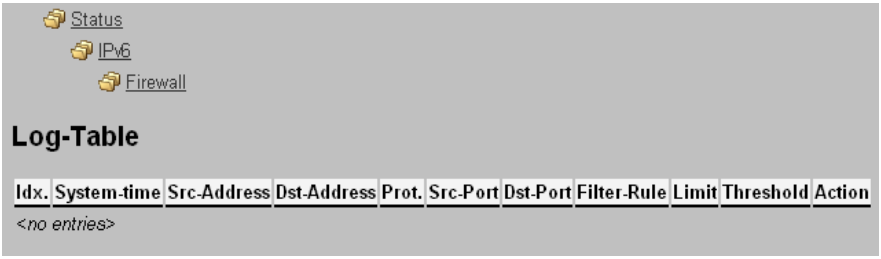
13.7.4 IPv6 Firewall Log Table

Similar to the IPv4 firewall, the IPv6 firewall provides a log table of events in the IPv6 environment.

The syntax of the log table is the same as the IPv4 log table with the exception of the IP address format (IPv6 addresses are in hexadecimal format, IPv4 in decimal format).

Analyzing the IPv6 Firewall Log Table with WEBconfig

You can open IPv6 log tables in WEBconfig with `HiLCOS menu tree:Status:IPv6:Firewall:Log table`.



The items have the following meanings:

- "Idx.": Sequential index. Furthermore, the table can also be checked via SNMP.
- "System time": System time in UTC encoding (converted to plain text for display).
- "Source address": Source address of the filtered packet.
- "Destination address": Destination address of the filtered packet
- "Prot.": Protocol (TCP, UDP, etc.) of the filtered packets.
- "Source port": Source port of the filtered packet (only for port related protocols).
- "Destination port": Destination port of the filtered packet (only for port related protocols).
- "Filter rule": Name of the rule that created the entry.
- "Limit": Bit field containing the description of the limit that caused the firewall to apply the filter. There following values are currently defined:
  - 0x01: Absolute number
  - 0x02: Number per second
  - 0x04: Number per minute
  - 0x08: Number per hour:
  - 0X10: Global limit
  - 0x20: Byte limit (if not set, it is a packet limit)
  - 0x40: Limit only applies in the inbound direction
  - 0x80: Limit only applies in the outbound direction

- "Threshold":Threshold limit value of the triggering limit.
- "Action": Bit field which lists all the actions performed. There following values are currently defined:
  - 0x00000001: Accept
  - 0x00000100: Reject
  - 0x00000200: Establish filter
  - 0x00000400: Internet (default router) filter
  - 0x00000800: Drop
  - 0x00001000: Disconnect
  - 0x00004000: Lock source address
  - 0x00020000: Lock destination address and port
  - 0X20000000: Send SYSLOG notification message
  - 0x40000000: Send SNMP trap
  - 0x80000000: Send e-mail

Note: All firewall actions also appear in the IP router trace .

Analyzing the IPv6 Firewall Log Table with LANmonitor

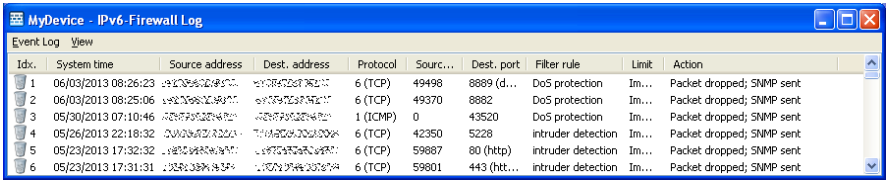
You can view the IPv6 log for a specific device in the LANmonitor.

Do this by starting LANmonitor from the link in the Windows Start menu. You can also launch the LANmonitor for a specific device with the context menu in LANconfig or with the keyboard shortcut `Ctrl + M`.

Via `Device:View firewall event log` you can view the firewall events for a selected device. The firewall events show the last 100 actions of the firewall with the following details:

- "Idx"
- "Timestamp"
- "Src address"
- "Dst address"

- "Protocol"
- "Src port"
- "Dst port"
- "Firewall rule"
- "Limit"
- "Action"



13.8 Additional Command-line Commands

Various IPv6 functions can be queried at the command line. The following command-line functions are available:

- „IPv6 Addresses“: `show ipv6-adresses`
- „IPv6 Prefixes“: `show ipv6-prefixes`
- „IPv6 Interfaces“: `show ipv6-interfaces`
- „IPv6 Neighbor Cache“: `show ipv6-neighbour-cache`
- „IPv6 DHCP Server“: `show dhcp6-server`
- „IPv6 DHCP Client“: `show dhcpv6-client`
- „IPv6 Route“: `show ipv6-route`

Additionally, IPv6 communications can be followed with the `trace` command (see page 998).

13.8.1 IPv6 Addresses

The command `show ipv6-addresses` shows a list of IPv6 addresses that are currently being used. This is sorted by interface. Note that an interface can have multiple IPv6 addresses. One of these addresses is always the link-local address, which starts with `fe80:`.

The output is formatted as follows:

<Interface> :

<IPv6 address>, <status>, <attribute>, (<type>)

Table 9: Components of the Command-line Output show ipv6-addresses:

Output	Comment
Interface	The name of the interface
IPv6 address	The IPv6 address
Status	The status field can contain the following values: ▶ TENTATIVE Duplicate Address Detection (DAD) is currently checking the address. It is not yet available for unicast. ▶ PREFERRED The address is valid ▶ DEPRECATED The address is still valid, but it is being discontinued. The optimal status for communication is PREFERRED. ▶ INVALID The address is invalid and cannot be used for communication. An address given this status after its lifetime has expired.
Attribute	Shows an attribute of the IPv6 address. Possible attributes are: ▶ None No special attributes ▶ (ANYCAST) This is an anycast address ▶ (AUTO CONFIG) The address was retrieved by auto-configuration ▶ (NO DAD PERFORMED) No DAD is performed
Type	The type of IP address

13.8.2 IPv6 Prefixes

The command `show ipv6-prefixes` displays all known prefixes. These are sorted according to the following criteria:

- **Delegated prefixes:** All prefixes that the router has obtained by delegation.
- **Advertised prefixes:** All prefixes that the router announces in its router advertisements.
- **Deprecated prefixes:** All prefixes that are being discontinued. These may still be functional, but they will be deleted after a certain time.

13.8.3 IPv6 Interfaces

The command `show ipv6-interfaces` displays a list of IPv6 interfaces and their status.

The output is formatted as follows:

<Interface> : <Status>, <Forwarding>, <Firewall>

Table 10: Components of the Command-line Output show ipv6-interfaces:

Output	Comment
Interface	The name of the interface
Status	The status of the interface Possible entries are: ▶ oper status is up ▶ oper status is down
Forwarding	The forwarding status of the interface. Possible entries are: ▶ forwarding is enabled ▶ forwarding is disabled

Table 10: Components of the Command-line Output show ipv6-interfaces:

Output	Comment
Firewall	The status of the firewall. Possible entries are: ▶ forwarding is enabled ▶ firewall is disabled

13.8.4 IPv6 Neighbor Cache

The command `show ipv6-neighbor-cache` displays the current neighbor cache.

The output is formatted as follows:

<IPv6 address> iface <interface> lladdr <MAC address> (<switch port>) <device type> <status> src <source>

Table 11: Components of the Command-line Output show ipv6-neighbor-cache:

Output	Comment
IPv6 address	The IPv6 address of the neighboring device
Interface	The interface where the neighbor is accessed
MAC address	The MAC address of the neighbor
Switch port	The switch port on which the neighbor was found
Device type	Neighbor's device type (host or router)

Table 11: Components of the Command-line Output show ipv6-neighbor-cache:

Output	Comment
Status	The status of the data connection to neighboring devices. Possible entries are: ▶ INCOMPLETE Resolution of the address was still in progress and the link-layer address of the neighbor was not yet determined. ▶ REACHABLE The neighbor was reached in the last 10 seconds. ▶ STALE The neighbor is no longer qualified as REACHABLE, but an update will only be performed when an attempt is made to reach it. ▶ DELAY The neighbor is no longer qualified as REACHABLE, but data was recently sent to it; waiting for verification by other protocols. ▶ PROBE The neighbor is no longer qualified as REACHABLE. Neighbor solicitation probes are sent to it to confirm availability.
Source	The IPv6 address at which the neighbor was detected.

13.8.5 IPv6 DHCP Server

The command `show dhcpv6-server` displays the current status of the DHCP server. The display includes information about the interface on which the server is active, which DNS server and prefixes it has, and what client preferences it has.

13.8.6 IPv6 DHCP Client

The command `show dhcpv6-client` displays the current status of the DHCP client. The display includes information about the interface being used by the client and the prefixes and DNS server that it is using.

13.8.7 IPv6 Route

The command `show ipv6-route` displays the complete IPv6 routing table. Routers with fixed entered routes are displayed with the suffix [static] and the dynamically obtained routes have the suffix [connected]. The loopback address is marked [loopback]. Other automatically generated addresses have the suffix [local].

13.8.8 Release IPv6 Address

Table 12: Command for IPv6 address release

Command	Description
Release [-x] <Interface 1> ... <Interface n>	The DHCPv6 client returns its IPv6 address and/or its prefix to the DHCPv6 server. It then submits a new request for an address or prefix to the DHCPv6 server. Depending on the provider, the server assigns a new address to the client, or reassigns the previous one. Whether the client receives a different address or prefix is determined solely by the server. The option switch `-x` suppresses the confirmation message. The `*` wildcard applies the command on all of the interfaces and prefix delegations.

13.8.9 Overview of Parameters

Note: The traces available for a particular model can be displayed by entering `trace` without any arguments.

Table 13: Overview of Trace Parameters

This parameter ...	...causes the following message in the trace:
Status	Data connection status messages
Error	Data connection error messages
IPX router	IPX routing
PPP	PPP protocol negotiation
SAP	IPX service advertising protocol
IPX watchdog	IPX watchdog spoofing
SPX watchdog	SPX watchdog spoofing
LCR	Least-cost router

Table 13: Overview of Trace Parameters

This parameter ...	**...causes the following message in the trace:**
Script	Script negotiation
IPX RIP	IPX routing information protocol
Firewall	Displays firewall events
RIP	IP routing information protocol
ARP	Address resolution protocol
ICMP	Internet control message protocol
IP Masquerading	Events in the masquerading module
DHCP	Dynamic host configuration protocol
NetBIOS	NetBIOS administration
DNS	Domain name service protocol
Packet dump	Displays the first 64 bytes of a packet in hexadecimal
D channel dump	Traces the D channel of the ISDN bus connected
ATM cell	ATM packet level
ATM error	ATM error
ADSL	ADSL link status
SMTP client	Email processing with the integrated mail client
Mail client	Email processing with the integrated mail client
SNTP	Simple network time protocol
NTP	Time server trace
Connact	Messages from the activity protocol
Cron	Activities of the scheduler (cron table)
RADIUS	RADIUS trace
Serial	Information on the state of the serial interface
USB	Information on the state of the USB interface
Load balancer	Information on load balancing
VRRP	Information about the virtual router redundancy protocol
Ethernet	Information on the Ethernet interfaces
VLAN	Information on virtual networks
IGMP	Information about the Internet group management protocol
WLAN	Information on activity in the wireless networks
IAPP	Trace of the inter-access point protocol, displays information about WLAN roaming.
DFS	Trace on dynamic frequency selection, automatic channel selection in the 5 GHz wireless LAN band
Bridge	Information on the wireless LAN bridge
EAP	Trace on EAP, the key negotiation protocol used with WPA/802.11i and 802.1x
Spgtree	Information on the spanning tree protocol
LANAUTH	LAN authentication (e.g. Public Spot)
SIP-Packet	SIP information that is exchanged between a VoIP router and a SIP provider or a upstream SIP telephone system
VPN status	IPSec and IKE negotiations
VPN packet	IPSec and IKE packets
XML-Interface-PbSpot	Messages from the Public Spot XML interface
IPv6 config	Information on the IPv6 configuration
IPv6 firewall	IPv6 firewall events
IPv6-Interfaces	Information about the IPv6 interfaces
IPv6-LAN-Packet	Data packets over the IPv6 LAN connection
IPv6-Router	Information about the IPv6 routing
IPv6-WAN-Packet	Data packets over the IPv6 WAN connection

13.9 Enhancements to LANconfig

13.9.1 IPv6 configuration menu

Where previous versions provided configuration menus for TCP/IP for IPv4, you now find the options "IPv4" and "IPv6".

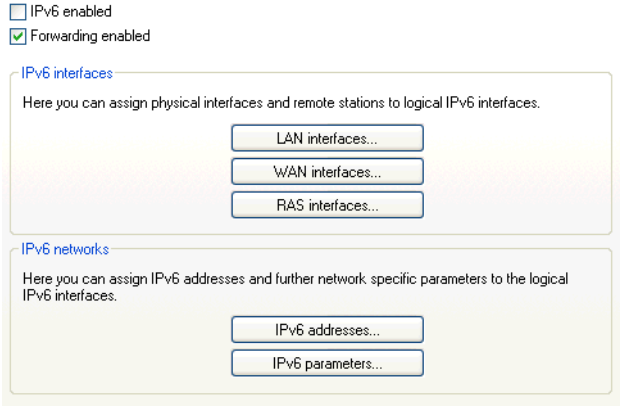
Click on "IPv6" to adjust the settings for this protocol. The "IPv6" configuration is divided into the options By default a click on "IPv6" takes you straight to the "General" options.

- "General",
- "Router advertisement",
- "DHCPv6" and
- "Tunnel".

General

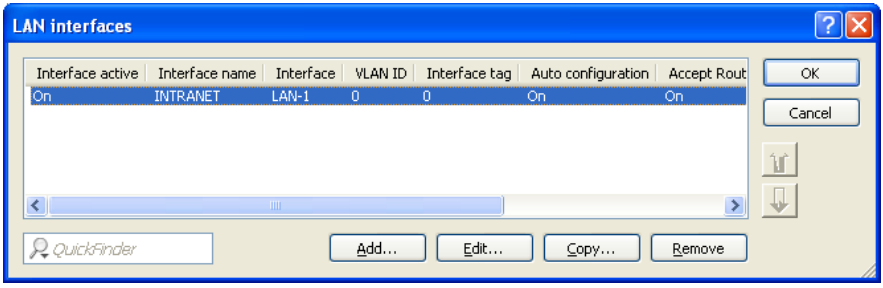
This is where you make the basic settings.

- "IPv6 enabled:" This is where you can enable or disable IPv6 for the device.
- "Forwarding enabled:" Forwarding is used for packet forwarding between IPv6 interfaces. This option is activated by default.



- The buttons "LAN interfaces" and "WAN interfaces" access the tables where you can add new interfaces, configure existing interfaces, or delete them.

For each existing IPv4 network, you must create an equivalent IPv6 network under "LAN interfaces". Here, the settings for interface binding, routing tag, and VLAN ID must match the settings of the corresponding IPv4 network settings. Because a device can have multiple IPv6 addresses, you must add statically configured IPv6 addresses under "IPv6 addresses".



Entries in the "LAN interfaces" table have the following meaning:

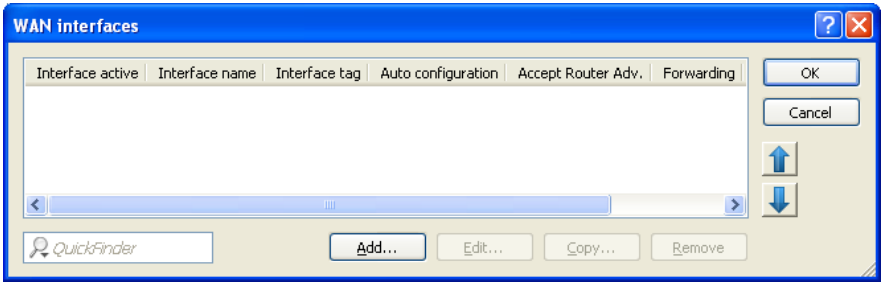
- "Interface active": Activates or deactivates this LAN interface.
- "Interface name" or "Network name": Enter a name for the logical IPv6 interface which is to apply to the physical interface (interface assignment) and the VLAN ID.

- "Interface": Select the physical interface to be combined with the VLAN ID to form the logical IPv6 interface. With IPv6, the mapping "any" used with IPv4 is no longer possible.
- "VLAN ID": Select the VLAN ID to be combined with the physical interface to form the logical IPv6 interface.
- "Interface tag": The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
- "Autoconfiguration": Enable or disable the automatic configuration of addresses (SLAAC or DHCPv6) for this interface in the client role.

  Note: If the device itself sends router advertisements from this interface, it does not produce IPv6 addresses from received router advertisements from other routers, even when auto-configuration is enabled.

- "Accept router advertisements": Enables or disables the processing of received router advertisement messages. With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.
- "Forwarding": Enables or disables the forwarding of data packets to other interfaces. With forwarding disabled, no router advertisements are transmitted from this interface.
- "MTU": Here you set the valid MTU for the corresponding link.
- "Firewall": If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here.
- "Comment": Enter a descriptive comment for this entry.

For each remote station with which you want to communicate using IPv6, you must additionally create an equivalent logical IPv6 WAN interface under "WAN interfaces". The name of the IPv6 WAN interface must match the name of the IPv4 remote station.

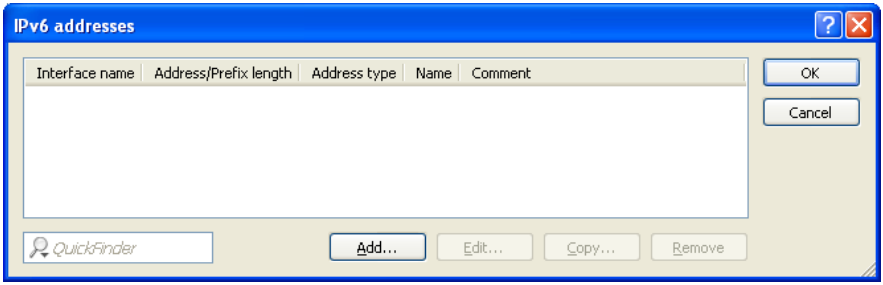


Entries in the "WAN interfaces" table have the following meaning:

- "Interface active": Activates or deactivates this WAN interface.
- "Interface name": The name of the logical IPv6 interface must match that of the corresponding IPv4 connection.
- "Interface tag": The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
- "Autoconfiguration": Enable or disable the automatic configuration of addresses (SLAAC or DHCPv6) for this interface in the client role.
- "Accept router advertisements": Enables or disables the processing of received router advertisement messages. With processing disabled, the device ignores any prefix, DNS and router information received via router advertisements.
- "Forwarding": Enables or disables the forwarding of data packets to other interfaces. With forwarding disabled, no router advertisements are transmitted from this interface.
- "Firewall": If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for an individual interface here.
- "Comment": Enter a descriptive comment for this entry.

The buttons "IPv6 addresses" and "IPv6 parameters" are used to assign IPv6 addresses to interfaces and to configure the interface parameters (gateway address, primary and secondary DNS).

The "IPv6 addresses" table is used to create IPv6 addresses for LAN and WAN interfaces.



Entries in the "IPv6 addresses" table have the following meaning:

- "Interface name": Give a name to the interface that you want to assign the IPv6 network.
- "Address/prefix length": Specify an IPv6 address including the prefix length for this interface.

  The default prefix length is ?64 bits ("/64")?. If possible do not use IPv6 addresses with longer prefixes, as many IPv6 mechanisms in the device (e.g. autoconfiguration) are designed for a maximum length of 64 bits.

  Example:

  - Global unicast address: "2001:db8::1/64"
  - Unique local address: "fd00::1/64"

  Note: Link-local addresses are fixed and not configurable.

- "Address type": Specify the type of IPv6 address.

  Options:

  - Unicast
  - Anycast
  - EUI-64

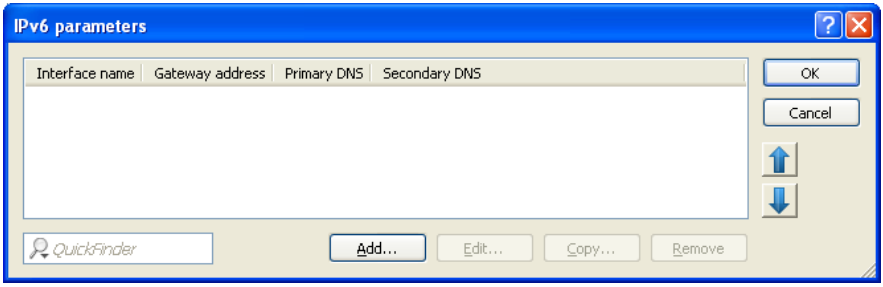
With the address type EUI-64, IPv6 addresses conform to the IEEE standard "EUI-64". The MAC address of the interface thus forms a uniquely identifiable part of the IPv6 address. The correct input format for an IPv6 address including the prefix length as per EUI-64 would be: "2001:db8:1::/64". "EUI-64" ignores any value set as interface identifier in the corresponding IPv6 address and replaces it with an interface identifier as per "EUI-64". The prefix length for "EUI-64" must be "/64".

With the Unicast address type, you use the "Address/prefix length" field to specify a full IPv6 address along with its interface identifier, e.g. "2001:db8::1234/64".

With the Anycast address type, you can also use the "Address/prefix length" field to specify a full IPv6 address along with its interface identifier, e.g. "2001:db8::1234/64". Internally, the device handles this address as an anycast address.

- "Name": Enter a descriptive name for this combination of IPv6 address and prefix.
- "Comment": Enter a descriptive comment for this entry.

The table "IPv6 parameters" is used to manually configure static parameters for LAN or WAN interfaces, IPv6 DNS servers, and IPv6 gateways if you choose not to use autoconfiguration or DHCPv6.



Entries in the "IPv6 parameters" table have the following meaning:

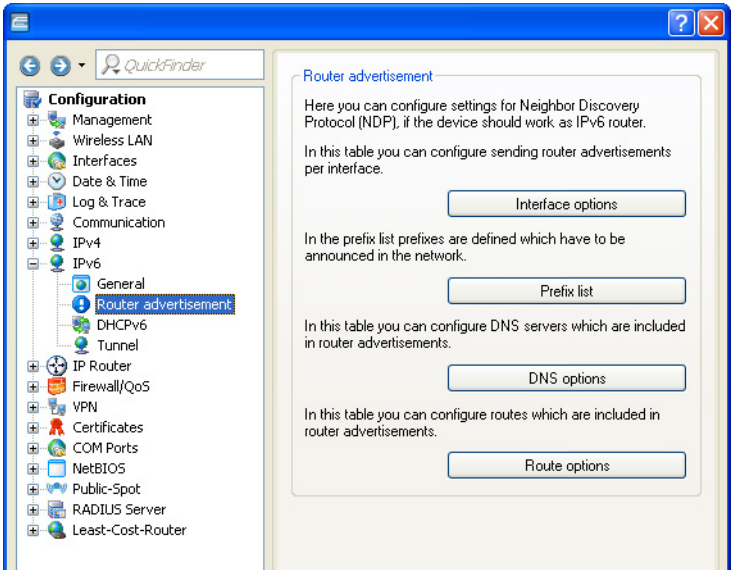
- "Interface name": Give a name to the interface for which the IPv6 parameters are to be configured.
- "Gateway address": Specify the IPv6 gateway to be used by this interface.

Note: This parameter overrides gateway information that the device may receive via router advertisements, for example.

- "Primary DNS": Specify the primary IPv6 DNS server to be used by this interface.
- "Secondary DNS": Specify the secondary IPv6 DNS server to be used by this interface.

Router Advertisement

The "Router advertisement" configuration provides you with four buttons for setting up the Neighbor Discovery Protocol (NDP) if the device is to operate as an IPv6 router:



Each button opens a table with the settings for the corresponding function:

Interface options:

Here you can enable or disable the following interface functions:

☐ "Send router advertisement"
Controls the periodic transmission of router advertisements and the response to router solicitations.

☐ "Managed flag"
With this function enabled, clients receiving this router advertisement will configure their addresses with stateful autoconfiguration (DHCPv6). Clients then automatically retrieve other information, such as the DNS server.

☐ "Other flag"
If this function is active, a client will attempt to obtain additional information via DHCPv6, such as DNS server addresses. For each prefix, you can specify whether or not a client should form addresses by auto-configuration: Navigate to the "Prefix list" under "Allow auto-configuration (SLAAC)".

☐ "Default router"
Defines how the device advertises itself as the default gateway or router. The parameters have the following functions:

- "Automatic": As long as a WAN connection exists, the device sends a positive router lifetime in the router advertisement messages. The result is that a client uses this router as the default gateway.

  If there is no WAN connection, the router sets the router lifetime to "0". A client then stops using this router as the default gateway.
- "Always": The router lifetime is always positive—i.e. greater than "0"—irrespective of the WAN connection status.
- "Never": The router lifetime is always "0".

☐ "Router priority"
Defines the preference of this router. Clients enter this preference into their local routing tables.

Prefix list:

Set the prefix options for the interfaces that are being used. The following settings are possible:

☐ "Prefix"
Enter a prefix that is announced with router advertisements, e.g. "2001:db8::/64". The prefix length must always be exactly "/64", otherwise it will be impossible for clients to generate their addresses by adding their interface identifiers (with a length of 64 bits). If a prefix delegated by the provider is to be propagated automatically, set "::/64" here and enter the name of the corresponding WAN interface as the parameter "Receive prefix from".

☐ "Subnet ID"
Here you enter the subnet ID that is to be combined with the prefix delegated by the provider. If the provider assigns the prefix "2001:db8:a::/48", for example, and the subnet ID is "0001" (or "1" for short), then the router advertisement on this interface is given the prefix "2001:db8:a:0001::/64". The maximum subnet length with a 48-bit long delegated prefix is ??16 bits (i.e. 65,536 subnets), with available subnet IDs ranging from "0000" to "FFFF". With a delegated prefix of "/56", the maximum subnet length is 8 bits (i.e. 256 subnets) with subnet IDs ranging from "00" to "FF". In general, the subnet ID "0" is used when the WAN IPv6 address is formed automatically. This is why subnet IDs for LANs start at "1". The default setting is "1".

☐ "Allow auto-configuration (SLAAC)"
Specifies whether the prefix is to be used for a stateless address autoconfiguration (SLAAC). The default setting is "enabled".

☐ "Receive prefix from"
Specifies the name of the interface used to receive a prefix via DHCPv6 prefix delegation or tunnel. This prefix can be used to derive and propagate a subnet for each interface.

DNS options

Specifies the DNS information in router advertisements according to RFC6106. The following settings are possible:

☐ "Interface name"
Name of the interface on which the IPv6 DNS server announces information in router advertisements.

☐ "Primary DNS"

IPv6 address of the first IPv6 DNS server (recursive DNS server, RDNSS, according to RFC 6106) for this interface.

- ☐ "Secondary DNS"
  IPv6 address of the secondary IPv6 DNS server for this interface.
- ☐ "Import DNS search list from the internal DNS server"
  Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain can be configured under `IPv4:DNS:General settings`. The default setting is "enabled".
- ☐ "Import DNS search list from WAN"
  Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. This feature is available only if the prefix list is connected to the corresponding WAN interface under "Receive prefix from".

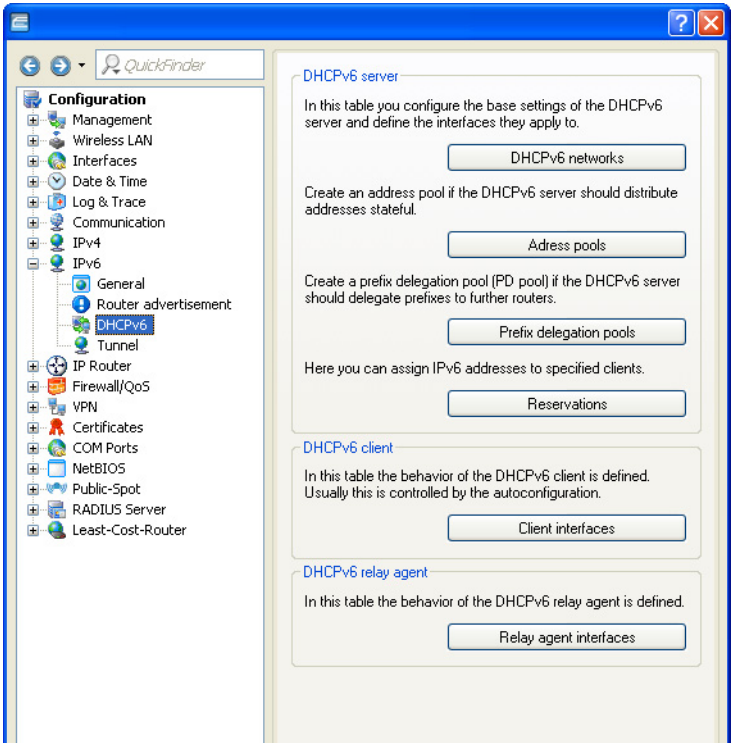
Route options

Specifies the route option in router advertisements according to RFC 4191 (Route Information Option). The following settings are possible:

- ☐ "Interface name"
  Specifies the name of the logical interface to be used for sending router advertisements with this route option.
- ☐ "Prefix"
  Prefix of the route option, e.g."2001:db8::/32".
- ☐ "Route preference"
  The preference of the route. Possible values are "high", "medium" (default) and "low".

DHCPv6

This is where you configure the DHCPv6 server, the DHCPv6 client and the DHCPv6 relay agent.

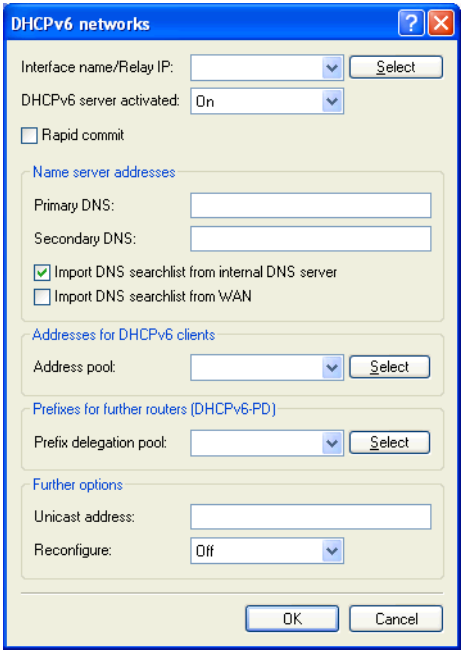


DHCPv6 server

Use the following buttons to access the tables and adjust the respective functions:

DHCPv6 networks

This table is used to configure the basic settings of the DHCPv6 server, and to specify which interfaces they apply to.



- ☐ "Interface name/Relay IP"
  Name of the interface on which the DHCPv6 server is working, for example "INTRANET". Alternatively, you can also enter the IPv6 address of the remote DHCPv6 relay agent.
- ☐ "DHCP server activated"
  Activates or deactivates the entry.
- ☐ "Rapid commit"
  With rapid commit activated, the DHCPv6 server responds directly to a solicit message with a reply message.

  Note: The client must explicitly include the rapid commit option in its solicit message.
- ☐ "DNS default"
  IPv6 address of the primary DNS server.
- ☐ "DNS backup"
  IPv6 address of the secondary DNS server.
- ☐ "Import DNS search list from internal DNS server"

Indicates whether the DNS search list or the own domain for this logical network should be inserted from the internal DNS server, e.g., "internal". The own domain can be configured under `IPv4:DNS:General settings`. The default setting is "enabled".

☐ "Import DNS search list from WAN"
Specifies whether the DNS search list sent by the provider (e.g., provider-xy.de) is announced in this logical network. The default setting is "disabled".

☐ "Address pool"
Name of the address pool used for this interface.

Note: If the DHCPv6 server operates 'stateful' addresses distribution, you must enter the corresponding addresses into the "Address pools" table.

☐ "Prefix delegation pool"
Name of prefix pools to be used by the DHCPv6 server.

Note: If the DHCPv6 server is to delegate prefixes to other routers, you must enter the corresponding prefixes in the table "Prefix delegation pools".

☐ "Unicast address"

By default the DHCPv6 server exclusively responds to multicast requests. If the DHCPv6 server should respond to a unicast request, this IPv6 address can be configured here. Generally speaking, multicast is sufficient for communication.

☐ "Reconfigure"

Each IPv6 address or IPv6 prefix has a default life time assigned by the server. At certain intervals, a client asks the server to renew its address (called renew/rebind times).

However, if the WAN prefix changes, for example, due to disconnection and reconnection of an Internet connection or a request for a new prefix (Deutsche Telekom Privacy feature), the server has no way to inform the network devices that the prefix or address has changed. This means that a client is still using an old address or an old prefix, and can no longer communicate with the Internet.

The reconfigure feature allows the DHCPv6 server to require the clients in the network to request a renewal of leases / bindings. If the client successfully negotiates a re-configuration (reconfigure) with the server during first contact, the server can request the client to update its address or other information at any time. The mechanism is protected by the so-called **Reconfigure Key**, so that only the original server with the correct key can make requests to the client. If the client receives a reconfigure message without a valid reconfigure key, the client rejects this invocation.

The **Reconfigure Key Authentication Protocol** according to RFC 3315 is supported for **Renew** and **Information-Request**, as well as **Rebind** according to RFC 6644. Reconfiguration is started on the console of the device using a "do" command in the status tree (see the description of the status tree).

Note: You can find more about the status of a client regarding the Reconfigure function under `Status:IPv6:DHCPv6:Server:Clients`.

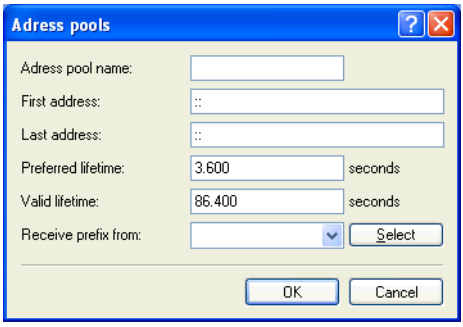
The following settings are available:

- "Off": Disables the reconfigure function
- "Reject": Clients that have used the Reconfigure Option in queries are rejected by the server and are not assigned an address, prefix or other options.

- "Allow": If the client sets the Reconfigure Option in queries, the server negotiates the necessary parameters with the client in order to start a reconfiguration at a later time.
- "Require": Clients have to set the Reconfigure Option in queries, otherwise the client rejects these clients. This mode is makes sense when you want to ensure that the server only serves clients which support Reconfigure. This ensure that all clients can use Reconfigure to update their addresses, prefixes, or other information at a later point in time.

Address pools

If distribution of the DHCPv6 server is to be stateful, this table defines an address pool:



☐ "Address pool name"
Name of the address pool

☐ "Start address"
First address in the pool, e.g. "2001:db8::1"

☐ "End address"
Last address in the pool, e.g. "2001:db8::9"

☐ "Preferred lifetime:"
Here you specify the time in seconds that the client should treat this address as 'preferred'. After this time elapses, a client classifies this address as "deprecated".

☐ "Validity period"
Here you specify the time in seconds that the client should treat this address as 'valid'.

Note: If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

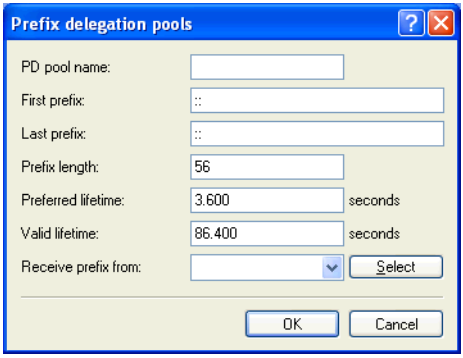
☐ "Receive prefix from"
With this parameter you can assign addresses to the network clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then enter the value "::1" in the parameter "First address" and "::9" in "Last address". In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g.,"/48" or "56", you must take subnetting for the logical network in to account in the address. **Example:**

- Assigned provider prefix: "2001:db8:abcd:aa::/56"
- "/64" as the prefix of the logical network (subnet ID 1): "2001:db8:abcd:aa01::/64"
- First address: "0:0:0:0001::1"
- Last address: "0:0:0:0001::9"

Note: You should only use this mechanism if the provider assigns a fixed prefix. Otherwise, it is possible that the provider delegates a new prefix to the router, but the client still has an address from the pool with the old prefix. In this case, the client must update its address at the server.

Prefix delegation pool

In this table, you specify the prefixes that the DHCPv6 server delegates to other routers:



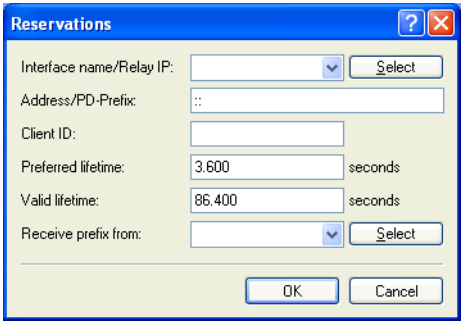
- ☐ "PD pool name"
  Name of the PD pool
- ☐ "First prefix"
  First prefix for delegation in the PD pool, e.g. "2001:db8:1100::"
- ☐ "Last prefix"
  Last prefix for delegation in the PD pool, e.g. "2001:db8:FF00::"
- ☐ "Prefix length"
  Length of the prefixes in the PD pool, e.g. "56" or "60"
- ☐ "Preferred lifetime:"
  Here you specify the time in seconds that the client should treat this prefix as 'preferred'. After this time elapses, a client classifies this address as "deprecated".
- ☐ "Validity period"
  Here you specify the time in seconds that the client should treat this prefix as 'valid'.

  Note: If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

- ☐ "Receive prefix from"
  Name of the WAN interface from which the client should use the prefix to form the address or prefix.

Reservations

If you want to assign fixed IPv6 addresses to clients or fixed prefixes to routers, you can use this table to make a reservation for each client.



☐ "Interface name or relay"
Name of the interface on which the DHCPv6 server is working, for example "INTRANET". Alternatively, you can also enter the IPv6 address of the remote relay agent.

☐ "Address/PD prefix"
IPv6 address or PD prefix that you want to assign statically.

☐ "Client ID"
DHCPv6 unique identifier (DUID) of the client.

DHCPv6 clients are no longer identified with their MAC addresses like DHCPv4 clients, they are identified with their DUID instead. The DUID can be read from the respective client, for example, on Windows with the shell command `ipconfig /all` or in WEBconfig under `Status:IPv6:DHCPv6:Client:Client ID`.

For devices working as a DHCPv6 server, the client IDs for clients that are currently using retrieved IPv6 addresses are to be found under `Status:IPv6:DHCPv6:Server:Address bindings`, and retrieved IPv6 prefixes are under `Status:IPv6:DHCPv6:Server:PD bindings`.

LANmonitor displays that client IDs under "DHCPv6 server".

☐ "Preferred lifetime:"
Here you specify the time in seconds that the client should treat this address as 'preferred'. After this time elapses, a client classifies this address as "deprecated".

☐ "Validity period"
Here you specify the time in seconds that the client should treat this address as 'valid'.

Note: If you use a prefix from a WAN interface for dynamic address formation, you cannot configure values for `preferred lifetime` and `valid lifetime`. In this case, the device automatically determines the values that apply to the prefix delegated by the provider.

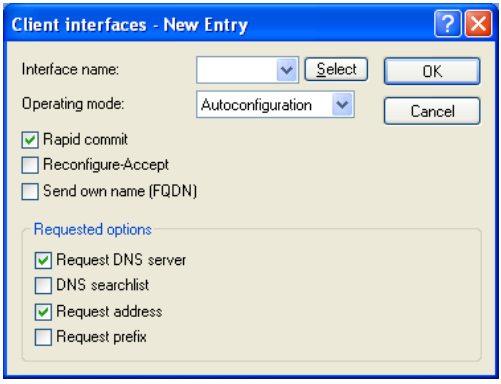
☐ "Receive prefix from"
Name of the WAN interface from which the client should use the prefix to form the address or prefix.

DHCPv6 client

Use the following buttons to access the tables and adjust the respective functions:

Interfaces

This table determines the behavior of the DHCPv6 client.



Note: Normally client behavior is controlled by the auto-configuration. Only make entries in this table if you want to use the client in "stand-alone" mode or if there are other specific options that deviate from the default settings.

☐ "Interface name"
Name of the interface that the DHCPv6 client operates on. These may be LAN interfaces or WAN interfaces (remote stations), such as "INTRANET" or "INTERNET".

☐ "Operating mode"
Determines if and how the device enables the client. Possible values are:

- "Autoconfiguration": The device waits for router advertisements, and then starts the DHCPv6 client. This option is the default setting.
- "Yes": The device starts the DHCPv6 client as soon as the interface is active, without waiting for router advertisements. The device ignores the specifications from router advertisements.
- "No": The DHCPv6 client is disabled on this interface. Even if the device receives router advertisements, it will not start the client.

☐ "Rapid commit"
When rapid commit is activated, the client attempts to obtain an IPv6 address from the DHCPv6 server with just two messages. If the DHCPv6 server is configured correspondingly, it immediately responds to this solicit message with a reply message.

☐ "Reconfigure accept"
If the client successfully negotiates a re-configuration (reconfigure) with the server during first contact, the server can request the client to update its address or other information at any time. The mechanism is protected by the so-called 'Reconfigure Key', so that only the original server with the correct key can make requests to the client. If the client receives a reconfigure message without a valid reconfigure key, the client rejects this invocation. The client supports the "Reconfigure Key Authentication Protocol" according to RFC 3315 for the options "Renew" and "Information Request", and also "Rebind" as per RFC 6644.

This option is enabled by default for WAN interfaces.

☐ "Send own name (FQDN)"

The client sends its own host name (fully qualified domain name). By default, this option is active on LAN interfaces.

☐ "Request DNS server"
Specifies whether the client queries the DHCPv6 server for DNS servers.

Note: You must enable this option in order for the device to obtain information about a DNS server.

☐ "DNS search list"
The client queries the DNS search list.

☐ "Request address"
Determines whether the client should request the DHCPv6 server for an IPv6 address.

Note: Only activate this option if addresses configured by the DHCPv6 server via this interface are stateful, i.e. not distributed by 'SLAAC'.

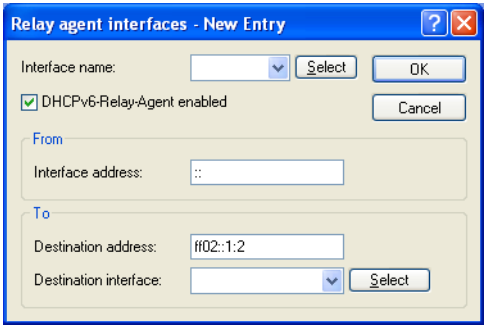
☐ "Request prefix"
Determines whether the client should request the DHCPv6 server for an IPv6 prefix. Activating this option is only necessary if the device itself functions as a router and redistributes these prefixes. This option is enabled by default on WAN interfaces in order for the DHCPv6 client to request a prefix from the provider for use in its local network. This option is disabled by default on LAN interfaces because devices in a local network are more likely to function as clients rather than as routers.

DHCPv6 Relay Agent

Use the following buttons to access the tables and adjust the respective functions:

Interfaces

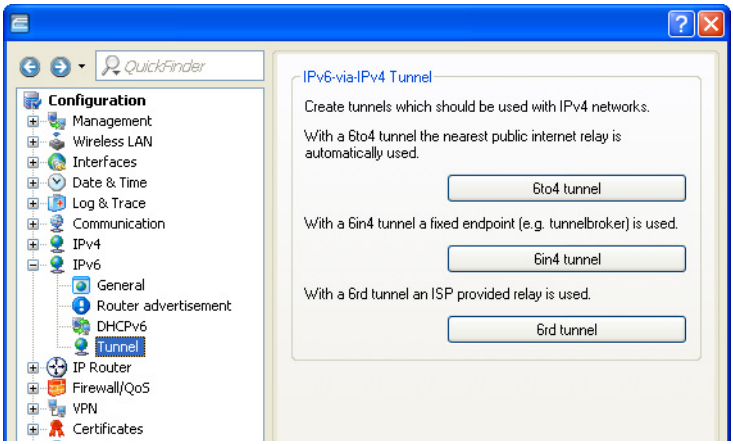
A DHCPv6 relay agent forwards DHCP messages between DHCPv6 clients and DHCPv6 servers, which are located in different networks. This table determines the behavior of the DHCPv6 relay agent.



- "Interface name"
  The name of the interface on which the relay agent receives requests from DHCPv6 clients, e.g. "INTRANET".
- "Relay agent enabled"
  Determines if and how the device enables the relay agent. Possible values are:
  - "Yes": Relay agent is enabled. This option is the default setting.
  - "No": Relay agent is not enabled.
- "Interface address"
  The relay agent's own IPv6 address at the interface that is configured under Interface Name. This IPv6 address is used as a sender address in DHCP messages that are forwarded. This sender address enables DHCPv6 clients to uniquely identify a relay agent. An explicit specification of the interface address is necessary because an IPv6 host can have multiple IPv6 addresses for each interface.
- "Dst address"
  The IPv6 address of the (destination) DHCPv6 server which the relay agent is to forward DHCP requests to. The address can be either a unicast or link-local multicast address. When using a link-local multicast address, you must specify the destination interface where the DHCPv6 server is to be reached. All DHCPv6 servers and relay agents are available at the link-local multicast address ff02::1:2.
- "Destination interface"
  The destination interface where the parent DHCPv6 server or the next relay agent is to be reached. This information is essential if a link-local multicast address is configured under the destination address, as link local-multicast addresses are only valid at that respective link.

Tunnel

The "Tunnel "configuration offers you 3 buttons to create IPv6 tunnels that can be used over IPv4 networks. Use these options to gain access to the IPv6 Internet using an IPv4 connection.



- "6to4 tunnel": This button opens the 6to4 tunnel settings.

  Note: Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the selected relay can change without the administrator knowing about it. For this reason, data connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

- "6in4 tunnel": This button opens the 6in4 tunnel settings.

  Note: 6in4 tunnels require more administrative effort, but they represent a secure and stable technology for IPv6 Internet access. This option is also suitable for professional use.

- "6rd tunnel": This button opens the 6rd tunnel settings.

Note: 6rd tunneling is suitable for end users and for professional applications because configuration is less complex than with 6in4 tunneling and the technology avoids the security risks of 6to4 tunneling.

13.9.2 Configuring PPP Negotiation Settings

In the PPP list, you are able to specify you own definition of PPP negotiation for every remote site contacting your network.

You can also specify whether communications should use an IPv4 or an IPv6 connection.

The authentication of point-to-point connections in the WAN commonly relies on one of the protocols PAP, CHAP, MS-CHAP or MS-CHAPv2. The protocols here have a "hierarchy" amongst themselves, i.e. MSCHAPv2 is a "higher-level" protocol than MSCHAP, CHAP and PAP (higher protocols provide higher security). Many dial-in routers at Internet providers allow up-front authentication using a higher-level protocol such as CHAP, but only support the use of PAP further down the line. If the setting for the protocol for authentication is fixed in the relevant device, the data connection may be lost because no common authentication protocol can be negotiated.

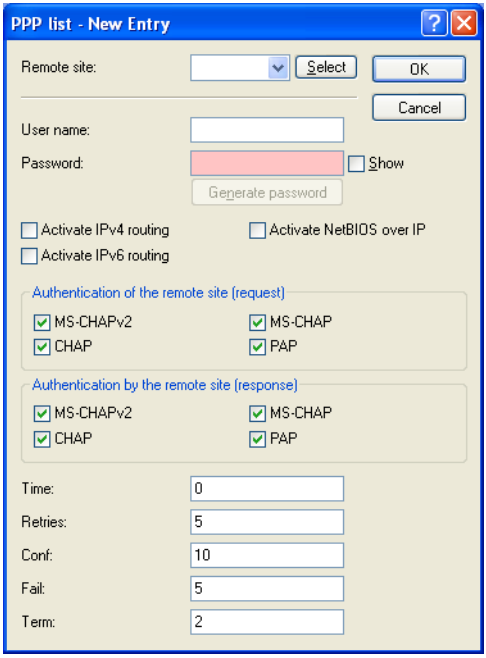
Note: In principle authentication can be repeated while the connection is being negotiated. Another protocol can be selected if, for example, it can only be recognized from the username at the earliest. However, this repeat negotiation is not supported in all scenarios. In particular when dialing in over UMTS, the device must explicitly refuse the provider's request for CHAP to be able to provide PAP user data for requests to be forwarded by the provider.

A flexible setting for the authentication protocols in the device ensures that the PPP connection is established as required. In addition, one or more protocols can be defined that are accepted for authentication of remote sites in the device (inbound data connections) and on login of the device into other remote sites (outbound data connections).

- When establishing inbound data connections, the device requires the lowest of the permitted protocols, but where possible it also permits the remote site to use one of the higher-level protocols (enabled in the device).
- When establishing outbound data connections, the device offers all enabled protocols, but only permits a selection from precisely these protocols. It is not possible to negotiate one of the disabled, possibly higher-level, protocols.

The PPP authentication protocols are set in the PPP list.

LANconfig: `Communication:Protocols:PPP list`

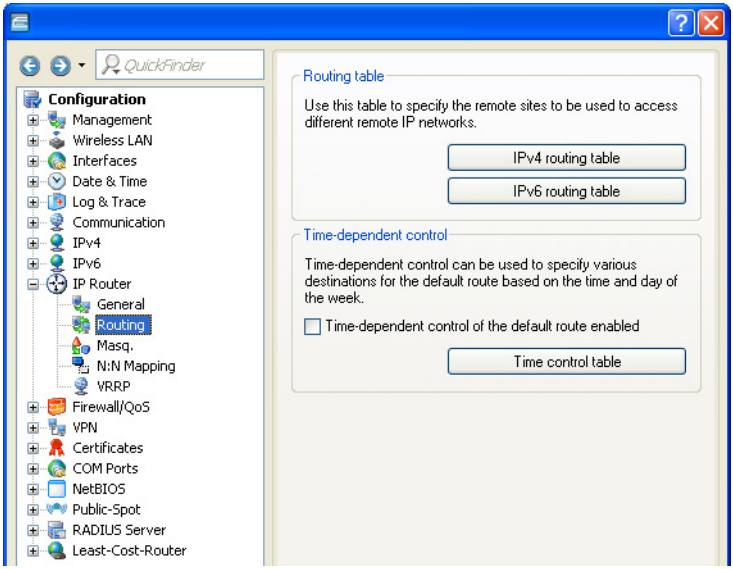


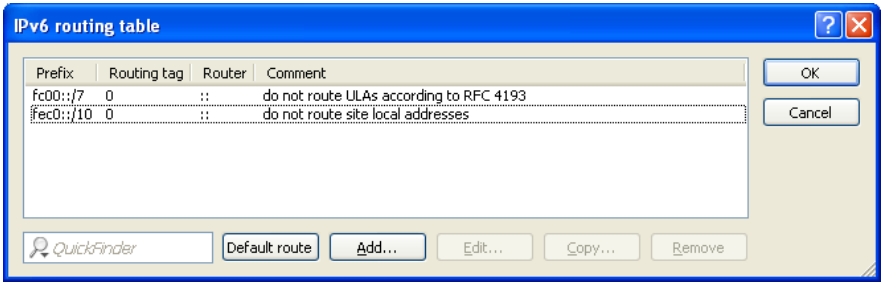
13.9.3 IP Routing Tables

Unlike previous versions where the configuration menu contained just a single IP routing table, this item now offers the configuration of separate routing tables for IPv4 and IPv6 connections.

You will find the new table under `IP router:Routing:IPv6 routing table`

The IPv4 settings that were previously in the table "IP routing table" are now located in the "IPv4 routing table ".





The table contains the entries to be used for routing packets with IPv6 addresses.

☐ **Prefix**

Specify the prefix of the network area for which the data is to be routed to the given remote station.

☐ **Routing tag**

Specify the routing tag for this route. This route is active only for packets with the same tag. The data packets receive the routing tag either from the firewall or depending on the LAN or WAN interface used.

☐ **Router**

This is where you specify the remote site for this route.

☐ **Comment**

Enter a descriptive comment for this entry.

Note: Entering a comment is optional.

13.9.4 Separate Views for the IPv4 and IPv6 Firewalls

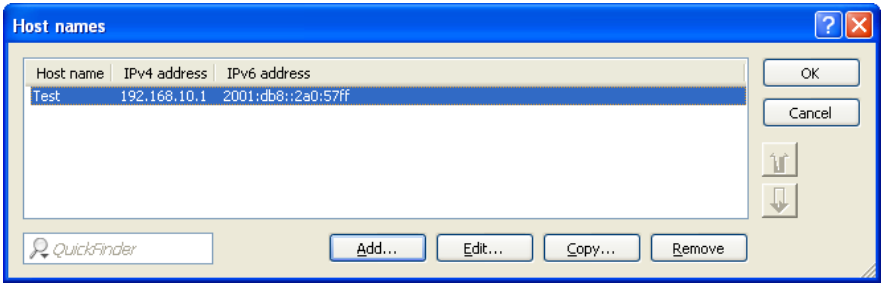
As of HiLCOS version 8.80, you can configure the rules for the IPv4 and IPv6 firewalls in separate views.

The corresponding configurations are located under `Firewall/QoS`IPv4 rules and `Firewall/QoS`IPv6 rules respectively.

13.9.5 IPv6 DNS Hosts in the DNS List

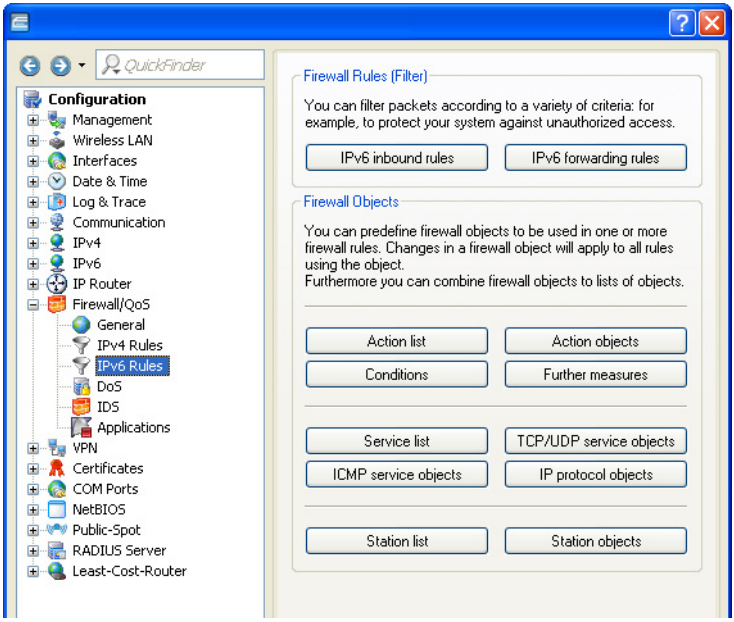
When the DNS server in your device receives a query about a station name, it responds with the IP address contained in the Host names list. For each station/host name you define either the IPv4 or the IPv6 address, or alternatively you can enter both IP addresses.

In LANconfig, the table with the station names and the associated IP addresses is under `IPv4:DNS:Host names`.



13.9.6 Configuring the IPv6 Firewall Rules

With LANconfig you can set the firewall rules under `Firewall/QoS:IPv6 Rules`.



The factory settings provide various objects and lists for the most important applications.

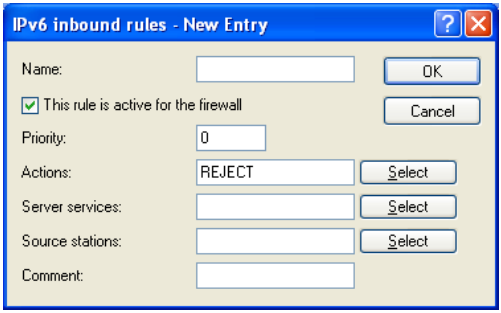
Note: You cannot delete objects or lists if the firewall uses them in a forwarding or inbound rule.

IPv6 Inbound Rules

Using the "IPv6 inbound rules" you set the rules that the IPv6 firewall should use to handle incoming traffic.

The factory settings provide various rules for the most important applications.

Click on "Add..." to create a new rule.



You can set the following properties for the rule:

☐ "Name"

Specifies the name of the rule.

☐ "This rule is active for the firewall"

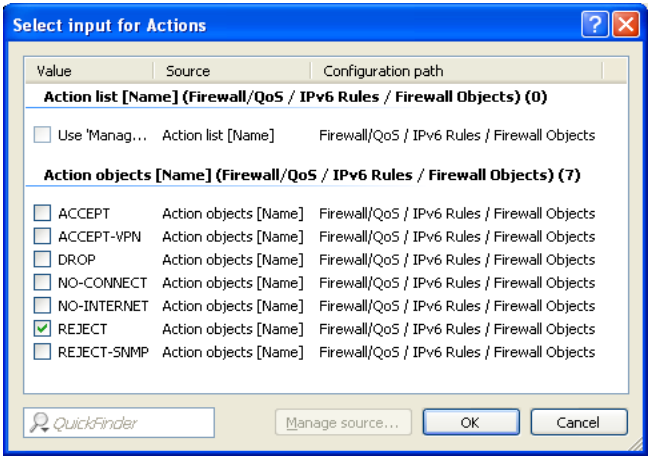
Enables the rule.

☐ "Priority"

Specifies the priority of the rule: The higher the value, the higher the priority.

☐ "Actions"

Specifies the action that the firewall performs if the rule condition is true. Using "Select" you can choose one action or a list of actions.



If you make a new entry here, it initially appears under "Unknown source". Next, highlight the entry for a source that you want to assign to the new entry, and click on "Manage source." Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

☐ "Server services"

Determines the services which the firewall applies this rule to. Using "Select" you can choose one service or a list of services.

☐ "Source stations"

Determines the source stations which the firewall applies this rule to. Using "Select" you can choose a terminal device or a list of stations.

☐ "Comment"

Here you assign a meaningful description for the filter rule.

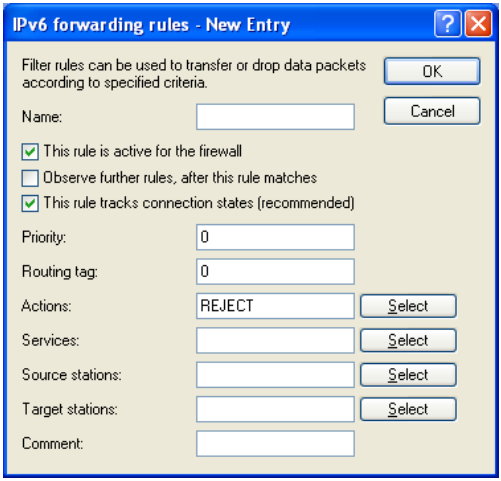
IPv6 Forwarding Rules

The "IPv6 forwarding rules" button accesses dialog where you set the rules that the IPv6 firewall should use to handle forwarded traffic.

The factory settings provide various rules for the most important applications.

In order to change the order of the rules, highlight the specific rule in the table and move it up or down in the table by clicking on the arrow buttons. The firewall applies the rules one after the other from top to bottom.

Click on "Add..." to create a new rule.



You can set the following properties for the rule:

☐ "Name"

Specifies the name of the rule.

☐ "This rule is active for the firewall"

Enables the rule.

☐ "Observe further rules after this rule matches"

If you enable this option, the firewall also applies the subsequent rules in the list. This is useful if the firewall should, for example, initially apply a group rule and then apply each rule to the individual objects in the group.

☐ "This rule tracks connection states (recommended)"

Select this option if the rule should track the TCP connection states.

☐ "Priority"

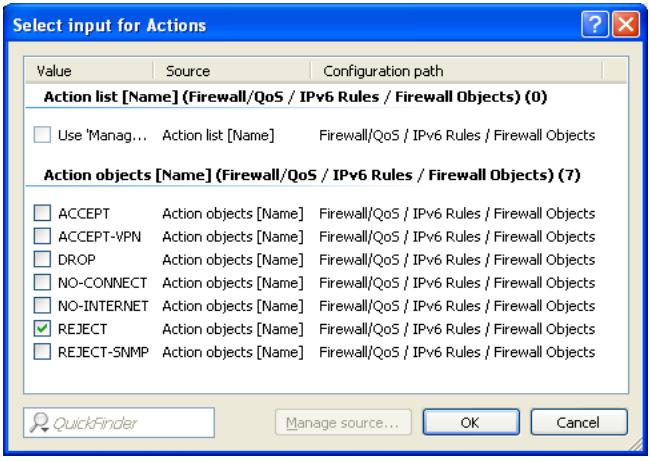
Specifies the priority of the rule: The higher the value, the higher the priority.

☐ "Routing tag"

The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag makes it possible to separate the rules valid for this network.

☐ "Actions"

Specifies the action that the firewall performs if the rule condition is true. Using "Select" you can choose one action or a list of actions.



If you make a new entry here, it initially appears under "Unknown source". Next, highlight the entry for a source that you want to assign to the new entry, and click on "Manage source." Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

☐ "Server services"

Determines the services which the firewall applies this rule to. Using "Select" you can choose one service or a list of services.

☐ "Source stations"

Determines the source stations which the firewall applies this rule to. Using "Select" you can choose a terminal device or a list of stations.

☐ "Target stations"

Determines the target stations which the firewall applies this rule to. Using "Select" you can choose a terminal device or a list of stations.

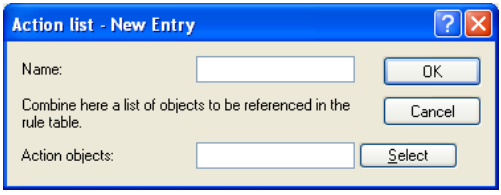
☐ "Comment"

Here you assign a meaningful description for the filter rule.

Action List

Using the "Action list" button, you can collect actions into groups. The actions available here must first be defined using "Action objects".

Click on "Add..." to create a new rule.



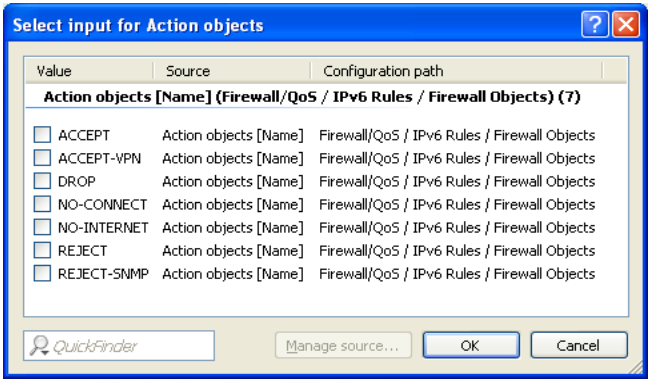
You can set the following properties for a list:

☐ "Name"

Determines the name of the list.

☐ "Action objects"

Determines the objects that you want to combine in this list. Using "Select" you can choose one or more objects from a list.

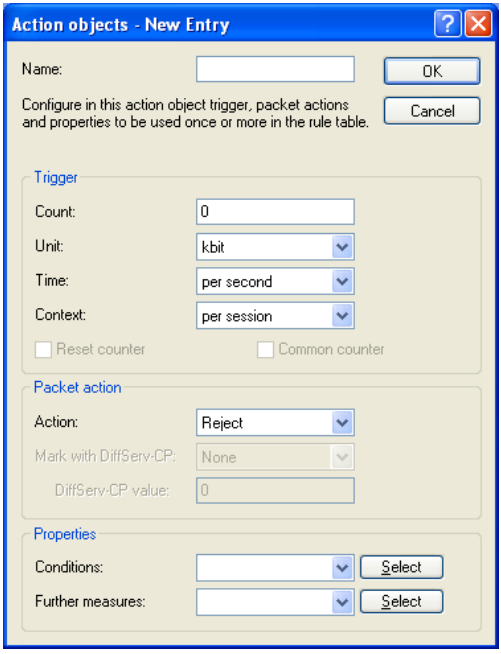


If you make a new entry here, it initially appears under "Unknown source". Next, highlight the entry for a source that you want to assign to the new entry, and click on "Manage source." Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Action Objects

Using the "Action objects" button, you define actions that the IPv6 firewall runs when a filter is true.

Click on "Add..." to create a new action.



You can set the following properties for the object:

☐ "Name"

Specifies the name of the object.

☐ "Count"

When this limit is exceeded, the firewall performs the action.

☐ "Unit"

Determines the unit for the limits. Select the corresponding value in the drop-down menu.

☐ "Time"

Determines the measurement period that the firewall applies to the limit. Select the corresponding value in the drop-down menu.

☐ "Context"

Determines the context that the firewall applies to the limit. Select the corresponding value in the drop-down menu.

☐ "Reset counter"

If you enable this option, the firewall resets the counter after running the action.

Note: You can only activate this option if you selected "absolute" in the "time" value.

☐ "Common counter"

If you enable this option, the firewall adds all action triggers together in one counter.

Note: You can only activate this option if you selected "per station" or "global" in the "Context" value.

☐ "Action"

Determines the action the firewall performs when the limit is reached.

The following options are possible:

- **Reject**: The firewall rejects the data packet and sends an appropriate notification to the sender.
- **Drop**: The firewall discards the data packet without notification.
- **Transmit**: The firewall accepts the data packet.

☐ "Mark with DiffServ-CP"

Determines the priority of the data packets (differentiated services, DiffServ), with which the firewall should transfer the data packets.

Note: You can only activate this option if you selected "transmit" in the "Action" value.

Note: Further information about DiffServ CodePoints is available under the section "QoS" on page 1073.

☐ "DiffServ-CP value"

Sets the value for the differentiated services code point (DSCP).

Note: You can only activate this option if you selected "Value" in "Mark with DiffServ-CP".

☐ "Conditions"

Determines which conditions must be met in order for the action to be performed. The item "Conditions" is used to specify any conditions.

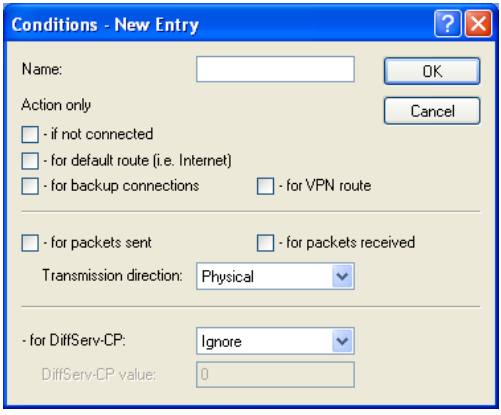
☐ "Further measures"

Determines which trigger actions the firewall should start in addition to filtering the data packets. You can specify trigger actions under the "Further measures".

Conditions

Use the "Conditions" button to specify the conditions that have to be met for the forwarding and inbound rules to apply.

Click on "Add..." to create a new condition.



You can set the following properties for the condition:

☐ "Name"

Specifies the name of the object.

☐ "Action only – if not connected"

Select this option if the firewall should only perform the action if there is no data connection.

☐ "Action only – for default route (e.g. Internet)"

Select this option if the firewall should only perform the action if there is a data connection over the default route.

☐ "Action only – for backup connections"

Select this option if the firewall should only perform the action if the connection is a backup connection.

☐ "Action only – for VPN route"

Select this option if the firewall should only perform the action if the connection is a VPN connection.

☐ "Action only – for packets sent"

Select this option if the firewall should only perform the action for packets sent.

☐ "Action only – for packets received"

Select this option if the firewall should only perform the action for packets received.

☐ "Transmission direction"

Determines whether the transport direction refers to the logical connection or the physical data transmission over the respective interface.

☐ "Action only – for DiffServ-CP"

Determines the priority that the data packets (differentiated services, DiffServ) have to have, so that the condition is met.

Note: Further information about DiffServ CodePoints is available under the section "QoS" on page 1073.

☐ "DiffServ-CP value"

Determines the value for the Differentiated Services Code Point (DSCP).

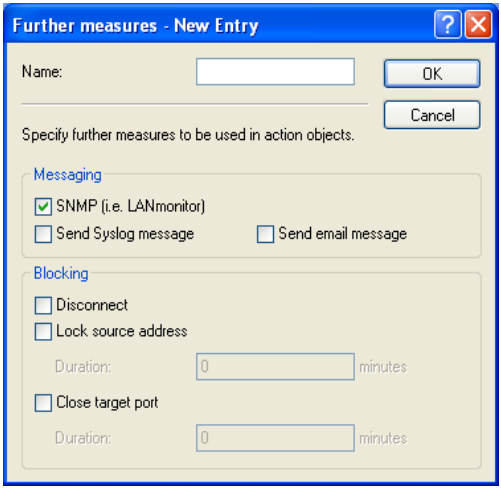
Enter a value here if you selected the "Value" option in the "– for DiffServ-CP" field.

Note: Further information about DiffServ CodePoints is available under the section "QoS" on page 1073.

Further Measures

Use the "Further measures" button to define further measures that the firewall performs after you apply the forwarding and inbound rules.

Click on "Add..." to create a new measure.



You can set the following properties for the trigger actions:

☐ "Name"

Specifies the name of the object.

☐ "SNMP (e.g. LANmonitor)"

Select this option if the firewall should send a notification via SNMP. You can receive this notification, e.g., with LANmonitor.

☐ "Send SYSLOG message"

Select this option if the firewall should send a SYSLOG notification via SNMP.

Note: For more information about SYSLOG, refer to the chapter "Diagnostics" in the section "SYSLOG" in the Reference Guide.

☐ "Send e-mail message"

Select this option, if the firewall should send a notification by e-mail.

Note: If you want to receive e-mail notifications, you must enter an e-mail address in `Firewall/QoS.General.Administrator e-mail`.

☐ "Disconnect"

Select this option if the firewall should disconnect.

☐ "Lock source address"

Select this option if the firewall should block the source address. The firewall registers the blocked IP address, the lockout period, as well as the underlying rule in the "Host-block-list" under `Status:IPv6:Firewall`.

☐ "Duration"

If the firewall should block the sender, you can set the duration of the lock in minutes. The value "0" disables the lock because, in practice, the lockout period expires after 0 minutes.

☐ "Close target port"

Select this option, if the firewall should block the target port. The firewall registers the blocked destination IP address, the protocol, the destination port, the lockout period, as well as the underlying rule in the "Port-block-list" under `Status:IPv6:Firewall`.

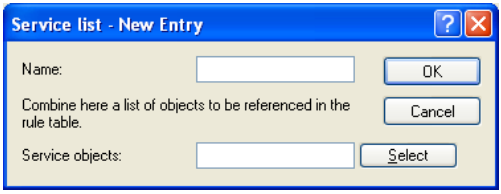
☐ "Duration"

If the firewall should block the target port, you can set the duration of the lock in minutes. The value "0" disables the lock because, in practice, the lockout period expires after 0 minutes.

Service List

Using the "Service list" button, you can collect services into groups. You first define the services under "TCP/UDP service objects", "ICMP service objects" and "IP protocol objects".

Click on "Add..." to specify a new service.



You can set the following properties for a list:

☐ "Name"

Determines the name of the list.

☐ "Service objects"

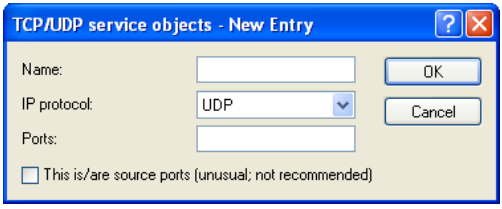
Determines the objects that you want to combine in this list. Using "Select" you can choose one or more objects from a list.

If you make a new entry here, it initially appears under "Unknown source". Next, highlight the entry for a source that you want to assign to the new entry, and click on "Manage source." Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

TCP/UDP Service Objects

Using the "TCP/UDP service objects" button, you define TCP/UDP services that the IPv6 firewall can use in filter rules.

Click on "Add..." to create a new service.



You can set the following properties for the rule:

☐ "Name"

Specifies the name of the object.

☐ "IP protocol"

Specifies the protocol of the service

☐ "Ports"

Specifies the ports for the service. Separate multiple ports with a comma.

Note: Lists with the official protocol and port numbers are available in the Internet at www.iana.org.

☐ "This is/are source ports"

Determines whether the specified ports are source ports.

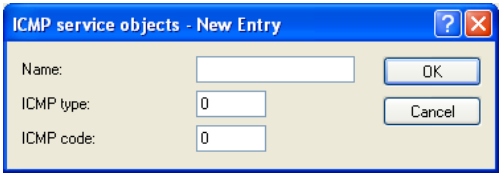
Note: In certain scenarios, it may be useful to specify a source port. This is unusual. Selecting "No" is recommended.

ICMP Service Objects

Using the "ICMP service objects" button, you define ICMP services that the IPv6 firewall can use in filter rules.

Note: Lists with the official ICMP types and port codes are available in the Internet under www.iana.org.

Click on "Add..." to create a new service.



You can set the following properties for the rule:

☐ "Name"

Specifies the name of the object.

☐ "ICMP type"

Specifies the type of the ICMP service.

☐ "ICMP code"

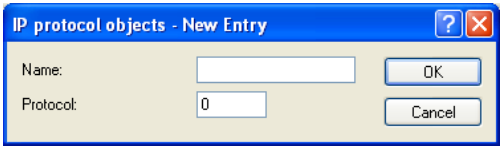
Specifies the code of the ICMP service.

IP Protocol Objects

Using the "IP protocol objects" button, you define IP protocol objects that the IPv6 firewall can use in filter rules.

Note: Lists with the official protocol and port numbers are available in the Internet at www.iana.org.

Click on "Add..." to create a new object.



You can set the following properties for the rule:

☐ "Name"

Specifies the name of the object.

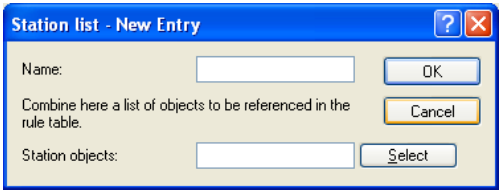
☐ "Protocol"

Defines the protocol number.

Station List

Using the "Station list" button, you can collect stations into groups. The terminal devices must previously be defined using "Station objects".

Click on "Add..." to create a new list.



You can set the following properties for a list:

☐ "Name"

Determines the name of the list.

☐ "Station objects"

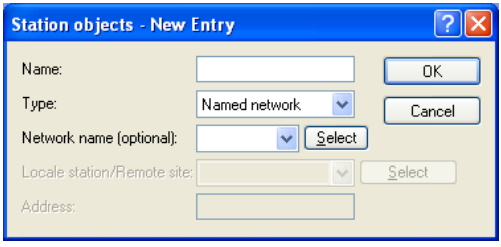
Determines the objects that you want to combine in this list. Using "Select" you can choose one or more objects from a list.

If you make a new entry here, it initially appears under "Unknown source". Next, highlight the entry for a source that you want to assign to the new entry, and click on "Manage source." Set the values for this entry, and save the new object. The new entry now appears as a new object in the list of the corresponding source.

Station Objects

Using the "Station objects" button, you define the terminal devices that the IPv6 firewall can use in filter rules.

Click on "Add..." to create a new object.



You can set the following properties for the object:

☐ "Name"

Specifies the name of the object.

☐ "Type"

Determines the station type.

☐ "Network name"

Here you enter the name of the network if you selected the appropriate option in the "Type" field.

Note: Entering the network name is optional.

☐ "Remote site"

Here you enter the name of the remote site if you selected the appropriate option in the "Type" field.

☐ "Address"

Here you enter the address of the remote site if you selected the appropriate option in the "Type" field.

13.10Tutorials

13.10.1Setting up IPv6 Internet Access

You can set up access to an IPv6 network if

- You have an IPv6-capable device,
- You use a tunneling technology and
- Your provider supports a native IPv6 network or you have access to a so-called tunnel broker who can mediate your IPv6 packets.

IPv6 Access Using the Setup Wizard in LANconfig

The Setup Wizard assists you with the configuration of IPv6 access with your equipment.

The Wizard presents following options:

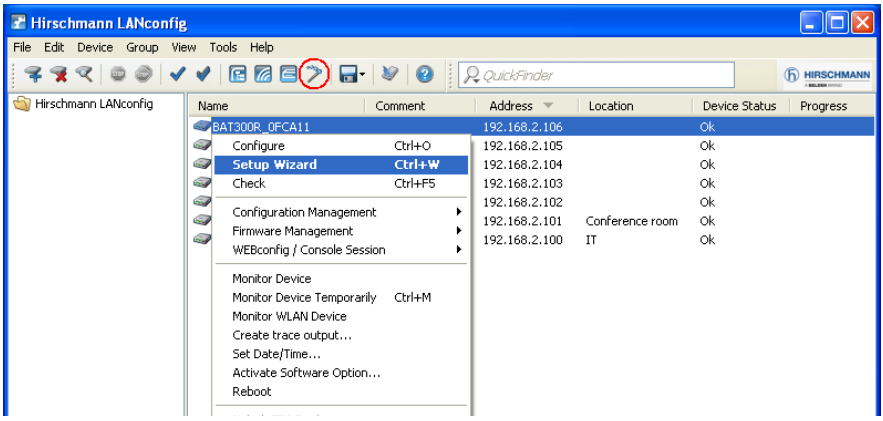
- `Set up IPv6 access for a new, unconfigured device.`
- `Set up IPv6 access in addition to a functioning IPv4 access for an existing device.`

Setup Wizard – Setting up IPv6 in a New Device

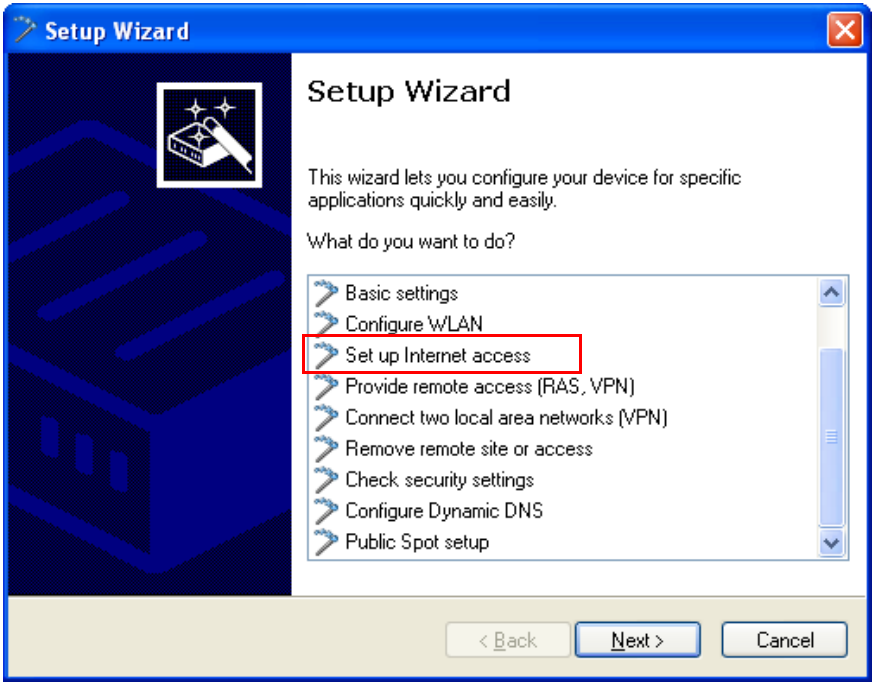
If you have connected up a new device but not have yet configured it, you have the option of using a Setup Wizard to set up IPv4 and IPv6 connections.

To save your entries and proceed to the next screen, click "Next".

☐ Then start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar.



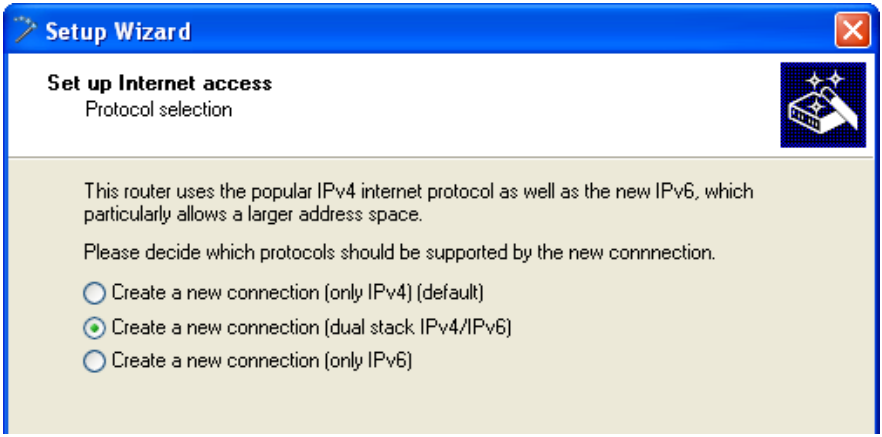
☐ In the Setup Wizard, select the option "Set up Internet access".



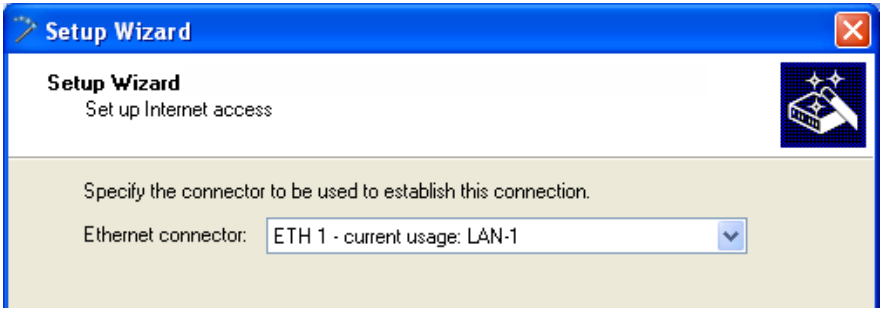
☐ You can choose from the following options:

- Set up a dual-stack connection. This is IPv4-and IPv6-capable and currently the recommended option for a new device.
- Set up an IPv4-only connection.
- Set up an IPv6-only connection.

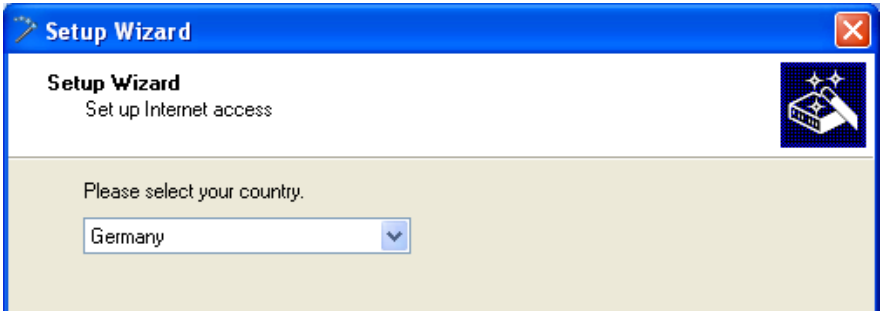
In the following we take you through the setup of a dual-stack connection. Activate the appropriate selection.



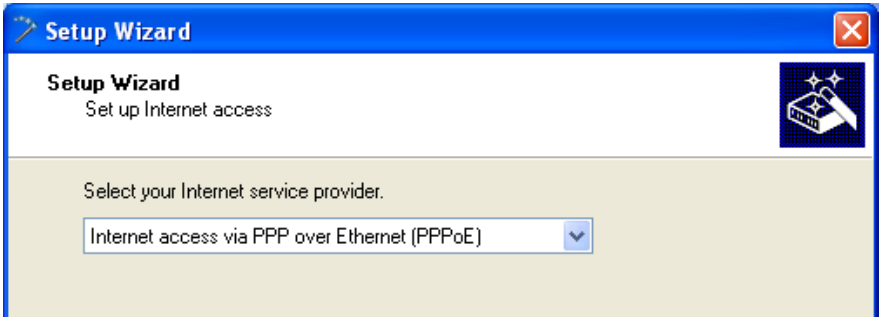
☐ Set the interface to be used for the connection.



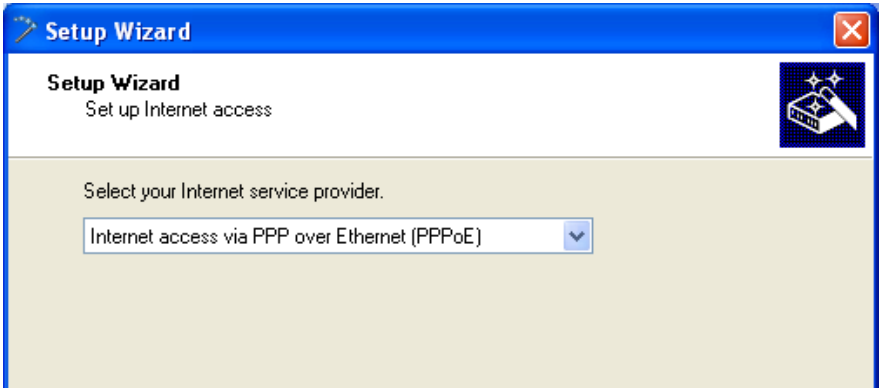
☐ Select your country from the list.



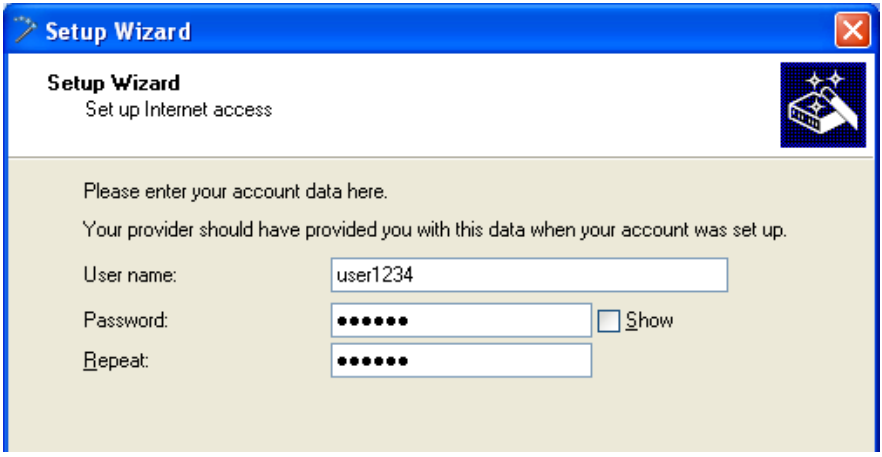
☐ Select your Internet provider.



☐ Enter a name for this data connection.

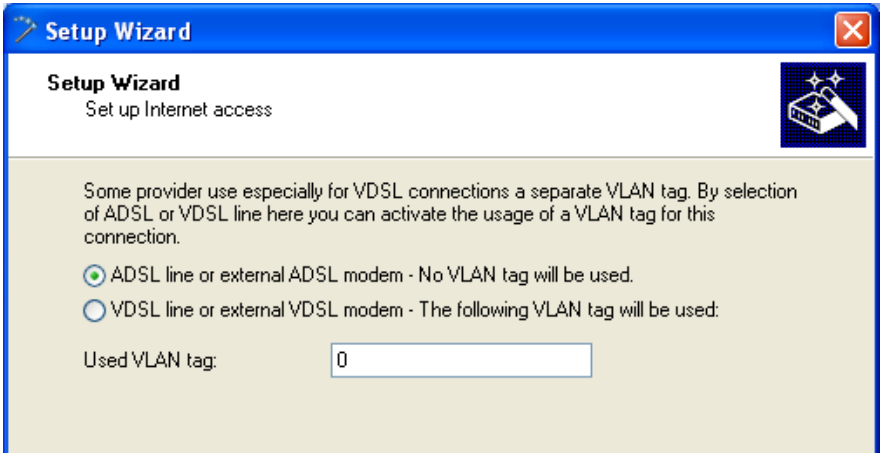


☐ Enter the login details given to you by your provider for setting up your Internet access.



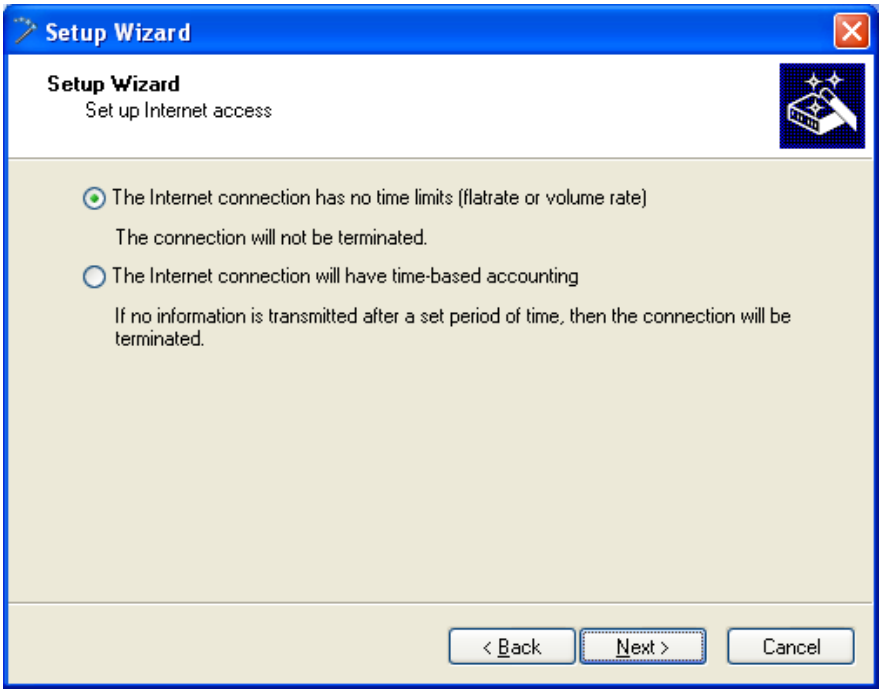
Note: Depending on the provider, the type and number of fields may vary.

☐ If you use PPPoE: Specify what kind of DSL connection you have and which particular VLAN tag your provider uses.



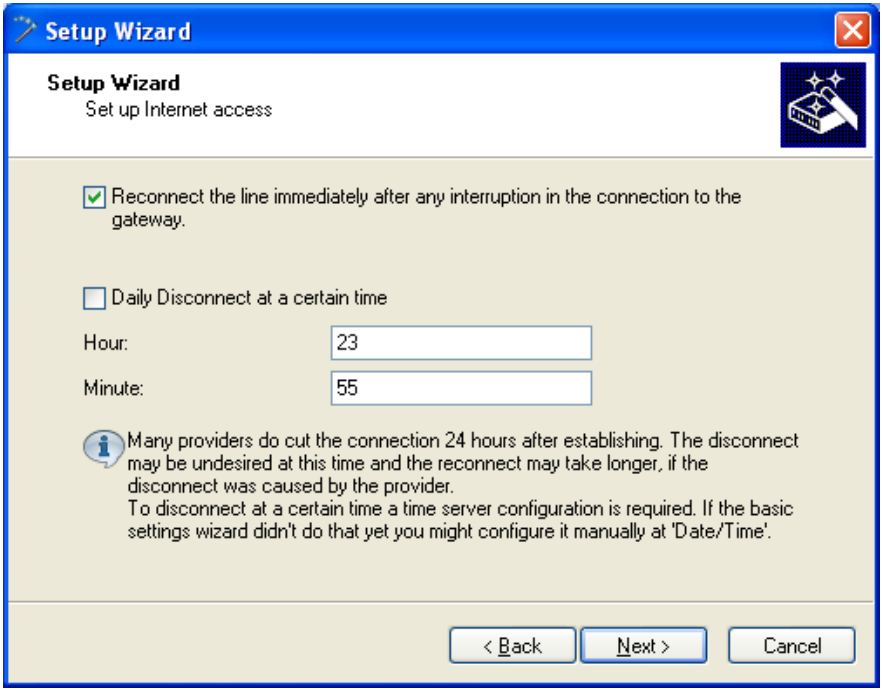
Note: Depending on the provider, the type and number of fields may vary.

☐ If you use PPPoE: Specify whether your Internet connection is subject to a data flat rate, a data quota, or if your provider charges your Internet access based on time.

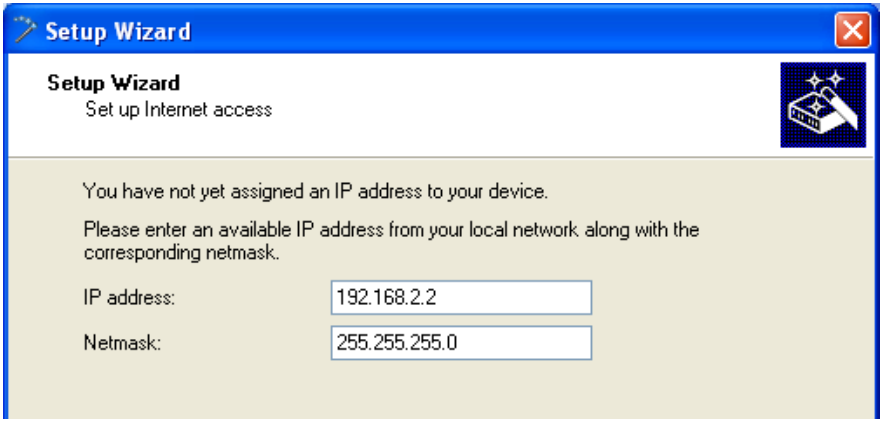


Note: Depending on the provider, the type and number of fields may vary.

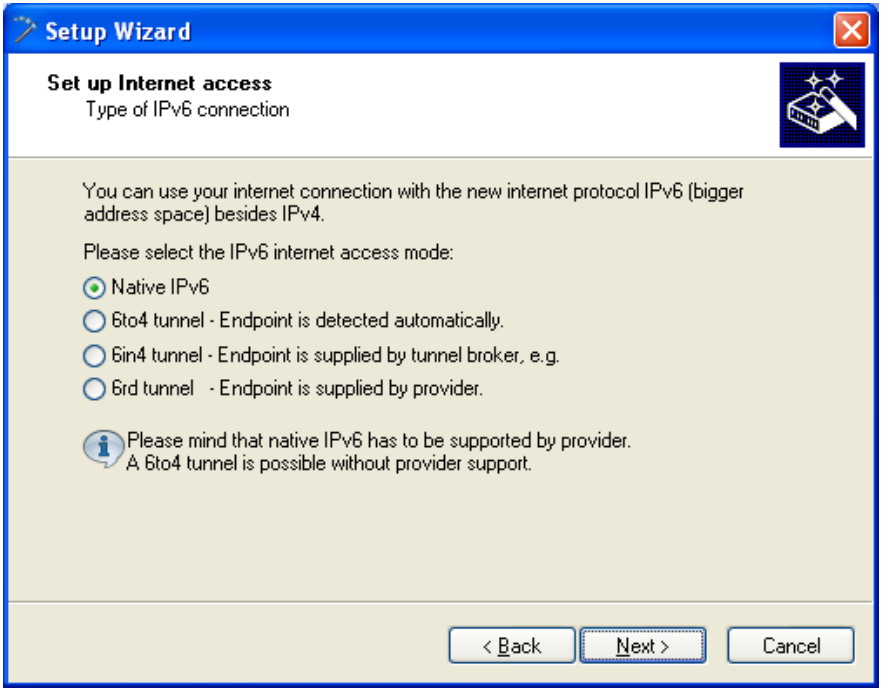
☐ Specify how you want the device to behave in case of disconnection. You can also specify if and when the device is to carry out a forced re-connection.



☐ If your device does not yet have an IP address, enter a new IP address and corresponding netmask.



☐ Select the type of IPv6 Internet access.

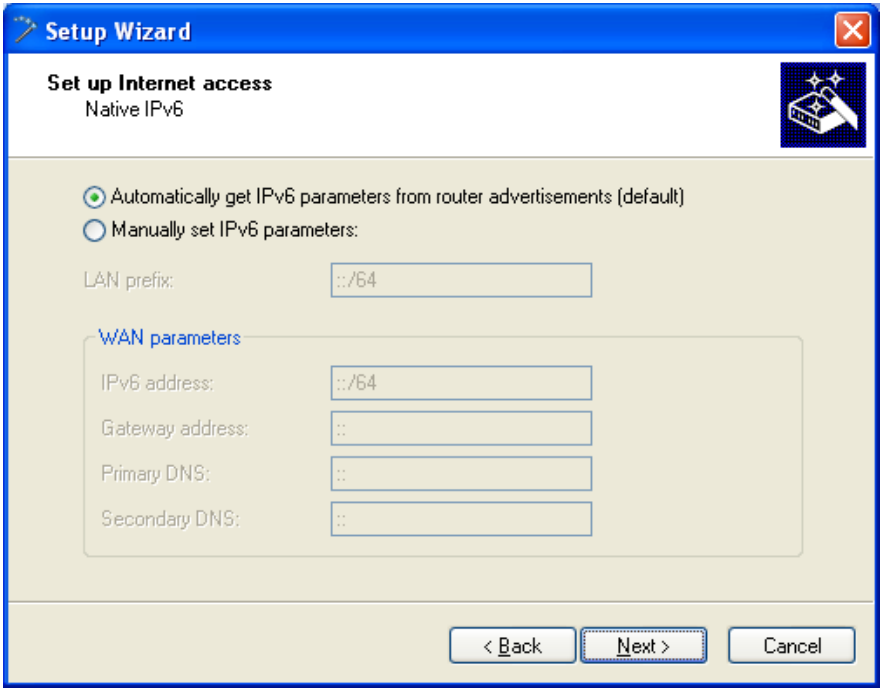


You can select from the following options:

- "Additional native IPv6": Configure a direct data connection without a tunnel.
- "6to4 tunnel": Start the wizard to configure a 6to4 tunnel.
- "6in4 tunnel": Use the input mask to set the parameters for the 6in4 tunnel.
- "6rd tunnel": Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

☐ Accept the default setting of "Automatically take IPv6 parameters from router advertisements."



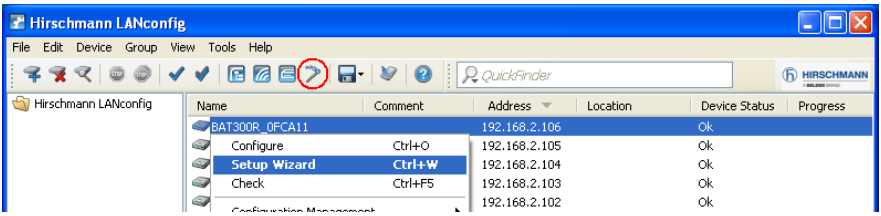
☐ You have completed the setup of the native IPv6 Internet access. Click on "Finish" when you are done and the wizard will save your entries to the device.

Setup Wizard – Setting up IPv6 on an Existing Device

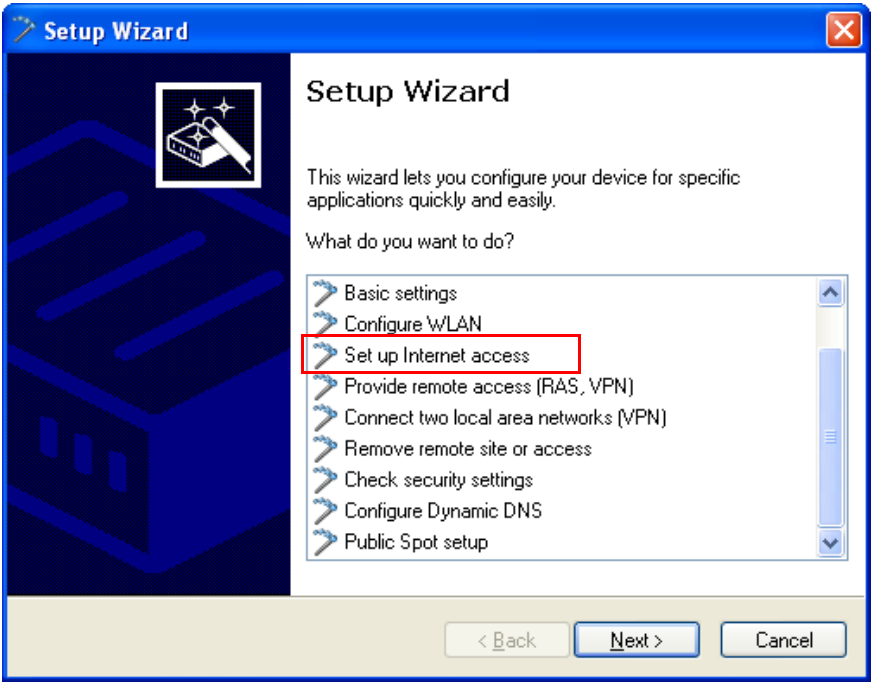
If you have a device configured for IPv4 and you wish to set up an additional IPv6 connection, you have the option of setting up the IPv6 connections with the Setup Wizard.

To save your entries and proceed to the next screen, click "Next".

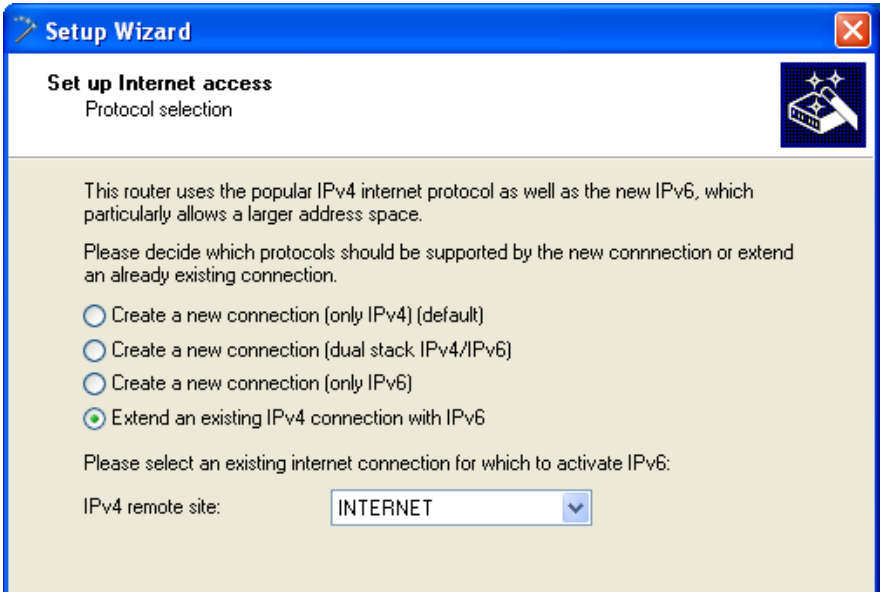
☐ Then start the Setup Wizard in LANconfig. Highlight the device to be configured. The Setup Wizard is started either by right-clicking and using the context menu, or with the Magic Wand icon in the toolbar



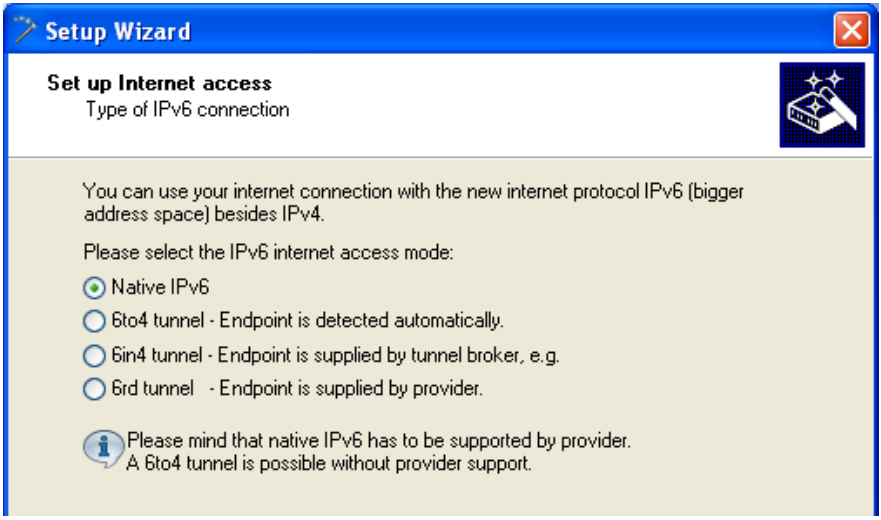
☐ In the Setup Wizard, select the option "Set up Internet access". To continue, click on "Next".



☐ Because your device is already IPv4-capable, the Setup Wizard gives you the opportunity to extend your existing settings with IPv6. Select this option and click on "Next."



☐ Select the type of IPv6 Internet access.

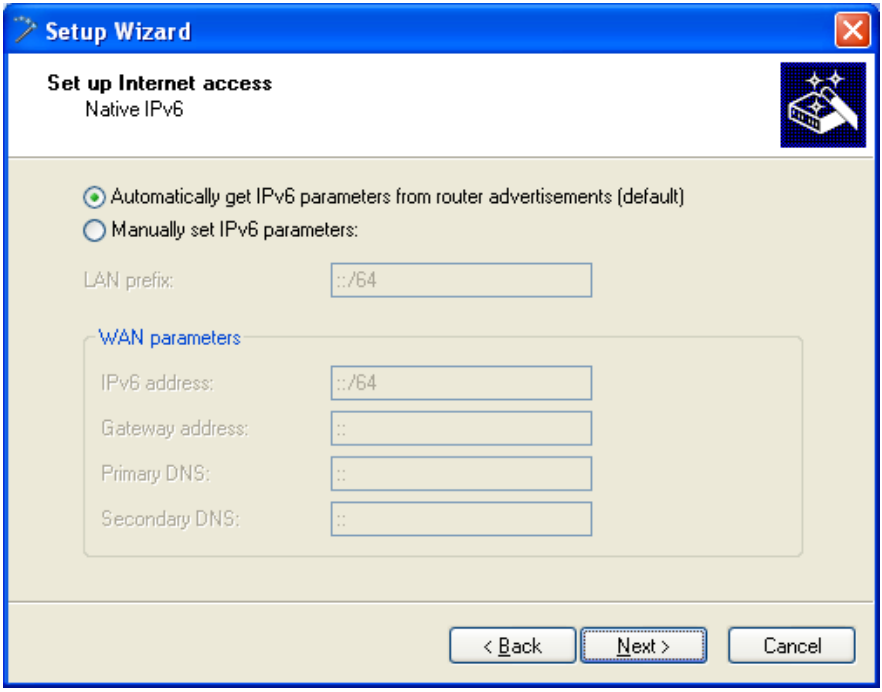


You can select from the following options:

- "Additional native IPv6": Configure a direct data connection without a tunnel.
- "6to4 tunnel": Start the wizard to configure a 6to4 tunnel.
- "6in4 tunnel": Use the input mask to set the parameters for the 6in4 tunnel.
- "6rd tunnel": Use the input mask to set the parameters for the 6rd tunnel.

Select the option for setting up a native IPv6 Internet connection.

☐ Accept the default setting of "Automatically take IPv6 parameters from router advertisements."



☐ You have completed the setup of the native IPv6 Internet access. Click on "Finish" when you are done and the wizard will save your entries to the device.

13.10.2Setting up a 6to4 Tunnel

The use of a 6to4 tunnel is feasible when

- Your device is IPv6 capable and you want to access IPv6 services,
- Your provider does not support a native IPv6 network and
- You do not have access to a so-called tunnel broker who can mediate your IPv6 packets.

When using a 6to4 tunnel, the lack of support of IPv6 by the provider means the device does not receive an IPv6 address or an IPv6 prefix.

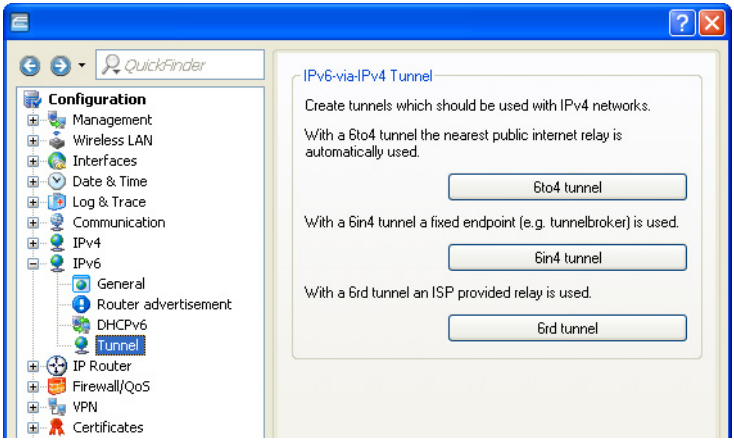
The device calculates its own unique prefix from "2002::/16" and the hexadecimal representation of its own public IPv4 address from the provider. This application only works if the device has a public IPv4 address. The device does not receive a public IPv4 address but an IPv4 address from a private address range only, for example when it accesses the Internet via UMTS and the provider supplies an IP address from its private address range, or if the device does not access the Internet directly, but is "behind" another router.

Note: Connections through a 6to4 tunnel work with relays that are selected by the IPv4 Internet provider's backbone. The device administrator has no influence on relay selection. Furthermore, the relay used can change without the administrator knowing about it. For this reason, data connections via a 6to4 tunnels are suitable **for test purposes only**. In particular, avoid using 6to4-tunnel data connections for productive systems or for the transmission of confidential data.

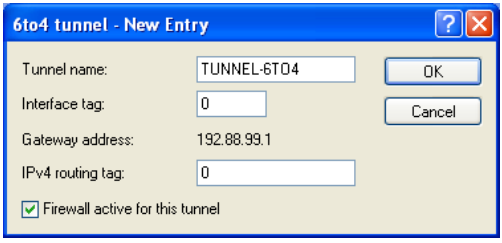
Working with LANconfig

To set up a 6to4 tunnel with LANconfig, proceed as follows:

- ☐ Start LANconfig. LANconfig now automatically searches the local network for devices.
- ☐ Select the device on which you want to set up a 6to4 tunnel. Select it with a left-click and start the configuration from the menu bar with `Device:Configure`.
- ☐ Navigate to `IPv6:Tunnel` and click on "6to4 tunnel".



☐ Click on "Add" to create a new 6to4 tunnel.



☐ Set the name of the 6to4 tunnel.

☐ Set the "Interface tag" to a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.

☐ The "Gateway address" is set by default to the anycast address "192.88.99.1". This address can only be changed with WEBconfig or Telnet.

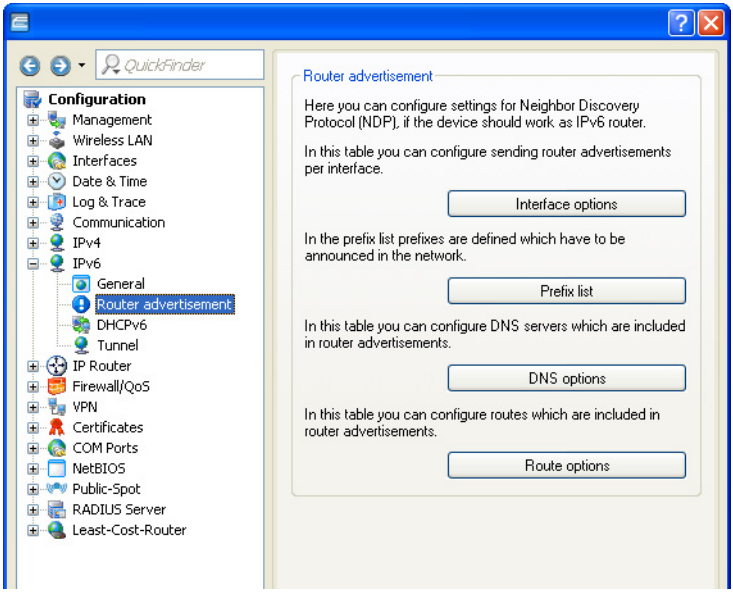
☐ Here you define the routing tag that the device uses to determine the route to the associated remote gateway. The "IPv4 routing tag" specifies which tagged IPv4 route is to be used for the data packets to reach their destination address.

☐ The default value is this tunnel's firewall.

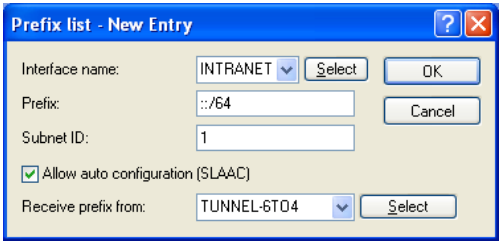
Note: If you disable the global firewall, you should also disable the firewall for the tunnel.

☐ Accept your entries with "OK".

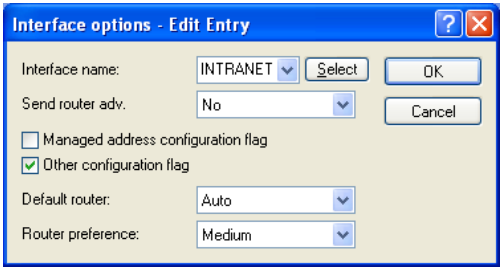
☐ Change to the directory `IPv6:Router advertisements`.



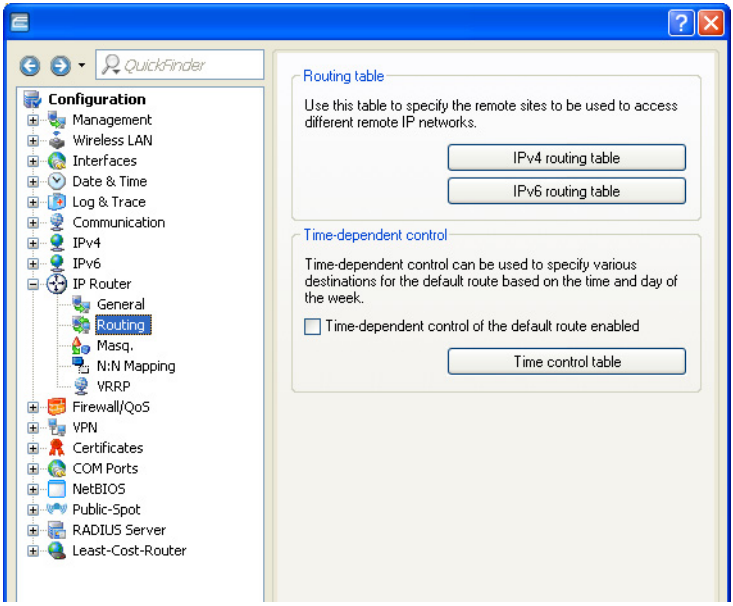
☐ Open the "Prefix list" and click on "Add."



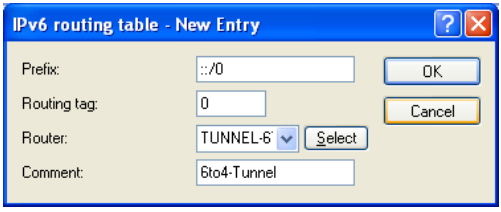
- ☐ Enter a name for the interface that is used by the 6to4 tunnel, e.g. "INTRANET".
- ☐ Set the value for the "Prefix" to "::/64" in order to accept the prefix issued by the provider automatically and in its entirety.
- ☐ Accept the default value of "1" for the "Subnet ID".
- ☐ Accept the activated option "Stateless address configuration".
- ☐ In the field "Prefix delegation from", enter the name of the tunnel that you have defined earlier, e.g. in the example above "TUNNEL-6TO4".
- ☐ Accept your entries with "OK".
- ☐ In the directory `IPv6:Router advertisements`, open the "Interface options", select the entry INTRANET and click on "Edit".
- ☐ In the drop-down menu "Send router advertisements" select the option 'Yes'.



- ☐ Accept all other default values ??without change.
- ☐ Save your entries with "OK".
- ☐ Change to the directory `IP router:Routing`.



☐ Open the "IPv6 routing table" and click on "Add".



☐ Set the "Prefix" to the value "::/0".

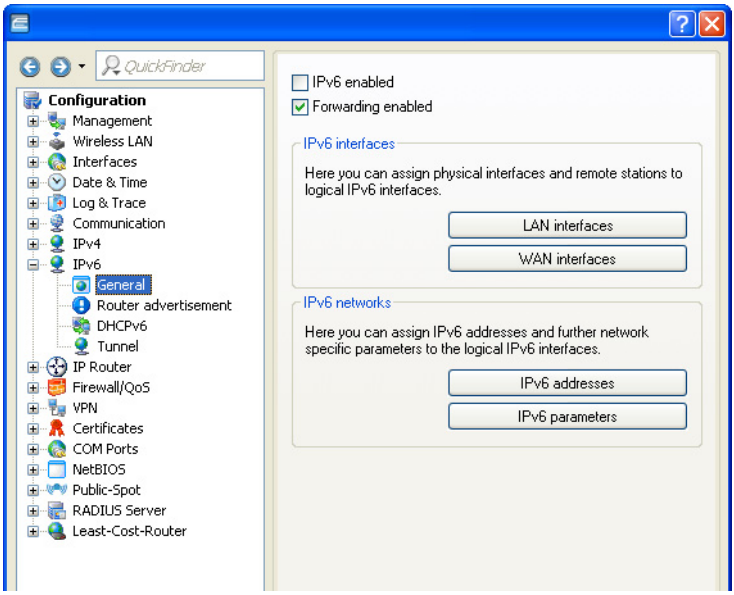
☐ In the field "Routing tag" accept the default value "0".

☐ In the field "Router", select from the list the name of the tunnel that you defined earlier, e.g. in the example above "TUNNEL-6TO4".

☐ Enter a descriptive "Comment "for this entry.

☐ Save your entries with "OK".

☐ Change to the directory `IPv6:General` and enable the IPv6 stack.

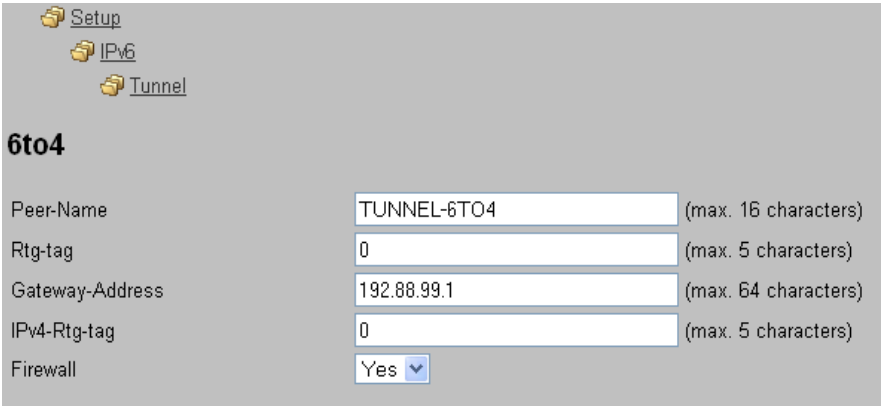


Working with WEBconfig

To set up a 6to4 tunnel with WEBconfig, proceed as follows:

☐ Type into your browser's address bar the address of the device to be set up with a 6to4 tunnel.

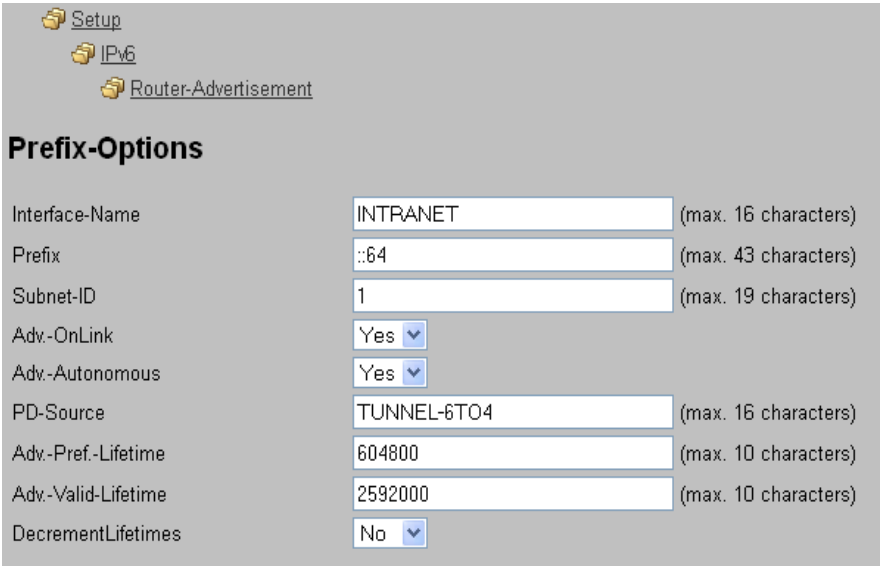
☐ Change to the directory `HiLCOS Menu Tree:Setup:IPv6:Tunnel:6to4` and click "Add".



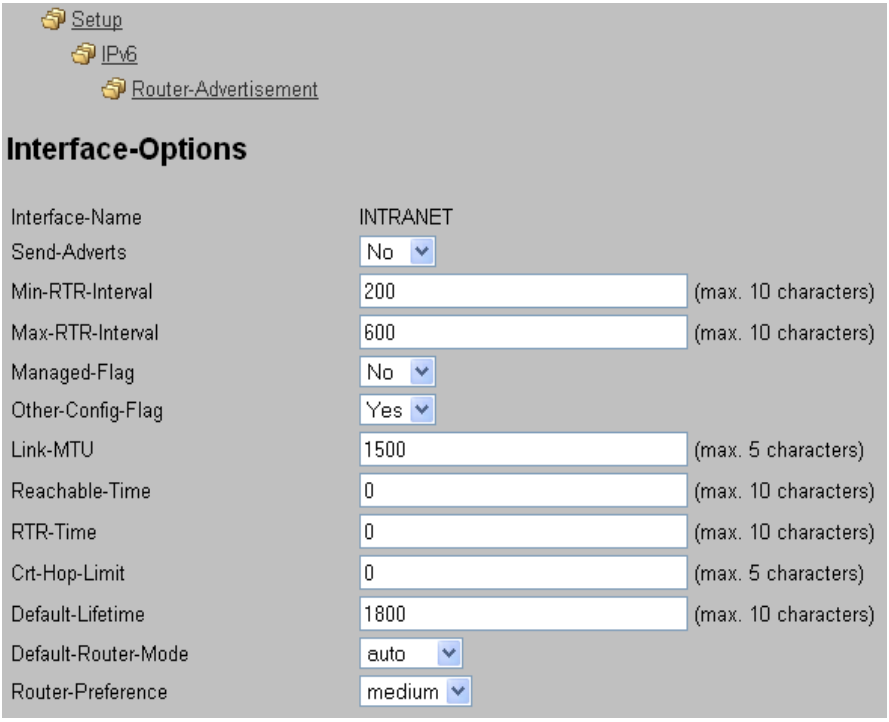
- ☐ Enter a name for the remote peer, e.g. "TUNNEL-6TO4".
- ☐ Leave the "Routing tag" unchanged as the default value "0".
- ☐ As the "Gateway address" you can accept the default value "192.88.99.1". This is the default anycast address for 6to4 relays that your device connects to.

  Note: This address is the reason why a 6to4 tunnel is unstable and susceptible to interception by unauthorized users. There is no assurance that a 6to4 relay will be available, and publicly available 6to4 relays may not be trustworthy. There is no certainty that the relay does not record your traffic.
- ☐ In the field "IPv4-Rtg-tag" accept the default value "0"
- ☐ Enable the "firewall" for this tunnel.

  Note: If you disable the global firewall, you should also disable the firewall for the tunnel.
- ☐ Save your entries with "Send".
- ☐ Change to the directory `HiLCOS Menu Tree:Setup:IPv6:Router advertisement`, open the "Prefix options" table and click "Add".



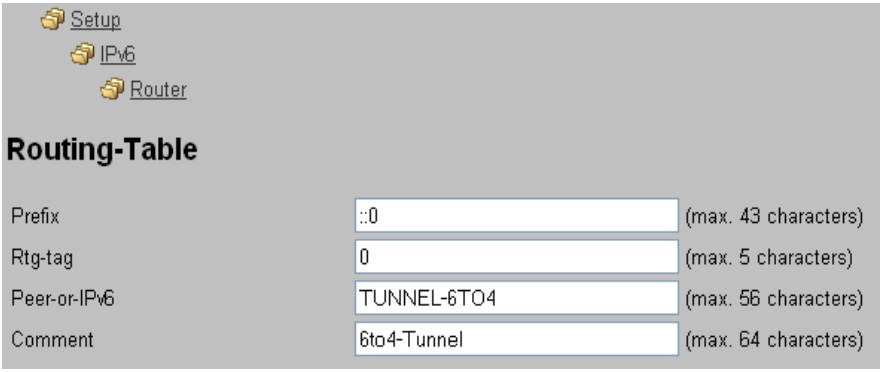
- ☐ Enter a name for the interface that uses the 6to4 tunnel, e.g. "INTRANET".
- ☐ Set the value for the "Prefix" to "::/64" in order to accept the prefix issued by the provider automatically and in its entirety.
- ☐ Accept the default value of "1" for the "Subnet ID".
- ☐ Set "PD source" to the name of the remote peer that you previously defined in the example above, e.g. "TUNNEL-6TO4".
- ☐ Save your entries with "Send".
- ☐ Change to the directory `HiLCOS Menu Tree:Setup:IPv6:Router advertisement`, open the "Interface options" table and click "Add".



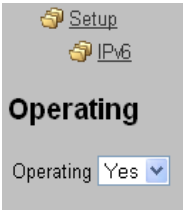
☐ Accept all other default values ??without change.

☐ Save your entries with "Send".

☐ Change to the directory `HiLCOS Menu Tree:Setup:IPv6:Router`, open the "Routing table" and click "Add".



- ☐ Set the "Prefix" to the value "::/0".
- ☐ In the field "Rtg-tag" accept the default value "0".
- ☐ In the field "Peer or IPv6", enter the name of the interface that will use the 6to4 tunnel, e.g. "TUNNEL-6TO4" in the example above.
- ☐ Enter a descriptive "Comment "for this entry.
- ☐ Save your entries with "Send".
- ☐ Enable the IPv6 stack under `HiLCOS Menu Tree:Setup:IPv6` by setting the option "Operating" to "yes" and save with "Send".



14 Quality of Service

Quality of Service (QoS) refers to two different aspects of communication performance:

- Applying pre-defined transmission priorities to communications relating to different applications or sources, and
- defining a transfer type for a particular data source.

14.1 QoS Objectives

The main objective of QoS is to transfer specified data packets either as securely or as quickly as possible.

14.2 Which packets to prioritize?

The QoS concept arises from the condition of bandwidth scarcity: available bandwidth is not always sufficient to transmit all sent data packets reliably and on time. Load peaks can result from simultaneously downloading large ftp files, exchanging e-mails, and operating VoIP telephones over the data line. In order to balance these competing demands for bandwidth, certain data packets should be treated preferentially.

There are two ways to mark a data packet for preferential treatment by the OpenBAT device:

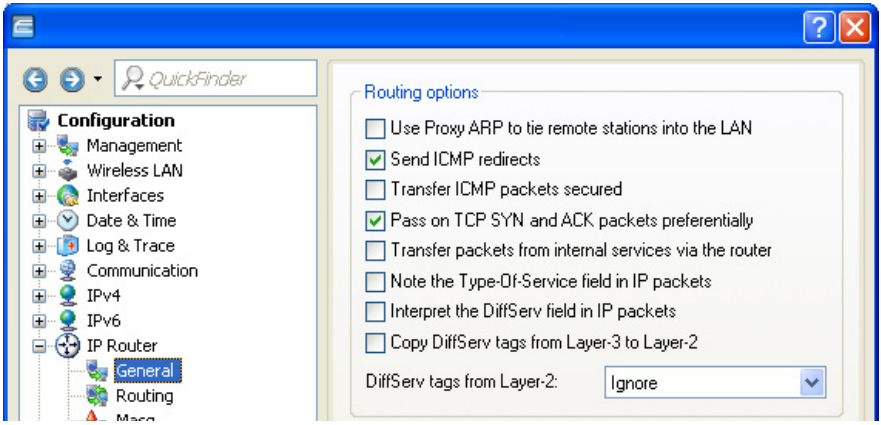
- The application, e.g., software operating in certain IP telephones, can mark the data packets appropriately. A tag is set within the header of the IP packets. The two different variants of this marking—ToS and DiffServ—assume the following states.
  - ToS “Low Delay“
  - ToS “High Reliability“
  - DiffServ “Expedited Forwarding“
  - DiffServ “Assured Forwarding“
- When the application itself cannot mark the data packets appropriately, the OpenBAT device can do so. It uses the existing functions of the firewall, which can classify data packets—for example, according to subnets or services (applications). Using these functions the OpenBAT device can mark data packets of an FTP connection or of a certain department (in a separate subnet) for prioritized treatment. For treatment of data packets classified by the firewall, the following two possibilities can be chosen:
  - Grant minimum bandwidth
  - Limited maximum bandwidth

14.3 Configuration of QoS

14.3.1 Evaluating ToS and DiffServ fields

ToS or DiffServ?

QoS is enabled if you have specified data packets for which the OpenBAT device issues priorities. This setting is made in LANconfig in the `Configuration : IP Router : General` dialog.



☐ Specify a QoS protocol, by making one of the following selections:

– Select "Note the Type-Of-Service Field in IP packets" to enable ToS checking. The OpenBAT device checks the bits for particularly fast or secured transmission.

– Select "Interpret the DiffServ field in IP packets" to enable DiffServ checking. The OpenBAT device checks the bits for Class Selector, Assured Forwarding, and Expedited Forwarding settings.

– To disable QoS, de-select both of the above settings (the default setting).

DiffServ in Firewall Rules

The code points from the DiffServ field can be evaluated by firewall rules for further control of QoS parameters such as minimum bandwidth or PMTU reduction. IP packets can be marked with DiffServ codepoints from suitable hardware (e.g. IP telephones) or applications (e.g. video telephony).

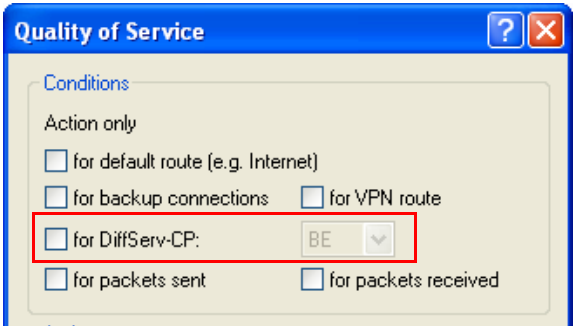
To create rules that give priority to specified DiffServ code points, follow these steps:

☐ Navigate to the following dialog:`Configuration : Firewall/QoS : IPv4 Rules` and click "Rules".

☐ In the ‘Firewall Rules’ list click ‘Add...’.

☐ In the ‘New Filter Rule’ dialog, select the ‘QoS’ tab.

☐ In the ‘QoS’ dialog, click ‘Add...’ then select ‘Add custom QoS’ to open the ‘Quality of Service’ dialog:



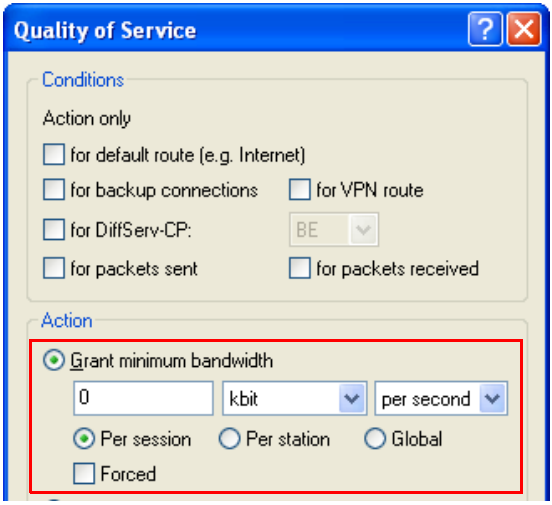
☐ Enable the setting "for DiffServ-CP" and choose from the dropdown list between:
- BE (Best Effort): Normal packet (corresponds CS0)
- CS (Class selector): 0 - 7 Is compatible to the TOS field of the IPv4 header and corresponds to the precedence of unset TOS bits
- AF (Assured forwarding): 0 - 4 / 0 - 3 The first digit represents the process priority and the second one represents the drop probability. The higher the priority and the lower the drop probability, the less frequently a packet will actually be dropped.
- EF (Expedited Forwarding): Self declaring.
- Value: An arbitrary tag—from 0 to 63—can be added.

Note: For additional information on how to configure firewall rules, refer to the chapter Firewall Configuration: LANconfig (see on page 921).

14.3.2 Granting Minimum Bandwidths

With the minimum bandwidth, you define how many packets will be transmitted with priority. The preference is active as long as the bandwidth limit is not exceeded. If the bandwidth is exceeded, the excess packets are transmitted, dropped or rejected as specified by other actions and rules. If no other applicable rule is configured, the corresponding packets are transmitted without preference.

You can create a grant of minimum bandwidth to selected transmissions in the ‘Quality of Service’ dialog. (Refer to the previous topic for the path to this dialog.)



To configure a firewall rule granting minimum bandwidth, configure the following parameters:

☐ Grant minimum bandwidth: Define the minimum bandwidth grant using the following elements:
  – a numeric value: This field accepts SI prefixes (k, Ki, M, Mi, G, Gi) as well as the SI unit bit, which will divide the value by 8 when exiting the entry field.
  – a unit of measure: kbit, kByte, packets, sessions, %bandwidth
  – a measure of time: absolute, per hour, per minute, per second

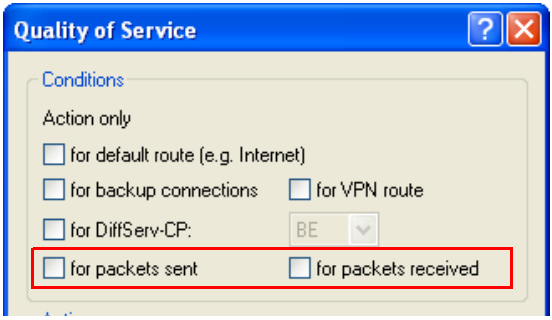
- ☐ The scope of the grant: Per session, Per station, Global
- ☐ Forced: This option exclusively reserves the specified bandwidth for each new session that matches this rule. The bandwidth is reserved for the entire duration of the session, even if the session temporarily requires less bandwidth. If the specified bandwidth is not available for a new rule matching session, the request to establish a connection is rejected.

Note: In addition to these settings, all other firewall rule parameters also apply to the grant of minimum bandwidth. Further information about configuring the firewall you find in 12 (see on page 921).

14.3.3 Configuring the send/receive direction

The OpenBAT configured by default to set the direction of the connection like the logical direction of the connection. You can change this default setting for the QoS firewall rule in the "Quality of Service" dialog.

- ☐ Navigate to the following dialog:`Configuration : Firewall/QoS : IPv4 Rules` and click "Rules".
- ☐ In the ‘Firewall Rules’ list click ‘Add...’.
- ☐ In the ‘New Filter Rule’ dialog, select the ‘QoS’ tab.
- ☐ In the ‘QoS’ dialog, click ‘Add...’ then select ‘Add custom QoS’ to open the ‘Quality of Service’ dialog:



☐ To configure the send/receive direction for packets with QoS tagging, do one of the following:

- Select "for packets sent" to apply the QoS firewall rule to packets physically sent from the LAN through the OpenBAT device.
- Select "for packets received" to apply the QoS firewall rule to packets physically received by the OpenBAT device and then forwarded to the LAN.

Note: For configuration with WEBconfig or Telnet, the interpretation of the data transfer direction is specified in a new firewall rule by parameters ‘R’ for receive, ‘T’ for transmit (send) and ‘W’ for reference to the WAN interface. For example, a limitation of the transmitted data to 16 KBit/s, based onto the physical WAN interface, can be achieved by the firewall rule `%Lcdstw16%d`.

14.3.4 Reducing Packet Length

You can increase the effectiveness of the QoS prioritization by reducing the length of the packets sent by the OpenBAT device. Extra-long packets can reduce the performance of QoS in prioritizing preferred packets.

Note: The packet length reducing firewall rule applies globally to all packets passing through the specified interface, regardless of protocol.

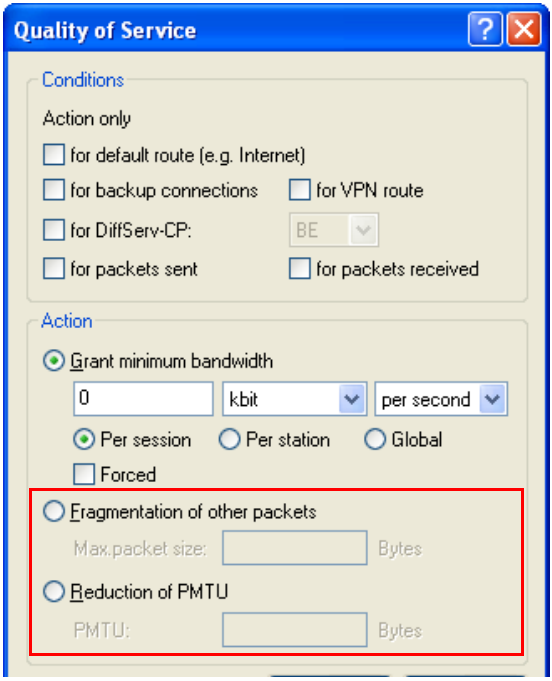
You can configure reduced packet length in the ‘Quality of Service’ dialog.

☐ Navigate to the following dialog:`Configuration : Firewall/QoS : IPv4 Rules` and click Rules.

☐ In the ‘Firewall Rules’ list click ‘Add...’.

☐ In the ‘New Filter Rule’ dialog, select the ‘QoS’ tab.

☐ In the ‘QoS’ dialog, click ‘Add...’ then select ‘Add custom QoS’ to open the ‘Quality of Service’ dialog:



To configure the send/receive direction for packets with QoS tagging, do one of the following:

- Select ‘Fragmentation of other packets’, then type in a ‘Maximum packet size’ (in Bytes). Packets larger than this size are subject to the rule, and will be handled according to the action defined for the rule.
- Select ‘Reduction of PMTU’ then type in a ‘PMTU’ (in Bytes) to establish the maximum transmission unit size for this path. Stations configured with the rule will adjust unit size to match this limit.

Note:

- For configuration with WEBconfig or Telnet, the reduction is entered in a new firewall rule by parameter “P” for PMTU reduction (Path MTU, MTU = Maximum Transmission Unit) and “F” for the fragment size.
- PMTU reduction and fragmentation always refer to the physical connection. Using the parameter “W” to represent the WAN sending direction is not required here and hence will be ignored if used.

The following example shows a setting for Voice over IP telephony:

Rule	Source	Destination	Action	Protocol
VOIP	IP addresses of IP telephones in the LAN, all ports	IP addresses of IP telephones in the LAN, all ports	%Qcds32 %Prt256	UDP

This rule defines the minimum bandwidth for sending and receiving 32 Kbps, forces and reduces the PMTU while sending and receiving to packets of 256 byte size. For the TCP connection, the maximum segment size of the local workstation is set at 216, so that the server will send packets of maximum 256 byte (reduction of the PMTU in sending and receiving direction).

14.4 QoS for WLANs: IEEE802.11e (WMM/WME)

Based on the 802.11e standard, QoS can be applied to WLAN transfers. The 802.11e standard supports, among other things, the prioritization of certain data-packet types. This extension of the 802.11 standard is an important basis for the use of voice applications in WLANs (Voice over WLAN, VoWLAN).

The WiFi alliance certifies products that support QoS according to 802.11e, and refer to WMM (WiFi Multimedia, formerly known as WME or Wireless Multimedia Extension). WMM defines four categories (voice, video, best effort and background) that constitute separate queues to be used for prioritization.

The 802.11e standard sets priorities by referring to the WLAN tags or, in the absence of these, by the DiffServ fields of IP packets. Delay times (jitter) are kept below 2 milliseconds, a magnitude which is inaudible to the human ear. 802.11e controls access to the transfer medium with EDCF, the Enhanced Distributed Coordination Function.

Note: Both of the following are preconditions to setting priorities:
- both the WLAN client and the access point support 802.11e or WMM
- the applications need to be able to mark the data packets with the corresponding priorities

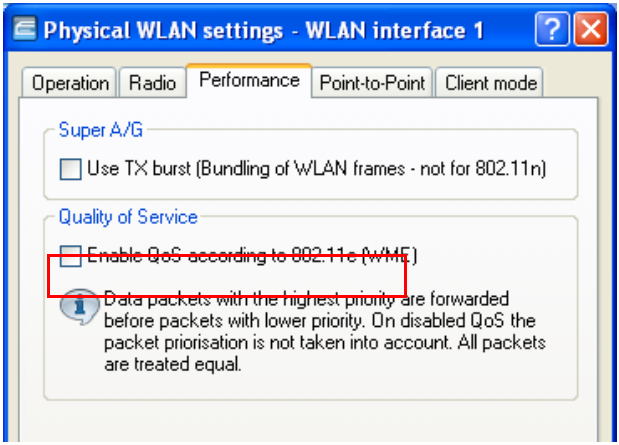
You can configure the OpenBAT device to separately activate 802.11e for each of its physical WLAN networks. Do the following:

☐ Open `Configuration : Wireless LAN : General`

☐ Click ‘Physical WLAN settings’ and select an interface

☐ In the ‘Physical WLAN settings’ dialog, select the ‘Performance’ tab.

☐ Select ‘Enable QoS according to 802.11e (WME)’


Physical WLAN settings - WLAN interface 1
Operation
Radio
Performance
Point-to-Point
Client mode
Super A/G
Use TX burst (Bundling of WLAN frames - not for 802.11n)
Quality of Service
Enable QoS according to 802.11e (WME)
Data packets with the highest priority are forwarded before packets with lower priority. On disabled QoS the packet priorisation is not taken into account. All packets are treated equal.

15 Additional Services

OpenBAT devices offer the additional services described in this chapter.

15.1 IP Address Administration via DHCP

15.1.1 Introduction

DHCP Server

All devices in a TCP/IP LAN require a unique IP address. They also may need the addresses of Domain Name System (DNS) and NetBIOS Name (NBNS) servers, and a standard gateway that can route data packets to addresses not located on the local network.

In a small network it is possible to manually enter these addresses on all the computers in the network. However, in a large network with many workstations this quickly becomes an unmanageable task. In the case of large networks, administrators typically use a DHCP server to dynamically assign the required addresses to individual workstations.

These OpenBATdevices come equipped with an integrated DHCP server that can take on the task of assigning IP addresses in the LAN. This process involves communicating the following parameters to the workstations:

– IP address
– Network mask
– Broadcast address
– Standard gateway
– DNS server
– NBNS server
– Lease (validity period) of the assigned parameters

The DHCP server either takes the IP addresses from a freely defined address pool or determines the addresses independently based on its own IP address. An unconfigured device in DHCP auto-mode can autonomously specify IP addresses for itself and for other network devices.

In the simplest scenario, you just need to connect a new out-of-the-box OpenBAT device to a network that has no other DHCP server and switch it on. The integrated DHCP server in the OpenBAT device manages all subsequent IP address assignment in the LAN, in cooperation with LANconfig wizards.

Note: DHCP settings can differ for each network. It is possible to define several IP networks in the OpenBAT devices in conjunction with advanced routing and forwarding (ARF). Thus, with the exception of a few general settings, DHCP settings apply to just a particular IP network.

DHCP Relay

If another DHCP server is located in the LAN, the OpenBAT device—if it is operating in client mode—can obtain its required address information from the other DHCP server.

The OpenBAT can operate as a DHCP relay agent and as a DHCP relay server:

- As a DHCP relay agent the OpenBAT device forwards DHCP requests to another DHCP server.
- As a DHCP relay server the OpenBAT device processes DHCP requests forwarded from DHCP relay agents.

BOOTP

The bootstrap protocol (BOOTP) can be used to send a specified IP address and other parameters to a workstation when it boots up. Workstations without hard drives can use BOOTP to load a boot image—i.e. a complete operating configuration—from a boot server.

15.1.2 Configuring DHCP parameters in LANconfig

Activating a DHCP Server for a Selected Logical Interface

The DHCP server can be activated or deactivated separately for each logical interface (e.g. LAN-1, WLAN-1, P2P-1-1 etc.). To do this:

- ☐ Navigate to the following dialog:`Configuration : IPv4 : DHCPv4.`
- ☐ Click "Port table" and select a logical interface from the list to open the following dialog, where you can enable and disable the DHCP server for this interface:

Configuring DHCP Networks

DHCP settings can be specified separately for any IP network defined in the OpenBAT device. As part of configuring DHCP networks, you need to define a range of addresses (an address pool) that can be assigned to DHCP clients.

When a client is activated in the network and requests an IP address via DHCP, the OpenBAT device with an activated DHCP server offers to issue an address. This address is selected from the pool of valid IP addresses. A computer that has received a specific IP address in the past requests the same address again and—if the DHCP server has not reassigned this address to another computer—the server attempts to issue the client its previous address.

The DHCP server also checks the LAN to confirm that the selected address is available. If the address is confirmed as unique, it is assigned to the requesting computer.

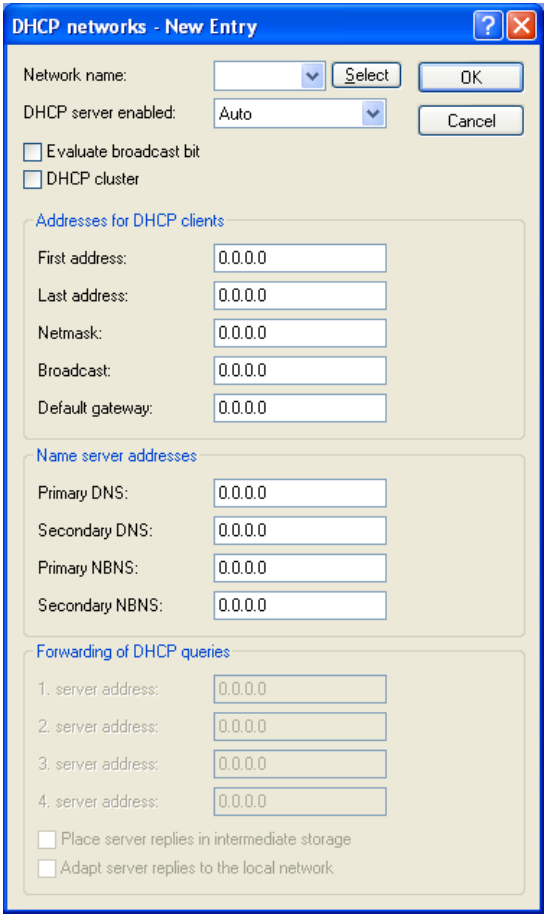
Note:

- The device factory settings include the IP networks "Intranet" and "DMZ," although there are no settings for IP addresses and netmasks. In the absence of a pre-existing address for networked devices, the OpenBAT device uses the IP address '172.23.56.254' for itself, and the address pool '172.23.56.x' for assigning IP addresses to the network.
- With the configuration of IP and DHCP networks, multiple networks with different DHCP settings can be active on the same logical interface. In this case, the DHCP settings for the first suitable network are applied. A prioritization of networks may be necessary.

To configure a DHCP network, follow these steps:

☐ Navigate to the following dialog:`Configuration : IPv4 : DHCPv4` and click "IP networks".

☐ In the ‘DHCP networks’ table, either select an existing network and click ‘Edit...’ or click ‘Add...’ to create a new DHCP network:



Configure the DHCP network by entering values for the following settings:

- Network name:
  Select the IP network for these DHCP settings.

  Note: Navigate to the following dialog:`Configuration : IPv4 : General` to add new IP networks if necessary.

- DHCP server enabled:
  Select a mode of operation:
  - No: The DHCP server is disabled.
  - Yes: The DHCP server is enabled. Use this setting if you are certain that no other DHCP server is active in the LAN. When this value is entered the server configuration (validity of the address pool) is checked:
    – If the configuration is correct then the device starts operating as a DHCP server in the network.
    – An incorrect DHCP configuration (e.g. invalid pool limits) will disable the DHCP server.
  - Auto (default): The device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress.
    – If another DHCP server is discovered, the device switches its own DHCP server off. If the OpenBAT device is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. Unconfigured devices introduced to the network cannot assign addresses unintentionally.OpenBAT
    – If no other DHCP servers are discovered, the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the OpenBAT device will be disabled.
  - Client Mode: The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN. Use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.
  - Forward queries: The DHCP server is enabled and receives requests from DHCP clients in the LAN. The device does not respond to requests itself, but forwards them to a central DHCP server in a different network segment.
- Evaluate broadcast bit:
  Select this to have the DHCP server evaluate the broadcast bit sent by the client. If the bit is not evaluated, then all DHCP responses are sent as broadcasts.

- DHCP cluster:
  Select this to have the DHCP server track running DHCP negotiations, adding hosts to its own table, including those that are registered to other DHCP servers. In this way, the DNS server can resolve the names of hosts registered to any member of the cluster.
- First / Last address:
  Use these parameters to define the IP address pool, as follows:
  - Create a range of IP address values to create an IP address pool; or
  - Enter a value of '0.0.0.0' in each field, to have the DHCP server determine the relevant first and last addresses itself using the settings for the IP network (network address and netmask).

  Note: Recall that the device is in a special operating mode if no IP network has yet been defined. In that case, it uses the IP address '172.23.56.254' and the address pool '172.23.56.x' for assigning IP addresses to the network.
- Netmask:
  The netmask is assigned in a similar way to assigning addresses. If a netmask has been entered here, it will be used when assignment is made. Otherwise the IP network's netmask will be used.
- Broadcast:
  Do one of the following:
  - Leave this field blank: the broadcast address is determined using the device's own address and netmask, if possible.
  - Enter an IP address: In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case enter that broadcast address here.

  Note: Experienced personnel exclusively should change the setting for the broadcast address.
- Default gateway:
  Normally, the address of this device is transferred to the stations as the standard gateway. To select a different standard gateway, enter its IP address here.

- Primary / Secondary DNS:
  Enter the address of a name server to which DNS queries should be forwarded. These fields may be left blank if you have an Internet provider or other remote station that automatically assigns a name server when logging in.
- primary / Secondary NBNS:
  Enter the address of a name server to which NBNS queries should be forwarded. These fields may be left blank if you have an Internet provider or other remote station that automatically assigns a name server when logging in.
- 1-4 server address:
  If the forwarding of DHCP queries is enabled, enter the IP addresses of the upstream DHCP servers here. These servers do not have to be located in the local network. Requests sent as broadcasts are forwarded to configured DHCP servers. You can enter directly the IP address of the particular server or the broadcast address of the network in which the server is located.
- Place server replies in intermediate storage:
  If this option is enabled, the device buffers the responses from the upstream DHCP server in order to respond directly to subsequent queries. Unnecessary connections can thus be avoided if the upstream server is located in a remote network.
- Adapt server replies to the local network:
  If this option is enabled, the device modifies the replies from the upstream DHCP server to adapt them to the local network. This involves replacing the Standard Gateway, DNS Server and NBNS Server values.

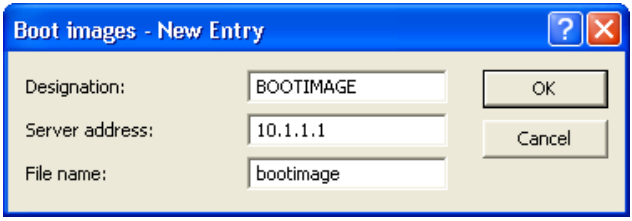
Assigning fixed IP addresses and boot images to clients

You can use LANconfig to create boot images for DHCP clients, then assign both that boot image and a fixed IP address to selected DCP clients.

To create a boot image:

☐ Navigate to the following dialog:`Configuration : IPv4 : BOOTP` and click "Boot images".

☐ In the ‘Boot images’ window, click ‘Add...’ to create a new entry:



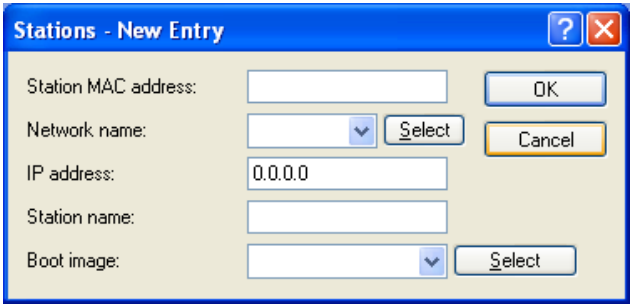
Enter settings for these parameters:

- Designation:
  Input a name for this boot image. This name will be used when assigning a boot image to a specific station in the station list.
- Server address:
  Enter the IP address of the server providing the boot image.
- File name:
  Specify the name of the file on the server that contains the boot image.

To assign a fixed IP address and (optionally) a boot image to a client:

☐ Navigate to the following dialog:`Configuration : IPv4 : BOOTP` and click "Stations".

☐ In the ‘Stations’ window, click ‘Add...’ to create a new entry:



Enter settings for these parameters:

- Station MAC address:
  Specify the MAC address (node ID) of the station's network adapter.
- Network name:
  Select the network name of the ARF network, for which these settings should apply. If this field is left empty, the device allocates the configured address from the ARF network from which the DHCP request took place. If the request derives from an ARF network for which no particular address has been configured, the device assigns an address dynamically from the address pool.

  Note: If the assigned IP address is not part of the address range of the configured ARF network, the assignment will be discarded and instead an IP address will be chosen from the address range of the ARF network from which the request took place.
- IP address:
  Enter the IP address to be assigned.
- Station name:
  Enter a name to identify the station. If a station does not transfer its name, the device will use the name entered here.
- Boot image (optional):
  Selected the image file that contains the station's operating system. The client needs to support the BOOTP protocol.

15.1.3 Configuring DHCP parameters via WEBconfig or Telnet

DHCP configuration and status parameters can also be accessed using either Telnet or WEBconfig.

DHCP configuration parameters can be accessed at:

```
HiLCOS Menu Tree : Setup : DHCP
```

Configurable DHCP settings in WEBconfig include:

- General DHCP settings
- Alias list
- Hosts table
- Network list
- Port table
- Additional options

DHCP status parameters are found in the be accessed at:

```
HiLCOS Menu Tree : Status : TCP/IP : DHCP : DHCP Table
HiLCOS menu tree : Setup : DHCP : DHCP table
```

General DHCP Statistics

This table contains information on IGMP packets. Field values include:

- User class identifier: The DHCP client in the OpenBAT device can insert additional information in the DHCP request sent, which simplifies recognition of requests within the network. The vendor class identifier (DHCP option 60) shows the device type, and is included in the transmission. The user class ID (DHCP option 77) specifies a user-defined string, and is transmitted when the user has configured a value.
- Default lease time minutes:
  When a client requests an address without asking for a specific lease, the address will be assigned this value as its lease.
- Max lease time minutes:
  When a client requests an IP address from a DHCP server, it can also ask for a lease for the address. This value governs the maximum length of lease that the client may request.

Alias List

The alias list defines the names for the boot images that are used to reference the images in the hosts table:

- Image alias:
  Enter any name you wish for this boot image. This name is used when you assign a boot image to a particular client in the station list.
- Image server:
  Enter the IP address of the server that provides the boot image.
- Image file:
  Enter the name of the file on the server containing the boot image.

Hosts Table

The bootstrap protocol (BOOTP) can be used to communicate a certain IP address and other parameters to a workstation when it boots up. To enable the initial communication, the workstation's MAC address is required.

- MAC address:
  Enter the MAC address of the workstation to which an IP address is to be assigned.
- Network name:
  Enter the name of a configured IP network here. A requesting client needs to be located in this IP network to be assigned the relevant IP address defined for the MAC address.

  Note: If the requesting client is located in an IP network for which there is no corresponding entry in the hosts table, the client will be assigned an IP address from the address pool of the appropriate IP network.
- IP address:
  Enter the client IP address that is to be assigned to the client.
- Hostname:
  Enter the name that is to be used to identify the client. If the client does not communicate its name, the device will use this name.
- Image alias:
  If the client uses the BOOTP protocol, you can select a boot image that the client should use from which to obtain its operating system.

Note: Enter the name of the server providing the boot image and the name of the file on the server in the boot image table.

Network List

DHCP settings for the IP networks are defined in this table.

- Network name:
  The name of the network to which the DHCP server settings apply.
- Operating:
  - No: The DHCP server is disabled.
  - Yes: The DHCP server is enabled. Use this setting if you are certain that no other DHCP server is active in the LAN. When this value is entered the server configuration (validity of the address pool) is checked:
    – If the configuration is correct then the device starts operating as a DHCP server in the network.
    – An incorrect DHCP configuration (e.g. invalid pool limits) will disable the DHCP server.
  - Auto (default): The device regularly searches the local network for other DHCP servers. The LAN-Rx/Tx LED flashes briefly when this search is in progress.
    – If another DHCP server is discovered, the device switches its own DHCP server off. If the OpenBAT device is not configured with an IP address, then it switches into DHCP client mode and queries the LAN DHCP server for an IP address. Unconfigured devices introduced to the network cannot assign addresses unintentionally.OpenBAT
    – If no other DHCP servers are discovered, the device switches its own DHCP server on. If another DHCP server is activated later, then the DHCP server in the OpenBAT device will be disabled.

- Client Mode: The DHCP server is disabled, the device behaves as a DHCP client and obtains its address from another DHCP server in the LAN. Use this setting if you are certain that another DHCP server is in the LAN and actively assigning IP addresses.
- Relay: The DHCP server is enabled and receives requests from DHCP clients in the LAN. The device does not respond to requests itself, but forwards them to a central DHCP server in a different network segment.

- Evaluate broadcast bit:
  Select this to have the DHCP server evaluate the broadcast bit sent by the client. If the bit is not evaluated, then all DHCP responses are sent as broadcasts.
- Start address pool:
  The first IP address in the pool available to the clients. If no address is entered here the DHCP takes the first available IP address from the network (as determined by network address and netmask).
- End address pool:
  The last IP address in the pool available to the clients. If no address is entered here the DHCP takes the first available IP address from the network (as determined by network address and netmask).
- Netmask:
  Corresponding netmask for the address pool available to the clients. If no address is entered here the DHCP server uses the netmask from the corresponding network.
- Broadcast address:
  As a rule, broadcast packets in a local network have an address which results from the valid IP addresses and the netmask. In special cases (e.g. when using subnets for a selection of workstations) it may be necessary to use a different broadcast address. In this case the broadcast address is entered into the DHCP module.

  Note: Experienced personnel exclusively should change the setting for the broadcast address.

- Gateway address: By default, the
  OpenBAT device issues its own IP address as the gateway address to computers making requests. If necessary, the IP address of another gateway can be transmitted if a corresponding address is entered.

- DNS default:
  IP address of the DNS name server for the forwarding of DNS requests.
- DNS backup:
  IP address of the backup DNS name server for the forwarding of DNS requests, in the event that the first named server ceases to operate.
- NBNS default:
  IP address of the NBNS name server for the forwarding of DNS requests.
- NBNS backup:
  IP address of the backup NBNS name server for the forwarding of DNS requests, in the event that the first named server ceases to operate.
- Master server / 2nd / 3rd / 4th master server:
  This is where the IP address for the superordinate DHCP servers can be entered when the mode 'Relay requests' is selected.
- Place server replies in intermediate storage:
  This option allows the responses from the higher-level DHCP server to be stored in the OpenBAT device. Subsequent requests can then be answered by the OpenBAT device itself. This option is useful if the higher-level DHCP server can be reached exclusively via a connection that incurs costs.
- Adaptation of server response to the local network:
  This option allows the responses from the higher-level DHCP server to be adapted to the local network. When activated, the OpenBAT device adapts the responses from the higher-level DHCP server by replacing the following entries with its own address (or locally configured addresses):
  – Gateway
  – Network mask
  – Broadcast address
  – DNS server
  – NBNS server
  – Server ID

This option is worthwhile if the superordinate DHCP server does not permit the separate configuration for DHCP clients in another network.

- Cluster:
  This option lets you ‘cluster’ multiple DHCP servers, causing them to work together to provide uninterrupted DHCP services in the event a single server ceases to function.

Port Table

The port table is where the DHCP server is enabled for the appropriate logical interface of the device.

- Port:
  Select the logical interface for which the DHCP server should be enabled or disabled.
- Enable DHCP:
  Enables or disables the DHCP server for the selected logical interface.

Additional Options

DHCP options can be used to send additional configuration parameters to the clients. The vendor class ID (DHCP option 60) shows, for example, the type of device. This table allows additional options for DHCP operations to be defined.

- Option number:
  Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example ‘17’ (root path) is the path to a boot image that a PC without its own hard disk uses to obtain its operating system via BOOTP. You can find a complete list of DHCP options in RFC 2132 – ’DHCP Options and BOOTP Vendor Extensions’ of the Internet Engineering Task Force (IETF).
- Network name:
  Name of the IP network where this DHCP option is to be used.

- Option type:
  Description of the DHCP option type.
- Option value:
  This field defines the contents of the DHCP option. For the option ‘17’ for example, the path is entered for a boot image that a PC without its own hard disk uses to obtain its operating system via BOOTP.

DHCP Table

The DHCP table provides an overview of the IP addresses used in the IP networks. The DHCP table is purely a status table where no parameters can be configured.

- IP address:
  IP address the DHCP server has assigned to the station.
- MAC address:
  The client's MAC address.
- Timeout:
  Period of validity (lease) for the address assignment in minutes.
- Hostname:
  Name of the client, if it was possible to determine this.
- Type:
  The 'Type' field indicates how the address was assigned. This field may contain the following values:
  - New: The client made the request for the first time. The DHCP checks that the address to be assigned to the client is unique.
  - Unknown: When the server checked if the address was unique, it was found that the address had already been assigned to another client. As a result, the server can obtain no additional information.
  - Stat: A client has informed the DHCP server that it has a fixed IP address. Because an IP address is defined as unique, this IP address is reserved exclusively for this client.
  - Dyn.: The DHCP server has assigned an address to the client.
  - Cache: The DHCP server has assigned an address from the cache to the client.

- LAN lfc:
  Logical interface connecting the client to the device.
- Ethernet port:
  Physical interface over which the DHCP server assigned the IP address to the station.
- VLAN ID:
  The VLAN ID used by the client.
- Network name:
  Name of the IP network where the client is located.
- Assignment:
  Point in time when the DHCP server assigned the IP address to the station

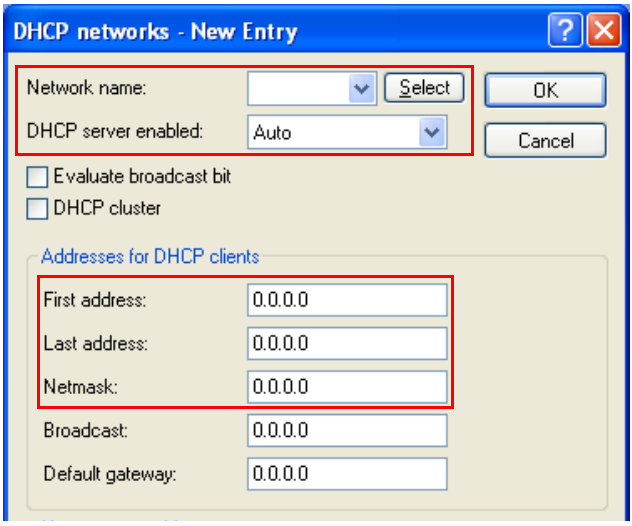
15.1.4 DHCP Relay Server

In addition to forwarding DHCP requests, a OpenBAT device is not limited to forwarding DHCP requests to higher-level DHCP servers; a OpenBAT device can also function as a central DHCP server (DHCP relay server). For a OpenBAT device to be configured as a DHCP relay server to other networks, enter the relay agent IP address (the gateway IP address—GI address) as the network name in the table of IP networks.

If the same network is being used by several relay agents (e.g. multiple access points are forwarding requests to a central DHCP server) then the GI address can also be abbreviated with an asterisk (*). If, for example, clients in the remote network "10.1.1.0/255.255.255.0" are to be assigned addresses and several relay agents are available in this network, all of which use the OpenBAT device as higher-level DHCP server, then the assignment of IP addresses and standard gateway to the clients can take place as follows:

☐ Navigate to the following dialog:`Configuration : IPv4 : DHCPv4` and click "IP networks".

☐ In the ‘DHCP networks’ dialog, either select an existing network and click ‘Edit...’ or click ‘Add...’ to create a new DHCP network.



In this example, enter values for at least the following fields:

- Network name: ‘10.1.1.*’
- DHCP server enabled: ‘Yes’
- First address ‘10.1.1.100’
- Last address: ‘10.1.1.105’
- Netmask: ‘255.255.255.0’

Note: To operate a DHCP relay server, define both the IP address range and the netmask.

DNS Resolution of Names Learned via DHCP

The DNS server considers the interface tags when resolving names learned via DHCP. The names to be resolved are exclusively those that were learned from a network with the same interface tag as the requesting computer. If the request arrives from an untagged network, then all names are resolved, including those that were learned via tagged networks. Similarly, all names that were learned from untagged networks are visible for tagged networks.

Names learned from relay agents are handled as though they were learned from an untagged network. These names are visible to all networks.

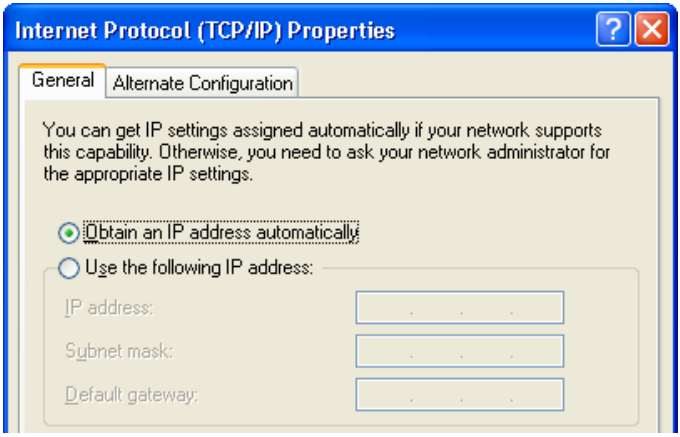
15.1.5 Configuring Clients

It is standard in a Windows network environment to configure settings so that parameters, which are necessary for device operation, can be requested via DHCP. To check your Windows settings, in your Windows desktop, select:

☐ Navigate to the Windows Control Panel and open the `Network Connections` dialog.

☐ Right click on a 'Local Area Connection' and select 'Properties' from the pop-up menu.

☐ Select 'Internet protocol (TCP/IP)' then click 'Properties' to open the 'TCP/IP Properties' dialog.



In the ‘General’ tab of this dialog, you can see if IP address settings are specially configured for this client, or if they are automatically obtained from a DHCP server.

If a client is to use different IP addressing parameters from the ones assigned (e.g. for a standard gateway), these need to be configured at the workstation itself. In that case, the client ignores the parameters assigned by the DHCP server.

15.1.6 Checking IP Addresses in the LAN

You can view a summary of the LAN IP addresses in the DHCP table at:

```
HiLCOS menu tree : Status : TCP/IP : DHCP : DHCP table
HiLCOS menu tree :Setup : DHCP : DHCP table
```

The DHCP table shows the assigned and used IP address, the MAC address, the lease, the client's name (if available) as well as the type of address assignment:

DHCP-Table

IP-Address	MAC-Address	Timeout	Hostname	Type	LAN-Ifc	Ethernet-Port	VLAN-ID	Network-name	Assignment
192.168.2.3	0001e37	441		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 12:35:52
192.168.2.28	848f69d1	393		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 13:29:48
192.168.2.29	0021709	94		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 09:45:41
192.168.2.56	bc47602	354		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 11:08:53
192.168.2.63	001f1fba	112		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 07:06:49
192.168.2.89	000085e	441		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 12:35:43
192.168.2.90	001d09d	422		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 13:30:27
192.168.2.98	74e2f50	4861		dyn.	LAN-1	unbekannt	0	INTRANET	14.07.2013 18:36:24
192.168.2.108	002170e	478		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 13:12:56
192.168.2.118	000c297	284		dyn.	LAN-1	unbekannt	0	INTRANET	15.07.2013 09:58:43

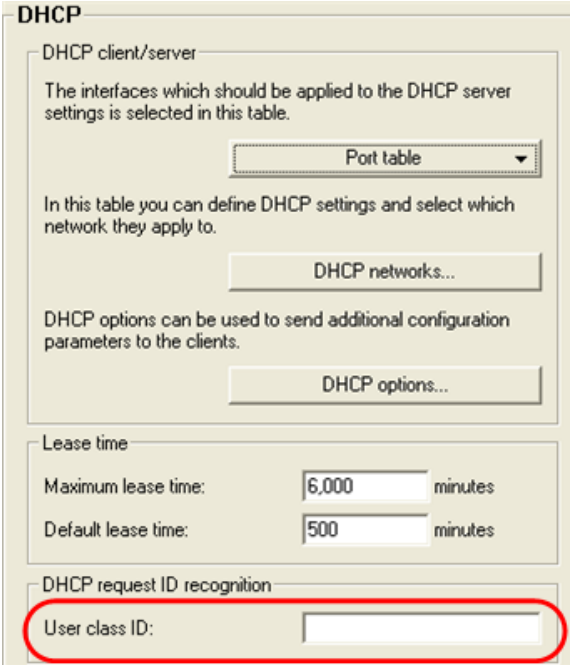
15.2 Vendor class and User class identifiers

The DHCP client in a OpenBAT device can insert additional information in the DHCP request sent, which simplifies request recognition within the network.

- The vendor class identifier (DHCP option 60) shows the device type. The vendor class ID is included in the transmission.
- The user class identifier (DHCP option 77) displays a user-defined string of up to 63 characters. The user class ID is transmitted when the user has configured a value.

To configure the user class ID:

☐ Navigate to the following dialog:`Configuration : IPv4 : DHCPv4` and enter a value into the field "User class ID".



15.3 DNS

The domain name service (DNS) in TCP/IP networks is responsible for associating computer names to network (domain) and IP addresses. This service is required for Internet communications. It is also useful to be able to clearly associate IP addresses to computer names within a local network or in a LAN interconnection.

15.3.1 DNS Functions

The names used in DNS server requests consist of several parts:

- One part is the actual name of the host or service to be addressed.
- Another part specifies the domain.

Specifying the domain is optional within a local network. These names could thus be 'www.domain.com' or 'ftp.domain.com', for example.

If no DNS server exists in the local network, all locally unknown names are searched for using the default route. By using a DNS server, it is possible to go immediately to the correct remote station for all of the names with known IP addresses. In theory, the DNS server can be a separate computer in the network. However, locating the DNS server directly in the OpenBAT device is a better design, for the following reasons:

- The OpenBAT device can automatically distribute IP addresses to the computers in the LAN when operating as a DHCP server. It already knows the names and IP addresses of all of the computers in its own network that were assigned IP addresses via DHCP. Because of the dynamic address assignments by the DHCP server, an external DNS server might have difficulties in keeping the associations current between the names and IP addresses.
- When routing Microsoft Networks via NetBIOS, the OpenBAT device also knows the computer names and IP addresses in the other connected NetBIOS networks. In addition, computers with fixed IP addresses can also enter themselves in the NetBIOS table and thus be known by both their names and addresses.
- The DNS server in the OpenBAT device can also be used as an extremely convenient filter mechanism. Requests for domains can be prohibited throughout the LAN, for subnetworks, or even for individual computers —simply by specifying the domain name.

How the DNS Server Responds to Requests

When processing requests for specific names, the DNS server takes advantage of all of the information available to it:

- First, the DNS server determines whether access to the name is prohibited by the filter list. If that is the case, the DNS servers returns an exception response to the requesting computer stating that access to the address is denied.
- Next, the DNS server searches in its own static DNS table for suitable entries.
- If the address cannot be found in the DNS table, the DNS server searches the dynamic DHCP table. The use of DHCP information can be disabled.

- If no information for the name can be located in the previous tables, the DNS server searches the lists of the NetBIOS module. The use of the NetBIOS information can also be disabled if necessary.
- Finally, the DNS server checks whether the request is to be forwarded to another DNS server via a WAN interface (special DNS forwarding via the DNS destination table).

If the requested name cannot be found in any of the information sources available to it, the DNS server sends the request to another server—that of the Internet provider, for example—using the general DNS forwarding mechanism, or returns an exception response to the requesting computer.

15.3.2 DNS Forwarding

If it cannot serve the request from its own DNS tables, the DNS server forwards the request to other DNS servers. This process is called DNS forwarding. Note that there is a distinction between:

- Special forwarding: Requests for certain name areas are forwarded to certain DNS servers.
- General DNS forwarding: All other names not specified in detail are forwarded to the ‘higher-level’ DNS server.

Special DNS Forwarding

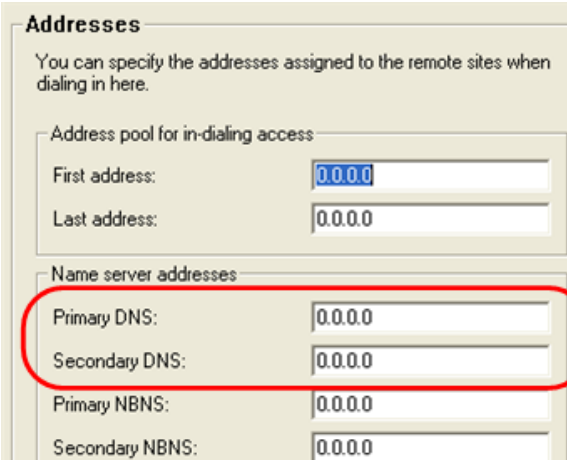
With special DNS forwarding, you can define name areas that can determine which specified DNS server is addressed. A typical application for special DNS involves the case of a home workstation. The user wants to be able to connect to the company intranet and directly to the Internet at the same time. The requests sent into the intranet need to be routed to the company DNS server, and other requests need to be routed to the DNS server of the provider.

General DNS Forwarding

DNS requests that cannot be resolved in another way are forwarded to a DNS server. The identity of this DNS server is determined according to the following rules:

- Initially, the router checks whether a DNS server has been identified in its own configuration settings. If so, it obtains the desired information from this server. Up to two higher-level DNS servers ('Primary DNS' and 'Secondary DNS') can be set in LANconfig at:

  ☐ `Configuration : IPv4 :Addresses.`



- If no DNS server has been identified in the device configuration, the router attempts to reach a DNS server over a PPP connection (e.g. from the Internet provider) to obtain the IP address assigned to the name. This can succeed if the address of a DNS server is sent to the router during PPP negotiation.
- If no such PPP connection exists, the default route is established and the DNS server searched for.

Entering the Intranet address of your router as the DNS server for the workstation computers is sufficient to enable you to obtain the name assignment. This procedure also automatically updates the address of the DNS server. Your local network receives the most current information even if, for example, the provider sending the address changes the name of his DNS server or you change to another provider.

15.3.3 Configuring the DNS Server

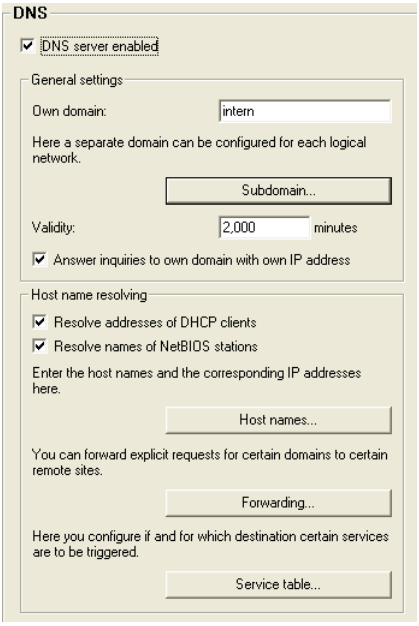
A DNS server translates the names of certain stations (e.g. www.company.com) to their IP addresses (e.g. 208.49.229.140). Normally, your Internet provider’s DNS server looks up the names of all Internet addresses. You can use the unit’s DNS server to translate the names of stations in your local network. Queries for names that are not known to the unit are automatically forwarded to your Internet provider's DNS server.

Configuring the DNS server is accomplished by enabling the DNS server, then making the following DNS settings:

- General settings
- Defining subdomains
- Host name resolution settings
- Creating host names
- Forwarding explicit requests
- Configuring services

To enable the DNS server:

☐ Navigate to the following dialog:`Configuration : IPv4 : DNS` and select the option "DNS server enabled".



DNS settings can be entered via this dialog.

General DNS Settings

Enter values for the following general DNS settings in the ‘DNS’ dialog:

- Own domain:
  If you have an intranet of your own to which you would like to assign a domain name, enter it here (e.g. myhome.intern). If, for example, a computer with the name myhost were located in your network, its full name would be myhost.myhome.intern. However, you may also enter the name of your local network here if it belongs to a valid Internet domain (e.g. company.com).
- Validity:
  Some computers save the names and addresses of locations looked up by the DNS server to provide faster access to this information in the future. Enter the duration for which this stored data will remain valid. It will be necessary for the computer to request the information again after this period has elapsed.
- Answer inquiries to own domain with own IP address: (Self-explanatory).

Defining Subdomains

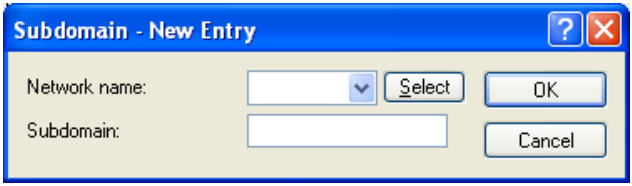
You can also define a separate sub-domain for each logical network. If, for example, your domain (own domain) is named 'internal' and the sub-domain of a logical network is named ‘intranet’, then the domain for this logical network would be intranet.internal. The name of a server in this network consists of:

hostname.subdomain.own-domain.

If your own domain is not specified, then define the desired domain for each logical network completely in the sub-domain. The domains defined here are distributed to the logical networks by the DHCP server in the device. To configure a subdomain:

☐ Beginning in the ‘DNS’ dialog, click ‘Subdomain...’.

☐ In the ‘Subdomain’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



Configure the following parameters for each subdomain:

- Network name: The hostname.
- Subdomain:
  The name of the subdomain and, if appropriate, the own domain.

Hostname Resolution Settings

Enter values for the following hostname resolution settings in the ‘DNS’ dialog:

- Resolve address of DHCP clients:
  Select this to have the DNS server look up the names of stations that have requested an IP address via DHCP.
- Resolve names of NetBIOS stations:
  Select this to have the DNS server translate the names of stations that are known to the NetBIOS router.

Creating Host Names

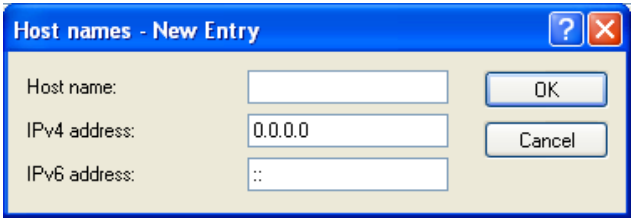
A client sends a query to the DNS server when it wants to have the name of a station looked up. The server responds to this query with the IP address entered here. You should create a list of host names, associating each entry with its respective IP address, including every client that meets all the following tests:

– the client hostname and IP address are known
– the client is located outside your own LAN
– the client is not on the Internet, and
– the client is accessible via the router

To enter a client to the host name list:

☐ Beginning in the ‘DNS’ dialog, click ‘Host names...’.

☐ In the ‘Host names’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



Configure the following parameters for each host name entry:

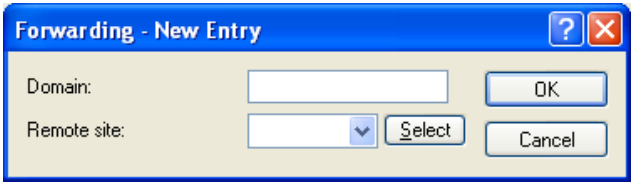
- Host name:
  Enter the name of the station here. For example, if you have a computer named myhost and the name of your domain is myhome.intern, then enter the host name myhost.myhome.intern.
- IPv4/IPv6 address: Enter the IP address of the station.

Forwarding Explicit Requests

To resolve entire name areas of another DNS server, you can add a forwarding entry consisting of a name area and remote station. When entering the name areas, you can use the wildcards '?' (for individual characters) and '*' (for multiple characters). To reroute all domains with the ending '.intern' to a DNS server in the LAN of the remote station 'COMPANY', create the following entry

☐ Beginning in the ‘DNS’ dialog, click ‘Forwarding...’.

☐ In the ‘Forwarding’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



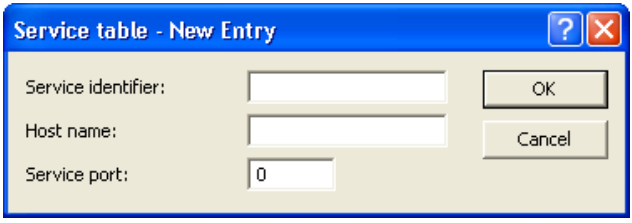
Configure the following parameters for each host name entry:

- Domain:
  Enter the name domain area. The entry `*.interal` for example causes all domains ending with '.intern' being redirected.
- Remote site:
  Enter the name of the remote station.

Configuring Services

☐ You can identify services to be resolved by the router.

☐ In the ‘Service table’, click ‘Add...’ to open the ‘New Entry’ dialog:



Configure the following parameters for each service to be resolved:

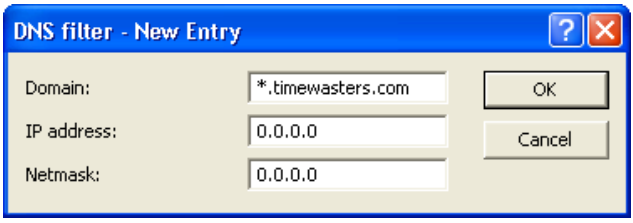
- Service identifier:
  Enter the service to be resolved according to RFC 2782.
- Host name:
  Enter the name of the host providing the specified service. If for example there is a computer named myhost and the name of your domain is myhome.intern, enter myhost.myhome.intern as the station name.
  – The station name '[self]' may be entered as name, if it is the device itself.
  – A dot '.' may be specified if this service is blocked and therefore not to be resolved. In this case the specification of a port number will be ignored.
- Service port:
  The port number used by the named service at the specified station.

15.3.4 URL Blocking

You can block access from your network to specific stations or domains with the filter list. To access the filter list:

☐ Navigate to the following dialog:`Configuration : IPv4 : DNS Filter` and click "DNS filter".

☐ In the ‘DNS filter’ list, click ‘Add...’ to open the ‘New Entry’ dialog:



To enter a new DNS filter item, complete these parameters:

- Domain:
  Enter the name of a destination station or domain that should be blocked from access. You can use the wildcards '?' for single characters and '*' for groups of characters, for example `*.mydomain.com`.
- IP address:
  Enter the IP address of a station, or range of stations, that are denied access to domain. A value of ‘0.0.0.0’ describes all computers in the network.
- Netmask:
  Enter the netmask of a station, or range of stations, that are denied access to domain. A value of ‘0.0.0.0’ describes all networks.
- IPv6 prefix:
  Specify the IPv6 prefix to be used by the device for filtering IPv6 addresses by domain. The value `::/0` describes all IPv6 addresses.

Note: The list in the DNS statistics contains the 64 most frequently requested names and provides a good basis for setting up the filter list. If your LAN uses subnetting, you can also apply filters to individual departments by carefully selecting the IP addresses and subnet masks.

15.3.5 Dynamic DNS

Systems with dynamic IP addresses become accessible over the WAN—for example over the Internet—via so-called Dynamic DNS service providers, e.g. www.dynDNS.org. Thereby a OpenBAT device becomes available under a certain DNS-resolvable name (FQDN – "fully qualified Domain Name," for example "http://MyDevice.dynDNS.org").

To accomplish maintenance for a remote site, for example, you just need to know the appropriate Dynamic DNS name.

Updating IP address entries in the Dynamic DNS server

Dynamic DNS providers support a set of client programs, which can determine the current assigned WAN IP address of a OpenBAT device via different methods (3, below), and transfer this address—in case of a change—to their respective Dynamic DNS server.

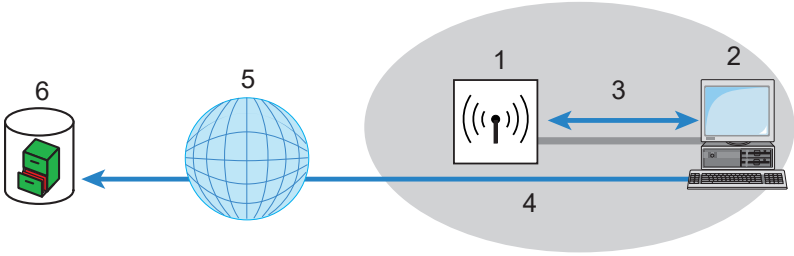
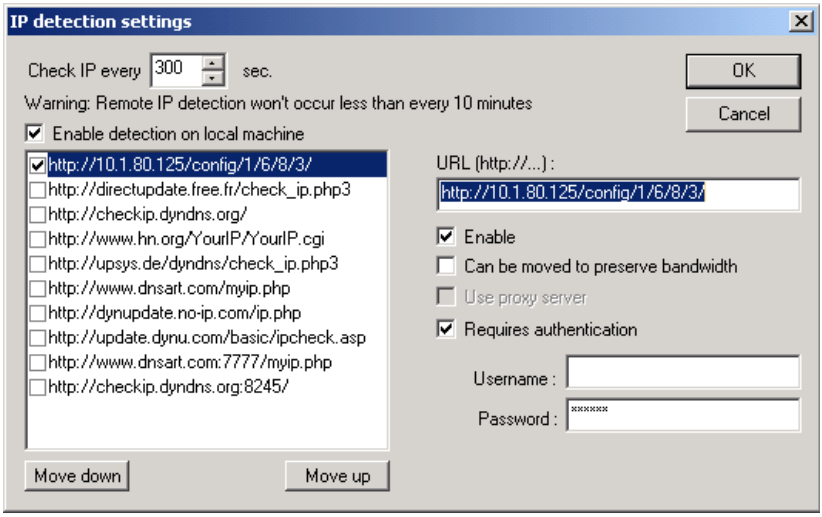


Figure 129:Updating the current IP address in the dynamic DNS server

1:OpenBAT device	4: PC updates DNS server
2: PC with DynDNS client program	5: Internet
3: PC determines current IP address of OpenBAT	6: Dynamic DNS server

The current WAN IP address of a device can be selected at:

```
http://<Address of the Device>/config/1/6/8/3/
```



Note: The above screenshot illustrates how to access the WAN IP address on the WEB interface from an external application.

Alternatively the OpenBAT device can directly transmit the present WAN IP to the DynDNS provider:

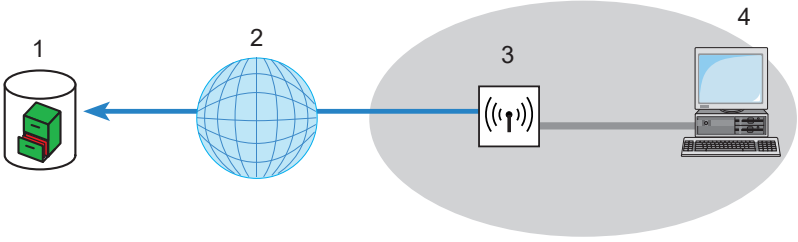
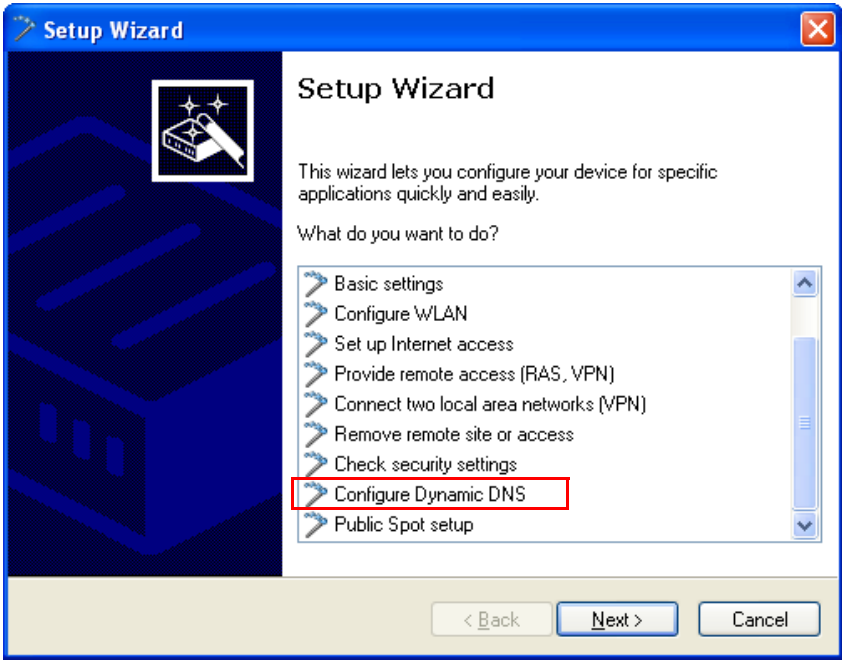


Figure 130:The OpenBAT device directly transmits its IP address to the DynDNS provider.

1: DynDNS provider	3: OpenBAT Device
2: Internet	4: Client

The settings necessary for this can be adjusted easily by using the ‘Configure Dynamic DNS’ Setup Wizard in LANconfig, see section "Configure Dynamic DNS":

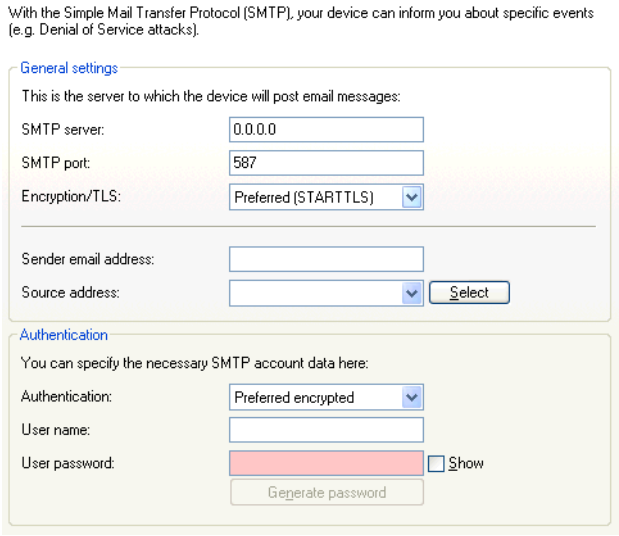

Setup Wizard
Setup Wizard
This wizard lets you configure your device for specific applications quickly and easily.
What do you want to do?
Basic settings
Configure WLAN
Set up Internet access
Provide remote access (RAS, VPN)
Connect two local area networks (VPN)
Remove remote site or access
Check security settings
Configure Dynamic DNS
Public Spot setup
< Back
Next >
Cancel

15.4 Setting up an e-mail address to send messages

A HiLCOS device can send e-mail to a predefined address if certain events should occur. These events can include:You set up the e-mail address as follows:

- Information about disconnections on a WAN interface
- Messages from the firewall
- Sending VPN profiles

In LANconfig you can can configure an e-mail under `Log & Trace:SMTP account`.



"SMTP server": In this field, enter the IP address of the SMTP server.

"SMTP port": By default, this is set to port 587 for transmitting unencrypted e-mails.

"Encryption/TLS": Here you determine if and how the device encrypts the connection. The available values have the following meaning:

- "None": No encryption. The device ignores any STARTTLS responses from the server.
- "Encrypted (SMTPS)": The device uses SMTPS, i.e. encryption is active from the connection establishment.
- "Preferred (STARTTLS)": The connection establishment is not encrypted. If the SMTP server offers STARTTLS, the device will use encryption. This is the default setting.
- "Required (STARTTLS)": The connection establishment is not encrypted. If the SMTP server does not offer STARTTLS, the device transmits no data.

"Sender e-mail address": Enter a valid e-mail address for the HiLCOS to use as the sender address. The specified SMTP server will message this address in case of delivery problems, for example. If this address is not specified or not valid, some SMTP servers may refuse to deliver any messages.

"Source address": You can optionally set an alternative sender address here to be used by the HiLCOS. If you have configured loopback addresses, you can specify them here as sender address. The field accepts various input formats:

- Name of the IP network (ARF network), whose address should be used by the device.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ. If there is an interface named "DMZ", then the device uses this address.
- "LB0" … "LBF" for one of the 16 loopback addresses, or its name
- Any IP address in the form `x.x.x.x`.

"Authentication:" Here you determine if and how the device authenticates at the SMTP server. The available values have the following meaning:

- "None": No authentication.
- "Preferred plain text": Authentication takes place in plain text (PLAIN, LOGIN) if the server requires authentication. If you do not want plain-text authentication, the device uses a secure authentication method.
- "Preferred encrypted": Secure authentication takes place, if possible. Otherwise the device uses either a plain text authentication or no authentication at all, depending on the server settings.
- "Encrypted": If the server requires authentication, the password is sent in encrypted (e.g. CRAM-MD5). Plain text authentication does not occur.

"Name": Enter the user name which the HiLCOS uses to login to the SMTP server.

"Password": Enter the password which the HiLCOS uses to login to the SMTP server.

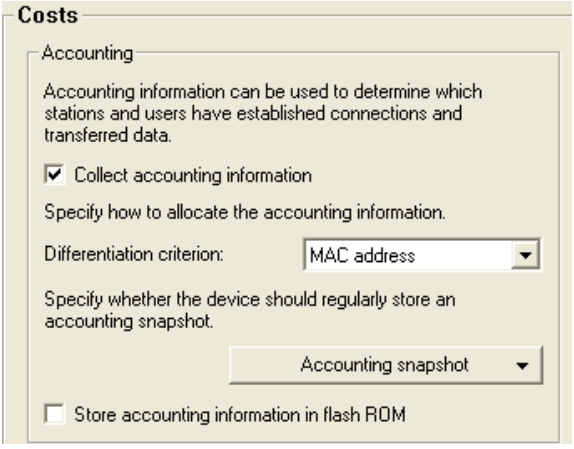
15.5 Accounting

Information on connections between clients in the local network and various remote stations is saved in the accounting table with entries for the connection time and the transferred data volume. Using accounting snapshots, accounting data can be regularly saved at specific times for later evaluation.

15.5.1 Configuring General Accounting Parameters

To configure general accounting parameters:

☐ Navigate to the following dialog:`Configuration : Management : Costs`.



Configure the following general accounting parameters:

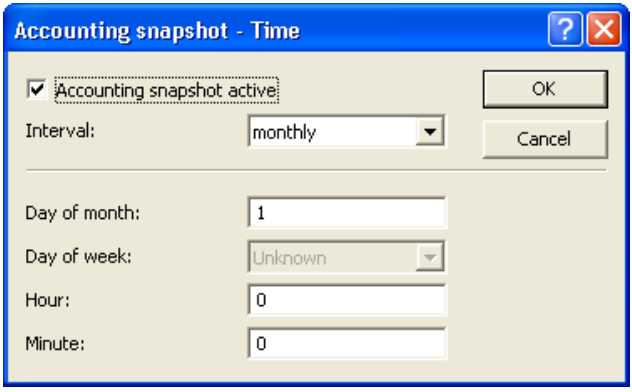
- Collect accounting information:
  Turns accounting on or off.
- Differentiation criterion:
  Select the feature according to which the accounting data are to be gathered:
  – MAC address: The data are collected according to the client's MAC address.
  – IP address: The data are collected according to the client's IP address.

  Note: When dynamic IP addresses are in use, the option 'IP address' can lead to inaccurate accounting data. In this case, it may not be possible to accurately assign the data to users. Conversely, with this setting, data can be separated from clients that are behind another router and therefore appear with the same MAC address as the router in the accounting list.
- Store accounting information in flash ROM:
  Turn accounting data in flash memory on or off. Accounting data saved to flash will be preserved in the event of a power outage.

15.5.2 Configuring the Snapshot

You can specify if and when the device should capture and store an accounting snapshot. To do this:

☐ In the ‘Accounting’ section of the ‘Costs’ dialog, click ‘Accounting snapshot’ and select the time menu item to open the ‘Time’ dialog:



In the ‘Time’ dialog, enter values for the following properties:

- Accounting snapshot active:
  Turns intermediate storage of accounting data on or off.
- Interval: Monthly, Weekly, Daily.
- Day of month:
  The day of the month on which caching will take place: Relevant if the interval is 'monthly'.
- Day of week:
  The weekday on which caching will take place. Relevant if the interval is 'weekly'.
- Hour: The hour on which caching will take place: 0 to 23
- Minute: The minute in which caching will take place: 0 to 59

15.6 Call Charge Management

The capability of the router to automatically establish connections to all desired remote sites, and to close them again when no longer required, provides users with extremely convenient access, e.g., to the Internet. However, very substantial costs can be incurred by data transfer over paid lines if the router is configured diffusely (e.g. in the filter configuration) or by excessive use of the communications opportunities (e.g. extended surfing in the Internet).

15.6.1 Connection limits for DSL and cable modem

Even though a DSL or cable modem connection behaves like a leased line, in that it is continuously online, connection charges can accrue over time, depending on the provider.

Note: Only DSL connections will be discussed in the remainder of this section The explanations apply equally well, however, to any other type of connection made via the Ethernet WAN port of the OpenBAT device, for example, cable modem connections.

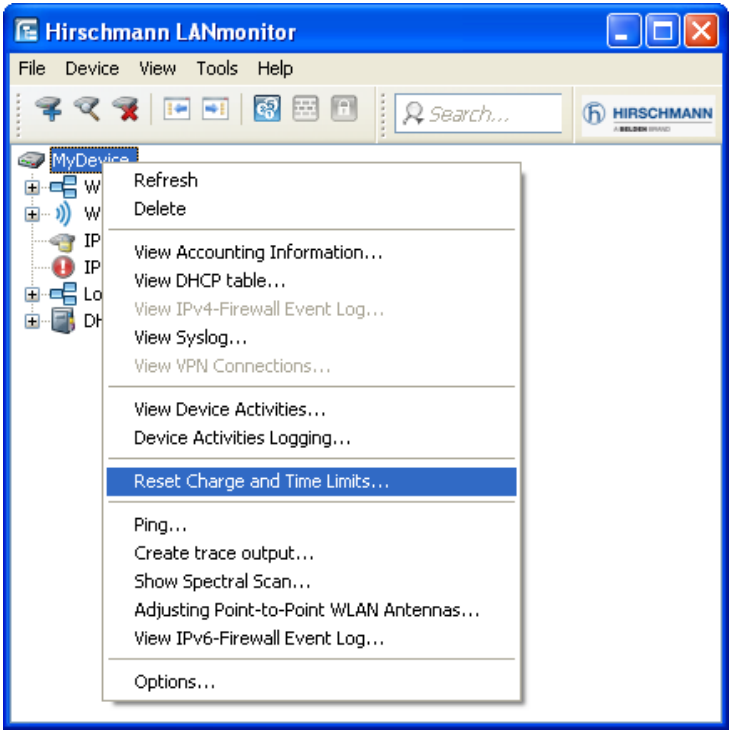
To limit the costs, a time limit for DSL connections can be set for a specified period of time. By default the DSL connections can be used for a maximum of 600 minutes in 6 days.

If the limit is reached, all DSL connections are automatically terminated. As soon as the current period has elapsed, the time count is reset and the connection enabled. The administrator can manually reset the time count and re-establish the connection before the connection is automatically re-enabled.

If the connection has a charge limit and a short hold of '0' or '9999' seconds, the charge control is switched off and the connection is kept open even if the limit is exceeded.

If in an exceptional case you would like to extend the online budget, e.g. to download a large file from the internet, you can manually reset the limit, as follows:

☐ In LANmonitor, select the device indicating a time event, click the right mouse button, then select '`Reset Charge and Time Limits...`' from the pop-up menu.



Note: If you cannot see the system information in LANmonitor, you can display it as follows:

☐ Select `View : Show Details : System Information`.

You can also access the commands to activate the additional time limit at:

`HiLCOS Menu Tree : Setup : Fees`

The additional time limit is activated for the current period, in the following period normal time limit is set.

15.7 Time Server

OpenBAT devices can obtain highly precise time information via publically accessible time servers in the Internet (NTP server with open access policy, e.g., that of the Physikalisch-Technische Bundesanstalt). The time obtained this way can be made available to all stations in the network.

15.7.1 Configuring the time server with LANconfig

To provide the current time in the local network your OpenBAT device has to regularly apply the time from a time server. Configuring a time server is a two-step process:

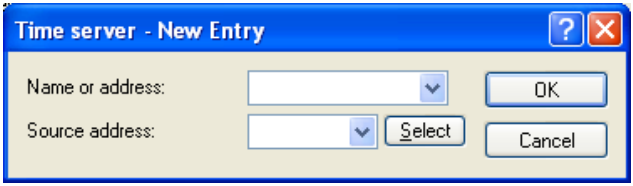
- Selecting a time server for the device
- Enabling the time server

Selecting a Time Server

You can create a list of available time servers in LANconfig. The OpenBAT device will attempt to obtain time information from time servers in the order in which they appear in the list. To enter a time server to this list, follow these steps:

☐ Navigate to the following dialog:`Configuration : Date & Time : Synchronization` and click "Time server".

☐ In the ‘Time server’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



Define a new time server entry using the following parameters:

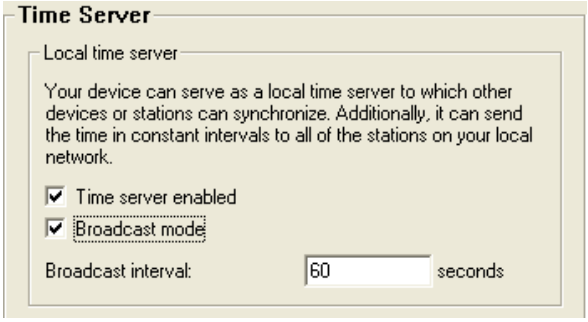
- Name or address:
  Select a time server from the list, or type in a time server using its name or IP address.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the 'Name or address' setting, which is otherwise obtained automatically for the respective destination address.

After an item has been entered into the list, you can use the up/down buttons to change the position of a selected list item.

Enabling the Time Server

After one or more time server entries have been created, and their relative positions established in the list, you can enable the time service, as follows:

☐ Navigate to the following dialog:`Configuration : Date & Time : time server`.



To enable the time service, configure the following parameters:

- Time server enabled:
  Enables the NTP time service.
- Broadcast mode:
  Select this to have the server broadcast the actual time to all reachable devices or stations in the local network in constant intervals.

15.7.2 Configuring the time server with WEBconfig

You can also use Telnet or WEBconfig to configure the time server, at:

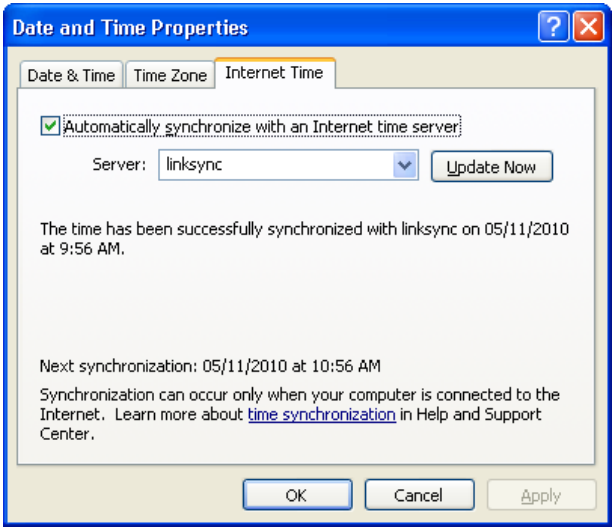
`HiLCOS Menu Tree : Setup : NTP`

15.7.3 Configuring NTP Clients

The NTP clients need to be configured so that they use the time information from the OpenBAT device. The Windows XP operating system provides an integrated NTP client; other operating systems may require installation of a separate NTP client. Linux distributions have to be installed with NTP.

You can open the settings for date and time in a Windows system as follows:

☐ Double click on the time setting on the Windows task bar, then select the ‘Internet time’ tab:

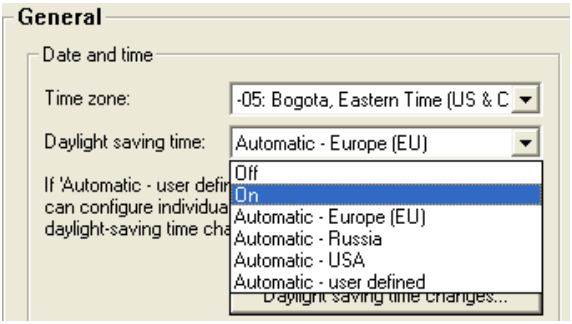


Configuring Time

OpenBAT devices work internally with coordinated world time (UTC). For protocol displays and time-related settings (e.g. cron jobs), the local time is derived from the selected time zone. To take local daylight-saving time into account, settings can be configured according to local conditions.

To configure the time for a device:

☐ Navigate to the following dialog:`Configuration : Date & Time : General`.



Configure the following parameters:

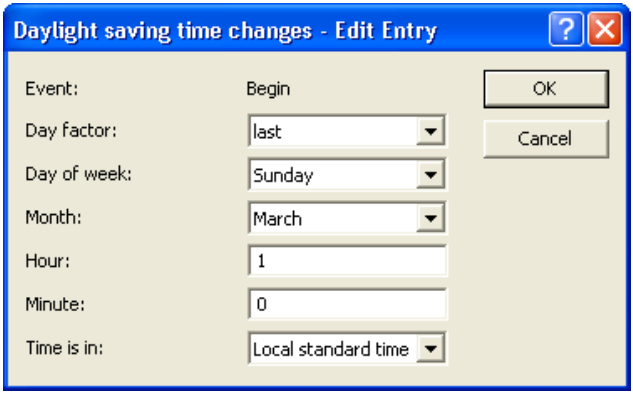
- Time zone:
  Select your time zone.
- Daylight saving time:
  Values include:
  - Off: The system time will not be adjusted to daylight-saving time.
  - On: One hour is added statically to the current system time (comprised of UTC and time zone).
  - Automatic (EU, USA, Russia): The daylight-saving time change is performed automatically in conformance with the time zone of the device's location.
  - Automatic (user-defined): If the device is located in an area that is not listed here, then the daylight-saving time change options can be manually defined by the user.

User-Defined Daylight Savings Time Settings

User-defined values can be set for the beginning and the end of the automatic daylight-saving time change.

☐ Open the `Configuration : Date & Time : General` and click "Daylight saving time changes".

☐ In the ‘Daylight saving time changes’ window, select the ‘Begin’ event and click ‘Edit...’:



Configure the following parameters: for the beginning of the daylight saving time period.

- Day Factor:
  Defines the recurring weekday of the month when the change will take place.
- Day of the Week: The day of the week the change begins.
- Month: The month the change begins.
- Hour: The hour the change begins.
- Minute: The minute the change begins.
- Time is in:
  Defines the time zone which is the basis for the time settings in this table (Coordinated Universal Time or Local Standard Time).

Next, select the ‘End’ entry in the ‘Daylight Saving time changes’ table, click ‘Edit...’ and configure the same parameters defining the end of the daylight savings time period.

15.8 Scheduled Events

This function is intended to allow the device to execute predefined commands in a telnet-like environment, at times defined by the user. The functionality is equivalent to the UNIX cron service. Any desired OpenBAT device command line function can be executed. Thus, the full feature set of all OpenBAT devices can be controlled by this timing function. The following examples illustrate the scheduled events function:

- A scheduled connection:
  Many leased lines disconnect automatically after 24 hours of continuous operation. This enforced disconnection can have some unwanted side-effects, for example if it occurs at an inconvenient time. To control the disconnecting time, a manual disconnection can be set, thereby avoiding ill-timed disconnections.
- Time-dependant firewall or QoS rules:
  Firewall and QoS rules are, at first, constant in their duration. However, it can be useful to apply variable settings for different times or days. For example: for off-hours or weekends may require different levels of bandwidth availability than during business hours.
- Regular firmware or configuration updates:
  Time-controlled rules let you toggle the settings of particular parameters, and switch to an entirely different configuration. This possibility allows you to pool a whole string of settings and change them all at once with a single command. Thus, you can apply one set of operating settings to the device over the weekend, then switch back to a different configuration on Monday mornings, with just one command. In addition, a regular update of the newest firmware from a single source is adjustable.
- E-mail messages:
  With time-controlled rules, you can configure the OpenBAT device to send e-mail notification to the administrator for specific firewall events, and also at scheduled times. A scheduled e-mail might contain information about successfully re-establishing an internet connection after an enforced disconnection, or a re-boot of the device after a restart.

- Time-dependent interfaces:
  The time dependant use of interfaces for a set duration can also be configured using time-controlled rules. For example, a WLAN interface can permit the wireless access to the network exclusively at certain times.
- Deleting specific tables:
  It can be useful to regularly clear the content of some tables in the OpenBAT device operating system. For example, if your Internet access has a monthly limited transfer volume, you can delete your accounting table monthly to contain a survey of just the present transferred data volume.

15.8.1 CRON Jobs With Time Delay

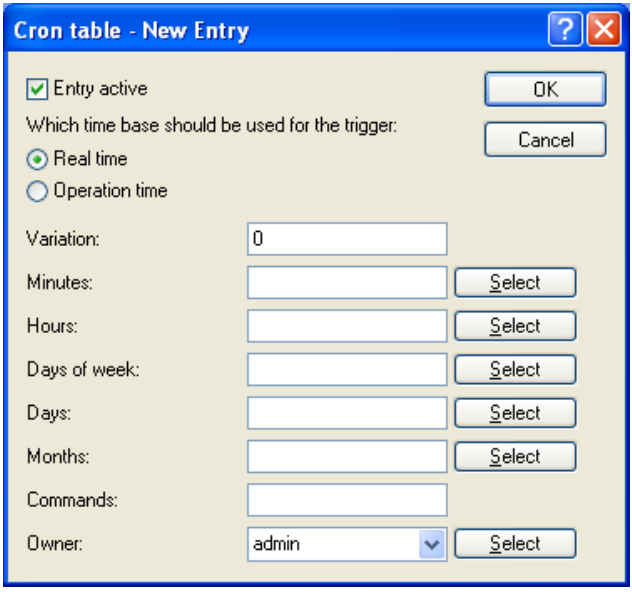
CRON jobs are used to automatically carry out recurring tasks on a OpenBAT device at specified times. If the installation features a large number of active devices, all of which are subjected to the same CRON job at the same time (e.g. updating a configuration by script), unpleasant side effects can result: All devices may simultaneously attempt to establish a connection, for example. To avoid these effects, CRON jobs can be set with a random delay time between 0 and 59 minutes.

15.8.2 Configuring a CRON Job

You can use LANconfig to configure a CRON job, as follows:

☐ Navigate to the following dialog: `Configuration : Date & Time : General` and click "Cron table".

☐ In the ‘Cron table’ window, click ‘Add...’ to open the ‘New Entry’ dialog:



Enter values for the following CRON job properties:

- Entry active: Activates or de-activates the CRON job entry.
- Which time base should be used for the trigger:
  This field determines whether time control is based on real time or on the device's operating time:
  – Real time: These rules evaluate all time/date information.
  – Operation time: These rules exclusively evaluate the minutes and hours since the last time the device was started.
- Variation:
  This specifies the maximum delay, from 0 to 65536 minutes, for the start of the CRON job after the set start time. The actual delay time is determined randomly and lies between 0 and the time entered here.
- Minutes:
  Enter a comma-separated list of those minutes for which you want the specified device commands to be executed. If all other specified time fields match, the associated device commands will be executed once for every minute specified.

- Hours:
  Enter a comma-separated list of those hours for which you want the specified device commands to be executed. If all other specified time fields match, the associated device commands will be executed once for every hour specified.
- Days of week:
  Use a comma-separated list to enter the days of the week on which you want the specified device commands to be executed. The days of the week are sequentially represented by numbers:
  – 0 = Sunday
  – ...
  – 7 = Saturday
- Days:
  Use a comma-separated list to enter all of the days of a month on which you want the specified device commands to be executed. If all other specified time fields match, the associated device commands will be executed on every day of month specified (can be refined optionally by stating specific hours and minutes).
- Months:
  Use a comma-separated list to enter all of the months of a year on which you want the specified device commands to be executed. If all other specified time fields match, the associated device commands will be executed in every specified month (can be refined optionally by stating specific days, days of week, hours and minutes).
- Commands:
  Use a semicolon separated list to enter all commands that you want to be executed if all time entries match. Any commands that you can enter in a Telnet session are allowed. Advisable commands are those that end in an action, e.g. PING, TESTMAIL, DO or SET.
- Owner:
  An administrator defined in the device can be designated as owner of the CRON job. If an owner is defined, then the CRON job commands will be executed with the rights of the owner.

Real-time based rules can be executed provided that the device has a time from a relevant source, e.g. via NTP. For example:

time base	min.	hours	w-days	m-days	months	Command
Real time	0	4	0/-6	1/-31	1/-12	do /oth/man/disconnect internet
Real time	59	3	0/-6	1/-31	1/-12	mailto:admin@mydevice.de?subject=disconnection?body=Manual disconnection of the internet connection
Real time	0	0	–	1	–	do /setup/accounting/delete
Real time	0	18	1.2, 3.4, or 5	–	–	do /oth/man/connect HEADQUARTER

- The first entry cuts the connection to the internet provider every morning at 4 am (forced disconnection).
- The second entry sends an information mail every morning at 3:59 am (directly before the forced disconnection) to the admin.
- The third entry deletes on the first of every month the accounting table.
- The fourth entry builds up a connection to the headquarter every week day at 6 pm.

Note: Time-based rules are performed with an exactness of one minute. Keep in mind that the language of the commands should be the same as the language of the console, otherwise the commands will be ignored. The default language is English, but can be changed.

15.9 RADIUS

The Remote Authentication Dial-In User Service (RADIUS) is referred to as a ‘triple-A’ protocol. The three ‘A’s stand for:

- Authentication
- Authorization
- Accounting

RADIUS enables you to grant users access to a network, to assign them specified rights, and to track their actions. Where necessary, the RADIUS server can also be used in the billing of user services such as WLAN hot spots. For every action performed by the user, the RADIUS server can run an authorization procedure releasing or blocking access to network resources on a per user basis.

RADIUS requires three different devices for its operation:

- Client: This is a device (PC, notebook etc.) from which the user wishes to dial in to the network.
- Authenticator: A network component positioned between network and client and which forwards on the authorization. This task can be performed by a OpenBAT Access Point, for example. The authenticator is referred to as the Network Access Server (NAS).

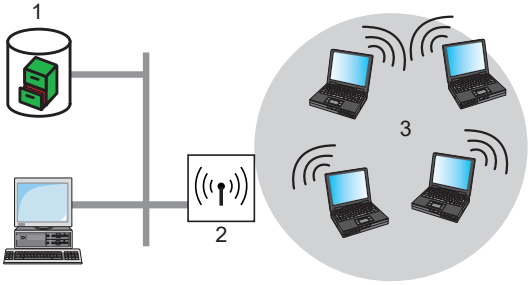


Figure 131:Remote Authentication Dial-in User Service

1: RADIUS Server
2: Authenticator
3: Clients

- Authentication server: A RADIUS server on which user data is configured. This is usually located within the same network for which it issues access authorizations. It is accessible to the client via the authenticator. Some scenarios may also allow the use of a OpenBAT access point for this task.

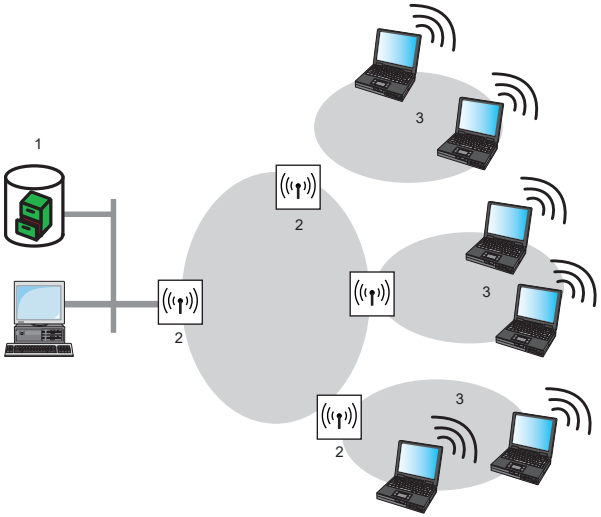


Figure 132:Authentication server

1: RADIUS Server
2: Authenticator
3: Clients

The authenticator has no initial information about the clients that want to register. This information is stored in a database on the RADIUS server. The registration information the RADIUS server needs for the authentication process is stored in the database, and can vary from network to network. The authenticator has just the one task: to transfer authentication information between the client and the RADIUS server. Access to a RADIUS server can be configured in several ways:

- Using PPP when dialing into a network (see on page 1150).
- Via WLAN (see on page 1153).
- Via the 802.1x protocol (see on page 1155).

15.9.1 How RADIUS Works

The authentication process of a client using the RADIUS server authenticator can vary in complexity, depending on the implementation. In a simplified application, the client sends its registration data to the RADIUS server via the authenticator and receives back either an ‘Accept’ or a ‘Reject’ message.

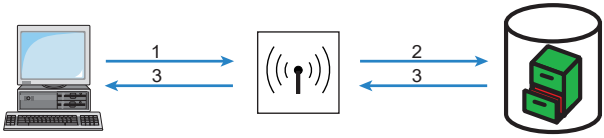


Figure 133:Simplified RADIUS application

1: User ID
2: User ID
3: Accept message

In more complicated applications, the RADIUS server can request additional registration data using what is known as a ‘Challenge’. The handshake sequence looks something like this:

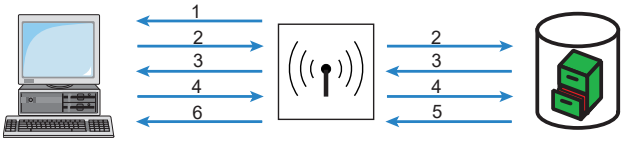


Figure 134:More complicated RADIUS application

1: Identity	4: Login data
2: User ID	5: Global key
3: Challenge	6: Session key

15.9.2 Configuring RADIUS as Authenticator or NAS

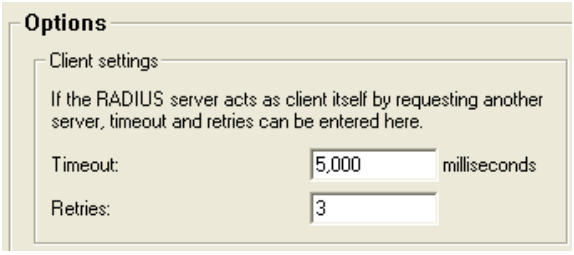
The RADIUS protocol is supported by OpenBAT devices in various application cases. For each of these cases, there is a specific set of parameters that can be configured independently of other applications. There are also general parameters that need to be configured for each of these applications. Some devices support all applications.

General Settings

General settings apply to all RADIUS client applications. Default values have been selected such that they need not usually be changed.

Perform the following steps to configure the OpenBAT device for dial-in via PPP in such a manner that the access authorization of the clients can be checked by RADIUS.

☐ Navigate to the following dialog:`Configuration : RADIUS Server : Options`.



Enter settings for the following parameters:

- Timeout:
  The number of milliseconds to wait before the next authentication attempt. Default = 5000.

  Note: With PPP authentication using RADIUS, the device dialing accepts the RADIUS timeout configured here.

- Retries:
  The number of attempts before the request is interpreted as rejected. Default = 3.

RADIUS Accounting

Accounting for a logical WLAN network can be enabled from a RADIUS server by enabling the ‘RADIUS Accounting’ option in the logical WLAN settings for the network. This can be performed at the following location:

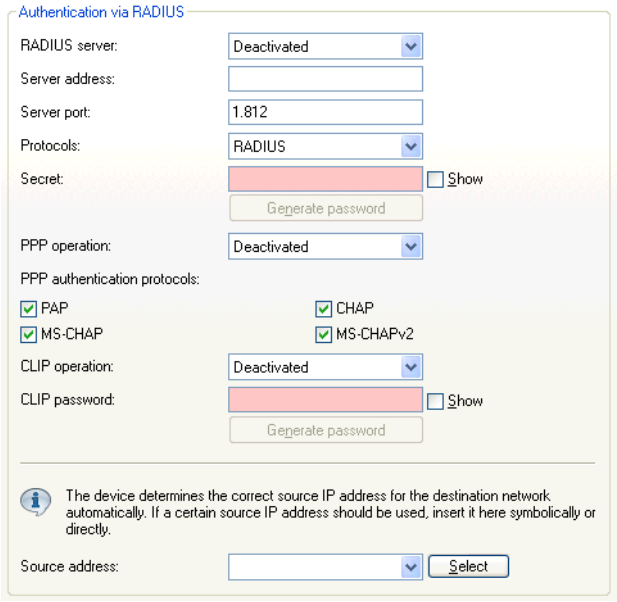
`HiLCOS Menu Tree : Setup : Interfaces : WLAN Network`

Access Checking Via PPP and RADIUS

When a client seeks to gain access using the point-to-point protocol (PPP), RADIUS can be used to check client authorizations. A client can dial in to the network from anywhere. The resulting data transmission between client and authenticator is encrypted.

Perform the following steps to configure the OpenBAT device for dial-in via PPP in such a manner that the access authorization of the clients can be checked by RADIUS.

☐ Navigate to the following dialog:`Configuration : Communication : RADIUS`.



Enter settings for the following parameters:

- RADIUS server:
  When authenticating using RADIUS, the user administration and authentication tasks are passed on to a RADIUS server. Values include:
  - Deactivated: The functionality of RADIUS is disabled and no requests are forwarded to the RADIUS server.
  - Activated: The functionality of RADIUS is enabled and requests may be forwarded to the configured RADIUS server. Depending on the setting, other sources may be used for the authentication process (e.g. PPP list).
  - Exclusive: RADIUS functionality is enabled and the authentication process is run exclusively by RADIUS.
- Server address:
  The IPv4/IPv6 address or the hostname of your RADIUS server from which users are managed centrally.
- Server port:
  The port used for communication to your RADIUS server.
- Protocols: Select ‘RADIUS”.
- Secret:
  The key to be used for coding data. The key also needs to be configured on the RADIUS server.

- PPP operation:
  A RADIUS server may be used for the authentication process when dialing-in using PPP. Settings include:
  - Deactivated: PPP clients are not authenticated using RADIUS. They are checked exclusively using the PPP list.
  - Activated: RADIUS authentication for PPP clients is enabled. User data supplied by clients is first checked using the PPP list. If no matching entry is found in the PPP list, the client is checked by the RADIUS server. Authentication is successful if the PPP list check or RADIUS server check returns as positive.
  - Exclusive: RADIUS authentication for PPP clients is enabled. User data supplied by clients is checked exclusively by the RADIUS server. In this mode, it is just the advanced settings of the PPP list for the user which are interpreted (e.g. check for PAP/CHAP – or the allowed protocols IP, IPX and/or NetBIOS).
- PPP authentication protocols:
  The security measures which apply when authenticating a remote station.
- CLIP operation:
  A RADIUS server may be used for control of a return call when dialing-in using PPP. The possible settings are:
  - Deactivated: The return call function is not controlled by RADIUS. An entry needs to appear in the name list to be used.
  - Activated: The RADIUS function for the return call is enabled. Telephone numbers reported by clients are first checked using the name list. If no matching entry is found in the name list, the telephone number is checked by the RADIUS server. If the name list check or RADIUS server check returns as positive, a return call can be established. If the telephone number communicated is in the name list, but no return call is active there, RADIUS ceases checking.
  - Exclusive: The RADIUS function for the return call is enabled. User data reported by clients is checked exclusively by the RADIUS server.

  In order to use the return call control from RADIUS, set up a user on the RADIUS server for each telephone number to be authenticated. The user name corresponds to the telephone number and the user password is the CLIP password specified here.

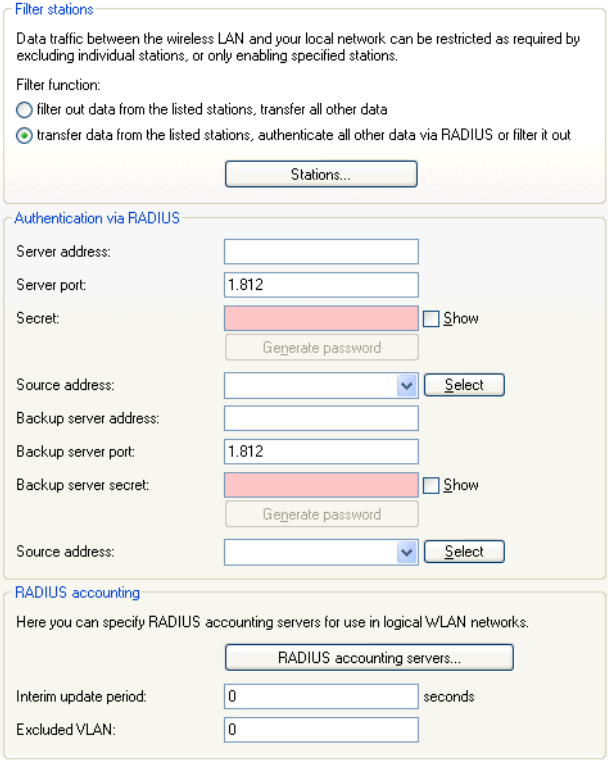
- CLIP password:
  Password for return call control. The generic values for retry and timeout also need to be configured. They are under PPP on the same screen as PPP parameters.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination address.

Access Checking via WLAN and RADIUS

When using a RADIUS server for the authentication of WLAN clients, the RADIUS server uses the MAC address to check client authorizations.

Perform the following steps to configure the OpenBAT device for dial-in via PPP in such a manner that the access authorization of the clients can be checked by RADIUS.

☐ Navigate to the following dialog:`Configuration : Wireless LAN :Stations`.



Enter settings for the following parameters:

- Filter function:
  Select the option ‘transfer data from the listed stations, authenticate all other via RADIUS or filter it out’.
- Server address:
  The IPv4/IPv6 address or the hostname of your RADIUS server from which users are managed centrally.

- Server port:
  The port used for communication to your RADIUS server.
- Secret:
  The key to be used for coding data. The key also needs to be configured on the RADIUS server.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the server IP address, which is otherwise obtained automatically for the respective destination address.
- Backup server IP address:
  The IPv4/IPv6 address or the hostname of your RADIUS server from which users are managed centrally.
- Backup server port:
  The backup port used for communication to your RADIUS server.
- Backup server secret:
  The backup key to be used for coding data. The key also needs to be configured on the RADIUS server.
- Source IP address:
  An optional source address can be configured here. This address is used instead of the source address, which is otherwise obtained automatically for the respective destination address.

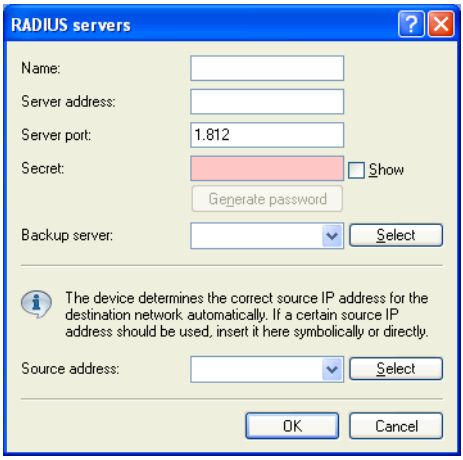
Access Checking via 802.1x and RADIUS

WLAN clients can use the 802.1x protocol for network registration. The OpenBAT device in access point mode can use this protocol to forward the log-ins to the RADIUS server. The MAC address is used for user identification.

To configure a public spot to forward data to one or more RADIUS servers:

☐ Navigate to the following dialog:`Configuration : Wireless LAN : IEEE 802.1x` and click "RADIUS server".

☐ In the ‘RADIUS server’ list, click ‘Add...’ to open the following dialog:



Enter settings for the following parameters:

- Name:
  In this table, each RADIUS server needs a unique name. The name 'DEFAULT' is reserved for WLAN networks that use an authentication process in line with IEEE 802.1x and that have not specified their own RADIUS server.

  By using the name defined in the "Key 1/passphrase" field, each WLAN network using authentication in line with IEEE 802.1x can be assigned its own RADIUS server
- Server address:
  The IPv4/IPv6 address or the hostname of your RADIUS server from which users are managed centrally.
- Server port:
  The port used for communication to your RADIUS server.
- Secret:
  The the key to be used for coding data. Configure the key also on the RADIUS server.

- Backup server:
  Name of the backup server from the list of RADIUS servers configured so far.
- Source address:
  An optional source address can be configured here. This address is used instead of the server IP address, which is otherwise obtained automatically for the respective destination address.

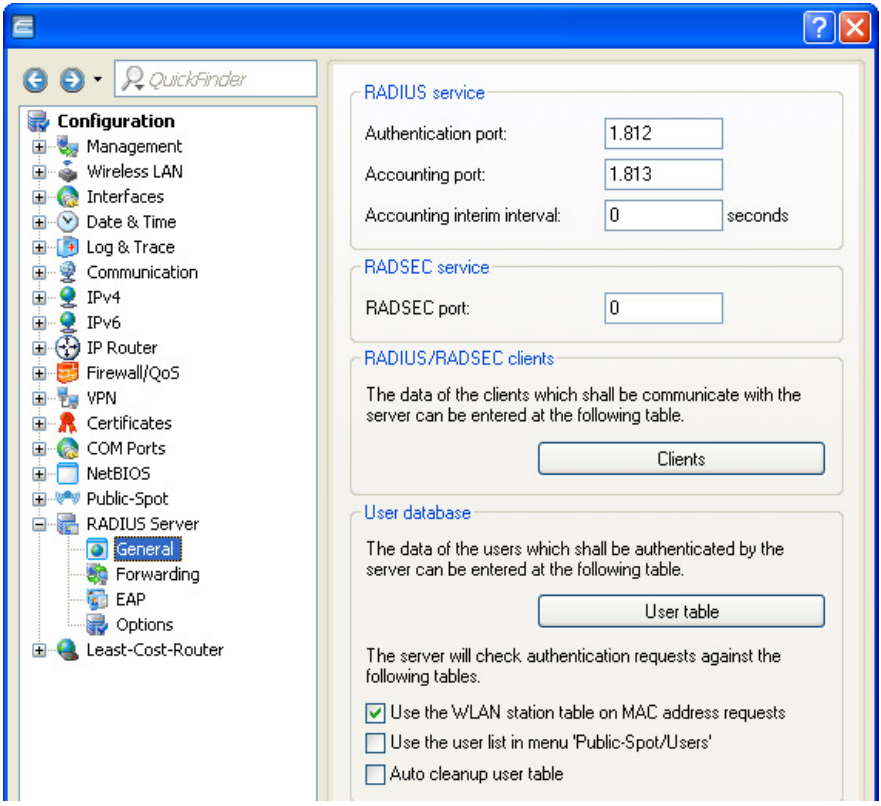
15.9.3 Configuring the RADIUS Server

In addition to its function as RADIUS authenticator or NAS, a OpenBAT device access point can also operate as a RADIUS server. When operating in this mode, information in the device on users authorized to register is made available to other access points operating in RADIUS authenticator mode.

General Settings

To configure the RADIUS Server, define the authenticator that may access the RADIUS server, the passphrase it needs for this access and the open port through which it can communicate with the RADIUS server. The authentication port applies globally to all authenticator instances. To enter general RADIUS server settings, do the following:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : General`.



Enter settings for the following parameters:

- Authentication port:
  The TCP port used by the authenticators to communicate with the RADIUS server in the OpenBAT access point. Port '1812' is normally used. Port '0' disables the RADIUS server.
- Accounting port:
  The RADIUS server TCP port for receiving accounting information. Port '1813' is normally used.
- Accounting interim interval:
  The update frequency (in seconds) of accounting data sent to the RADIUS server.
- RADSEC port:
  The TCP port for transferring RADSEC encrypted accounting- or authentication requests to the server. Port '2083' is normally used. Port '0' deactivates the RADSEC service (see on page 1174).
- Use the WLAN station table on MAC address requests:
  Self-explanatory.
- Use the user list in menu 'Public-Spot/Users':
  Compatibility setting for the Public Spot module. If you enable this setting, the RADIUS server also refers to the Public Spot's internal user list.

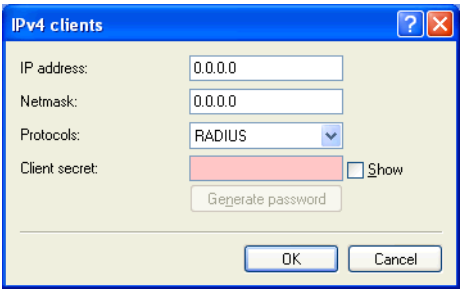
  Note: During technical development, this list was replaced as of HiLCOS 7.70 by the user administration via RADIUS. Also see the information in the chapter on creating Public Spot users, page 456 „Manual set up and management“.
- Auto cleanup user table:
  Expired user accounts will be deleted automatically if this option is enabled. Auto cleanup will work both for accounts with either absolute or relative expiry. Relative account expiry and time or volume budgets work provided that the device is both the authentication and the accounting server.

Adding Clients

The client table can contain up to 16 clients that can communicate with the RADIUS server. To add clients:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : General` and click "IPv4 Clients".

☐ In the ‘Clients’ window, click ‘Add...’ to open the ‘New Entry’ dialog:

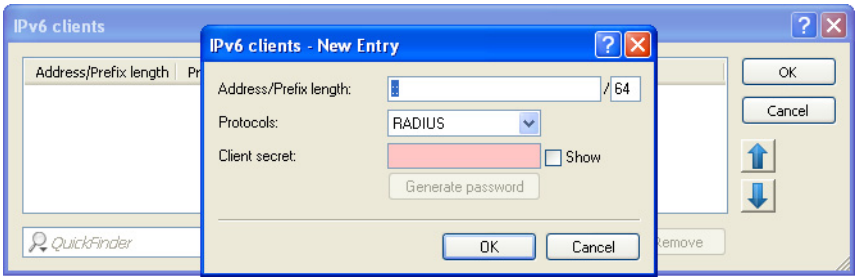


For each new RADIUS client, configure the following parameters:

- IP address:
  The IP network—i.e., the range of client IP addresses—to which the defined password applies.
- Netmask: The IP network mask of the clients.
- Protocols:
  Select the protocol to be used to communicate between the RADIUS server and clients: RADIUS, RADSEC, or All.
- Client secret: The client password.

Accessing the RADIUS server via IPv6

As of HiLCOS 8.90, the RADIUS server is also accessible for IPv6 clients. You can configure these clients in LANconfig under `RADIUS server : General` by clicking on "IPv6 clients".



The following values are entered for each client:

☐ **Address/prefix length**

IP address (or address range) of the clients for which the password entered in this dialog applies.

Important: To use an address, the prefix length must be 128 bits. The entry "fd00::/64", for example, permits access to the entire network, the entry "fd00::1/128" only permits exactly one client.

☐ **Protocols**

Protocol for communication between the internal server and the clients.

☐ **Client secret**

Password required by the clients for access to the internal server.

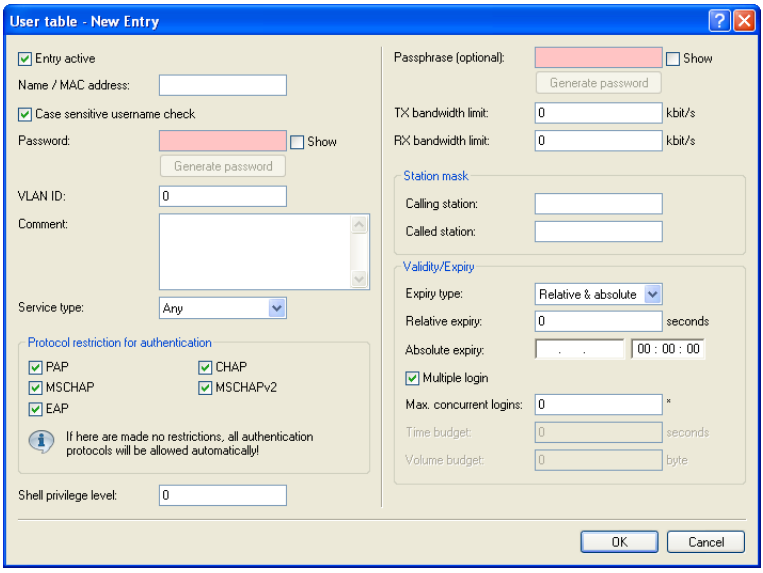
Note: In order for IPv6 clients to access the RADIUS server, a corresponding inbound rule must be entered in the IPv6 firewall, if necessary.

Adding Users

Up to 64 users can be entered into the user table, and these can be authenticated by the RADIUS server without reference to other databases. This user table is used for local requests to the RADIUS server, i.e. for requests with user name but no realm. To add users:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : General` and click "User table".

☐ In the ‘User table’, click ‘Add...’ to open the ‘New Entry’ dialog:



For each new RADDIUS client, configure the following parameters:

- Entry active:
  Option to enable or disable individual RADIUS user accounts. In this way, you can temporarily disable individual user accounts without deleting the account entirely
- Name / MAC address:
  The user name.
- Please note that the user name is case-sensitive:
  You can specify whether the RADIUS server should carry out a case-sensitive user name check.

- Password:
  The user password.
- VLAN ID:
  Using this option, each user can be assigned a specific VLAN ID on successful authentication. The value '0' indicates no VLAN ID will be assigned.
- Comment:
  Here you can enter an arbitrary comment.
- Service type: The types of service this account may be used for:
  – Any
  – Framed
  – Login
  – Authorization only
  Depending on the device, the number of entries with ‘Any’ or’ Login’ service type may be limited.
- Protocol restriction for authentication:
  Select one or more authentication methods to be applied to the user. If you do not select a restriction, all methods are allowed automatically.
- Shell privilege level
  This field contains a vendor-specific RADIUS attribute to communicate the privilege level of the user in a RADIUS-Accept.
- Passphrase:
  You can optionally specify a custom passphrase with at least 8 characters for any physical (MAC) address used in networks secured using 802.11i/WPA/AES-PSK.
  If no custom passphrase is specified, the device authenticates this MAC address with the passphrase stored for each logical WLAN under `Configuration: Management : 802.11i/WEP`.

  Note: This field has no significance for networks secured by WEP.

- TX bandwidth limit:
  To restrict the uplink for the corresponding user account, enter a value larger than `0` here. The value `0` stands for "unlimited".

  Note: The bandwidth limitation for sending applies regardless of the interface used (LAN and WLAN).

- RX bandwidth limit:
  To restrict the downlink for the corresponding user account, enter a value larger than `0` here. The value `0` stands for "unlimited".

  Note: The bandwidth limitation for receiving applies regardless of the interface used (LAN and WLAN).

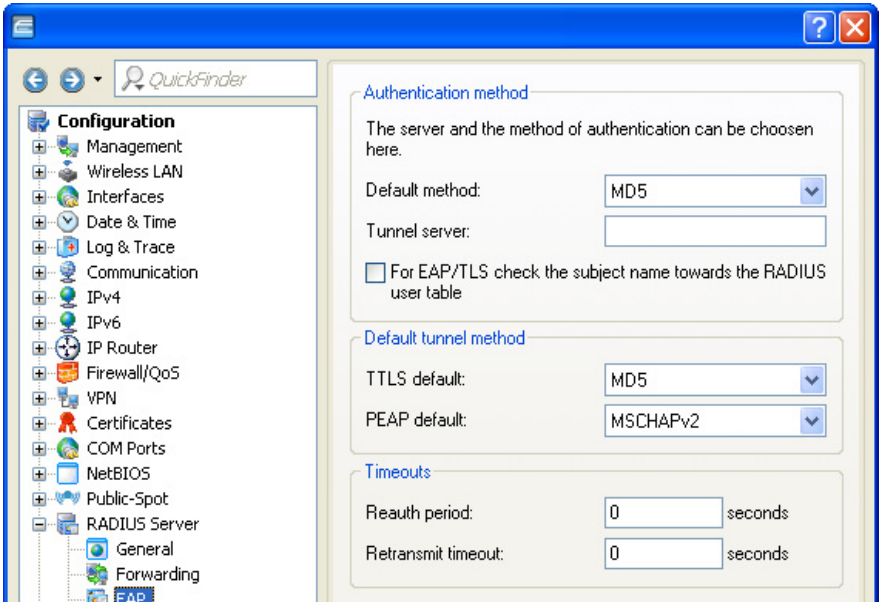
- Calling station mask:
  This mask restricts entries to particular IDs that are transmitted by the calling station (WLAN client). On authentication via 802.1x the MAC address of the calling station is provided in ASCII format (in capital letters), where character pairs are divided by hyphens (e.g. '00-10-A4-23-19-C0'). Using an * as placeholder, whole groups of IDs can be defined (e.g. '00-10-A4-*').
- Called station mask:
  This mask restricts entries to particular IDs that are transmitted by the called station (BSSID and SSID of the access point). On authentication via 802.1x MAC addresses of the called stations are transmitted in ASCII format (in capital letters), where character pairs are divided by hyphens. The SSID is added following a colon as separation mark (e.g. '00-10-A4-23-19-C0:AP1'). Using an * as placeholder whole groups of IDs can be collected and defined as a mask. For example, the mask '*:AP1' defines an entry which applies for a client in the radio cell which is named 'AP1', independent from the access point it is registered to. Thus, the client can roam from one access point to another, keeping its authentication data.
- Expiry type:
  A point in time when validity of this account shall end. There are two types of limited validity, which may be selected independently, or together:
  – Relative: The validity of the account ends at a set amount of time after the first successful login.
  – Absolute: The validity of the account ends at a fixed point in time.
  – Never: The validity of the account does not end.
- Relative expiry:
  The relative amount of time, in seconds, until the account expires.
- Absolute expiry:
  The specific time and date when the account expires.

- Multiple login:
  Select this to permit more than one parallel session with the same user ID. If de-selected, the device rejects an authentication request for the given user ID if there is an ongoing session in the active session accounting table for this user. De-selecting this option is often a prerequisite for a reasonable enforcement of time and volume budgets.
- Max. concurrent logins:
  If multiple login is enabled, this field is used to specify the maximum number of parallel sessions allowed. The value `0` stands for "unlimited".
- Time budget:
  This setting set a maximum amount of time (in seconds) that may be consumed via this user account before access is denied. The time budget setting should be used exclusively if the device is both the authentication server and the accounting server. This selection is available on if Multiple login is de-selected.
- Volume budget:
  The maximum amount of bytes that may be transmitted by this user account before access is denied. This selection is available on if Multiple login is de-selected.

EAP Authentication

EAP operates as a framework for various authentication methods. Authentication methods cannot be suppressed. The EAP supplicant and the RADIUS server negotiate the EAP method with the standard EAP mechanism. Clients requesting a non-EAP method will be rejected by the RADIUS server. To configure EAP:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : EAP`.



For each new RADIUS client, configure the following parameters:

- Default method:
  Select the method by which the RADIUS server should offer a client outside a TTLS/PEAP tunnel:
  - MD5: Defined in RFC 2284, EAP/MD5 is a simple challenge/response protocol. It does not cater for mutual authentication nor does it offer a dynamic key such as those required for 802.1x authentication in wireless networks (WLANs). Thus it is used exclusively for the authentication of non-wireless clients or as a tunneled method as a part of TTLS.
  - GTC: (generic token card) Defined in RFC 2284 and RFC 3748, this protocol employs a text challenge from the authentication server, and a security token reply. Provides for the use of a one-time password.
  - MSCHAPv2: Defined in draft-kamath-pppext-eap-mschapv2-01.txt. As opposed to EAD/MD5, EAP/MSCHAPv2 supports mutual authentication but does not support dynamic keys, making it just as prone to dictionary attacks as EAP/MD5. This method is usually used within PEAP tunnels.
  - TLS: Defined in RFC2716. The use of EAP/TLS requires the use of a root certificate, a device certificate and a private key in the device. EAP/TLS provides enhanced security and the dynamic keys necessary for wireless connections; its implementation is complex, however, because each individual client requires a certificate and a private key.
  - TTLS,: Defined in draft-ietf-pppext-eap-ttls-05.txt. TTLS is based on TLS; it ignores client certificates and it utilizes the existing TLS tunnel to authenticate the client. The RADIUS server supports the following TTLS methods: PAP, CHAP, MSCHAP, MSCHAPv2, and EAP.
  - PEAP: Defined in draft-kamath-pppext-peapv0-00.txt. Similar to TTLS, PEAP is based on TLS and works with an EAP negotiation inside the TLS tunnel.

- Tunnel server:
  To handle tunneled EAP requests for TTLS and PEAP, enter an account listed in the forwarding table. Select a realm that does not conflict with other used realms. If left empty, the local RADIUS server forwards requests to itself, meaning that both the outer and inner EAP phases are handled by the local RADIUS server.
- For EAP/TLS check the subject name towards thr RADIUS user table:
  For TLS, the client only uses its certificate for authentication. If this is selected, the RADIUS server additionally checks to see if the certificate username is enclosed in the RADIUS user table.
- TTLS default / PEAP default:
  When using TLS or PEAP, two authentication methods are negotiated. Initially, a secure TLS tunnel is negotiated via EAP. Within this tunnel, a second authentication method is negotiated. In this negotiation, the server respectively offers a method to be accepted (ACK) or rejected (NAK) by the client. If the client rejects, it sends a proposal containing a method which it would prefer to use. If the suggested method is allowed by the server, it will be used. Otherwise the negotiation is aborted by the server. This parameter sets the method to be offered by the server for authenticating clients within TLS tunnels.
- Reauth period:
  If the internal RADIUS server answers CHALLENGE to a client request (authentication method negotiation not yet finished), the RADIUS server can notify the authenticator, how long (in seconds) it has to wait for a client answer before CHALLENGE will be sent anew. Value '0' deactivates the timeout for the authenticator.
- Retransmit timeout:
  If the internal RADIUS server answers ACCEPT to a client request (authentication method negotiation successfully finished), the RADIUS server can notify the authenticator, after which time (in seconds) it should do a re-authentication of the client. Value '0' deactivates the timeout for the authenticator.

As of HiLCOS 8.90 the RADIUS server contains an EAP-SIM module, which enhances the device with the ability to simulate the home location register (HLR) of a mobile provider. An HLR usually generates the keys for registered SIM cards so that a RADIUS server can authenticate a client by means of EAP-SIM.

The required keys can be manually configured and stored on the RADIUS server, which makes an HLR unnecessary. An example where EAP-SIM is used is 802.11u.

RADIUS Forwarding

In the case of multi-layer EAP protocols such as TTLS or PEAP, the actual internal authentication can be carried out by a separate RADIUS server. Thus, an existing RADIUS server can continue to be operated to provide user tables, even though it is not EAP(/TLS) capable itself. In this situation the TLS/TTLS/PEAP tunnel is managed from the RADIUS server. The configuration of multi-layer protocols of this type is an element of a general method for the forwarding of RADIUS requests, whereby a RADIUS server can also be used as a RADIUS proxy. The concept of ‘realms’ is the basis for request forwarding and the proxy function. A realm is a character string which defines the validity of a range of user accounts. Once defined, the realm is a suffix to the user name separated by an @ character as follows:

user@realm

The realm can be seen as a pointer to the RADIUS server where the user account is managed. The realm is removed from the string prior to the search of the RADIUS server's user table. Realms allow entire networks which are mutually trustworthy to work with common RADIUS servers located in partner networks, and to authenticate users who move between these networks. The RADIUS server stores any connected RADIUS servers along with their associated realms in a forwarding table. The realm is searched for in this table in connection with the communicated user name. If no entry is found, the request is answered with an access reject. An empty realm is treated as a local request, i.e. the RADIUS server searches its own user tables and generates its response accordingly.

To support the processing of realms the RADIUS server uses two special realms:

- Default realm: This realm is used where a realm is communicated for which no specific forwarding server has been defined. Significantly, a corresponding entry for the default realm itself needs to be present in the forwarding table.
- Empty realm: This realm is used when no realm is communicated, just the user name.

In the default state the forwarding table is empty, i.e. the default and empty realms are empty. This means that all requests are treated as local requests and any realms that are communicated are ignored. To operate the RADIUS server purely as a forwarding server or RADIUS proxy, set the default and empty realms to a value that corresponds to a server defined in the forwarding table.

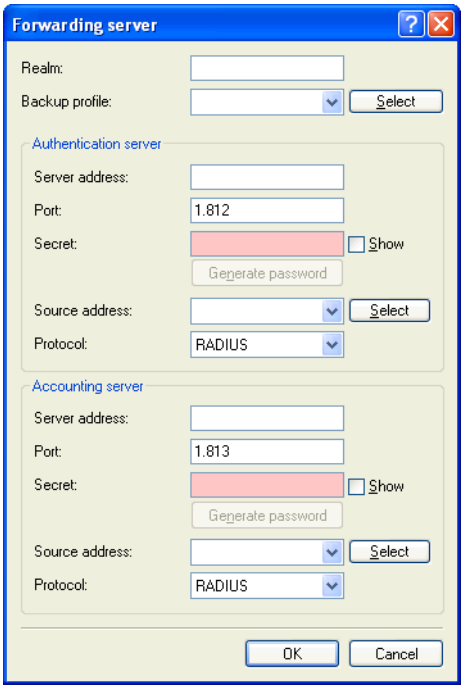
The forwarding of RADIUS requests does not alter the user name. No realm is added, changed or removed. The next server may not be the last one in the forwarding chain, and the realm information may be required by that server so that forwarding is carried out correctly. The active RADIUS server that processes the request resolves the realm from the user name, and subsequently a search is made of the table containing the user accounts. Accordingly the RADIUS server resolves the realm from the user name for processing requests locally.

The processing of tunneled EAP requests using TTLS and PEAP makes use of a special EAP tunnel server, which is also in the form of a realm. Here you select a realm that will not conflict with other realms. If no EAP tunnel server is defined then the RADIUS server forwards the request to itself, meaning that both the internal and the external EAP authentications are handled by the RADIUS server itself.

To configure RADIUS forwarding, create a list of forwarding servers, and define realms for this device, as follows:

☐ Navigate to the following dialog:`Configuration : RADIUS Server : Forwarding` and click "Forwarding server".

☐ In the ‘Forwarding server’ table, click ‘Add...’ to open the ‘New Entry’ dialog:



For each new forwarding server entry, configure the following parameters:

- Realm: Enter a string that defines the validity range of user accounts.
- Backup profile:
  Use this item to select the profile of an alternative forwarding server. Requests are forwarded to this server if the configured forwarding server is unavailable (see page 482 „Chaining of backup servers“).
- Server address:
  Enter the IPv4/IPv6 address or the hostname of the RADIUS Authentication server and/or the RADIUS accounting server you use for central user administration and/or central accounting.
- Port:
  Enter the port of the respective RADIUS server.
- Secret:
  Enter the key to be used as a Shared Secret.

- Source IP address:
  You have the option to enter a different address here (name or IP) to which the respective RADIUS server sends its reply message.
  By default, the server sends its replies back to the IP address of your device without having to enter it here. By entering an optional loopback address you change the source address and route used by the device to connect to the server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.
- Protocol:
  Select the protocol for communication between the internal RADIUS server and the forwarding server: RADIUS or RADSEC.

Next, in the `Configuration : RADIUS Server : Forwarding` dialog, configure the following local RADIUS server parameters:

- ☐ Default-Realm: Enter the name of a realm that will be used if a realm is communicated for which no specific forwarding server has been defined. This realm needs to appear in the 'Forwarding server' table.
- ☐ Empty-Realm: Enter the name of the realm that will be used when no realm, just a user name, is communicated. This realm needs to appear in the 'Forwarding server' table.

WLAN Access List as a Basis for RADIUS Information

512 WLAN clients, that are able to register with the OpenBAT access point, may be entered in the access list. When operating in RADIUS server mode, this list can also be used to check on RADIUS clients that attempt to register at other access points. In an installation that includes several access points, this allows client access authorizations to be centrally maintained. The following settings for this configuration can be accessed at:

`HiLCOS menu tree : Setup : WLAN : RADIUS-Access-Check`

The following parameters can be configured for this purpose:

- **Provide server database:**
  This parameter specifies whether the WLAN access list is to be used as an information source for the RADIUS server in the OpenBAT access point. The WLAN access list contains the user name in the form of the MAC address and the password ('WPA passphrase'). In addition to this access data, the access list provides information such as bandwidth restriction and association to a specific VLAN.
- **Recheck cycle:**
  Enter a period, in minutes, to enable periodic checking of the client activity status. After a WLAN client is authenticated and logged on by RADIUS, it remains active until it logs off itself or is logged off by the RADIUS server. When you enter a value in this field, the RADIUS server periodically checks—at the specified period—whether the WLAN clients logged in are still in the access list. If a WLAN client is removed from the access list, it remains logged in to the WLAN up to the point when the recheck cycle runs again.

WPA Passphrase in the RADIUS Server User Table

The configuration of LEPS merely involves the assignment of an individual passphrase to the MAC address of each client that is approved for the WLAN. To this end, the MAC filter is set to positive, i.e. the data from clients entered here will be transmitted.

Note: The passphrases should consist of a random string at least 32 characters long.

The client-specific passphrase is stored in the RADIUS server's user table. This enables a device which is connected to the LAN to operate as a central RADIUS server and use the benefits of LEPS.

`HiLCOS Menu Tree:Setup:RADIUS:Server:Users:WPA passphrase`

15.10RADSEC

RADSEC is an alternative protocol that transmits RADIUS packets through a TLS-encrypted tunnel. TLS is based on TCP, thus providing a proven mechanism for monitoring packet loss. Furthermore, TLS is highly secure and it features a method of mutual authentication by means of X.509 certificates.

15.10.1Configuring RADSEC in the OpenBAT device

The OpenBAT device as RADIUS client.

To function as a RADIUS client, a OpenBAT device is set up to use RADIUS via UDP or RADSEC via TCP with TLS. Additionally set the port to be used. 1812 for authentication with RADIUS, 1813 for accounting with RADIUS, and 2083 for RADSEC.

These settings are made at all locations in the WEBconfig software where a OpenBAT device is configured as a RADIUS client, including:

`HiLCOS Menu Tree : Setup : WLAN : RADIUS`

and

`HiLCOS Menu Tree : Setup : WLAN : RADIUS Access Check`

and

`HiLCOS Menu Tree : Setup : WLAN : RADIUS Accounting`

and

`HiLCOS Menu Tree : Setup : IEEE802.1x : RADIUS Server`

The OpenBAT device as RADIUS server.

If a OpenBAT device operates as a RADIUS server, you can configure the RADSEC port for receiving RASDSEC logins. In addition to that, the protocol to be used (RADIUS, RADSEC or all) can be set for each of the RADIUS clients in the client list. This allows, for example, RADIUS to be used for LAN-based clients and the more robust RADSEC via TCP to be used for registrations arriving over the Internet.

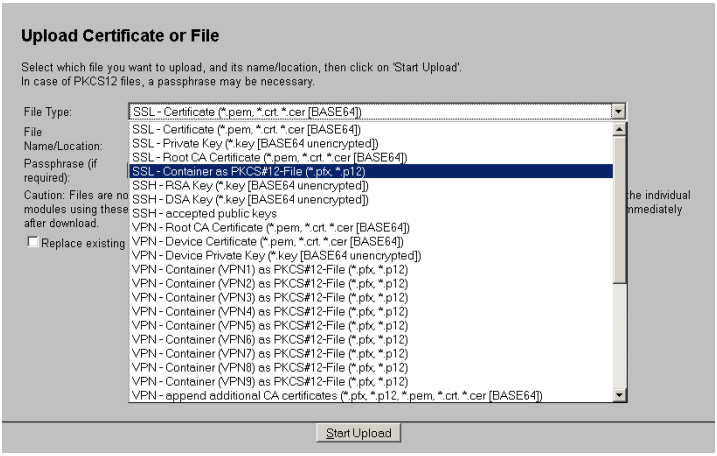
You can access and configure the ‘RADSEC port’ setting in LANconfig at:

☐ `Configuration : RADIUS Server : General`

15.10.2Certificates for RADSEC

Separate X.509 certificates are required for TLS encryption of the RADSEC connection. The individual certificates (root certificate, devices certificate and private key) can be uploaded to the device individually or as a PKCS#12 container. This can be done at:

`File Management : Upload Certificate or File`


Upload Certificate or File
Select which file you want to upload, and its name/location, then click on 'Start Upload'.
In case of PKCS12 files, a passphrase may be necessary.
File Type:
File Name/Location:
Passphrase (if required):
Caution: Files are no modules using these after download.
Replace existing
SSL - Certificate (*.pem, *.crt, *.cer [BASE64])
SSL - Private Key (*.key [BASE64 unencrypted])
SSL - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
SSL - Container as PKCS#12-File (*.pfx, *.p12)
SSH - RSA Key (*.key [BASE64 unencrypted])
SSH - DSA Key (*.key [BASE64 unencrypted])
SSH - accepted public keys
VPN - Root CA Certificate (*.pem, *.crt, *.cer [BASE64])
VPN - Device Certificate (*.pem, *.crt, *.cer [BASE64])
VPN - Device Private Key (*.key [BASE64 unencrypted])
VPN - Container (VPN1) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN2) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN3) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN4) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN5) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN6) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN7) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN8) as PKCS#12-File (*.pfx, *.p12)
VPN - Container (VPN9) as PKCS#12-File (*.pfx, *.p12)
VPN - append additional CA certificates (*.pfx, *.p12, *.pem, *.crt, *.cer [BASE64])
the individual
mmediately
Start Upload

15.11TACACS+

15.11.1Introduction

TACACS+ (Terminal Access Controller Access-Control System Plus) is a protocol for authentication, authorization and accounting (AAA). It provides access to the network for authorized users, it regulates the rights of those users, and it is a logging mechanism to keep track of user actions. TACACS+ is an alternative to other AAA protocols such as RADIUS.

Note: Use TACACS+ in order to meet PCI (Payment Card Industry) compliance requirements.

Modern networks with their numerous types of service and network components present a challenge in terms of controlling access rights for the user. In large installations in particular, the overhead would be enormous to keep user data consistent on all devices or for all services. For this reason, user data should be managed on a central server.

As a simple example, a user wishes to register at a router and sends the corresponding login details (user ID) to it. In this case the router functions as a Network Access Server (NAS)—it does not check the user data itself; rather, the data is forwarded to the central AAA server, which responds by checking the data and answering with an „accept“ or a „reject“.

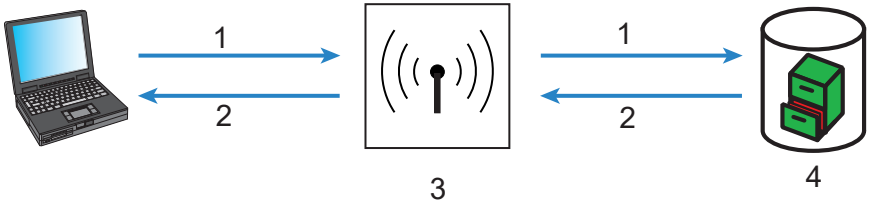


Figure 135:TACACS+ Network

1: User ID	3: NAS
2: Accept	4: AAA server

The advanced TACACS+ functions include, the option of requesting that users change their passwords after logging in for the first time, or if the password has expired. The corresponding messages are sent from the NAS to the user.

Note: LANconfig cannot process all of the messages in the extended login dialog. If LANconfig rejects a login attempt at a OpenBAT device even if the correct data is entered, use an alternative method of configuration (such as WEBconfig or Telnet).

TACACS+ is an alternative AAA server to RADIUS servers. The following table shows some of the major differences between RADIUS and TACACS+:

TACACS+	RADIUS
Connection-orientated data transfer via TCP	Connectionless data transfer via UDP
Fully encrypted data transfer	Password is encrypted, other content remains unencrypted
Complete separation of authentication, authorization and accounting possible	Authentication and authorization combined

- TCP-based communication with TACACS+ is more reliable with RADIUS. Communications between the NAS and AAA server are confirmed, so the NAS is informed if the AAA server is unavailable.
- TACACS+ encrypts the entire data payload (except for the TACACS+ header). This helps provide for the confidentiality of information such as user names or the permitted services. TACACS+ encryption works with a one-time pad based on MD5 hashes.
- The separation of the three AAA functions enables TACACS+ to operate with multiple servers. RADIUS combines authentication and authorization, TACACS+ allows these to be separated. In this way, for example, TACACS+ servers can be employed for authentication exclusively.

Note: Kindly note: Even if TACACS+ is used to centrally manage user accounts on an AAA server, you should by all means set a secure password for root access to the OpenBAT device. If no root password is set, access to the device configuration can be blocked to preserve security if no connection is available to the TACACS+ server. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

15.11.2Configuring TACACS+

The parameters for configuring TACACS+ can be accessed at:

`HiLCOS Menu Tree : Setup : TACACS+`

The following parameters can be configured:

- Accounting:
  Activates or deactivates accounting via TACACS+ server. If TACACS+ accounting is activated, all accounting data is transmitted via TACACS+ protocol to the configured TACACS+ server. Default = Deactivated.

  Note: TACACS+ accounting will activate provided the defined TACACS+ server is available.

- Authentication:
  Activates or deactivates authentication via TACACS+ server. If TACACS+ authentication is activated, all authentication data is transmitted via TACACS+ protocol to the configured TACACS+ server. Default = Deactivated.

  Note: TACACS+ authentication will activate only if an accessible TACACS+ server is defined. Fallback to local users is possible if a root password has been set for the OpenBAT device. Fallback to local users must be deactivated for devices without a root password, because otherwise access to the OpenBAT device without a password would be possible in case of a network failure (TACACS+ server not available).

- Authorization:
  Activates or deactivates authorization via TACACS+ server. If TACACS+ authorization is activated, all authorization data is transmitted via TACACS+ protocol to the configured TACACS+ server. Default = Deactivated.

  Note: TACACS+ authorization will activate provided the defined TACACS+ server is available. If TACACS+ authorization is activated, the TACACS+ server will be queried for authorization each time a user enters a command. Data traffic during configuration will increase correspondingly. Also, the user rights need to be defined in the TACACS+ server.

- Fallback to local users:
  If the defined TACACS+ server is unavailable, it is possible to fall back to local user accounts on the OpenBAT device. This allows for access to the device even if the TACACS+ connection is lost, e.g. when deactivating the usage of TACACS+ or for correcting the configuration. Default = Allowed.

Note: The fallback to local user accounts presents a security vulnerability if no root password is set for the OpenBAT device. For this reason, TACACS+ authentication with fallback to local user accounts can only be activated if a root password has been set. If no root password is set, access to the device configuration can be blocked for security reasons if a connection to the TACACS+ servers is unavailable. In this case, the device may have to be reset to its factory settings in order to regain access to the configuration.

- Shared secret:
  The password for encrypting the communications between NAS and TACACS+ servers, up to 31 alphanumeric characters.
- SNMP GET requests accounting:
  Numerous network management tools use SNMP for requesting information from network devices. LANmonitor also uses SNMP to access the OpenBAT device to display information about current connections, etc., or to execute actions such as disconnecting a connection. Since a device can also be configured via SNMP, TACACS+ evaluates these accesses as events that require authorization. Since LANmonitor regularly queries these values, a large number of unnecessary TACACS+ connections would be established. If authentication, authorization and accounting by TACACS+ are activated, then each request will initiate three sessions with the TACACS+ server.

  This parameter allows the regulation of the behavior of OpenBAT devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for accounting. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally.

  Note: Entering a read-only community enables authentication by TACACS+ to be deactivated for LANmonitor. The read-only community defined here is then entered into LANmonitor as a user name.

Values include:

- only_for_SETUP_tree (default): In this setting, accounting via the TACACS+ server is only required for SNMP access to the setup branch of HiLCOS.
- All: Accounting by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
- **None:**
  Accounting by TACACS+ server will not be carried out for SNMP accesses.

- SNMP GET requests authorization:
  This parameter allows the regulation of the behavior of OpenBAT devices with regard to SNMP access in order to reduce the number of TACACS+ sessions required for authorization. Authentication via the TACACS+ server remains necessary if authentication for TACACS+ is activated generally. Possible values:
  - only_for_SETUP_tree (default): In this setting, authorization via the TACACS+ server is only required for SNMP access to the setup branch of HiLCOS.
  - All: Authorization by TACACS+ server will be carried out for every SNMP access. In case of regular request for status information, for example, the load on the TACACS+ server will increase significantly.
  - None: Authorization by TACACS+ server will not be carried out for SNMP accesses.
- Bypass TACACS for CRON/scripts/action table:
  Select this to bypass TACACS+ for actions initiated by the CRON-Jobs table, the Action table, or configuration scripts. When selected, the OpenBAT device does not provide authorization or accounting messages for these actions.
- Encryption:
  Activates or deactivates the encryption of communications between NAS and TACACS+ servers. Default = Deactivated.

Note: For security reasons, operate TACACS+ with encryption. If encryption is activated here, the password for encryption entered here needs to match the password on the TACACS+ server.

- Include value into authorization request:
  Select this to require that both the configuration path and the parameter value need to be authorized by the TACACS+ Server, as in the following example:
  ```
  set /Setup/SNMP/Comment-1 "test"
  ```
  If this setting is de-selected, only the path needs to be authorized for the user, as in the following example:
  ```
  set /setup/SNMP/
  ```

15.11.3 Configuring the TACACS+ Server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one ceases to operate. When logging in via telnet or WEBconfig, the user can select the server to be used.

The parameters for configuring the TACACS+ server can be accessed at:

```
HiLCOS Menu Tree : Setup : TACACS+ : Server
```

The following parameters can be configured:

- Server address:
  Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded. Values include any valid DNS resolvable name or valid IP address.
- Loopback address: (Optional)
  You can configure a loopback address here. Possible values include:
  – Name of the IP networks whose addresses are to be used
  – ‘INT’ for the address of the first intranet.
  – ‘DMZ’ for the address of the first DMZ

- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

- Compatibility mode:
  Activated or deactivated. TACACS+ servers are available as open-source or commercial versions, each of which works with different messages. The compatibility mode enables the processing of messages from free TACACS+ servers. Default = Deactivated.

15.11.4Login to the TACACS+ Server

After TACACS+ has been activated for authentication and/or authorization, all logins to the device are redirected to the TACACS+ server. The remaining login procedure differs according to the access method.

TACACS+ Login via LANconfig

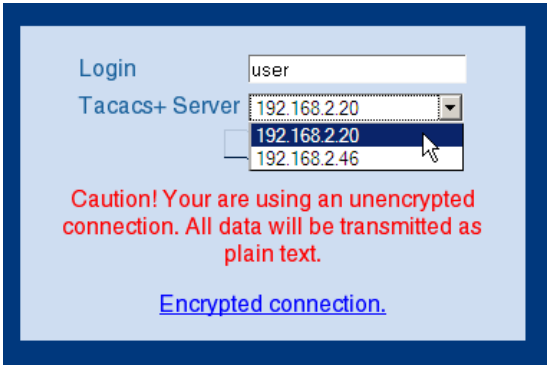
Using LANconfig to log in to a device with activated TACACS+ authentication requires the user named ‘root’. Correspondingly, the user ‘root’ needs to be configured on the TACACS+ server. To log in via LANconfig, enter the password as configured for the user ‘root’ on the TACACS+ server.

Note:

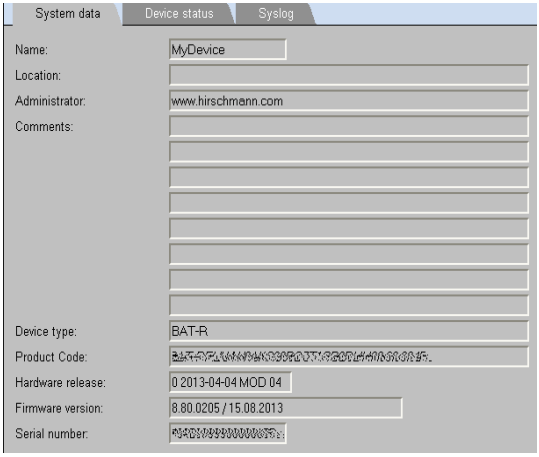
- After it is authenticated by TACACS+, ‘root’ is the sole user automatically assigned with full supervisor rights, and thus able to edit the configuration without having to change privilege level. When authorization is in use, the TACACS+ server decides whether this is allowed or not.
- If authorization is activated for the device as well as authentication, the TACACS+ server needs to permit the commands ‘readconfig’ and ‘writeconfig’ for the user ‘root’ in order for the user to read the configuration from the device and to upload any changes (see on page 1188).

TACACS+ Login via WEBconfig

Using WEBconfig to log in to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server. When logging in with WEBconfig, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication:



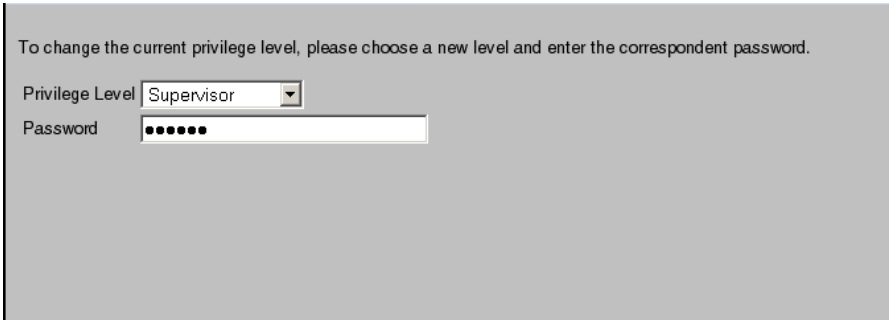
The corresponding password is requested in the following dialog. After logging in, the user initially sees a reduced WEBconfig user interface. If authorization is not being used, all WEBconfig users (except for the user ‘root’) initially have read rights exclusively.



To gain further rights, on the left of the screen click the following command:

`Change privilege level`

The following dialog opens where you can select the desired user rights and enter the corresponding password:

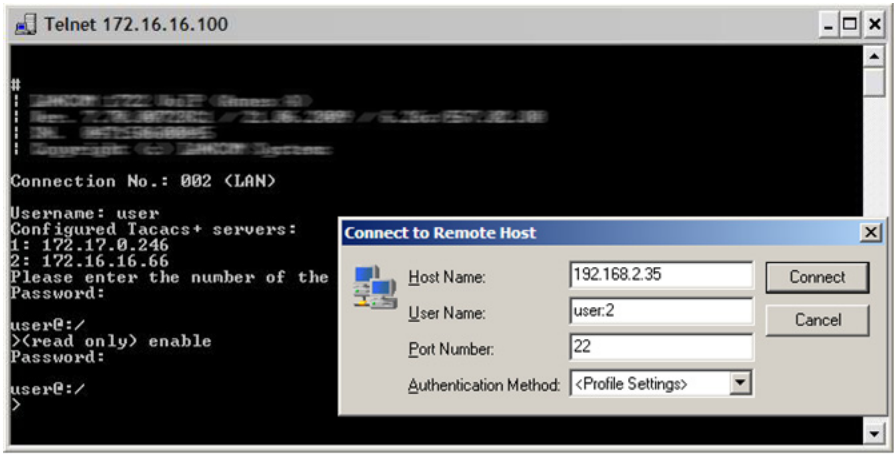


Note:

- The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.
- If authorization is activated for the device as well as authentication, the TACACS+ server needs to permit the assigned commands for each user in order for the user to read and edit the device configuration (see on page 1188).

15.11.5TACACS+ Login via Telnet or SSH

Using Telnet or SSH to log in to a device with activated TACACS+ authentication is possible for any user configured on the TACACS+ server. When logging in with Telnet, enter the user name configured on the TACACS+ server and select the server which is to carry out authentication. When logging in with SSH, enter the user name followed by a colon and then the server name, i.e. "user:1" or "user:2".



After login, all users initially have read-only rights exclusively (except for the user ‘root’). To gain further rights, enter the command enable and enter the password. Rights will be assigned according to configuration for that password. The parameters for the enable command are the numbers 1-15. 1 is the lowest level, 15 the highest. If no parameter is entered, 15 is taken automatically.

Note:

- The passwords for individual user rights are configured as "enable" passwords in the TACACS+ server.
- If authorization is activated for the device as well as authentication, the TACACS+ server needs to permit the assigned commands for each user in order for the user to read and edit the device configuration (see on page 1188).

15.11.6 Assigning Rights Under TACACS+

TACACS+ uses privilege levels to separate users into different groups. For the local authorization of users via the 'enable' command under telnet/SSH or via privilege levels under WEBconfig, the various administrator rights are mapped to the TACACS+ privilege levels:

TACACS+ level	Administrator rights
0	No rights
1	Read only
3	Read-write
5	Read-only limited admin
7	Read-write limited admin
9	Read only admin
11	Read-write admin
15	Supervisor (root)

15.11.7 Authorization Functions

If authorization is activated for the device as well as authentication, the TACACS+ server needs to permit the corresponding functions for the user. Enter the required values into the user configuration on the TACACS+ server.

LANconfig

Command	Argument	Comment
readconfig	None	Read out the entire configuration
writeconfig	None	Write the entire configuration

WEBconfig

Command	Argument	Comment
delRow	SNMP-ID of the table	Delete row
addrow	SNMP-ID of the table	Add row
editRow	SNMP-ID of the table	Edit row

Command	Argument	Comment
modifyItem	SNMP-ID of the menu item	Edit a menu item
viewTable	SNMP-ID of the table	View table
viewRow	SNMP-ID of the row	View row
setValue	SNMP-ID of the menu item	Set value of a menu item
listmenu	SNMP-ID of the menu	List sub menu
action	SNMP-ID of the action	Execute an action
reboot	None	Restart device
$URL	None	Display a certain URL

Note: For access via WEBconfig, all URLs sent to the TACACS+ server during configuration must be enabled. For example, the URL "config2" under WEBconfig provides access to the configuration branch of the Hirschmann menu tree. Additionally, the individual parameters that the user may edit also need to be enabled. You can view the URLs sent by WEBconfig to the TACACS+ server with the "trace+ tacacs" trace.

Telnet/SSH

Command	Argument	Comment
dir	SNMP-ID of the directory	View directory content
list	SNMP-ID of the directory	View directory content
ls	SNMP-ID of the directory	View directory content
llong	SNMP-ID of the directory	View directory content
del	SNMP-ID of the table	Delete row
delete	SNMP-ID of the table	Delete row
rm	SNMP-ID of the table	Delete row
cd	SNMP-ID of the target directory	Change directory
add	SNMP-ID of the table	Add row
tab	SNMP-ID of the table	Changes the order of the columns for adding value
do	SNMP-ID of the action	Execute action
show	Parameter name	View information
trace	Parameter name	Execute trace
time	Parameter name	Time
feature	Parameter name	Add function
repeat	Parameter name	Repeat the command
readmib	None	Read-out SNMP-MIB
readconfig	None	Read out the entire configuration
readstatus	None	Read-out status menu
writefiash	None	Update firmware
activateimage	Parameter name	Activate another firmware image
ping	Parameter name	Start ping

Command	Argument	Comment
wakeup	Parameter name	Sends wakeup packet
linktest	Parameter name	WLAN link test
writeconfig	None	Write the entire configuration
scp	Parameter name	Secure copy
rcp	Parameter name	Secure copy
readscript	Parameter name	Read-out script
beginscript	None	Start script
endscript	None	Stop script
flash	Parameter name	Activate/deactivate flash mod

Note: For telnet access, all of the parameters that the user may edit need to be enabled. You can view the values sent by telnet to the TACACS+ server with the trace 'trace+ tacacs'.

SNMP

Command	Argument	Remark
get	SNMP-ID of the menu item	Read out value
set	SNMP-ID of the menu item	Set value

15.12 Login to the HiLCOS administration interface via RADIUS

Currently, users can login to the administration interface of the device by using RADIUS, TACACS+, or the internal user management of the device.

With RADIUS, this is possible over the following connections:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

Note: A RADIUS authentication over SNMP is currently not supported.

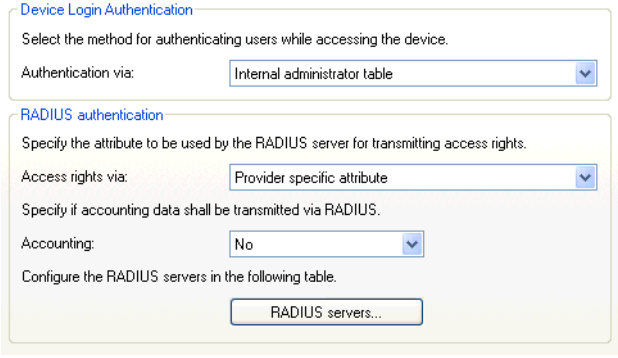
Note: A RADIUS authentication via LL2M (Hirschmann Layer 2 Management protocol) is not supported as LL2M requires plain-text access to the password stored in the OpenBAT.

The RADIUS server handles user management with regard to authentication, authorization and accounting (triple-A protocol), which greatly simplifies the management of admin accounts in large network installations with multiple routers.

Authentication via a RADIUS server is conducted as follows:

- ☐ On login, the OpenBAT sends the user credentials to the RADIUS server in the network. The necessary server data are in stored in the OpenBAT.
- ☐ The server checks the credentials for their validity.
- ☐ If the credentials are invalid, it sends the OpenBAT a corresponding message and the OpenBAT aborts the login process with an error message.
- ☐ If the credentials are valid, the server informs the OpenBAT that the user has permission of access, and also sends information on the access rights and function rights, so that the user has access only to the corresponding functions and directories.
- ☐ If the user's sessions are budgeted by the RADIUS server (accounting section), the OpenBAT stores the session data such as start, end, user name, authentication mode and, if available, the port used.

In the LANconfig, you can set the authentication method under `Management : Authentication`.



In the section "Device login authentication", you choose the method for users to authenticate when accessing the OpenBAT administration interface:

- Internal administrator table: The OpenBAT handles the user management itself by means of user login name, password, and the assignment of access and function rights.
- RADIUS: User management is handled by a RADIUS server in the network.
- TACACS+: User management is handled by a TACACS+ server in the network.

In the the "RADIUS authentication" section, you enter the necessary RADIUS server data and additional administrative data.

☐ **Access rights via**

The authorization of the user is stored in the RADIUS server. When a request arrives, the RADIUS server sends the access- and function rights to the OpenBAT along with the login data, which then logs in the user with the appropriate privileges.

Access and function rights are usually defined in the RADIUS management privilege level (attribute 136), and the OpenBAT simply maps these values to its internal access and function rights. However, some RADIUS servers use this attribute differently, or they may use different, vendor-specific attributes for the authorization. In this situation, the OpenBAT is also able to evaluate provider-specific authorizations. Possible values are:

- Provider-specific attribute: The OpenBAT processes the provider-specific attribute (default).
- Management privilege level attribute: The OpenBAT processes the RADIUS server's management privilege level attribute.

☐ **Accounting**

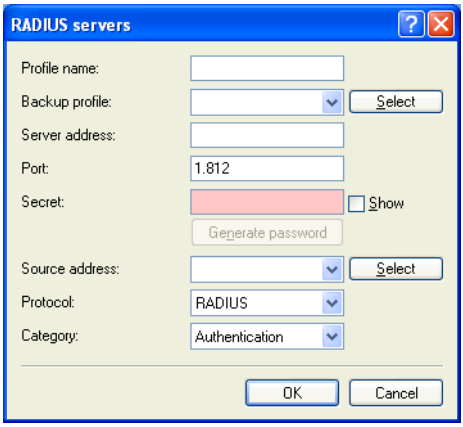
Here, you specify whether the OpenBAT should record the user's session. Possible values are:

– No: The OpenBAT does not record any session data (default).

– Yes: The OpenBAT records the session data (start, end, user name, authentication mode, port).

☐ **RADIUS server**

This table is used to define the RADIUS server settings.



– "Profile name": Enter a name for the RADIUS server here.

– "Backup profile": Enter the name of the alternate RADIUS server to which the OpenBAT forwards its requests if the first RADIUS server is unavailable.

The backup server requires an additional entry in the Server table.

– "Server address": Enter the IPv4 address of the RADIUS server here.

– "Port": Enter the port used by the RADIUS server to communicate with the OpenBAT (default: 1812).

– "Secret": Enter the password for accessing the RADIUS server here, and repeat the entry in the second input field.

– "Source address": This is where you can configure an optional sender address to be used by the OpenBAT instead of the one that would normally be automatically selected for this target address.

– "Protocol": Enter the protocol used by the RADIUS server to communicate with the OpenBAT. Possible values are:

  RADIUS (default)

  RADSEC

– "Category": Set the category for the RADIUS server. Possible values are:

  Deactivated

  Authentication (default)

  Accounting

  Authentication & accountin

15.13Support from TLS 1.1 / 1.2

The encryption protocols SSL and TLS (“Secure Sockets Layer” and “Transport Layer Security”) support secure data communication between 2 communication partners. This is effected by, for example, encrypting, authenticating and checking certificates that are sent. The protocol is mainly used to secure HTTP connections as “HTTPS” or “HTTP over SSL”. In addition, it is used by many other transmission protocols to provide secure communication.

HiLCOS uses the TLS protocol in the following modules:

- HTTP over SSL
- Telnet over SSL
- RADSEC
- CAPWAP/DTLS
- EAP-TLS/PEAP/TTLS

The TLS encryption protocol has developed from 1999 to the current version TLS 1.2. To use the corresponding enhanced functions of clients and Web browsers, Hirschmann devices support the current TLS protocol versions 1.0, 1.1 and 1.2 for secure data transmission.

All devices with HiLCOS versions before 8.60 use encryption protocols SSL 3.0 and TLS 1.0 as standard. From HiLCOS version 8.60 on, you have the option of selecting TLS versions 1.1 and 1.2.

A Glossary

802.11	WLAN specification of the IEEE; data rate up to 2 Mbit/s; in 2.4 GHz ISM band; FHSS and DSSS; infrared spectrum communications also planned
802.11a	Extension to 802.11; data rate up to 54 Mbit/s; in 5 GHz band; OFDM
802.11b	Extension to 802.11; data rate up to 11 Mbit/s; in 2.4 GHz band; high market penetration; DSSS/CCK
802.11g	Extension to 802.11; data rate up to 54 Mbit/s; in 2.4 GHz band; OFDM and DSSS
802.11h	802.11a customization, data rate up to 54 Mbit/s; in 5 GHz band; in area of transmission power and frequency management; for use in Europe; OFDM
802.11i	Future 802.11 extension with additional security features
802.11n	An improvement to 802.11 that adds multiple input/multiple output (MIMO) and other features.
802.11x	Specification of a port-based authentication mechanism from the IEEE.
AAA	Authentication, Authorization and Accounting
Access point (AP)	Base station in a WLAN; can be used in many different designs, including: ▶ connecting wireless communication client devices to either a WLAN or a wired LAN ▶ forming part of a wireless bridge connecting two wired LANs ▶ serving as a wireless bridge relay
Access router	Active network component for connection of a local network to the Internet or a company network.
ACL	Access Control List: a list of wireless stations that either may (whitelist) or may not (blacklist) access a wireless LAN.
ADSL	Asymmetrical Digital Subscriber Line – transmission process for high-speed data transmission over normal telephone lines. With ADSL, transmissions (downstream) of up to 6 Mbps can be implemented over normal telephone lines; for bidirectional transmission there is a second frequency band with transmission speeds of up to 640 kbps (upstream) - hence the name “asymmetric.”
AES	Advanced Encryption Standard; successor of DES.
ARF	Advanced Routing and Forwarding
ARP	Address Resolution Protocol
Bandwidth	Channel capacity or data rate through a communication path; the higher the bandwidth, the faster the connection.
Blowfish	A symmetric block cipher, eclipsed in popularity by AES.
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
Bridge	Transport protocol-independent, transparent network component; transmits all packets that are identified as “not local” and only understands the difference between “local” and “remote.” Works on Layer 2 of the OSI model.
Broadband	Service which provides high bandwidth; e.g.: DSL or WLAN

Broadcast	Broadcasts are packets to all stations of a local network; bridges transmit broadcasts; routers do not transmit broadcasts.
BSS	Basic Service Set
CAPI	Common ISDN Application Programming Interface - CAPI is a standard for control of ISDN adapters.
CBCP	Callback Control Protocol
CCK	Code Complementary Keying; type of modulation used by DSSS
CCP	Compression Control Protocol
CGI	Common Gateway Interface
Chaining	Concatenation of bit sequences.
CHAP	Challenge Handshake Authentication Protocol
Client	Common ISDN Application Programming Interface - CAPI is a standard for control of ISDN adapters.
CSD	Cyclic Shift Diversity
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance; access procedure to the radio channel used under 802.11.
CRC	Cyclic Redundancy Check; process for detecting inaccurate bit patterns.
CTS	Clear to send: Part of the RTS/CTS (Request to Send/Clear to Send) 802.11 function designed to help prevent an occurrence of the 'hidden station' phenomenon.
Data throughput	Speed at which you can send and receive data over a connection; depends on the bandwidth and the number of users
DDC	Direct Data Connect
DES	Data Encryption Standard: a form of shared secret encryption.
DFS	Dynamic Frequency Selection: a protocol for selecting only unused channels within a frequency, so as to avoid interference with radar systems.
DHCP	Dynamic Host Configuration Protocol
DMZ	Demilitarized Zone: a physical or logical subnetwork that exposes an organization's external services to an untrusted network.
DNS	Domain Name Server Computers communicate with one another in remote networks via IP addresses. DNS servers translate names into IP addresses. Without DNS servers you could only operate with IP addresses and not with names.
Domain	Area of network closed to outside => Intranet
DoS	Denial of Service
Download/ Downstream	Denotes the direction of dataflow in a WAN. Downstream is the direction from the head end or Internet to the participant connected to the network.
DPP	Dead Peer Protection
DS	Distribution System
DSCP	DiffServe code point: a 6-bit header in IP packets used to prioritize packets.
DSL	Digital Subscriber Line - DSL procedures include all procedures for digital-broadband use of telephone lines, such as ADSL, HDSL, SDSL, VDSL and so on, which are also called xDSL.
DSSS	Direct Sequence Spread Spectrum; code multiplex -- band spreading process
DTIM	Delivery Traffic Indication Message: a parameter for configuring beaconing.

DynDNS	Dynamic Domain Name System: IPsec-VPN implementation which allows the transparent connection of local networks into a VPN solution, even when their routers are working with dynamic addresses (dial-up).
EAP	Extensible Authentication Protocol
EAP-MD5	EAP variant which uses passwords for one-sided authentication.
EAP-TLS	EAP Transport Layer Security; EAP variant which uses certificates for mutual authentication.
EAP-TTLS	EAP Tunneled Transport Layer Security; EAP variant which uses certificates for mutual authentication.
EIRP	Effective Isotropic Radiated Power
ERP	Enterprise Resource Planning
ESS	Extended Service Set
ESSID	Extended Service Set Identity; “network name” of the wireless LAN.
Ethernet	The communication protocol defined by the IEEE as the 802.3 standard, Ethernet provides a wired access method for local area network (LAN) devices. The wireless version of Ethernet is WiFi.
FHSS	Frequency Hopping Spread Spectrum; frequency skipping band spread procedure.
Firewall	Protective mechanism for an Intranet against attacks from outside.
FQDN	Fully Qualified Domain Name
Frequency	Number of oscillations per second (given in Hertz; 1 Hz = 1 oscillation per second; GHz = Gigahertz = 1 billion Hertz or oscillations per second).
Frequency band	Contiguous frequency range which has the same transmission properties.
FTP	File Transfer Protocol: This protocol enables data transfer between different systems and simple file manipulation; FTP is based on the TCP transmission protocol.
FXP	File Exchange Protocol
Gateway	Network component which provides access to other network components on a layer of the OSI model. Packets which do not go to a local partner are sent to the gateway. The gateway takes care of communication with remote networks.
GPRS	General Packet Radio Service
HDLC	High-Level Data Link Control protocol
HiLCOS	Equivalent to Hirschmann operating system.
HotSpot	Locally limited wireless network with a base station with Internet access; public wireless Internet access.
HTTP	Hypertext Transfer Protocol
Hub	Network component; distributor; collector; also used to translate from one connection type to another.
IAPP roaming	Roaming between the cells of a wireless network using IAPP (Inter Access Point Protocol).
IBSS	Independent Basic Service Set
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System -- earliest possible detection of attacks on the network
IETF	Internet Engineering Task Force

IGMP	Internet Group Management Protocol
IMAP2	Internet Message Access Protocol version 2
Inband	The sending of control metadata—for example, parameter configuration values—on the same channel, or band, used for data.
IP Masquerading	Combination of PAT (Port Address Translation) and NAT (Network Address Translation) used for connection of an intranet (multiple workstations) to the Internet over a single IP address; simultaneously, the internal computers are shielded from attacks from outside.
IP Quality of Service	These functions give precedence to enterprise-critical applications, particular services, or user groups.
IPCP	Internet Protocol Control Protocol
IPSec	Internet Protocol Security
IPXCP	Inter-network Packet Exchange Control Protocol
IRC	Internet Relay Chat
ISDN	Integrated Services Digital Network -- fast connection; two independent channels; higher transmission rates than analog (up to 128 Kbit/s); uses the old analog lines; convenience features (call forwarding, callback on busy, etc.); supports both analog and digital services
ISM frequency band	Industrial-Scientific-Medical, license-free frequency bands which can be used for industrial, scientific, and medical purposes.
ISP	Internet Service Provider -- service provider with a connection to the Internet (backbone) who provides connection points for end customers.
IV	Initialization Vector
LAN	Local Area Network - local network limited to one site.
LANcapi	Virtual CAPI offered via the network. With LANcapi, which is implemented in all OpenBATs with an ISDN interface, a PC connected to the LAN can use ISDN telematic services.
LANconfig	Software for configuring OpenBATs in Windows.
LANmonitor	Software for monitoring LANs, consisting of OpenBATs in Windows.
LANtools	Extensive, user-friendly set of tools for the management and monitoring of OpenBAT devices, and related products and systems.
LCP	Link Control Protocol, part of the point-to-point (PPP) protocol.
LEPS	Hirschmann Enhanced Passphrase Security
MAC	Media Access Control; radio access protocol on ISO Layer 2 data link; it defines packet format, packet addressing, and error detection.
MAC address	Serial number of a network component which is assigned by the manufacturer.
Mbit	Megabit: standard unit for the specification of data quantities in the context of bandwidths.
MCS	Modulation and Coding Scheme
MIC	Message Integrity Check, cryptographic integrity testing mechanism.
MS-CHAP	Microsoft version of Challenge Handshake Authentication Protocol
MTU	Maximum Transmission Unit
NAT	Network Address Translation
NBNS	NetBIOS Naming Service

NetBIOS	Network Basic Input/Output System. Non-routable network protocol for local networks developed by IBM and later taken over by Microsoft.
NNTP	Network News Transfer Protocol
NTBA	The NTBA (network termination basic adapter) is responsible in an ISDN base connection for the translation of the connection created by the telephone company to the S0 bus.
NTP	Network Time Protocol
OFDM	Orthogonal Frequency Division Multiplex
Outband	The sending of control metadata—for example, parameter configuration values—over a separate channel and not over the channel used for data.
P2MP	Point to multipoint: Multiple WLAN stations log into a base station and constitute a common network with the wired stations
P2P	Point to point: Two base stations connect two wired networks over WLAN; point-to-point operation enables coupling of networks even across streets without cables
PAP	Password Authentication Protocol
PCI	1. Peripheral component interconnect: a standardized bus for connecting peripheral components to the computer. 2. Payment Card Industry
PEAP	Protected EAP, EAP variant for mutual authentication
PKI	Public Key Infrastructure
PMK	Pairwise Master Key
PMTU	Path Maximum Transmission Unit
POP3	Post Office Protocol version 3
PPP	Point to Point Protocol: Network protocol for connecting two computers. PPP is based on TCP/IP.
PPPoE	Point-to-Point-Protocol over Ethernet: The protocol for encryption of PPP frames inside Ethernet frames.
PPTP	Point to Point Tunneling Protocol: Network protocol for the construction of virtual private networks over the Internet.
QoS	Quality of Service (see also IP Quality of Service)
Radio frequency	Every WLAN application uses globally regulated radio frequencies
RADIUS	Remote Authentication Dial-In User Service; authentication and monitoring protocol on the application level for authentication, integrity checking, and accounting for network access
RC4	Streaming cipher process by Ron Rivest, “Ron’s Code.”
RFC	Request for Comments
RIP	Routing Information Protocol
Router	Intelligent network component;, comparable to a post office, which can determine from the logical destination address of a packet which next network component should transmit the packet; knows the overall topology of the network.
RSA	An algorithm for public key cryptography, named for its inventors Rivest, Shamir and Adleman.
RSTP	Rapid Spanning Tree Protocol

RTS	Request to Send: Part of the RTS/CTS (Request to Send/Clear to Send) 802.11 function designed to help prevent an occurrence of the ‘hidden station’ phenomenon.
SDSL	Single Line Digital Subscriber Line - downstream and upstream at 2.048 Mbit/s (two-core cable).
Server	Computer which provides services over the network (e.g. files, news, email, WWW pages).
SINA	Secure Inter-Network Architecture
SMTP	Simple Mail Transfer Protocol - SMTP protocol is the Internet standard for distribution of electronic mail; the protocol is based on the TCP protocol.
SNMPv3	Simple Network Management Protocol Version 3
SPI	Stateful Packet Inspection
SSH	Secure shell
SSID	Service Set Identity; “network name” of the wireless LAN.
SSL	Secure Socket Layer
Splitter	The splitter is comparable to an audio frequency filter; in an ADSL connection, the splitter separates the ISDN signals from the DSL signals; the ISDN signals go to the NTBA and the DSL signals go to the DSL modem
STP	Spanning Tree Protocol
Switch	A central distributor in a network that connects network segments. A switch sends data packets on the OSI Data Link Layer (Layer 2). The switch can also carry out this task on the OSI Network Layer (Layer 3). Switches are used to reduce collision, thereby increasing the overall throughput of the network.
SYN/ACK	Synchronization/acknowledge
SYSLOG	A standard for logging program messages—it allows for separation of the program that generates the message from the program that analyzes the messages.
TACACS+	Terminal Access Controller Access-Controller System Plus: A proprietary protocol for controlling accesses – such as authentication, authorization and accounting – to network devices.
TAE	Telephone connection unit used in Germany. Plug for the connection of analog devices like a telephone or modem into the telephone network.
TCP/IP	Transmission Control Protocol/Internet Protocol; family of protocols (ARP, ICMP, IP, UDP, TCP, HTTP, FTP, TFTP) used mainly in the Internet, although it is making headway in intranets as well.
Telnet	TELE NETwork: a protocol providing bi-directional, text-based, interactive communication.
TFTP	Trivial File Transfer Protocol
TKIP	Temporal Key Integrity Protocol
TLS	Transport Layer Security
TPC	Transmission Power Control
TTLS	Transport Layer Security
TU	Timer Unit: a time unit of measure for the IEEE 802.1 standard, equal to 1 k?s.
UDP	User Datagram Protocol: one of the core protocols of the IP suite that enable unconnected messaging.

Upload/Upstream	Upload/upstream denotes the direction of dataflow in a WAN; upstream is the direction from the node connected to the network to the head end/ Internet
URL	Uniform Resource Locator
USB	Universal Serial Bus
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol: a group of technologies for the transmission of voice communications over IP.
VPN	Virtual Private Network: a VPN is a network consisting of virtual connections over which non-public or company internal data can be transmitted securely, even if public network infrastructures are used.
WAN	Wide Area Network: network connection over long distances (e.g., via ISDN with a OpenBAT).
WDS	Wireless Distribution System
WECA	Wireless Ethernet Compatibility Alliance: alliance of manufacturers of wireless LAN components based on IEEE 802.11; renamed the WiFi Alliance.
WEBconfig	Web-based configuration interface for OpenBATs.
WEP	Wired Equivalent Privacy
WiFi	wireless fidelity; marketing term promulgated by the WECA. WiFi is defined by IEEE as the 802.11 standard and is the wireless counterpart to wired Ethernet.
WiFi-Alliance	Wireless Ethernet Compatibility Alliance: alliance of manufacturers of wireless LAN components based on IEEE 802.11; renamed the WiFi Alliance.
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WME	Wireless Multimedia Extensions
WMM	WiFi Multimedia
WPA	WiFi Protected Access; name for security mechanisms beyond IEEE 802.11; generated by the WiFi Alliance.
WPA2	Successor to WPA.
WLAN	Wireless Local Area Network - local radio network
xDSL	xDSL stands for the family of Digital Subscriber Line technologies.
XOR	Logical operation “exclusive OR”

B Index

Numerics

3 DES 625
802.11 1197
802.11a 1197
802.11b 1197
802.11g 1197
802.11h 1197
802.11i 1197
802.11n 1197
802.11x 1197

A

AAA 1197
Access control list 228
Access Point 31, 33
Access point 1197
Access Point example
  DHCP server 82
Access point example
  basic settings 55
  configuration file 52
  configuring DHCP WLAN 86
  configuring the LAN 83
  WLAN settings 63
Access restricted 730
  by IP address 732
  by source 730
Access router 1197
Accounting 1128
ACL 1197
Action table 876
  configuring 882, 885
  dynamic DNS 876
Address translation configuration 821
ADSL 1197
AES 625, 1197
Aggressive mode 625
AH 625
Antenna settings
  diversity 248
  grouping 247
  power attenuation settings 249
ARF 739, 780, 788, 1197
ARP 1197

B

Background WLAN scanning 725
Bandwidth 1197
  granted minimum 1079
Beaconing 274
Blowfish 625, 1197
Boot images list 1095
BOOTP 1089, 1197
BPDU 1197
Bridge 1197
Bridge group 393
Broadband 1197
Broadcast 1198
Brute force attack 729
BSS 1198

C

Callback 845
  CBCP 846
  configuring 846, 848
  fast 847
  Other Router 848
  PPP LCP 848
CAPI 1198
CAPWAP data tunnel 388
CAPWAP standard
  Control channel 384
  Data channel 384
  Data-channel advantages 385
  Payload data 385
  Transmission channels 384

CAST 625
CBCP 846, 1198
CCK 1198
CCP 1198
CGI 1198
Chaining 1198
Channel setting 246
CHAP 1198
Client 1198
Client configuration settings 255
COM port adapters 904
COM port server 889
  byte counters 902
  COM port errors 903
  COM port status 901
  configuring 891
  connections 903
  device ports table 892
  network interface table 895
  network status 900
  operating modes 890
  serial interface table 893
  status 900
Communication layers list 800
Configuration
  download 45
  offline 44
  online 44
  Software 41
Configuration file
  create by copying 83, 136, 160, 182
  creating 48
Controlling WLAN data traffic 220
CRC 1198
CRON table 1141
CSD 1198
CSMA/CA 1198
CTS 1198

D

Data throughput 1198
Daylight savings time 1139
DDC 1198
Deflate 625
DES 625, 1198
Device
  configuration 47
  roles 31
Device authentication 279
  IEEE 802.1x and EAP 281
  RADIUS 279
Device operating state table 899
Device ports table 892
DFS 1198
DHCP 1198
  address tracking 226
  vendor class and user class ID 1110
DHCP network table 1100
DHCP networks table 1105
  configuring 1090
DHCP relay 1089
DHCP relay server 1105
DHCP server 1088
  additional options 1103
  alias list 1099
  assign client boot image 1096
  assign client IP address 1096
  boot image list 1099
  configuring 1090
  configuring via Telnet 1097
  configuring via WEBconfig 1097
  create a boot image 1095
  DHCP status table 1104
  enable/disable by logical interface 1090
  hosts table 1099
  IGMP packet data 1098
  networks list 1100
  port table 1103
  relay server 1105
DHCP table 1108
DiffServ 1075
  firewall rules 1077
  VLAN 747
DMZ 811, 1198
  assignment of network zones to 812
  multiple IP address design 814
  separation from intranet LANs 814
  unmasked internet access 813
DNS 1088, 1111, 1198
  dynamic 1122, 1199
  forwarding 1113
  URL blocking 1121
DNS server
  configuring 1115

Domain 1198
DoS 963, 1198
Download 1198
Download configuration 45
Downstream 1198
DS 1198
DSCP 1198
DSL 1198
DSL connection
limiting call charges 1131
DSSS 1198
DTIM 1198
Dynamic DNS 1199

E

EAP 281, 1166, 1199
EAP-MD5 1199
EAP-TLS 1199
EAP-TTLS 1199
EIRP 1199
E-mail
WLAN events 207
Encryption 230
WPA and WEP 231
ERP 1199
ESP 625
ESS 1199
ESSID 1199
Ethernet 1199
Example of an Access Point 51

F

FAQ 1219
Fast callback 847
FHSS 1199
Firewall 1199
action objects 946
action table 951
actions 932
and masked connections 929
configuration tips 922
configuring 925
connection list 956
creating new filter rule 930
default setting 922
defining objects 944
denial of service (DoS) attacks 963
diagnosing 952
DoS configuration 963
e-mail event notification 926
enable/disable 926
filter list 954
FTP 941
host block list 958
HTML configuration 948
intrusion detection system (IDS) 960
IRC 941
limitations 959
log table 952
Network Address Translation (NAT) 923
objects table 949
packet fragments 926
ping blocking 928
port block list 957
QoS objects 946
rule settings 932
rules table 948
service objects 947
session recovery 926
station objects 947
stealth mode 928
Firewall strategies
deny all 923
FQDN 1199
Frequency 1199
band 1199
Frequency setting 246
FTP 1199
FXP 1199

G

Gateway 1199
GPRS 1199
backup connection 854

Granted minimum bandwidths 1079

H

Hash algorithms 625
HDLC 1199
HiLCOS 1199
HotPlug-capable adapters 899
Hotpluggable adapters 890
HotSpot 1199
Hub 1199
HyperTerminal 41

I

IAPP roaming 1199
IBSS 1199
ICMP 1199
  redirects 770
IDS 960, 1199
  address checking 813
  configuring 961
IETF 1199
IGMP 1200
IGMP snooping 905
  configuring 911
  multiple bridges 908
  operation 907
  status 916
IKE 625
IMSP2 1200
Indoor-only mode 207
Inverse IP masquerading 806
IP address assignment to PC in Windows 1107
IP Masquerading 1200
IP masquerading 803
  and stateful inspection 808
  configuring 805
  inverse 806
  transmittable protocols 805
IP networks table 786
IP QoS 1200
IP routing 762
IPCOMP 625
IPCP 1200
IPSec 625, 1200
IPXCP 1200
IRC 1200
ISAKMP 625
ISDN 1200
ISM frequency band 1200
ISP 814, 1200
IV 1200

K

Keep-Alive-Functionn 843
Key lengths 625

L

LAN 1200
LANcapi 1200
LANconfig 1200
LANmonitor 1200
LANtools 1200
Layer-3 roaming 395
LCP 1200
  PPP connection checking 827
LEPS 724, 1200
Login lock 729

M

MAC 1200
MAC address 1200
MAC filter enabled 264
Main mode 625
Mbit 1200
MCS 1200
MIC 1200
Modem
  serial interface 850
MS-CHAP 1200
MTU 862, 1200
  configuring 862
  statistics 863

N

NAT 815, 923, 1200
  address translation 821
  network coupling 815, 816
  remote monitoring/control 815, 817

NAT table 821
NBNS 1200
NetBIOS 1088, 1201
NetBIOS proxy 795
Network
assigning interfaces 786
defining 786
Network coupling 815, 816
Network interface table 895
Network separation
Application example 390
Networks
separating 388
NNTP 1201
NTBA 1201
NTP 1136, 1201

O

OFDM 1201
Offline configuration 44
Online configuration 44
Overlay network 385, 388
Configuration public spot 398

P

Packet filter
protocol based 221
PAP 1201
Password
SNMP read 728
Password configuring 728
Payload data
Forwarding from WLANs 395
PCI 1177, 1201
PEAP 1201
Peer list 848
Ping blocking 928
PKI 1201
PMK 1201
PMTU 1201
Point-to-multipoint 1201
Point-to-point 1201
configuration settings 253
Point-to-point (1 subnet) example
WLAN settings 118
Point-to-point (2 subnets) example
creating a transfer network 149
routing the transfer network 154
Point-to-point example
(1 subnet)

Point-to-point example (1 subnet) 109
Point-to-point example (2 subnets) 146
Point-to-point partner configuration 259
Point-to-point relay (1 radio) example
configure master 171
configure slave 165, 176
Point-to-point relay (2 radios) example
configure master 183
configure slave 195, 198
Point-to-point relay example (1 radio) 159
Point-to-point relay example (2 radios) 181
Poisoned reverse 778
Polling table 859
POP3 1201
Port forwarding table 808
Port mapping 808
Port table 787, 1103
PPP 824, 1201
application scenarios 825
assigning IP addresses 828
configuring 830
description 824
negotiation phases 826
RADIUS authentication 833
PPP list 830, 833
PPPoE 832, 835
configuring 839
example application 836
limited to subnet 835
PPTP 768, 1201
DSL dial-in 841
PPTP list 841
Preshared key 625
Protocol based packet filters 221
Public spot
WLAN Controller 398

Q

QoS 1073, 1200, 1201
enabled/disabled 1076
objective 1074
Reducing packet length 1081
Transmission and reception direction 1080
WLANs 1084

R

radio
enable/disable 243

Radio frequency 1201
Radio interface 242
default setting 43
Radio settings 245
channel 246
frequency 246
RADIUS 279, 833, 1145, 1201
802.1x client access 1155
access list 1172
accounting 1149
client configuring 1174
operation 1147
PPP client access 1150
server configuring 1175
versus TACACS+ 1178
WLAN client access 1153
X.509 certificates 1175
RADIUS Server
Add clients 1160
RADIUS server
adding users 1162
configuring 1157
EAP authentication 1166
forwarding 1169
general settings 1158
RC4 1201
Redirect
IPv4 packets 225
Remote site
configuring 798
Remote site (peer) list 798
Remote sites (serial) list 857, 858
RFC 1201
RIP 771, 1201
configuring 773
configuring filter 774
for separate networks 775
LAN triggered update 777
poisoned reverse 778
static routes 778
WAN triggered update 777
RIP filter 774
RIP table 773
Roaming 220, 275
Application example 397
Layer-3 395
Roles 31
Router 1201
Routing 759, 762
Advanced 780
assign WAN interface tags 789
assignment of network zones to DMZ 812
DMZ 811
dynamic 771
ICMP redirects 770
IP masquerading 803
NAT 815
NetBIOS proxy 795
network definition 786
on the LAN 770
policy based 766
port mapping 808
PPP 824
PPTP connection tags 768
remote site confguring 798
routing vs. interface tags 784
SYN/ACK speedup 779
virtual router 794
virtual routers 788
VPN connection tags 768
Routing table 762
configuring 763
IP masquerading setup 805
RSA 625, 1201
RSTP 867, 1201
configuring 870
enable/disable 870
statistics 872
versus STP 868
RTS 1202
RTS/CTS function 270

S

SDSL 1202
Separation of networks 388
Serial interface
backup connection 858
Configuration 890
configuring for modem 852
modem operation 850
remote site connection 857
statistics 855
trace output 856

Serial interface table 893
Server 1202
Session recovery 926
Setup wizard
access point basic settings 56
access point WLAN settings 63
Check security settings 726
point-to-point basic settings 110
point-to-point WLAN settings 118
wireless client basic settings 93
wireless client WLAN settings 98
Silent rejection
TCP and UDP packets 928
SINA 1202
SMTP 1202
SNMP 41
read password 728
SNMPv3 1202
SPI 1202
Splitter 1202
SSH 1202
SSID 262, 1202
SSL 1202
STP 1202
Switch 1202
Symbol 29
SYSLOG 1202
System requirements 851

T

Table Clients 1160
Table Forwarding server 1170
TACACS+ 1177
assigning rights 1188
authorization functions 1188
configuring 1179
server configuring 1183
server login (LANconfig) 1184
server login (Telnet/SSH) 1187
server login (WEBconfig) 1185
versus RADIUS 1178
TAE 1202
TCP packet
silent rejection 928
TCP/IP 1202
Technical Questions 1219
Telnet 41, 1202
modem command 855
TFTP 41, 1202
Time server 1134
configuring 1134
configuring clients 1136
Time zone 1137
TKIP 723, 1202
TLS 1174, 1202
ToS 1075
VLAN 747
TPC 1202
Trace 283
Training Courses 1219
Transport mode 625
Triple DES 625
TTLS 1202
TU 1202
Tunnel mode 625

U

UDP 1202
UDP packet
silent rejection 928
Upload 1203
Upstream 1203
URL 1203
USB 1203
User table 1162

V

Virtual router 794
Virtual routers 788
VLAN 1203
ARF 739
assigning clients 745
configuring 739
define 741
description 738
enable/disable 740
general settings 740
port configuration 742
special DSL IDs 746
tags on layers 2/3 747
VoIP 1203
VPN 1203

W

WAN 1203
connections 759
functions 760
WAN RIP table
configuring 864

WAN tag table 789
WDS 1203
WEBconfig 1203
WECA 1203
Well known groups 625
WEP 231, 1203
group keys 236
WiFi 1203
WiFi-Alliance 1203
Windows
assigning IP address to a PC 1107
Wireless client
configuration settings 255
Wireless client example
creating configuration file 89
Wireless network
transmission settings 267
Wireless network configuration 262
WISP 1203
WLAN 1203
access control list 228
access point or client mode 243
beaconing 274
broadcast rate 268
client mode configuration 255
default settings 43
device authentication 279
increasing data transmit rates 252
logical network configuration 262
network transmission settings 267
packet size 268
point-to-point configuration 253
point-to-point partner configuration 259
radio interface 242
radio interface enable 243
radio settings 245
roaming 275
SSID 263
trace 283
transmit rates 268
WLAN Bridge 31
Point-to-Point 34
WLAN bridge example
WLAN settings 118
WLAN Bridge Relay 31
WLAN bridge relay 36
WLAN Client 32, 38
WLAN client
roaming 220
WLAN Client example 89
WLAN Controller 388
Public spot 398
WLAN data traffic control 220
WLAN Distribution Point 31
WLAN distribution point
point-to-multipoint 37
WLAN encryption 230
WPA and WEP 231
WLAN parameters
configuring 205
general settings 206
indoor only mode 207
security settings 219
WLAN profile 392
WLAN roaming client 32, 39
WLAN settings 391
WLC interfaces (virtual) 386
WLC tunnel 386, 391
WME 1084, 1203
WMM 1084, 1203
WPA 231, 723, 1203
WPA2 723, 1203

X

X.509 625
xDSL 1203
XOR 1203

Z

ZLIB 625

C Maintenance

Hirschmann is continually working to improve and develop our software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website.

D Further Support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You find the addresses of our partners on the Internet at
http://www.hirschmann.com

A list of local telephone numbers and email addresses for technical support directly from Hirschmann is available at
https://hirschmann-support.belden.com

This site also includes a free of charge knowledge base and a software download section.

Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.

▶ Training offers you an introduction to the basics, product briefing and user training with certification.
You find the training courses on technology and products currently available at
https://www.belden.com/solutions/customer-innovation-center

▶ Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against making any compromises in any case. Our client-customized package leaves you free to choose the service components you want to use.

Internet:
https://www.belden.com/solutions/customer-innovation-center

HIRSCHMANN

A **BELDEN** BRAND

HIRSCHMANN
A BELDEN BRAND

Addendum
HiLCOS Rel. 9.00

Contents

1 LCMS.....7

1.1 Enhancements to LANconfig.....7

1.1.1 Automatic authentication for read-only access to LANmonitor.....7

1.1.2 Display of administrator user name.....8

1.1.3 Authenticating against a proxy server.....9

1.2 Enhancements to LANmonitor.....10

1.2.1 Internal IPv6 support.....10

2 Configuration.....11

2.1 Output additional ports in SYSINFO at the console.....11

2.2 Sorted display of a menu on the console.....11

2.3 Customize the management ports for device access.....12

2.4 Comment box for access stations.....12

2.5 Elliptic curve cryptography (ECC).....13

3 IPv6.....15

3.1 IPv6 support for RAS services.....15

3.1.1 RAS interfaces.....15

3.1.2 Prefix pools.....17

3.2 RADIUS attribute extensions for IPv6 RAS services.....18

3.3 Loopback addresses for IPv6.....19

3.3.1 Loopback addresses.....19

3.4 Lightweight DHCPv6 relay agent (LDRA).....20

3.5 Router advertisement snooping....23

4 RADIUS....25

4.1 New attribute in the RADIUS server, shell privilege level....25

4.1.1 Using RADIUS to login to the HiLCOS management GUI....25

5 Public Spot....29

5.1 Number format for Smart Ticket....29

5.2 Viewing Public Spot clients....29

5.3 Displaying advertising to Public Spot users....30

5.3.1 Extensions to the RADIUS attributes....31

5.4 Additional attributes for the XML interface....32

5.5 Dynamic change of a user session via the XML interface....33

6 WLAN....36

6.1 Support of 802.11ac WLAN interfaces....36

6.2 Specifying client-bridge mode and bandwidth limit for each SSID....36

6.3 Separation of P2P and WLAN/SSID configuration....38

6.3.1 Configuration of P2P connections....39

6.4 Band steering with delayed scan at 2.4 GHz....42

6.5 WPA2 with AES as factory setting....43

6.6 WLAN protected management frames (PMF)....43

6.7 Opportunistic key caching (OKC)....46

6.7.1 Tutorial: Activating OKC on an AP / the client side....47

6.8 Wireless IDS....49

6.8.1 Wireless IDS Counter....50

6.8.2 Wireless IDS Types of Attack....51

6.8.3 Tutorial: Configuring Wireless IDS....53

6.9 Redundant connections using PRP.....55
6.9.1 Basic function.....56
6.9.2 Advantages of WLAN PRP.....56
6.9.3 Implementation of PRP in the access points.....57
6.9.4 Implementing PRP exclusively over WLAN.....57
6.9.5 Dual roaming.....58
6.9.6 Diagnostic options.....59
6.9.7 Tutorial: Setting up a PRP connection over a point-to-point network (P2P).....59
6.9.8 Tutorial: Roaming with a dual-radio client and PRP.....63
6.9.9 Queue Processing for Wireless PRP.....67
6.9.10 Wireless PRP Micro-reordering Buffer.....67
6.9.11 Tutorial PRP Micro-reordering Buffer.....69

7 WLAN management.....71

7.1 AutoWDS – wireless integration of APs via P2P connections.....71
7.1.1 Notes on operating AutoWDS.....74
7.1.2 How it works.....77
7.1.3 Setup by means of preconfigured integration.....87
7.1.4 Accelerating preconfigured integration by pairing.....90
7.1.5 Express integration.....92
7.1.6 Switching from express to preconfigured integration.....93
7.1.7 Manual topology management.....94
7.1.8 Redundant paths by means of RSTP.....98
7.2 IP-dependent auto configuration and tagging of APs.....99
7.2.1 Setting up assignment groups for IP-dependent auto configuration.....101

7.2.2 Setting up tag groups for the detailed selection of APs.....102
7.2.3 Enhancements to command-line commands 103
7.3 Automatic selection of the 2.4-/5-GHz mode.....105
7.4 WLC cluster.....107
7.4.1 WLC tunnel for internal communication.....108
7.4.2 Setting up a CA hierarchy.....108
7.4.3 Enabling/disabling CAPWAP in the WLC.....110
7.4.4 Finding the ideal WLC.....110
7.4.5 Determining the ideal AP distribution.....111
7.4.6 Manually initiate ideal AP distribution.....112
7.5 One-click backup of the SCEP-CA.....113
7.6 Automatic restart of managed APs after firmware update.....114
7.6.1 Load firmware in managed AP.....114
7.7 Automatic search for alternative WLCs.....115
7.8 U-APSD configurable by WLC.....115
7.9 Group-related radio field optimization.....115
7.10 Adding new APs with the WEBconfig Setup Wizard.....117
7.11 Maximum bandwidth can be adjusted for each WLAN module.....118
7.12 Client steering by WLC.....120
7.12.1 Configuration.....121
7.13 Automatic frequency-band selection.....125

8 VPN.....126

8.1 VPN remote access wizard in WEBconfig:.....126
8.2 L2TPv2 (Layer-2 Tunneling Protocol version 2).....126
8.2.1 Configuring the L2TP tunnel.....127
8.2.2 Authentication via RADIUS.....131

8.2.3 Operation as an L2TP access concentrator (LAC).....133
8.2.4 Operation as the L2TP network server (LNS) for RAS clients.....135
8.2.5 Operation as an L2TP network server (LNS) with authentication via RADIUS.....137
8.3 Support of the DH groups 15 and 16.....139
9 Routing and WAN connections.....140
9.1 AC name configurable for PPPoE server.....140
10 Other services.....141
10.1 Deactivating device LEDs – boot-persistent.....141
10.2 Comment box for CRON jobs.....142
10.2.1 Configuring the scheduler.....142
10.3 DHCP snooping and DHCP option 82.....145
10.4 Enabling LLDP with LANconfig.....148
10.5 L2 Firewall.....148
10.5.1 L2-Firewall Functions.....148
10.5.2 Tutorial Configuring the L2 firewall.....149

1 LCMS

1.1 Enhancements to LANconfig

1.1.1 Automatic authentication for read-only access to LANmonitor

As of 9.00, LANconfig offers a new user-friendly feature: With a device configuration opened in LANconfig, LANmonitor can be started without you having to enter access credentials again.

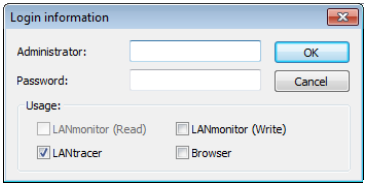
Login information

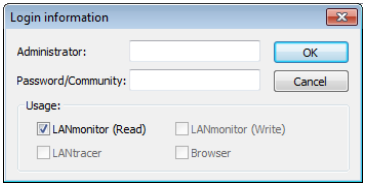
Enter the access credentials for the external programs in this field. Click **New** to select one or more application(s) and enter the corresponding access credentials. Depending on your selection, the dialog window requests different access credentials. If you invoke the program from LANconfig, you have the option of authenticating yourself with the username and password of your administrator login.

In the case of LANmonitor, you have the option to specify an individual SNMP community for read-only access. By default, when LANconfig opens a device configuration it checks whether and to what extent you have stored access credentials for external programs. If you do not have access credentials or if these credentials have been configured in the form of an SNMP community only, then invoking LANmonitor prompts LANconfig to take the SNMP community from the loaded device configuration. If you edit a configuration in LANconfig and you have set an SNMP community here, LANconfig automatically saves the SNMP community for the corresponding device. This convenient behavior reduces the scope of authentication for LANmonitor, so no separate configuration of the read-only access is required.

Note: LANconfig evaluates the setup parameter 2.9.15 Read-Only-Community for the convenient behavior described above. Any additional read-only SNMP communities configured in the device are ignored.

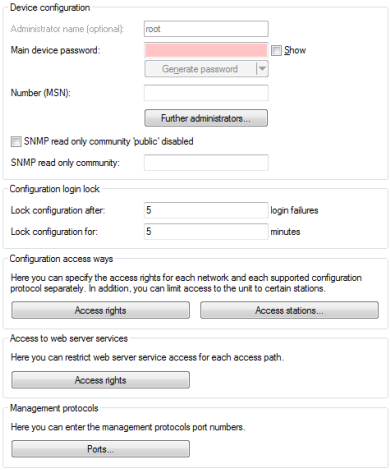
For more information about the SNMP access through single or multiple SNMP communities, see the section *Configuring SNMP read-only access*.





1.1.2 Display of administrator user name

In order to show which username is linked to the main password, as of version 9.00 LANconfig shows **root** as the administrator user name in the device configurations and in the Wizards.



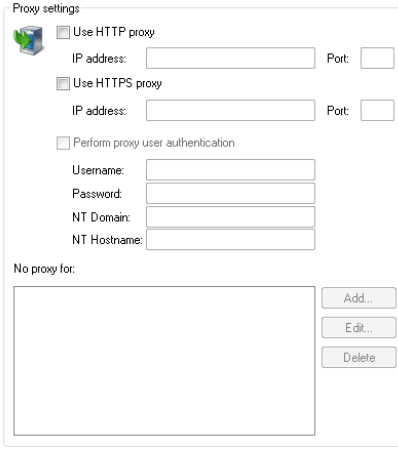
1.1.3 Authenticating against a proxy server

As of version 9.00 it is possible for LANconfig to authenticate against an external proxy.

Proxy

If you wish to use a proxy server for access to your device, you can configure this here. Activate the required protocol and enter the address and port for accessing the proxy server.

Depending on the protocol, it may be possible to specify a list of networks or individual hosts for which the proxy settings do not apply.



Use HTTP proxy

Enables the use of an HTTP proxy.

- **Address**: Enter the IP address of the the HTTP proxy server.
- **Port**: Enter the port used by the HTTP proxy server.

Use HTTPS proxy

Enables the use of an HTTPS proxy.

- **Address**: Enter the IP address of the the HTTPS proxy server.
- **Port**: Enter the port used by the HTTPS proxy server.

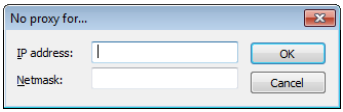
Perform proxy user authentication

If the proxy server requires authentication, enter the user name and password here.

Note: This option is available only if the proxy setting is enabled.

No proxy for

Enter the IP addresses and the corresponding netmask to which the proxy settings do not apply.



Note: This option is available only if the proxy setting is enabled.

1.2 Enhancements to LANmonitor

1.2.1 Internal IPv6 support

As of version 9.00, LANmonitor can handle IPv6 addresses internally and can thus communicate with devices via IPv6.

2 Configuration

2.1 Output additional ports in SYSINFO at the console

As of HiLCOS version 9.00, the `sysinfo` command also outputs the numbers of the following ports:

- HTTP
- HTTPS
- TELNET
- TELNET-SSL
- SSH
- SNMP
- TFTP

2.2 Sorted display of a menu on the console

As of HiLCOS 8.90 you have the option of sorting the output of the menu items by using the argument `-s`.

Command	***Description***
`dir|list|ls|llong [-a] [-r] [-s] [<Path>] [<Filter>]`	Displays the current directory content. Possible arguments are: ▶ `-a`: In addition to the content of the query, this also lists the SNMP IDs. The output begins with the SNMP ID of the device followed by the SNMP ID of the current menu. The SNMP IDs of the subordinate items can be read from the individual entries. ▶ `-r`: Also lists all subdirectories as well as the tables they contain.

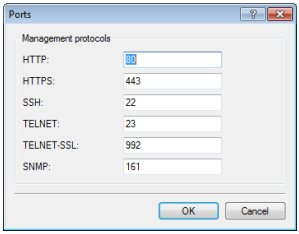
Command	*Description*
	▶ `-s`: Sorts the display of the current directory; grouped by sub directories, tables, values, and actions; in ascending alphabetical order.

Alternatively, you have the option of setting the default to sorted output using the corresponding setup parameter **Setup** > **Config** > **Sort-menu**.

2.3 Customize the management ports for device access

LANconfig features the option to change the port numbers for the management protocols.

1. Start LANconfig and open the configuration dialog for the device.
2. Switch to the dialog **Management** > **Admin** and click **Ports**.
3. Enter the port numbers for the required management protocols.

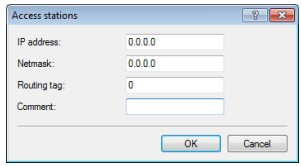


4. Close all open dialog windows by clicking on **OK**.

LANconfig writes the configuration back to the device.

2.4 Comment box for access stations

As of HiLCOS 9.00 you can add comments to the filter entries in the table of access stations.



2.5 Elliptic curve cryptography (ECC)

As of HiLCOS 9.00 you can generate ECDSA keys on a device in addition to the RSA and DSA keys.

SSH key generation with HiLCOS

To generate a key pair consisting of a public and a private key, you enter the following command at the console:

```
sshkeygen [-?|-h] [-t (dsa|rsa|ecdsa)] [-b <Bits>] -f <OutputFile> [-q]
```

-?, -h

Displays a brief help text about the available parameters

-t (dsa|rsa|ecdsa)

This parameter specifies what type of key is generated. SSH supports the following types of keys:

- RSA keys are most widely used and have a length between 512 and 16384 bits. If possible you should work with keys of 1024 to 2048 bits in length.
- DSA keys follow the Digital Signature Standard (DSS) set down by the National Institute of Standards and Technology (NIST) and are typically used in environments which are required to comply with the Federal Information Processing Standard (FIPS). DSA and DSS keys are always 1024 bits long, but they are slower to process than a corresponding RSA key.
- ECDSA keys are a variant of DSA keys, whereby the device uses elliptic curves for key generation (elliptic curve cryptography, ECC). ECC is an alternative to the conventional signature and key exchange techniques such as RSA and Diffie-Hellman. The main advantage of

elliptic curves is that their mathematical properties offer the same key strength as RSA or Diffie-Hellman but with a significantly shorter key length. This provides for better hardware performance. ECC and its integration in SSL and TLS are described in RFCs 5656 and 4492.

If no type is specified, the command generates an RSA key by default.

-b <bits>

This parameter sets the length of the RSA key in bits. If you do not specify a length, the command produces a key with a length of 1024 bits by default.

-f <OutputFile>

These parameters specify the mounting point of the generated key file in the device file system. The choice of mounting point depends on what type key you are generating. The choices available to you are:

- **ssh_rsakey** for RSA keys
- **ssh_dsakey** for DSA keys
- **ssh_ecdsakey** for ECDSA keys

-q

This parameter enables the 'quiet' mode for the key generation. If you set this parameter, HiLCOS overwrites any existing RSA or DSA keys without asking; there is no information about the progress of the operation. You can, for example, use this parameter in a script to suppress any security prompts for the users.

3 IPv6

3.1 IPv6 support for RAS services

As of firmware version 8.90, RAS remote stations are able to login via IPv6. The configuration is done in LANconfig under **IPv6** > **General** and the setup of prefix pools under **IPv6** > **Router advertisement**.

3.1.1 RAS interfaces

There are basically two ways to manage the configuration of RAS remote stations:

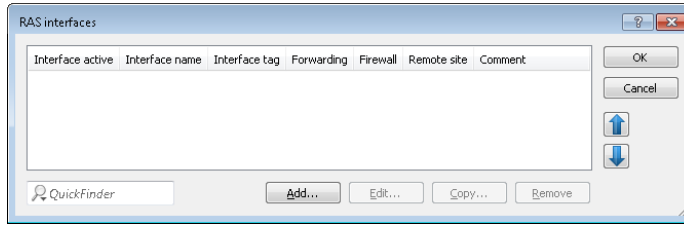
The user data or the configurations are locally stored on the device.

The advantage of this alternative is that a RADIUS server is not necessary, which reduces the management and cost of the network infrastructure.

The user data or the configurations are stored on an external RADIUS server.

The advantage of this alternative is the centralized user management for extensive distributed network scenarios.

For RAS access via IPv6, you must also set up the corresponding **RAS interface**.



Entries in the **RAS interfaces** table have the following meaning:

- **Interface active**: Enable or disable this interface here.
- **Interface name**: Here you define the name of the RAS interface that the IPv6 remote sites use for access.
- **Interface tag**: The interface tag that you enter here is a value that uniquely identifies the network. All packets received by this device on this network will be internally marked with this tag. The interface tag enables the routes which are valid for this network to be separated even without explicit firewall rules.
- **Forwarding**: Enables or disables the forwarding of data packets to other interfaces.
- **Firewall**: If the global firewall is enabled for IPv6 interfaces, you can disable the firewall for each interface individually here. To globally enable the firewall for all interfaces, navigate to **Firewall/QoS** > **General** and check the option **IPv6 firewall/QoS enabled**.

  Attention: If you disable the global firewall, the firewall of an individual interface is also disabled. This applies even if you have enabled this option.

- **Remote site**: Specify the remote site or a list of remote sites for RAS dial-in users.

  The following values are possible:

  - A single remote station from the tables under **Setup** > **WAN** > **PPTP-Peers**, **Setup** > **WAN** > **L2TP-Peers** or **Setup** > **PPPoE-Server** > **Name-list**.
  - The wildcard "*" makes the interface valid for all PPTP, PPPoE and L2TP peers.
  - The "*" wildcard as a suffix or prefix of the peer, such as "COMPANY*" or "*TUNNEL" .

  Using the wildcards you can create several peers for IPv6 RAS services based on so-called template interfaces These template interfaces can be used as normal interfaces for IPv6 services such as DHCPv6 server or router advertisements. For example, using these, a group of RAS interfaces can be provided from an IPv6 prefix pool.

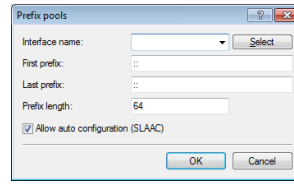
- **Comment**: Enter a descriptive comment for this entry.

Information on RADIUS attributes for IPv6 RAS services can be found under *RADIUS attribute extensions for IPv6 RAS services* on page 18.

Note: If RAS clients are to be delegated to an IPv6 DNS server or are to receive their prefixes by prefix delegation, you must create a corresponding entry in the table **DHCPv6 networks** under **IPv6** > **DHCPv6**.

Note: If you wish to authenticate a user by PPP list, you navigate to **Communication** > **Protocols** > **PPP list** and enable the option **Activate IPv6 routing** for that user.

3.1.2 Prefix pools



This table contains the pools of prefixes which RAS users receive when they connect remotely via IPv6. The following settings are possible:

Interface name

Specifies the name of the RAS interface that is valid for this prefix pool.

First prefix

Specifies the first prefix in the pool that is assigned to remote users by the router advertisement, e.g., "2001:db8::". Each user is assigned precisely one /64 prefix from the pool.

Last prefix

Specifies the last prefix in the pool that is assigned to remote users by the router advertisement, e.g. '2001:db9:FFFF::'. Each user is assigned precisely one /64 prefix from the pool.

Prefix length

Specifies the length of the prefix that the remote user is assigned by the router advertisement here. The size of the dial-in pool depends directly on the first and last prefix. Each user is assigned precisely one /64 prefix from the pool.

Attention: In order for a client to be able to form an IPv6 address from the auto-configuration prefix, the prefix length must always be 64 bits.

SLAAC

Specifies whether the prefix can be used for a stateless address auto-configuration (SLAAC).

3.2 RADIUS attribute extensions for IPv6 RAS services

The RADIUS client can request RADIUS attributes, such as the “Framed-IP-Address”, from an external RADIUS server and provide these, for example, to a PPPoE server in order to authenticate them at PPPoE, PPTP or L2TP servers. The device accepts the following attributes in access-accept messages:

96

Framed-Interface-ID

This attribute conveys the IPv6 interface identifier that should be configured for the user in the IPv6CP.

97

Framed-IPv6-Prefix

Prefix, which is sent to the user via router advertisements.

99

Framed-IPv6-Route

This attribute conveys the route to be used for this user. The device supplements the IPv6 routing table with this route and the next hop to this user.

100

Framed-IPv6-Pool

This indicates the IPv6 pool from which a prefix is to be taken for the user. The IPv6 pool is referenced by its name and must be present under **IPv6** > **Router advertisement** > **Prefix pools**.

123

Delegated-IPv6-Prefix

Prefix, which is sent to the user via DHCPv6 prefix delegation.

The newly available RADIUS attributes are implemented according to RFCs 3162 and 4818. An example for a PPP user `test` with IPv6 in the FreeRADIUS is as follows:

```
test Cleartext-Password := "1234"
 Service-Type = Framed-User,
 Framed-Protocol = PPP,
 Framed-IPv6-Prefix = "fec0:1:2400:1::/64",
 Delegated-IPv6-Prefix = "fec0:1:2400:1100::/56",
 Framed-IP-Address = 172.16.3.33,
```

The user "test" in a dual-stack PPP session receives the IPv4 address 172.16.3.33, the prefix fec0:1:2400:1::/64 via router advertisement, and the prefix fec0:1:2400:1100::/56 via DHCPv6 prefix delegation.

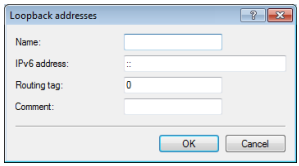
3.3 Loopback addresses for IPv6

As of HiLCOS 8.90, you can use IPv6 loopback addresses as the sender address for ping commands at the command line.

Parameters	Meaning
`-6 <Loopback-Interface>`	Sets an IPv6 loopback interface as the sender address.

3.3.1 Loopback addresses

IPv6 loopback addresses can be specified in the **Loopback addresses** table. The device sees each of these addresses as its own address, which is also available if a physical interface is disabled, for example.



Entries in the **Loopback addresses** table have the following meaning:

- **Name**: Enter a unique name for this loopback address.
- **IPv6 address**: Enter a valid IPv6 address here.
- **Routing tag**: Here you specify the routing tag of the network that the loopback address belongs to. Only packets with this routing tag will reach this address.
- **Comment**: You have the option to enter a comment here.

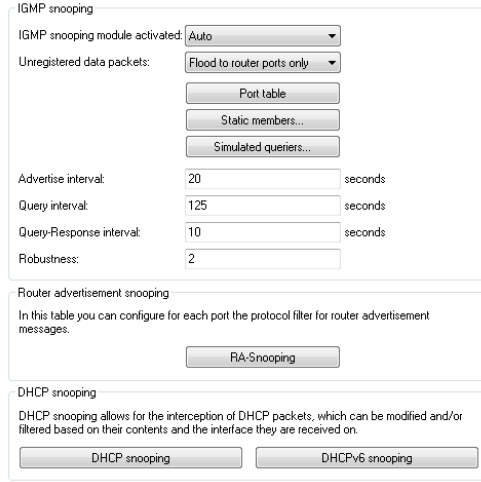
3.4 Lightweight DHCPv6 relay agent (LDRA)

Unlike a DHCPv6 relay agent, which has the full IPv6 features (such as ICMPv6) and can route data packets on the network (layer 3), a lightweight DHCPv6 relay agent as per RFC 6221 enables only the creation and forwarding of relay-agent information between DHCPv6 clients and DHCPv6 servers (layer 2).

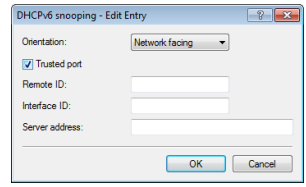
In contrast to DHCPv4 snooping, the LDRA does not simply append the DHCPv6 packets with information about the relay agent: Instead, it packs the message from the client into a separate option, prepends its own relay-agent header and then forwards this DCHPv6 packet with its supplementary information to the DHCPv6 server (relay forward message).

The DHCPv6 server evaluates this data packet and sends a similarly packaged response to the relay agent. This then extracts the message and sends it to the requesting client (relay-reply message).

In LANconfig you can set up DHCPv6 snooping for each interface under **Interfaces** > **Snooping** and a click on **DHCPv6 snooping**.



After selecting the appropriate interface, you can set the following:



Orientation

This is where you enable or disable DHCPv6 snooping. The following options are possible:

- **Network facing**: The LDRA uses this interface to communicate with a DHCPv6 server.
- **Client facing**: The LDRA uses this interface to communicate with DHCPv6 clients connected to the network.

The default setting **Network facing** disables the LDRA.

Trusted port

With this option enabled, the LDRA forwards DHCP requests from clients and also DHCP responses from DHCP servers. If this interface is classified as not trusted, the LDRA discards DHCPv6 requests to this interface.

Similarly, the LDRA does not forward DHCPv6 responses with the wrong interface ID to the client.

Remote ID

According to RFC 4649, the remote ID uniquely identifies the client making a DHCPv6 request.

Interface ID

The interface ID uniquely identifies the interface used by a client to make a DHCPv6 request.

Server address

You can set the IPv6 address of a DHCPv6 server here.

Note: Leave this field blank if you want to receive responses from all DHCPv6 servers on the network. Otherwise the LDRA reacts only to DHCPv6 responses from the server you have specified. In this case, the LDRA discards responses from other DHCPv6 servers.

You can use the following variables for **Remote ID** and **Interface ID**:

- %%: Inserts a percent sign.
- %c: Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- %i: Inserts the name of the interface where the relay agent received the DHCP request.
- %n: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- %v: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- %p: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, %p and %i are identical.
- %s: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.

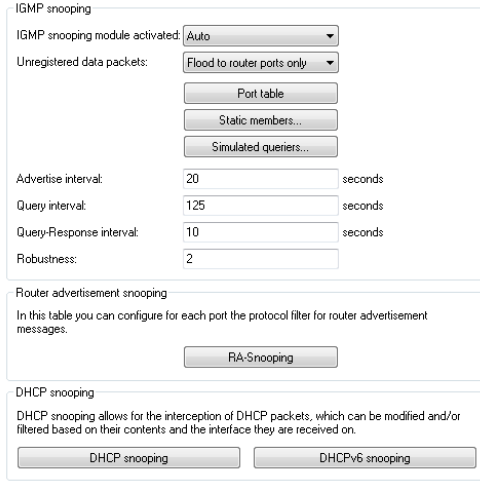
- %e: Inserts the serial number of the relay agent, to be found for example under **Management** > **General**.

3.5 Router advertisement snooping

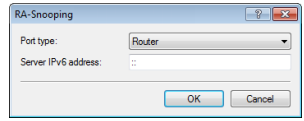
In an IPv6 network, router advertisements are sent by routers, either periodically or upon request, to present themselves as a gateway for networked clients. As with DHCPv4, attackers can use this mechanism to deliver a fake network configuration to the requesting clients.

With RA snooping, the device mediates router advertisements from routers only, and not from clients. By specifying the address of a router, the router advertisements can be restricted to one specific router as the broadcaster.

In LANconfig you can set up RA snooping for each interface under **Interfaces** > **Snooping** and a click on **RA snooping**.



After selecting the appropriate interface, you can set the following:



Port type

Specify the preferred interface type here. The following options are possible:

- **Router**: The device mediates all of the RAs arriving at this interface (default).
- **Client**: The device discards all of the RAs arriving at this interface.

Router-Address

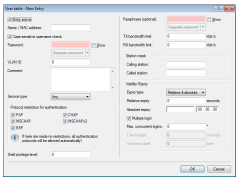
If you have selected the interface type **Router**, enter an optional router address here. If you specify a router address, the device will only mediate RAs from that router.

With the interface type **Client** selected, the device ignores this input field.

4 RADIUS

4.1 New attribute in the RADIUS server, shell privilege level

As of HiLCOS version 8.90, the RADIUS server supports a vendor-specific RADIUS attribute to communicate the privilege level of the user in a RADIUS-Accept. This attribute can be specified under **RADIUS Server** > **General** > **User table**.



4.1.1 Using RADIUS to login to the HiLCOS management GUI

Currently users can login to the management interface of a device by means of RADIUS, TACACS+, or the internal user management. With RADIUS, this is possible for the following protocols:

- Telnet
- SSH
- WEBconfig
- TFTP
- Outband

Note: RADIUS authentication via SNMP is not currently supported.

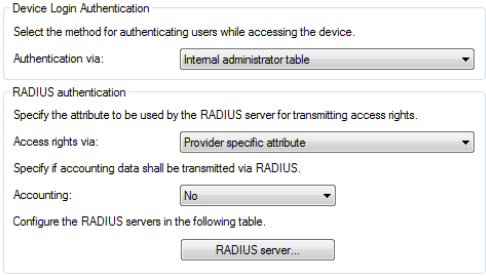
Note: A RADIUS authentication via LL2M is not supported, because LL2M requires plain text access to the password that is stored in the device.

The RADIUS server handles user management in terms of authentication, authorization and accounting (triple-A protocol), which greatly simplifies the management of admin access accounts in large network installations with multiple routers.

Logging in via a RADIUS server follows this procedure:

1. At login, the device sends the user's credentials to the RADIUS server on the network. The server data are stored in the device.
2. The server checks the credentials for validity.
3. If the data is invalid, the server sends a corresponding message to the device, which aborts the login process with an error message.
4. If the credentials are valid, the server returns the access rights and privileges to the device and the user then has access to the approved features and directories.
5. If the user's sessions are subject to budgeting by the RADIUS server (accounting), the device stores the session data including the start time, end time, user name, authentication mode and, if available, the port used.

In LANconfig you can set the authentication method under **Management** > **Authentication**.



Device login authentication

In the section **Device login authentication** you select the method for authenticating users when they access the device management GUI:

- **Internal administrator table**: The device handles over the overall user administration including the user login name, password, access rights, and privileges.
- **RADIUS**: User administration is handled by a RADIUS server on the network.
- **TACACS+**: User administration is handled by a TACACS+ server on the network.

RADIUS authentication

In the **RADIUS authentication** section you specify the necessary RADIUS server data and the additional administrative data.

Access rights via

The RADIUS server stores the user authorization. When a request arrives, the RADIUS server returns the access rights, privileges and the login data to the device, which then logs in the user with the appropriate rights.

Normally access rights are set in the RADIUS management privilege level (attribute 136), so that the device only needs to map the returned value to its internal access rights. However, it may be that the RADIUS server additionally needs to transfer privileges, or that attribute 136 is already used for other purposes and/or for vendor-specific authorization attributes. In this case, the device can evaluate a manufacturer-specific authorization.

- **Provider specific attribute**: The unit evaluates the vendor-specific attribute.
- **Management privilege level attribute**: The unit evaluates the management privilege level attribute from the RADIUS server.
- **Shell privilege attribute**: The unit evaluates the shell privilege attribute from the RADIUS server.

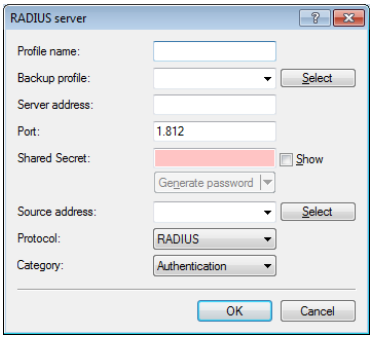
Accounting

Here you specify whether the device should record the user's session.

- **No**: The device does not record the session.
- **Yes:** The device records the session (start, end, username, authentication mode, port).

RADIUS server

You can adjust the RADIUS server settings in this table.



- **Profile name**: Enter a name for the RADIUS server.
- **Backup profile**: Specify the name of the alternative RADIUS server to which the device forwards requests when the first RADIUS server cannot be reached.

  Note: The backup server requires an additional entry in the Server table.

- **Server address**: Enter the IPv4 address of the RADIUS server here.
- **Port**: Specify here the port used by the RADIUS server to communicate with the device.
- **Shared secret**: Enter the password for accessing the RADIUS server and repeat it in the second input field.
- **Sender address**: This is where you can specify an optional sender address to be used by the device instead of the one that would normally be automatically selected for this target address.
- **Protocol**: Specify here the protocol used by the RADIUS server to communicate with the device.
- **Category**: Set the category for which the RADIUS server applies.

5 Public Spot

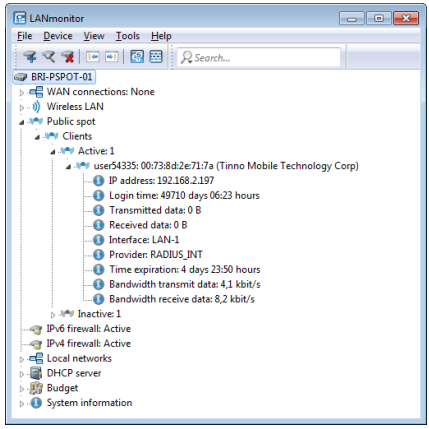
5.1 Number format for Smart Ticket

Starting with version 9.00, HiLCOS checks the entered phone number for invalid characters. Only numbers between 0 and 9 are allowed. The user must enter 5 to 15 numbers (excluding the country code).

5.2 Viewing Public Spot clients

LANmonitor can optionally display detailed information about the clients associated with the Public Spot.

1. Open the menu item **Public Spot** > **Clients**.
2. Double-click on **Active** to display the active clients, or on **Inactive** to display inactive clients.
3. Double-click on a client to retrieve detailed information about it.



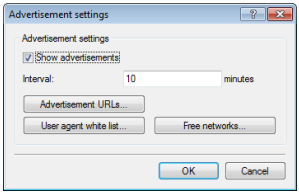
5.3 Displaying advertising to Public Spot users

You can optionally display advertising to Public Spot users at configurable time intervals. The Public Spot shows the advertisement in the normal browser window of the user and not using a pop-up, since all modern browsers normally block pop-ups. In the Public Spot station table, a client can have one of three states:

- Authenticated: The client is logged on and can surf in Internet.
- Unauthenticated: The client is not logged on and cannot surf in Internet.
- Advertisement: The next time a client calls a URL, it is redirected to an advertisement URL.

You have the option to exclude certain networks and user agents from the display of advertisements by means of a whitelist.

1. In the device configuration, select the menu branch **Public Spot** > **Server** and click on **Advertisement settings**.
2. Enable the **Show advertisements** checkbox.



   You can now change the interval between advertisement displays, and also other settings.
3. Under **Interval** you specify the time in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of `0` forwarding occurs directly after login.
4. Click on **Advertisement URLs** to add an advertisement URL. If you add multiple URLs, the Public Spot displays them in sequence after the specified interval.
5. Optional: Click on **User agent white list** to add user agents, which the Public Spot excludes from the display of advertisements.
6. Optional: Click on **Free networks** to add networks, which the Public Spot excludes from the display of advertisements. This can be used in various

ways, for example to enter the automatic search URLs used by the browser, e.g. `*.google.com`. Typically, a browser sends keyboard input at the address bar to a search engine; by setting the exception, the advertisement page does not responding to this.

Note: Login-free networks are generally ad-free networks. There is no need to explicitly include these networks into the whitelist.

7. Close all dialog windows by clicking on **OK**.

Public Spot users will be redirected to an advertisement URL after the specified time interval unless they are using a whitelisted user agent or they are located in a free network.

The timing of the advertisements refers to the session time of the active Public Spot clients. If a client stop sending data for a certain time, then the interval before the Public Spot displays advertising again will be delayed by this time.

5.3.1 Extensions to the RADIUS attributes

The Public Spot additionally evaluates the following vendor-specific RADIUS attributes in the Access Accept of the RADIUS authentication server.

Note: The **Advertisement enabled** switch does not have to be set. It is sufficient if the attribute is present in the RADIUS message.

26

Vendor 2356(LCS) ID 13

LCS-Advertisement-URL

Specifies a comma-separated list of advertisement URLs.

26

Vendor 2356(LCS) ID 14

LCS-Advertisement-Interval

Specifies the interval in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of `0` forwarding occurs directly after login.

5.4 Additional attributes for the XML interface

With HiLCOS 8.90 the scope of the attributes that are available for creating a new user via the XML interface has been extended. The attributes below mostly correspond to the parameters which are also configurable over the RADIUS user table.

The XML interface can now process the following XML elements in the **login request**:

`VLAN_ID` (optional)

Custom VLAN ID assigned by the device to the Public Spot user upon login. After authentication by the RADIUS server, the individual VLAN ID overwrites a global VLAN ID that a user would otherwise obtain from the XML interface.

The value `0` disables use of a VLAN.

`PROVIDER` (occasionally required)

Name of the RADIUS server used by the Public Spot for user authentication and accounting. If you do not specify a RADIUS server, the Public Spot uses the server configured globally for the module.

This XML element is mandatory if you

- have configured multiple RADIUS servers for the Public Spot module.
- want to use the XML interface without RADIUS authentication but with RADIUS accounting.

Specifying this XML element is otherwise optional.

Important: The referenced RADIUS server must be present in the configuration.

`TXRATELIMIT` (optional)

Maximum bandwidth (in kbps) provided to the Public Spot user for the uplink.

`RXRATELIMIT` (optional)

Maximum bandwidth (in kbps) provided to the Public Spot user for the downlink.

SECONDSEXPIRE (optional)

The maximum online time for a user account in seconds. The user can use this duration of access time until a relative or absolute expiry time (if set) is reached.

The value `0` switches off the monitoring of the time budget.

TRAFFICEXPIRE (optional)

Maximum data volume for a user account in bytes. The user can use this data volume until a relative or absolute expiry time (if set) is reached.

The value `0` switches off the monitoring of the data volume.

5.5 Dynamic change of a user session via the XML interface

If a Public Spot user has to authenticate only and no further changes are required throughout the login, then the parameter `RADIUS_LOGIN` will meet your needs. On the other hand, if you need to change the attributes of an ongoing session for a Public Spot user, you have the option of using `RADIUS_CoA`. To implement a change, your external hotspot gateway sends a `RADIUS-CoA-Request` to the Public Spot, which directly transfers the changes in it to the **Station table** under **Status** > **Public-Spot**.

One application for CoA messages is the automatic throttling of bandwidth: If a Public Spot user has consumed his/her volume budget, an external hotspot gateway is able to throttle the user's bandwidth by evaluating the accounting data and sending a CoA message to the Public Spot.

The XML messages for negotiations between the hotspot gateway and the Public Spot appear as follows:

RADIUS-CoA-Request

The external gateway sends the data with the session change to the Public Spot. The Public Spot then changes the session data in the station table for the authenticated user 'user2350'.

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<PUBLICSPOTXMLINTERFACE>
  <ACCESS_CUBE COMMAND="RADIUS_COA_REQUEST">
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <SUB_PASSWORD>5juchb</SUB_PASSWORD>
    <SUB_MAC_ADDR>00164115208c</SUB_MAC_ADDR>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
  </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

In the example above, the user is assigned a session duration of 3,600 seconds, a transferable data volume of 10,000,000 bytes, and a transmit and receive bandwidth of 100 kbps.

RADIUS-CoA-Response:

The XML interface sens a confirmation to the external hotspot gateway that the session data was changed:

```
<?xml version="1.0" encoding="ISO-8859-1" ?>
<PUBLICSPOTXMLINTERFACE>
 <ACCESS_CUBE ID="WLC_PM" IP="192.168.100.2" COMMAND="USER_STATUS">
    <SUB_STATUS>RADIUS_COA_ACCEPT</SUB_STATUS>
    <SUB_MAC_ADDR>00:16:41:15:20:8b</SUB_MAC_ADDR>
    <SUB_USER_NAME>user2350</SUB_USER_NAME>
    <TXRATELIMIT>100</TXRATELIMIT>
    <RXRATELIMIT>100</RXRATELIMIT>
    <SECONDSEXPIRE>3600</SECONDSEXPIRE>
    <TRAFFICEXPIRE>10000000</TRAFFICEXPIRE>
    <ACCOUNTCYCLE>0</ACCOUNTCYCLE>
    <IDLETIMEOUT>0</IDLETIMEOUT>
    </ACCESS_CUBE>
</PUBLICSPOTXMLINTERFACE>
```

In case of throttling, the change to the user session always affects the quota that is still available to the user. For instance, if the user was logged on for one hour already, then a change of the time quota to six hours means that just five hours remain. If the time quota is less than the time the user is already

logged on, the Public Spot logs out the user and sends a logout message to the hotspot gateway.

6 WLAN

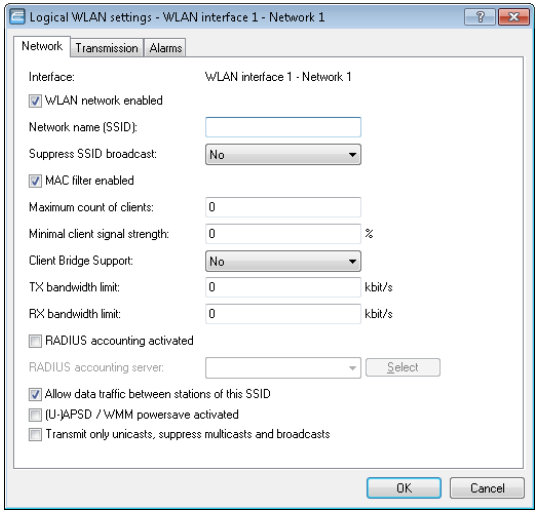
6.1 Support of 802.11ac WLAN interfaces

As of version 8.90, HiLCOS provides support of the 802.11ac standard for devices with the appropriate hardware.

6.2 Specifying client-bridge mode and bandwidth limit for each SSID

As of HiLCOS 8.90 you have the option of specifying the client-bridge mode and bandwidth limits for individual SSIDs.

Changes to stand-alone APs



The following settings are made in LANconfig in **Wireless LAN** > **General** > **Logical WLAN settings** > **Network**.

- **Client-bridge support**

  Enable this option for an access point if you have enabled the client-bridge support for a client station in WLAN client mode ().

  Note: The client-bridge mode only operates between two OpenBAT devices.

- **TX bandwidth limit**

  With this setting, you define the overall bandwidth that is available for transmission within this SSID (limit in kbps). A value of `0` disables the limit.

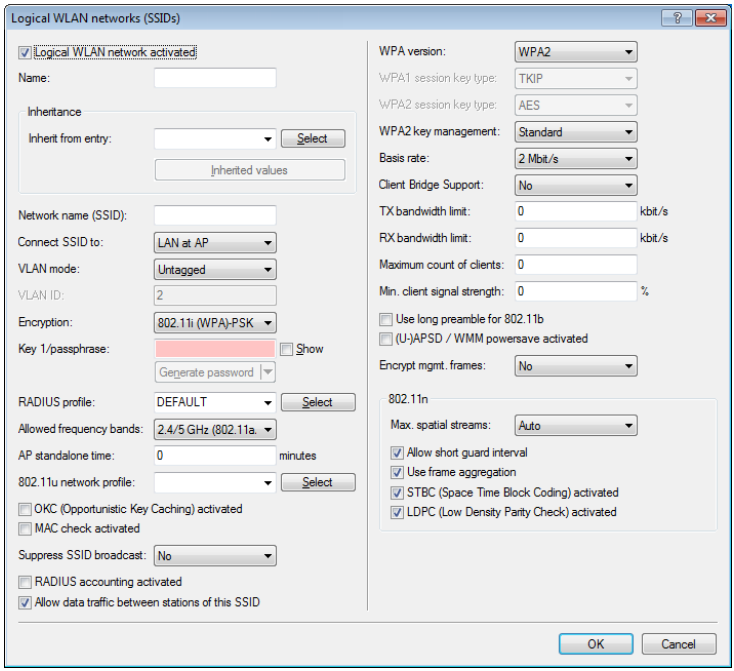
- **RX bandwidth limit**

  With this setting, you define the overall bandwidth that is available in the reception direction within this SSID (limit in kbps). A value of `0` disables the limit.

The settings of this name are thus removed from LANconfig under **Wireless LAN** > **General** > **Physical WLAN settings.** > **Client mode**an also from the following menu items in WEBconfig:

- **Setup** > **Interfaces** > **WLAN** > **Client-Modes** > **Cl.-Brg.-Support**
- **Setup** > **Interfaces** > **WLAN** > **Client-Modes** > **Tx-Limit**
- **Setup** > **Interfaces** > **WLAN** > **Client-Modes** > **Rx-Limit**

Changes to WLCs



The explanations added for a stand-alone AP to the changes in LANconfig also apply in the same manner to a WLC under **WLAN Controller** > **Profiles** > **Logical WLAN networks**.

6.3 Separation of P2P and WLAN/SSID configuration

As of HiLCOS 8.90, the transmission and encryption settings for P2P connections can be configured separately from the settings for the first logical WLAN network of the corresponding physical WLAN interface. P2P devices no longer use a configured SSID as an administrative network for connection establishment and for availability checks ("Alive") of a point-to-point partner. Instead, they now use the fixed SSID ***** P2P INFO *****.

This feature, among others, forms the basis for the structure of *AutoWDS networks*.

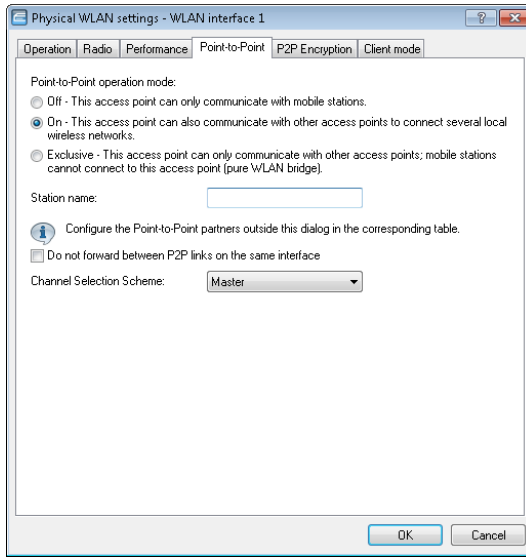
6.3.1 Configuration of P2P connections

In the configuration of point-to-point (P2P) connections, enter the point-to-point operation mode and the channel selection scheme, along with the MAC addresses or station names of the remote sites. The configuration can be done in LANconfig either by using the Setup wizard **Configure WLAN** or manually using the configuration dialog.

The following steps show you how you create an encrypted or unencrypted P2P basic configuration.

Note: Along with a P2P connection, each of the APs automatically operates an SSID ***** P2P INFO *****. This SSID works purely as an administrative network for establishing the connection and for the availability check ("Alive") of a point-to-point partner. It is not possible for the WLAN clients to connect to this network.

1. Open the configuration dialog for the device that is to operate as the P2P master or P2P slave, and navigate to the page **Wireless LAN** > **General** > **Physical WLAN settings**.
2. Select the WLAN interface which you want to use explicitly for the P2P connection and move to the tab **Point-to-Point**.



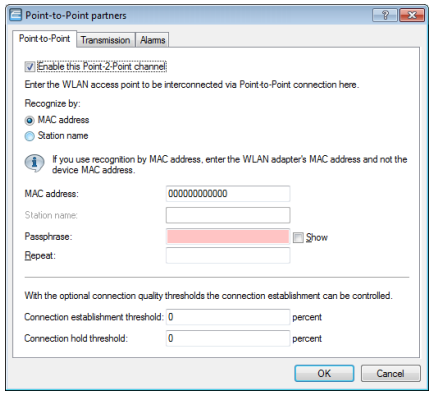
3. Enable the desired **Point-to-point operation mode**, such as **On**.
4. Set the **Channel selection scheme** to **Master** or **Slave**.
5. Optional: If the remote site should identify the physical interface by an alias and not the MAC address, then enter a corresponding descriptor into the field **Station name**, for example `P2P_MASTER` or `P2P_SLAVE`.
6. Optional: Adjust the settings on the tab **P2P encryption** for the IEEE 802.11i encryption of the P2P connection, if necessary.

   IEEE 802.11i can attain a significant increase in the security of WLAN point-to-point connections. All of the advantages of 802.11i such as the simple configuration and the powerful encryption with AES are thus available for P2P mode, as are the improved security of the passphrase from the Enhance Passphrase Security (LEPS).

   The setting options are practically identical with those of the physical WLAN interfaces, see *WPA and private WEP settings*. By default, P2P encryption is enabled and filled-out with meaningful values.

   Note: In HiLCOS versions prior to 8.90, the settings for encryption are tied to the settings for the first logical WLAN network on the corresponding physical WLAN interface (i.e. WLAN-1 if you are using the first WLAN module for the P2P connection, WLAN-2 if you are using the second WLAN module for an access point with two WLAN modules). In this case, you find the settings under **Wireless LAN** > **802.11i/WEP** > **WPA or private WEP settings**.

7. Close the dialog with **OK** and under **Point-to-Point partners** on the same page of the configuration dialog select a logical P2P connection, such as **P2P-1-1**.



8. Enable the selected P2P channel on the **Point-to-Point** tab and specify whether the device identifies the remote station using a **MAC address** or a **Station name**. Here you then enter either the MAC address of the physical WLAN interface which the remote station uses for the P2P connection, or its station name accordingly.
   You will find the WLAN MAC address on a sticker located under each of the antenna connectors on the housing of the device. Only use the string that is marked as the "WLAN-MAC" or "MAC-ID". The other addresses that may be found are not the WLAN MAC address but the LAN MAC address.

   Alternatively, you will also find the MAC address in the status menu under **WLAN** > **Interfaces** > **MAC-Address**.

9. In **Passphrase**, enter a shared secret of at least 8 characters (recommended: 32 characters), which is used to additionally encrypt the P2P connection. The P2P encryption must be enabled for this (see above).
   When set as P2P Master, the passphrase entered here will be used to check the Slave's authorization to access. When set as P2P Slave, the access point transfers this information to register with the remote site.
10. Optional: Move to the **Transmission** tab to enter the limits and settings for packet transmission.

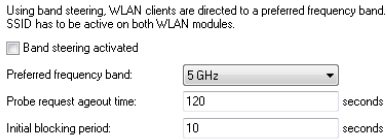
    The setting options are practically identical with those of the logical WLAN networks (see *Transmission settings*). By default, all parameters are adjusted for optimization and automatic operation.

11. Close the dialog with **OK** and save the configuration to your device.

12. You continue by performing the corresponding configuration steps for the remote station (slave or master).

6.4 Band steering with delayed scan at 2.4 GHz

With an AP as of HiLCOS version 8.90, you can delay the band steering to the 2.4-GHz band under **Wireless LAN** > **Band steering**.



Initial block time

If an access point with a 5-GHz DFS radio module is put into operation for the first time, and also following a restart, it cannot detect any dual-band capable WLAN clients during the DFS scan. As a result, the access point cannot direct a WLAN client to a preferred 5-GHz band. Instead, the 2.4-GHz radio module would answer the client request and forward it to the 2.4-GHz band.

By setting an initial block time, the radio module that is configured to 2.4-GHz only responds to client requests after the specified delay. The default value is 10 seconds.

The delayed response to the 2.4GHz probes causes WLAN clients, which would otherwise expect to find an access point in the 2.4GHz band, to scan again in the 5GHz band.

Note: Registration of a purely 2.4-GHz WLAN client also occurs after this delay time. If no 5-GHz WLAN clients are present in the network, the delay time should be set to 0 seconds.

On the WLC you activate client steering for an AP under **WLAN controller** > **Profiles** > **Physical WLAN parameters** using the selection list **Client steering**. Refer to section *Client steering by WLC* on page 120 for further information on this.

6.5 WPA2 with AES as factory setting

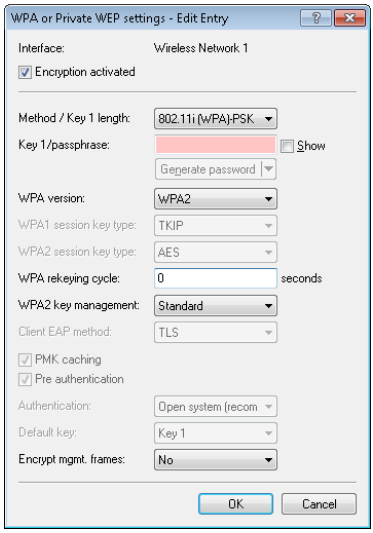
As of HiLCOS 8.90, WPA2 encryption in LANconfig and HiLCOS uses the session key type AES by default.

6.6 WLAN protected management frames (PMF)

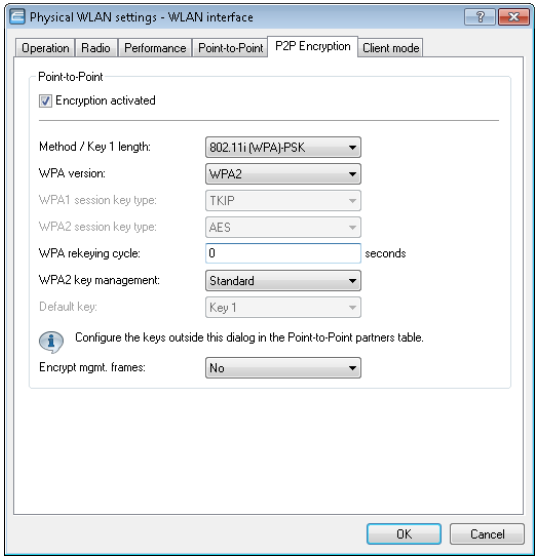
By default, the management information transmitted on a WLAN for establishing and operating data connections is unencrypted. Anybody within a WLAN cell can receive this information, even those who are not associated with an access point. Although this does not entail any risk for encrypted data connections, the injection of fake management information could severely disturb the communications within a WLAN cell.

The IEEE 802.11w standard encrypts this management information, meaning that potential attackers can no longer interfere with the communications without the corresponding key.

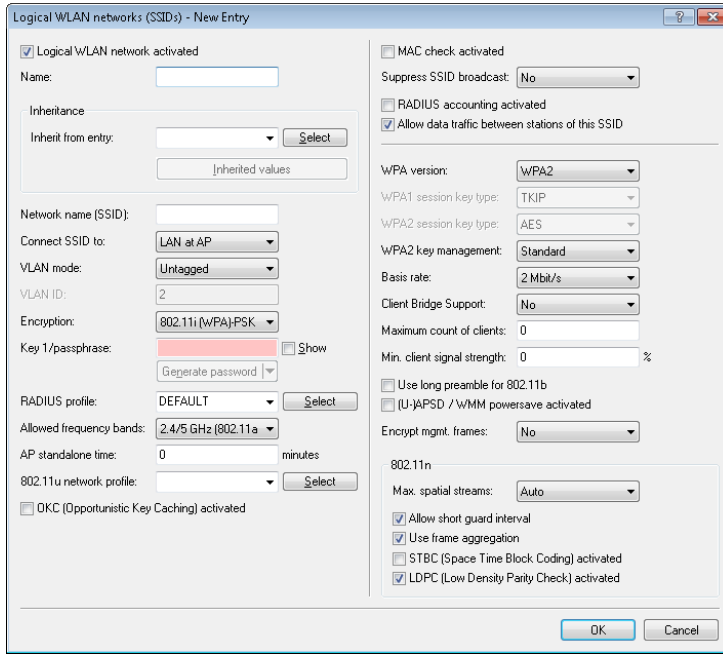
To enable protected management frames for a logical WLAN interface, in LANconfig you navigate to **Wireless LAN** > **802.11i/WEPWPA or Private WEP settings**, open the configuration of the appropriate WLAN interface and click the appropriate option in the selection list **Encrypt mgmt. frames**.



To encrypt the management frames for P2P connections between base stations, in LANconfig you navigate to **Wireless LAN** > **General**, click on **Physical WLAN settings** and click the appropriate option in the selection list **Encrypt mgmt. frames**.



To manage the encryption of management frames for a WLAN controller, in LANconfig you navigate to **WLAN Controller** > **Profiles**, click on **Logical WLAN networks (SSIDs)** and click the appropriate option in the selection list **Encrypt mgmt. frames**.



The following options are available in each of these configurations:

No

The WLAN interface does not support PMF. The WLAN management frames are not encrypted.

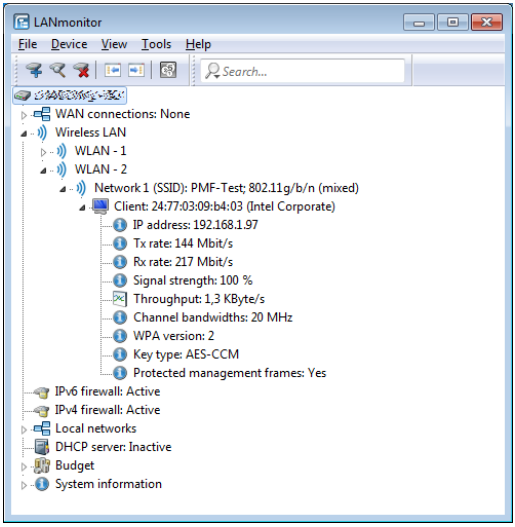
Mandatory

The WLAN interface supports PMF. The WLAN management frames are always encrypted. It is not possible to connect with WLAN clients that do not support PMF.

Optional

The WLAN interface supports PMF. Depending on the WLAN client's PMF support, the WLAN management frames are either encrypted or unencrypted.

LANmonitor displays information about WLAN management frame encryption below each client.



6.7 Opportunistic key caching (OKC)

Authentication of wireless clients using EAP and 802.11X has become standard in corporate networks, and these methods are becoming even more widespread with the integration of the Hotspot 2.0 specification for public Internet access. The disadvantage of 802.11X authentication is the significantly longer time between login and connection, because up to twelve data packets have to be exchanged between the WLAN client and the access point. For most applications, which are all about data exchange, this may not be particularly important. However, for time-critical applications such as Voice over IP, it is important that the authentication at neighboring WLAN radio cells does not affect communication.

To counteract this, authentication strategies such as PMK caching and pre-authentication have become established, although pre-authentication does not fix all of the problems. On the one hand, there is no guarantee that the WLAN client can recognize whether the access point can perform pre-authentication. On the other hand, pre-authentication causes considerable load on the RADIUS server, which needs to handle the authentication of all clients and all access points in the WLAN.

Opportunistic key caching delegates the key management to a WLAN controller, or to a central switch, which manages all of the access points in the network. If a client logs on to an access point, the WLAN controller behind it works as an authenticator to manage the keys and send the PMK to the access point, which is ultimately received by the client. If the client moves to another cell, it uses this PMK and the MAC address of the new access point to calculate a PMKID. It then send this to the new access point in the hope that OKC is enabled there (therefore "opportunistic"). If the access point cannot handle the PMKID, then it negotiates an 802.11X authentication with the client in the usual manner.

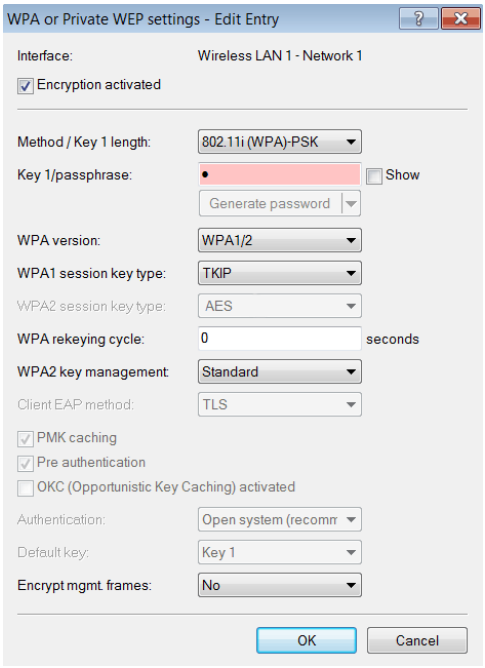
A OpenBAT access point can even perform OKC if the WLAN controller is temporarily unavailable. In this case, it stores the PMK and sends this to the WLAN controller when it becomes available again. Ultimately it sends the PMK to all of the access points in the network, which allows clients to use OKC to login after a change of radio cell.

To use the OKC function it is necessary to activate OKC on both the access point and the client side. For further information about activating an access point operating in WLAN mode **Client** or **Station**, see *Tutorial: Activating OKC on an AP / the client side* on page 47. If you manage your access points with WLC (WLAN operation type **Managed**), you can find informations under "Logical WLAN Networks".

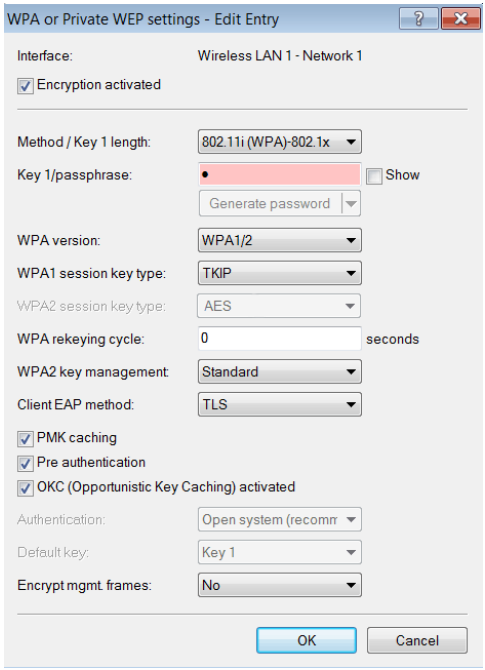
6.7.1 Tutorial: Activating OKC on an AP / the client side

You have an OpenBAT in Access Point / Client Mode. In the following you will find the configuration described for an OpenBAT with a WLAN module with an enabled logical WLAN network. For an OpenBAT with 2 WLAN modules, carry out the following steps for both WLAN modules similarly.

1. Open the view **Wireless-LAN** > **802.11i/WEP** > **WPA or Private WEP settings.**



2. Select **Wireless LAN 1 Network 1** and click **Edit...**.
3. Select **802.11i (WPA)-802.1x as Method/Key 1 type**.
4. Enable the option **OKC (Opportunistic Key Caching)**.



You have enabled OKC.

Note:

If OKC is enabled, **Pre authentication** will be automatically disabled even if its checkbox is selected.

6.8 Wireless IDS

The implementation of WLAN within industrial networks introduces a new class of threats to network security. Radio signals penetrate walls and may reach much further than required. This presents new opportunities for unauthorized users to disrupt the network.

Hirschmann is aware of these threats and supports users through their Wireless Intrusion Detection System (Wireless IDS) by detecting and averting such attacks. Typical attacks on a WLAN network have characteristic patterns.

6.8.1 Wireless IDS Counter

The Wireless Intrusion Detection System provides APs with the ability to detect potential intrusion attacks and provide warnings to the network management software when the attack activities exceed the corresponding user-defined threshold value/interval.

The default threshold values in HiLCOS 9.00 are guidelines which may not be suitable for your particular application. The threshold values for your application depend on the environmental conditions of your AP. Hirschmann therefore recommends adapting the threshold values to your environmental conditions.

Frame counter	**Threshold value factory setting**	**Time interval factory setting (1 interval corresponds to 1 second)**
EAPOL Start	250	10
Broadcast Probe	500	10
Broadcast Deauthenticate	2	1
Deauthenticate	250	10
Associate Request	250	10
Re-Associate Request	250	10
Authenticate Request	250	10
Dis-Associate Request	250	10

A reference measurement is required in order to adapt the counters to the environmental conditions. Suitable programs for this are available for free. One such program is Wireshark.

In many countries authorization from the network operator is required for intercepting radio transmission and for saving and processing data gained from this. Unauthorized recording, storing as well as forwarding of data is subject to a penalty in many countries.

6.8.2 Wireless IDS Types of Attack

Attacks on a WLAN can be characterized by the following properties:

- the target of the attack (AP or client)
- how many targets the attack contained (one or several)
- the type of attack

Some attacks are virtually impossible to avoid as they exploit mechanisms which by their design enable the WLAN to be constructed in the first place. These attacks, which are virtually impossible to prevent, include, e. g., disruption of radio transmission using an interference source.

Types of attack:

- Denial-of-service attacks (DoS) aim to shutdown a service.
- Man-in-the-middle attacks (MitM) aim to intervene between 2 subscribers. Under certain conditions the attacker is then able to intercept radio transmission of both subscribers involved and manipulate the data exchanged.
- SSID attacks (SSID) aim to detect a disabled SSID. A disabled SSID improves safety by means of concealment.

Name of attack	***Target of attack (AP, client, other)***	***Number of targets (one or several)***	***Types of attacks***
EAPOL-Start	Other (infrastructure)	one	DoS
Deauthentication broadcast	Client	several	DoS, MitM SSID
Probe request flood	AP	one	DoS
Disassociation flood	Client	one	DoS
Deauthentication flood	Client	one	DoS, SSID
Association / authentication flood	Client	one	DoS

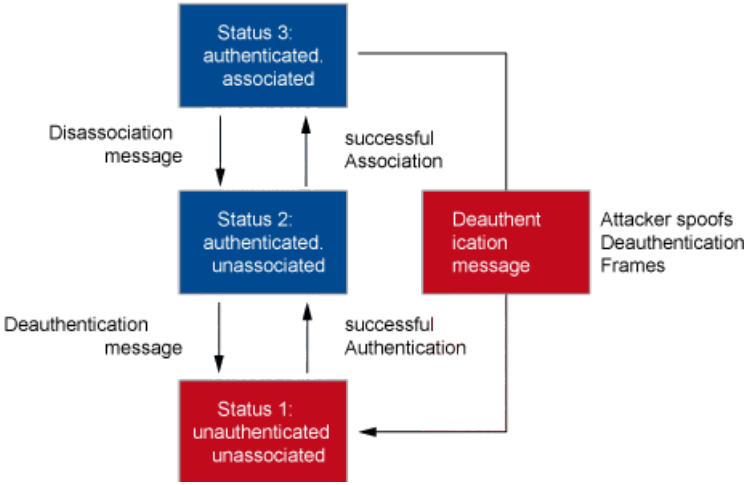
Table 1: Type of attack on WLAN

EAPOL-Start (Extensible Authentication Protocol over LAN): If an AP receives an EAPOL-Start frame, it starts the identification process and allocates

resources internally to the new client. An attacker can generate a lot of EAPOL-Start frames to exhaust the access point interval resource and overload the RADIUS server.

Deauthentication broadcast: An attacker sends a spoof deauthentication frame with broadcast destination address to the network. Clients that receive the frame will be deauthenticated and re-authentication to the AP is required. Management frames that include deauthentication are not protected and are sent in clear text. The described attack is thus easy to carry out. Data communication between the AP and the clients is not possible until the clients reauthenticate.

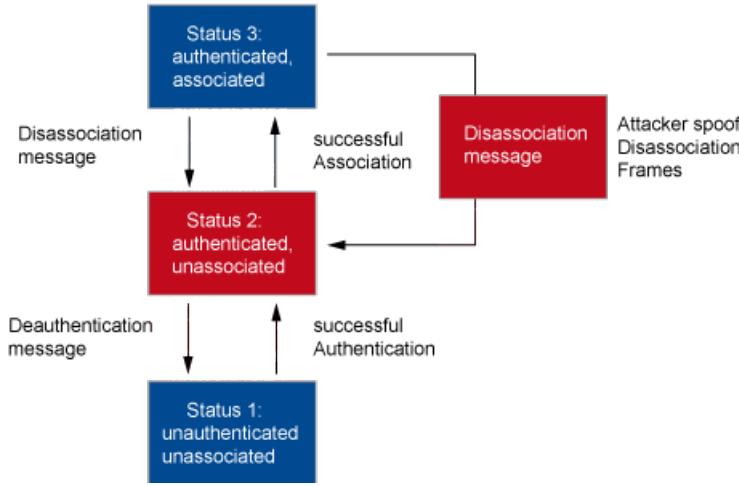
Figure 1: Behavior of a Client during Deauthentication



Probe request flood: An attacker continually sends probe requests to the network. Basically, probe requests are frames used by clients to ask: “Is there a WLAN here?" Probe responses are sent by the APs to reply “Yes, there's a WLAN here with SSID”. This is a mechanism for discovering WLAN services in WLAN networks. If the attacker sends sufficient probe requests, the AP will be overloaded with these probe requests and the wireless medium will be flooded with probe responses.

Disassociation flood: An attacker spoofs disassociation frames in order to log off a client from the AP. All clients affected then attempt to reassociate with the AP. No data communication is possible until the clients reassociate.

Figure 2: Behavior of a Client during disassociation



Deauthentication flood: An attacker continually sends spoof deauthentication frames from the AP to a client. Similarly, the client will be deauthenticated and data communication will be terminated until the client reassociates to the AP.

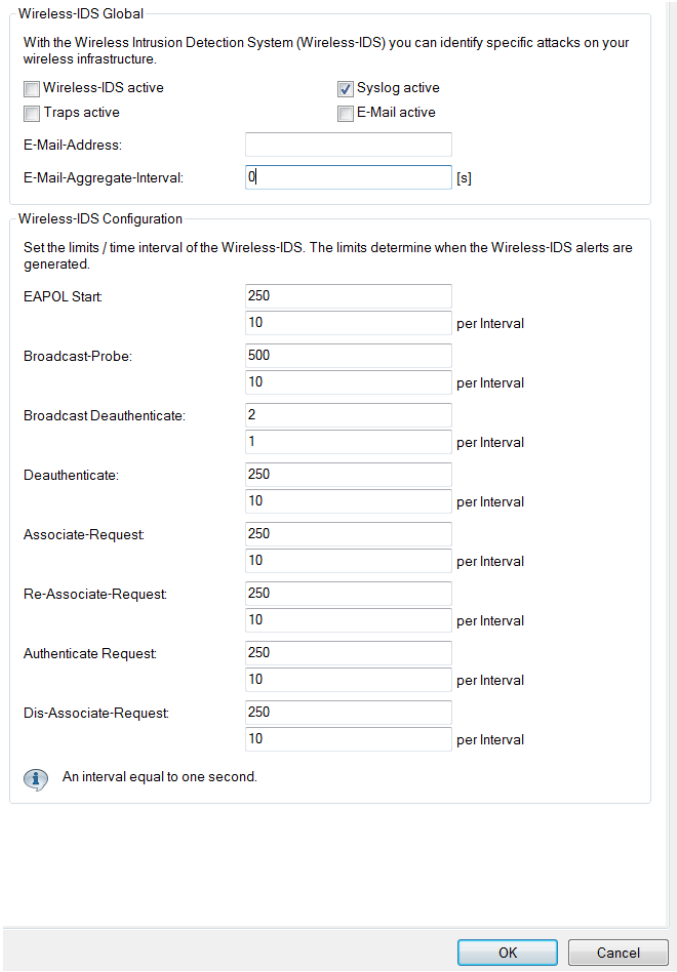
Association / authentication flood: An attacker continually sends association or authentication frames to the AP. This overloads the AP's association/authentication table.

6.8.3 Tutorial: Configuring Wireless IDS

Carry out a reference measurement at the location where the WLAN is used.

To activate and configure the Wireless IDS proceed as follows:

1. Open the view **Wireless LAN** > **Wireless IDS.**



2. Enable the option **Wireless-IDS active**.
3. In order to log wireless IDS function alerts, enable the option **Traps active**.
4. In order to receive e-mail notifications, enable the option **E-mail active** and enter the relevant e-mail address.

   For successful transmission of access data as an e-mail, a valid SMTP account must be set up under **Log & Trace** > **SMTP Account** and **Log & Trace** > **SMTP Options** .
5. Set the threshold value/interval according to your reference measurement.

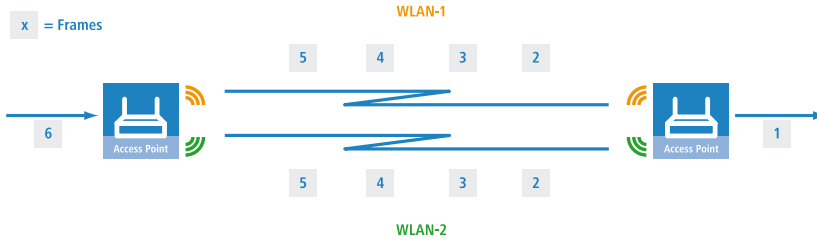
You have activated and configured Wireless IDS.

6.9 Redundant connections using PRP

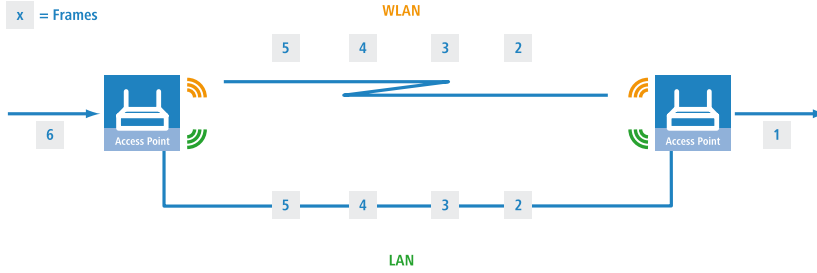
Applications that are sensitive to connection failures require uninterrupted communications. Examples are to be found in automation, transport and mobile applications.

As of HiLCOS 8.90, you have the option of operating redundant connections in your WLAN by means of the parallel redundancy protocol (PRP). Redundant point-to-point links offer you a high level of failover reliability.

PRP achieves high failover reliability by sending twin packets over 2 independent WLANs. While 1 WLAN is active, PRP transports data packets.



You can choose to implement PRP with only WLAN interfaces. Alternatively, you can use one wired and one WLAN interface to implement PRP.



In applications with difficult conditions (moving parts, high temperatures), the wireless link acts as an automatic backup to a wired connection.

6.9.1 Basic function

PRP devices act as the sender and receiver of PRP packets, whereby PRP devices are capable of assuming both roles.

The sender operates as follows:

1. It duplicates packets to produce twin pakets, and sends them over 2 independent (W)LANs.
2. Each packet is given a redundancy control trailer (RCT).

The RCT provides the following information for the recipient:

- It identifies the packet as a PRP packet.
- It contains a sequence ID.
- It shows which (W)LAN the packet arrived from.
- It contains the packet size.

The sequence ID is a consecutive incremented number. The sequence ID together with the the source MAC address allow the receiver to detect duplicate packets. Duplicate detection causes the packet arriving later to be discarded.

The receiver operates as follows:

- It reads the RCT.
- It forwards the first of the duplicated packets without its RCT.
- Through duplicate detection, the receiver discards the packet that arrives later.

6.9.2 Advantages of WLAN PRP

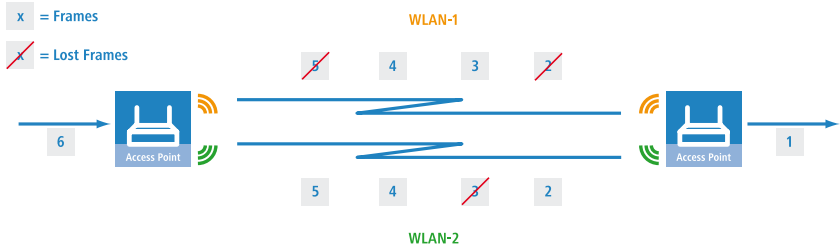
The functions of PRP offer you significant advantages for your WLAN. In practice, PRP improves the 3 most important quality indicators for a network: Jitter, latency and packet loss.

With PRP, the receivers will accept and forward the first copy of the PRP packets and discard those that arrive later. Because the devices always forward the first incoming packet, latency is reduced. In practice, significant improvements were seen to average and maximum jitter.

Like Ethernet, WLAN is designed to be a shared medium. Within a single WLAN connection, the devices hold back packets if the medium is busy.

Because the devices with PRP transport the data via 2 different WLANs, in effect 2 media are available thanks to frequency division.

Because the devices send each packet twice, PRP can to some extent compensate for unsystematic packet loss. As long as the receiver receives one of the packets, then communication was successful. Under certain circumstances there is no need to retransmit lost packets, which also positively affects jitter.



6.9.3 Implementation of PRP in the access points

Any access point (AP) with at least 3 interfaces can be used to setup a PRP network. The AP handles all of the functions necessary for establishing a PRP network.

The devices offer the following options:

1. PRP networks can be implemented on any interface; wireless, wired, or mixed
2. Each device can implement up to 2 PRP networks
3. In addition to a PRP network, connect additional clients to an AP
4. Activate dual roaming so that the 2 WLAN modules can roam asynchronously with PRP.
5. Comprehensive diagnostic options

6.9.4 Implementing PRP exclusively over WLAN

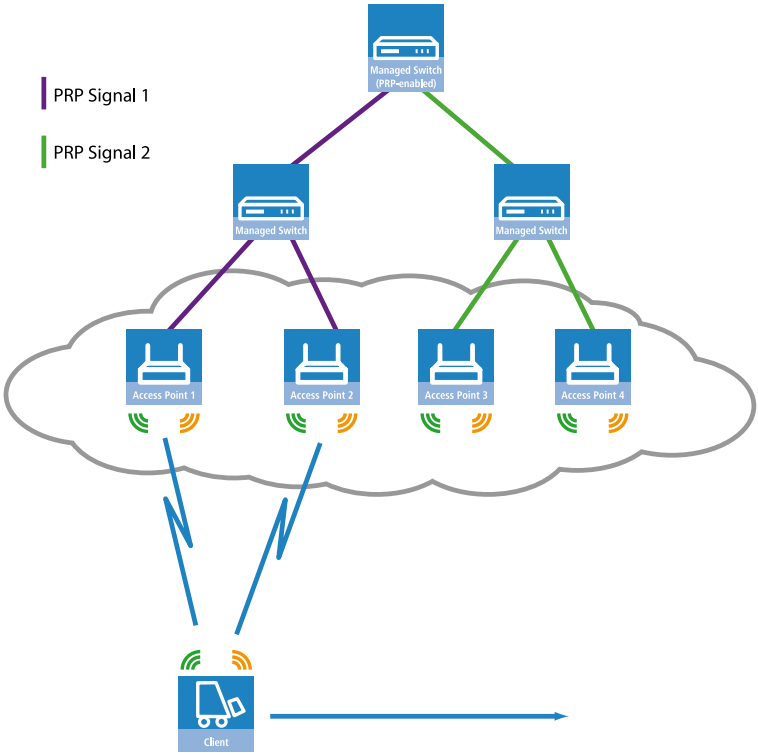
You can optionally setup a PRP network that operates over WLAN only. This is useful if the costs of cabling are high. A WLAN solution is suitable when the application type or environmental conditions demand this.

6.9.5 Dual roaming

A device with just 1 WLAN module will lose its connection to the infrastructure in a handover scenario.

However, a device with 2 WLAN modules can use PRP to reduce interruptions if the corresponding LANconfig setting prevents both WLAN modules from roaming at the same time. This mode is called dual roaming.

A practical example is a client moving past an access point. Due to the design of the network, one WLAN module stays connected and receives PRP packets, while the other WLAN module can already associate with the next AP.



A concrete example would be for materials management, and for the real-time monitoring of inventory flow in particular.

Another example is the railway. An AP in a train connects to the trackside APs throughout the journey.

In addition, you can specify the block time in LANconfig. The block time specifies the minimum time that passes before the different WLAN modules of the same device can perform roaming operations.

6.9.6 Diagnostic options

Recipients of PRP packets discard duplicates during normal operation and remove the RCT from packets that they pass on to their bundled output port.

HiLCOS provides you the following options to assist you in network diagnostics:

1. Forwarding packet duplicates without RCT
2. Forwarding single packets with RCT
3. Forwarding packet duplicates with RCT

HiLCOS also features the following trace options:

1. trace # PRP-DATA
2. trace # PRP-NODES

PRP-DATA contains information about packets that are sent and received. Information included: Name of the interface group transporting the packet: Direction of transport of the packet (RX|TX): Trailer sequence number: MAC address of the partner device: Interface within the PRP group (A|B) transporting the packet: Treatment of the packet (accept|discard)

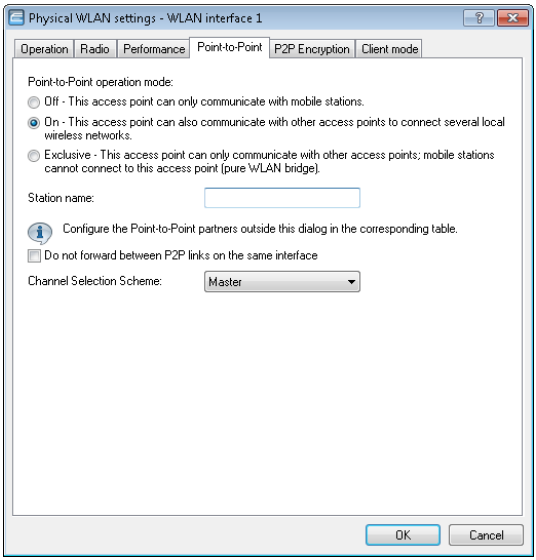
PRP-NODES contain the following information: Removed new address (proxy) node table address from the table (proxy) node, node type an address has changed.

6.9.7 Tutorial: Setting up a PRP connection over a point-to-point network (P2P)

Note: The following steps must be conducted for both P2P partners.

Proceed as follows to set up a P2P connection between two PRP-enabled APs:

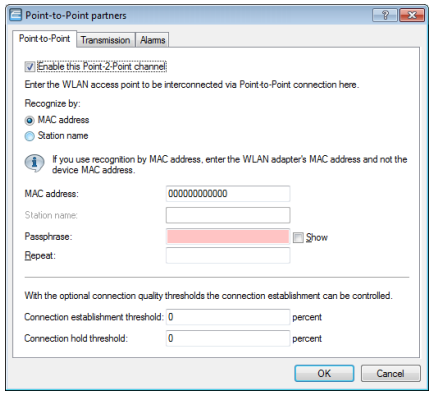
1. Under **Wireless LAN** > **General** > **Physical WLAN settings**, go to the **Operation** tab for each physical WLAN interface (WLAN interface 1, WLAN interface 2) and, on the **Point-to-point** tab, enable the **Point-2-Point operation mode**.



2. In the field **Station name**, give each of the physical WLAN interfaces a name that is unique on the WLAN. If the P2P partner can or should identify this interface using the MAC address, leave this field blank.

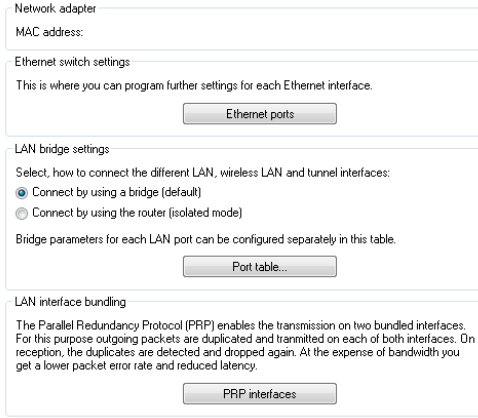
   Important: In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

3. Under **Wireless LAN** > **General** > **Point-to-point partners**, enable the point-to-point channels "P2P-1-1" and "P2P-2-1" and specify the interface identifier for each point-to-point partner (**MAC address** or **Station name**).

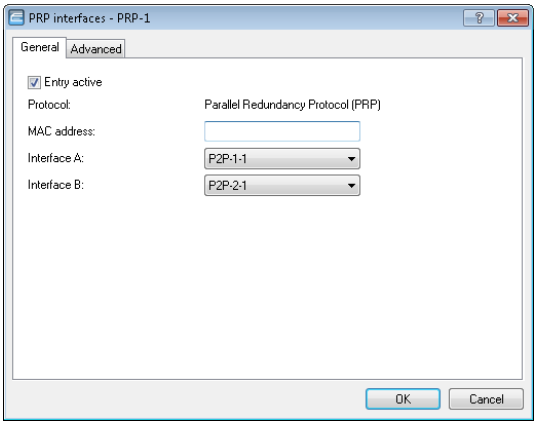


Specify either the MAC address or the station name of the corresponding WLAN interface of the P2P partner. You set these station names in the previous step.

4. Open the PRP configuration under **Interfaces** > **LAN** with a click on **PRP interfaces**.



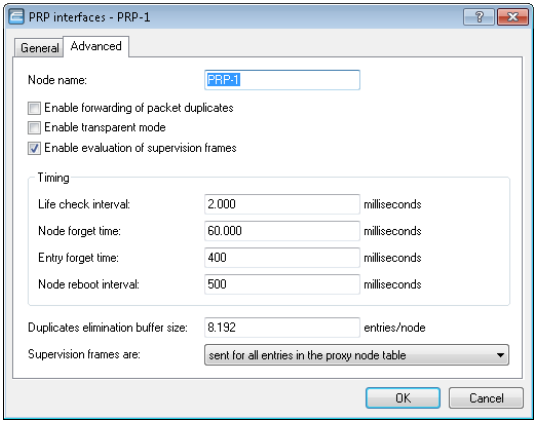
5. Enable the PRP interfaces and set the interfaces that the AP uses for bundling.



Here you select the previously activated point-to-point interfaces "P2P-1-1" and "P2P-2-1".

Important: In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

6. You can accept the advanced settings from the default configuration by clicking on **OK**.



This completes the setup of a PRP connection over a point-to-point network.

6.9.8 Tutorial: Roaming with a dual-radio client and PRP

A common way to increase the resilience of a WLAN infrastructure is to operate the various APs in different frequency bands. One way to implement this is for the physical WLAN interfaces of the APs to operate SSID-1 on the 2.4-GHz band and SSID-2 on the 5-GHz band, for example. A PRP-capable dual-radio client moving from the radio cell of one physical WLAN interface to a neighboring cell of the same infrastructure can experience uninterrupted cell switching thanks to PRP.

To do this, the dual-radio client using PRP initially connects its physical WLAN interface WLAN-1 to SSID-1 and WLAN-2 to SSID-2. If the reception for SSID-1 deteriorates and another radio cell with better reception is within range, the dual-radio client will perform a cell change. During the cell change the dual-radio client continues to send the data via WLAN-2 on SSID-2, while WLAN-1 already starts sending the same data with better reception on SSID-1. A PRP-enabled switch filters out the duplicate PRP packets before forwarding the data to the LAN.

Note: In this scenario, the APs in the WLAN infrastructure do not have to be configured to operate PRP.

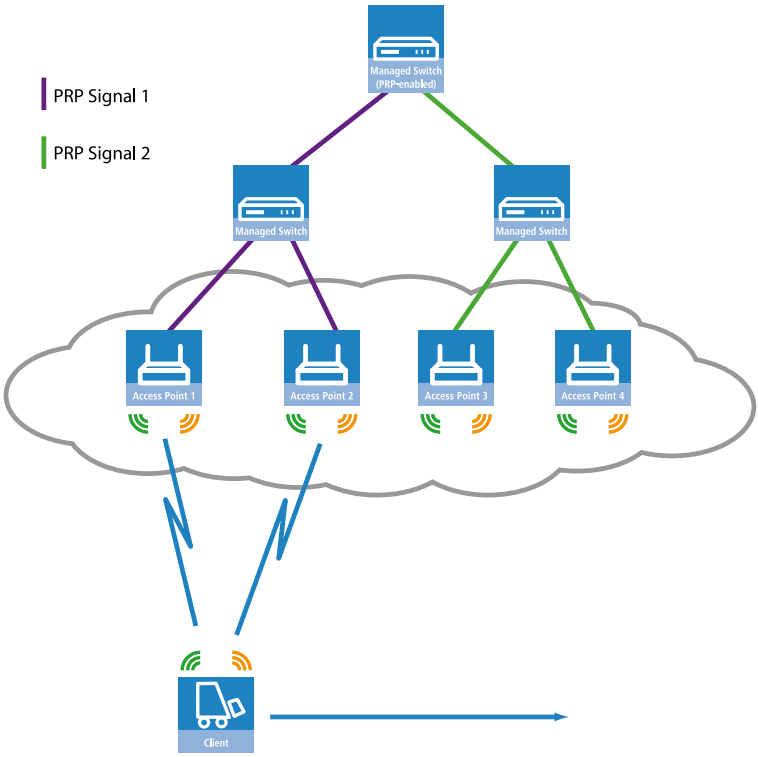
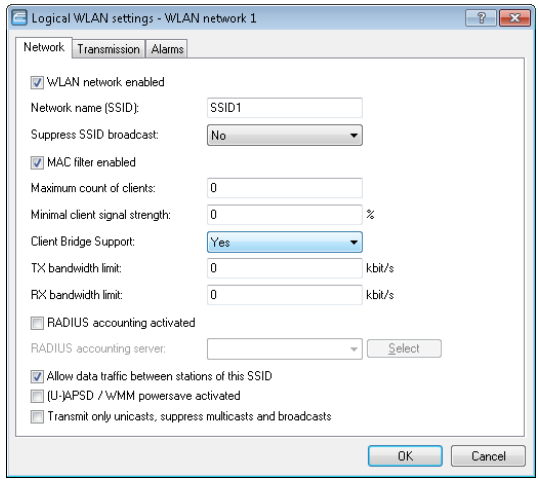


Figure 3: Roaming by a dual-radio client in a PRP-based WLAN infrastructure

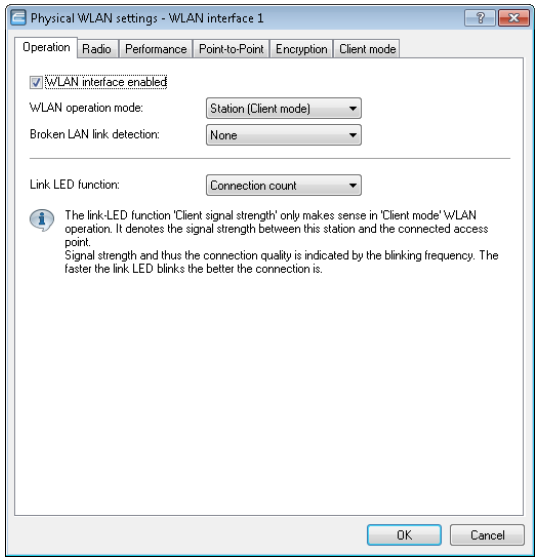
In order for the receiver to detect duplicate data packets, the APs in the WLAN infrastructure must be operating in client-bridge mode. The MAC address of the dual-radio client together with the RCT ensure that the receiver detects the duplicate packets. Without client-bridge support, an AP in the WLAN infrastructure would replace the MAC address of the dual-radio client with its own MAC address, so preventing the detection of duplicates.

Client-bridge support is enabled with LANconfig under **Wireless LAN** > **General** > **Logical WLAN settings** on the **Network** tab.



The PRP configuration of the dual-radio clients involves the following steps:

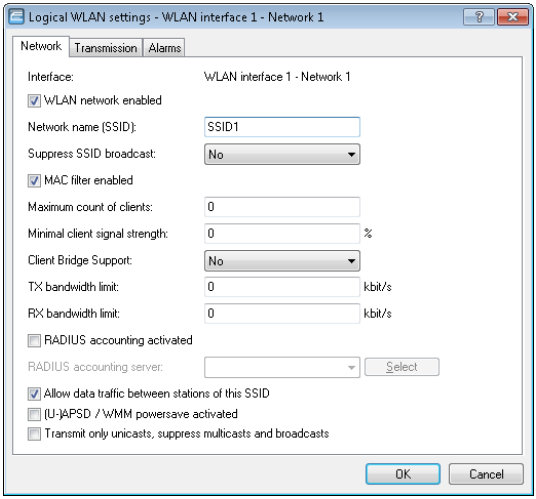
1. Under **Wireless LAN** > **General** > **Physical WLAN settings**, go to the **Operation** tab for each WLAN interface (WLAN interface 1, WLAN interface 2) and set the **WLAN operation mode** for each one to **Client**.



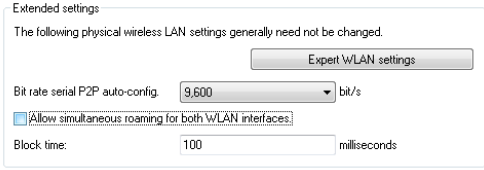
Specify the remaining WLAN parameters under **Radio**, **Performance**, **Encryption** and **Client mode** according to the requirements of the WLAN radio cells.

Important: In order for PRP to operate smoothly, the two instances of PRP must be operating on separate physical interfaces. If you are operating PRP on two logical interfaces of a single physical interface (e.g. "P2P-1-1" and "P2P-1-2"), then the device transmits the data sequentially. Apart from causing a loss of redundancy, this can also lead to delays in data transmission and a reduction in the bandwidth.

2. To enter the SSID, switch to the view **Wireless LAN** > **General**, click **Logical WLAN settings** and, for each WLAN interface, select network 1.
3. In the field **Network name (SSID)**, enter the name of the WLAN which the WLAN interface is to be connected to.



4. Under **Wireless LAN** > **General** in the section **Extended settings**, disable the option **Allow simultaneous roaming for both WLAN interfaces**.



By deactivating the parallel roaming, you prevent the two physical WLAN interfaces from roaming at the same time or performing background scans. The result could be that both could lose connectivity to their radio cell.

When configured in this way, the dual-radio client can move past a line of APs and roam between the individual APs (see *Figure 3: Roaming by a dual-radio client in a PRP-based WLAN infrastructure* on page 64).

6.9.9 Queue Processing for Wireless PRP

The performance of wireless PRP is decremented if the data volume in a wireless connection is too large. This can be explained by means of the following example::

- The WLAN interface cannot access the channel temporarily due to contention or interface.
- The number of frames buffered in the WLAN interface increases.
- If the buffered frames are waiting in the queue for too long, the frame delay can be greater than the PRP-EntryForgetTime.
- The duplicate detection function is therefore canceled.
- This prevents the recognition and deletion of redundant PRP frames.
- As a result, the data stream grows unnecessarily.

The controlled delay algorithm from Hirschmann makes it possible to avoid the scenario described above. The controlled delay algorithm helps to keep the data stream delay to a minimum using optimized queue processing.

6.9.10 Wireless PRP Micro-reordering Buffer

The wireless PRP micro-reordering buffer helps to prevent frame reordering in the data stream when PRP is setup using WLAN interfaces. Frames in the data stream may get into a wrong sequence if a frame is delayed on one WLAN interface and the corresponding frame is lost on the other WLAN interface.

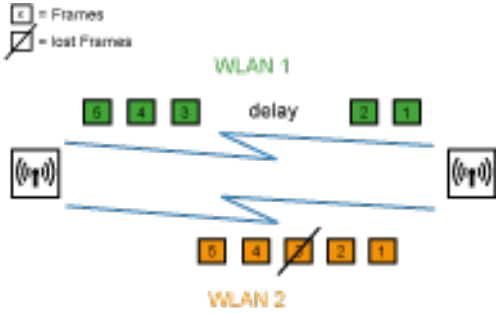
The following factors can lead to delays on a WLAN path:

- Different data rates and therefore latency in the transmission of a frame onto a WLAN path
- Delays due to frame aggregation
- Delays due to contention with other devices operating on the same channel

Interferences could be the cause of the loss of frames.

The following example shows schematically how the frames in the resulting data stream can end up in the wrong sequence:

- WLAN path 1 sends frames 3–5 with delay and WLAN path 2 loses frame 3:



- The frames in the resulting data stream end up in the wrong sequence:

The PRP micro-reordering buffer makes it possible to sequence the frames correctly despite the scenario described above. The PRP micro-reordering buffer works as follows:

- It monitors the frame counters in order to determine missing frames.
- It buffers all frames as soon as a frame arrives for which a predecessor frame or several predecessor frames are missing.

The subsequent micro-reordering buffer procedure depends on whether the missing frame arrives on time:

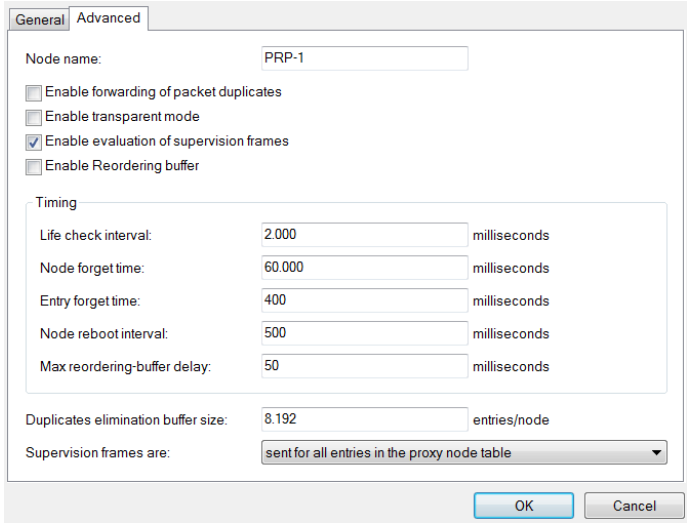
- If the missing frame arrived within the specified delay time, the wireless PRP micro-reordering buffer will place the frame into the correct sequence. It then removes the frames from the buffer and forwards them.
- If the specified buffer delay is exceeded before the missing frame arrives, the wireless PRP micro-reordering buffer will place the existing frames into the correct sequence. It then removes the frames from the buffer and forwards them without the missing frame.
- If the buffer capacity is exceeded before the missing frame arrives, the wireless PRP micro-reordering buffer places the existing frames into the

correct sequences. It then removes the frames from the buffer and forwards them without the missing frame.

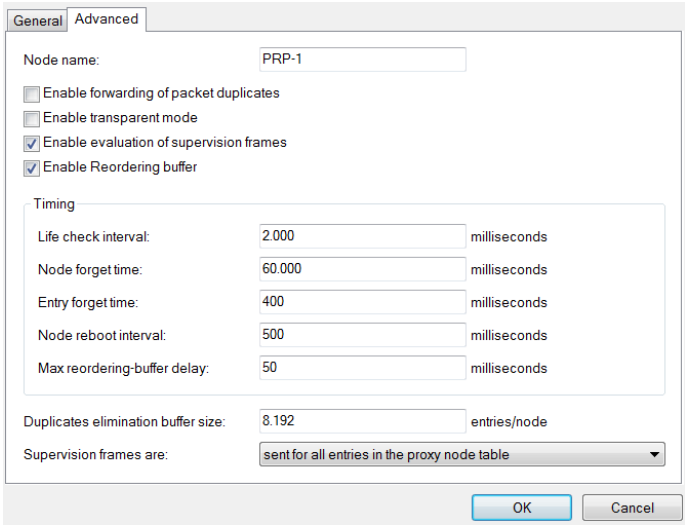
6.9.11 Tutorial PRP Micro-reordering Buffer

You have an OpenBAT with enabled PRP interfaces PRP-1.

1. Open the view **Interfaces** > **LAN** > **PRP interfaces** > **PRP-1** > **Advanced**



2. Enable the option **Reordering buffer activated**.
3. Specify the **Maximum buffer delay** .



4. Click **OK**.

You have enabled the PRP micro-reordering buffer and specified the maximum buffer delay.

7 WLAN management

7.1 AutoWDS – wireless integration of APs via P2P connections

In a centrally managed WLAN network, access points (APs) are typically connected to the WLAN controller (WLC) via the LAN. The LAN connections simultaneously determine the topology of the managed network. Network extension by means of additional APs is restricted to the reach of the hard-wired network architecture and requires the extension of the corresponding infrastructure.

By means of **AutoWDS**, you have the option of extending a WLAN by means of point-to-point (P2P) connections for the cost-effective and fast installation of highly scalable networks. "AutoWDS" stands for "automatic wireless distribution system". This feature enables you to create a radio network from several APs, which are interconnected via wireless only: a logical connection is all you need. Potential applications include the seamless connection of smaller properties or even entire districts to the Internet, or the establishment of a company network where connections via LAN are impracticable.

In the simplest case, all you need is a WLC connected via LAN to an AutoWDS-enabled AP. The AP supports the managed network and at the same time acts as an "anchor AP". Using this anchor AP, unassociated AutoWDS-enabled APs connect to the WLC, which transmits a configuration to them by means of CAPWAP. After obtaining the configuration and being incorporated into the managed WLAN, the individual APs use P2P links to forward user data, to communicate with one another, and to support the topology. Additional APs that join later are able to use the associated APs as their anchor APs. In this manner, several APs can be chained together to establish meshed networks, which can optionally feature redundant connections via RSTP. From the perspective of an unassociated AP, associated APs are master APs. From the perspective of the master AP, unassociated APs are slave APs.

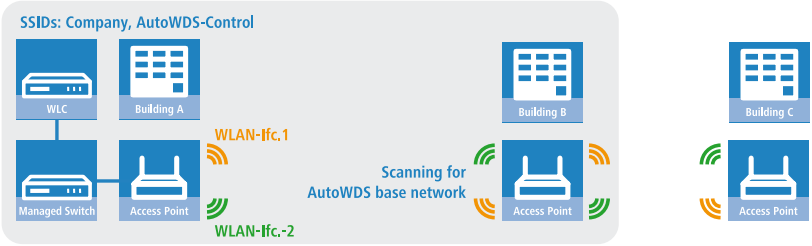


Figure 4: Phase 1 – unassociated AP in building B seeks AutoWDS base network and finds anchor AP in building A

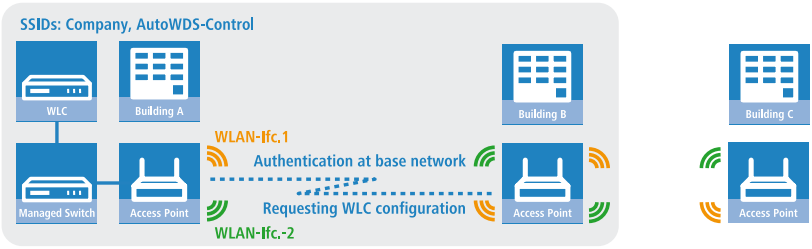


Figure 5: Phase 2 – unassociated AP in building B finds WLC and retrieves AP configuration via CAPWAP

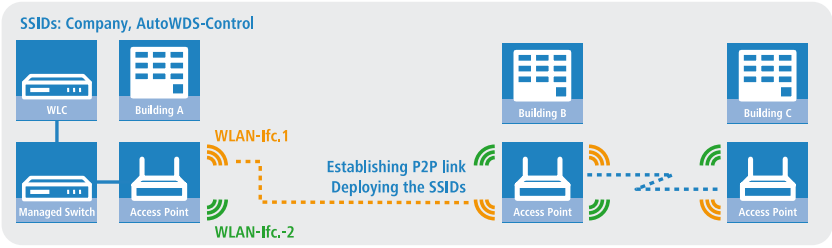


Figure 6: Phase 3 – unassociated AP in building B joins the managed WLAN. Unassociated AP in building C seeks AutoWDS base network and finds anchor AP in building B

Precise information about the integration process and the operating modes for topology management can be found in the following sections, which describe how AutoWDS functions.

Important: AutoWDS is suitable for static infrastructure only, not for mobile APs. If an AP should move out of range of its P2P partner and lose the connection to the network, there is a temporary downtime and a subsequent *reconfiguration*. However, the roaming of WLAN clients between individual AutoWDS APs is no different than the roaming between conventional APs.

Important: AutoWDS does not support the network separation of SSIDs to VLANs by means of a static configuration or a dynamic VLAN assignment via RADIUS. Implementing a network separation of SSIDs requires these to be separated by means of layer-3 tunnels.

Important: The DFS processing by an AP in 5-GHz operation is unaffected by AutoWDS and has a higher priority. DFS radar recognition may cause the AP to suddenly change the channel during operation. It can even completely deactivate the WLAN for a period if radar recognition is running on different channels and the available frequencies drop out. The impacted AP can cause interference to the entire AutoWDS group, and may not be able to deploy any SSIDs for some time. Within buildings you have the option of counteracting interference by enabling the indoor mode.

Note:

If you operate AutoWDS on a device with a single physical WLAN interface, its data rate will be reduced to just a third, since the device must send incoming/outgoing data multiple times: To the WLAN clients, to a master AP and, if applicable, to a slave AP. This effect is mitigated by operating only devices that have multiple WLAN physical interfaces and using these to divide up the data traffic. You do this by reserving one physical WLAN interface for connecting the APs and one physical WLAN interface for connecting the clients.

MultiHop on the same WLAN interface can be enabled in the AutoWDS profile configuration, if necessary. This is disabled by default due to the associated loss of performance.

7.1.1 Notes on operating AutoWDS

Owing to technical restrictions, the applications of AutoWDS are limited to certain specific application scenarios. Please carefully observe the general remarks in this chapter to avoid possible complications. The items listed here are intended to supplement the remarks elsewhere in the AutoWDS chapter, so some redundancies are possible.

- APs must switch channels when radar is detected (5-GHz band, outdoor and DFS). This can potentially lead to temporary interruptions to the WLAN due to necessary changes of channel.
- In general, we recommend a maximum of 3 hops for AutoWDS operations.
- When operating AutoWDS on one radio channel only, problems with multiple transfers and hidden stations can occur. For this reason we recommend the use of APs with two physical WLAN interfaces (dual radio) operating on separate radio channels.
- AutoWDS does not support the network separation of SSIDs to VLANs by means of a static configuration or a dynamic VLAN assignment via RADIUS. Implementing a network separation of SSIDs requires these to be separated by means of layer-3 tunnels.

Important: If you are operating DFS in combination with AutoWDS, you should set the continuation time for autonomous operation of the AutoWDS profile to at least 2 minutes. After the downtime of a P2P connection, this extra minute allows for the one-minute DFS scan, after which the CAPWAP layer restores the CAPWAP connection to the WLC via the P2P connection.

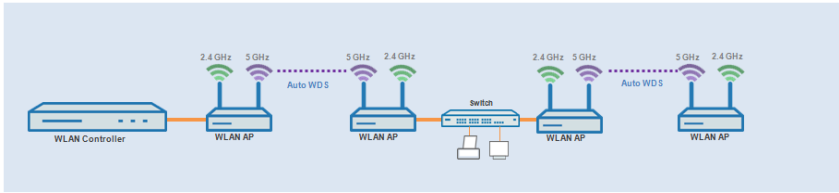
Important: If possible, ensure that all APs on each physical WLAN interface (WLAN-1, WLAN-2) consistently use the same frequency band (2.4 GHz or 5 GHz) to exclude any potential problems with the automatic topology configuration.

The following is a overview of the **suitability of AutoWDS** for certain application scenarios.

Suitable:

Use of a **dedicated** physical WLAN interface for the P2P links.

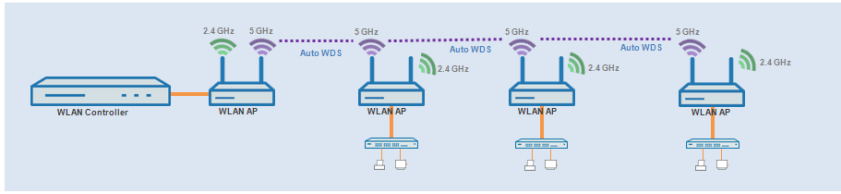
- Use of different channels for the P2P links (indoor)
- Use of AutoWDS with up to 3 hops



Partly suitable:

Use of single physical WLAN interface **simultaneously** for the AutoWDS uplink and downlink (repeater mode) where all P2P links operate on the same radio channel.

- Use for operation without DFS (indoor)
- Use of AutoWDS with up to 3 hops



Difficulties can arise from the hidden station problem or throughput loss due to multiple transmissions.

- **Hidden station problem**: Over larger distances, widely separated APs on the same network may not be able to "see" each other. In this case, several APs could end up transmitting simultaneously to cause interference for the APs between them. These collisions lead to multiple transmissions and performance losses.

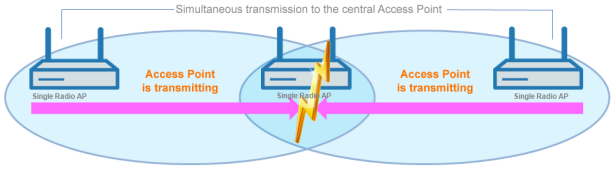


Figure 7: Simultaneous transmissions to the middle AP: The two outer APs are unaware of the collision.

- **Throughput-loss due to multiple transmissions**: An AP transmitting data packets multiple times on the same channel leads to a reduction of the maximum available throughput (by half per hop).

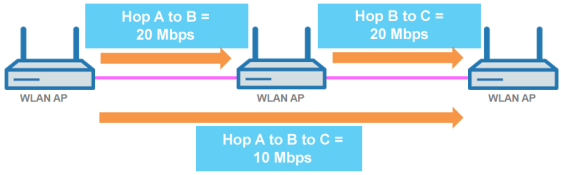
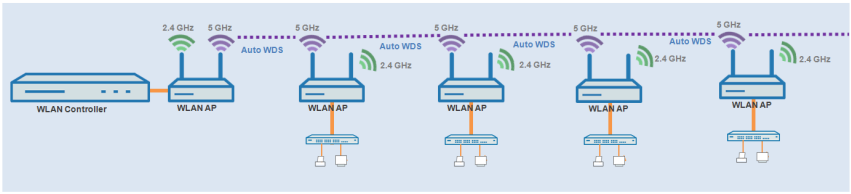


Figure 8: Transmission of data packets on every hop

Unsuitable:

Use of a physical WLAN interface **simultaneously** for AutoWDS uplink and downlink (repeater mode) during outdoor operations with more than one hop in the 5-GHz band.



In repeater mode, the physical WLAN interface has a dual role: In the direction of the WLC the interface operates as a master, while in the direction of neighboring APs it operates as a slave. For this purpose, all APs necessarily

operate on the same radio channel. However, if the DFS feature detects signals, the APs are required to stop transmitting on the affected frequencies. This means that the APs cannot inform the WLC about the DFS event and the WLC cannot initiate a change of frequency for the network. As a result, the affected APs are potentially permanently separated from the network.

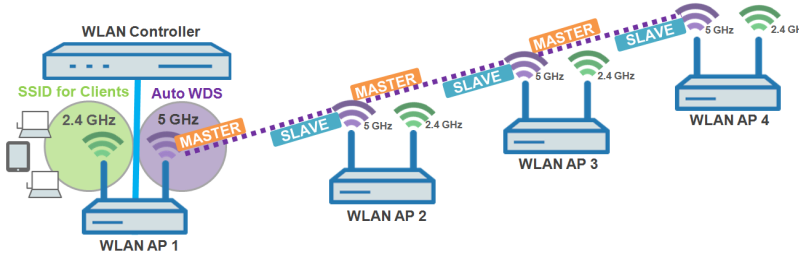


Figure 9: Connection lock after DFS detection

7.1.2 How it works

Deploying the AutoWDS base network

AutoWDS provides different integration modes for managing P2P links for meshed networks. The majority of the configuration is performed on the WLC which manages the individual logical WLAN networks. You link an active AutoWDS profile with an established WLAN profile of your managed wireless network. The AutoWDS profile groups the settings and limits to form the P2P topology and of the AutoWDS base network.

The AutoWDS base network and its associated SSID (default name: **AutoWDS-Rollout**) is a management network only. It serves two purposes: The first is to authenticate an AP during the preconfigured integration, and the second is to establish the WLC tunnel for configuration exchange. In this way, unassociated APs remain isolated from operations while they are being integrated into the managed WLAN. As soon as there is a P2P connection to a master AP, an unassociated AP is considered to be integrated and it processes further communications via the bridge on Layer 2. Similar to conventional P2P links, the P2P partners set up a management SSID, which they use to process the data traffic and the CAPWAP tunnel to the WLC (see *Updating the AP configuration and establishing the P2P link* on page 82).

Note: The AutoWDS base network cannot be used by other WLAN clients such as smartphones, laptops, etc. These devices require their own SSID within the WLAN infrastructure.

After assigning an active AutoWDS profile to your managed WLAN, the corresponding anchor APs deploy the AutoWDS base network and transmit their beacons (assuming you have enabled 'SSID broadcast' in the AutoWDS profile) with an additional manufacturer-dependent identifier. This identifier, also known as an "AutoWDSInfoFlag", signals the general support of the feature to unassociated AutoWDS-capable APs and informs them...

- whether AutoWDS is enabled/disabled for the detected SSID;
- whether the AP of the corresponding SSID has an enabled/disabled WLC connection;
- whether the WLC accepts or prohibits the express mode for unassociated APs; and
- whether integration requires the APs to connect to the equivalent physical WLAN interface of the anchor AP (strict interface pairing, i.e. with WLAN-1 to WLAN-1 and with WLAN-2 to WLAN-2), or whether mixed interface pairs are allowed.

A managed AP will automatically work as an AutoWDS AP after it has been initially paired with a WLC via LAN cable and a valid certificate and an AutoWDS profile with the additional AP configuration has been transferred correctly. A configured AutoWDS AP will automatically function as an unassociated AP after it has failed to establish a CAPWAP connection to a WLC after a predefined time, for example if there is no wired LAN connection. This access point then temporarily switches its operating mode to **Client** mode and scans each WLAN until it detects a suitable anchor AP. The scan is carried out in the 2.4-GHz and 5-GHz frequency bands.

If your device has two physical WLAN interfaces and both are enabled, both WLAN interfaces simultaneously scan for a suitable AutoWDS base network. If a physical WLAN interface detects a suitable SSID, then it associates with the anchor AP, assuming that the interface pairing mentioned above permits this. The other physical WLAN interface continues to scan in case the already associated physical WLAN interface loses the connection again. Until then, this physical WLAN interface does not connect to any other AutoWDS base network. Once your device has received the WLC configuration, the two

physical WALN interfaces behave as specified in the profile, i.e. they deploy the SSIDs assigned to them and the AutoWDS base network.

The procedure for searching for an AutoWDS base network is identical with that of the reconfiguration in the case that the WLAN connection is lost (see *Connectivity loss and reconfiguration* on page 82).

Differences between the integration modes

When integrating unassociated APs into your managed WLAN, you have the choice of two different integration modes. The integration mode determines the conditions under which your WLC accepts an unassociated AP:

- **Preconfigured integration** is the controlled and preferred method to integrate an unassociated AP into a managed WLAN over a point-to-point link. In this mode, the WLC only allows the integration of APs that have a local, preconfigured SSID and a valid WPA2 passphrase for the AutoWDS base network.

  This mode is suitable for all productive environments, and is used to create a predefined relationship between an unassociated AP and an AutoWDS base network. As soon as the AP obtains a configuration from the WLC, the AP gives this configuration a higher priority than its own local AutoWDS configuration. This remains so until the WLC revokes the configuration via CAPWAP or you reset the device.

- **Express integration** is the quick way to integrate an unassociated AP into a managed WLAN via a point-to-point link. In this mode, the WLC allows both the integration of preconfigured devices as well as devices that are not configured at all. Unconfigured APs have neither a registered SSID nor an individual WPA2 passphrase for the AutoWDS base network. Instead, APs can authenticate with any AutoWDS base network by using a pre-shared key hard-coded in the firmware.

  This mode is suitable for the easy integration of new APs into a managed WLAN. The choice of AutoWDS base network is automatic and is outside your control. As soon as the corresponding APs obtain configurations from the WLC, these devices save the settings as default values until the WLC revokes the configuration via CAPWAP, the device executes the express *reconfiguration* after an interruption in the connection, or you reset the device.

Important: For the express integration make sure that no other AutoWDS base network is in range. Otherwise it is possible for an external WLC to take control of your AP and revoke your remote access. Having the express mode enabled increases the vulnerability to attack. For this reason it is advisable to disable the express mode if it is not absolutely necessary.

Important: For the security reasons name above, Hirschmann recommends a preconfigured integration. Through the pairing of WLC and APs, you can further reduce the effort required for the preconfigured integration. Learn more about this in section *Accelerating preconfigured integration by pairing* on page 90.

After successful authentication on the AutoWDS base network and retrieval of an IP address, the unassociated APs scan the network for a WLC. As soon as they have detected a WLC, they attempt to connect with it and retrieve a configuration. In LANmonitor, these APs are shown as unassociated devices. To include these in the managed WLAN, the administrator must still confirm them and assign WLAN profiles to them. Assigning profiles in this way is no different from accepting normal APs. Alternatively, assignment can be handled by the WLC if you

- set up a default WLAN profile and activate its automatic assignment; or
- enter the associated AP into the access point table and link it with a WLAN profile.

Important: By simultaneously setting the automatic acceptance of unassociated APs by the WLC ("Auto Accept"), the integration of unassociated APs can be fully automated. However, for express integration you should ensure that you disable this setting in order to maintain a minimum level of security and hinder rogue AP intrusion.

Note: The procedures for certificate generation, certificate checks, and the automatic acceptance or rejection of connection requests by the WLC are identical to a WLAN scenario with cable-connected APs.

Designing the topology

When the WLAN profile is assigned by the WLC, the slave APs simultaneously receive information about how their P2P links in the meshed network are to be established. The topology results directly from the hierarchy of the P2P connections established between the APs. The WLC offers the following management modes for this:

- **Automatic**: The WLC automatically generates a P2P configuration. The device ignores manually specified P2P links.
- **Semi-automatic**: The WLC only generates a P2P configuration if no manual P2P configuration exists for the unassociated AP. Otherwise the WLC uses the manual configuration.
- **Manual**: The WLC does not automatically generate a P2P configuration. A manual P2P configuration is taken, if available. Otherwise, the WLC does not transmit a P2P configuration to the AP.

Normally, the WLC handles the automatic calculation of the topology, where a slave AP generally connects with the closest master AP. Calculated in real-time, the topology is recorded by the WLC in the status table **AutoWDS-Auto-Topology**. If you use semi-automatic or manual management, you define the static P2P links in the setup table **AutoWDS-Topology**. To achieve this, you specify the relationships between the individual master APs and slave APs in a similar manner to a normal P2P connection. For more on this, see the section *Manual topology management* on page 94.

Note: The automatic generation of a P2P configuration (e.g., for initial connection or reconnection of an AP) replaces any existing entry in the AutoWDS-Auto-Topology table.

Note: The automatically generated topology entries are not boot-persistent. The table is emptied when the WLC is restarted.

Note: For manual topology configuration, it is important for a configured P2P master AP within the topology to be closer to the WLC than a corresponding P2P slave AP. This is because a brief interruption to the P2P connection will cause the slave AP to scan for the master AP.

Updating the AP configuration and establishing the P2P link

If an unassociated AP has received the full WLAN profile with all its settings from the WLC via CAPWAP, as a slave it attempts to establish a P2P link to the master AP assigned to it. The AP simultaneously changes its WLAN operation mode from **Client** back to **Managed**.

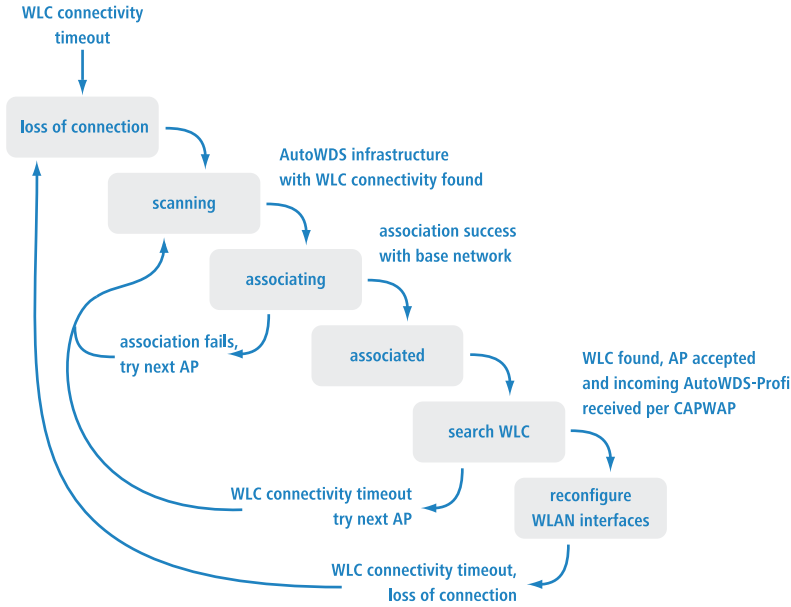
Since the master AP is already in managed mode, it obtains only an update to its P2P configuration from the WLC via CAPWAP. This informs the AP of the WPA2 passphrase and the peer identification of the AP. For an automatically generated P2P configuration, the peer identification corresponds to the MAC address; for a manual P2P configuration, it corresponds to the name of the slave AP. The master AP labels the SSIDs with ***** P2P Info *****.

Once both APs are successfully interconnected over a P2P link, the AutoWDS integration process is concluded. The unassociated AP can then be used by clients (smartphones, laptops, other APs in client mode looking for a master, etc.).

Note: As long as the unassociated AP is in client mode, bridging between a physical WLAN interface and a LAN interface or another physical radio interface is disabled throughout the integration process. The device automatically puts all physical WLAN interfaces on different bridges. Not until successful creation of a P2P connection does the AP switch the bridging back to the original state.

Connectivity loss and reconfiguration

An automatic process of (re-)configuration is triggered as soon as you enable AutoWDS on an unassociated AP, if authentication at an anchor AP fails, or if an associated AP loses contact to the WLC. This process follows the scheme shown here:



An AP does not run the (re-)configuration process if it is in client mode and can connect to an anchor AP but not to the WLC. The AP waits for 5 minutes after connecting to the AutoWDS base network to see whether the WLC performs a configuration of the device. If no configuration is performed by the WLC by then (e.g., because no administrator accepts the AP), the AP disconnects from the AutoWDS base network and scans for further suitable SSIDs. If there is only one SSID in range, the AP contacts it again to repeat the integration process.

Important: If there is a connection to a LAN, the AP tries to reach the WLC by broadcast over the LAN for the duration of the downtime. If the AP finds the WLC via LAN, then no new P2P link is set up and the WLC deletes all automatically generated P2P links that set the AP to be a slave.

Configuration timeouts

The initial configuration and the reconfiguration of an unassociated AP are triggered by various timeouts, which together control the behavior of the device. This includes, if specified:

1. The duration of standalone P2P-link operation if the CAPWAP connection is lost (except for reconfiguration);
2. The wait time until the start of the automatic (re-)configuration for the pre-configured integration; as well as
3. The wait time until the start of the automatic (re-)configuration for the express integration.

The continuation time refers to the lifetime of any P2P link if the AP loses the CAPWAP connection to the WLC. If the AP detects a loss of the CAPWAP connection, it attempts to reconnect within the specified continuation time. Connections to P2P partners and associated WLAN clients remain intact during these times. If the recovery fails and the continuation time expires, the AP discards the P2P part of the WLC configuration. If the standalone continuation time is specified as `0`, the AP discards this part of the configuration immediately.

Next, the device uses the remaining configuration parts—the SSID of the AutoWDS base network, the related WPA2 passphrase, and the wait times for the preconfigured and express integration—as a basis to count down the preset time until the start of the (re-)configuration for the preconfigured integration. After this wait time expires, the device switches its physical WLAN interface(s) into client mode and scans the available SSIDs for the last detected AutoWDS base network. At the same time, the timer starts the countdown to the start of the automatic (re-)configuration for the express integration.

If the device has not found the expected AutoWDS base network when the express timer expires, the device automatically switches to express integration. It then searches for any AutoWDS-enabled network until a suitable anchor AP is detected.

By adjusting the interaction between the various wait times, you can allow the device to react flexibly to unforeseen events. This facilitates the implementation of a fallback solution, for example in the case that you change the pre-shared key for the AutoWDS base network. If the change should fail on an unassociated AP, the device becomes inaccessible as it has an invalid configuration. Please observe the notes under *Differences between the integration modes* on page 79.

The relevant counters are configured on the AP (e.g. via LANconfig) and also on the WLC (Setup menu only). The counters are only observed by the AP if no WLC configuration (initial configuration) is available. As soon as a config-

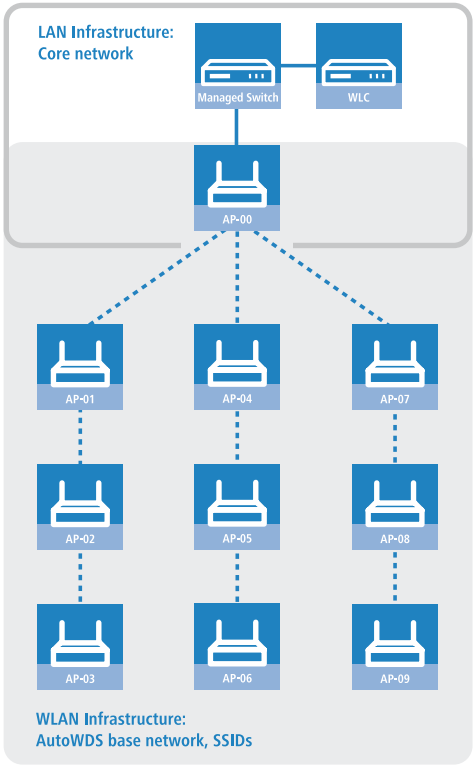
uration is available, then the values specified in the AutoWDS profile apply (reconfiguration). Learn more about the setting the priorities for configurations under *Differences between the integration modes* on page 79.

Important: If you disable the express timer or the preconfiguration timer, the device skips the corresponding integration step. The automatic reconfiguration can be switched off by disabling both timers. This means that, after being disconnected for long enough, the device can no longer be reached by AutoWDS. However, the device remains accessible over the LAN interface and searches the LAN for a WLC.

Important: The process of preconfigured integration does not start if the settings for the AutoWDS base network (SSID, passphrase) are incomplete or if the preconfiguration timer is set to `0`.

Example: Failure of an AP

Each AP maintains its CAPWAP connection by issuing echo requests to the WLC at a specified interval. If an AP fails or its connection is interrupted, these requests will be lost. If the APs repeat the echo request and receive no response from the WLC, the CAPWAP connection is considered to be lost and the APs start the reconfiguration process described under *Connectivity loss and reconfiguration* on page 82.



For the infrastructure illustrated above, a failure of AP-01 would have the following impact, assuming that automatic topology management is enabled:

1. AP-01 is defective.
2. AP-02 and AP-03 repeat their echo-requests; all repeats fail.
3. AP-02 and AP-03 start the standalone operation of their P2P link (if configured) and continue to try to reach the WLC (over wireless and LAN, assuming connectivity exists).
4. AP-02 and AP-03 stop their autonomous operation of P2P connections.
5. AP-02 and AP-03 count down the wait time until the start of the preconfigured integration.
6. After the wait time expires, AP-02 and AP-03 switch into client mode and scan the WLAN for the last known AutoWDS base network.
7. AP-02 and AP-03 find a new anchor AP (e.g. B. AP-05 or AP-06) and login as clients.

8. AP-02 and AP-03 restore the CAPWAP connection via the **WLC-TUNNEL-AUTOWDS** and inform the WLC about the new anchor AP and the physical WLAN interfaces they are using.
9. The WLC generates a P2P link for the corresponding physical WLAN interfaces and delivers the configuration to the APs by CAPWAP.
10. The APs set up the new P2P link to the master APs assigned to them and stop communicating with the WLC via the **WLC-TUNNEL-AUTOWDS**; they are bridged to the LAN instead.

7.1.3 Setup by means of preconfigured integration

The following sections show you how to set up an AutoWDS network by means of the preconfigured integration. Configuration relies on the automatic topology management of the WLC.

In this scenario, a company is expanding its business premises into a new building. The company wants to integrate the new business premises into its existing managed WLAN. The relevant APs should be connected exclusively via point-to-point link. Between building A (old) and B (new), no wired network connection can be installed.

To keep the configuration simple, a single WLC is used to configure all of the APs. The exact number of APs in building A and building B is immaterial. Particular features, such as multiple physical WLAN interfaces, are automatically taken into account by the WLC topology management.

The configuration itself is divided into two parts:

1. Configuration of the WLC in building A
2. Configuration of all APs in building B

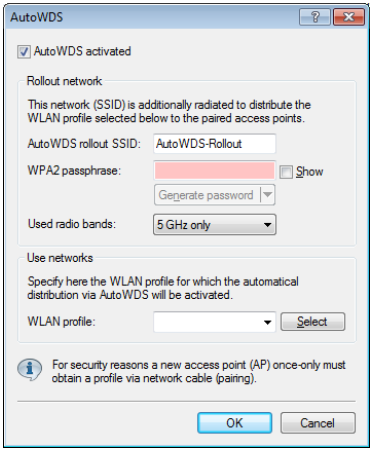
Note: The example application requires a valid WLAN configuration with valid certificates in the WLC. Just how to set up a managed WLAN is described in the chapter on WLAN management.

Configuring the WLC

The following instructions describe how to configure the AutoWDS of a central WLC for preconfigured integration.

Note: Ensure that the AutoWDS APs, which integrate with the network as WLAN clients, are able to reach a DHCP server via the WLC-TUNNEL-AUTOWDS interface. Without an IP address, the APs do not search for the WLC and thus do not receive a configuration from it.

1. Open the configuration dialog in LANconfig and click on **WLAN controller** > **Profiles** > **AutoWDS** to access the AutoWDS dialog.



2. Click on **AutoWDS activated** to enable the feature on the device.
3. Enter the name of the AutoWDS base network under **AutoWDS-Rollout-SSID**. By default LANconfig uses the identifier `AutoWDS-Rollout`.

   The SSID specified here acts as the management network for all APs that are searching for the AutoWDS network and, apart from the passphrase, it offers no further options for configuration. The WLC internally connects the specified SSID automatically using a WLC tunnel (**WLC-TUNNEL-AUTOWDS**). Normal WLAN clients are unable to use this management network.

   Important: In this case, enter a custom AutoWDS rollout SSID that is different from the LANconfig default.

Note: Setting up this AutoWDS base network reduces the maximum number of SSIDs that your device can support on a physical WLAN interface by 1.

4. Under **WPA2 passphrase** you enter a key to secure the AutoWDS base network.

   Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength.

5. Under **Used radio bands** you specify the frequency band used by the APs for the AutoWDS base network.
6. Select the **WLAN profile** with the SSID which is to be enhanced with AutoWDS.

   The APs with this WLAN profile serve as anchor APs and support the AutoWDS base network. At the same time, associated APs receive this WLAN profile via AutoWDS as a default configuration, which they use to transmit the corresponding SSID.

7. Close the dialog window with **OK** and save the configuration to the device.

The WLC now assigns the AutoWDS settings to all managed AutoWDS-capable APs in your WLAN. These now form the basis for your AutoWDS base network. For future reconfiguration processes, the APs use only the SSID and passphrase stored here, unless configured otherwise (see *Differences between the integration modes* on page 79).

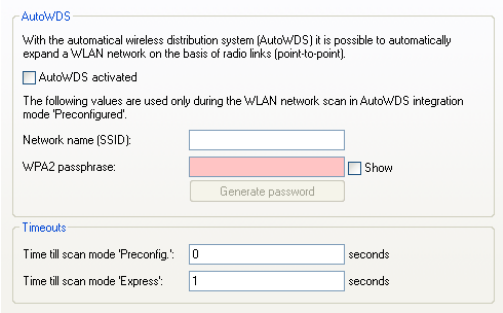
This concludes the configuration of the WLC. We now continue with the configuration of the APs.

Configuring the APs

The following instructions describe how to configure the AutoWDS of an AP for preconfigured integration. The configuration steps are identical for all unassociated APs.

Note: There is no need to configure an AP that is already paired with a WLC. If devices are out of range of the WLC, thus making pairing impossible, then the SSID and passphrase can optionally be entered manually.

1. Open the configuration dialog in LANconfig and click on **Wireless LAN** > **AutoWDS** to access the AutoWDS dialog.



2. Click on **AutoWDS activated** to enable the feature on the device.
3. Under **Network name (SSID)** enter the name of the AutoWDS base network that you configured on the WLC (e.g. `AutoWDS-Rollout`).
4. Enter the key for the AutoWDS base network under **WPA2 passphrase** that you have configured on the WLC (e.g. AutoWDS-Control).
5. Change the timeout values for the **Time till search mode 'Preconfig'** to `1` and for the **Time until search mode 'Express'** to `0`.
6. Under **Wireless LAN** > **General** > **Physical WLAN settings.**, make sure that at least one physical WLAN interface is in **Managed** mode. Otherwise the device will never search for an AutoWDS base network.
7. Close the dialog window with **OK** and save the configuration to the device.

After a successful configuration update, the AP switches its physical WLAN interface(s) into client mode and searches for the specified AutoWDS base network. To learn more about the procedure, refer to the *chapter about the function*.

7.1.4 Accelerating preconfigured integration by pairing

Through the one-time pairing of WLC and APs, you can further reduce the effort required for the preconfigured integration. For pairing, you reset an AP and connect it via LAN to the WLC used for running your managed WLAN

including AutoWDS. In the reset state, the AP is automatically in managed mode after being switching on. Once the AP finds the WLC and the WLC accepts the AP, the AP automatically receives all relevant certificates and partial configurations required to configure the parameters in the device. Pairing is then complete. On location, a coworker installs the AP and switches it on. Your device then searches for the preconfigured AutoWDS base network.

The following steps summarize the pairing procedure. They also include the steps for automatic configuration assignment, which further simplifies the pairing of a high number of APs.

1. Start LANconfig and, on your WLC, set up a managed WLAN with a valid WLAN profile, if you have not already done so. In LANconfig you configure this type of profile under **WLAN controller** > **Profiles** > **WLAN profiles**.
2. Activate AutoWDS for this WLAN profile as described in *Configuring the WLC* on page 87.
3. Create a profile that is valid for all APs under **WLAN controller** > **AP configuration** > **Access point table** with the button **Default**. Assign the **WLAN profile** you created earlier to this profile
4. Enable the option **Automatically provide APs with a default configuration** under **WLAN controller** > **General**.
5. **Optional:** To avoid having to manually accept unassociated APs in LANmonitor by allowing the WLC to do this automatically, you should additionally select the option **Automatically accept new APs (auto-accept)**.

   Important: For security reasons, you should only enable this option if you have connected the unassociated APs to the WLC via a LAN interface. To exclude the possibility of rogue AP intrusion, make sure that no other devices are connected with the WLC.

6. Send the configuration to the WLC.
7. Reset the unassociated AP and connect the device to the WLC via the LAN.
   The device automatically starts to search for a WLC.
8. In LANmonitor, you accept the new AP under **Wireless LAN** > **New APs**, unless you have set up automatic acceptance.

The WLC sends the device those parts of the configuration that it needs for its future operation in managed mode. After successful configuration, LANmonitor lists the device in the **Active APs**.

This completes the pairing and the AP is ready for AutoWDS operation.

7.1.5 Express integration

The following sections show you how to set up an AutoWDS network by means of the express integration. Configuration relies on the automatic topology management of the WLC.

The initial scenario is similar to the *preconfigured integration*.

Note: By default, AutoWDS is disabled on a reset AP and you must first use a wired access to activate the feature. However, an exception is made for devices that are explicitly setup with this feature at the customer's request: In this case, AutoWDS is enabled by default. The *second part of the configuration* is eliminated and the devices in express-integration mode can be commissioned directly.

Important: Express configuration has certain characteristics that are relevant to security. We recommend that you read the section *Differences between the integration modes* on page 79 carefully.

Configuring the WLC

The following instructions describe how to configure the AutoWDS of a central WLC for express integration.

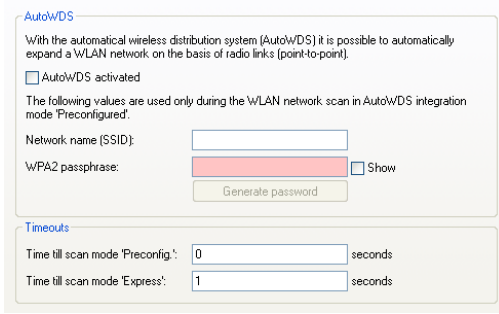
1. Carry out each step under *Configuring the WLC* on page 87 for the preconfigured integration.
2. Log on to your device via WEBconfig or the console.
3. In the setup menu, navigate to the table **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**.
4. Edit the AutoWDS default profile by clicking on the entry **DEFAULT**.
5. Change the **Allow-Express-Integration** parameter to **Yes** and save the settings by clicking on **Send**.

This concludes the configuration of the WLC. We now continue with the configuration of the APs.

Configuring the APs

The following instructions describe how to configure the AutoWDS of an AP for express integration. The configuration steps are identical for all unassociated APs.

1. Open the configuration dialog in LANconfig and click on **Wireless LAN** > **AutoWDS** to access the AutoWDS dialog.



2. Click on **AutoWDS activated** to enable the feature on the device.
3. Under **Wireless LAN** > **General** > **Physical WLAN settings.**, make sure that at least one physical WLAN interface is in **Managed** mode. Otherwise the device will never search for an AutoWDS base network.
4. Close the dialog window with **OK** and save the configuration to the device.

After a successful configuration update, the AP switches its physical WLAN interface(s) into client mode and searches for any AutoWDS base network. For further information on this procedure please refer to *Deploying the AutoWDS base network* on page 77.

7.1.6 Switching from express to preconfigured integration

Following a network rollout and the express integration, the switch to a preconfigured integration is implemented by disabling the express integration on the WLC. There is no need to change anything on the APs because they have already received an AutoWDS configuration during the express integration,

and this pre-configures an AutoWDS network for subsequent re-configuration procedures.

1. Log on to your device via WEBconfig or the console.
2. In the setup menu, navigate to the table **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**.
3. Edit the AutoWDS default profile by clicking on the entry **DEFAULT**.
4. Change the **Allow-Express-Integration** parameter to **No** and save the settings by clicking on **Send**.

You have now disabled the express integration of further unassociated APs.

7.1.7 Manual topology management

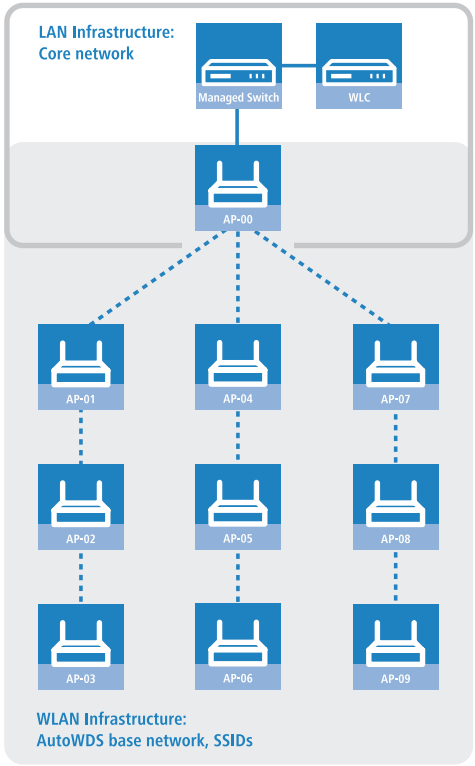
The examples of AutoWDS installation rely upon automatic topology management by the WLC, which simplifies the configuration. Depending on the usage scenario, it may be necessary to setup individual or all of the P2P links manually.

The following section shows you how to disable the automatic topology management on the WLC and create a manual P2P configuration. To configure the P2P links, you first assign unique names to each of the APs. Then link these names with the topology configuration and the physical WLAN interfaces being used. The chapter assumes that you have already performed the steps for the WLC under *Setup by means of preconfigured integration* on page 87, so that you can complete the basic configuration and enable AutoWDS on the WLC.

Note: In general, we recommend a maximum of 3 hops for AutoWDS operations.

Changes to the initial scenario

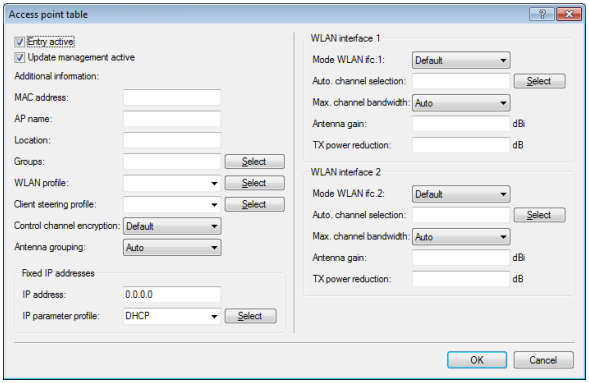
The initial scenario is similar to the preconfigured integration. The entire infrastructure is based on dual-radio APs, which are arranged according to the illustration below. The managed WLAN initially consists of a single AP, which serves as the initial anchor AP for the unassociated APs.



Configuring the WLC

The following instructions describe how to disable the automatic topology management and the configuration of manual P2P links according to the scenario described under *Manual topology management* on page 94.

1. Open the configuration dialog in LANconfig and click on **WLAN controller** > **AP configuration** > **Access point table** to access the list of managed access points.



2. For each unassociated AP, enter the **MAC address** and a unique identifier under **AP name**. You will reference this name later in the topology configuration.

   For the example scenario, the individual configuration entries are as follows:

Entry	*MAC address*	*AP name*
01	00-80-63-a6-3d-f0	AP-00
02	00-a0-57-99-c6-4f	AP-01
03	00-80-63-b1-df-87	AP-02
04	00-a0-57-12-a8-01	AP-03
05	00-80-63-d9-ae-22	AP-04
06	00-a0-57-60-c4-3d	AP-05
07	00-a0-57-24-d4-1b	AP-06
08	00-80-63-a8-b1-37	AP-07
09	00-80-63-b1-df-99	AP-08
10	00-a0-57-33-e1-05	AP-09

Table 2: Configuring the unassociated APs in the access point table

   Note: The table entry AP-00 refers to your existing AP, which the unassociated APs use as an anchor AP.

3. Select the **WLAN profile** for which you have enabled AutoWDS.

By means of the corresponding WLAN profile, the APs automatically receive the settings for AutoWDS and hence for the P2P configuration.

4. Close the dialog window with **OK** and save the configuration to the device.
5. Log on to your device via WEBconfig or the console.
6. In the setup menu, navigate to the table **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**.
7. Edit the AutoWDS default profile by clicking on the entry **DEFAULT**.
8. Change the **Topology-Management** parameter to **Manual** and save the settings by clicking on **Send**.
9. Navigate to the table **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology** and click on **Add**.
10. For each P2P pair, create a manual P2P configuration. The specified P2P link is always considered from the perspective of the slave AP.
    a) In the field **AutoWDS-Profile**, specify the AutoWDS profile that applies for the manual P2P configuration, for example `DEFAULT`.
    b) Set the **Priority** of the P2P configuration to `0` (highest priority).
    c) For the **Slave-AP-Name** and **Master-AP-Name**, enter the names of the APs according to your hierarchy.

    For the example scenario, the individual configuration entries in the case of strict interface pairing are as follows:

Entry	*Slave-AP-Name*	*Slave-AP-WLAN-Ifc.*	*Master-AP-Name*	*Master-AP-WLAN-Ifc.*
01	AP-01	WLAN-1	AP-00	WLAN-1
02	AP-02	WLAN-2	AP-01	WLAN-2
03	AP-03	WLAN-1	AP-02	WLAN-1
04	AP-04	WLAN-2	AP-00	WLAN-2
05	AP-05	WLAN-1	AP-04	WLAN-1
06	AP-06	WLAN-2	AP-05	WLAN-2
07	AP-07	WLAN-1	AP-00	WLAN-1
08	AP-08	WLAN-2	AP-07	WLAN-2

Entry	*Slave-AP-Name*	*Slave-AP-WLAN-Ifc.*	*Master-AP-Name*	*Master-AP-WLAN-Ifc.*
09	AP-09	WLAN-1	AP-08	WLAN-1

Table 3: Configuring the P2P pairs in the AutoWDS topology table

d) Under **Key** specify the WPA2 passphrase used by the P2P partners to encrypt the P2P link.

   Select the most complex key possible, with at least 8 and maximum 63 characters. The key requires at least 32 characters to provide encryption of suitable strength. If you leave the field blank, the device automatically generates a passphrase with a length of 32 characters.

e) Switch the entry **Enabled** to **Yes**.
f) Save the entries by clicking on **Send**.

If APs were already connected, the WLC sends the new configuration to these APs, which triggers the reconfiguration procedure for each one. If no APs were connected, the WLC transmits the P2P configuration when the unassociated APs connect for the first time.

7.1.8 Redundant paths by means of RSTP

In combination with the rapid spanning tree protocol (RSTP), manual topology management allows you to set up redundant P2P links to improve the failover reliability of your entire AutoWDS base network. To do this, you must first enable RSTP in the Setup menu of each AP, because the WLC management settings do not include this part of the configuration. You can reduce the work involved by transmitting a script to all of the APs by means of the WLC script management.

The following steps show you how to do this. These steps assume that you have successfully set up an AutoWDS base network. After activation, RSTP automatically performs the path search.

1. Create a text file with the name `WLC_Script_1.lcs`.
2. Copy the following lines of code into the text file and save it.

```
# Script (9.000.0000 / 15.07.2014)

lang English
```

```
flash No

set /Setup/LAN-Bridge/Spanning-Tree/Protocol-Version        Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Path-Cost-Computation   Rapid
set /Setup/LAN-Bridge/Spanning-Tree/Operating               yes

flash Yes

# done
exit
```

3. Login to the WEBconfig interface of your WLC and navigate to **File management** > **Upload certificate or file**.
4. In the **File type** selection list, select **CAPWAP - WLC_Script_1.lcs** and use the **Browse** button to locate your script file. Then click on **Start upload**. You can check if the file was successfully uploaded to the WLC in the Status menu under **File system** > **Contents**.
5. Navigate to the Setup menu item **WLAN management** > **Central firmware management** > **Script management** and click on **Add**.
6. For the **Profile** enter the corresponding WLAN profile and under **Name** enter `WLC_Script_1.lcs` in order to link the AutoWDS profile with the script name and to roll it out to the APs.
7. As described in section *Configuring the WLC* on page 95, assign unique names to the APs in the WLC and set up the manual P2P links.

You have now successfully completed the configuration.

7.2 IP-dependent auto configuration and tagging of APs

The easiest way to manage all of the APs that you add to a managed network is to use a flat hierarchy. However, in the largest installations with hundreds of APs across several locations, this type of organization quickly becomes confusing and creates a high level of administrative effort. Setting up **Assignment groups** can help to simplify the management of distributed APs. The WLC can automatically to configure each new AP based on the IP addresses it receives. Manual assignment of an IP parameter profile, a WLAN profile and a Client-steering profile by an administrator is no longer required.

The following describes how an assignment group is used when an unassociated AP registers with a central WLC: After the new APs are installed on site (e.g. at a company or branch network), they try to establish a connection to the specified WLC and obtain a configuration via CAPWAP. The WLC detects the connection requests and, for each new AP, it checks the access point table for a suitable AP profile (e.g., the default profile) and/or whether a suitable assignment group has been defined. If one or more configuration options are available, the WLC checks them for the following states:

1. For a new AP there is an assignment group but no AP profile. In this case, the WLC assigns the profile specified in the assignment group to the new AP.
2. For a new AP there is both an assignment group as well as an AP profile. In this case, the WLC ignores the assignment group and assigns the profile defined in the AP profile to the new AP.
3. For a new AP, there is an AP profile but no assignment group. The behavior is the same as point (2).

If a new AP has neither an AP profile nor an assignment group, the WLC issues an alarm to notify the administrator of the incorrect configuration.

After successful group assignment, the WLC automatically creates an AP profile for every new AP in the access point table. In the **Groups** field, the WLC references the assignment group used when it added the new AP.

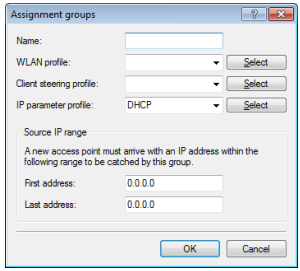
Important: An AP is only ever allowed to receive one assignment group. If the IP address ranges of the assignment groups should overlap, HiLCOS immediately detects the configuration error and writes the messages to the corresponding status table under **Status** > **WLAN-Management** > **AP-Configuration**.

The group field also gives you the the option of assigning individually definable tags to an AP. For example, these **Tag groups** can be used to act as filter criteria in order for the WLC to restrict the actions it performs to a selection of APs.

7.2.1 Setting up assignment groups for IP-dependent auto configuration

The following tutorial shows you how you setup assignment groups on a WLC for the IP-dependent automatic configuration of new APs.

1. Open the configuration dialog for your device and select **WLAN controller** > **AP configuration** > **Assignment groups**
2. Click on **Add** to create a new group.



3. Enter under **Name** a unique descriptor for the assignment group, for example, `Berlin_branch`.
4. Select the **WLAN profile** that the WLC automatically assigns to a new AP if the IP address of the new AP is within the source IP range.
5. Enter the **IP parameter profile** if the new AP should receive a manual network configuration. Otherwise, leave the value as **DHCP**, whereby the AP automatically gets a network configuration from the DHCP server. The DHCP server must be configured to do this.

   If you wish to assign a manual network configuration in which a new AP receives a different IP address, you specify the corresponding address range in the **IP parameter profile** under **Address assignment pool**.

6. **Optional**: Specify a **Client-steering profile** in order to forward future WLAN clients to the ideal AP in case there are several new APs within transmission range.

   Important: If you activate client steering, this must be activated for every AP in the managed infrastructure. Refer to section *Client steering by WLC* on page 120 for further information on this.

7. Enter the start and end of the **Source IP range** relevant to the assignment group.
   A new AP must register at the WLC with an IP address from this range in order to obtain the configuration for this group.
8. Close all dialog windows with **OK** and save the configuration to your device.

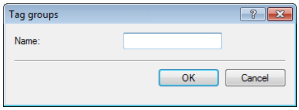
From now on, the WLC assigns the profiles referenced in the assignment groups to all new APs. The HiLCOS console can now provide you with information about the categorization, see *Overview of CAPWAP parameters with the show command* on page 103.

Important: Please ensure that the access point table does not contain an AP profile (e.g., the default profile), which the WLC would assign to the unassociated APs. If an appropriate AP profile is available, this always takes higher priority than the assignment groups.

7.2.2 Setting up tag groups for the detailed selection of APs

The following tutorial shows you how a tag group can be added to an AP configuration on a WLC. To do this, you first create a tag group and then assign it to a WLAN profile.

1. Open the configuration dialog for your device and select **WLAN controller** > **AP configuration** > **Tag groups**
2. Click on **Add** to create a new group.



3. Under **Name** you enter the new tag and save the entry with **OK**.
4. Navigate to the dialog with **WLAN controller** > **AP configuration** > **Access point table**.
5. Select an existing access point profile with **Edit** or add a new one, if necessary.
6. Under **Groups** select the tag group(s) created earlier.
   Multiple tag groups can be specified in a comma-separated list.

Note: The tag groups are independent of the assignment groups, the assignment of which is specified in the same field. Assignment groups are generally assigned by the device, so this does not need to be done by the user. The manual allocation of an assignment group has no effect on the AP configuration, which is in line with the state check described under *IP-dependent auto configuration and tagging of APs* on page 99. The only effects are on the filtering in the command `show capwap group` at the console

Important: The manual addition of assignment group for filtering purposes is not recommended. You should create separate tag groups instead.

7. Close all dialog windows with **OK** and save the configuration to your device.

From now on the WLC gives the tags in the edited WLAN profile to those APs that received it.

7.2.3 Enhancements to command-line commands

Overview of CAPWAP parameters with the show command

The following information about the CAPWAP service can be viewed using the command line:

Parameters	*Meaning*
`-addresses [<IfcNum>]`	Shows the address tables of an individual or all WLC tunnels. In the case of an individual WLC tunnel, enter for the `<IfcNum>` the number of logical WLC tunnel interface, for example `10`.
`-groups`	Shows the information for an individual or all available assignment/tag groups.

Table 4: Overview of all CAPWAP parameters with the show command

You can supplement the command `show capwap groups` with the parameters listed below, which control the scope of the displayed information:

Parameters	*Meaning*
`all`	Shows the names configured in the setup menu and the device's internal names for all assignment/tag groups as well as the default groups that were set up. The default group represents an internal group which contains all APs.
`<group1> <group2> <…>`	Shows all APs of the respective assignment/tag groups.
`-l <location>`	Shows all APs of the respective location.
`-c <country>`	Shows all APs of the respective country.
`-i <city>`	Shows all APs of the respective city.
`-s <street>`	Shows all APs of the respective street.
`-b <building>`	Shows all APs of the respective building.
`-f <floor>`	Shows all APs of the respective floor.
`-r <room>`	Shows all APs of the respective room description.
`-d <device>`	Shows all APs that have the specified device name.
`-a <antenna>`	Shows all APs which have the specified antenna number.
`-v <firmware>`	Shows all APs which have the specified firmware. To do this, enter the version number for `<firmware>` followed by the build number, e.g., `9.00.0001`.
`-x <firmware>`	Shows all APs with a firmware version lower than the one installed on the current device.
`-y <firmware>`	Shows all APs with a firmware version the same or lower than the one installed on the current device.
`-z <firmware>`	Shows all APs with a firmware version higher than the one installed on the current device.
`-t <firmware>`	Shows all APs with a firmware version the same or higher than the one installed on the current device.
`-n <intranet>`	Shows all APs with an IP belonging to the specified Intranet address.
`-p <profile>`	Shows all APs that have been assigned with the specified WLAN profile.
`rmgrp <group1 intern_name> <group2 intern_name> …`	Deletes the group(s) with the specified internal names from the memory of the device. Use this command to free up the main memory if too large a number of groups is degrading the performance of the device. The entry in the setup menu is unaffected by this action.

Parameters	*Meaning*
`resetgrps`	Deletes all groups except the default group.

Table 5: Overview of all CAPWAP group parameters with the show command

For location information the device evaluates the information entered under **Location** in the access point table. The following field names are available:

- co=Country
- ci=City
- st=Street
- bu=Building
- fl=Floor
- ro=Room

For instance, the location entry `co=Germany, ci=Aachen` allows you to list all of the managed APs in Aachen from the console of the WLC with the command `+show capwap group -i Aachen`.

Example commands

```
show capwap group all
show capwap group group1
show capwap group -l yourlocation
show capwap group -s yourstreetname
show capwap group -d yourdevicename
show capwap group -p yourprofilename
show capwap group -d yourdevicename -p yourprofile -v yourfirmversion …
```

7.3 Automatic selection of the 2.4-/5-GHz mode

As of HiLCOS 8.90, the configuration of the WLAN physical parameters on WLCs and also on APs now includes the option of allowing the AP to select a suitable 2.4-/5-GHz mode.

- 2.4-GHz mode / 5-GHz mode

  Here you specify the wireless standard(s) that the physical WLAN interface provides to the WLAN clients.

In the 2.4-GHz and the 5-GHz frequency bands, there are several different wireless standards that an AP can use for transmission. In the 2.5-GHz frequency band, these were to date the standards IEEE 802.11b, IEEE 802.11g and IEEE 802.11n; in the 5-GHz frequency band, the standards are IEEE 802.11a, IEEE 802.11n and IEEE 802.11ac. Depending on the device type and selected frequency band, you have the option of operating an AP in just one particular mode or one of the compatibility modes.

Important: Please observe that WLAN clients supporting only a slower standard may not be able to associate with the WLAN if the value for the mode is set too high. However, compatibility is always achieved at the expense of performance. It is therefore recommended to allow only those modes of operation that are absolutely necessary for the wireless LAN clients in use.

For example, if there are only 802.11n-enabled devices in your WLAN, it is recommended to select greenfield mode (**802.11n only**): By doing this you prevent login of slower clients which would otherwise act as a brake on the network.

By selecting a compatibility mode, you are able to achieve the best possible data rates without excluding slower WLAN clients (e.g., for 2.4 GHz **802.11g/b/n (mixed)**; for 5 GHz **802.11a/n (mixed)**). In compatibility mode, a physical WLAN interface works according to the fastest standard, but reverts to a slower standard if a slower WLAN client logs on to the network. When using 802.11b, you can select whether the physical WLAN interface should exclusively support 11-Mbps mode or also the older 2-Mbps mode (**... (2-Mbps-compatible)**).

For APs operating according to the 802.11g standard you can optionally increase the data transfer speeds up to 108Mbps. In what is referred to as Turbo mode, an AP simultaneously uses two neighboring free channels for the radio transmission. With an AP in the 108Mbps Turbo mode, the only WLAN clients that can establish a connection to this AP are those also operating with the 108Mbpss Turbo mode.

Note: Turbo mode is associated with the 802.11g standard, although it was never officially adopted by the IEEE. The technology represents the proprietary extensions of various chipset manufacturers who also market

this technology under the name “802.11g+” or “802.11g++”. Turbo mode is therefore exclusively available on APs with pure 802.11g hardware.

If you leave the selection of the 2.5/5-GHz mode up to the device with the **Automatic** setting, the selection of the best mode depends on the frequency band in use and the capabilities of the device hardware:

- In the 2.4-GHz mode, the automatic setting results in either **802.11g/b/n (mixed)** or **802.11 g/b (mixed)**.
- In the 5-GHz mode, the automatic setting results in either **802.11ac/a/n (mixed)**, **802.11 a/n (mixed)**, or **54Mbps mode**.

In principle, according to 802.11n APs in the 2.4-GHz frequency band are backwards compatible to the IEEE 802.11b and IEEE 802.11g standards. Only the 802.11n-specific functions are not available for 802.11n hardware operated in 802.11b or 802.11g mode. However, this backwards compatibility is not available in the 5-GHz frequency band: The affected 802.11n devices must explicitly support 802.11a.

7.4 WLC cluster

If you are operating multiple WLCs in your network, you can collect these devices into a cluster. The APs in a managed WLAN are no longer managed by a single, central WLC but by multiple, synchronized WLCs. For large networks in particular, a WLC cluster provides numerous advantages:

- Automatic network “load balancing” between the individual APs and WLCs;
- Increased failover reliability through the provision of backup WLCs (“hot standby”) and automatic redistribution of the APs in the case of a WLC failure;
- Setting up a certificate hierarchy: Management of certificates by a central certification authority (CA), represented either by a master WLC or an external station (such as a server).

As of HiLCOS 8.90, the cluster function received numerous enhancements described below.

7.4.1 WLC tunnel for internal communication

The use of WLC tunnels is essential for a WLC cluster. The WLCs in the WLC cluster use this tunnel to communicate with one another and keep their status information aligned. With the feature extensions as of HiLCOS 8.90, the way that HiLCOS deals with WLC tunnels is also improved:

- WLCs are able to find one another automatically.
- You have the option to statically configure WLC tunnels.
- WLCs disconnect a WLC tunnel only after a timeout.
- WLC tunnels can be switched on or off globally.

The settings for the WLC tunnels and other WLCs (remote WLCs) are located in the section **WLAN controller** > **General** > **WLC cluster**. The setting **WLC tunnel active** allows you to disable the usage of WLC tunnels, which in effect causes the clustering feature to be switched off.

7.4.2 Setting up a CA hierarchy

In order to operate multiple WLAN controllers in a WLC cluster, they must all have identical configurations. This also includes the certificates used within the WLC cluster. The solution lies in establishing a certificate hierarchy, also known as a CA hierarchy: This involves defining the CA of a WLC as the root-CA. The other WLCs retrieve this certificate for their (sub-) CA.

The following scenario shows you the configuration steps which are necessary for setting up a CA hierarchy. As examples, the configuration is done using two WLCs:

- WLC-MAIN represents the device with the root-CA;
- WLC-SUB is the device which obtains a certificate from the root-CA in order to issue further certificates as a sub-CA.

Configuring the root-CA

The following section describes how to set up a root CA on a WLC. These steps assume that the device has been reset, that you have commissioned the device in the standard manner, and that you have set the correct time.

1. Login to your device via WEBconfig or the command line.

2. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** > **CA-Certificates**. Customize the name of the certificate authority (CA) and the registration authority (RA) with the parameters **CA-Distinguished-Name** and **RA-Distinguished-Name**.

   Example: `/CN=WLC-MAIN CA/O=HIRSCHMANN/C=DE`

3. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** and set the parameter **Operating** to **Yes**.

You have now completed the configuration of the root CA. The command `show ca cert` on the command line allows you to verify that the WLC has created the certificate correctly.

Configuring the sub-CA

The following section describes how to set up a sub-CA on a WLC. These steps assume that the device has been reset, that you have commissioned the device in the standard manner, and that you have set the correct time.

1. Login to your device via WEBconfig or the command line.
2. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** and set the parameter **Root-CA** to **No**.
3. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** > **CA-Certificates**. Customize the name of the certificate authority (CA) and the registration authority (RA) with the parameters **CA-Distinguished-Name** and **RA-Distinguished-Name**.

   Example: `/CN=WLC-SUB CA/O=HIRSCHMANN/C=DE`

4. Switch to the menu **Setup** > **Certificates** > **SCEP-CA** > **Sub-CA** and enter the distinguished name of the root-CA under the parameter **CADN**.

   Example: `/CN=WLC-MAIN CA/O=HIRSCHMANN/C=DE`

5. For the parameter **Challenge-Pwd** , enter the challenge password that is stored on WLC-MAIN under **Setup** > **Certificates** > **SCEP-CA**.
6. Enter the URL (address) to the root CA in the **CA-Url-address** parameter. If another WLC with the HiLCOS operating system provides the root CA, all you need to do is replace the IP address in the default value with the address where the corresponding device is to be reached. Example: `http://192.168.1.1/cgi/bin/pkiclient.exe`.

7. Optional: Specify the **Ext-Key-Usage** and **Cert-Key Usage** to restrict the functions of the sub-CA. For more information, see the CLI-Reference.
8. Set the parameter **Auto-generated-request** to **Yes** to activate the sub-CA.
9. Navigate to the menu **Setup** > **Certificates** > **SCEP-CA** and set the parameter **Operating** to **Yes** to enable the CA server with SCEP.

You have now completed the configuration of the sub-CA. The command `show ca cert` on the command line allows you to verify that the WLC has created the certificate correctly. The hierarchy of certificates must be visible here: The WLC first displays the certificate of the root CA and then the certificate of the sub-CA.

7.4.3 Enabling/disabling CAPWAP in the WLC

In order to operate multiple WLAN controllers in a cluster, they must all have identical configurations. This is not the case on one WLC by default, since it automatically generates certain configuration parts (such as certificates). By disabling CAPWAP on all devices except one, you have the option of setting one of the devices in your WLC cluster as a master controller. The other WLCs can be synchronized with the master controller's configuration.

7.4.4 Finding the ideal WLC

The algorithms implemented in HiLCOS ensure that the APS are intelligently distributed between the individual WLCs. This allows the APs to equally distribute the network load between all of the WLCs in a cluster, or to select an alternative WLC if one should fail. For this, an AP first sends out a discovery request on the network to identify all available WLCs. The WLCs then respond with a discovery response which an AP uses to create a prioritized list of WLCs. This AP prioritizes the list based on various criteria.

An AP works through the different criteria sequentially: If multiple WLCs appear to be ideal candidates after applying a criterion, the AP uses the next criteria to prioritize. This process ends when a WLC finally identifies just one WLC as being ideal after the prioritization described in the following.

Criteria for prioritization

- **Specificity of the AP configuration**: An AP evaluates whether a WLC can provide it with a configuration, and whether this contains a specific AP

profile or a default profile. The AP prioritizes a specific AP profile as highest, followed by a default profile. If a profile is missing, it is given the lowest priority.

- **The preference value**: The AP evaluates the preference value that you have assigned to a WLC. The higher the number between 0 and 255, the higher the AP prioritizes the WLC.

If there still remain several WLCs which are considered to be ideal, the prioritization process continues by evaluating the connection status and the type of selection process (automatically vs. manually initiated):

- When the **calculation is triggered for the first time**, an AP calculates a weighted value for each of the remaining WLCs by taking the number of APs connected to each WLC and comparing this with the maximum possible number of APs (**license usage**). Ultimately, the ideal WLC is taken as that with the lowest license usage.

  Note: If a WLC has reached the maximum possible number of AP connections (license quota exhausted), an AP no longer considers the affected WLC for the current selection.

- In the case of **automatic checking** of the ideal AP distribution, an AP stays with the WLC it is connected to if this WLC is included in the list of the remaining WLCs. Otherwise, a **randomized algorithm** causes the AP to select an arbitrary AP.
- In the case of a **manually triggered check**, a **randomized algorithm** ensures that the APs distribute the available license quotas as evenly as possible across the network.

7.4.5 Determining the ideal AP distribution

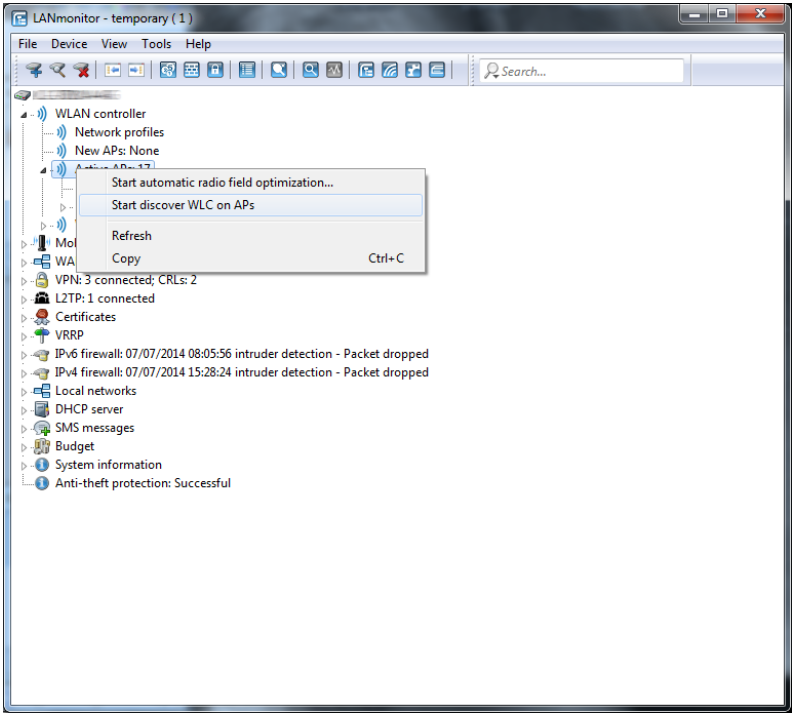
The identification of the ideal AP distribution in a WLC cluster and any redistribution that may be triggered by it occur automatically. Every AP automatically performs the *Finding the ideal WLC* process at irregular intervals between 30 and 60 minutes. If the result of the process is positive for the WLC which is already connected, no redistribution takes place. If a different WLC has a higher priority, the AP attempts to connect to this WLC.

However, as an administrator you can use LANmonitor to manually trigger a calculation of the ideal AP distribution and the resulting redistribution of the APs (see *Manually initiate ideal AP distribution* on page 112).

7.4.6 Manually initiate ideal AP distribution

The following steps show you how to start the recalculation of an ideal distribution, and if necessary to trigger a redistribution.

1. Start LANmonitor and select a WLC.
2. Navigate to the menu item **Wireless LAN** > **Active APs**.
3. Open the context menu on any AP and select **Start WLC search on APs**.



The access points each find their optimum WLC and distribute themselves across the WLC cluster according to the specifications.

7.5 One-click backup of the SCEP-CA

In order to simplify the backup of the CA in the WLC, the device offers the option to generate a complete certificate record with a single action (one-click backup). This record makes it possible to completely back up and restore the CA and prevent certificate conflicts from occurring.

These conflicts can occur if you have downloaded the individual PKCS12 containers from the device separately and then reloaded: If the WLC has created a new CA in the meantime and has issued new certificates, the deviating CAs temporarily lead to authentication problems for the different services in HiLCOS. If you cannot wait until the individual services request new certific-ates, a manual resolution requires deleting the SCEP files from the HiLCOS file system and re-initialization of the SCEP clients. By reloading a one-click backup, on the other hand, HiLCOS performs the necessary steps automatic-ally.

Creating a backup file

In order to create a certificate record, perform the action **Create PKCS12 backup files** under **Setup** > **Certificate** > **SCEP-CA** > **CA certificate**. This action generates a ZIP file within the HiLCOS file system that contains all necessary files. To protect the certificates and keys contained therein, the ZIP file is automatically protected with the device password, unless you enter another password. The ZIP file that was generated can then be downloaded, for example, in WEBconfig via **File management** > **Download certific-ate or file** > **SCEP-CA - One Click Backup**.

Reloading the backup file

In order to reload certificate records, load the saved ZIP file directly into the device using the passphrase. In WEBconfig, for example, this is done by selecting **File management** > **Upload certificate or file** > **SCEP-CA - One Click Backup**. Enable the option **Replace existing CA certificates** so that the device automatically restores the certificate record after the upload.

Note: If you do not use this option, or if you upload the backup file to the device by other means, you must execute the action 2.39.2.2.11 Restore-certificates-from-Backup in order for the device to restore the certificate record.

7.6 Automatic restart of managed APs after firmware update

As of HiLCOS 8.90 you have the option in the WEBconfig menu **Extras** > **Load firmware in managed APs** to automatically start the APs after the manual upload of a new firmware version.

7.6.1 Load firmware in managed AP

This menu item is only available on WLAN controllers (WLCs).

On this page, you have the option of using remote access to manually update the firmware on an AP managed by the WLC. For example, this might make sense in order to test firmware on selected APs before using it productively. To do this, select an AP by its MAC address and select the appropriate firmware file. Next click on **Start upload** to load the firmware in the AP.

Note: Please note that this process disables the firmware management in the AP table for the selected AP. This prevents the WLC from automatically uploading a different firmware version. Firmware management can be re-enabled at any time in the setup menu under **WLAN-Management** > **AP-Configuration** > **Manage-firmware**.

In order for the access point to use the loaded firmware, you must subsequently perform a restart. By enabling the setting **Restart AP after updating the firmware** you trigger an automatic restart as soon as the firmware upload is completed.

7.7 Automatic search for alternative WLCs

As of HiLCOS 8.90, an AP no longer attempts to reconnect to the last known WLC in case of a disconnection. Instead, the AP searches in the network for an available WLC which corresponds to the criteria for the *Finding the ideal WLC*.

7.8 U-APSD configurable by WLC

As of HiLCOS 9.00 you have the additional option of enabling WLCs to configure the power-saving mechanism (U-)APSD for individual SSIDs.

7.9 Group-related radio field optimization

The Hirschmann WLAN controllers can form groups of access points based on location information, device properties or network structure. This grouping can also be used as a basis for radio field optimization. Instead of performing a radio field optimization either for all access points or just for one of them, you can address all of the access points within a building tract, with a particular name, or with a particular firmware version.

You can address the groups by using the appropriate group parameters in WEBconfig, LANmonitor and from the command line:

```
do /Setup/WLAN-Management/start optimization <Group>
```

The access points can be filtered with the following group-parameter options:

`-g <Group name>`

Access points belonging to the group. Multiple group names can be separated by commas.

`-l <Location>`

Access points with the matching setting for location.

Note: The combination of `-l` and one of the location options `-c` to `-r` is not useful.

`-c <Country>`

Access points with the matching country.

`-i <City>`

Access points with the matching city.

`-s <Street>`

Access points with the matching street.

`-b <Building>`

Access points with the matching building.

`-f <Floor>`

Access points with the matching floor.

`-r <Room>`

Access points with the matching room.

`-d <Device name>`

Access points with the matching device name.

`-a <Antenna>`

Access points with the matching number of antennas.

Note: A combination of the options `-d` and `-a` is not useful.

`-v <Firmware>`

Access points with this firmware version only.

`-x <Firmware>`

Access points with a firmware version lower than that specified here.

-y <Firmware>

Access points with a firmware version lower than or equal to that specified here.

-z <Firmware>

Access points with a firmware version higher than that specified here.

-t <Firmware>

Access points with a firmware version higher than or equal to that specified here.

Note: Combinations are possible, e.g. to address access points with a firmware version between two versions.

-n <Intranet address>

Access points located on the intranet with the address specified here.

-p <Profile name>

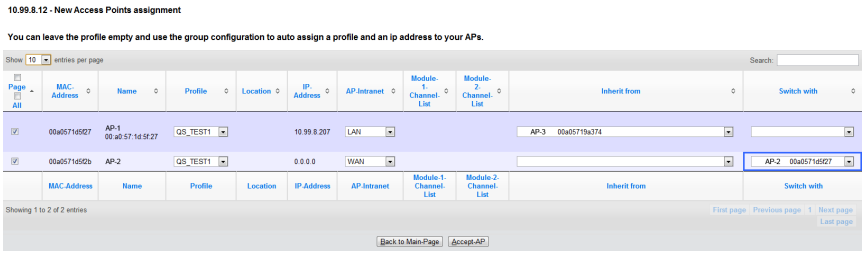
Access points included in the WLAN profile specified here.

7.10 Adding new APs with the WEBconfig Setup Wizard

As of HiLCOS 9.00, WLCs have a revised Setup Wizard **Assign Access Points to Profiles**, which makes it easier to add new APs via WEBconfig. Just a few mouse clicks with the new Setup Wizard allows you to

- Make a targeted search for a new AP;
- Accept one or more new APs at the same time;
- Assign a WLAN profile or a channel list to a new AP;
- Allow a new AP to inherit the configuration from an accepted AP;
- To exchange the configuration in a new AP for that of an accepted missing AP. When exchanging a configuration, the new AP receives the complete configuration of the accepted missing AP (except for its MAC address).

When the new AP has been integrated, the WLC then deletes the configuration of the accepted missing AP.



Click **Accept AP** to include the new AP with its new settings into the network.

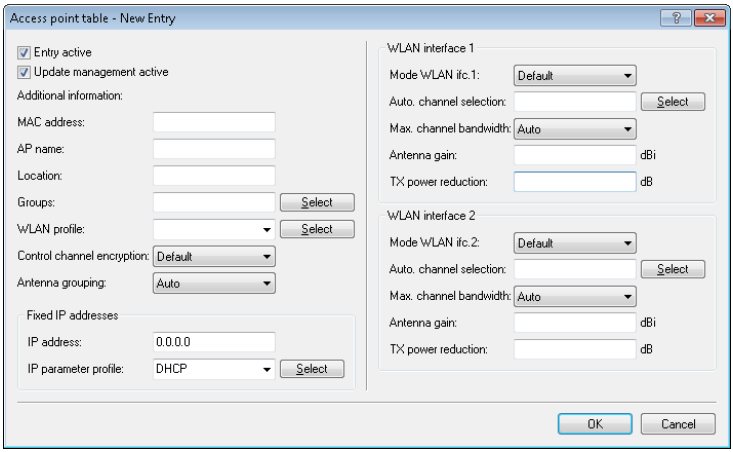
Note: If you have allowed an AP to be configured via assignment groups, there is no need for any further settings for this AP in the Setup Wizard. The WLC automatically assigns the settings for the appropriate groups to the AP.

7.11 Maximum bandwidth can be adjusted for each WLAN module

As of HiLCOS 8.90, you are able to set the maximum bandwidth for each WLAN module.

It is no longer possible to force 40MHz channel bundling.

Changes to WLCs



Max. channel bandwidth

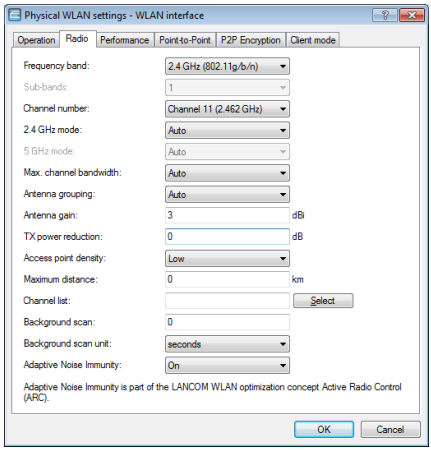
Enter how and to what extent the AP specifies the channel bandwidth for the physical WLAN interface(s). The following values are possible:

- **Automatic**: The access point automatically detects the maximum channel bandwidth (default).
- **20MHz**: The access point uses channels bundled at 20 MHz.
- **40MHz**: The access point uses channels bundled at 40MHz.
- **80MHz**: The access point uses channels bundled at 80MHz.

By default, the physical WLAN interface automatically determines the frequency range used to modulate the data onto the carrier signals. 802.11a/b/g use 48 carrier signals in one 20-MHz channel. The use of double the frequency range of 40 MHz means that 96 carrier signals can be used, resulting in a doubling of the data throughput.

802.11n can use 52 carrier signals in a 20-MHz channel for modulation, and even up to 108 carrier signals in a 40-MHz channel. The use of the 40 MHz option for 802.11n therefore means a performance gain of more than double.

Changes to stand-alone APs



7.12 Client steering by WLC

With client steering, certain criteria are used to help WLAN clients located within transmission range to connect to the best suited AP. These criteria are centrally defined in the WLAN controller. Managed access points constantly report the current values to the WLAN controller, which uses these criteria to decide which access points may respond to requests from WLAN clients. For this reason, client steering is only possible with access points that are centrally managed by a WLAN controller.

In managed networks a WLC centralizes the client steering for all connected APs. In this case, client steering works as follows:

1. The WLC collects the data about the associated WLAN clients from the APs connected to it. These data are the basis for the WLC to control the client steering.
2. All APs are configured so that client steering is handled by the WLC.
3. An unassociated WLAN client sends a probe request to the APs within its range.
4. Using CAPWAP, the APs transmit the request and the signal strength of the WLAN client to the WLC.

5. For each AP within range of the WLAN client, the WLC calculates a value from three factors:
   - A value for signal strength
   - A value for the number of clients associated at the AP
   - A value for the frequency band

   The WLC weights these factors and multiplies them together to derive the final value.
6. APs with the highest value, or a value that deviates from it within a specified tolerance level, receive a message from the WLC that they may accept the WLAN client at the next login attempt.
7. WLAN clients attempting to connect to an AP before it has received the response from the WLC are rejected.
8. If a WLAN client is acting "sticky", i.e. it does not attempt to connect to another AP with a good connection quality even though its current connection is of a lower quality, the WLC can prompt the current AP to log off the WLAN client. The WLAN client is then forced to connect with the AP offering the better connection.

Note: If an AP loses connection to the WLC which is responsible for client steering, the AP accepts all connections from authenticated WLAN clients.

Important: In order to optimize managed client steering, all APs require the installation of HiLCOS 9.00 or later. If you have mixed operations with APs using earlier versions of HiLCOS, your WLAN will not be capable of optimizing the distribution of clients.

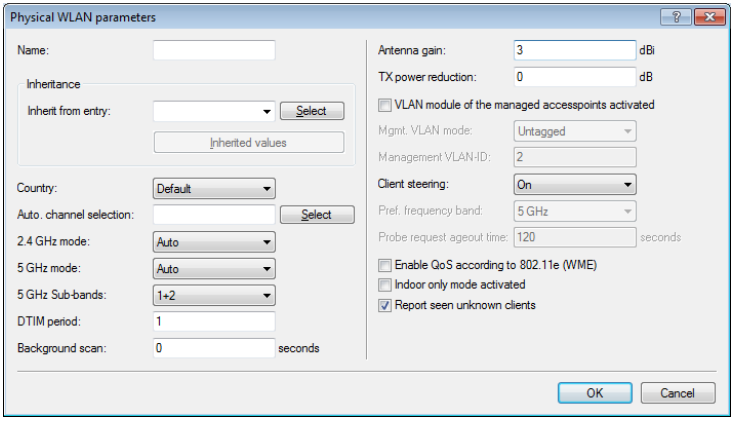
Important: In scenarios with time-critical roaming, such as with VoIP phones, you should not use client steering, as this can delay the client's login process.

7.12.1 Configuration

You configure client steering with LANconfig as follows:

1. First, in the WLC you activate client steering for an AP under **WLAN controller** > **Profiles** > **Physical WLAN parameters** using the selection list **Client steering**.

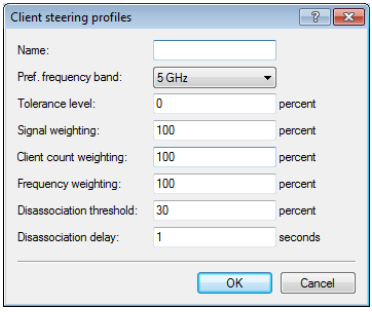
- **Off**: Client steering is deactivated.
- **AP-based band steering**: The AP independently steers the WLAN client to a preferred frequency band.
- **On**: The AP lets the WLC handle the client steering.



2. Create a client-steering profile under **WLAN controller** > **AP configuration** > **Client steering profiles**.

Note: This menu already contains two preconfigured default profiles (high density, default), which are sufficient for most use cases.

Client-steering profiles control how the WLC decides which APs are to accept a client at the next login attempt.



The items have the following meanings:

Name

Name of the client steering profile.

Pref. Frequency band
Specifies the frequency band to which the WLC steers the AP.

- **2.4GHz**: The WLC steers the AP to the 2.4 GHz frequency band.
- **5GHz**: The WLC steers the AP to the 5 GHz frequency band.

Tolerance level
The calculated value for an AP may deviate from the maximum calculated value by this percentage value in order for the AP to be allowed to accept the client at the next login attempt.

Signal weighting
Specifies with how many percent the signal-strength value is entered into the final value.

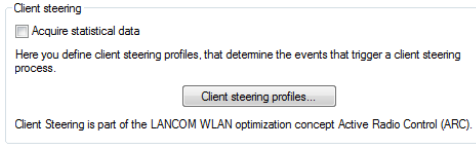
Associated-Clients-Weighting
Specifies with how many percent the number of clients associated with an AP is entered into the final value.

Radio weighting
Specifies with how many percent the value for the frequency band is entered into the final value.

Disassociation threshold
Specifies the threshold value below which the connection to the client must drop before the AP disconnects from the client and initiates a new client-steering operation.

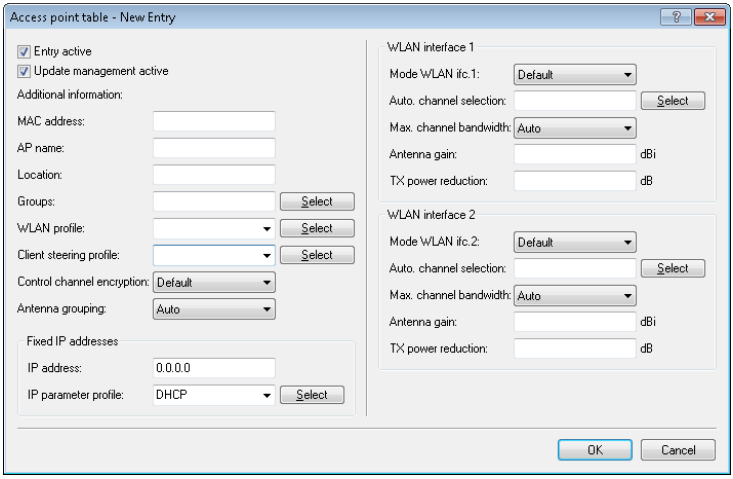
Disassociation delay
Specifies the number of seconds in which no data is transferred between AP and client before the AP disconnects the client.

3. Optional: Enable the capture of client-steering statistics with the parameter **Acquire statistical data**. This statistical data is suitable for analysis by LANmonitor, for example.

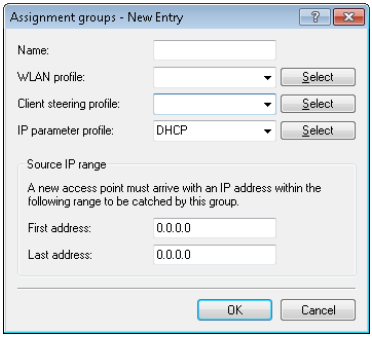


Note: Statistics capture increases the load on the WLC. Hirschmann does not recommend the permanent recording of statistics.

4. Now assign one of the client-steering profiles to the corresponding AP in the AP table under **WLAN controller** > **AP configuration** > **Access point table**.



5. Optional: If necessary, assign a suitable client-steering group to the defined assignment groups.



You have now completed the configuration of the client steering.

7.13 Automatic frequency-band selection

As of HiLCOS 9.00 you have the option to allow a managed AP to choose the preferred frequency band for the physical WLAN interface by itself. In LANconfig the configuration is carried out in the dialog **WLAN Controller** > **AP configuration** > **Access point table**:

Mode WLAN ifc. 1

This setting allows you to configure the frequency band in which the AP operates the 1st physical WLAN interface. When set to **Default**, the AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 2.4GHz band, if available.

Mode WLAN ifc. 2

This setting allows you to configure the frequency band in which the AP operates the 2nd physical WLAN interface. When set to **Default**, the AP independently selects the frequency band for the physical WLAN interface. The AP prefers the 5GHz band, if available.

Note: If a managed AP only has one physical WLAN interface, the AP ignores the settings for the 2nd physical WLAN interface.

8 VPN

8.1 VPN remote access wizard in WEBconfig:

As of HiLCOS 8.90 you have the option of using WEBconfig to create VPN-client dial-in accounts using the Hirschmann Advanced VPN Client or an alternative VPN client. This is possible as the existing Setup-Wizard **Provide remote access** has been extended with the VPN option. The setup steps are the same as those for LANconfig.

Note: The 1-Click VPN configuration is not available in WEBconfig due to restrictions on browser access.

8.2 L2TPv2 (Layer-2 Tunneling Protocol version 2)

With L2TP, an L2TP access concentrator (LAC) tunnels the PPP request from a client via a public connection (e.g. Internet, ATM, frame relay) to an L2TP network server (LNS). The LNS serves as a gateway to the remote network. There, a connected RADIUS server initially authenticates the client, if necessary. The LNS then sends the IP address to the LAC and starts the L2TP tunnel. The LAC communicates the IP address to the client. As of this moment, the client has joined the remote network via an L2TP connection.

Within the firmware, the LAC and the PPP client are collected in a role. Thus a device operating as a LAC starts the control channel and the PPP session. For network virtualization, multiple PPP sessions are supported in an L2TP tunnel. An L2TP-enabled device is able to operate as an LAC and also as an LNS.

Data types

L2TP uses two types of data:

Control data

The control data are used to establish, maintain and tear down the tunnel connections. The control data includes a data-flow control to ensure that the sender and receiver correctly exchange the control data.

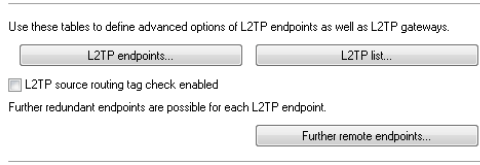
Payload data

The payload data are encapsulated in PPP frames, which are exchanged between the LAC and the LNS via the tunnel. In contrast to the control data, payload data contains no data flow control. Thus there is no guarantee that the sender and receiver are exchanging data correctly.

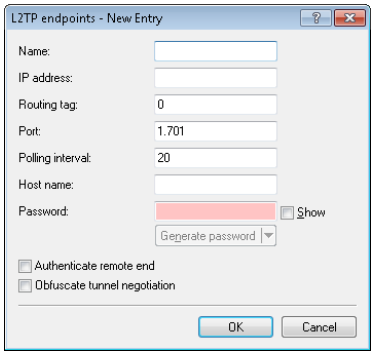
Unlike PPTP, which transfers control and payload data via different protocols (TCP and GRE), L2TP only uses UDP for both data types. You also have the option to operate multiple logical payload-data channels on each control-data channel.

8.2.1 Configuring the L2TP tunnel

With LANconfig, you configure L2TP under **Communication** > **Remote sites**.



The tunnel configuration for the control data of an L2TP tunnel to a tunnel endpoint is located under **L2TP endpoints**.



Name

Name of the tunnel endpoint

IP address

IP address of the tunnel endpoint (IPv4, IPv6, FQDN).

Routing tag

The routing tag of the route to the tunnel endpoint

Port

UDP Port

Polling interval

Polling interval in seconds

Host name

Name used by the device to authenticate at the tunnel endpoint

Password

Password used by the device to authenticate at the tunnel endpoint

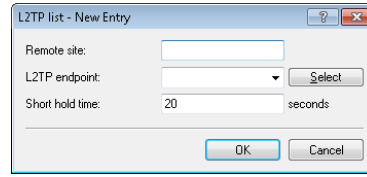
Authenticate remote end

Enable this option if two tunnel endpoints (LAC and LNS) are required to mutually authenticate one another before establishing a tunnel. In this case, the tunnel endpoint name and password for this device are configured as the tunnel endpoint and the option to **Authenticate remote end** is similarly enabled.

Obfuscate tunnel negotiation

If the tunnel negotiations between the LAC and the LNS are to be encrypted, you enable this option. The two L2TP partners encrypt and decrypt the L2TP messages with the help certain AVPs (attribute value pairs) of a common preshared secret.

Under **L2TP list**, you make the link between the L2TP remote sites and a previously configured tunnel endpoint.



An entry in this table is necessary only under the following conditions:

- Outgoing connections
- Incoming connections with an idle timeout not equal to "20" or
- If incoming links specify the use of a specific tunnel only.

Remote site

Name of the L2TP remote device

L2TP endpoint

Name of the tunnel endpoint used by this remote site.

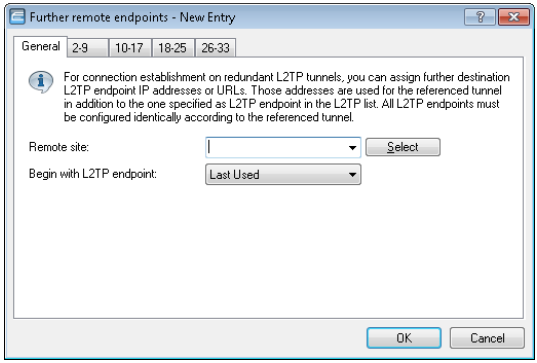
Short hold time

Determines how long the L2TP tunnel endpoint keeps the tunnel open when inactive.

In the case of incoming tunnel requests, a check is performed either by RADIUS or by means of an entry for the requesting host in the L2TP endpoints table. If the table contains an entry with the same IP address (or no IP address is specified for this entry), the device permits tunnel establishment to this host.

For additional protection, for example to enable encryption of the L2TP sessions via IPSec, the device can additionally check the routing tag of the remote site from which it received the data. This option is enabled with **L2TP source routing tag check enabled**.

You have the option to configure up to 32 additional gateways per tunnel endpoint by clicking on **Further remote endpoints**.



Important: Ensure that all additionally specified L2TP endpoints are configured identically to the referenced tunnel endpoint.

Remote site

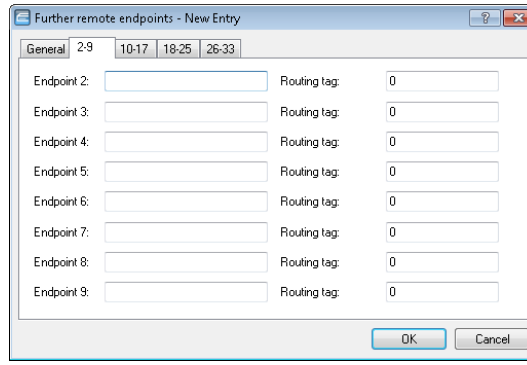
Name of the tunnel endpoint, as configured in the table of **L2TP endpoints**.

Begin with L2TP endpoint

Option for selecting the next gateway. The following options are available:

- **Last used**: Select the last successful address
- **First**: Select the first gateway in the list
- **Random**: Random selection from the gateways in the list

On the following tabs you configure the names and the respective routing tags of the alternative gateways.



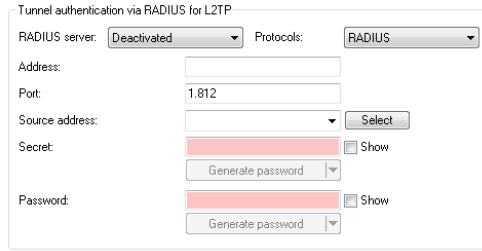
8.2.2 Authentication via RADIUS

RADIUS authentication for L2TP is possible in two cases:

- Tunnel authentication: The RADIUS server checks to see whether a LAC is allowed to establish a L2TP connection.
- PPP session: The RADIUS server checks the user data of the corresponding PPP session.

For this reason, the configuration of the RADIUS server for L2TP-tunnel authentication and the PPP user data are carried out independently of one another.

In the case of tunnel authentication by RADIUS, the settings in LANconfig are configured under **Communication** > **RADIUS** in the section **Tunnel authentication via RADIUS for L2TP**.



RADIUS server

Enables or disables the RADIUS server for the authentication of the tunnel endpoint, regardless of a PPP-session authentication. The following options are possible:

- **Deactivated**: The RADIUS server is not enabled for the authentication of tunnel endpoints.
- **Activated**: The RADIUS server handles the authentication of tunnel endpoints.
- **Exclusive**: Enables the use of the external RADIUS server as the only possibility for authenticating PPP remote sites. The PPP list is ignored.

Protocols

Protocol for communication between the internal RADIUS server and the tunnel endpoint.

Address

IP address or DNS name of the RADIUS server.

Port

The port the RADIUS server

Source address

Optional sender address of the device. If you have configured loopback addresses, these can also be specified here. Following input formats are allowed:

- Name of the IP network (ARF network) whose address is to be used instead
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Secret

Shared secret between the RADIUS server and the device

Password

Dummy password for tunnel authentication

If an L2TP tunnel request arrives from a remote host (Start Control Connection Request), the device sends a request to the RADIUS server that has been enabled for L2TP. This request contains among other things the name of the host, the dummy password, the IP address of the device, and also the service type "Outbound User". The RADIUS server authenticates the host and sends a "RADIUS accept" to the device together with; the tunnel password to be used; the tunnel type "L2TP" with the tag "0"; and also the Tunnel-Client-Auth-ID, which must match with the host name transmitted earlier by the device. The device checks this data and, if the result is positive, it takes the tunnel password to authenticate the dial-in client and, if applicable, to obfuscate the L2TP tunnel negotiations.

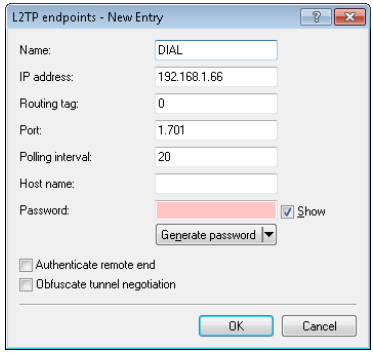
Note: Configuring the RADIUS server to authenticate PPP sessions is conducted as described in the section **Other services** > **RADIUS** > **Configuration of RADIUS as authenticator or NAS** > **Dial-in using PPP and RADIUS**.

8.2.3 Operation as an L2TP access concentrator (LAC)

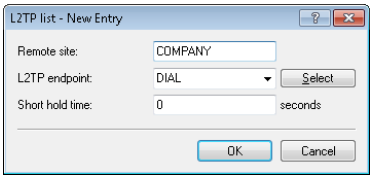
In the following example, the device operating as a L2TP access concentrator (LAC) establishes an L2TP tunnel to an L2TP network server (LNS) with the IP address 192.168.1.66.

Proceed as follows to configure the device as a LAC:

1. Under **Communication** > **Remote sites** in the table **L2TP endpoints** create an entry for an LNS as the remote L2TP gateway.

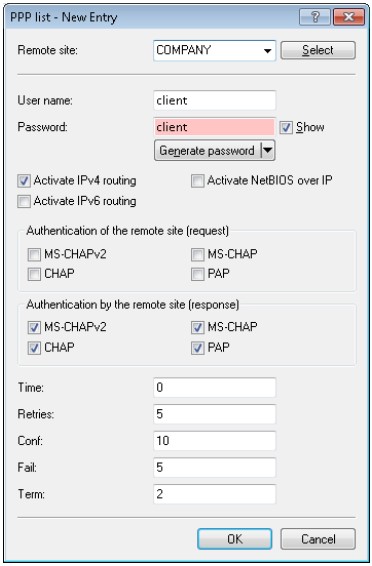


2. Enter a name for this site under **Communication** > **Protocols** in the table **L2TP list** and connect it with the L2TP endpoint you created previously.

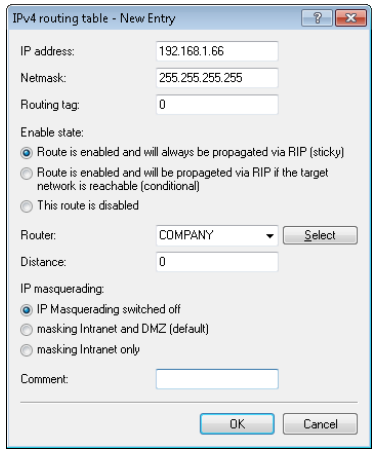


It is possible to connect several remote sites with an L2TP tunnel. This allows multiple PPP sessions to be transported through an L2TP tunnel. For this purpose, configure in this table several remote sites with the same L2TP endpoint.

3. Under **Communication** > **Protocols** in the table **PPP list** create an entry for the L2TP tunnel.



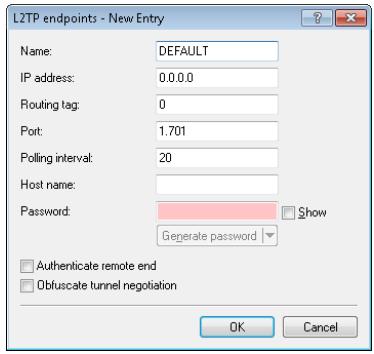
4. For this site, go to **Configuration** > **IP router** > **Routing** and create an entry in the corresponding IPv4 or IPv6 routing table.



8.2.4 Operation as the L2TP network server (LNS) for RAS clients

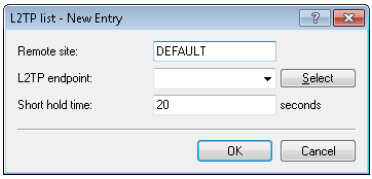
In order to configure the device as the L2TP network server (LNS) for authenticating RAS clients without configuring a RADIUS server in the device, you have two options:

1. Under **Communication** > **Remote sites** in the table **L2TP endpoints**, create an entry "DEFAULT".



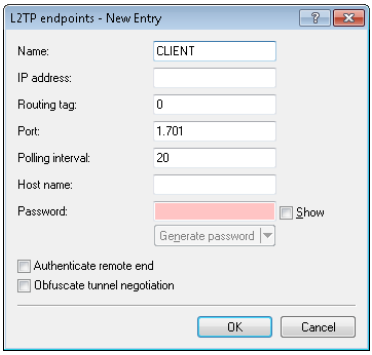
   The entry for the IP address is "0.0.0.0", because the IP address of the L2TP-LAC is unknown to the device.

2. Then, under **Communication** > **Remote sites** in the table **L2TP list**, configure a "DEFAULT" entry.

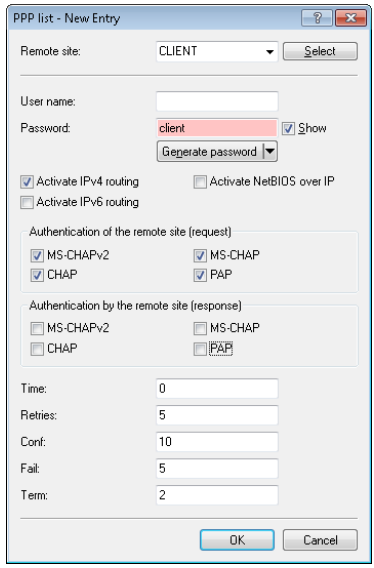


If the L2TP tunnel is to be connected permanently, set the short hold time to "9999".

3. Alternatively, you make a separate entry for the RAS client (e.g., "CLIENT") under **Communication** > **Remote sites** in the **L2TP endpoints** table.



4. You then configure a new entry for the client under **Communication** > **Protocols** in the **PPP list**.

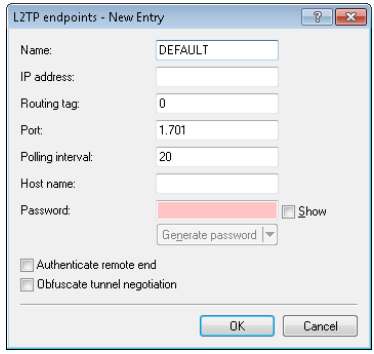


8.2.5 Operation as an L2TP network server (LNS) with authentication via RADIUS

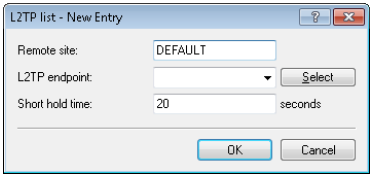
In the following example, the device functions as an L2TP network server (LNS). RADIUS is used to authenticate the incoming L2TP tunnel and the PPP sessions.

Proceed as follows to configure the device as an LNS:

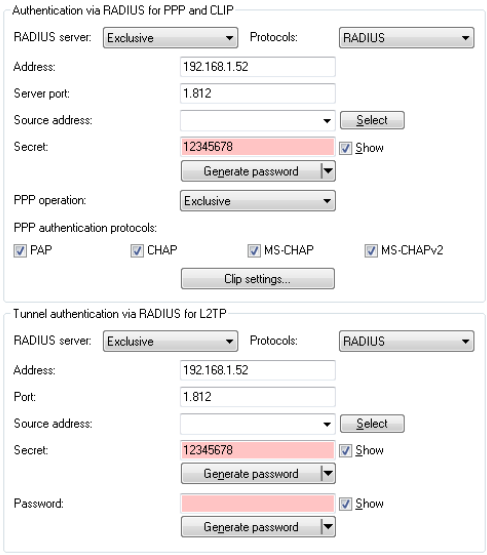
1. Under **Communication** > **Remote sites** in the table **L2TP endpoints**, create an entry "DEFAULT".



2. Then, under **Communication** > **Remote sites** in the table **L2TP list**, configure a "DEFAULT" entry.



3. Configure the RADIUS server under **Communication** > **RADIUS**.



Note: You only configure the lower section **Tunnel authentication via RADIUS for L2TP** if L2TP tunnel authentication should be done via the RADIUS server.

4. Configure the RADIUS server in order for it to be able to authenticate the L2TP tunnel and the PPP sessions.

If a LAC needs to authenticate itself at the L2TP tunnel with the station name "router1" and the password "abcde", you configure the appropriate entry in the RADIUS server (e.g. FreeRADIUS) as follows:

```
router1 Cleartext-Password := "password"
        Service-Type = Outbound-User,
        Tunnel-Type  = L2TP,
        Tunnel-Password = "abcde",
        Tunnel-Client-Auth-ID = "router1"
```

For the authentication of the PPP session of a user with the username "test" and the password "test", you configure the appropriate entry in the RADIUS server as follows:

```
test Cleartext-Password := "1234"
     Service-Type = Framed-User,
     Framed-Protocol = PPP
```

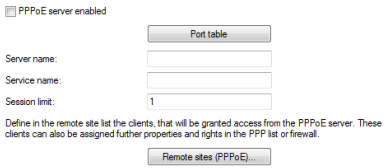
8.3 Support of the DH groups 15 and 16

As of version 9.00, for the encryption of VPN connections LANconfig offers you improved options for key exchange according to the Diffie-Hellmann algorithm. The DH groups 15 and 16 can be used for this on compatible devices. The relevant settings are located in the configuration menu under **VPN** > **General** > **Connection parameters** > **Add**and also under **VPN** > **Defaults**.

9 Routing and WAN connections

9.1 AC name configurable for PPPoE server

As of HiLCOS 8.90, you have the option of assigning an AC name to a PPPoE server (Access Concentrator Name).



Server name

This input field provides the option to give the PPPoE server a name that is independent of the device name (AC-Name = access concentrator name). If you leave this field blank, the PPPoE server uses the device name as the server name.

10 Other services

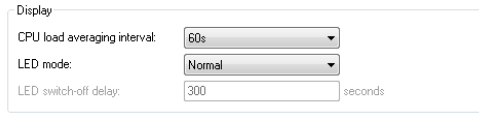
A single device offers a range of services for the PCs on the LAN. These are essential functions for use by the workstations. In particular these are:

- Automatic address management with DHCP
- Name administration of computers and networks by DNS
- Network traffic logging with SYSLOG
- Charging
- Time server

10.1 Deactivating device LEDs – boot-persistent

To operate an access point as unobtrusively as possible, you can disable the operating and status LEDs on the device. Even after restarting the device, the LEDs stay switched off. You can set up the device so that the LEDs light up briefly for a certain time after a restart, before the device disables them. This is useful for access points that are managed by WLAN controllers, for example to monitor the establishment of the connection to a WLAN controller.

You can set the operating mode of the LEDs in the **Display** section under **Management** > **Advanced**.



The selection list **LED mode** has three options to choose from:

Normal
The LEDs are always enabled, also after rebooting the device.

All off
The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

The **Timed off** option uses the setting in the field **LED switch-off delay** in seconds to control the time before the LEDs are disabled after a restart.

Notice: The "LED-Test" function is available despite the LEDs being disabled.

Note: If you change this value and save it within the previously set time, you should restart the timer.

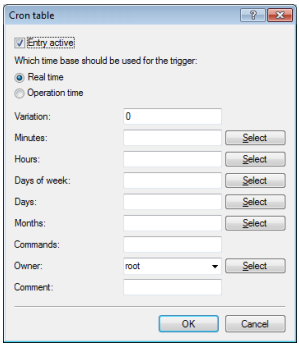
10.2 Comment box for CRON jobs

As of HiLCOS 9.00 you can add comments to CRON job entries.

10.2.1 Configuring the scheduler

The following tutorial shows you how to create a new CRON job and which parameters are available to you.

1. In LANconfig, open the configuration for your device.
2. Open the **Cron table** in the dialog **Date & Time** > **General** and click **Add...** to create a new CRON job.



3. Enter a time base.
   The time base determines whether HiLCOS performs the timing of future actions based on the real time or the uptime of the device. With the setting **Real time**, the system evaluates time and dates. With the setting **Operating time**, the system evaluates only the minutes and hours since the device was last started.
4. The value for **Variation** specifies the maximum delay in minutes for the start of the CRON job after the specified start time.
   The device determines the actual delay time at random. It lies between 0 and the time entered here. With the variation set to zero the CRON job will be executed at the specified time.

   Note: Rules based on real-time can only be executed if the device has a time from a valid source, e.g. via NTP.

5. Enter the minute(s), hour(s), day(s) of the week, day(s) of the month and the month(s) when your device should execute the specified command.
   If you do not enter a value, your device ignores the corresponding value. For each parameter you can optionally specify a comma-separated list of values or a range of values (in the form of `<Min.>-<Max.>`).

   The syntax of the field **Days of week** corresponds to the usual CRON interpretation:

Sunday	Monday	Tuesday	Wednes-day	Thursday	Friday	Sat-urday
0	1	2	3	4	5	6

   Note: The day-of-the-week field is also significant for rules relating to the operating time. This is useful for actions that you perform only once when you start the device (i.e., with zero days uptime). In this way you can match the day of the week to the days of operating time, for example.

6. Under **Commands** you enter the command or a comma-separated list of commands.
   Any command-line function can be executed.
7. Specify the **Owner** of the CRON job.

An owner is able to select an administrator defined in the device. If an owner is specified, then the CRON job commands will be executed with the rights of the owner.

8. A brief description of the CRON job can be entered in the **Comment** field.
9. Click **OK** to save the entry. You then write the configuration back to the device.

Other configuration examples:

Time base	At least	Hr.	W. days	M. days	Months	Command
Real time	0	4	0-6	1-31	1-12	do /so/man/disconnect internet
Real time	59	3	0-6	1-31	1-12	mailto:admin@example.com?subject=Forced-disconnect?body=Manual Internet disccon-nect
Real time	0	0		1		do /setup/accounting/delete
Real time	0	18	1,2,3,4,5			do /so/man/connect MAINOFFICE

- The first entry disconnects from the ISP every morning at 04:00h (forced disconnect).
- The second entry sends a brief e-mail to the admin each morning at 03:59h, just before the forced disconnect.
- The third entry deletes the accounting table on the 1st day of each month.
- The fourth entry establishes a connection to the main office each weekday at 18:00h.

Important: The device executes scheduled rules with an accuracy of one minute. Please ensure that the language you use to enter commands matches with that set for the console, otherwise scheduler commands will be ignored.

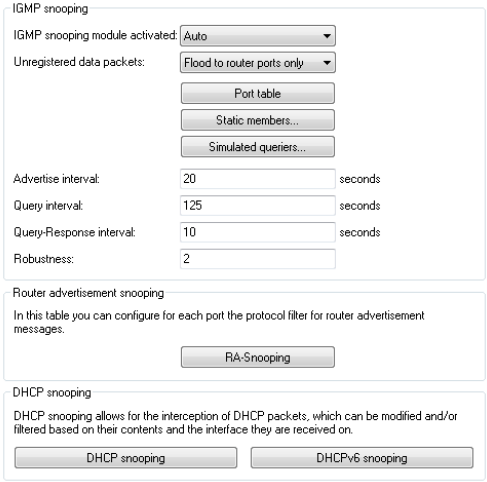
10.3 DHCP snooping and DHCP option 82

In its original form, DHCP has no safeguards to protect from attacks on the assignment of the network configuration. For example, if a client sends a 'DHCP discover' packet on the network in order to retrieve a valid network configuration from a DHCP server, an attacker can send the client fake 'DHCP offer' packets and trick it into using a false default gateway (DHCP spoofing).

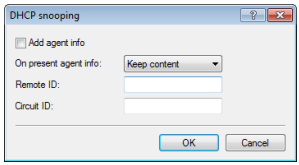
With DHCP snooping, the devices that receive and redirect DHCP packets are able to analyze and change these data packets, and to filter them by certain criteria. Additionally inserted information about the origin of the DHCP packets improves a DHCP server's capacity to manage extensive networks. Further, as this additional information is missing from the attacker's DHCP packets, they can no longer be used to interfere with the DHCP negotiations between DHCP servers, DHCP relay agents and the DHCP clients.

The access point supports DHCP snooping on layer 2. This enables it, for example, to add information (such as the SSID) to the DHCP packets received from the client on the WLAN before forwarding them to the LAN. The access point then adds the DHCP relay agent information option (option 82) according to RFC 3046.

In LANconfig you can set up DHCP snooping for each interface under **Interfaces** > **Snooping** and a click on **DHCP snooping**.



After selecting the appropriate interface, you can set the following:



Add agent info

Here you decide whether the DHCP relay agent appends incoming DHCP packets with the DHCP option "relay agent info" (option 82), or modifies an existing entry, before forwarding the request to a DHCP server.

The "relay agent info" is composed of values for the **Remote ID** and the **Circuit ID**.

On present agent info

Here you set how the DHCP relay agent handles the "relay agent info" in incoming DHCP packets. The following settings are possible:

- Keep content: In this setting, the DHCP relay agent forwards a DHCP packet and any existing "relay agent info" unchanged to the DHCP server.

- Replace content: In this setting, the DHCP relay agent replaces any existing "relay agent info" with the values specified in the fields **Remote ID** and **Circuit ID**.
- Drop packet: In this setting, the DHCP relay agent deletes any DHCP packet containing "relay agent info".

Remote ID

The remote ID is a sub-option of the "Relay agent info" option. It uniquely identifies the client making a DHCP request.

Circuit ID

The circuit ID is a sub-option of the "Relay agent info" option. It uniquely identifies the interface used by the client to make a DHCP request.

You can use the following variables for **Remote ID** and **Circuit ID**:

- %%: Inserts a percent sign.
- %c: Inserts the MAC address of the interface where the relay agent received the DHCP request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- %i: Inserts the name of the interface where the relay agent received the DHCP request.
- %n: Inserts the name of the DHCP relay agent as specified under **Setup** > **Name**.
- %v: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- %p: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, %p and %i are identical.
- %s: Inserts the WLAN SSID if the DHCP packet originates from a WLAN client. For other clients, this variable contains an empty string.
- %e: Inserts the serial number of the relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

10.4 Enabling LLDP with LANconfig

As of HiLCOS 8.90, LLDP can also be enabled via LANconfig.

In LANconfig, LLDP is enabled under **Interfaces** > **LAN**.

10.5 L2 Firewall

It is increasingly popular for service technicians to carry out maintenance and diagnosis activities using mobile devices. For example, a service technician uses a tablet to communicate with sensors in an Ethernet based machine network via WLAN access provided by the OpenBAT configured as an AP. Connecting an AP to the machine network provides the opportunity for potential attackers to carry out unauthorized activities in the machine network. Hirschmann supports you by means of the L2 Firewall to defend against such threats. The various applications in the machine network can be assigned to different logical WLAN networks offered by the OpenBAT. By using the L2 Firewall, access can be restricted by specifying individual firewall rules for any logical WLAN and LAN interfaces which are assigned to a bridge group. In the above example, the administrator can specify which sensors the service technician may access, and which firewall rules restrict this access.

10.5.1 L2-Firewall Functions

The L2 Firewall is located on layer 2 on the bridge between the logical interfaces and is also able to filter based on the protocols from layer 3 and layer 4. It is designed as a stateful firewall and supports the following protocols:

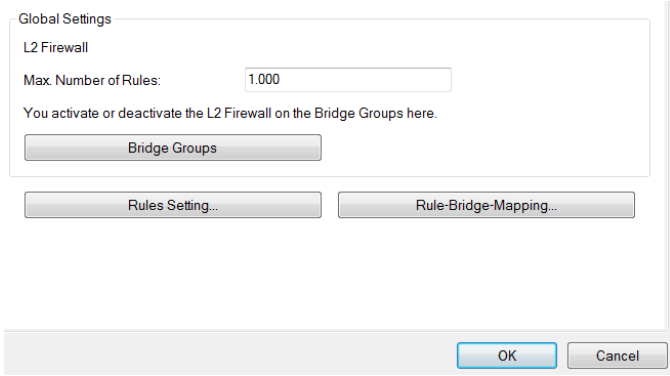
- IPv4
- ICMP
- TCP
- UDP

The L2 Firewall offers you the opportunity to specify rules. You can then map the rules to the bridges.

10.5.2 Tutorial Configuring the L2 firewall

To enable and configure the L2 Firewall proceed as follows:

1. Open the view **Firewall/QoS** > **L2 Firewall.**



2. Specify the **max. number of rules.**
3. Activate the L2 Firewall on the required **Bridge Groups**.
4. Specify the **rule setting**.
5. Specify the **rule bridge mapping**.
6. Click **OK**.

You have enabled and configured the L2 Firewall.

HIRSCHMANN
A BELDEN BRAND

Addendum
HiLCOS Rel. 9.10

Contents

1 Smart certificates.....11

1.1 Using smart certificates.....11

1.1.1 Creating templates for certificate profiles.....12

1.1.2 Creating a profile in LANconfig.....13

1.1.3 Certificate creation with WEBconfig.....18

1.1.4 Certificate management with WEBconfig.....20

1.1.5 Managing certificates in LANmonitor.....21

1.1.6 Creating certificates via URL-API.....22

1.1.7 Tutorials.....23

1.2 Additions to the Status menu.....33

1.2.1 SCEP-CA.....33

1.3 Additions to the Setup menu.....49

1.3.1 Web interface.....49

2 Configuration.....76

2.1 Encrypted storage of configurations with LANconfig.....76

2.1.1 Saving and loading device-configuration and script files.....77

2.1.2 Additions to the Status menu.....82

2.2 Each device has its own SSL key & changes to the default SSL settings.....84

2.2.1 Automatic generation of device-specific SSH/SSL keys.....84

2.2.2 Manually create custom SSH keys.....85

2.2.3 Additions to the Setup menu.....87

3 Diagnosis.....89

3.1 Advanced config version information under Status.....89

3.1.1 Additions to the Status menu.....89

3.2 SSH identifier in the event log.....90

3.2.1 Additions to the Status menu.....90

4 LCMS.....92

4.1 Proxy authentication via NTLM.....92

4.1.1 Proxy.....92

4.2 Special LANconfig icon for devices in a cluster or using Config Sync.....93

4.3 Special LANmonitor icon for devices in a cluster or using Config Sync.....94

4.4 Hirschmann "Wireless Quality Indicators" (WQI).....95

4.5 Extended number of characters for device names.....97

4.6 Different notations for MAC addresses.....97

4.6.1 Different notations for MAC addresses.....97

4.7 LANconfig: Text corrections relating to access rights.....97

5 IPv6.....99

5.1 Prefix-exclude option for DHCPv6 prefix delegation.....99

5.1.1 Prefix-exclude option for DHCPv6 prefix delegation.....99

6 Public Spot.....100

6.1 Restricting administrators to voucher output only.....100

6.1.1 Wizard for creating and managing users.....100

6.1.2 Setting up limited administrator rights for Public Spot managers.....101

6.2 Specify volume budget on vouchers....103
6.3 XML interface: Enhanced VLAN handling....103
6.3.1 Additions to the Setup menu....104
6.3.2 Messages to and from the authentication server....106
6.4 "Small header image": Optimized display for 19" devices....110
6.5 New button "Manage user wizard"....110
6.5.1 Additions to the Setup menu....110
6.6 Only show user accounts generated by the currently logged-on administrator....111
6.6.1 Additions to the Setup menu....112
6.7 Evaluation of DHCP option 82 in RADIUS and Public Spot....112
6.7.1 AP-specific login to a central Public Spot....112
6.7.2 Additions to the Setup menu....115
6.8 Additions to the Status menu....116
6.8.1 Max. no. users....116
6.8.2 PbSpot authenticated users....117
6.8.3 PMS authenticated users....117
6.8.4 Local configured users....117
6.9 Additions to the Setup menu....118
6.9.1 Password input set....118
6.9.2 Hide CSV export....118

7 WLAN....120

7.1 Upgrade to 16 SSIDs per WLAN module....120
7.2 Wildcards for MAC address and SSID filters....120
7.2.1 Access-control list....121
7.2.2 Additions to the Setup menu....124

7.3 Conformity with current ETSI radio standards in the 2.4GHz/5GHz bands....136
7.3.1 DFS configuration....136
7.3.2 Additions to the Setup menu....138
7.4 Time of the DFS rescan configurable via LANconfig....139
7.5 Bandwidth limit for each WLAN client per SSID....140
7.5.1 Additions to the Setup menu....140
7.6 Opportunistic key caching (OKC) adjustable on the client side....141
7.6.1 Additions to the Setup menu....142
7.7 Counter for WPA login attempts....142
7.7.1 Additions to the Status menu....143
7.8 Wireless IDS....145
7.8.1 Wireless IDS counter....145
7.8.2 Wireless IDS Types of Attack....147
7.8.3 Wireless IDS intruder identification....152
7.8.4 Tutorial: Configuring Wireless IDS....153
7.9 C2C coupling....155
7.9.1 Programming the C2C interface protocol....156
7.9.2 Troubleshooting....159
7.9.3 Tutorial: Configuring the C2C coupling function....162
7.10 WLAN link status log....164
7.10.1 Tutorial: Configuring the WLAN link status log....164
7.11 Tutorial: N:N mapping via the WLAN interface....166
7.12 Additions to the Setup menu....167
7.12.1 Channel change delay....167
7.13 Additions to the Status menu....168
7.13.1 Delete values....168

8 WLAN management.....169

8.1 AutoWDS operation.....169

8.1.1 Additions to the Status menu.....169

8.2 Wireless-IDS – detecting attacks on your wireless infrastructure.....171

8.2.1 Tutorial: Configuring Wireless-IDS with the WLAN controller.....171

8.3 Disable responses to CAPWAP requests from a WAN connection.....175

8.3.1 Protection against unauthorized CAPWAP access from the WAN.....175

8.3.2 Additions to the Setup menu.....176

8.4 Additional date information for central firmware management.....177

8.4.1 Firmware management table.....177

8.4.2 Additions to the Setup menu.....178

8.5 Display of channel and frequency of clients logged on to the AP.....178

8.5.1 Additions to the Status menu.....179

8.6 Using LANconfig to backup certificates.....180

8.6.1 Using LANconfig to backup and restore certificates.....180

8.7 Displaying the certificate status of an AP.....181

8.7.1 Additions to the Status menu.....181

8.8 On/off switch for AP LEDs per WLC.....182

8.8.1 Device LED profiles.....183

8.8.2 Additions to the Setup menu.....184

8.8.3 Additions to the Status menu.....186

8.9 Managing Wireless-ePaper and iBeacon profiles with WLCs.....191

8.9.1 ESL- and iBeacon profiles.....191

8.9.2 Additions to the Setup menu.....193

8.10 The modules iBeacon and Wireless ePaper have an additional "Managed" mode....199
8.10.1 Additions to the Setup menu....199
8.11 WLAN profiles divided into basic and advanced profiles....202
8.12 General LBS profile and device location profile....202
8.12.1 General LBS profile and device location profile....203
8.12.2 Additions to the Status menu....206
8.12.3 Additions to the Setup menu....207
8.13 Additions to the Status menu....207
8.13.1 Acquire statistical data....207
8.14 WLC Clustering Wizard....208

9 VPN....209

9.1 SCEP-CA function in VPN environments....209
9.2 SCEP algorithms updated....209
9.2.1 Configuring the CAs....209
9.2.2 Additions to the Setup menu....213
9.3 Loopback address for L2TP connections....220
9.3.1 Additions to the Setup menu....220
9.4 Download link for the public portion of the CA certificate....221
9.4.1 Download link for the public portion of the CA certificate....222
9.5 Configurable one-time password (OTP) for SCEP-CA....222
9.5.1 Configuring challenge passwords....222
9.5.2 Additions to the Setup menu....225
9.6 Deleting VPN error messages in the status table....226
9.6.1 Additions to the Setup menu....226
9.7 IPv4 addresses for VPN tunnels in the IP parameter list....227

9.7.1 Additions to the Setup menu....227

10 Routing and WAN connections....232

10.1 Client binding....232

10.1.1 Client binding....232

10.1.2 Load balancing with client binding....233

10.1.3 Enhancements in the menu system....235

10.2 Interface binding "Any" removed in IPv4....242

10.2.1 Defining networks and assigning interfaces....243

10.2.2 Additions to the Setup menu....243

10.3 Generic routing encapsulation (GRE)....244

10.3.1 Understanding the generic routing encapsulation (GRE) protocol....244

10.3.2 Additions to the Setup menu....247

10.3.3 Additions to the Status menu....252

10.4 Ethernet-over-GRE tunnel (EoGRE)....256

10.4.1 Ethernet-over-GRE (EoGRE)....256

10.4.2 Additions to the Status menu....259

10.4.3 Additions to the Setup menu....260

10.5 Loopback addresses for RIP....265

10.5.1 Additions to the Setup menu....266

10.6 PPPoE snooping new....266

10.6.1 PPPoE snooping....266

10.6.2 Additions to the Setup menu....267

10.7 Default settings in the access table for WAN connections....272

10.7.1 Additions to the Setup menu....272

11 Other services....282

11.1 Prefer perfect forward secrecy (PFS) for connections....282
11.1.1 Additions to the Setup menu....282
11.2 Additions to the Setup menu....285
11.2.1 E-mail....285
11.3 TACACS+ extension for the passwd command....286
11.4 Input field for DHCP options extended to 251 characters....286
11.4.1 Additions to the Setup menu....286
12 Other parameters....288
12.1 Profile....288
12.2 Renegotiations....288
12.3 TLS connections....289
12.3.1 Port....289
12.4 Renegotiations....290
12.5 LBS-Tracking....291
12.6 LBS-Tracking-List....291
12.7 OKC....292
12.8 Network name....293
12.9 Manage user wizard....293
12.9.1 Show status information....294
12.10 Renegotiations....294
12.11 LBS-Tracking-List....295
12.12 Max. number of concurrent updates....296
12.13 CAPWAP-Port....296
12.14 RS count....297
12.15 RS count....297
12.16 Flash restore....298

12.17 Additions to the Status menu.....298
12.17.1 DSLAM chipset manufacturer dump.....298
12.17.2 DSLAM manufacturer dump.....299
12.17.3 DSLAM chipset manufacturer dump.....299
12.17.4 DSLAM manufacturer dump.....299

1 Smart certificates

As of HiLCOS version 9.10 you have the option to use a Hirschmann router to create and issue digital certificates.

Furthermore, LANmonitor as of HiLCOS version 9.10 displays an overview of active and revoked certificates.

Description: [1]LANconfig, [2]Setup menu	*Hex notation in the console*	*Rights description*
1. CA-Web-Interface Wizard **2.** CA-Web-Interface	0x1000000	Creates profiles for the CA web interface

Table 1: Overview of function rights

1.1 Using smart certificates

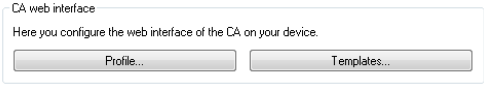
The configuration of the SCEP client for the generation and distribution of certificates can quickly become a complex and laborious task in extensive network infrastructures. This work required for this task can be reduced with the help of predefined, selectable profiles and access via a web interface.

A Hirschmann router enables you to create and issue highly secure certificates. It is easy to manage the certificates via the WEBconfig interface of the corres-ponding device. An external CA is no longer required, which is particularly advantageous for small-scale infrastructures.

Using the Certificate Wizard from Hirschmann, even users without certificate know-how can create certificates in just a few steps.

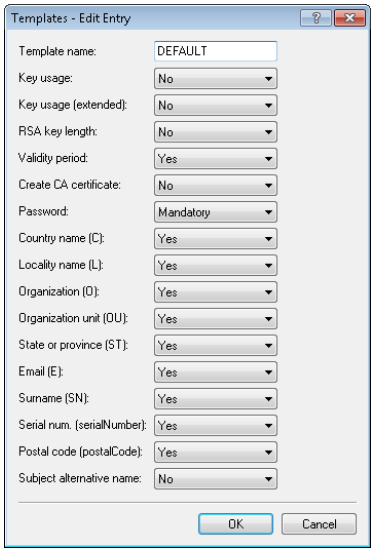
The devices administrator creates the profile as a collection of certificate properties. It contains the configuration of the certificate and also a unique certificate ID. From this point on, all you need to do to create and distribute a certificate is to select one of the profiles.

Profiles can also be managed in LANconfig under **Certificates** > **Certificate handling** in the section **CA web interface**.



1.1.1 Creating templates for certificate profiles

In LANconfig, profiles are created under **Certificates** > **Certificate handling** > **Templates**.



Note: A “DEFAULT” a template is already available.

The administrators specifies which of the profile properties are mandatory and which are to be edited by the user. The following options are available:

- No: The field is invisible, the value entered is considered to be a default value.
- Fixed: The field is visible, but cannot be changed by the user.
- Yes: The field is visible and can be changed by the user.
- Mandatory: The field is visible, the user must enter a value.

These permissions apply to the following profile and ID fields:

Profile fields

- Key usage
- Key usage (extended)
- RSA key length
- Validity period
- Create CA certificate
- Password

Identifier

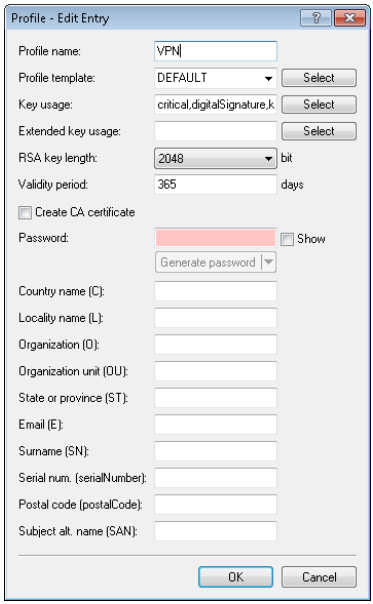
- Country code (C)
- Locality name (L)
- Organization (O)
- Organization unit (OU)
- State or province (ST)
- E-mail (E)
- Surname (SN)
- Serial no. (serialNumber)
- Postal code (postalCode)
- Subject alt. name

Tip: If the Templates table is empty, the user can only see the input fields for the profile name, the common name (CN), and the password. The other profile fields retain the default values as set by the device administrator.

1.1.2 Creating a profile in LANconfig

Note: The user needs the appropriate access rights to create, select, modify and assign profiles.

In LANconfig, profiles are created under **Certificates** > **Certificate handling** > **Profile**.



Note: By default three profiles are already available for common application scenarios.

Profile name

The unique name of the profile.

Profile template

Select a suitable profile template here, if applicable.

The profile template specifies which certificate information is mandatory and which can be changed. Templates are created under **Certificates** > **Certificate handling** > **Templates**.

Key usage

Specifies for which application the profile is to be used. The following usages are available using the **Select** button:

Value	*Meaning*
critical	This restriction requires the extended key usage to be considered. If the extension is not supported, the certificate is rejected as invalid.

Value	*Meaning*
digitalSignature	Is this option is used, the public key is used for digital signatures.
nonRepudiation	With this option set, the key is used for digital signatures of a non-repudiation service, i.e. one with a rather long-term character such as notary public service.
keyEncipherment	If this option is set, the key is used for encrypting other keys or security information. It is possible to restrict the use of **encipher only** and **decipher only**.
dataEncipherment	If this option is set, the key is used for encrypting user data (but not other keys).
keyAgreement	If this option is used, the "Diffie-Hellman" algorithm is used for key agreement.
keyCertSign	If this option is set, the key is applied to certificates for signature verification. This is useful for CA certificates, for example.
cRLSign	If this option is set, the key is applied to CRLs for signature verification. This is useful for CA certificates, for example.
encipherOnly	This is only useful with the Diffie-Hellman keyAgreement.
decipherOnly	This is only useful with the Diffie-Hellman keyAgreement.

Table 2: The available key usages

Note: Multiple comma-separated entries can be selected.

Ext. key usage

Specifies the extended application for which the profile is to be used. The following usages are available using the **Select** button:

Value	*Meaning*
critical	
serverAuth	SSL/TLS Web server authentication
clientAuth	SSL/TLS Web client authentication
codeSigning	Signing of program code
emailProtection	E-mail protection (S/MIME)
timeStamping	Furnishing data with reliable time stamps
msCodeInd	Microsoft Individual Code Signing (authenticode)
msCodeCom	Microsoft Commercial Code Signing (authenticode)
msCTLSign	Microsoft Trust List Signing
msSGC	Microsoft Server Gated Crypto
msEFS	Microsoft Encrypted File System

Value	*Meaning*
nsSGC	Netscape Server Gated Crypto

Table 3: Extended usages

Note: Multiple comma-separated entries can be selected.

RSA key length

Sets the length of the key.

Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

Create CA certificate

Indicates whether this is a CA certificate.

Password

Password to protect the PKCS12 certificate file.

The following input creates a certificate ID. The following options are available:

Country code (C)

Enter the country identifier (e.g. “DE” for Germany).

This entry appears in the subject or issuer of the certificate under C= (**C**ountry).

Locality name (L)

Enter the name of the locality.

This entry appears in the subject or issuer of the certificate under L= (**L**ocality).

Organization (O)

Specify the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under O= (**O**rganization).

Organization unit (OU)

Specify the unit within the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under `OU=` (**O**rganization **U**nit).

State or province (ST)

Enter the State or province.

This entry appears in the subject or issuer of the certificate under `ST=` (**ST**ate).

E-mail (E)

Enter an e-mail address:

This entry appears in the subject or issuer of the certificate under `emailAddress=`.

Surname (SN)

Enter a surname.

This entry appears in the subject or issuer of the certificate under `SN=` (**S**ur**N**ame).

Serial no. (serialNumber)

Enter a serial number.

This entry appears in the certificate under `serialNumber=`.

Postal code (postalCode)

Enter the location post code.

This entry appears in the subject or issuer of the certificate under `postalCode=`.

Subject alt. name (SAN)

The “Subject Alternative Name” (SAN) links additional data with this certificate. The following data are allowed:

- E-mail addresses
- IPv4 or IPv6 addresses
- URIs
- DNS names
- Directory names

- Any names

  This entry appears in the subject or issuer of the certificate under `subjectAltName=` (e.g. `subjectAltName=IP:192.168.7.1`).

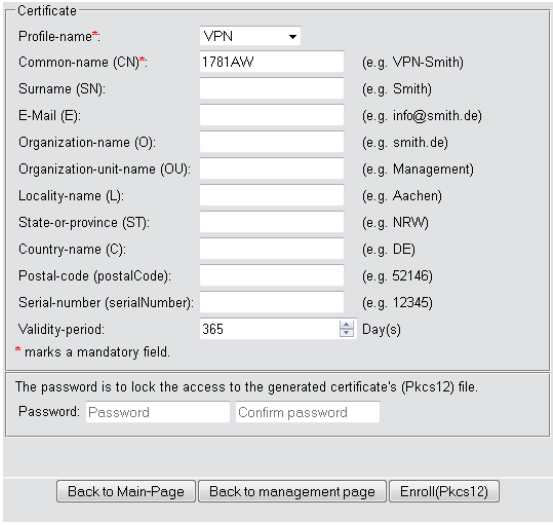
Note: The certificate issuer assigns the general name "CN". The "CN" is required as a minimum.

1.1.3 Certificate creation with WEBconfig

Note: You need the appropriate access rights to select, modify and assign profiles.

To create your certificates, navigate to the WEBconfig of the OpenBAT device.

1. To create a certificate using the web interface, navigate to the view **Setup Wizards** > **Manage certificates** and select **Create new certificate**.



2. From the **Profile name** drop-down menu, select the profile to be used as the basis for the certificate.

   Tip: Empty templates only contain fields with the selection “No”. If the user selects a profile based on an empty template, the input mask displays

only the common name. The other profile fields retain the default values as set by the device administrator.

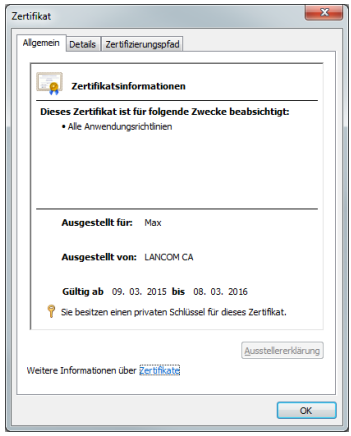
3. Fill out the **common name (CN)** field. Set a validity period for the certificate and give it a secure password (PIN). The other fields such as **Email** and **Organization name** are optional information. However, under certain circumstance this information can help to find the certificate recipient if there are problems with the certificate.

   Note: The following characters are allowed in the password: [A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

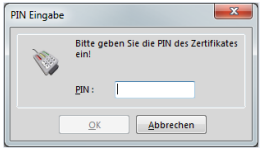
4. To complete of the changes, click the **Enroll (PKCS12)** button. In the following dialog box, you can set the name and location of the file.

   Note: The newly created certificates appear in the certificate status table under **Status** > **Certificates** > **SCEP-CA** > **Certificates**.

5. Issue the newly enrolled certificate to the recipient together with the access password set in step 3.



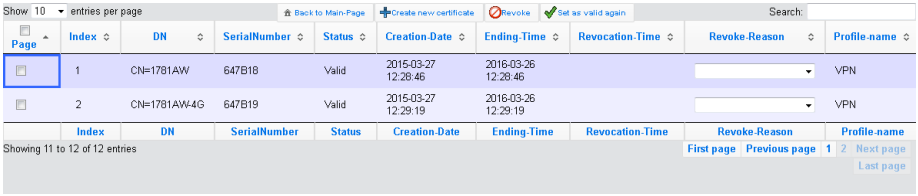
6. The recipient is now able to use a secure VPN dial-in. For the dial-in to succeed, the user must enter the password (PIN) set in step 3.



1.1.4 Certificate management with WEBconfig

Note: You need the appropriate permissions to be able to manage the certificates.

To manage a certificate via the web interface, navigate to the view **Setup Wizards** > **Manage certificates**. This gives you an overview of the enrolled certificates, which you can revoke if necessary.



The column headers have the following meanings:

Page

This column is used to mark the entry.

Index

Displays the sequential index of the entry.

Name

Displays the name the certificate.

Serial number

Contains the serial number of the certificate.

Status

Displays the current status of the certificate. Possible values are:

- V: Valid
- R: Revoked
- P: Pending

Creation date

Displays the date of the certificate's creation (date, time).

Ending time

Indicates the date and time of (regular) certificate expiry.

Revocation time

Indicates the date and time of (premature) certificate revocation.

Revoke reason

Indicates the cause of the premature revocation. The selection is made via a drop-down selection list.

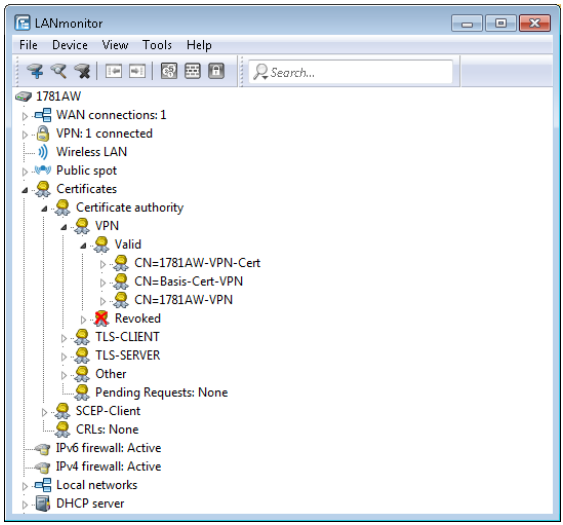
To revoke a certificate, select it in the **Page** column, in the **Revoke reason** column you select why you are revoking the certificate, and then click the **Revoke** button.

The column entries for **Status**, **Revocation time** and **Revoke reason** change accordingly.

To reverse a revocation, highlight the certificate again in the first column and click **Set as valid again**.

1.1.5 Managing certificates in LANmonitor

LANmonitor displays the active and revoked certificates, as well as the certificate requests from the SCEP clients.



To revoke a certificate, right-click on the corresponding certificate and select **Revoke certificate** from the context menu.

An overview of all revoked certificates is located in the **Revoked** section.

Certificate requests from SCEP clients can be seen in the **Pending requests** section. Right-click on the corresponding request and select either **Reject** or **Accept** in the context menu.

1.1.6 Creating certificates via URL-API

A special API can greatly simplify the creation of certificates for a complex and extensive network infrastructure.

For example, you can use a script to automate the process by sending a call to a URL with parameters attached. The following parameters are possible:

- a: Specifies the profile name.
- b: Specifies the common name.
- c: Specifies the surname.
- d: Specifies the email.
- e: Specifies the organization.
- f: Specifies the organization unit.
- g: Specifies the locality.

- h: Specifies the State or province.
- i: Specifies the country.
- j: Specifies the postal code.
- k: Specifies the serial number.
- l: Specifies the subject alternative name.
- m: Specifies the key usage.
- n: Specifies the extended key usage.
- o: Specifies the key length
- p: Specifies the validity period in days.
- q: Specifies the password for the PKCS12 file.
- r: Indicates whether this is a CA certificate.
  - 1: CA certificate
  - 0: No CA certificate

Important: The Wizard only processes the parameters set with the appropriate permissions in the presets table.

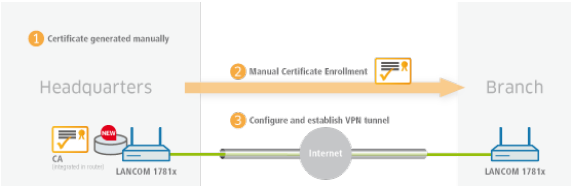
The call to the URL with the appropriate parameters looks like this:

```
192.168.10.74/scepwiz/a=VPN&b=iPhone&q=company
```

1.1.7 Tutorials

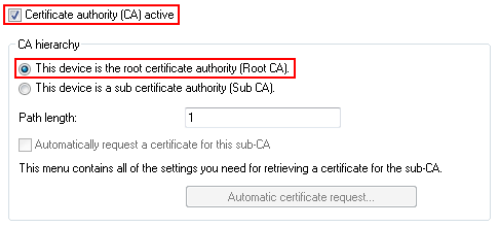
Setting up a CA and creating and using certificates for a VPN connection

This tutorial describes how you enable a CA (certificate authority) on a Hirschmann router and how the CA helps you to create and use new certificates for a VPN connection between two Hirschmann routers (manual certificate distribu-tion).

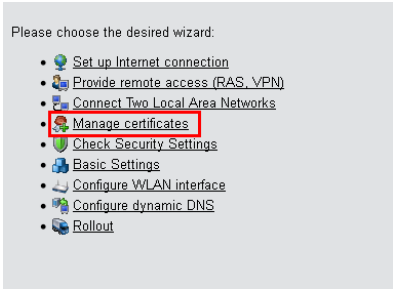


Important: All devices need to be set with a valid date and time.

1. You enable the certificate authority in LANconfig and you set the device as the root CA. You will find these settings under **Certificates** > **Cert. authority (CA)**.

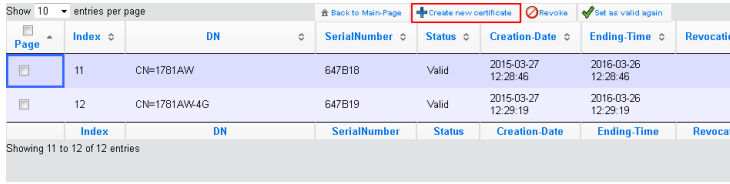


2. You are now able to create CA certificates for the VPN endpoints that will later provide the connection.
   a) The Setup Wizard **Manage certificates** helps you to create certificates easily and conveniently.



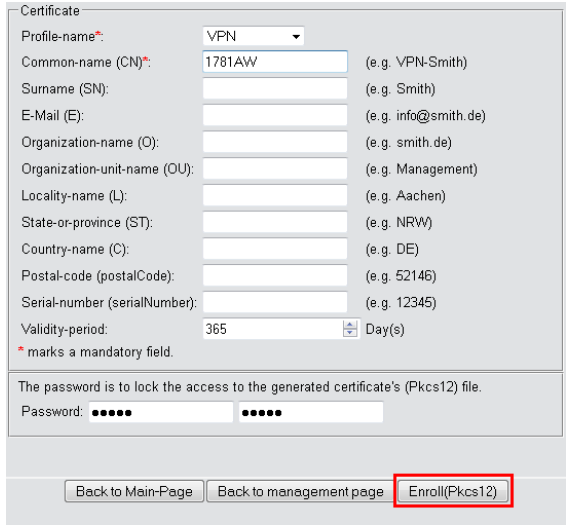
   b) The first page of the Wizard is an overview of all certificates previously issued by the CA.

      Note: The certificate of the CA itself is not displayed here.



With the **Create new certificate** button you start the process that generates a new certificate.

c) Under the entry to **Enroll certificates**, you have the option to configure the profile, the official name of the certificate (common name or CN), and other information that is useful for identifying the certificate. Set the validity period of the certificate and the password for the Pkcs12 file that contains the new certificate, the corresponding private key, and the certificate of the CA.



Once you have entered all the necessary information, you create the certificate by clicking the button **Enroll (Pkcs12)**. The dialog for saving the Pkcs12 file appears automatically once the certificate has been created on the device. This process can take several seconds.

d) In the **Save the Pkcs12 file** window, choose the location and name of the Pkcs12 file. By default, the file is named according to the following format:

`pkcs12<YYYY_MM_DD-hh_mm_ss>.p12`

YYYY: Year

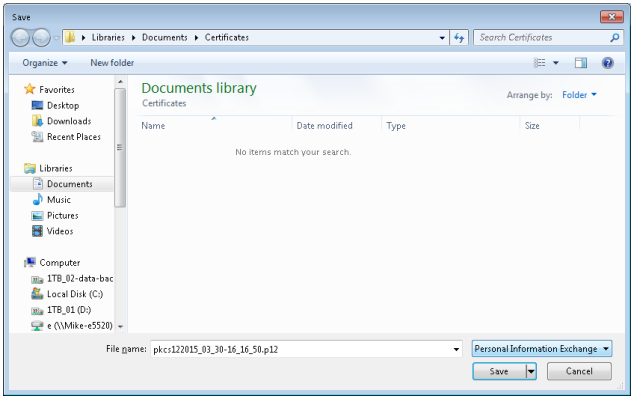
MM: Month

DD: Day

hh: Hour

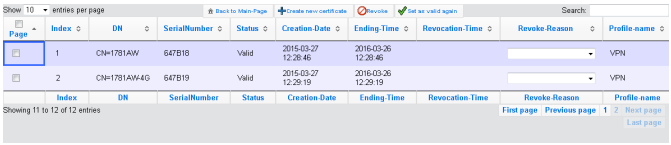
mm: Minute

ss: Second



Note: As shown by the example, the file can have any name.

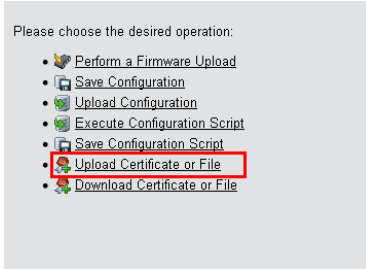
e) Use the same method to create further certificates.



Note: Overview page with two created certificates.

3. In order to use the certificates for a VPN connection, you need to upload them to the devices.

a) Uploading to the corresponding VPN endpoints is easy to do with WEBconfig under **File management** > **Upload certificate or file**.



b) **Upload certificate or file**

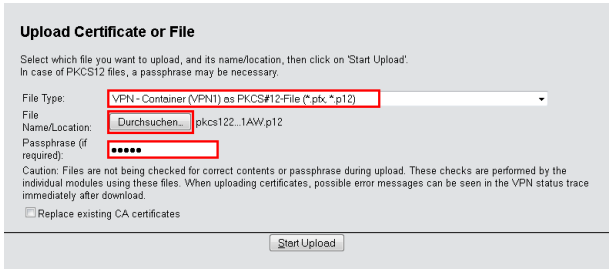
First, select the file type and where to save it. For VPN connections, please choose an unused VPN container.

Note: As long as no certificates were set up for VPN, all of the VPN containers are unused.

In the next step you select the Pkcs12 file that contains the certificate that you want to use for this VPN endpoint.

Enter the password that you have set for the file in step 2.c.

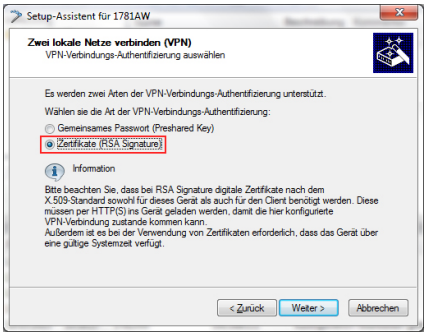
Finally, start the upload.



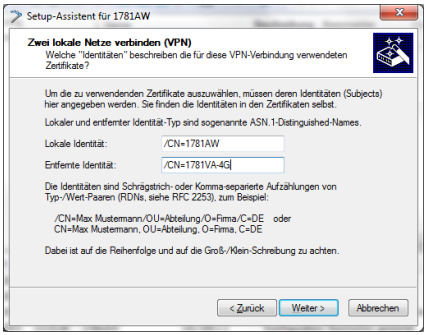
Important: This process is required for all VPN endpoints. Please bear in mind that each VPN endpoint needs a certificate of its own.

4. Establish a VPN connection between two VPN endpoints. This is carried out via the Setup Wizard **Connect two local area networks (VPN)**.

a) In the Setup Wizard, set the VPN connection authentication to **Certificates (RSA signature)**.



b) In the **Local and remote identity** window, specify the "ASN.1-Distinguished-Name". This is the official name of the certificate plus any additional information that you entered in step 2.c. You can see this additional information in the overview of certificates (step 2.e) in the "Name" column. For the **Local identity**, enter the information for the certificate on the local machine. The item **Remote identity** contains the certificate information of the other VPN endpoint.



c) Continue to run the Wizard. You repeat this process for the other VPN endpoint of this VPN connection.

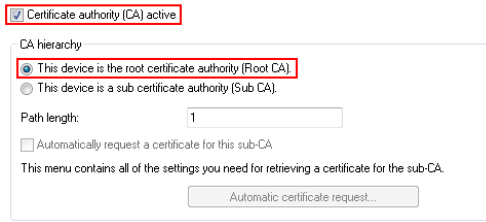
Setting up a CA and creating and using certificates for a VPN connection with certificate rollout via SCEP

This tutorial describes how you enable a CA (certificate authority) on a Hirschmann router and how the CA helps you to create and use new certificates for a VPN connection between two Hirschmann routers (certificate distribution via SCEP).

Note: We only explain the menu items that are important for the successful conclusion of the tutorial.

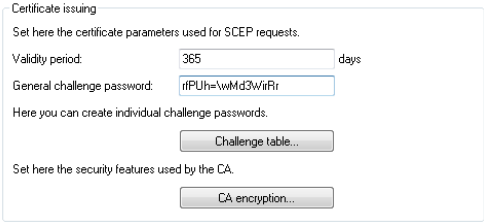
Important: All devices must be set with the correct date and time and the certificate authority must be accessible via "HTTPS".

1. You enable the certificate authority in WEBconfig or LANconfig and you set the device as the root CA. You will find these settings under **Certificates** > **Cert. authority (CA)**.



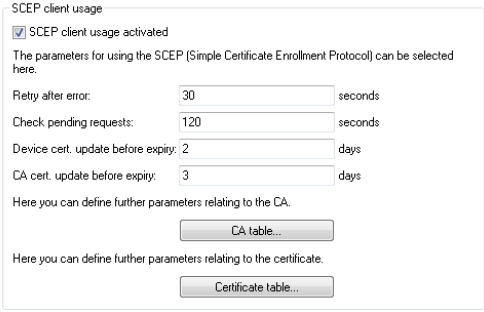
2. SCEP clients can automatically obtain certificates by SCEP (simple certificate enrollment protocol). A necessary step for this is for you to set a general challenge password in the root CA. Set a password at **Certificates** > **Certificate handling**.

Note: If you write the configuration back to the device after enabling the CA, the CA automatically generates a general challenge password.

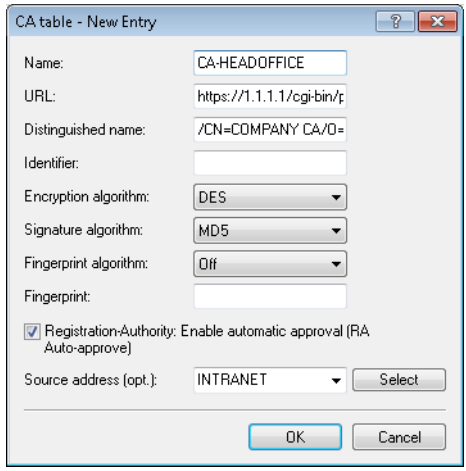


You are now able to create CA certificates for the VPN endpoints that will later provide the connection.

3. In order for the VPN endpoints to obtain their certificates via SCEP, the SCEP client must be configured on each of them. This setting is located under **Certificates** > **SCEP client**.



a) Specify the further information about the certificate authority under **Certificates** > **SCEP client** > **CA table**. This table contains information about the CA from which a certificate is to be obtained.



Name

The name can be freely selected and used to identify this device.

URL

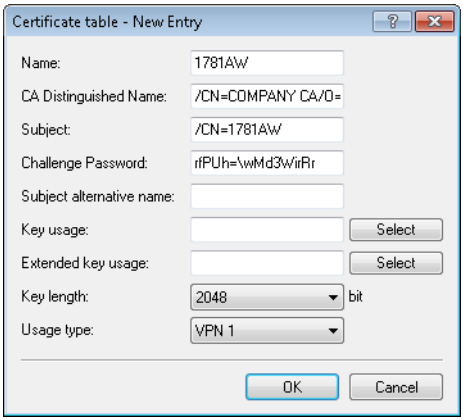
The URL is always constructed in the same way: `https://<IP address>/cgi-bin/pkiclient.exe`. Replace `<IP address>` with the IPv4 address where the CA is accessible from the WAN.

Important: If the VPN endpoint is also the CA, you need to enter the loopback address here.

Distinguished name

The distinguished name of the CA (see screenshot in step 1).

b) The additional information about the certificate that the CA is to issue to this device is specified under **Certificates** > **SCEP client** > **Certificate table**.



Name

The name can be freely selected and used to identify this device.

CA Distinguished Name

The CA distinguished name (see screenshot in step 1).

Subject

The desired distinguished name of the certificate. In this example, only the common name is used.

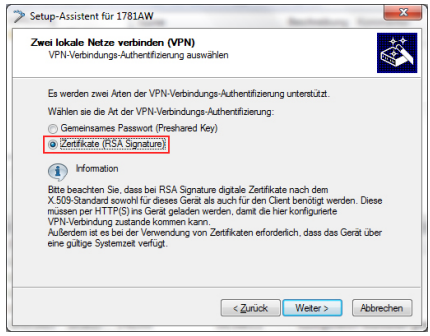
Challenge password

The general challenge password set on the certificate authority (see step 2).

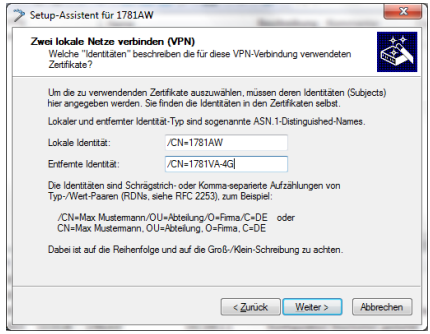
Usage type

The location where this certificate is to be stored. In this example "VPN 1".

4. Once you have set up a SCEP client on each of the VPN endpoints, you can establish a VPN connection between two VPN endpoints. This is carried out via the Setup Wizard **Connect two local area networks (VPN)**.
   a) In the Setup Wizard, set the VPN connection authentication to **Certificates (RSA signature)**.



b) In the **Local and remote identity** window, specify the "ASN.1-Distinguished-Name". This is the official name of the certificate plus any additional information that you entered under "Subject" in step 3.b. For the **Local identity**, enter the information for the certificate on the local machine. The item **Remote identity** contains the certificate information of the other VPN endpoint.



c) Continue to run the Wizard. You repeat this process for the other VPN endpoint of this VPN connection.

1.2 Additions to the Status menu

1.2.1 SCEP-CA

Displays an overview of SCEP CA certificates and requests and allows you to manage these certificates.

SNMP ID:

1.61.2

Telnet path:

Status > **Certificates**

Certificates

Displays current SCEP CA certificates and allows you to manage them.

SNMP ID:

1.61.2.1

Telnet path:

Status > **Certificates** > **SCEP-CA**

Certificate status table

This table displays the status of current SCEP CA certificates.

SNMP ID:

1.61.2.1.1

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates**

Index

Displays the sequential index of the entry.

SNMP ID:

1.61.2.1.1.1

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Serial number

Displays the serial number of the certificate.

This entry appears in the certificate under `serialNumber=`.

SNMP ID:

1.61.2.1.1.2

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Status

Displays the status of the certificate. Possible values are:

- V: Valid
- R: Revoked
- P: Pending

SNMP ID:

1.61.2.1.1.3

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Creation date

Displays the creation date of the certificate.

SNMP ID:

1.61.2.1.1.4

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Ending time

Displays the expiry time of the certificate.

This entry appears in the certificate under `Validity`.

SNMP ID:

1.61.2.1.1.5

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Revocation time

Displays the certificate revocation time if the certificate has been revoked.

SNMP ID:

1.61.2.1.1.6

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Revoke reason

Displays the reason for certificate revocation if the certificate has been revoked.

SNMP ID:

1.61.2.1.1.7

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Possible values:

unspecified
No reason given.

keyCompromise
The private key is compromised.

cACompromise
The private CA key is compromised.

affiliationChanged
Details of the holder or the issuer of the certificate have changed.

superseded
The certificate is outdated and has been replaced by a new certificate.

cessationOfOperation
The certificate is no longer required for the original purpose.

certificateHold
The certificate is on hold until it is finally revoked or released again.

privilegeWithdrawn
The certificate contains a right that is not longer valid.

aACompromise
The private AA key is compromised.

MAC address

Displays the MAC address of the device for which the certificate was issued.

SNMP ID:
1.61.2.1.1.8

Telnet path:
Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Name

Displays the CN of the certificate.

SNMP ID:
1.61.2.1.1.9

Telnet path:
Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Profile name

Displays the name of the profile that the certificate is based on.

SNMP ID:

1.61.2.1.1.10

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates** > **Certificate status table**

Revoke certificate

This action revokes a certificate. This is necessary if the certificate has been compromised or if there have been changes (rights, information about the issuer) to the certificate.

This action requires the specification of up to three parameters in the form `<Index>,<Reason>[,<Date>]`:

`Index`

The index of the corresponding certificate in the certificate table (required).

`Reason`

The reason of the revocation (required). The following values are possible:

- 0: Unspecified
- 1: Key compromise
- 2: CA compromise
- 3: Affiliation changed
- 4: Superseded
- 5: Cessation of operation
- 6: Certificate hold
- 8: Remove from CRL
- 9: Privilege withdrawn

- 10: Attribute authority compromise

`Date`

This specification describes the time in UTC format (`YYMMDDHHSSZ`) when the certificate is compromised (optional if you specify the reasons 1, 2 and 10).

Important: Specify the parameters each separated by a comma and without spaces.

Note: Entering ? generates a help text.

SNMP ID:

1.61.2.1.2

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates**

Set certificate on hold

This action sets a certificate on “Hold”. This option is available if you want to clarify the status of the certificate before fully revoking it.

This action requires a parameter to be specified in the form `<Index>`:

`Index`

The index of the corresponding certificate in the certificate table (required).

Note: Entering ? generates a help text.

SNMP ID:

1.61.2.1.3

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates**

Declare certificate as valid again

With this action you declare a certificate that was previously on “Hold” to be valid again.

This action requires an index list to be specified in the form `<Index1>,<Index2>,<Index3>`:

`Indexn`

The indexes of the corresponding certificates in the certificate table (required).

Important: Specify the indexes each separated by a comma and without spaces.

Note: Entering ? generates a help text.

SNMP ID:

1.61.2.1.4

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Certificates**

Requests

Displays current requests for SCEP CA certificates and allows you to manage them.

SNMP ID:

1.61.2.2

Telnet path:

Status > **Certificates** > **SCEP-CA**

Pending-Requests

This table displays the status of pending requests for SCEP CA certificates.

SNMP ID:

1.61.2.2.1

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests**

Index

Displays the sequential index of the entry.

SNMP ID:

1.61.2.2.1.1

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

Transaction ID

Displays the transaction ID of the entry.

SNMP ID:

1.61.2.2.1.2

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

MAC address

Displays the MAC address of the requesting device.

SNMP ID:

1.61.2.2.1.3

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

Name

Displays the name of the requesting device.

SNMP ID:

1.61.2.2.1.4

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

IP address

Displays the IP address of the requesting device.

SNMP ID:

1.61.2.2.1.5

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

PKI-Status

Displays the status of the public-key infrastructure of the requesting device.

SNMP ID:

1.61.2.2.1.6

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

Reason

Displays the reason for the request.

SNMP ID:

1.61.2.2.1.7

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

DN

Displays the fingerprint for the request.

SNMP ID:

1.61.2.2.1.8

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

Receive date

Displays the time of the request.

SNMP ID:

1.61.2.2.1.9

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests** > **Pending-requests**

Issue certificate

With the syntax `do Issue-Certificate [index-list]` you issue a SCEP-CA certificate for a device. `[index-list]` is a comma-separated list of the indexes from the table "Pending requests". Each request index entered here receives a certificate.

SNMP ID:

1.61.2.2.2

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests**

Grant all certificates

With the syntax `do Issue-Certificate` you issue a SCEP-CA certificate for all devices. You do not have to specify any additional parameters. All pending requests will receive a certificate.

SNMP ID:

1.61.2.2.3

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests**

Decline request

With the syntax `do Decline-Request [index-list]`, you reject the request from a device. `[index-list]` is a comma-separated list of the indexes from the table "Pending requests". Any request with the index you specified will be declined. The requesting device does not receive a certificate.

SNMP ID:

1.61.2.2.4

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests**

Deny all requests

With the syntax `do Deny-all-requests [index-list]`, you reject the requests from all devices. You do not have to specify any additional parameters. All pending requests will be rejected.

SNMP ID:

1.61.2.2.5

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests**

Delete-pending-request

You delete a pending request with the syntax `do Delete-Pending-Request [index-list]`. `[index-list]` is a comma-separated list of the indexes from the table "Pending requests". Any request with the index you specified will be deleted.

SNMP ID:

1.61.2.2.6

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests**

Delete-all-pending-requests

With the syntax `do Delete-all-pending-requests` you delete all pending requests. You do not have to specify any additional parameters. All pending requests will be deleted.

SNMP ID:

1.61.2.2.7

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Requests**

CA-Status

Displays the current status of SCEP-CA certificates and allows you to manage them.

SNMP ID:

1.61.2.3

Telnet path:

Status > **Certificates** > **SCEP-CA**

Log table

This table displays current events relating to the CA status.

SNMP ID:

1.61.2.3.7

Telnet path:

Status > **Certificates** > **SCEP-CA** > **CA-Status**

Web interface

This directory gives you an overview of the settings for the SCEP-CA web interface.

SNMP ID:

1.61.2.4

Telnet path:

Status > **Certificates** > **SCEP-CA**

Profiles

The configured profiles are shown in this table. To view the certificate properties, click on a profile name.

SNMP ID:

1.61.2.4.1

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Web-Interface**

Template

The templates for the certificate profiles are shown in this table. To view the custom settings, click the name of a template.

SNMP ID:

1.61.2.4.2

Telnet path:

Status > **Certificates** > **SCEP-CA** > **Web-Interface**

1.3 Additions to the Setup menu

1.3.1 Web interface

In this directory, you configure the settings for the SCEP-CA web interface.

SNMP ID:

2.39.2.14

Telnet path:

Setup > **Certificates** > **SCEP-CA**

Profiles

In this table you create profiles with collected certificate properties.

Note: By default three profiles are already available for common application scenarios.

SNMP ID:

2.39.2.14.1

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface**

Profile name

Here you assign a unique name for the profile.

SNMP ID:

2.39.2.14.1.1

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:
empty

Key usage

Specifies for which application the profile is to be used. The following usages are available:

- critical
- digitalSignature
- nonRepudiation
- keyEncipherment
- dataEncipherment
- keyAgreement
- keyCertSign
- cRLSign
- encipherOnly
- decipherOnly

Multiple comma-separated entries can be selected.

SNMP ID:
2.39.2.14.1.2

Telnet path:
Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:
Max. 251 characters from
`[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:
critical,digitalSignature,keyEncipherment

Extended key usage

Specifies the extended application for which the profile is to be used. The following usages are available:

- critical
- serverAuth: SSL/TLS Web server authentication
- clientAuth: SSL/TLS Web client authentication
- codeSigning: Signing of program code
- emailProtection: E-mail protection (S/MIME)
- timeStamping: Furnishing data with reliable time stamps
- msCodeInd: Microsoft Individual Code Signing (authenticode)
- msCodeCom: Microsoft Commercial Code Signing (authenticode)
- msCTLSign: Microsoft Trust List Signing
- msSGC: Microsoft Server Gated Crypto
- msEFS: Microsoft Encrypted File System
- nsSGC: Netscape Server Gated Crypto

Multiple comma-separated entries can be selected.

SNMP ID:

2.39.2.14.1.3

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 251 characters from
`[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

RSA key length

Sets the length of the key.

SNMP ID:

2.39.2.14.1.4

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

1024
2048
3072
4096
8192

Default:

2048

Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

SNMP ID:

2.39.2.14.1.5

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 10 characters from `0123456789`

Default:

365

CA

Indicates whether this is a CA certificate.

SNMP ID:

2.39.2.14.1.6

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Yes
No

Default:

No

Password

Password to protect the PKCS12 certificate file.

SNMP ID:

2.39.2.14.1.7

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:
empty

Country

Enter the country identifier (e.g. “DE” for Germany).

This entry appears in the subject or issuer of the certificate under `C=` (**C**ountry).

SNMP ID:
2.39.2.14.1.8

Telnet path:
Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:
2 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:
empty

Locality name

Enter the name of the locality.

This entry appears in the subject or issuer of the certificate under `L=` (**L**ocality).

SNMP ID:
2.39.2.14.1.9

Telnet path:
Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Organization

Enter the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under 0= (**O**rganization).

SNMP ID:

2.39.2.14.1.10

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Organization unit name

Enter the organization that issues the certificate.

This entry appears in the subject or issuer of the certificate under 0U= (**O**rganization **U**nit).

SNMP ID:

2.39.2.14.1.11

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

State or province

Enter the State or province.

This entry appears in the subject or issuer of the certificate under ST= (**ST**ate).

SNMP ID:

2.39.2.14.1.12

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

E-mail

Enter an e-mail address:

This entry appears in the subject or issuer of the certificate under `emailAddress=`.

SNMP ID:

2.39.2.14.1.13

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 36 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Surname

Enter a surname.

This entry appears in the subject or issuer of the certificate under `SN=` (**S**ur**N**ame).

SNMP ID:

2.39.2.14.1.14

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 32 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:
empty

Serial number

Enter a serial number.

This entry appears in the certificate under `serialNumber=`.

SNMP ID:
2.39.2.14.1.15

Telnet path:
Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:
Max. 32 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:
empty

Postal code

Enter the location post code.

This entry appears in the subject or issuer of the certificate under `postalCode=`.

SNMP ID:

2.39.2.14.1.16

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 25 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Template

Select a suitable profile template here, if applicable.

The profile template specifies which certificate information is mandatory and which can be changed. Templates are created under **Setup** > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**.

SNMP ID:

2.39.2.14.1.17

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 31 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Subject-Alternative-Name

Specify the subject alternative name (SAN) here. The SAN contains further information for use by applications.

SNMP ID:

2.39.2.14.1.18

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 254 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Template

In this table, you define the templates for certificate profiles.

Here you specify which of the profile properties are mandatory and which are to be edited by the user. The following options are available:

- No: The field is invisible, the value entered is considered to be a default value.
- Fixed: The field is visible, but cannot be changed by the user.
- Yes: The field is visible and can be changed by the user.
- Mandatory: The field is visible, the user must enter a value.

Note: A “Default” template is already available.

SNMP ID:

2.39.2.14.2

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface**

Name

Give the template a unique name here.

SNMP ID:

2.39.2.14.2.1

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Max. 31 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*-:<>?[\]_.`

Default:

empty

Key usage

Specifies for which application the profile is to be used.

SNMP ID:

2.39.2.14.2.2

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Extended key usage

Specifies the extended application for which the profile is to be used.

SNMP ID:

2.39.2.14.2.3

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

RSA key length

Sets the length of the key.

SNMP ID:

2.39.2.14.2.4

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Validity period

Specifies the duration, in days, for which the key is valid. After this period, the key becomes invalid unless the user renews it.

SNMP ID:

2.39.2.14.2.5

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

CA

Indicates whether this is a CA certificate.

SNMP ID:

2.39.2.14.2.6

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Password

Password to protect the PKCS12 certificate file.

SNMP ID:

2.39.2.14.2.7

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Country

Specifies the country identifier (e.g. “DE” for Germany).

SNMP ID:

2.39.2.14.2.8

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:
Yes

Locality name

Specifies the locality.

SNMP ID:
2.39.2.14.2.9

Telnet path:
Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes
The field is visible and can be changed by the user.

No
The field is invisible, the value entered is considered to be a default value.

Mandatory
The field is visible, the user must enter a value.

Fixed
The field is visible, but cannot be changed by the user.

Default:
Yes

Organization

Specifies the organization issuing the certificate.

SNMP ID:

2.39.2.14.2.10

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Organization unit name

Specifies the unit within the organization that issues the certificate.

SNMP ID:

2.39.2.14.2.11

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

State or province

Specifies the State or province.

SNMP ID:

2.39.2.14.2.12

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

E-mail

Specifies the e-mail address.

SNMP ID:

2.39.2.14.2.13

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:
Yes

Surname

Specifies the surname.

SNMP ID:
2.39.2.14.2.14

Telnet path:
Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes
The field is visible and can be changed by the user.

No
The field is invisible, the value entered is considered to be a default value.

Mandatory
The field is visible, the user must enter a value.

Fixed
The field is visible, but cannot be changed by the user.

Default:
Yes

Serial number

Specifies the serial number.

SNMP ID:

2.39.2.14.2.15

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Postal code

Specifies the postal code.

SNMP ID:

2.39.2.14.2.16

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

Subject-Alternative-Name

The “Subject Alternative Name” (SAN) links additional data with this certificate.

SNMP ID:

2.39.2.14.2.17

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

2 Configuration

2.1 Encrypted storage of configurations with LANconfig

As of HiLCOS version 9.10, it is possible to encrypt configuration and script files and to give them a checksum. Configuration files can be given password protection for encryption and secure storage with LANconfig, so preventing any unauthorized access to configurations.

Command	*Description*
`readconfig [-h] [-s <password>]`	Shows the complete configuration in the format of the device syntax. ▶ `-h`: Adds a checksum to the configuration file. ▶ `-s <password>`: Encrypts the configuration file with the use of the specified password. **Access rights**: Supervisor-Read
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>]`	The readscript command generates a text dump of all commands and parameters required to configure the device in its current state. You can use the following option switches for this: ▶ `-n`: The text output is only numerical without identifiers. The output only contains the current status values of the configuration as well as the associated SNMP IDs. ▶ `-d`: The default values are included in the text output. ▶ `-i`: The table designations are included in the text output. ▶ `-c`: Includes any comments contained in the script file. ▶ `-m`: The text is output to the screen in a compact but difficult to read format (no indentations). ▶ `-h`: Adds a checksum to the script file. ▶ `-s <password>`: Encrypts the script file with the use of the specified password.

Command	Description
	Access rights: Supervisor-Read

Table 4: Overview of all commands available at the command line

2.1.1 Saving and loading device-configuration and script files

A device configuration file contains all of its settings. Script files are useful for managing the settings of a device automatically. To protect of these files against unauthorized access or transmission errors, it is possible to export them from or upload them to the device in an encrypted state and with a checksum.

There are three different file types:

- No checksum, no encryption: A text file with content readable by a text editor.
- Checksum: The text file contains information about the checksum and the hash algorithm for calculating this checksum. The contents of this text file is readable with a simple text editor.

  Note: LANconfig prior to version 9.10 recognizes files with checksums.

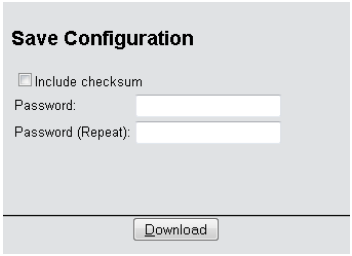
- Encryption: Before the file is exported it is encrypted by the device using a password chosen by the administrator. The text file contains information about the encryption algorithm used, as well as a checksum. The contents of the text file is no longer decipherable by a text editor, with the exception of the file header.

  Note: LANconfig prior to version 9.10 cannot read encrypted files.

Note: The file extensions of these files are `.lcf` for configuration files or `.lcs` for script files. The detection of a file that is encrypted and/or contains a checksum relies exclusively on the file header.

Configuration management with WEBconfig and the console

To export a configuration file from WEBconfig, navigate to the view **File management** > **Save configuration**.



The following options are available:

No entries

By default, all options are disabled. A click on **Download** invokes the dialog for downloading an unencrypted configuration file without a checksum.

Include checksum

A click on **Download** invokes the dialog for downloading an unencrypted configuration file with a checksum.

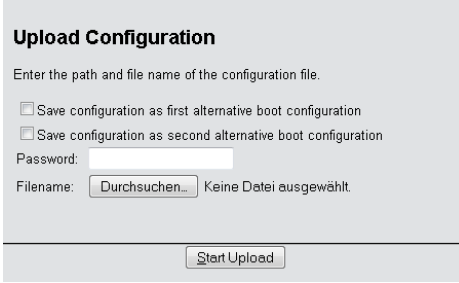
Password

Specify a password if you want to encrypt the configuration file before downloading it.

To save the configuration from the console, use the following parameters:

- `readconfig`: Backs up the configuration without checksum and encryption.
- `readconfig -h`: Adds a checksum to the configuration file.
- `readconfig -s <password>`: Encrypts the configuration file with the use of the specified password.

To upload a configuration file with WEBconfig, navigate to the view **File management** > **Upload configuration**.

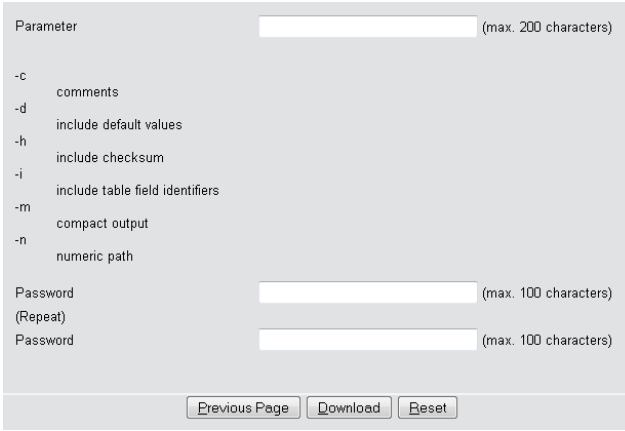


If the configuration file is encrypted, enter the appropriate password and click on **Start upload**.

Note: For more information about alternate boot configurations, see the chapter *Alternative boot config*.

Script management with WEBconfig and the console

To export a script file from WEBconfig, navigate to the view **File management** > **Save configuration script**.



The following options are available:

Parameters

By default, all options are disabled. A click on **Download** invokes the dialog for downloading an unencrypted script file without a checksum.

Password

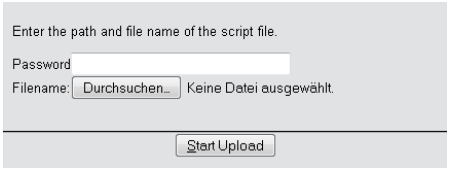
Specify a password if you want to encrypt the script file before downloading it.

To save the script file from the console, the following parameters are available:

- `readscript`: Backs up the configuration without checksum and encryption.
- `readscript -h`: Adds a checksum to the configuration file.
- `readscript -s <password>`: Encrypts the configuration file with the use of the specified password.

Note: More information about the parameters, see the chapter *Commands for the console* in the section about `readscript`.

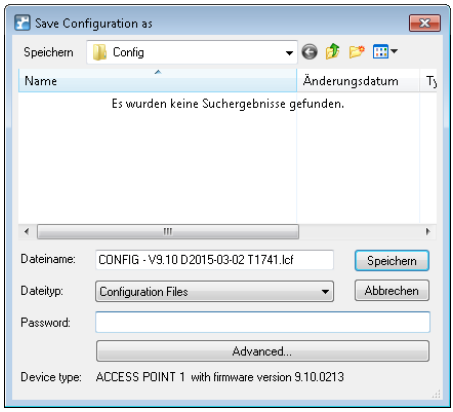
To upload a script file with WEBconfig, navigate to the view **File management** > **Execute configuration script**.



If the script file is encrypted, enter the appropriate password and click on **Start upload**.

Configuration management with LANconfig

You can use LANconfig to save a configuration file by right-clicking on the corresponding device in the list of devices. From the context dialog, open the save dialog under **Configuration management** > **Save as file**.



The following entries are available:

File name

LANconfig composes the file name from various pieces of information (including version number, date and time). Change the name to suit your needs.

File type

Choose whether this is a configuration file or something else.

Password

Specify a password if you want to encrypt the configuration file before downloading it.

Under **Advanced** you can set optional parameters that are processed by the device when a configuration file is loaded automatically (auto-load). Use this to customize the configuration.

You can use LANconfig to upload a configuration file to the device by right-clicking on the device where the configuration is to be uploaded. From the context dialog, open the restore dialog under **Configuration management** > **Restore from file**.

Select the required configuration file, enter the password (if applicable) and click **Open** to upload the configuration to the device.

2.1.2 Additions to the Status menu

Script log

This table provides an overview of the executed scripts.

SNMP ID:

1.11.23

Telnet path:

Status > **Config**

Index

Shows the index of this entry.

SNMP ID:

1.11.23.1

Telnet path:

Status > **Config** > **Script-Log**

Time

Shows the time of this entry.

SNMP ID:

1.11.23.2

Telnet path:

Status > **Config** > **Script-Log**

Comment

Shows the comment for this entry.

SNMP ID:

1.11.23.3

Telnet path:

Status > **Config** > **Script-Log**

Successful

Shows whether the script was successfully completed.

SNMP ID:

1.11.23.4

Telnet path:

Status > **Config** > **Script-Log**

Error line

In the event of an error, this shows which line of the script caused the abort.

SNMP ID:

1.11.23.5

Telnet path:
Status > **Config** > **Script-Log**

2.2 Each device has its own SSL key & changes to the default SSL settings

As of HiLCOS version 9.10, after a configuration reset each device generates its own SSL RSA key of 2048-bit length.

Further, “RC4-128” is no longer set as the default for HTTPS connections.

2.2.1 Automatic generation of device-specific SSH/SSL keys

If you have a device with HiLCOS 8.90 or higher and you have not loaded an individual key into the device, then resetting the configuration will prompt the internal SSH server to try and compile its own device-specific SSH keys directly at the system startup. These include:

- an SSH-2-RSA key with 2048 bit length;
- an SSH-2-DSS key with 1024 bit length (as per FIPS 186-2);
- an SSH-2-ECDSA key with 256, 384 or 521 bit length;
- an SSL-RSA key with 2048 bit length;

which the device stores in its internal file system as `ssh_rsakey`, `ssh_dsakey`, `ssl_privkey` or `ssh_ecdsakey`.

If key generation is successful, the entry `SSH ... host key generated` is entered into the SYSLOG as a “notice”; If it fails, the entry `SSH: host key generation failed, try later again with '...'` is entered as an “alert”. The failure to generate a key, for example if there is too little entropy, causes the system to revert to the factory implemented cryptographic key.

Important: When you an update from an older HiLCOS version to 8.90 or higher without subsequently doing a configuration reset, the device does not generate a device-specific SSH/SSL key. This maintains compatibility with

existing installations. However, you can trigger the key generation manually. Enter the following commands in the console:

```
sshkeygen -t rsa -b 2048 -f ssh_rsakey
sshkeygen -t dsa -b 1024 -f ssh_dsakey
sshkeygen -t ecdsa -b 256 -f ssh_ecdsakey
sshkeygen -t rsa -b 2048 -f  ssl_privkey
```

2.2.2 Manually create custom SSH keys

You have the option to replace the factory installed and automatically generated SSH/SSL keys with your own RSA, DSA or DSS keys, in order to achieve stronger encryption. A number of alternatives are available here:

- You can generate the individual keys on the console using HiLCOS.
- Using an external program, you can create an OpenSSH private key and then upload this key to the device as `SSH- DSA-key [...]` or `SSH-RSA key (*.key [BASE64 unencrypted])`.

The use of an external program is an option if your device has insufficient entropy, so causing key creation with HiLCOS to fail.

SSH key generation with HiLCOS

To generate a key pair consisting of a public and a private key, you enter the following command at the console:

```
sshkeygen [-?|-h] [-t (dsa|rsa|ecdsa)] [-b <Bits>] -f <OutputFile> [-q]
```

-?, -h
Displays a brief help text about the available parameters

-t (dsa|rsa|ecdsa)
This parameter specifies what type of key is generated. SSH supports the following types of keys:

- RSA keys are most widely used and have a length between 512 and 16384 bits. If possible you should work with keys of 1024 to 2048 bits in length.
- DSA keys follow the Digital Signature Standard (DSS) set down by the National Institute of Standards and Technology (NIST) and are

typically used in environments which are required to comply with the Federal Information Processing Standard (FIPS). DSA or DSS keys are always 1024 bits long, but they are slower to process than a corresponding RSA key.

- ECDSA keys are a variant of DSA keys, whereby the device uses elliptic curves for key generation (elliptic curve cryptography, ECC). ECC is an alternative to the conventional signature and key exchange techniques such as RSA and Diffie-Hellman. The main advantage of elliptic curves is that their mathematical properties offer the same key strength as RSA or Diffie-Hellman but with a significantly shorter key length. This provides for better hardware performance. ECC and its integration in SSL and TLS are described in RFCs 5656 and 4492.

If no type is specified, the command generates an RSA key by default.

-b <bits>

This parameter sets the length of the RSA key in bits. If you do not specify a length, the command produces a key with a length of 1024 bits by default.

-f <OutputFile>

These parameters specify the mounting point of the generated key file in the device file system. The choice of mounting point depends on what type key you are generating. The choices available to you are:

- `ssh_rsakey` for RSA keys
- `ssh_dsakey` for DSA keys
- `ssh_ecdsakey` for ECDSA keys
- `ssl_privkey` for SSL-RSA keys

-q

This parameter enables the 'quiet' mode for the key generation. If you set this parameter, HiLCOS overwrites any existing RSA or DSA keys without asking; there is no information about the progress of the operation. You can, for example, use this parameter in a script to suppress any security prompts for the users.

SSH key generation with Linux systems

Many Linux distributions already feature the OpenSSH package. All you have to do to generate the key file is to enter a simple command into the shell. The syntax corresponds to the HiLCOS command `sshkeygen`:

```
ssh-keygen [-t (dsa|rsa)] [-b <Bits>] [-f <OutputFile>]
```

The command `ssh-keygen -t rsa -b 4096 -f hostkey` creates an RSA key of 4096 bits in length, which consists of the private component 'hostkey' and the public component 'hostkey.pub'.

SSH key generation with Windows systems

Windows systems not are inherently capable of compiling SSH keys. You should instead use a suitable utility program such as the free software PuTTYgen.

A guide on how to create an individual key with PuTTYgen is available in the section *Generating an SSH keypair with PuTTY*. After following the various steps to generate the key, do **not** use the buttons **Save public key** and **Save private key**, but instead choose **Conversions** > **Export OpenSSH key**. The resulting OpenSSH private key can then be uploaded into the device without further processing.

2.2.3 Additions to the Setup menu

Crypro algorithms

This bitmask specifies which cryptographic algorithms are allowed.

SNMP ID:

2.21.40.5

Telnet path:

Setup > **HTTP** > **SSL**

Possible values:

RC4-40

RC4-56
RC4-128
DES40
DES
3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

Default:

3DES
AES-128
AES-256
AESGCM-128
AESGCM-256

3 Diagnosis

3.1 Advanced config version information under Status

As of HiLCOS version 9.10, you will find additional information about your current configuration (date, hash, version) in WEBconfig and via the console under **Status** > **Config**.

3.1.1 Additions to the Status menu

Configuration date

This entry indicates when you last changed the configuration of the device.

Note: The time is displayed in UTC format.

SNMP ID:

1.11.20

Telnet path:

Status > **Config**

Configuration hash

This entry shows you the hash value of the current configuration.

Note: The displayed value is a SHA1 hash.

SNMP ID:
1.11.21

Telnet path:
Status > **Config**

Configuration version

This entry shows you the current version of the device configuration.

SNMP ID:
1.11.22

Telnet path:
Status > **Config**

3.2 SSH identifier in the event log

As of HiLCOS version 9.10, the device displays the SSH identifier in the event log for connections encrypted by SSH.

3.2.1 Additions to the Status menu

Event log

This log table is an overview of all of the logged event messages that affect the configuration of the device, such as failed logins or firmware update history.

SNMP ID:
1.11.12

Telnet path:

Status > **Config**

Possible values:

Idx.

Index number of the event

System time

Time of the event

Event

Event message in abbreviated form

Access

Access protocol used, e.g. SSH or HTTPS

IP address

IP address that was used to access the device

Info1

Event code

Info2

Description of the event code

Info3

SSH identifier

4 LCMS

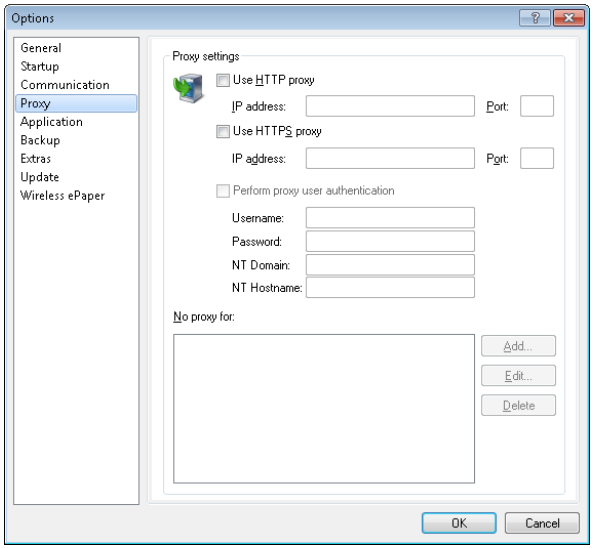
4.1 Proxy authentication via NTLM

As of HiLCOS version 9.10, proxy authentication of LANconfig via NT LAN Manager (NTLM) is now possible.

4.1.1 Proxy

If you wish to use a proxy server for access to your device, you can configure this here. Activate the required protocol and enter the address and port for accessing the proxy server.

Depending on the protocol, it may be possible to specify a list of networks or individual hosts for which the proxy settings do not apply.



Use HTTP proxy

Enables the use of an HTTP proxy.

- **Address**: Enter the IP address of the the HTTP proxy server.
- **Port**: Enter the port used by the HTTP proxy server.

Use HTTPS proxy

Enables the use of an HTTPS proxy.

- **Address**: Enter the IP address of the the HTTPS proxy server.
- **Port**: Enter the port used by the HTTPS proxy server.

Perform proxy user authentication

If the proxy server requires authentication, enter the user name and password here. If the NT LAN Manager (NTLM) is to carry out the authentication, you additionally enter the NT domain and computer name.

Note: This option is available only if the proxy setting is enabled.

No proxy for

Enter the IP addresses and the corresponding netmask to which the proxy settings do not apply.

Note: This option is available only if the proxy setting is enabled.

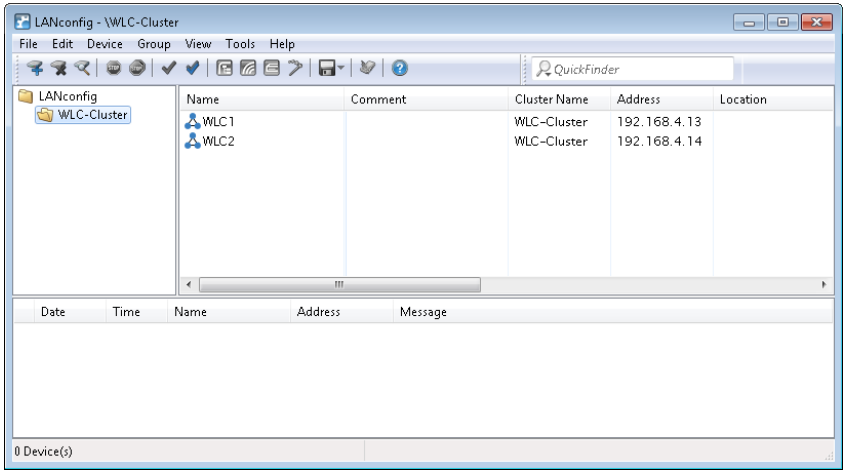
4.2 Special LANconfig icon for devices in a cluster or using Config Sync

LANconfig has a specific icon to mark devices that share their configuration via Config Sync. Furthermore, the **Config Cluster** column shows the configuration group for each device. LANconfig is thus able to sort and edit the device listing according to cluster name.

If you try to make changes to the configuration of a cluster member, you will receive following warning:

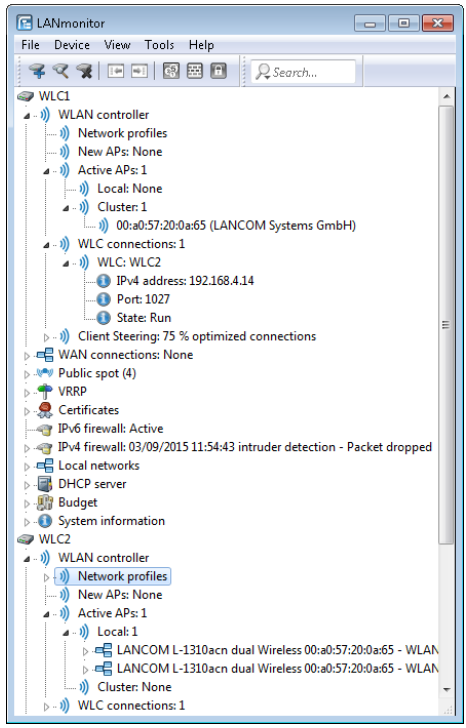
"This device belongs to the Config Cluster: [cluster name]. Editing this configuration also affects the following devices: [Listing of all devices in the same cluster]"

You can bypass this message if necessary. To do this, enable the option **Don't show again** in the displayed window.



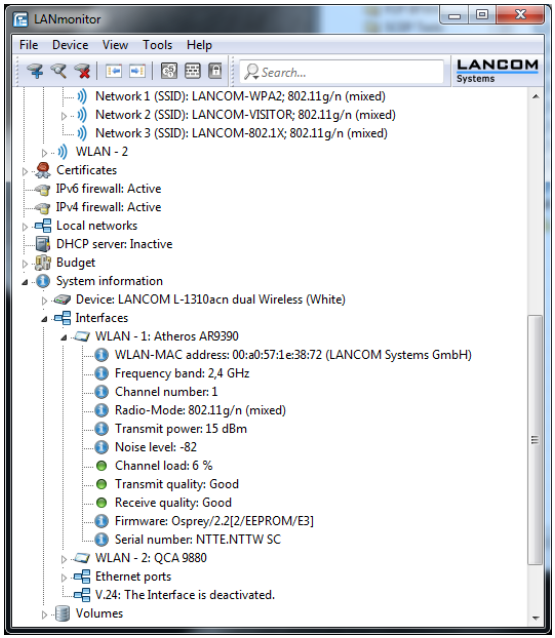
4.3 Special LANmonitor icon for devices in a cluster or using Config Sync

LANmonitor has a specific icon to mark devices that share their configuration via Config Sync. Also, the name of the configuration group (cluster name) is shown after the device name. LANmonitor thus makes it easier to see which devices share the same configuration.

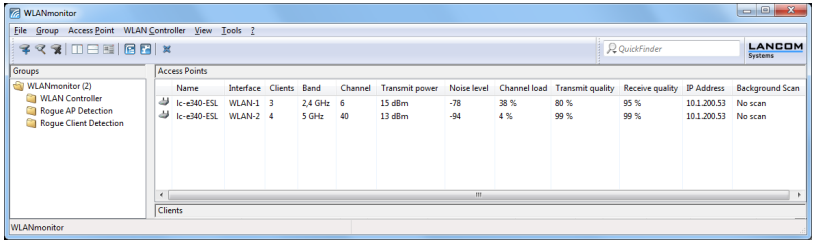


4.4 "Wireless Quality Indicators" (WQI)

LANmonitor optionally displays the signal quality of the individual interfaces with the **Wireless Quality Indicators**. This representation of reception and transmission quality (RX and TX) helps you to make a quick assessment of signal quality. To display this information in LANmonitor, open the section **System information** for the device. The indicators are displayed under **Interfaces**.



The WLANmonitor also displays the **Wireless quality indicators**. To do this click on the main folder for the group.



4.5 Extended number of characters for device names

The current release of HiLCOS allows you to assign longer device names in LANconfig and WEBconfig. The number of characters allowed is now 64 instead of 16.

4.6 Different notations for MAC addresses

As of HiLCOS version 9.10, LANconfig allows MAC addresses to be entered in other formats.

4.6.1 Different notations for MAC addresses

To make it easier to enter MAC addresses by using copy and paste from other applications into LANconfig, the following formats can be used when entering MAC addresses:

- 000000000000
- 00:00:00:00:00:00
- 00-00-00-00-00-00
- 000000-000000

The input is then automatically converted into the form `00:00:00:00:00:00`.

4.7 LANconfig: Text corrections relating to access rights

As of HiLCOS version 9.10, the descriptions of the access rights in the configuration menu **Management** > **Admin** in the section **Configuration access ways** have been corrected:

- From a LAN interface
- From a WLAN interface

- From a WAN interface

LANconfig also used the new names in the section **Access to web-server services** > **Access rights**.

5 IPv6

5.1 Prefix-exclude option for DHCPv6 prefix delegation

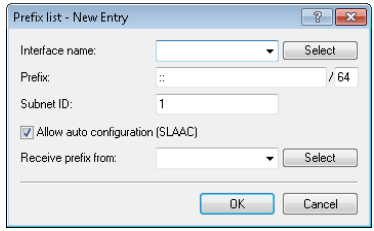
As of HiLCOS version 9.10, the DHCPv6 client of the device supports the prefix exclude option for DHCPv6-based prefix delegation according to RFC 6603.

5.1.1 Prefix-exclude option for DHCPv6 prefix delegation

The DHCPv6 client of the device supports the prefix exclude option for DHCPv6-based prefix delegation according to RFC 6603.

Providers use this mechanism with DHCPv6 prefix delegation in order to exclude a prefix from the delegated prefix set from being used on the customer LAN. This means that the device does not require an additional prefix for the WAN link, but instead it uses the prefix that was excluded from the delegated DHCPv6 prefix set. This prefix is no longer available for the LAN on the customer site.

If a device is configured to use the excluded prefix for the LAN, is a syslog message is issued and the prefix is not advertised on the LAN. To resolve this conflict, you configure a different subnet ID for this LAN under **IPv6** > **Router advertisement** > **Prefix list**.



6 Public Spot

6.1 Restricting administrators to voucher output only

If in HiLCOS you have created an administrator who is restricted to the function rights of the **Public Spot Wizard (create account)** only, then this administrator now has access only to the input mask of the add user wizard. The navigation toolbar in WEBconfig remains concealed.

6.1.1 Wizard for creating and managing users

Using the setup wizard **Create Public Spot account** you can use WEBconfig to create temporary accesses to the Public Spot network with just a few clicks of the mouse. In the simplest case, you only need to enter the duration of access, the wizard assigns the username and password automatically and stores the credentials in the user database of the internal RADIUS server. The user receives a printed, personalized voucher, which the user can immediately use to login to the Public Spot network for the specified period.

Alternatively, a stock of vouchers can be created and printed out to speed up the voucher issue at peak times or to allow employees without access to the device to issue vouchers. In this case the Public Spot account is created with an online time duration that starts when the user logs in for the first time. You also set a maximum validity period for the access. After this time, the Public Spot automatically deletes the access account, even if the online time was not used up yet.

The setup wizard **Manage Public Spot account** displays all registered Public-Spot access accounts in a table on a web page. This gives you an overview of your most important user data, as well as a user-friendly way to extend or reduce the validity of an access account with a single click, or even delete user accounts completely. In addition, the administrator can call up information about the user account using the wizard, such as the password in cleartext,

the authentication status, the IP address, the sent/received data volume or any restrictions that apply to the user account.

If several administrators are involved with the management of Public Spot accounts, you have the option of restricting the accounts that are displayed to those created by the respective administrator. As a result, the overview table only displays those accounts that were created by the administrator who is currently logged-on.

Note: This restriction has no effect if an administrator account has a full name that is a part of the other administrator account names. "PSpot_Admin" for example sees the entries made by "PSpot_Admin1" and "PSpot_Admin2". "PSpot_Admin" acts as a super-admin in this scenario. All other administrators ("PSpot_AdminX"), however, do not see the entries made by the others.

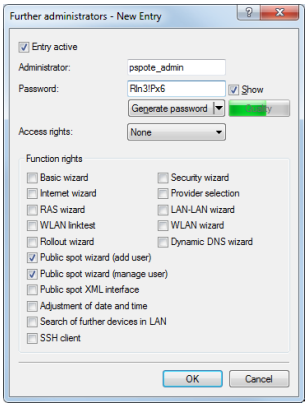
6.1.2 Setting up limited administrator rights for Public Spot managers

It is possible to allow employees to create and manage user accounts even though they do not have access rights to the device configuration. This is done by setting up a limited administrator, who only has the right to use the *Public Spot Wizard*. This tutorial describes the steps and the necessary access rights and privileges to do this in LANconfig.

The rights to use the Public Spot Wizards are configurable separately from one another, so it is possible to restrict a limited administrator to any single Wizard. In the case of the Public Spot setup wizard, the restricted administrator logging in to WEBconfig is automatically forwarded to the corresponding input mask.

1. In LANconfig, open the configuration dialog for the device you want to add a Public Spot administrator to.
   The Public Spot option has to be enabled on this device.
2. Navigate to the item **Management** > **Admin**. In the section **Device configuration**, click **Further administrators** and then click **Add**.

   To allow an existing user to perform Public Spot management, you instead select the user's entry in the table and click on **Change**.

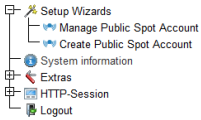


3. You activate the profile by checking the **Entry active** box.
4. Assign a descriptive name in the field **Administrator**.
5. Enter a **Password** and repeat it as a check.
6. Set the **Access rights** to **None**.
7. In the section **Function rights** enable the options **Public Spot wizard (add user)**, and **Public Spot wizard (manage user)** for the Public Spot setup wizard.

   Note: The function right **Public Spot XML interface** is not required by a Public Spot administrator. The right is only relevant if you use the XML interface and should not be combined with the function rights described above for security reasons.

8. Save the new or modified administrator profile by clicking on **OK**.

If you have granted the feature rights to several Wizards, the limited administrator can navigate between these using the navigation bar in WEBconfig.



If you have set the function right for the **Public Spot Wizard (create user)** only, then a limited administrator can only navigate within this Wizard, and the navigation bar is hidden. In this case it is not possible to logout of WEB-

config manually. For security reasons, this means that the lifetime of the WEBconfig session is very short. In case of inactivity, the device automatically logs out the limited administrator.

Note: For technical reasons, the Create Public Spot Account wizard does not update automatically after use of the **Create and CSV export** button. A limited administrator who wishes to set up additional users and print vouchers must invoke the Wizard again (e.g. via a URL or by refreshing the web page if the navigation bar is hidden).

6.2 Specify volume budget on vouchers

HiLCOS9.10 now enables you to use the placeholder tag `<pbelem vollimit>` in the voucher template, so as to inform Public Spot users of the data volume assigned to them.

VOLLIMIT

Valid for:`<pbelem><pbcond>`

This identifier contains the amount of data, expressed in bytes, that the client is still allowed to transfer before the device terminates the current session. This identifier is zero for a session with no data limit.

6.3 XML interface: Enhanced VLAN handling

As of HiLCOS version 9.10, you have the option to communicate the user's source VLAN to the Public Spot via an external gateway, and to forward the VLAN-ID dependent authentication to an external RADIUS server.

`SOURCE_VLAN` (optional, only in conjunction with authentication by RADIUS server)

The VLAN ID of the network from which a Public Spot user attempts to login (source VLAN). The Public Spot forwards the source VLAN in its access request to the internal or external RADIUS server. The Public Spot uses the RADIUS attribute 81 (**tunnel-private-group-ID**) together with

the RADIUS attributes 64 (**tunnel-type**) and 65 (**tunnel-medium-type**). The RADIUS server uses the source VLAN to decide whether to accept or decline the access request from the Public Spot.

If the RADIUS server accepts the request, it returns an access-accept with the RADIUS attributes mentioned above to the Public Spot. The Public Spot then saves the source VLAN for the client and its station list and allows the user to access the Public Spot network.

Tip: Use the source VLAN in conjunction with the setup parameter 2.24.47. This prevents Public Spot users in VLAN-separated Public Spot networks/SSIDs from authenticating once at the RADIUS server and then accessing all of the managed Public Spot networks/SSIDs.

Note: The `SOURCE_VLAN` should not be confused with the `VLAN_ID`. The `VLAN_ID` is not sent to the RADIUS server. However, the Public Spot uses it to assign a VLAN ID provided by the gateway to a successfully authenticated user.

For internal checking, the Public Spot stores the source VLAN to its station table as soon as the external RADIUS server has accepted the authentication request. If a user then switches to a different Public Spot network/SSID with a VLAN-ID which is different to that stored, then the Public Spot sets the user to "unauthenticated" and displays the login page again at the next opportunity.

6.3.1 Additions to the Setup menu

Check origin VLAN

Use this parameter to specify whether the VLAN ID of the network where a user is authenticated is used by the XML interface to verify user requests. This is relevant, for example, in scenarios where several Public Spot SSIDs are separated by means of VLAN and a one-time authentication at one of these SSIDs should not automatically entitle the user to access the other SSIDs.

Note: The parameter requires that you have also enabled the setup parameters 2.24.40.1 (the XML interface itself) and 2.24.40.2 (authentication by the XML interface via an internal or an external RADIUS server) .

SNMP ID:

2.24.47

Telnet path:

Setup > **Public-Spot-Module**

Possible values:

No

The Public Spot does not take the VLAN ID into account when verifying users. A one-time authentication entitles a user to access all of the SSIDs managed by the Public Spot. As long as the user account is valid, authentication is automatic.

Yes

The Public Spot takes the VLAN ID into account when verifying users. The Public Spot stores the VLAN ID to the column of the same name in the station table, assuming that the authentication by the RADIUS server was successful. This VLAN ID is the value for `SOURCE_VLAN` in the login request from the external gateway. If the Public Spot user moves to a network with a different VLAN ID, the Public Spot updates their station-table entry to “unauthenticated” and prompts the user to authenticate at the RADIUS server again. In this case, the user receives the sign-in page to authenticate again.

Note: To learn more about the request and response types, as well as the `SOURCE_VLAN` element, refer to the User Guide.

Default:

No

VLANs

This parameter optionally defines a list of VLAN IDs which control the approved site(s) that are available to the corresponding host name. Only users who have the VLAN ID stored in the station table are able to access this host without having to authenticate. Use this parameter, for example, in application scenarios where Public Spot networks/SSIDs are separated by VLAN and you wish to set different access restrictions for different user groups.

SNMP ID:

2.24.31.3

Telnet path:

Setup > **Public-Spot-Module** > **Free-Networks** > **VLans**

Possible values:

Default:

empty

Comma-separated list, max. 16 characters from `[0-9],`

Special values:

empty, **0**

Access to the host entered here is possible from all VLANs.

6.3.2 Messages to and from the authentication server

Transferred attributes

As previously mentioned, your device transmits far more than just the user-name and password in a RADIUS request. RADIUS servers might choose to completely ignore these additional attributes, or only use a subset of these attributes. Many of these attributes are used for access to the server using dial-in, and are defined as standard attributes in the RADIUS RFCs. However, some important information for hotspot operation can not be represented with

standard attributes. These additional attributes are manufacturer-specific with the manufacturer code 2356 (Hirschmann Automation and Control GmbH).

ID	Name	Meaning	Possible values in HiLCOS
1	User name	The name entered by the user.	
2	User-Password	The password entered by the user.	
4	NAS-IP-Address	IP address of your device	<IPv4 address of the device>
6	Service-Type	Type of service that the user requested. The value “1” stands for Login.	
8	Framed-IP-Address	Specifies the IP address that is assigned to the client.	<IP address of the client>
30	Called-Station-Id	MAC address of your device	<nn:nn:nn:nn:nn:nn>
31	Calling-Station-Id	MAC address of the client The address is given byte-wise in hexadecimal notation with separators.	<nn:nn:nn:nn:nn:nn>
32	NAS identifier	Name of your device, if configured.	<Device-Name>
61	NAS-Port-Type	Type of physical port over which a user had requested authentication.	▶ **ID 19** denotes clients from WLAN. ▶ **ID 15** denotes clients from Ethernet.
87	NAS-Port-Id	Description of the interface over which the client is connected to your device. This may be a physical and a logical interface. **Note:** Consider that more than one client may be connected to one interface at a time, so that, unlike dial-in servers, port numbers are not unique for clients.	For example ▶ LAN-1 ▶ WLAN-1-5 ▶ WLC-TUNNEL-27

Table 5: Overview of the RADIUS attributes transmitted by the device to the authentication server

Processed attributes

Your device evaluates the authentication response of a RADIUS server for attributes that it may possibly process further. Most attributes however only have a meaning if the authentication response was positive, so that they influence the subsequent session:

ID	Name	Meaning	Possible values in HiLCOS
18	Reply-Message	An arbitrary string from the RADIUS server that may transport either a login failure reason or a user welcome message. This message may be integrated into user-defined start or error pages via the SEVERMSG element.	
25	Class	An arbitrary octet string that may contain data provided by the authentication/accounting backend. Whenever the device sends RADIUS accounting requests, they will contain this attribute as-is. Within an authentication response, this attribute can occur multiple times in order, for example, to transmit a string that is longer than 255 bytes. The device processes all occurrences in accounting requests in the order they appeared in the authentication response.	
26	Vendor 2356, Id 1 LCS-Traffic-Limit	Defines the data volume in bytes after which the device automatically ends the session. This value is useful for volume-limited accounts. If this attribute is missing in the authentication response, it is assumed that no volume limit applies. A traffic limit of 0 is interpreted as an account which is principally valid, however with a used-up volume budget. The device does not start a session in this case.	
26	Vendor 2356, Id 3 LCS-Redirection-URL	This can contain any URL that is offered as an additional link on the start page. This can be the start page of the user or a page with additional information about the user account.	
26	Vendor 2356, Id 5 LCS-Account-End	Defines an absolute point in time (measured in seconds since January 1, 1970 0:00:00) after which the account becomes invalid. If this attribute is missing, an unlimited account is assumed. The device does not start a session if its internal clock has not been set, or the given point in time is in the past.	
26	Vendor 2356, Id 7 LCS-Public-Spot-Username	Contains the name of a Public Spot user for auto-login. Auto-login refers to the table of MAC authenticated users who are automatically assigned usernames by the server.	
26	Vendor 2356, Id 8 LCS-TxRateLimit	Defines the maximum downstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.	
26	Vendor 2356, Id 9 LCS-RxRateLimit	Defines the maximum upstream rate in kbps. This restriction may be combined with the corresponding Public Spot function.	

ID	*Name*	*Meaning*	*Possible values in HiLCOS*
26	Vendor 2356, Id 13 LCS-Advertisement-URL	Specifies a comma-separated list of advertisement URLs.	
26	Vendor 2356, Id 14 LCS-Advertisement-Interval	Specifies the interval in minutes after which the Public Spot reroutes a user to an advertisement URL. With an interval of 0 forwarding occurs directly after login.	
27	Session-Timeout	Defines an optional maximum duration of the session, measured in seconds. If this attribute is missing in the response, an unlimited account is assumed. A Session timeout of zero seconds is interpreted as an account which is principally valid, however with a used-up time budget. The device does not start a session in this case.	
28	Idle timeout	Defines a time period in seconds after which the device will terminate the session if no packets were received from the client. This value may possibly overwrite the idle timeout that is defined locally under **Public Spot** > **Server** > **Idle timeout**.	
64	Tunnel-Type	Defines the tunneling protocol which will be used for the session.	
65	Tunnel-Medium-Type	Defines the transport medium over which the tunneled session will be established.	
81	Tunnel-Private-Group-ID	Defines the group ID if the session is tunneled.	
85	Acct-Interim-Interval	Defines the amount of time between subsequent RADIUS accounting updates. This value is only evaluated if the RADIUS client does not have a local accounting interval defined, i.e. if you have not set an **Accounting update cycle** for the Public Spot module.	

Table 6: Overview of the supported RADIUS attributes

Note: Note that the LCS-Account-End and Session-Timeout attributes are mutually exclusive, and it therefore does not make sense to include both in the response. If both attributes are included in a response, the attribute that appears as the last one in the attribute list will define the session’s time limit.

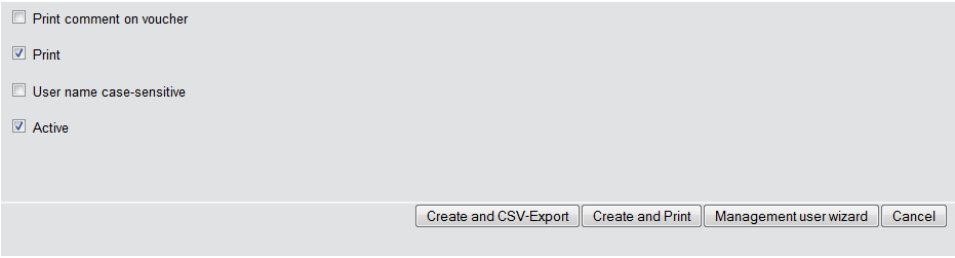
6.4 "Small header image": Optimized display for 19" devices

As of HiLCOS version 9.10, 19-inch devices also have a login page with a customizable header image for narrow screens. This improves the way the Public Spot appears on mobile devices.

6.5 New button "Manage user wizard"

As of HiLCOS version 9.10 you have the option in the Setup Wizard **Create Public Spot account** to display the additional button **Manage user wizard**.

The button **Manage User Wizard** button takes you to the **Manage Public Spot Account** Setup Wizard.



Note: You have the option to either show or hide this button. It is displayed by default.

6.5.1 Additions to the Setup menu

Hide-User-Management-Button

This parameter gives you the option to hide the **Manage user wizard** button in the Setup Wizard.

SNMP ID:

2.24.19.20

Telnet path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Yes

The **Create Public Spot account** Setup Wizard hides the **Manage user wizard** button.

No

The Setup Wizard displays the **Manage user button**.

Default:

No

6.6 Only show user accounts generated by the currently logged-on administrator

As of HiLCOS version 9.10, the Setup Wizard **Manage Public Spot account** gives you have the option to hide accounts that were created by other administrators.

If several administrators are involved with the management of Public Spot accounts, you have the option of restricting the accounts that are displayed to those created by the respective administrator. As a result, the overview table only displays those accounts that were created by the administrator who is currently logged-on.

Note: This restriction has no effect if an administrator account has a full name that is a part of the other administrator account names. "PSpot_Admin" for example sees the entries made by "PSpot_Admin1" and "PSpot_Admin2". "PSpot_Admin" acts as a super-admin in this scenario. All other administrators ("PSpot_AdminX"), however, do not see the entries made by the others.

6.6.1 Additions to the Setup menu

show-all-users-admin-independent

This entry allows you to display only those user accounts in the Setup Wizard that were created by the currently logged-in administrator.

SNMP ID:

2.24.44.11

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard displays all Public Spot accounts.

No

The Setup Wizard only displays the Public Spot accounts created by the currently logged-on administrator.

Default:

Yes

6.7 Evaluation of DHCP option 82 in RADIUS and Public Spot

As of HiLCOS version 9.10, RADIUS client and Public Spot devices evaluate the DHCP option 82.

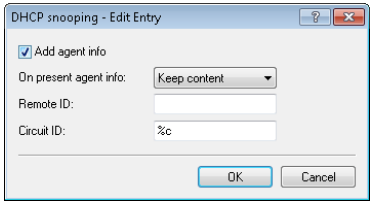
6.7.1 AP-specific login to a central Public Spot

A central WLC manages a Public Spot in a distributed infrastructure. Accordingly, the configuration of the Public Spot (Public Spot SSID, security standards) is identical on all of the participating APs. This allows a Public Spot provider to offer an identical Public Spot at all of the different locations.

After receiving a voucher, customers would have access to this Public Spot at any branch. In order to limit access to the branch where the customer has received the voucher, the AP transmits its own identifier in addition to the user name and password. This identifier enables the voucher to be associated with this AP. To transfer the identifier, the AP attaches the circuit ID (DHCP option 82) to the DHCP requests. These DHCP packets pass through the central Public Spot, which checks the identifier based on the entries in the RADIUS user table.

The Public Spot only allows a request if the voucher in the RADIUS user table is associated with this AP. Customers who have received a voucher at branch A cannot login to the same Public Spot at branch B, since the two APs transmit different identifiers.

The AP identifier is configured as the circuit ID for the corresponding interface under **Interfaces** > **Snooping** > **DHCP snooping**.

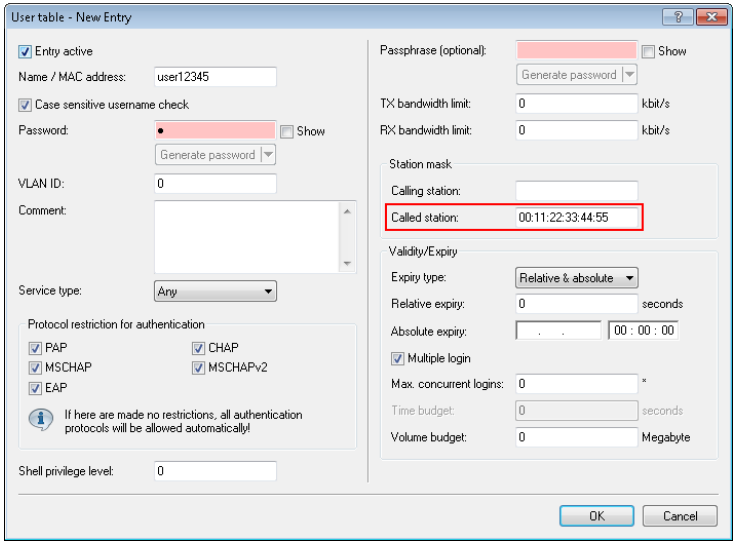


You can use the following variables:

- **%%**: Inserts a percent sign.
- **%c**: Inserts the MAC address of the interface used by the Public Spot user to authenticate. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- **%c**: Inserts the name of the interface used by the Public Spot user to authenticate.
- **%n**: Inserts the name of the AP as specified under **Management** > **General**.
- **%v**: Inserts the VLAN ID of the DHCP request packet. This VLAN ID is sourced either from the VLAN header of the DHCP packet or from the VLAN ID mapping for this interface.
- **%p**: Inserts the name of the Ethernet interface that received the DHCP packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, **%p** and **%i** are identical.

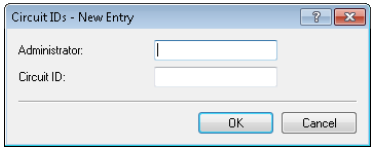
- **%s**: Inserts the WLAN SSID if a WLAN client is used for the authentication. For other clients, this variable contains an empty string.
- **%e**: Inserts the serial number of the AP, to be found for example under **Management** > **General**.

On the WLC, you configure this identifier in the RADIUS user table under **RADIUS server** > **General** > **User table**.



As the “Called station”, you add the ID of the AP that should enable access by means of the corresponding voucher.

When setting up new Public Spot users, the Public Spot Setup Wizard automatically uses the ID of the device if this is configured under **Public Spot** > **Wizard** > **Circuit IDs**.



When you create a new Public Spot account, the setup wizard checks to see whether this table contains an entry for the logged-in **administrator**. If this is the case, the setup wizard inserts the **circuit ID** into the RADIUS user table as the “called station”.

6.7.2 Additions to the Setup menu

Circuit-IDs

When a user authenticates at a Public Spot, the circuit ID configured in this table is an additional identifier sent by the AP to the WLC along with the user name and password.

When you create a new Public Spot account, the Public Spot setup wizard checks to see whether this table contains an entry for the logged-in administrator. If this is the case, the setup wizard inserts the circuit ID into the RADIUS user table as the “called station”.

SNMP ID:

2.24.48

Telnet path:

Setup > **Public Spot**

Administrator

Contains the name of the administrator who is entitled to assign this circuit ID.

SNMP ID:

2.24.48.1

Telnet path:

Setup > **Public-Spot** > **Circuit-IDs**

Possible values:

Max. 16 characters from
`[A-Z][a-z][0-9]@{|}~!$%&'()+-,/;<=>?[\]^_.`

Default:

empty

Circuit ID

Contains the circuit ID sent by the AP to the WLC as an additional identifier along with the user name and password when a user authenticates at a Public Spot.

SNMP ID:

2.24.48.2

Telnet path:

Setup > **Public-Spot** > **Circuit-IDs**

Possible values:

Max. 64 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

6.8 Additions to the Status menu

6.8.1 Max. no. users

This entry indicates the maximum number of users that may be authenticated with the Public Spot at the same time.

SNMP ID:

1.44.11

Telnet path:

Status > **Public-Spot**

6.8.2 PbSpot authenticated users

This entry displays the number of Public Spot users who are currently authenticated via the Public Spot itself.

SNMP ID:

1.44.12

Telnet path:

Status > **Public-Spot**

6.8.3 PMS authenticated users

This entry displays the number of Public Spot users who are currently authenticated via the PMS interface.

SNMP ID:

1.44.13

Telnet path:

Status > **Public-Spot**

6.8.4 Local configured users

This entry indicates how many Public Spot users are currently setup locally on the device.

SNMP ID:

1.44.14

Telnet path:

Status > **Public-Spot**

6.9 Additions to the Setup menu

6.9.1 Password input set

This setting specifies the character set used by the **Create Public Spot Account** wizard to create passwords for new users.

SNMP ID:

2.24.19.18

Telnet path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

Character+digits
Characters
Digits

6.9.2 Hide CSV export

This parameter determines whether or not to display the button for exporting information to a CSV file in the Wizard for creating new Public Spot accounts.

SNMP ID:

2.24.19.19

Telnet path:

Setup > **Public-Spot-Module** > **Add-User-Wizard**

Possible values:

No
Yes

Default:

No

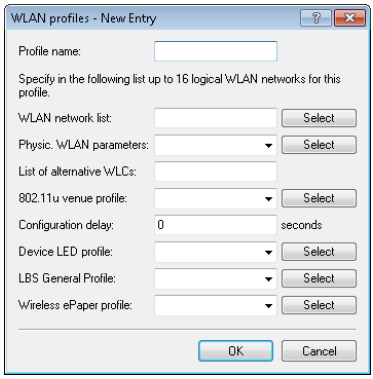
7 WLAN

7.1 Upgrade to 16 SSIDs per WLAN module

As of HiLCOS version 9.10 IEEE 802.11n WLAN modules support up to 16 SSIDs and IEEE 802.11ac WLAN modules support 15 SSIDs.

WLCs with the HiLCOS version 9.10 manage up to 16 SSIDs per AP profile.

For each WLAN profile you can specify the following parameters under **WLAN controller** > **Profiles** > **WLAN profiles**:



7.2 Wildcards for MAC address and SSID filters

As of HiLCOS version 9.10 wildcards (* and ?) can be used to specify MAC addresses. You can also restrict access by WLAN clients to specific SSIDs.

Note: In WEBconfig, the new station list replaces the previous station list under **Setup** > **WLAN** > **Access-list** (APs) or **Setup** > **WLAN-management** > **Access-list** (WLCs).

When updating to the new version, HiLCOS takes the available values from the existing station list.

This parameter ...	*...causes the following message in the trace:*
WLAN-ACL	Status messages about MAC filtering rules. **Note:** The display depends on how the WLAN data trace is configured. If a MAC address is specified there, the trace shows only the filter results relating to that specific MAC address.

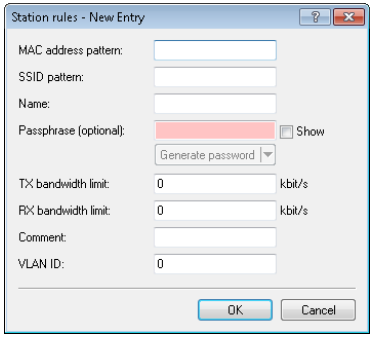
Table 7: Overview of all possible traces

7.2.1 Access-control list

With the **A**ccess **C**ontrol **L**ist (ACL) you can permit or prevent individual WLAN clients accessing your WLAN. The decision is based on the MAC address that is permanently programmed into WLAN adapters.

Note: If you are centrally managing your and Hirschmann APs with a WLC, you will find the station table under **WLAN controller** > **Stations** under the button **Stations**.

Check under **Wireless LAN** > **Stations** to see if the setting **Filter out data from the listed stations, transfer all other** is activated. New stations to be included in your wireless network are added with the button **Stations**.



MAC address pattern

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address

A MAC address in the format `00a057112233`, `00-a0-57-11-22-33` or `00:a0:57:11:22:33`.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. `00a057*`, `00-a0-57-11-??-??` or `00:a0:??:11:*`.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

Note: It is possible to use wildcards.

SSID pattern

WLAN clients with the corresponding MAC addresses have access that is limited to this SSID.

Note: The use of wildcards makes it possible to allow access to multiple SSIDs.

Name

You can enter any name you wish and a comment for any WLAN client. This enables you to assign MAC addresses more easily to specific stations or users.

Passphrase

Here you may enter a separate passphrase for each physical address (MAC address) that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

TX bandwidth limit

Transmission-bandwidth restriction for WLAN clients currently authenticating themselves. A WLAN device in client mode communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

RX bandwidth limit

Reception-bandwidth restriction for WLAN clients currently authenticating themselves. A WLAN device in client mode communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

Note: The RX bandwidth restriction is only active for WLAN devices in client mode. For value is not used by normal WLAN clients.

VLAN-ID

This VLAN ID is assigned to packets that are received from the client with the MAC address entered here. In case of VLAN-ID '0', the station is not assigned a specific VLAN ID. Instead, the VLAN ID of the radio cell (SSID) applies.

If filter rules contradict, the individual rule has a higher priority: A rule without wildcards in the MAC address or SSID takes precedence over a rule with wildcards. When creating these entries, the user should ensure that filter rules do not contradict. The definitions in the filters can be checked in a Telnet session with the trace command `trace WLAN-ACL`.

Important: The filter criteria in the station list either allow or deny WLAN clients to access your wireless network. The entries **Name**, **Bandwidth limit**, **VLAN ID** and **Passphrase** are meaningless if the device uses valid filter criteria to deny access to the WLAN.

7.2.2 Additions to the Setup menu

Access rules

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

SNMP ID:

2.12.89

Telnet path:

Setup > **WLAN**

MAC address pattern

Enter the MAC address of a station.

Note: It is possible to use wildcards.

SNMP ID:

2.12.89.1

Telnet path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 20 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Possible arguments:

MAC address

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address

A MAC address in the format `00a057112233`, `00-a0-57-11-22-33` or `00:a0:57:11:22:33`.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. `00a057*`, `00-a0-57-11-??-??` or `00:a0:??:11:*`.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

Note: It is possible to use wildcards.

Name

You can enter any name you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

SNMP ID:

2.12.89.2

Telnet path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 32 characters from

`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Comment

You can enter any comment you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

SNMP ID:

2.12.89.3

Telnet path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 30 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

WPA passphrase

Here you may enter a separate passphrase for each entry that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

Important: The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

Note: This field has no significance for networks secured by WEP.

SNMP ID:

2.12.89.4

Telnet path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 63 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Tx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

Note: The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

SNMP ID:

2.12.89.5

Telnet path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 9 characters from `0123456789`

0 … 999999999

Default:

0

Special values:

0

No limit

Rx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

Note: The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

SNMP ID:

2.12.89.6

Telnet path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 9 characters from `0123456789`

0 … 999999999

Default:

0

Special values:

0

No limit

VLAN-ID

The device assigns this VLAN ID to packets received by the WLAN client and containing the MAC address entered here.

SNMP ID:

2.12.89.7

Telnet path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 4 characters from `0123456789`

0 … 4096

Default:

0

Special values:

0

No limit

SSID pattern

For WLAN clients with the appropriate MAC addresses, this entry allows them to access this SSID or it restricts them to it.

Note: The use of wildcards makes it possible to allow access to multiple SSIDs.

SNMP ID:

2.12.89.9

Telnet path:

Setup > **WLAN** > **Access rules**

Possible values:

Max. 40 characters from

`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Special values:

*****

Placeholder for any number of characters

?

Placeholder for exactly one character

Default:

empty

Access rules

You can limit the data traffic between the wireless LAN and its local network by excluding certain stations from transferring data, or you can approve specific stations only.

SNMP ID:

2.37.21

Telnet path:

Setup > **WLAN-Management**

MAC address pattern

Enter the MAC address of a station.

Note: It is possible to use wildcards.

SNMP ID:

2.37.21.1

Telnet path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 20 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Possible arguments:

MAC address

MAC address of the WLAN client for this entry. The following entries are possible:

Individual MAC address

A MAC address in the format `00a057112233`, `00-a0-57-11-22-33` or `00:a0:57:11:22:33`.

Wildcards

The wildcards '*' and '?' uses to specify MAC address ranges, e.g. `00a057*`, `00-a0-57-11-??-??` or `00:a0:??:11:*`.

Vendor ID

The device contains a list of the major manufacturer OUIs (organizationally unique identifier). The MAC address range is valid if this entry matches the first three bytes of the MAC address of the WLAN client.

Note: It is possible to use wildcards.

Name

You can enter any name you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

SNMP ID:

2.37.21.2

Telnet path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 32 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Comment

You can enter any comment you wish for any station. This enables you to assign MAC addresses more easily to specific stations or users.

SNMP ID:

2.37.21.3

Telnet path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 30 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

WPA passphrase

Here you may enter a separate passphrase for each entry that is used in a 802.11i/WPA/AES-PSK-secured network. If no separate passphrase is specified for this MAC address, the passphrases stored in the **802.11i/WEP** area will be used for each logical wireless LAN network.

Important: The passphrases should consist of a random string at least 22 characters long, corresponding to a cryptographic strength of 128 bits.

Note: This field has no significance for networks secured by WEP.

SNMP ID:

2.37.21.4

Telnet path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 63 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Tx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

Note: The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

SNMP ID:

2.37.21.5

Telnet path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 9 characters from `0123456789`

0 … 999999999

Default:

0

Special values:

0

No limit

Rx-Limit

Bandwidth restriction for registering WLAN clients. A client communicates its setting to the AP when logging on. This then uses uses these two values to set the minimum bandwidth.

Note: The significance of the Rx and Tx values depends on the device's operating mode. In this case, as an AP Rx stands for "Send data" and Tx stands for "Receive data".

SNMP ID:

2.37.21.6

Telnet path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 9 characters from `0123456789`

0 … 999999999

Default:

0

Special values:

0

No limit

VLAN-ID

The device assigns this VLAN ID to packets received by the WLAN client and containing the MAC address entered here.

SNMP ID:

2.37.21.7

Telnet path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 4 characters from `0123456789`

0 … 4096

Default:

0

Special values:

0

No limit

SSID pattern

For WLAN clients with the appropriate MAC addresses, this entry allows them to access this SSID or it restricts them to it.

Note: The use of wildcards makes it possible to allow access to multiple SSIDs.

SNMP ID:

2.37.21.9

Telnet path:

Setup > **WLAN-Management** > **Access rules**

Possible values:

Max. 40 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Special values:

*****

Placeholder for any number of characters

?

Placeholder for exactly one character

Default:

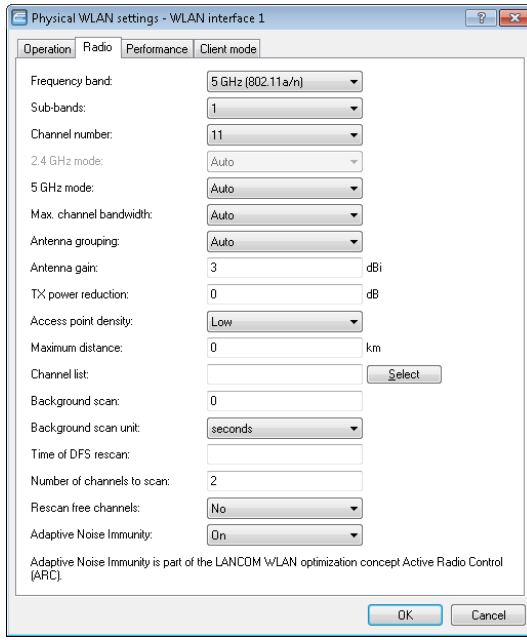
empty

7.3 Conformity with current ETSI radio standards in the 2.4GHz/5GHz bands

As of HiLCOS version 9.10, the AP additionally supports the radio standards ETSI EN 300328-V1.7.1, ETSI EN 300328-V1.8.1 and ETSI EN 301893-V1.7.1.

7.3.1 DFS configuration

In LANconfig you access the DFS settings under **Wireless LAN** > **General**, then click **Physical WLAN settings** and select the **Radio** tab.



Time of DFS rescan

This entry determines at what time (0 - 24h) the device deletes the DFS database and performs a DFS rescan. If this item is left empty, the device only performs a DFS rescan when no further free channel is available. This is the case when the number of channels determined during the initial DFS scan falls below the minimum number of free channels.

Tip: The cron command options can be used to define the time: The entry '1,6,13' starts the rescan at 01:00h, 06:00h and 13:00h. The entry ' 0-23/4 ' starts a rescan every four hours between 00:00h and 23:00h.

Number of channels to scan

This entry determines the minimum number of free channels that a DFS scan has to achieve. The default value of '2' means that the device performs a DFS scan for as long as it takes to detect 2 free channels. If the device has to switch channels, for example if it detects an active radar pattern, the second channel is immediately available for the change.

For value '0' the best available free channel is automatically selected. If no free channel is available, a DFS scan will be performed first.

Rescan free channels

With this item you select whether, following the completion of a DFS rescan, the physical WLAN interface deletes occupied channels or saves them for subsequent DFS rescans.

- **Yes:** The physical WLAN interface deletes occupied channels after completing a DFS rescan so that they are available again for a new DFS rescan.
- **No**: The device saves occupied channels after completing a DFS rescan and so that the device immediately skips them during a new DFS rescan.

7.3.2 Additions to the Setup menu

Preferred DFS scheme

In order to operate the WLAN device in accordance with current ETSI radio standards, select the corresponding standard here.

Note: When upgrading a HiLCOS version to a current radio standard, the previous setting is retained.

SNMP ID:

2.23.20.8.20

Telnet path:

Setup > **Interfaces** > **WLAN** > **Radio settings** > **Preferred DFS scheme**

Possible values:

EN 301 893-V1.3
EN 301 893-V1.5
EN 301 893-V1.6
EN 301 893-V1.7

Default:
EN 301 893-V1.7

Preferred 2.4 scheme

This parameter sets the version of the EN 300 328 standard operated by the device in the 2.4-GHz band.

Note: Should you carry out a firmware update, the current version is retained. New devices and devices subject to a configuration reset operate version 1.8 by default.

SNMP ID:
2.23.20.8.28

Telnet path:
Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:
EN300328-V1.7
EN300328-V1.8

Default:
EN300328-V1.8

7.4 Time of the DFS rescan configurable via LANconfig

As of HiLCOS version 9.10, the time for a DFS rescan can be configured in LANconfig.

7.5 Bandwidth limit for each WLAN client per SSID

As of HiLCOS version 9.10, a general bandwidth limit can be applied to all WLAN clients in each SSID.

Client TX bandwidth limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of `0` disables the limit.

Client RX bandwidth limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of `0` disables the limit.

7.5.1 Additions to the Setup menu

Per-Client-Tx-Limit

Here, you set the transmit-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

SNMP ID:

2.23.20.1.23

Telnet path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

Max. 10 characters from `0123456789`

Default:

0

Special values:

0

Disables the limit.

Per-Client-Rx-Limit

Here, you set the receive-direction bandwidth limit (in kbps) available to each wireless client on this SSID. A value of 0 disables the limit.

SNMP ID:

2.23.20.1.24

Telnet path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

Max. 10 characters from `0123456789`

Default:

0

Special values:

0

Disables the limit.

7.6 Opportunistic key caching (OKC) adjustable on the client side

As of HiLCOS version 9.10, the OKC can also be adjusted for devices in client mode.

7.6.1 Additions to the Setup menu

OKC

This option enables or disables the opportunistic key caching (OKC).

The device uses this value only if the interface works in client mode. The interface is in AP mode, the enabling or disabling of OKC is only possible by means of profile management with a WLC.

In the PMK caching status under **Status** > **WLAN** > **PMK-Caching** > **Contents**, OKC PMKs can be identified by the authenticator address `ff:ff:ff:ff:ff:n`, where `n` is the assigned profile number (e.g. `0` for “WLAN-1”, `1` for “WLAN1-2”, etc.).

SNMP ID:

2.23.20.3.17

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

Yes
No

Default:

Yes

7.7 Counter for WPA login attempts

As of HiLCOS version 9.10, the device stores the number of successful and failed WPA login attempts on each interface.

7.7.1 Additions to the Status menu

Ports

This table provides an overview of the accepted or rejected connection requests for each logical interface.

SNMP ID:

1.46.3

Telnet path:

Status > **IEEE802.1x**

Port

Displays the name of the interface.

SNMP ID:

1.46.3.1

Telnet path:

Status > **IEEE802.1x** > **Ports**

Num-accept

Displays the number of successful WPA requests on this interface.

SNMP ID:

1.46.3.2

Telnet path:

Status > **IEEE802.1x** > **Ports**

Num-reject

Displays the number of failed WPA requests on this interface.

SNMP ID:

1.46.3.3

Telnet path:

Status > **IEEE802.1x** > **Ports**

WPA-PSK-Num-Wrong-Passphrase

Displays the number of WPA requests on this interface that were rejected due to an incorrect passphrase.

SNMP ID:

1.3.64.20

Telnet path:

Status > **WLAN** > **Encryption**

WPA-PSK-Num-Success

Displays the number of successful WPA requests on this interface.

SNMP ID:

1.3.64.21

Telnet path:

Status > **WLAN** > **Encryption**

WPA-PSK-Num-Failures

Displays the number of failed WPA requests on this interface.

SNMP ID:

1.3.64.22

Telnet path:

Status > **WLAN** > **Encryption**

7.8 Wireless IDS

The implementation of WLAN within industrial networks introduces a new class of threats to network security. Radio signals penetrate walls and may reach much further than required. This presents new opportunities for unauthorized users to disrupt the network.

Hirschmann is aware of these threats and supports users through their Wireless Intrusion Detection System (Wireless IDS) by detecting and averting such attacks. Typical attacks on a WLAN network have characteristic patterns.

7.8.1 Wireless IDS counter

The Wireless Intrusion Detection System provides APs with the ability to detect potential intrusion attacks and provide warnings to the network management software when the attack activities exceed the corresponding user-defined threshold value/interval. By setting a counter to "0", attack detection is disabled.

The default threshold values are guideline values which may or may not be suitable for your particular application. The threshold values for your application depend on the environmental conditions of your AP. For this reason you should carry out an initial reference measurement with a trial run of the Wireless IDS at the location of your WLAN.

Additional reference values can be collected by capturing data with a free program such as Wireshark. In many countries authorization from the regulatory authority is required for intercepting radio transmission and for saving and processing data gained from this. Unauthorized recording, storing as well as forwarding of data is subject to a penalty in many countries.

Frame counter	**Threshold value factory setting**	**Time interval factory setting (1 interval corresponds to 1 second)**
EAPOL Start	250	10
Broadcast probe	500	10
Broadcast disassociation	2	1
Broadcast deauthentication	2	1
Deauthentication	250	10
Association request	250	10
Reassociation request	250	10
Authentication request	250	10
Disassociation request	250	10
Out of window	200	5
BA session	100	5
Null data (null-data DoS attack)	500	5
Data (null-data PS attack)	200	5

Frame counter	Threshold value factory setting	Time interval factory setting (1 interval corresponds to 1 second)
Listen interval difference	5	n/a
PS poll	100	5
Multi-stream data	100	5
No-Ack-MS-Data	100	5

7.8.2 Wireless IDS Types of Attack

Attacks on a WLAN can be characterized by the following properties:

- the target of the attack (AP or client)
- how many targets the attack contained (one or several)
- the type of attack

Some attacks are virtually impossible to avoid as they exploit mechanisms which by their design enable the WLAN to be constructed in the first place. These attacks, which are virtually impossible to prevent, include, e. g., disruption of radio transmission using an interference source.

Types of attack:

- Denial-of-service attacks (DoS) aim to shutdown a service.
- Man-in-the-middle attacks (MitM) aim to intervene between 2 subscribers. Under certain conditions the attacker is then able to intercept radio transmission of both subscribers involved and manipulate the data exchanged.
- SSID attacks (SSID) aim to detect a disabled SSID. A disabled SSID improves safety by means of concealment.

Name of attack	*Target of attack (AP, client, other)*	*Number of targets (one or several)*	*Types of attacks*
EAPOL Start	Other (infrastructure)	one	DoS
Broadcast probe	AP	one	DoS
Broadcast disassociation	Client	several	DoS, MitM, SSID
Broadcast deauthentication	Client	several	DoS, MitM, SSID
Deauthentication	Client	one	DoS, SSID

Name of attack	*Target of attack (AP, client, other)*	*Number of targets (one or several)*	*Types of attacks*
Association request	Client	one	DoS
Reassociation request	Client	one	DoS
Authentication request	Client	one	DoS
Disassociation request	Client	one	DoS
Block-Ack DoS attack	AP, client	one	DoS
Null-data DoS attack	AP	one	DoS
Null-data PS attack	Client	one	DoS
PS-poll attack	Client	one	DoS
Spatial multiplexing PS attack	Client	one	DoS

Table 8: Type of attack on WLAN

EAPOL Start (Extensible Authentication Protocol over LAN)

If an AP receives an EAPOL-Start frame, it starts the identification process and allocates internal resources to the new client. An attacker generating a large number of EAPOL Start frames will exhaust the internal resources of the AP and overload the RADIUS server.

Broadcast probe

An attacker continually sends probe requests to the network. Put simply, probe requests are frames used by clients to ask: “Is there a WLAN here?" Probe responses are sent by the APs in reply, saying: “Yes, there's a WLAN here with [SSID]”. This is a mechanism for discovering WLAN services in WLAN networks. If the attacker sends sufficient probe requests, they will overload the AP and the wireless medium will be flooded with probe responses.

Broadcast disassociation

An attacker broadcasts a spoof disassociation frame on the network. Clients that receive the frame will be disassociated, so that they need to re-associate with the AP. The disassociation frames are unprotected and sent in clear text, which makes it easy to conduct this type of attack. Data communication between the AP and the clients is not possible until the clients re-associate.

Broadcast deauthentication

An attacker broadcasts a spoof deauthentication frame on the network. Clients that receive the frame will be deauthenticated and re-authentication to the AP is required. The deauthentication frames are unprotected and sent in clear text, which makes it easy to conduct this type of attack. Data communication between the AP and the clients is not possible until the clients reauthenticate.

Deauthentication

An attacker continually sends spoof deauthentication frames from the client to an AP. Similarly, the client will be deauthenticated and data communication will be terminated until the client reassociates to the AP.

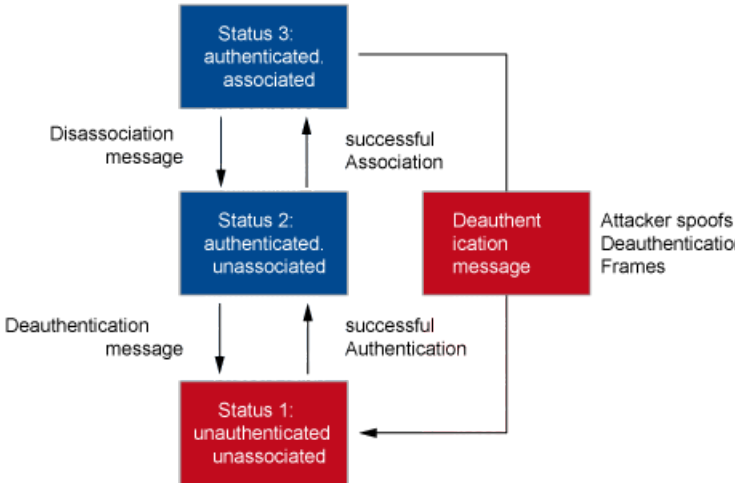


Figure 1: Behavior of a Client during Deauthentication

Association request

An attacker continually sends association frames to the AP. This overloads the AP's association table.

Reassociation request

An attacker continually sends re-association frames to the AP with the aim of overloading the association table of the AP. Re-association frames in large numbers can also be an indication of attacks on clients, which then try to connect to the AP again.

Authentication request

An attacker continually sends authentication frames to the AP. This overloads the AP's authentication table.

Disassociation request

An attacker spoofs disassociation frames in order to log off a client from the AP. All clients affected then attempt to reassociate with the AP. No data communication is possible until the clients reassociate.

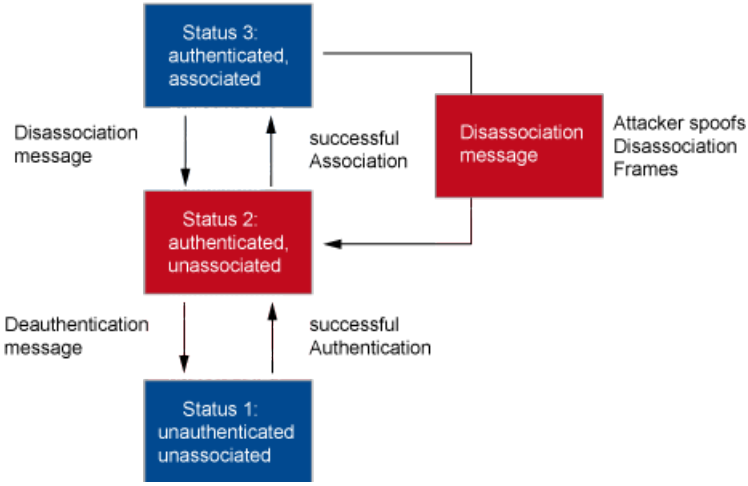


Figure 2: Behavior of a Client during disassociation

Block-Ack DoS attack

An attacker spoofs the MAC address of the client and is able to conduct the following attacks:

- During the setup phase of a block-ACK session, the attacker sends an ADDBA frame with a manipulated starting sequence number to the AP. In this way, the attacker causes the AP to discard legitimate frames.
- The attacker sends manipulated A-MPDU frames, which overload of the re-ordering buffer on the AP.
- The attacker stops the block-ACK session with a fake DELBA frame from the client to the AP, resulting in the loss of buffered frames on the AP. An attack with manipulated DELBA frames can also reduce throughput, because the client is forced to re-establish the block-ACK session.

Null-data DoS attack

If a client is inactive for a long period, the AP is unable to decide whether the client is switched off or merely outside of the radio cell. One consequence could be for the AP to deauthenticate the client. To prevent accidental deauthentication, the client sends null-data frames to the AP after a period of inactivity in order to keep the session alive. The AP then acknowledges the receipt of the null-data frame.

An attacker can take advantage of this scenario in the following way: The attacker sends large numbers of null-data frames to the AP. Because the AP is forced to acknowledge the receipt of every individual null-data frame, the bandwidth on the radio channel is reduced to such an extent that legitimate client requests are discarded.

Null-data PS attack

A client can use null-data frames to inform the AP that it is entering into the sleep mode. In this case, the AP buffers the packets that arrive for the client in sleep mode, and it informs the client that packets are buffered at the AP by using the TIM field of beacon frames. Upon receipt of beacon frames that have the corresponding TIM bit set, the client uses a PS-poll frame to request the packets from the buffer of the AP.

An attacker can take advantage of this scenario in the following way: The attacker spoofs the MAC address of the client and sends the AP a fake notification about going into sleep mode. The AP now buffers the incoming packets for the client and these packets will be dropped after a certain timeout. This continues as long as the client does not send a PS-poll frame. Because in reality the client is not in the sleep mode at all, it will not send a PS-poll frame to request buffered packets from the AP. This leads to the loss of the packets addressed to the client.

PS-poll attack

The attacker spoofs the MAC address of the client in sleep mode and sends fake PS-poll frames to the AP in order to request the buffered packets. The attacker now retrieves the packets that were intended for the client.

Spatial multiplexing PS attack

The use of multiple antennas on the same transmission channel enhances data throughput and improves the signal coverage. The operation of multiple antennas is energy intensive, so in times of low data throughput a client switches into static spatial multiplexing power save mode (SM power save mode) and just one antenna remains active. The client uses SM-power-save-

action frames to inform the AP about a change into SM power save mode or the end of the SM power save mode.

An attacker can take advantage of this scenario in the following way:

- The attacker spoofs the MAC address of a client with multiple active antennas and uses a fake SM-power-save-action frame to inform the AP that it is going into the static SM power save mode. The AP then communicates with the client over a single spatial stream, which significantly reduces the throughput.
- The attacker spoofs the MAC address of a client in static SM power save mode with just one active antenna and uses a fake SM-power-save-action frame to inform the AP that it is ending its static SM power save mode. The AP then communicates with the client via multiple spatial streams, which the client is not able to receive using only one active antenna.

7.8.3 Wireless IDS intruder identification

Wireless IDS intruder identification enables you to gain the following information about potential attackers:

- MAC address
- Attack type
- Current activity
- RSSI value (received signal strength)
- Attack rate
- Identification of the attacker as a known client
- DHCP requests from the attacker, which can be stored to a ring buffer and downloaded via WEBconfig as a .pcap file at the following location:

  File management > **Download certificate or file** > **File type** > **WIDS – Intruder Identification Packet Capture (*.pcap)**

The information collected about potential attackers is to be found in WEBconfig under **HiLCOS menu tree** > **Status** > **WLAN** > **Wireless-IDS** > **Intruder-Table**.

You can exclude certain stations from intruder identification by entering them into in a white list. This is useful, for example, if the administrator is aware that a trusted station has been mistakenly identified as an attacker.

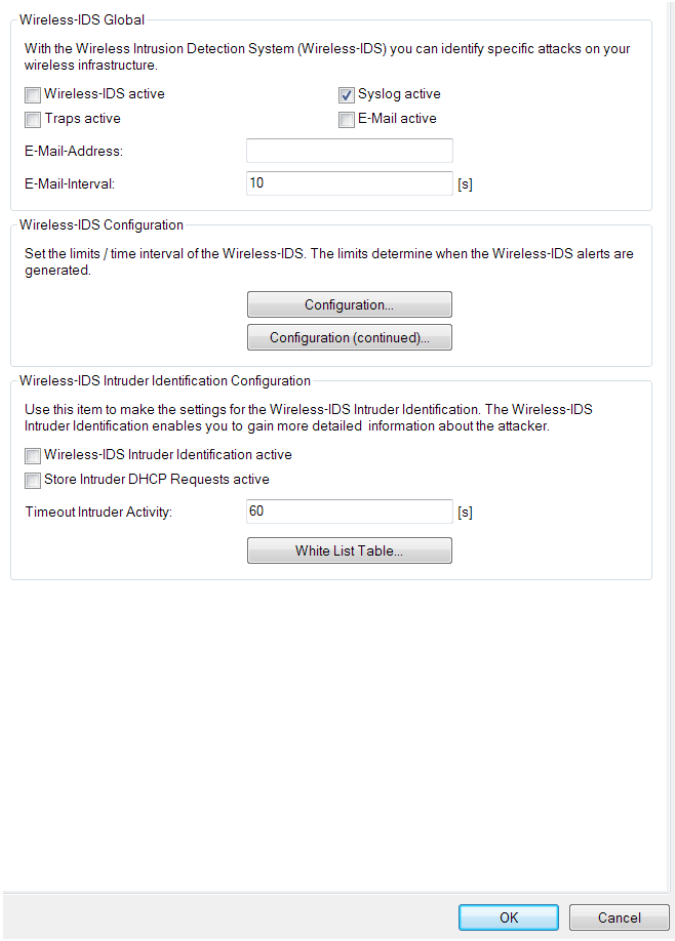
7.8.4 Tutorial: Configuring Wireless IDS

The default threshold values are guideline values which may or may not be suitable for your particular application. The threshold values for your application depend on the environmental conditions of your AP. For this reason you should carry out an initial reference measurement with a trial run of the Wireless IDS at the location of your WLAN.

Additional reference values can be collected by capturing data with a free program such as Wireshark. In many countries authorization from the regulatory authority is required for intercepting radio transmission and for saving and processing data gained from this. Unauthorized recording, storing as well as forwarding of data is subject to a penalty in many countries.

To activate and configure the Wireless IDS proceed as follows:

1. Open the view **Wireless LAN** > **Wireless-IDS.**



2. Enable the option **Wireless-IDS active**.
3. Choose the required logging method: By default, Wireless IDS logs to the **syslog**. In order to log Wireless IDS traps, enable the option **Traps active**.
4. In order to receive e-mail notifications, enable the option **E-mail active** and enter the relevant e-mail address.

   Note: In order to successfully send access credentials as an e-mail, you must set up a valid SMTP account under **Log & Trace** > **SMTP account** and **Log & Trace** > **SMTP options**.

5. Set the threshold values for the frames and intervals according to your reference measurement.
6. In order to gain information about the attackers, enable the option **Wireless-IDS intruder identification active**.
7. In order to gain information about the intruder DHCP requests, enable the option **Store intruder DHCP requests active**.
8. Set a value for the **Timeout intruder activity**.
9. To exclude any stations from the intruder identification, add them to the **White list table**.
10. Click the **OK** button.

You have activated and configured Wireless IDS.

7.9 C2C coupling

Wireless C2C coupling enables you to connect APs by means of point-to-point links without having to preconfigure the MAC address or AP name in order to identify the partner AP. Connections are established between the P2P partners that are separated by the shortest distance. The wireless identification of the P2P partner in train carriages has the following advantages over a cabled solution:

- The serial bridging cable that was previously required for establishing the P2P connection between the two devices in the train carriages is now unnecessary.
- No more problems caused by stolen bridging cables, for example.

In the case of C2C coupling, the P2P partner is not detected on the basis of its MAC address but instead by a C2C identifier. The C2C coupling function offers 2 modes of operation:

- Automatic: The APs start searching for P2P partners automatically. P2P partners with same C2C identifier automatically establish a P2P link. If several partners have same C2C identifier, the connection is established to the closest partner.
- Manual: The APs start and stop the search for P2P partners via the CLI or the serial C2C interface protocol. The corresponding commands are

issued by a control unit (one for each AP), which also assigns the C2C identifiers to the APs.

Note:

Encrypt the P2P link according to your needs. The settings for the encryption over a P2P link are to be found in chapter 6.3.1 Configuration of P2P connections under "Addendum HiLCOS 9.00" on page 39.

7.9.1 Programming the C2C interface protocol

The APs must be able to decode the serial packets used to control the C2C-coupling function. The outband port of the APs can still be used as a configuration interface. Detection of the controller unit (master) happens as follows:

1. Set the serial port to the specified bitrate and disable handshaking.
2. Send STX characters with a bit rate of at least 10 characters per second for a period of approx. 0.5 sec.
3. If at least 3 STX characters were received over the 0.5 sec., it is safe to assume that the control unit is ready to communicate via the C2C interface protocol.
4. Now an exclusive registration of the outband ports of the APs is carried out, and the C2C interface protocol starts.

The communication packets are enclosed by the following ASCII control characters: STX (start of text) and ETX (end of text). The AP discards the data outside of this frame. Data fields are separated by a colon. The receiver checks for forward and backward packets and discards any with code violations.

Forward packet

A forward packet is structured as follows:

```
<STX>:<WLANn>:<CMD>:<LENGTH>:<DATA>:<CRC><ETX>
```

WLANn	Specification of the WLAN identifier as n = 1, 2, 3,...
CMD	1 byte of data "XXXX XXXX" contains the relevant commands

LENGTH	1 byte of data "XXXX XXXX" contains the length of the data field
DATA	255 octets or less contain data in accordance with the commands
CRC	CRC-32 check of the fields CMD, LENGTH and DATA (starting with the first character after STX to the last character of the value) expressed as a decimal

Backward packet

A backward packet is returned after a command was received and is structured as follows:

```
<STX><DATA>:<CRC><ETX>
```

DATA Depending on the command (= response), 1 byte of data "XXXX XXXX" contains either a "Yes", "No", or 8-bit information:

- "Yes": 1111 1111
- "No": The AP should not respond
- 8 bit information: XXXX XXXX

CRC CRC-32 check of the fields CMD, LENGTH and DATA (starting with the first character after STX to the last character of the value) expressed as a decimal

Definition of the control command

Command 0: 0x00 "OFF"

Stops the C2C-coupling function on the selected WLAN and deletes the stored C2C identifier.

Example:

```
<STX>:<WLAN1>:<0x00>:<0x00>:CRC><ETX>
```

Command 1: 0x01 "START"

Starts the C2C-coupling function on the selected WLAN and creates the C2C identifier. The "START" command is sent when the compilation of the train changes or after the "OFF"command.

Example:

```
<STX>:<WLAN1>:<0x01>:<0x07>:<UId2015>:<CRC><ETX>
```

Command 2: 0x02 "SCHEDOFF"

The C2C-coupling function is switched off after the specified timeout "C2C_OFF_TIMEOUT" (max. 600 seconds). While the timeout is running, bit 5 of the status register displays "OFFTIMERRUN". If the C2C-coupling function is already switched off, no further change takes place.

Example:

```
<STX>:<WLAN1>:<0x02>:<0x03>:<600>:<CRC><ETX>
```

Commands 3-15

Reserved for future applications. The AP does not respond to these commands.

Definition of the query command

Command 16: 0x10 "STATUS"

The responses in the "STATUS INFORMATION" byte are defined as follows:

- Bit 0 "1" = ACTIVE (the C2C coupling engine is running.)
- Bit 1 "1" = DISCOVERY (the C2C coupling engine is in search mode.)
- Bit 3 "1" = CONNECTED (the P2P link of the AP is enabled.)
- Bit 4 "1" = CONNLOST (The connection to the P2P partner is lost.)
- Bit 5 "1" = OFFTIMERRUN (the timeout is running.)

The AP regularly updates the "STATUS INFORMATION" according to the current circumstances.

Example:

```
<STX>:<WLAN1>:<0x10>:<0x00>:<CRC><ETX>
```

Overview of the commands

Command number	*Command code*	*Command name*
0	0x00	OFF
1	0x01	START
2	0x02	SCHEDOFF
3-15	-	RESERVED
16	0x10	STATUS

7.9.2 Troubleshooting

This section helps you to identify possible causes for any errors during C2C coupling and to take corrective measures.

Troubleshooting the operating mode "Automatic"

Error	*Possible cause*	*Troubleshooting*
C2C coupling cannot be established	Poor WLAN connection during the coupling procedure	**1.** Are both antennas correctly aligned? **2.** Is there a direct line of sight between the antennas?
	Connection to the other AP cannot be established	**1.** Check the quality of the WLAN connection. Are both antennas correctly aligned? Is there a direct line of sight between the antennas? **2.** Is the P2P link correctly configured? **3.** Is the connection establishment threshold value set too high?
	No power supply to the AP	Check the power supply of the AP.
C2C coupling restarts repeatedly	Connection quality thresholds not suitable	Check the settings for the connection establishment threshold and the connection hold threshold.

Error	*Possible cause*	*Troubleshooting*
C2C coupling to a new carriage is not possible	Connection loss not detected	Set a suitable value for the connection hold threshold. A loss of connection is detected only when the signal-to-noise ratio for the current P2P partner is less than the specified connection hold threshold.
Data connection to the wrong carriage	C2C coupling to the wrong carriage	Set a suitable connection establishment threshold so as to prevent coupling attempts to carriages that are too far away.
Connection to the other AP cannot be established	Misconfigured P2P link	Check the configuration of the P2P link.
	Connection establishment threshold value set too high	Set a suitable value for the connection establishment threshold.
	Poor WLAN connection	**1.** Are both antennas correctly aligned? **2.** Is there a direct line of sight between the antennas?

Troubleshooting the operating mode "Manual"

Error	*Possible cause*	*Troubleshooting*
C2C coupling cannot be established	Defective control unit	Check that the control unit is functioning properly.
	Defective serial connection	Check cable and connectors of the serial connection.
	The AP does not connect to the control unit during the coupling procedure	Check the serial connection between the control unit and the AP: **1.** Parameters of the serial connection OK? **2.** Test connection by means of STATUS command successful?
	Incorrect commands received during the coupling procedure	**1.** Check cable and connectors of the serial connection. **2.** Check whether the commands sent by the control unit before the coupling procedure comply with the specification.

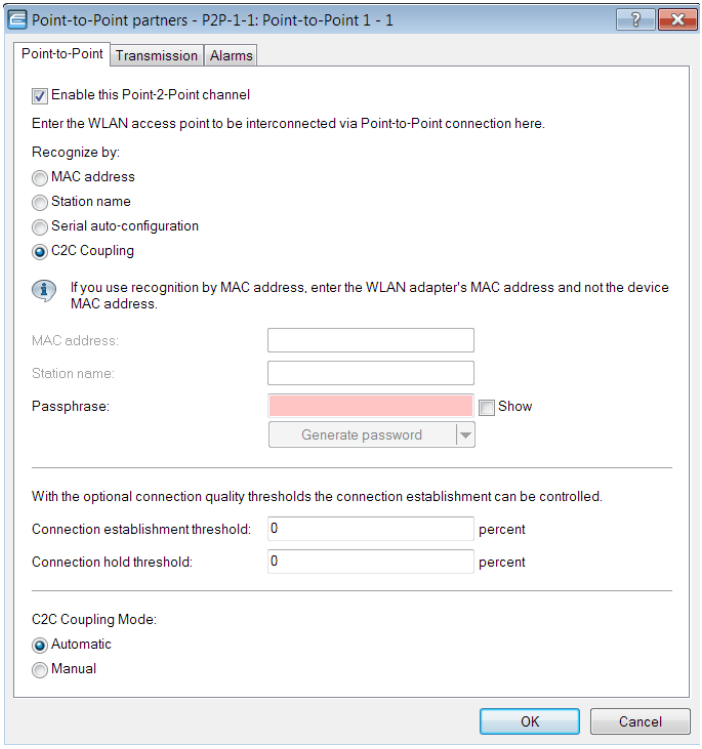
Error	*Possible cause*	*Troubleshooting*
	Coupling procedure starts too late at one of the APs	Check that the control units are sending the coupling trigger synchronously.
	Poor WLAN connection during the coupling procedure	**1.** Are both antennas correctly aligned? **2.** Is there a direct line of sight between the antennas?
	Connection to the other AP cannot be established	**1.** Check the quality of the WLAN connection. Are both antennas correctly aligned? Is there a direct line of sight between the antennas? **2.** Is the P2P link correctly configured? **3.** Is the connection establishment threshold value set too high?
	No power supply to the AP	Check the power supply of the AP.
C2C coupling temporarily out of service	Incorrect commands received after a successful coupling procedure	Check whether the commands sent by the control unit after the coupling procedure comply with the specification.
	Connection loss not detected	Set a suitable value for the connection hold threshold. A loss of connection is detected only when the signal-to-noise ratio for the current P2P partner is less than the specified connection hold threshold.
C2C coupling aborts	No power supply to the AP	Check the power supply of the AP.
Connection to the other AP cannot be established	Misconfigured P2P link	Check the configuration of the P2P link.
	Connection establishment threshold value set too high	Set a suitable value for the connection establishment threshold.
	Poor WLAN connection	**1.** Are both antennas correctly aligned? **2.** Is there a direct line of sight between the antennas?

7.9.3 Tutorial: Configuring the C2C coupling function

Proceed as follows to enable and configure C2C coupling:

1. Open the view **Wireless LAN** > **General** > **Point-to-point partners**.
2. Select a point-to-point partner, for example P2P-1-1.

   Note: The C2C-coupling function supports the following P2P connections: P2P-1-1 and P2P-2-1.

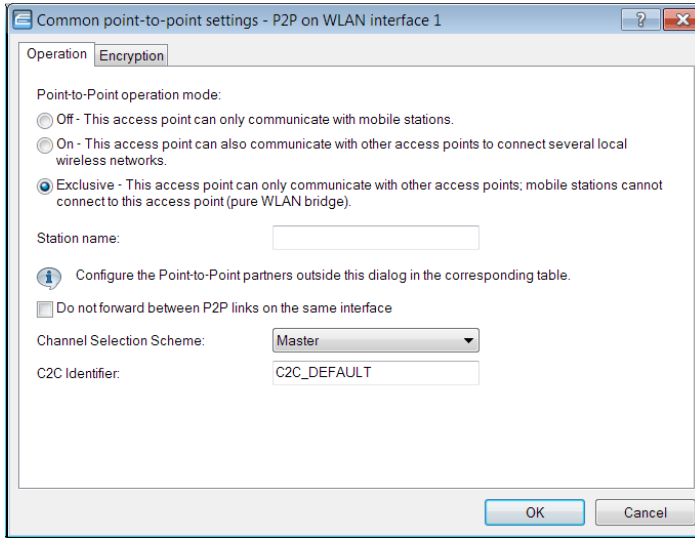


3. On the **Point-to-point** tab, activate the option **Enable this point-2-point channel**.
4. Select the recognition of the P2P partner by **C2C coupling**.
5. Enter the **passphrase**.
6. Set the operating mode of the C2C coupling to **Automatic** or **Manual**.

7. Set the values for the optional connection quality thresholds.
   - **Connection establishment threshold**: This value specifies the signal strength (in percent) that a P2P partner has to show as a minimum in order for an AP to attempt to associate with this P2P partner.
   - **Connection hold threshold**: This threshold specifies the minimum signal strength (in percent) that the current P2P partner needs to have in order for the connection to be considered intact.

   Note: The connection establishment threshold allows you to limit the distance within which P2P partners are searched for. By default the connection quality thresholds are switched off (values set to 0%). You will need to determine the values depending on your specific use case.

8. Click the **OK** button.
9. Navigate to the view **Wireless LAN** > **General** > **Common point-to-point settings**.
10. Select a common point-to-point setting, for example "P2P on WLAN interface 1".



11. On the **Operation** tab, activate the point-to-point operation mode **Exclusive**.

12. Set the **Channel selection scheme** to the option **Master**.
13. Enter the intended name for the C2C identifier into the field **C2C identifier**. The purpose of the C2C identifier in the context of C2C coupling is to identify the P2P partner. The default setting is "C2C_DEFAULT".
14. Click the **OK** button.
15. On the **Operation** tab, activate the option **Encryption enabled**.
16. Click the **OK** button.

You have enabled and configured the C2C coupling function.

7.10 WLAN link status log

The WLAN link status log enables you to capture and monitor information about the quality of the WLAN links. P2P links and AP-client links are monitored. Monitoring starts when the WLAN link is activated. The information about the WLAN link quality is written to the WLAN link status log at specific time intervals as set by the user. Monitoring of disabled WLAN links stops after a time interval specified by the user. Any existing entries are retained. The information from the WLAN link status logs is available from a device log table, from a USB memory stick, from syslog entries, or via SNMP traps.

During operations you can view the information on the quality of the WLAN links via WEBconfig under **HiLCOS menu tree** > **Status** > **WLAN** > **WLAN-Link-Status-Log**:

- **Audit**

  This table provides current information about the quality of the WLAN links and is updated constantly.

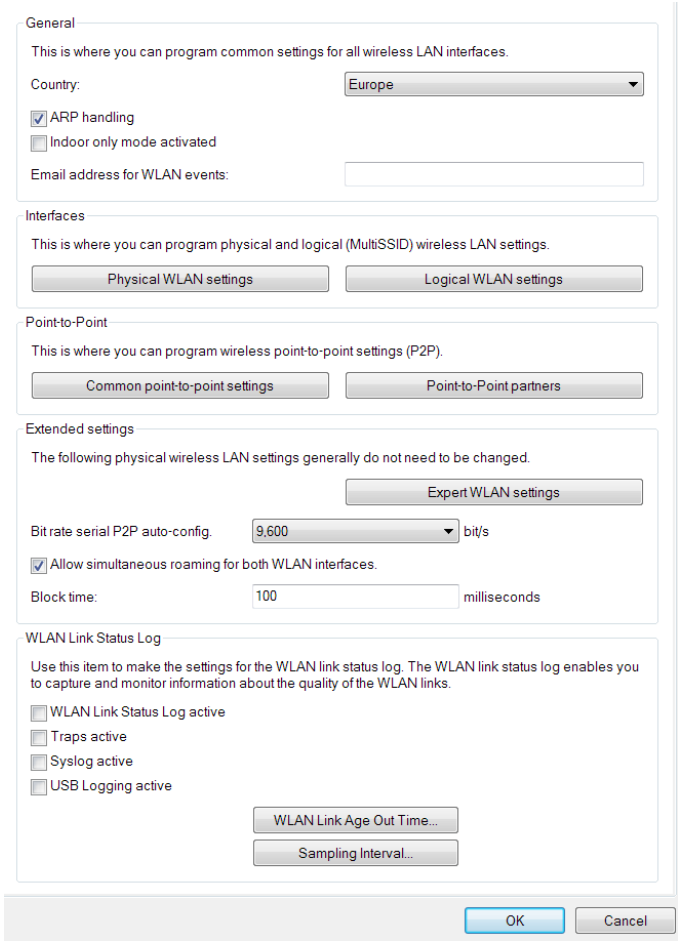
- **Log table**

  This table provides information stored about the quality of the WLAN links at the configured interval.

7.10.1 Tutorial: Configuring the WLAN link status log

To activate and configure the WLAN link status log, proceed as follows:

1. Open the view **Wireless LAN** > **General**.



2. In the **WLAN link status log** section, select the option **WLAN link status log active**.
3. Select the required form of notification (multiple selections are possible) by enabling the options **Traps active**, **Syslog active** or **USB logging active** accordingly.

Note: For further information on configuring syslog, please see chapter 6.12.4 Setting up an external SYSLOG server under "User Manual" on page 612.

Note: Traps generated by the option **Traps active** and all other traps generated by the device are sent to all of the manually configured trap recipients.

4. You set the time interval for storing information about the quality of WLAN links in the dialog **Sampling interval**.
5. You set the time interval after which the monitoring of an inactive WLAN link is stopped in the dialog **WLAN link age out time**.
6. Click **OK**.

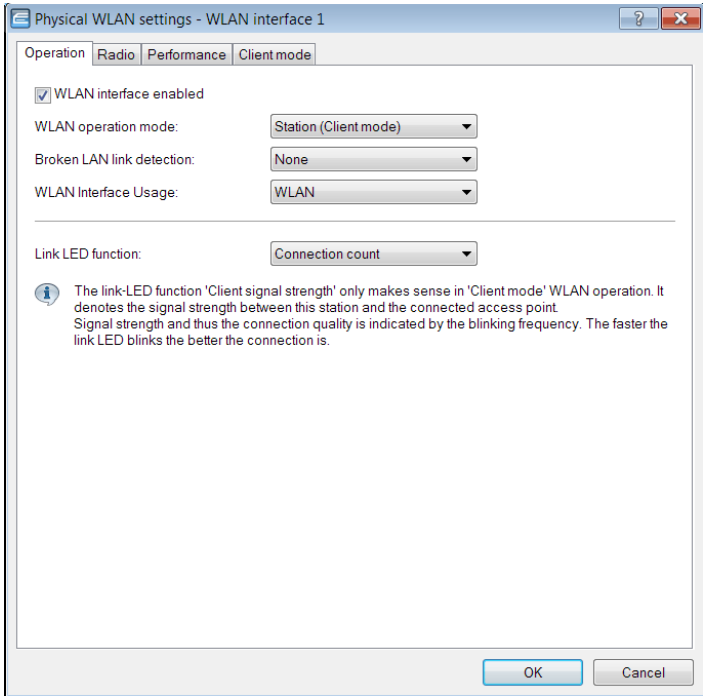
You have activated and configured the WLAN link status log.

7.11 Tutorial: N:N mapping via the WLAN interface

For detailed information about use cases and configuring the N:N mapping, see chapter 11.8 N:N Mapping under "User Manual" on page 87.

Proceed as follows to enable the function N:N mapping via the WLAN interface:

1. Open the view **Wireless LAN** > **General** > **Interfaces** > **Physical WLAN settings**.
2. Select an interface, for example the WLAN interface 1.



3. On the **Operation** tab, activate the option **WLAN interface enabled**.
4. Under **WLAN operating mode** select the option **Station (Client mode)**.
5. Under **WLAN interface usage** select the option **DSL**.
6. Click the **OK** button.

The N:N mapping function is now enabled.

7.12 Additions to the Setup menu

7.12.1 Channel change delay

Here you specify how long an access point, which has detected a radar, waits until it changes to a different channel.

SNMP ID:

2.12.130.9

Telnet path:

Setup > **WLAN** > **DFS**

Possible values:

Max. 3 characters from `[0-9]`

Default:

0

Special values:

0

The value 0 disables this function.

7.13 Additions to the Status menu

7.13.1 Delete values

SNMP ID:

1.46.99

Telnet path:

Status > **IEEE802.1x**

8 WLAN management

8.1 AutoWDS operation

8.1.1 Additions to the Status menu

CAPWAP up

Indicates whether CAPWAP is active.

SNMP ID:

1.59.109.2

Telnet path:

Status > **WLAN Management** > **AutoWDS-operation**

Possible values:

No
Yes

CAPWAP up again after config

Indicates whether CAPWAP is active again after a successful configuration.

SNMP ID:

1.59.109.3

Telnet path:

Status > **WLAN Management** > **AutoWDS-operation**

Possible values:

No
Yes

AutoWDS fallback timer

Displays the value of the AutoWDS fallback timer.

SNMP ID:

1.59.109.4

Telnet path:

Status > **WLAN Management** > **AutoWDS-operation**

AutoWDS fallback force deassoc timer

Displays the value of the AutoWDS force deassoc timer.

SNMP ID:

1.59.109.5

Telnet path:

Status > **WLAN Management** > **AutoWDS-operation**

CAPWAP continuation timer

Displays the value of the CAPWAP continuation timer.

SNMP ID:

1.59.109.6

Telnet path:

Status > **WLAN Management** > **AutoWDS-operation**

CAPWAP silent timer

Displays the value of the CAPWAP silent timer.

SNMP ID:

1.59.109.7

Telnet path:

Status > **WLAN Management** > **AutoWDS-operation**

8.2 Wireless-IDS – detecting attacks on your wireless infrastructure

For further information on the subject "Wireless-IDS", refer to the section *Wireless IDS* on page 145.

8.2.1 Tutorial: Configuring Wireless-IDS with the WLAN controller

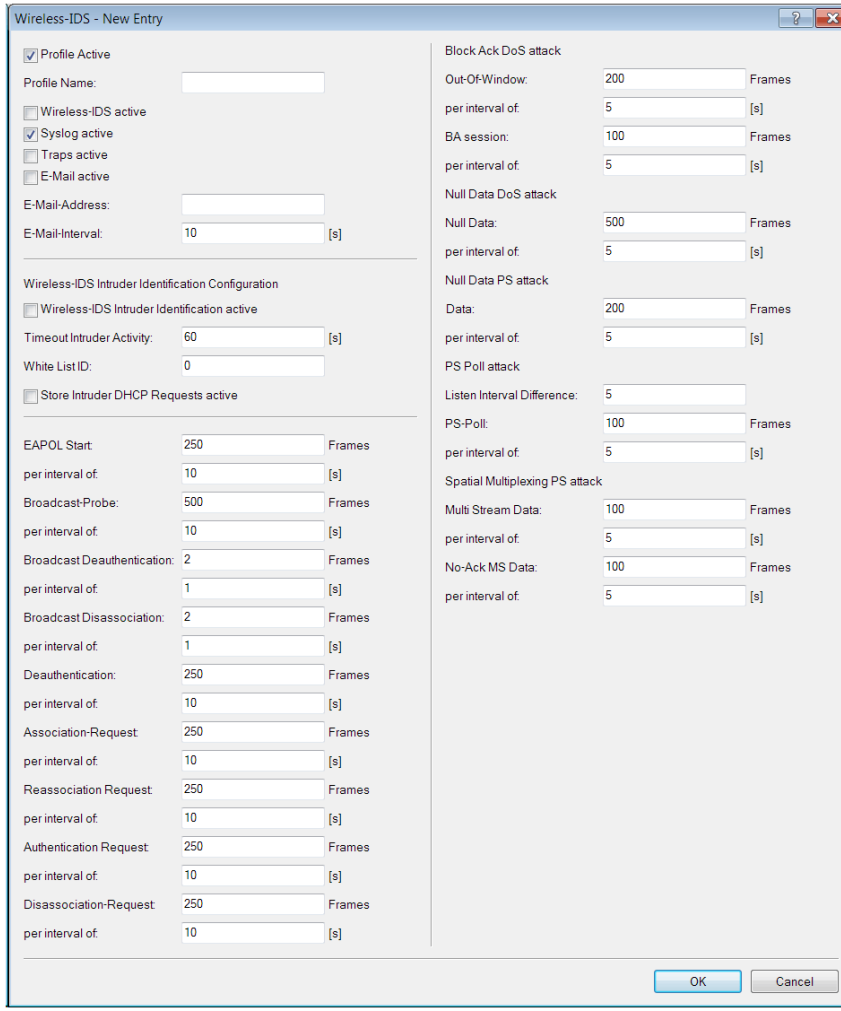
The default threshold values are guideline values which may or may not be suitable for your particular application. The threshold values for your application

depend on the environmental conditions of your AP. For this reason you should carry out an initial reference measurement with a trial run of the Wireless IDS at the location of your WLAN.

Additional reference values can be collected by capturing data with a free program such as Wireshark. In many countries authorization from the regulatory authority is required for intercepting radio transmission and for saving and processing data gained from this. Unauthorized recording, storing as well as forwarding of data is subject to a penalty in many countries.

To activate and configure the Wireless IDS with the WLAN controller, proceed as follows:

1. Open the view **WLAN Controller** > **Profiles** > **Wireless-IDS** > **Add**.



2. Specify a name for the Wireless-IDS profile under **Profile name**.
3. Enable the option **Wireless-IDS active**.

Note: Enabling Wireless IDS via the WLC causes local Wireless IDS configurations on the APs to be overwritten. Attempts to configure Wireless IDS directly on APs that are managed by the WLC are discarded and they produce an error message.

4. Choose the required logging method: By default, Wireless IDS logs to the **syslog**. In order to log Wireless IDS traps, enable the option **Traps active**.

   Note: It is not possible to specify settings for SNMP traps directly on the WLC. Instead, these are rolled out to the APs by means of an additional script. Please see chapter 5.7.2 Central firmware and script management under "User Manual" on page 365 for further information about scripts.

5. In order to receive e-mail notifications, enable the option **E-mail active** and enter the relevant e-mail address.

   Note: It is not possible to specify settings for the required SMTP account directly on the WLC. Instead, these are rolled out to the APs by means of an additional script. Please see chapter 5.7.2 Central firmware and script management under "User Manual" on page 365 for further information about scripts.

6. In order to gain information about the attackers, enable the option **Wireless-IDS intruder identification active**.

   Note: Enabling Wireless IDS intruder identification via the WLC causes local Wireless IDS intruder identification configurations on the APs to be overwritten. Attempts to configure Wireless IDS intruder identification directly on APs that are managed by the WLC are discarded and they produce an error message.

7. Set a value for the **Timeout intruder activity**.
8. To exclude stations from the intruder identification, create a **white list ID** for the Wireless IDS profile.
9. In order to gain information about the intruder DHCP requests, enable the option **Store intruder DHCP requests active**.
10. Set the threshold values for the frames and intervals according to your reference measurement.
11. Click the **OK** button.
12. To exclude stations from the intruder identification, switch to the view **WLAN controller** > **Profiles** > **White list table** and add an entry for each

station. Group the excluded stations by means of their white-list ID (see item 8 of this tutorial) in white lists for the relevant Wireless IDS profile.

13. Navigate to the view **WLAN controller** > **Profiles** > **WLAN profiles**.
14. Add the **Wireless-IDS profile** to the corresponding WLAN profile.
15. Click the **OK** button.

You have activated and configured Wireless IDS.

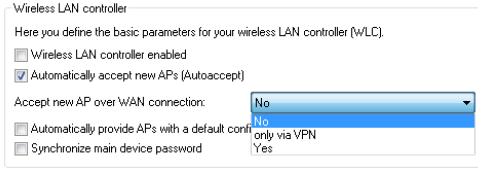
8.3 Disable responses to CAPWAP requests from a WAN connection

As of HiLCOS version 9.10 it is possible to disable responses to CAPWAP requests from a WAN remote station.

8.3.1 Protection against unauthorized CAPWAP access from the WAN

The WLC or handles CAPWAP requests from the LAN and the WAN in the same way. In the case of requests from WAN remote stations, it accepts the APs into its AP management and, under certain circumstances, it sends a default configuration. If configured appropriately, the CAPWAP service is no longer available to WAN remote stations, meaning that for WAN remote stations, APs are no longer accepted and configurations are not provisioned.

The configuration is done under **WLAN Controller** > **General** in the section **Wireless LAN controller**. If the automatic acceptance of new APs is enabled, you can use the feature **Accept new AP over WAN connection** to control whether the CAPWAP service is available to WAN remote stations.



No

The device accepts no new APs over the WAN connection.

Only via VPN

The device only accepts new APs if the WAN connection is via VPN.

Yes

The device accepts all new APs over the WAN connection.

8.3.2 Additions to the Setup menu

Allow WAN connections

This item configures the way that the WLC handles requests from the WAN. For example, it is desirable to prevent CAPWAP requests from unknown WAN peers from accidentally assigning a default configuration with internal network settings to these APs.

SNMP ID:

2.37.29

Telnet path:

Setup > **WLAN-Management**

Possible values:

Yes

When an AP sends a request from the WAN, the WLC includes it into the AP management and, with the appropriate setting, it sends a default configuration.

VPN

When an AP sends a request from the WAN, the WLC includes it into the AP management and, with the appropriate setting, it sends a default configuration only if the WAN connection uses a VPN tunnel.

No

When an AP sends a request from the WAN, the WLC does not include it into the AP management.

Default:

No

8.4 Additional date information for central firmware management

As of HiLCOS version 9.10, the table for central firmware management by the WLC now contains date information.

8.4.1 Firmware management table

This table is used to store information about which firmware versions are to be operated with which devices (MAC address) and device types.

Device types

Select here the type of device that the firmware version specified here is to be used for.

- Possible values: All or a selection from the list of available devices.
- Default: All

MAC address

Select here the device (identified by its MAC address) that the firmware version specified here is to be used for.

- Possible values: Valid MAC address
- Default: Blank

Version

Firmware version that is to be used for the devices or device types specified here.

- Possible values: Firmware version in the form `X.XX`
- Default: Blank

Date

The date allows you to downgrade to a specific firmware version within a release, for example from a Release Upgrade (RU) on an earlier upgrade.

- Possible values: 8 characters from 0123456789 The entry must match the format of the UPX header, e.g. "01092014" for the September 01, 2014.

- Default: Blank

8.4.2 Additions to the Setup menu

Date

Date of the corresponding firmware version.

SNMP ID:

2.37.27.15.5

Telnet path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Firmware-Version-Management**

Possible values:

Max. 8 characters from `[0-9]`

Default:

Corresponds to the UPX header of the firmware (such as "01072014" for the July 01, 2014)

8.5 Display of channel and frequency of clients logged on to the AP

As of HiLCOS version 9.10, the station table in the WLC additionally displays the channel and frequency of clients logged on to active WLAN networks.

Note: For APs with an older firmware version and unable to transmit this data, the WLC takes the channel and frequency information from the **Active radios** status table under **Status** > **Active-Radios** > **WLAN-Management** > **AP-Status**.

8.5.1 Additions to the Status menu

Radio band

This value displays the radio band used by the client that is logged in to the AP.

SNMP ID:

1.73.100.27

Telnet path:

Status > **WLAN-Management** > **Station-table**

Possible values:

0

Unknown

2.4GHz

The client is using the 2.4GHz band.

5GHz

The client is using the 5GHz band.

Radio channel

This value displays the radio channel used by the client that is logged in to the AP.

SNMP ID:

1.73.100.28

Telnet path:

Status > **WLAN-Management** > **Station-table**

Possible values:

1 … 140

8.6 Using LANconfig to backup certificates

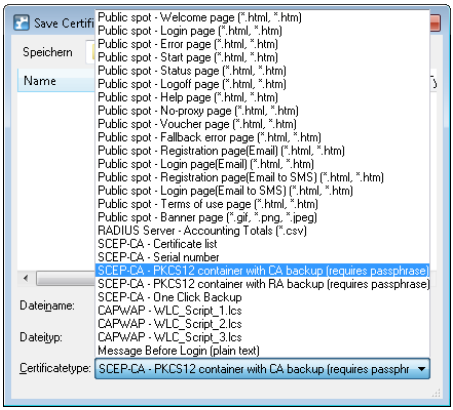
As of HiLCOS version 9.10, LANconfig is fully able to backup and upload certificates.

8.6.1 Using LANconfig to backup and restore certificates

Certificates are stored and uploaded with LANconfig as follows:

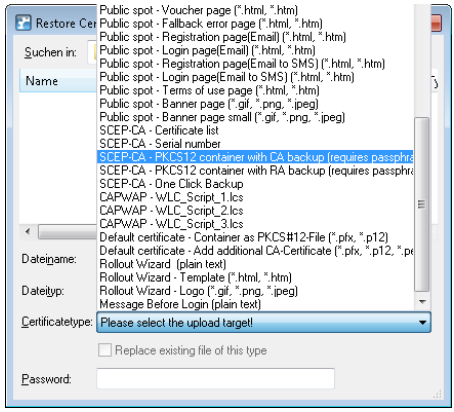
Save

1. Highlight the WLC in the device view section and in the menu select **Device** > **Configuration management** and the item **Save certificate as file**.
2. Set the **Certificate type** to PKCS12 container and click **Save**.



Upload

1. Highlight the WLC in the device view section and in the menu select **Device** > **Configuration management** and the item **Upload certificate or file**.
2. Set the **Certificate type** to PKCS12 container.
3. Now navigate to the desired file, enter the password if necessary and click **Open**.



One Click Backup

For the One Click Backup, select the entry "SCEP-CA - One Click Backup" from the dialog list.

8.7 Displaying the certificate status of an AP

As of HiLCOS version 9.10, an AP transmits its certificate status to the WLC.

8.7.1 Additions to the Status menu

Certificate status

Displays the status of the APs.

SNMP ID:

1.73.9.3.9

Telnet path:

Status > **WLAN-Management** > **AP-Status** > **New-AP**

Possible values:

0

Unknown (default for APs with older firmware)

1

Missing

2

Expired

3

Incompatible (certificate does not match the CA chain of the WLC)

4

Still not valid (e.g. if clocks in the WLC and AP are not synchronized)

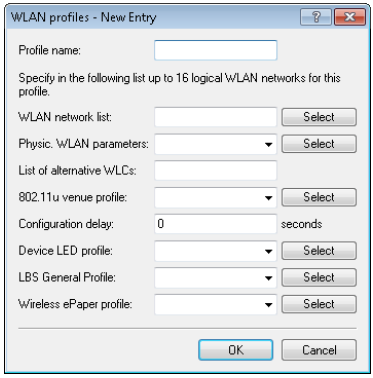
5

Valid

8.8 On/off switch for AP LEDs per WLC

As of HiLCOS version 9.10, the device LEDs of every AP in a multi-AP environments an be separately configured on a WLC.

For each WLAN profile you can specify the following parameters under **WLAN controller** > **Profiles** > **WLAN profiles**:

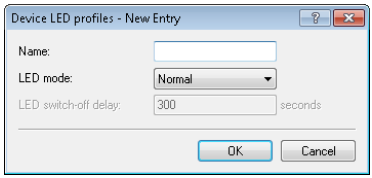


Device LED profile

The device LED profile selected here applies to the WLAN profile. To manage the devices LED profiles, see **WLAN controller** > **Profiles** > **Device LED profiles**.

8.8.1 Device LED profiles

The LEDs on the device are configurable so that you can, for instance, operate an AP while drawing a minimum of attention to it. In order to perform this configuration by WLC, you need to create the corresponding profile under **WLAN Controller** > **Profiles** > **Device LED profiles** and assign this to a WLAN profile.



Name

Give a name to the device LED profile here.

LED mode

The following options are available:

- **Normal**: The LEDs are always enabled, also after rebooting the device.
- **Timed off**: After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.
- **All off**: The LEDs are all off. Even after restarting the device, the LEDs remain off.

LED switch-off delay

The **Timed off** option uses the setting in the field **LED switch-off delay** in seconds to control the time before the LEDs are disabled after a restart.

8.8.2 Additions to the Setup menu

LED profiles

The LEDs on the device are configurable so that you can, for instance, operate an AP while drawing a minimum of attention to it. In order to perform this configuration by WLC, you need to create the corresponding profile and assign this to a WLAN profile.

SNMP ID:

2.37.1.21

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration**

Name

Give a name to the device LED profile here.

SNMP ID:

2.37.1.21.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LED-Profiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]`

Default:

empty

LED mode

Set the operating mode for the LEDs here.

SNMP ID:

2.37.1.21.4

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LED-Profiles**

Possible values:

On

The LEDs are always enabled, also after rebooting the device.

Off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

Default:

On

LED off seconds

In the operating mode **Timed off** you can specify the delay in seconds after which the LEDs are disabled following a restart. This is useful for the LEDs to indicate critical errors during the restart process.

SNMP ID:

2.37.1.21.5

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LED-Profiles**

Possible values:

Max. 4 characters from `[0-9]`

Default:

300

LED profiles

The device LED profile selected here applies to the WLAN profile.

SNMP ID:

2.37.1.3.8

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]`

Default:

empty

8.8.3 Additions to the Status menu

LED profiles

This entry displays the existing LED profiles.

SNMP ID:

1.59.110

Telnet path:

Status > **WLAN-Management**

LED profiles

Displays information about the LED profiles.

SNMP ID:

1.73.2.23

Telnet path:

Status > **WLAN-Management** > **AP-Configuration**

Name

Contains the name of the LED profile.

SNMP ID:

1.73.2.23.1

Telnet path:

Status > **WLAN-Management** > **LED-Profiles** >

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]`

Default:

empty

LED mode

Indicates the LED mode.

SNMP ID:

1.73.2.23.4

Telnet path:

Status > **WLAN-Management** > **LED-Profiles** >

Possible values:

On

The LEDs are always enabled, also after rebooting the device.

Off

The LEDs are all off. Even after restarting the device, the LEDs remain off.

Timed off

After a reboot, the LEDs are enabled for a certain period of time and are then turned off. This is useful for the LEDs to indicate critical errors during the restart process.

LED off seconds

In the operating mode **Timed off** this column indicates after how many seconds the device disables the LEDs after a restart.

SNMP ID:

1.73.2.23.5

Telnet path:

Status > **WLAN-Management** > **LED-Profiles** >

Possible values:

Max. 4 characters from `[0-9]`

Default:
300

LED profiles

This column indicates the assigned LED profile.

SNMP ID:
1.73.2.3.8

Telnet path:
Status > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:
Max. 31 characters from `[A-Z][a-z][0-9]`

Default:
empty

LED prof. errors

Contains the error codes displayed by the device LEDs.

SNMP ID:
1.73.2.22

Telnet path:
Status > **WLAN-Management** > **AP-Configuration**

Index

Contains the sequential index of the error messages.

SNMP ID:

1.73.2.22.1

Telnet path:

Status > **WLAN-Management** > **AP-Configuration** > **LED-Prof.-Errors**

Index

Contains the name of the LED profile.

SNMP ID:

1.73.2.22.2

Telnet path:

Status > **WLAN-Management** > **AP-Configuration** > **LED-Prof.-Errors**

Error

Contains the error that occurred.

SNMP ID:

1.73.2.22.3

Telnet path:

Status > **WLAN-Management** > **AP-Configuration** > **LED-Prof.-Errors**

Possible values:

None
No error

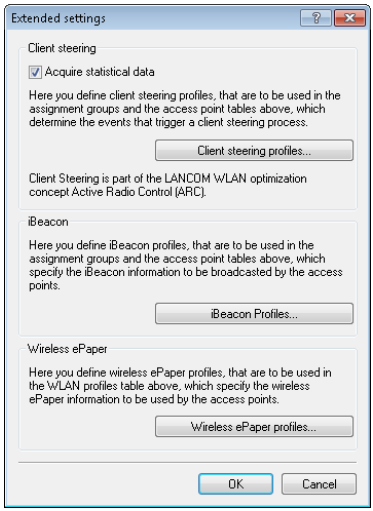
Inheritance error
No profile
Profile not found
No memory
SSID missing
Network not found
AP parameters not found
AP intranet not found
RADIUS profile not found
AutoWDS profile not found
Master equal to slave
No profile either Group found
Info profiles WINS group
Group wrong defined
SSID WLC tunnel missing
SSID inter-station traffic allowed
Too many networks for AutoWDS
Reported by AP

8.9 Managing Wireless-ePaper and iBeacon profiles with WLCs

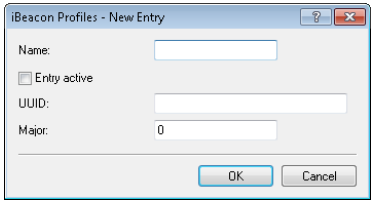
As of HiLCOS version 9.10, it is possible to create and distribute Wireless-ePaper and iBeacon profiles for E-series access points.

8.9.1 ESL- and iBeacon profiles

In order to use a WLC to manage the settings of the Wireless ePaper information and iBeacon information of the individual APs, you create the corresponding profiles for Wireless ePaper and iBeacon via **WLAN-Controller** > **AP-Configuration** with the button **Extended settings**.



The button **iBeacon profiles** is used to create iBeacon profiles for the assignment groups and the AP table, which specify the iBeacon information to be broadcast by the individual APs.



Name

Name of the profile

Entry active

Activates or deactivates this profile.

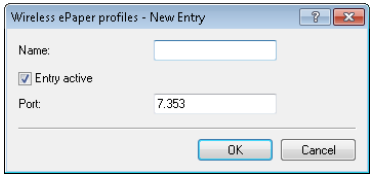
UUID

Unique identification of the transmitter

Major

Specifies the Major value of the iBeacon.

The button **Wireless ePaper profiles** is used to create Wireless ePaper profiles for the WLAN-profiles table, which specify the Wireless ePaper information to be broadcast by the individual APs.



Name
Name of the profile

Entry active
Activates or deactivates this profile.

Port
Specifies the port.

8.9.2 Additions to the Setup menu

iBeacon

This entry allows you to configure the iBeacon module.

SNMP ID:
2.23.90.1

Telnet path:
Setup > **Interfaces** > **Bluetooth**

UUID

This entry allows you to assign a "universally unique identifier" (UUID) to the iBeacon module.

SNMP ID:

2.23.90.1.2

Telnet path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Max. 36 characters from `[0-9][a-f][A-F]-`

Default:

00000000-0000-0000-0000-000000000000

Major

Assign a unique major ID to the iBeacon module.

SNMP ID:

2.23.90.1.3

Telnet path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Max. 5 characters from `[0-9]`

1 … 65535 Integer value

Default:

2002

Minor

Assign a unique minor ID to the iBeacon module.

SNMP ID:

2.23.90.1.4

Telnet path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Max. 5 characters from `[0-9]`

1 … 65535 Integer value

Default:

1001

Reception power shift

Specify the reception power shift.

SNMP ID:

2.23.90.1.5

Telnet path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Max. 4 characters from `[0-9]-`

-128 … 127

Default:

0

Transmission power

Set the transmission power of the iBeacon module.

SNMP ID:

2.23.90.1.6

Telnet path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Low

The module sends with minimum power.

Medium

The module sends with medium power.

High

The module sends with maximum power.

Default:

High

Channel/channels

Set which channels the iBeacon module should use to transmit.

SNMP ID:

2.23.90.1.7

Telnet path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

2402MHz

The module transmits on channel 2402.

2426MHz
The module transmits on channel 2426.

2480MHz
The module transmits on channel 2480.

2402MHz, 2426MHz, 2480MHz
The module transmits on all channels.

Default:
2402MHz, 2426MHz, 2480MHz

Coexistence

Specify here whether iBeacon is to be operated in parallel with the Wireless ePaper service.

SNMP ID:
2.23.90.1.8

Telnet path:
Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

No
Yes

Default:
Yes

Wireless ePaper

Configure the settings for the Wireless ePaper module here.

SNMP ID:
2.88

Telnet path:
Setup

Port

Assign a port to the Wireless ePaper module.

SNMP ID:
2.88.2

Telnet path:
Setup > **Wireless-ePaper**

Possible values:
Max. 5 characters from `[0-9]`

Default:
2002

Channel

Set which channel the Wireless ePaper module should use.

SNMP ID:
2.88.3

Telnet path:
Setup > **Wireless-ePaper**

Possible values:

2404MHz
2410MHz
2422MHz
2425MHz
2442MHz
2450MHz
2462MHz
2470MHz
2474MHz
2477MHz
2480MHz
Auto

Default:
2425MHz

8.10 The modules iBeacon and Wireless ePaper have an additional "Managed" mode

As of HiLCOS version 9.10 you can operate the iBeacon/BLE and Wireless ePaper modules in "Managed" mode.

Note: Existing configurations continue to run in the "Manual" mode and the corresponding module uses the local configuration. New configurations start in the "Managed" mode. In this case it is necessary for the configuration to be carried out by a WLAN controller.

8.10.1 Additions to the Setup menu

iBeacon

This entry allows you to configure the iBeacon module.

SNMP ID:

2.23.90.1

Telnet path:

Setup > **Interfaces** > **Bluetooth**

Operating

This entry allows you to set the operating mode of the module.

SNMP ID:

2.23.90.1.1

Telnet path:

Setup > **Interfaces** > **Bluetooth** > **iBeacon**

Possible values:

Off

The module is not enabled.

Manual

iBeacon configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Managed

Wireless ePaper

Configure the settings for the Wireless ePaper module here.

SNMP ID:

2.88

Telnet path:

Setup

Operating

This entry allows you to set the operating mode of the module.

SNMP ID:

2.88.1

Telnet path:

Setup > **Wireless-ePaper**

Possible values:

Off

The module is not enabled.

Manual

Wireless ePaper configurations are done manually.

Managed

The module is managed by a WLAN controller.

Default:

Manual

8.11 WLAN profiles divided into basic and advanced profiles

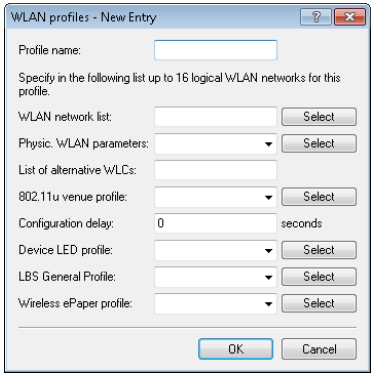
As of HiLCOS version 9.10, LANconfig can be used to configure advanced profiles of a WLC under **WLAN controller** > **Profiles**, for example to manage profiles for the location-based services (LBS).

8.12 General LBS profile and device location profile

As of HiLCOS version 9.10, you can create and map LBS servers and device location profiles for WLAN profiles on WLCs.

These profiles are mapped to WLAN profiles as follows:

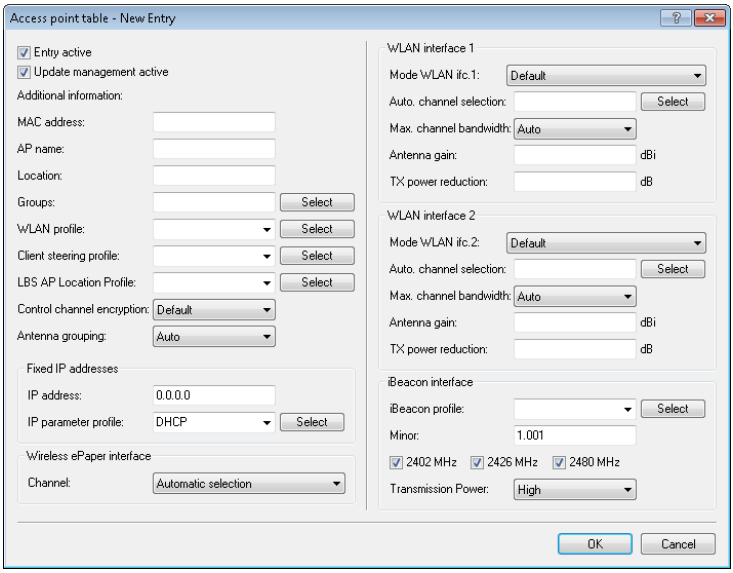
For each WLAN profile you can specify the following parameters under **WLAN controller** > **Profiles** > **WLAN profiles**:



LBS general profile

The general LBS profile selected here applies to the WLAN profile. You select the general LBS profile under **WLAN Controller** > **Profiles** > **Advanced profiles** with the button **LBS - General**.

The AP table is a central element of the configuration for WLCs. Here, the WLC assigns WLAN profiles (i.e. the combinations of logical and physical WLAN parameters) to the APs via their MAC addresses. Furthermore, the existence of an entry in the AP table for a specific AP affects its ability to connect to a WLC. Under **WLAN Controller** > **AP Configuration** > **Access Point Table** you can define the following parameters for each AP:

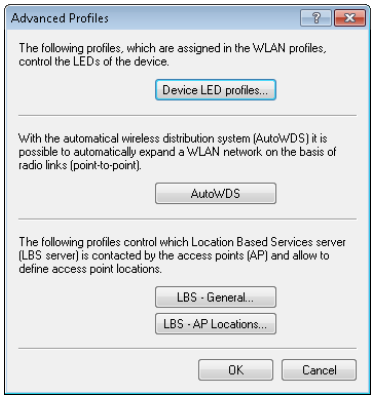


LBS AP location profile

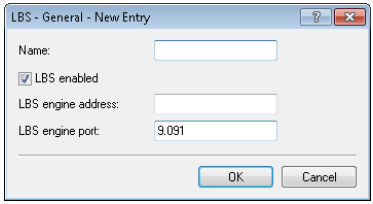
LBS location profile from the list of defined profiles.

8.12.1 General LBS profile and device location profile

In order to conveniently manage the settings for location-based services servers (LBS) and the AP locations by means of a WLC, you create the appropriate profiles for LBS servers and AP device locations via the menu **WLAN Controller** > **Profiles** and the button **Advanced profiles**.



The button **LBS - General** opens the dialog for creating a general LBS server profile.



Name

Enter a descriptive name for the profile.

LBS enabled

Enable or disable LBS.

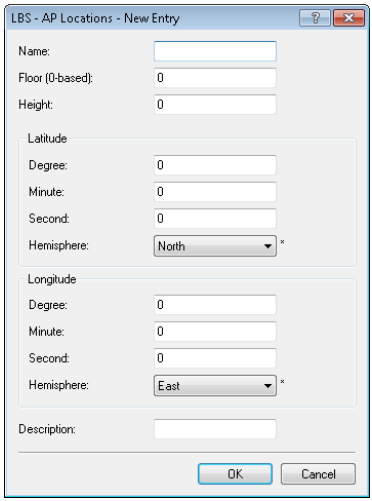
LBS server address

Enter the address of the LBS server.

LBS server port

Enter the port used by the LBS server (default: 9091).

The button **LBS - AP locations** opens the dialog for creating a location profile for the LBS APs.



Name

Enter a descriptive name for the profile.

Floor (0-based)

Here you enter the floor on which the device is located. This allows you to differentiate between the top floor and bottom floor, for example.

Height

Here you enter the height of the device installation. It is possible to specify a negative value so that you can differentiate between a location above and below sea level.

Degrees (latitude)

This field specifies the angle in degrees of the geographic coordinate system.

Minutes (latitude)

This field specifies the minutes of the geographic coordinate system.

Seconds (latitude)

This field specifies the seconds of the geographic coordinate system.

Hemisphere (latitude)

This field specifies the orientation of the geographic coordinate system. The following values are possible for geographical latitude:

- North: Northerly latitude
- South: Southerly latitude

Degrees (longitude)

This field specifies the angle in degrees of the geographic coordinate system.

Minutes (longitude)

This field specifies the minutes of the geographic coordinate system.

Seconds (longitude)

This field specifies the seconds of the geographic coordinate system.

Hemisphere (longitude)

This field specifies the orientation of the geographic coordinate system. The following values are possible for geographical longitude:

- East: Easterly longitude
- West: Westerly longitude

Description

Enter a description of the device.

8.12.2 Additions to the Status menu

Common profiles

This column indicates the assigned LBS general profile.

SNMP ID:

1.73.2.3

Telnet path:

Status > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

8.12.3 Additions to the Setup menu

LBS general profile

The LBS general profile selected here applies to the WLAN profile.

SNMP ID:

2.37.1.3.9

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]`

Default:

empty

8.13 Additions to the Status menu

8.13.1 Acquire statistical data

This entry indicates whether the device collects statistical data.

SNMP ID:

1.73.123.9

Telnet path:

Status > **WLAN-Management** > **Client-Steering**

Possible values:

Yes

The device collects statistical data.

No

The device does not collect statistical data.

8.14 WLC Clustering Wizard

As of HiLCOS version 9.10 it is possible to use the Clustering Wizard in LANconfig to configure the WLCs all at once.

Note: With WLCs equipped with the “WLC High Availability Clustering XL option” you are able to select all of the listed WLCs and configure them all in one go using the WLC Clustering Wizard (see *1-Click WLC High Availability Clustering Wizard*).

9 VPN

9.1 SCEP-CA function in VPN environments

As of HiLCOS version 9.10, it is possible to use the existing CA with SCEP function in the VPN environment.

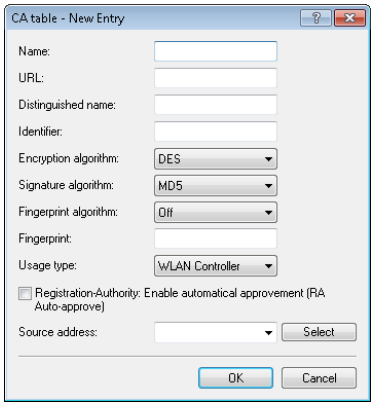
9.2 SCEP algorithms updated

As of HiLCOS version 9.10, the SCEP client and server additionally support AES192 and AES256 and also SHA256, SHA384, and SHA512.

Note: The default entries remain unchanged so as to maintain compatibility with the remote stations in the event of a firmware update. Only use the latest algorithms when the remote stations have also been updated accordingly.

9.2.1 Configuring the CAs

The configuration is carried out with LANconfig under **Certificates** > **SCEP client** with the button **CA table**.



Name

Configuration name of the CA.

URL

URL of the CA.

Distinguished name

Distinguished name of the CA. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration.

You can also use reserved characters by using a preceding backslash ("\"). The supported reserved characters are:

- Comma (",")
- Slash ("/")
- Plus ("+")
- Semicolon (";")
- Equals ("=")

You can also use the following internal firmware variables:

- %% inserts a percent sign.
- %f inserts the version and the date of the firmware currently active in the device.
- %r inserts the hardware release of the device.
- %v inserts the version of the loader currently active in the device.

- %m inserts the MAC address of the device.
- %s inserts the serial number of the device.
- %n inserts the name of the device.
- %l inserts the location of the device.
- %d inserts the type of the device.

Identifier

CA identifier (as required by some web server to identify the CA).

Encryption algorithm

This algorithm encrypts the payload of the certificate request. Possible values are:

- DES (Default)
- 3-DES
- Blowfish
- AES128
- AES192
- AES256

Signature algorithm

The certificate request is signed with this algorithm. Possible values are:

- MD5 (default)
- SHA1
- SHA256
- SHA384
- SHA512

Fingerprint algorithm

Algorithm for signing the fingerprint. This determines whether the CA certificate is to be checked by means of fingerprint, and which algorithm is used for this. The CA fingerprint has to agree with the checksum which results when this algorithm is applied. Possible values are:

- Off (default)
- MD5
- SHA1
- SHA256

- SHA384
- SHA512

Fingerprint

The authenticity of a received CA certificate can be checked by means of the the checksum (fingerprint) entered here (corresponding to the set CA fingerprint algorithm).

Usage type

Indicates the intended application of the specified CA. The CA entered here is only queried for the corresponding application. Possible values are:

- VPN
- EAP/TLS
- WLAN controller
- General

Note: If a general CA exists no further CAs can be configured. Otherwise the choice of CA would be unclear.

RA autoapprove

Some CAs provide the option of using an earlier certificate issued by this CA as proof of authenticity for future requests. This option defines whether an existing system certificate should be used to sign new requests. Possible values are:

- Yes
- No (Default)

Source address

This is where you configure an optional source address to be used instead of the one otherwise automatically selected for the source address. If you have configured loopback addresses, you can specify them here as source address.

You can enter an address in various forms:

- Name of the IP network (ARF network), whose address should be used.

- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ (Note: If there is an interface named "DMZ", its address will be taken).
- LB0 ... LBF for one of the 16 loopback addresses or its name
- Furthermore, any IP address can be entered in the form x.x.x.x.

Note: If the source address set here is a loopback address, these will be used unmasked on the remote client.

9.2.2 Additions to the Setup menu

Enc-Alg

The encryption algorithm is specified here as used by the SCEP protocol (Simple Certificate Enrollment Protocol). Both the certification authority (CA) and the certificate holder (client) must support the algorithm. A number of methods are available:

Note: If possible you should employ one of the last methods (3DES, BLOWFISH, AES) if the certification authority (CA) and all the clients support it. The default value here is DES encryption to ensure interoperability.

SNMP ID:

2.39.1.14.4

Telnet path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

DES

Data Encryption Standard: The DES algorithm uses a 64-bit key. This is the SCEP standard encryption. DES is an algorithm developed by the National Bureau of Standards (NBS) in the USA. The DES algorithm uses a 64-bit key which allows combinations of a substitution cipher, transposition cipher and exclusive-OR (XOR) operations. The

64-bit block size consists of an effective key length of 56 bits and 8 parity bits. The algorithm is based on the Lucifer cipher.

3DES

Triple-DES: This is an improved method of DES encryption using two keys of 64-bits in length.

BLOWFISH

The BLOWFISH algorithm works with a variable key length of between 32 and 448 bits. It is a fast and highly secure algorithm. It has major advantages over other symmetrical methods such as DES and 3DES.

AES

Advanced Encryption Standard: The AES algorithm has a variable block size of 128, 192 or 256 bits and a variable key length of 128, 192 or 256 bits, providing a very high level of security.

Default:

DES

CA signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the certification authority (CA) and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. Two cryptographic hash functions are relatively widespread.

SNMP ID:

2.39.1.14.6

Telnet path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

CA fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. Both the certification authority (CA) and the certificate holder (client) must support the algorithm.

The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data.

SNMP ID:

2.39.1.14.8

Telnet path:

Setup > **Certificates** > **SCEP-Client** > **CAs**

Possible values:

Off

MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

Encryption algorithm

The encryption algorithm is specified here as used by the SCEP protocol (Simple Certificate Enrollment Protocol). Both the certification authority (CA) and the certificate holder (client) must support the algorithm. A number of methods are available:

Note: If possible you should employ one of the last methods (3DES, BLOWFISH, AES) if the certification authority (CA) and all the clients support it. The default value here is DES encryption to ensure interoperability.

SNMP ID:

2.39.2.3

Telnet path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

DES

Data Encryption Standard: The DES algorithm uses a 64-bit key. This is the SCEP standard encryption. DES is an algorithm developed by the National Bureau of Standards (NBS) in the USA. The DES algorithm uses a 64-bit key which allows combinations of a substitution cipher, transposition cipher and exclusive-OR (XOR) operations. The 64-bit block size consists of an effective key length of 56 bits and 8 parity bits. The algorithm is based on the Lucifer cipher.

3DES

Triple-DES: This is an improved method of DES encryption using two keys of 64-bits in length.

BLOWFISH

The BLOWFISH algorithm works with a variable key length of between 32 and 448 bits. It is a fast and highly secure algorithm. It has major advantages over other symmetrical methods such as DES and 3DES.

AES

Advanced Encryption Standard: The AES algorithm has a variable block size of 128, 192 or 256 bits and a variable key length of 128, 192 or 256 bits, providing a very high level of security.

Default:

DES

Signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the certification authority (CA) and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. Two cryptographic hash functions are relatively widespread.

SNMP ID:

2.39.2.6

Telnet path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

Fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. Both the certification authority (CA) and the certificate holder (client) must support the algorithm.

The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data.

SNMP ID:

2.39.2.7

Telnet path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

MD5

Message Digest Algorithm 5: The MD5 algorithm generates a 128-bit hash value. MD5 was developed in 1991 by Ronald L. Rivest. The results reveal no conclusive information about the key. This method takes a message of any length to generate a 128-bit message digest, which is attached to the unencrypted message. The recipient compares the message digest with that determined from the information.

SHA1

Secure Hash Algorithm 1: The SHA1 algorithm generates a 160-bit hash value. This is used to calculate a unique checksum for any data. Generally this data makes up messages. It is practically impossible to come across two messages with exactly the same SHA value.

SHA256

Like SHA1 but with a 256-bit hash value.

SHA384

Like SHA1 but with a 384-bit hash value.

SHA512

Like SHA1 but with a 512-bit hash value.

Default:

MD5

9.3 Loopback address for L2TP connections

As of HiLCOS version 9.10 it is possible to specify a loopback address for L2TP connections.

Note: If a loopback address is entered as the source address and the routing tag has a value of "0", the device uses the routing tag of the loopback address.

9.3.1 Additions to the Setup menu

Source address

Here you can optionally specify a loopback address for the device to use as the target address instead of the one that would normally be selected automatically.

Note: If the list of IP networks or source addresses contains an entry named 'DMZ', then the associated IP address will be used.

Important: If the source address set here is a loopback address, this will be used unmasked even on masked remote clients.

SNMP ID:

2.2.35.10

Telnet path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

Valid entry from the list of possible addresses.

Name of the IP networks whose addresses are to be used.

"INT" for the address of the first intranet

"DMZ" for the address of the first DMZ

LB0 to LBF for the 16 loopback addresses

Any valid IP address

empty

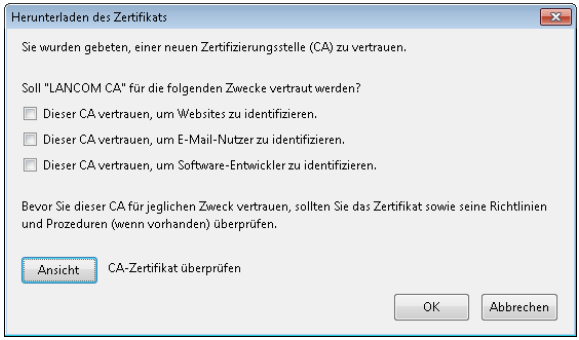
Default:

9.4 Download link for the public portion of the CA certificate

As of HiLCOS version 9.10, the public part of the CA certificate is available by means of a download link.

9.4.1 Download link for the public portion of the CA certificate

You can download the public part of the CA certificate without having to authenticate by using the link `http://<URL>/getcacert/cacert.crt`. The transmission uses the MIME type `application/x-x 509-ca-cert`, so that software with the appropriate functionality will immediately offer to the install the certificate.



Note: The download is only possible if the CA is enabled. An error message appears if the CA is disabled.

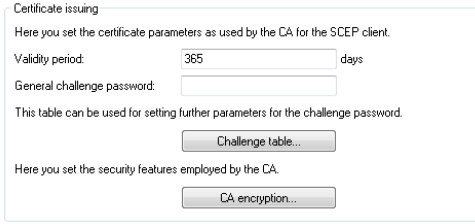
If the CA is enabled, WEBconfig is also able to download the certificate under **Extras** > **Download current CA certificate**.

9.5 Configurable one-time password (OTP) for SCEP-CA

As of HiLCOS version 9.10, it is also possible to create one-time passwords (OTP) for SCEP-CA.

9.5.1 Configuring challenge passwords

In LANconfig, you configure the certificate parameters under **Certificates** > **Certificate handling** in the section **Certificate issuing**.



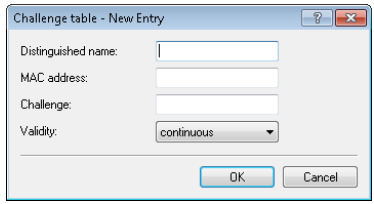
Validity period

Here you specify the validity period of the certificate in days.

General challenge password

An additional “Password” can be entered here, which is transmitted to the CA. This can be used by default to authenticate revocation requests. If CAs operate Microsoft-SCEP (mscep), the one-time passwords issued by the CA can be entered here for the authentication of requests.

The **Challenge table** contains the certificate recipients' (clients') own passwords.



Distinguished name

The “Distinguished name” must be entered here. With this parameter the CAs are assigned to system certificates (and vice versa) on the one hand. On the other hand this parameter is also important for evaluating whether received or available certificates match with the configuration. Separated by commas or forward slashes, this is a list where the name, department, state and country can be specified for the gateway. The following are examples of how an entry might appear: `CN=myCACN, DC=mscep, DC=ca, C=DE, ST=berlin, O=myOrg /CN=HIRSCHMANN CA/O=HIRSCHMANN/C=DE`

MAC address

Enter the MAC address of the client whose password is to be managed by the challenge-password table.

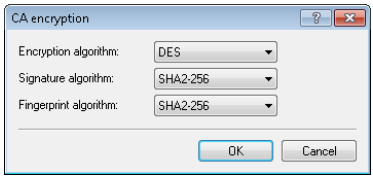
Challenge

Enter the challenge (password) for the client here.

Validity

Enter the validity period of the password here. By selecting “one-time” the password becomes a one-time password (OTP) so that, for example, it can only be used for authentication once.

Under **CA encryption** you configure the security parameters for the CA encryption.



Encryption algorithm

The encryption algorithm is specified here as used by the SCEP protocol. Both the certification authority (CA) and the certificate holder (client) must support the algorithm. The following methods are available:

- DES
- 3DES
- BLOWFISH
- AES128
- DES192
- DES256

Signature algorithm

Here you select the signature algorithm used by the Certificate Authority (CA) to sign the certificate. This method must be supported by the CA and the certificate recipient (client) as the client uses this signature to check the integrity of the certificate. The following cryptographic hash functions are available for selection:

- MD5
- SHA1

- SHA2-256
- SHA2-384
- SHA2-512

Fingerprint algorithm

Here you select the fingerprint algorithm that the Certificate Authority (CA) uses to calculate the signature's fingerprint. Both the CA and the certificate recipient (client) must support the method.

The fingerprint is a hash value of data (key, certificate, etc.), i.e. a short number string that can be used to check the integrity of the data. The following cryptographic hash functions are available for selection:

- MD5
- SHA1
- SHA2-256
- SHA2-384
- SHA2-512

9.5.2 Additions to the Setup menu

Challenge

Enter the validity period of the password here. By selecting “one-time” the password becomes a one-time password (OTP), so it can only be used for authentication once.

SNMP ID:

2.39.2.5.3.5

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **CA-certificates** > **Challenge-Passwords**

Possible values:

One-time
Permanent

Default:
Permanent

9.6 Deleting VPN error messages in the status table

As of HiLCOS version 9.10 the device automatically deletes VPN-connection error messages from the status table after a defined period. By default, this option is disabled (time = 0 minutes).

By default, the device retains the VPN error messages in the status table. Depending on the installation LANmonitor may display a large number of open error messages, which clutters the display. For this reason the WEBconfig setting under **Setup** > **Config** > **Error-Aging-Minutes** enables you to define a period of time in minutes after which the device automatically deletes these error messages from the status table.

Note: To document sporadic errors, disable this option with the entry `0`.

9.6.1 Additions to the Setup menu

Error aging minutes

Here you set the length of time in minutes after which the device deletes VPN errors from the status table.

Note: To document sporadic errors, disable this option with the entry `0`.

SNMP ID:
2.11.65

Telnet path:
Setup > **Config**

Possible values:

Max. 4 characters from `0123456789`

Default:

0

Special values:

0

Disables this option. Errors will remain in the status table.

9.7 IPv4 addresses for VPN tunnels in the IP parameter list

As of HiLCOS version 9.10, devices supporting VPN manage the IPv4 addresses for VPN tunnels in the IP parameter list.

9.7.1 Additions to the Setup menu

IP-List

If certain remote sites do not automatically transmit the IP parameters needed for a connection, then enter these values here.

Use this table to configure the extranet address of a VPN tunnel, for example.

SNMP ID:

2.2.20

Telnet path:

Setup > **WAN**

Remote site

Enter the name for the remote station here.

When configuring a VPN tunnel, this entry corresponds to the appropriate service under **Setup** > **VPN** > **VPN-Peers** or **Setup** > **VPN** > **IKEv2** > **Connections**.

SNMP ID:

2.2.20.1

Telnet path:

Setup > **WAN** > **IP-List**

Possible values:

Select from the list of defined peers.

Max. 16 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Masq.-IP-Addr.

Almost all Internet providers usually have the remote device assign a dynamic IP address to your router when it establishes the connection. If your Internet provider has assigned you static IP addresses, or if you wish to operate masquerading for your VPN network, you assign it to the respective connection here. If the masquerading IP address is not set, then the address assigned when the connection was established is used for masquerading.

Note: You need to set a masquerading address for a VPN connection if you wish to mask a private network behind this address in the VPN network.

Note: This setting is also necessary if a private address (172.16.x.x) is assigned during PPP negotiation. Normal masquerading is thus impossible as this type of address is filtered in the Internet.

SNMP ID:

2.2.20.9

Telnet path:

Setup > **WAN** > **IP-List**

Possible values:

Valid IPv4 address, max. 15 characters from `[0-9].`

Default:

0.0.0.0

Masquerading

You can use IP masquerading to hide a hide a logical network behind a single address (that of the router). If, for example, you have an Internet connection, you can us it to connect your entire network to the Internet.

Almost all Internet providers usually have the remote device assign a dynamic IP address to your router when it establishes the connection. If your Internet provider has assigned fixed IP addresses, you can assign them to the relevant connection in the IP parameter list.

Select “on” to enable IP masquerading for all LAN interfaces. If you wish to assign fixed IP addresses to computers in the demilitarized zone (DMZ) and yet you still wish to activate IP masquerading for the computers on the other LAN interfaces (intranet), then select “Intranet”.

If you want this entry to mask a VPN connection, select “on”.

SNMP ID:

2.8.2.5

Telnet path:

Setup > **IP-Router** > **IP-Routing-Table**

Possible values:

No

IP masking off

On

Intranet and DMZ masquerading

Intranet

Intranet - Intranet masquerading only

Default:

No

Extranet address

In HiLCOS versions before 9.10, this field contained the IPv4 address used by the local stations to mask their own IP address in certain scenarios.

As of HiLCOS version 9.10, masquerading uses the entry under **Setup** > **WAN** > **IP-List** in the field **Masq.-IP-Addr.**.

SNMP ID:

2.19.9.2

Telnet path:

Setup > **VPN** > **VPN-Peers**

Possible values:

Max. 15 characters from `[0-9].`

Default:

empty

10 Routing and WAN connections

10.1 Client binding

As of HiLCOS version 9.10, load balancing additionally features client binding.

10.1.1 Client binding

The use of load balancing leads to problems for servers that use an IP address to identify a logged-on user. If a user is logged in to a web site, for example, and the load balancer then takes a different Internet connection, then the server interprets this as a connection attempt by a user who is not logged on. In the best case the user sees a new login dialog, but not the desired web page.

One possible workaround would be to use a firewall rule (policy based routing) to direct the traffic to this server over a specific Internet connection. However, this would limit all of the traffic to that server to the bandwidth of a single connection. What's more, there is no way to establish a backup if the first connection should fail.

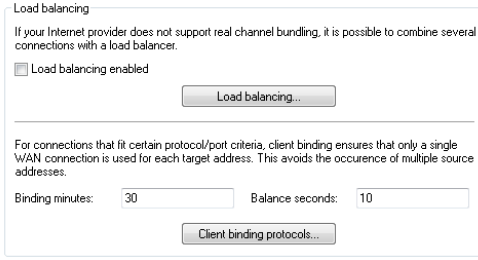
In contrast to this, client binding does not monitor the individual TCP/IP sessions but the client that opened an Internet connection in the initial session. It directs all subsequent sessions through this Internet connection, which corresponds in principle to the policy-based routing mentioned above. How this is done depends on the protocol, i.e. it transports only data of the same protocol type (e.g. HTTPS) over this Internet connection. If the client loads additional data via an HTTP connection, it probably does this with a different connection.

To prevent data from being bottle-necked into this one Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the

timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

10.1.2 Load balancing with client binding

In LANconfig, client binding is configured under **IP router** > **Routing** in the section **Load balancing**.



Binding minutes

Here you specify the time in minutes for the binding entries to be valid for a client.

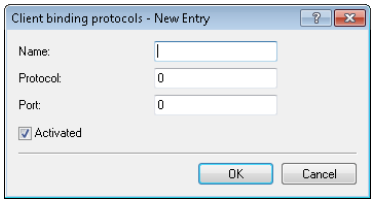
Balance seconds

To prevent data from flowing the this main-session Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

Here you specify the time in seconds, following the start of the main session, during which the load balancer is free to distribute new sessions to other Internet connections.

Client binding is protocol-oriented. You set the corresponding protocols under **Client binding protocols**. The table already contains the default entries

- HTTPS
- HTTP
- ANY



Name

Contains a descriptive name for this entry.

Protocol

Contains the IP protocol number.

Note: Learn more about IP protocol numbers in the IANA *Online database*.

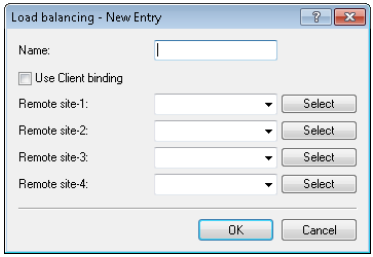
Port

Contains the port of the IP protocol.

Activated

Activates or deactivates this entry.

Client binding can be activated or deactivated for each of the entries under **Load balancing**.



10.1.3 Enhancements in the menu system

Additions to the Setup menu

Client binding

In this menu, you can configure the client binding.

The use of load balancing leads to problems for servers that use an IP address to identify a logged-on user. If a user is logged in to a web site, for example, and the load balancer then takes a different Internet connection, then the server interprets this as a connection attempt by a user who is not logged on. In the best case the user sees a new login dialog, but not the desired web page.

One possible workaround would be to use a firewall rule (policy based routing) to direct the traffic to this server over a specific Internet connection. However, this would limit all of the traffic to that server to the bandwidth of a single connection. What's more, there is no way to establish a backup if the first connection should fail.

In contrast to this, client binding does not monitor the individual TCP/IP sessions but the client that opened an Internet connection in the initial session. It directs all subsequent sessions through this Internet connection, which corresponds in principle to the policy-based routing mentioned above. How this is done depends on the protocol, i.e. it transports only data of the same protocol type (e.g. HTTPS) over this Internet connection. If the client loads additional data via an HTTP connection, it probably does this with a different connection.

To prevent data from being bottle-necked into this one Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

SNMP ID:

2.8.20.3

Telnet path:

Setup > **IP-Router** > **Load-Balancer**

Protocols

In this table, you specify the protocols and the associated ports for monitoring by the client binding.

Note: The table already contains the default entries

- HTTPS
- HTTP
- ANY

SNMP ID:

2.8.20.3.1

Telnet path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Name

Enter a descriptive name for this entry.

SNMP ID:

2.8.20.3.1.1

Telnet path:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protocols**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]`

Default:
empty

Protocol

Select the IP protocol number.

Note: Learn more about IP protocol numbers in the *online database* of the IANA.

SNMP ID:
2.8.20.3.1.2

Telnet path:
Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protocols**

Possible values:
Max. 3 characters from `[0-255]`

Special values:

0
All protocols

Default:
0

Port

Select the port.

SNMP ID:

2.8.20.3.1.3

Telnet path:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protocols**

Possible values:

Max. 5 characters from `[0-65535]`

Special values:

0

All ports

Default:

0

Operating

Here you enable or disable the client binding for this entry.

SNMP ID:

2.8.20.3.1.4

Telnet path:

Setup > **IP-Router** > **Load-Balancer** > **Client-Binding** > **Protocols**

Possible values:

Yes

Enables the entry

No

Disables the entry

Default:

Yes

Binding minutes

Specify the time in minutes for the binding entries to be valid for a client.

SNMP ID:

2.8.20.3.2

Telnet path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Possible values:

Max. 3 characters from `[0-999]`

Special values:

0

Default:

30

Balance seconds

To prevent data from flowing through this main-session Internet connection when it could easily be transferred via parallel connections, a timer ensures that the load balancer distributes additional sessions between the available Internet connections for a specified period. After the timer expires, the client binding forces a new session over the original Internet connection and the timer is restarted. The server thus continues to recognize the login status for the user due to the current IP address.

Here you specify the time in seconds, following the start of the main session, during which the load balancer is free to distribute new sessions to other Internet connections.

SNMP ID:

2.8.20.3.3

Telnet path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Possible values:

Max. 3 characters from `[0-999]`

Special values:

0

The timer is deactivated. All sessions are bound to the existing Internet connection.

Default:

10

Client binding

Here you enable or disable the client binding for each load balancer.

SNMP ID:

2.8.20.2.10

Telnet path:

Setup > **IP-Router** > **Load-Balancer** > **Bundle-Peers**

Possible values:

Yes

Client binding is enabled.

No

Client binding is disabled.

Default:

No

Additions to the Status menu

Client binding

This table shows the details of current client bindings.

SNMP ID:

1.10.32.3

Telnet path:

Status > **IP-Router** > **Load-Balancer**

Source-IP

This entry shows the source IP addresses of the client.

SNMP ID:

1.10.32.3.1

Telnet path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Bundle-Peer

This entry shows the name of the selected Internet connection.

SNMP ID:

1.10.32.3.2

Telnet path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Timeout

This entry indicates the remaining time until the load balancer deletes this entry.

SNMP ID:

1.10.32.3.3

Telnet path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

Balance

This entry indicates whether the timer is enabled for allowing further Internet connections.

SNMP ID:

1.10.32.3.4

Telnet path:

Status > **IP-Router** > **Load-Balancer** > **Client-Binding**

10.2 Interface binding "Any" removed in IPv4

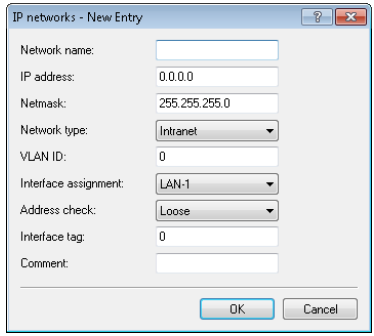
As of HiLCOS version 9.10 it is no longer possible to select "Any" when assigning interfaces to IPv4 networks.

Note: The new default setting is "LAN-1" or "BRG-1".

10.2.1 Defining networks and assigning interfaces

When defining a network, the first setting is for the IP address range which is to be valid for a certain local interface on the router. “Local interfaces” are logical interfaces which are assigned either to a physical Ethernet port (LAN) or to a wireless port (WLAN). To realize the scenarios outlined above, it is possible for several networks to be active on one interface: Conversely, a network can also be active on multiple interfaces (via bridge groups or with the interface assignment 'Any').

The networks are defined in a table under **IPv4** > **General** > **IP networks**. A unique name for the networks is set along with definitions for the address range and interface assignment. The network name allows the identification of networks in other modules (DHCP server, RIP, NetBIOS, etc.) and to enable control over which services are available in which networks.



10.2.2 Additions to the Setup menu

Interface

Here you select the interface that is to be allocated to the network.

Note: The values for 'x' in the list vary per model.

SNMP ID:

2.7.30.5

Telnet path:

Setup > **TCP-IP** > **Network-List**

Possible values:

LAN-1
LAN-x
WLAN-x-x
P2P-x-x
BRG-x

Default:

LAN-1

10.3 Generic routing encapsulation (GRE)

As of HiLCOS version 9.10 it is possible to transmit data packets of any transmission protocol as IP packets within GRE tunnels.

The trace command has an additional parameter in case of issues with GRE tunnels:

This parameter ...	*...causes the following message in the trace:*
GRE	Messages to GRE tunnels

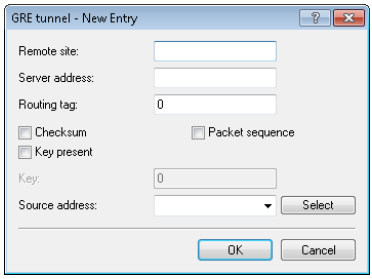
Table 9: Overview of all possible traces

10.3.1 Understanding the generic routing encapsulation (GRE) protocol

GRE is a tunneling protocol that encapsulates any layer-3 data packets (including IP, IPSec, ICMP, etc.) into virtual point-to-point network connections. This is very useful, among other things, when the two communication partners wish to use a particular transport protocol (for example, IPSec) that is unavailable on the transmission path. Since GRE itself does not encrypt the tunneled data, the two communication partners themselves must ensure that the data is protected.

Configuring a GRE tunnel

To configure a GRE tunnel with LANconfig, navigate to **Communication** > **Remote sites** > **GRE tunnel** and click **GRE tunnel**.



Remote site

The name of the remote station for this GRE tunnel. Use this name in the routing table in order to send data through this GRE tunnel.

Server address

Address of the GRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

Routing-Tag

Routing tag for the connection to the GRE tunnel endpoint. The device maps data packets to this GRE tunnel by means of the routing tag.

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this GRE tunnel. The device only maps incoming data packets to this GRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this GRE tunnel if their GRE header similarly does not contain a key value.

Key

The key that assures data-flow control in this GRE tunnel. Two devices connected via several GRE tunnels use this key to map the data packets to the appropriate GRE tunnel.

Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the GRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

Source address

Here you can optionally specify a source address for the device to use as the target address instead of the one that would normally be selected automatically. Possible values are:

- Name of the IP networks whose addresses are to be used.
- "INT" for the address of the first intranet
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses
- Any valid IP address

Note: If the list of IP networks or source addresses contains an entry named 'DMZ', then the associated IP address will be used.

To use IPv6 as the GRE tunnel transport protocol, navigate to **IPv6** > **WAN interfaces** and create a new entry named "IPV6GRE", for example. When you subsequently configure the GRE tunnel, you set this interface as the **Remote site**.

If you need to specify an IP address for the tunnel interface, proceed as follows:

IPv4 address

Create a new entry under **Communication** > **Protocols** > **IP parameters** and set the name of the remote site as the name of the GRE tunnel remote site. Finally, enter the necessary values for the **IP address** and **Netmask**.

IPv6

Create a new entry under **IPv6** > **General** > **IP addresses** and set the network name as the name of the GRE tunnel remote site. Finally, enter the necessary values for the **Address/Prefix length**.

10.3.2 Additions to the Setup menu

GRE-Tunnel

GRE is a tunneling protocol that encapsulates any layer-3 data packets (including IP, IPSec, ICMP, etc.) into virtual point-to-point network connections. You configure the various GRE tunnels here.

SNMP ID:

2.2.51

Telnet path:

Setup > **WAN**

Remote site

The name of the remote station for this GRE tunnel. Use this name in the routing table in order to send data through this GRE tunnel.

SNMP ID:

2.2.51.1

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

IP address

Address of the GRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

SNMP ID:

2.2.51.3

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Max. 64 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Routing-Tag

Routing tag for the connection to the GRE tunnel endpoint.

SNMP ID:

2.2.51.4

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

0 … 65535

Default:

0

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this GRE tunnel. The device only maps incoming data packets to this GRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this GRE tunnel if their GRE header similarly does not contain a key value.

SNMP ID:

2.2.51.5

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Yes
No

Default:

No

Key value

The key that assures data-flow control in this GRE tunnel.

SNMP ID:

2.2.51.6

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

0 … 4294967295

Default:

0

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

SNMP ID:

2.2.51.7

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Yes
No

Default:

No

Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the GRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

SNMP ID:

2.2.51.8

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Yes
No

Default:

No

Source address

Here you can optionally specify a source address for the device to use as the target address instead of the one that would normally be selected automatically.

Note: If the list of IP networks or loopback addresses contains an entry named 'DMZ', then the associated IP address will be used.

SNMP ID:

2.2.51.9

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Valid entry from the list of possible addresses.

Name of the IP networks whose addresses are to be used.

"INT" for the address of the first intranet

"DMZ" for the address of the first DMZ

LB0 to LBF for the 16 loopback addresses

Any valid IP address

empty

Default:

10.3.3 Additions to the Status menu

GRE-Tunnel

This table shows the status values of the GRE tunnel.

SNMP ID:

1.86

Telnet path:
Status

Remote site

This column contains the name of each GRE tunnel remote station.

SNMP ID:
1.86.1

Telnet path:
Status > **GRE-Tunnel**

Server address

This column contains the addresses of the GRE tunnel endpoints (valid IP address or FQDN).

SNMP ID:
1.86.3

Telnet path:
Status > **GRE-Tunnel**

Routing-Tag

This column contains the routing tags for the connections to each of the GRE tunnel endpoints.

SNMP ID:

1.86.4

Telnet path:

Status > **GRE-Tunnel**

Key present

This column indicates whether the GRE header of the respective tunnel contains a key.

SNMP ID:

1.86.5

Telnet path:

Status > **GRE-Tunnel**

Key

This column contains the key if one is present in the GRE header of the corresponding tunnel.

SNMP ID:

1.86.6

Telnet path:

Status > **GRE-Tunnel**

Checksum

This column indicates whether the GRE header of the corresponding tunnel contains a checksum.

SNMP ID:

1.86.7

Telnet path:

Status > **GRE-Tunnel**

Sequencing

This column indicates whether the GRE header of the corresponding tunnel contains packet sequencing.

SNMP ID:

1.86.8

Telnet path:

Status > **GRE-Tunnel**

Source address

This column contains the source address specified for the respective GRE tunnel.

SNMP ID:

1.86.9

Telnet path:

Status > **GRE-Tunnel**

10.4 Ethernet-over-GRE tunnel (EoGRE)

As of HiLCOS version 9.10 it is possible to transmit Ethernet packets as IP packets within EoGRE tunnels.

The trace command has an additional parameter in case of issues with GRE tunnels:

This parameter ...	*...causes the following message in the trace:*
GRE	Messages to GRE tunnels

Table 10: Overview of all possible traces

10.4.1 Ethernet-over-GRE (EoGRE)

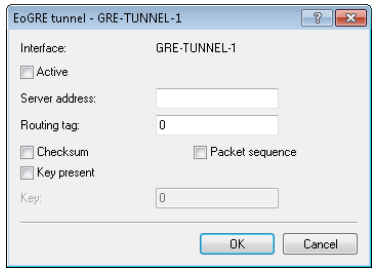
Note: For more information about the GRE protocol, see *Understanding the generic routing encapsulation protocol (GRE)*.

The current version of HiLCOS provides a number of “Ethernet over GRE” tunnels (EoGRE) to transmit Ethernet packets via GRE. Since these Ethernet packets move on OSI layer 2 only, the EoGRE tunnel only functions as a bridge.

This can be used to implement L2VPN (VPN as a simple level-2 bridge) or a transparent Ethernet bridge over WAN.

Configuring an EoGRE tunnel

To configure an EoGRE tunnel with LANconfig, navigate to **Communication** > **Remote sites** > **GRE tunnel**, click **EoGRE tunnel** and select the appropriate tunnel.



Interface

Name of the selected EoGRE tunnel.

Operating

Activates or deactivates the EoGRE tunnel. Deactivated EoGRE tunnels do not send or receive any data.

Server address

Address of the EoGRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

Routing-Tag

Routing tag for the connection to the EoGRE tunnel endpoint. The device maps data packets to this EoGRE tunnel by means of the routing tag.

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this EoGRE tunnel. The device only maps incoming data packets to this EoGRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this EoGRE tunnel if their GRE header similarly does not contain a key value.

Key

The key that assures data-flow control in this EoGRE tunnel. Two devices connected via several EoGRE tunnels use this key to map the data packets to the appropriate EoGRE tunnel.

Sequencing

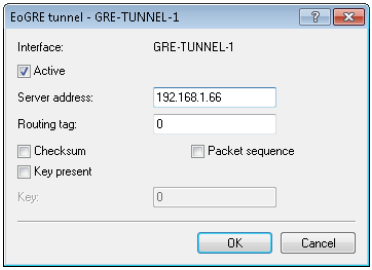
Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the EoGRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

Connecting a local interface to an EoGRE tunnel

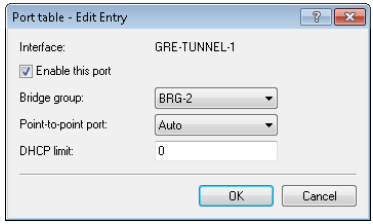
Connecting a local interface to an EoGRE tunnel involves the following steps:

1. Create a new entry under **Communication** > **Remote sites** > **GRE tunnel** > **EoGRE tunnel**.



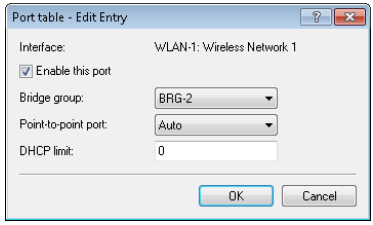
Activate the tunnel and, under **Server address**, enter the address of the remote device to which the EoGRE tunnel is to connect (IPv4 address, IPv6 address, or FQDN).

2. Add a bridge group for the activated EoGRE tunnel under **Interfaces** > **LAN** > **Port table**.



Enable the port and select the required bridge group.

3. Again under **Interfaces** > **LAN** > **Port table**, supplement the same bridge group with the local interface that you want to connect through the EoGRE tunnel (e.g. WLAN-1).



Enable the port and select from the list the bridge group that contains the EoGRE tunnel.

10.4.2 Additions to the Status menu

EoGRE-Tunnel

This table shows you information about the EoGRE tunnels.

SNMP ID:

1.87

Telnet path:
Status

10.4.3 Additions to the Setup menu

EoGRE-Tunnel

The current version of HiLCOS provides a number of "Ethernet over GRE" tunnels (EoGRE) to transmit Ethernet packets via GRE. You configure the various EoGRE tunnels here.

SNMP ID:
2.2.50

Telnet path:
Setup > **WAN**

Interface

Name of the selected EoGRE tunnel.

SNMP ID:
2.2.50.1

Telnet path:
Setup > **WAN** > **EoGRE-Tunnel**

Operating

Activates or deactivates the EoGRE tunnel. Deactivated EoGRE tunnels do not send or receive any data.

SNMP ID:

2.2.50.2

Telnet path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Yes
No

Default:

No

IP address

Address of the EoGRE tunnel endpoint (valid IPv4 or IPv6 address or FQDN).

SNMP ID:

2.2.50.3

Telnet path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Max. 64 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Routing-Tag

Routing tag for the connection to the EoGRE tunnel endpoint.

SNMP ID:

2.2.50.4

Telnet path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

0 … 65535

Default:

0

Key present

Here you specify whether the GRE header should contain a key for data-flow control.

If you enable this feature, the device inserts the value set in the **key** field into the GRE header for this EoGRE tunnel. The device only maps incoming data packets to this EoGRE tunnel if their GRE header contains an identical key value.

With this feature disabled, the GRE header of outgoing data packets does not contain a key value. The device only maps incoming data packets to this EoGRE tunnel if their GRE header similarly does not contain a key value.

SNMP ID:

2.2.50.5

Telnet path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Yes
No

Default:

No

Key value

The key that assures data-flow control in this EoGRE tunnel.

SNMP ID:

2.2.50.6

Telnet path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

0 … 4294967295

Default:

0

Checksum

Here you specify whether the GRE header should contain a check sum.

With the check sum function enabled, the device calculates a checksum for the transmitted data and attaches this to the GRE tunnel header. If the GRE header of incoming data contains a checksum, the device checks this against the transmitted data. The device discards any data received with an erroneous or missing check sum.

With the checksum function disabled, the device sends all tunnel data without a checksum and it expected data packets without a checksum. Incoming data packets with a checksum in the GRE header are discarded.

SNMP ID:

2.2.50.7

Telnet path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

Yes
No

Default:

No

Sequencing

Here you specify whether the GRE header contains information about the sequence of the data packets.

With this feature enabled, the device includes a counter in the GRE header of outgoing data packets in order to communicate the sequence of the data packets to the EoGRE tunnel endpoint. The device analyses the sequence of incoming data packets and drops packets with an incorrect or missing packet sequence.

SNMP ID:

2.2.50.8

Telnet path:

Setup > **WAN** > **EoGRE-Tunnel**

Possible values:

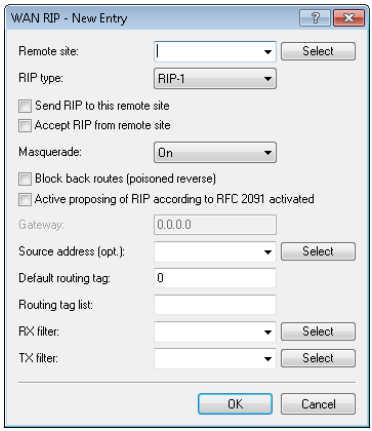
Yes
No

Default:

No

10.5 Loopback addresses for RIP

As of HiLCOS version 9.10 it is possible to specify a loopback address for WAN RIP.



Source address (opt.)

This is where you can configure an optional sender address to be used instead of the one otherwise automatically selected for the destination address.

If you have configured loopback addresses, you can specify them here as source address. You can enter an address in various forms:

- Name of the IP network (ARF network), whose address should be used.
- “INT” for the address of the first intranet.
- “DMZ” for the address of the first DMZ (Note: If there is an interface named “DMZ”, its address will be taken).
- LB0…LBF for one of the 16 loopback addresses or its name.
- Furthermore, any IP address can be entered in the form x.x.x.x.

Note: If the source address set here is a loopback address, these will be used unmasked on the remote client.

10.5.1 Additions to the Setup menu

Loopback address

Enter a loopback address here. Possible values are:

- The name of an ARF network
- Configured loopback address
- IPv4 address

SNMP ID:

2.8.8.4.13

Telnet path:

Setup > **IP-Router** > **RIP** > **WAN-Table**

Possible values:

Specify a valid IPv4 address here.

Default:

empty

10.6 PPPoE snooping new

As of HiLCOS version 9.10 PPPoE snooping is also implemented.

10.6.1 PPPoE snooping

PPPoE snooping enables devices that receive and forward PPPoE discovery (PPPoED) packets to analyze these packets and to supplement them with additional information. This information can be used by a PPPoE access concentrator (AC) to process the PPPoED data packets accordingly. This role is called the “PPPoE-Intermediate-Agent”.

PPPoE snooping in the HiLCOS processes the following PPPoED packets:

- PADI (PPPoE Active Discovery Indication)

- PADR (PPPoE Active Discovery Request)
- PADT (PPPoE Active Discovery Terminate)

The PPPoE intermediate agent, which is responsible for the PPPoE snooping, supplements the PPPoED packet with manufacturer-specific attributes (circuit ID and remote ID), and any existing IDs in received packets are replaced with its own values.

- The remote ID: Uniquely identifies the client making a PPPoE request.
- Circuit ID: Uniquely identifies the interface used by a client to make a PPPoE request.

PPPoE snooping is configured for each LAN/WLAN interface.

10.6.2 Additions to the Setup menu

PPPoE snooping

Here you configure PPPoE snooping for each interface.

SNMP ID:

2.20.43

Telnet path:

Setup > **LAN-Bridge**

Port

Indicates the physical or logical interface to which this PPPoE-snooping configuration applies.

SNMP ID:

2.20.43.1

Telnet path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

LAN-x
All physical LAN interfaces

WLAN-x
All physical WLAN interfaces

WLAN-x-x
All logical WLAN interfaces

P2P-x-x
All logical P2P interfaces

WLC-TUNNEL-x
All virtual WLC tunnels

GRE-TUNNEL-x
All virtual GRE tunnels

Add agent info

Here you decide whether the PPPoE intermediate agent gives incoming PPPoE packets a manufacturer-specific PPPoE tag with the vendor ID “3561” before forwarding the request to a PPPoE server.

This option allows the PPPoE intermediate agent to deliver additional information to the PPPoE server about the interface used by the client to make the request.

The PPPoE tag is composed of values for the **Remote ID** and the **Circuit ID**.

Note: If these two fields are empty, the PPPoE intermediate agent does not add a PPPoE tag to the data packets.

SNMP ID:

2.20.43.2

Telnet path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

Yes

Adds “relay agent info” to the PPPoE packets.

No

This setting disables PPPoE snooping for this interface.

Default:

No

Remote ID

The remote ID is a sub-option of the PPPoE intermediate agent option. It uniquely identifies the client making a PPPoE request.

You can use the following variables:

- %%: Inserts a percent sign.
- %c: Inserts the MAC address of the interface where the PPPoE intermediate agent received the PPPoE request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- %c: Inserts the name of the interface where the PPPoE intermediate agent received the PPPoE request.
- %n: Inserts the name of the PPPoE intermediate agent as specified under **Setup** > **Name**.
- %v: Inserts the VLAN ID of the PPPoE request packet. This VLAN ID is sourced either from the VLAN header of the PPPoE data packet or from the VLAN ID mapping for this interface.
- %p: Inserts the name of the Ethernet interface that received the PPPoE data packet. This variable is useful for devices featuring an Ethernet switch or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, %p and %i are identical.
- %s: Inserts the WLAN SSID if the PPPoE packet originates from a WLAN client. For other clients, this variable contains an empty string.

- %e: Inserts the serial number of the PPPoE relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

SNMP ID:

2.20.43.3

Telnet path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

Max. 30 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Circuit ID

The circuit ID is a sub-option of the PPPoE intermediate agent info option. It uniquely identifies the interface used by the client to make a PPPoE request.

You can use the following variables:

- %%: Inserts a percent sign.
- %c: Inserts the MAC address of the interface where the PPPoE intermediate agent received the PPPoE request. If a WLAN-SSID is involved, then this is the corresponding BSSID.
- %c: Inserts the name of the interface where the PPPoE intermediate agent received the PPPoE request.
- %n: Inserts the name of the PPPoE intermediate agent as specified under **Setup** > **Name**.
- %v: Inserts the VLAN ID of the PPPoE request packet. This VLAN ID is sourced either from the VLAN header of the PPPoE data packet or from the VLAN ID mapping for this interface.
- %p: Inserts the name of the Ethernet interface that received the PPPoE data packet. This variable is useful for devices featuring an Ethernet switch

or Ethernet mapper, because they can map multiple physical interfaces to a single logical interface. For other devices, `%p` and `%i` are identical.

- `%s`: Inserts the WLAN SSID if the PPPoE packet originates from a WLAN client. For other clients, this variable contains an empty string.
- `%e`: Inserts the serial number of the PPPoE relay agent, to be found for example under **Status** > **Hardware-Info** > **Serial number**.

SNMP ID:

2.20.43.4

Telnet path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

Max. 30 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Discard server packets

Here you decide whether the PPPoE intermediate agent retains or discards any existing PPPoE tags.

SNMP ID:

2.20.43.5

Telnet path:

Setup > **LAN-Bridge** > **PPPoE-Snooping**

Possible values:

Yes

The PPPoE intermediate Agent removes existing PPPoE tags and leaves both the “Circuit ID” and the “Remote ID” empty.

No

The PPPoE intermediate agent takes over any existing PPPoE tags.

Default:

No

10.7 Default settings in the access table for WAN connections

As of HiLCOS version 9.10, all protocols for WAN connections are disabled in the access table.

10.7.1 Additions to the Setup menu

Telnet

Use this option to set the access rights for configuring the device via the TELNET protocol. This protocol is required for text-based configuration of the device with the Telnet console, which is independent of the operating system.

SNMP ID:

2.11.15.2

Telnet path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

Note: VPN-capable devices only.

Yes

Access is generally possible.

Note: By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Note: Default setting for the WAN interface.

Default:

Yes
No

TFTP

Use this option to set the access rights for configuring the device via the TFTP protocol (Trivial File Transfer Protocol). This protocol is required, for example, for configuration using the LANconfig application.

SNMP ID:

2.11.15.3

Telnet path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

Note: VPN-capable devices only.

Yes

Access is generally possible.

Note: By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Note: Default setting for the WAN interface.

Default:

Yes
No

HTTP

Use this option to set the access rights for configuring the device via the HTTP protocol (Hypertext Transfer Protocol). This protocol is required for configuring the device via the implemented web-based browser interface independent of the operating system.

SNMP ID:

2.11.15.4

Telnet path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

Note: VPN-capable devices only.

Yes

Access is generally possible.

Note: By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Note: Default setting for the WAN interface.

Default:

Yes
No

SNMP

Use this option to set the access rights for configuring the device via the SNMP protocol (Simple Network Management Protocol). This protocol is required, for example, for configuring the device using the LANmonitor application.

SNMP ID:

2.11.15.5

Telnet path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

Note: VPN-capable devices only.

Yes

Access is generally possible.

Note: By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Note: Default setting for the WAN interface.

Default:

Yes
No

HTTPS

Use this option to set the access rights for configuring the device via the HTTPS protocol (Hypertext Transfer Protocol Secure or HTTP via SSL). This protocol is required for configuring the device via the implemented web-browser interface independent of the operating system.

SNMP ID:

2.11.15.6

Telnet path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

Note: VPN-capable devices only.

Yes

Access is generally possible.

Note: By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Note: Default setting for the WAN interface.

Default:

Yes
No

Telnet-SSL

Use this option to set the access rights for configuring the device via the TELNET protocol. This protocol is required for text-based configuration of the device with the Telnet console, which is independent of the operating system.

SNMP ID:

2.11.15.7

Telnet path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

Note: VPN-capable devices only.

Yes

Access is generally possible.

Note: By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Note: Default setting for the WAN interface.

Default:

Yes
No

SSH

Use this option to set the access rights for configuring the device via the TELNET/SSH protocol. This protocol is required for configuring the device securely via the implemented Telnet console from text-based systems independent of the operating system.

SNMP ID:

2.11.15.8

Telnet path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

Note: VPN-capable devices only.

Yes

Access is generally possible.

Note: By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Note: Default setting for the WAN interface.

Default:

Yes

No

Config Sync

Indicates whether a config sync is possible (restricted) via this interface.

SNMP ID:

2.11.15.10

Telnet path:

Setup > **Config** > **Access-Table**

Possible values:

VPN

Access is only possible via VPN.

Note: VPN-capable devices only.

Yes

Access is generally possible.

Note: By default via all interfaces except WAN.

Read

Access is read only.

No

Access is not possible.

Note: Default setting for the WAN interface.

Default:

Yes
No

11 Other services

A single device offers a range of services for the PCs on the LAN. These are essential functions for use by the workstations. In particular these are:

- Automatic address management with DHCP
- Name administration of computers and networks by DNS
- Network traffic logging with SYSLOG
- Charging
- Time server

11.1 Prefer perfect forward secrecy (PFS) for connections

As of HiLCOS version 9.10 it is possible to enter a PFS encryption method (cipher suite) irrespective of whether the client has a different setting.

11.1.1 Additions to the Setup menu

Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.11.29.6

Telnet path:

Setup > **Config** > **Telnet-SSL**

Possible values:

On
Off

Default:

On

Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.21.40.7

Telnet path:

Setup > **HTTP** > **SSL**

Possible values:

On
Off

Default:

On

Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.25.10.10.19.6

Telnet path:

Setup > **RADIUS** > **Server** > **EAP** > **EAP-TLS**

Possible values:

On
Off

Default:

On

Prefer PFS

When setting the cipher suite, the device usually takes over the same setting as the requesting client. Certain client applications by default require a connection without perfect forward secrecy (PFS), even though both the device and the client are PFS-capable.

This option means that your device always prefers to connect with PFS, regardless of the default setting of the client.

SNMP ID:

2.25.20.5

Telnet path:
Setup > **RADIUS** > **RADSEC**

Possible values:
On
Off

Default:
On

11.2 Additions to the Setup menu

11.2.1 E-mail

Here you specify whether you want to receive notifications by e-mail.

The option presettings differ depending on the cause.

SNMP ID:
2.41.2.2.9.2

Telnet path:
Setup > **UTM** > **Content Filter** > **Global settings** > **Notifications**

Possible values:
Off
Immediate
Daily

11.3 TACACS+ extension for the passwd command

As of HiLCOS version 9.10, a user password can additionally be changed using the console command `passwd` even with TACACS+ authentication enabled.

Command	*Description*
`setpass|passwd [-u <User>][-n <new> <old>]`	Changes the password of the current user account. In order to change the password without a subsequent input prompt, use the option switch `-n` while entering the new and old password. In order to change the password of the local user account when authentication by TACACS+ is enabled, use the option switch `-u` with the name of the corresponding user. If the local user does not exist or the user name is missing, the command aborts. The user must also have supervisor rights, or authorization by TACACS must be enabled.

Table 11: Overview of all commands available at the command line

11.4 Input field for DHCP options extended to 251 characters

As of HiLCOS version 9.10, it is possible to enter 251 characters when specifying DHCP options.

11.4.1 Additions to the Setup menu

Option value

This field defines the contents of the DHCP option. IP addresses are normally specified using the conventional IPv4 notation, e.g. `123.123.123.100`. Integer tapes are usually entered in decimal digits and string types as simple text. Multiple values in a single field are separated with commas, e.g.`123.123.123.100, 123.123.123.200`.

Note: The maximum possible length value depends on the selected option number. RFC 2132 lists the maximum length allowed for each option.

SNMP ID:

2.10.21.3

Telnet path:

Setup > **DHCP** > **Additional-Options**

Possible values:

Max. 251 characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

12 Other parameters

12.1 Profile

Displays the profile of the cellular modem.

SNMP ID:

1.49.45

Telnet path:

Status > **Modem-Mobile**

12.2 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

SNMP ID:

2.11.29.7

Telnet path:

Setup > **Config** > **Telnet-SSL**

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:
Allowed

12.3 TLS connections

In this directory, you specify the address and port to be used by the device to accept incoming configuration changes.

SNMP ID:
2.11.51.3

Telnet path:
Setup > **Config** > **Sync**

12.3.1 Port

Specify the port to be used by the device to receive incoming configuration changes.

SNMP ID:
2.11.51.3.1

Telnet path:
Setup > **Config** > **Sync** > **TLS-Connections**

Possible values:

Max. 5 characters from `[0-9]`

0 … 65535

Default:

1941

12.4 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

SNMP ID:

2.21.40.8

Telnet path:

Setup > **HTTP** > **SSL**

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored

The device ignores the request to renegotiate sent by the remote station.

Default:

Allowed

12.5 LBS-Tracking

This entry enables or disables the LBS tracking for this SSID.

SNMP ID:

2.23.20.1.25

Telnet path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

No

LBS tracking is disabled.

Yes

LBS tracking is enabled.

12.6 LBS-Tracking-List

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the client transfers the specified list name, the MAC address of the access point, and its own MAC address to the LBS server.

SNMP ID:

2.23.20.1.26

Telnet path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

Name from **Setup** > **WLAN** > **Network** > **LBS-Tracking**

Max. 16 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:
empty

12.7 OKC

This option enables or disables the opportunistic key caching (OKC).

The device uses this value only if the interface works in client mode. The interface is in AP mode, the enabling or disabling of OKC is only possible by means of profile management with a WLC.

In the PMK caching status under **Status** > **WLAN** > **PMK-Caching** > **Contents**, OKC PMKs can be identified by the authenticator address `ff:ff:ff:ff:ff:n`, where `n` is the assigned profile number (e.g. `0` for “WLAN-1”, `1` for “WLAN1-2”, etc.).

SNMP ID:
2.23.20.3.17

Telnet path:
Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:
Yes
No

Default:
Yes

12.8 Network name

Enter a unique name for the network where this WLAN interface is located.

SNMP ID:
2.23.20.5.15

Telnet path:
Setup > **Interfaces** > **WLAN** > **Interpoint-Settings**

Possible values:
Max. 32 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:
empty

12.9 Manage user wizard

In this entry, you will find the advanced settings for the **Public Spot Manage Users** wizard.

SNMP ID:
2.24.44

Telnet path:
Setup > **Public-Spot-Module**

12.9.1 Show status information

This entry gives you the option to hide status information in the Setup Wizard.

SNMP ID:

2.24.44.10

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

No

The Setup Wizard hides the following columns: **Online-Time**, **Traffic**, **Status**, **MAC-Address**, **IP-Address**.

Yes

The Setup Wizard displays all status information.

12.10 Renegotiations

This setting gives you control over whether the client can trigger a renegotiation of SSL/TLS.

SNMP ID:

2.25.20.6

Telnet path:

Setup > **RADIUS** > **RADSEC**

Possible values:

Forbidden

The device disconnects from the remote station if this requests a renegotiation.

Allowed

The device permits renegotiations with the remote station.

Ignored
The device ignores the request to renegotiate sent by the remote station.

Default:
Allowed

12.11 LBS-Tracking-List

With this entry, you set the list name for the LBS tracking. When a client successfully associates with this SSID, the client transfers the specified list name, the MAC address of the AP, and its own MAC address to the LBS server.

SNMP ID:
2.37.1.1.47

Telnet path:
Setup > **WLAN-Management** > **AP-Configuration**

Possible values:
Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **LBS-Tracking**

Max. 16 characters from
`[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:
empty

12.12 Max. number of concurrent updates

Here you specify how many firmware updates the WLC may perform at the same time.

SNMP ID:

2.37.27.38

Telnet path:

Setup > **WLAN-Management** > **Central-Firmware-Management**

Possible values:

1-30
10

Default:

10

12.13 CAPWAP-Port

In this entry, you specify the CAPWAP port for the WLAN controller.

SNMP ID:

2.59.5

Telnet path:

Setup > **WLAN-Management**

Possible values:

Max. 5 characters from `[0-9]`

0 … 65535

Default:
1027

12.14 RS count

Configures the number of IPv6 router solicitations that the device should send after the IPv6 LAN interface is started.

SNMP ID:
2.70.6.13

Telnet path:
Setup > **IPv6** > **LAN-Interfaces**

Possible values:
Max. 1 characters from `[0-9]`

Default:
3

12.15 RS count

Configures the number of IPv6 router solicitations that the device should send after the IPv6 WAN interface is started.

SNMP ID:
2.70.7.11

Telnet path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

Max. 1 characters from `[0-9]`

Default:

3

12.16 Flash restore

With the device in test mode, you can restore the configuration from the Flash memory. You do this from the command-line interface with the command `do/Other/Flash-Restore`. This command restores the original configuration that was active before executing the command "Flash No" from the Flash memory.

SNMP ID:

4.7

Telnet path:

Other > **Flash-Restore**

12.17 Additions to the Status menu

12.17.1 DSLAM chipset manufacturer dump

Displays additional information provided by the manufacturer of the DSLAM chipset. The content is variable and depends on the manufacturer.

SNMP ID:

1.41.25.47

Telnet path:

Status > **ADSL** > **Advanced**

12.17.2 DSLAM manufacturer dump

Displays additional information provided by the manufacturer of the DSLAM. The content is variable and depends on the manufacturer.

SNMP ID:

1.41.25.48

Telnet path:

Status > **ADSL** > **Advanced**

12.17.3 DSLAM chipset manufacturer dump

Displays additional information provided by the manufacturer of the DSLAM chipset. The content is variable and depends on the manufacturer.

SNMP ID:

1.75.25.47

Telnet path:

Status > **VDSL** > **Advanced**

12.17.4 DSLAM manufacturer dump

Displays additional information provided by the manufacturer of the DSLAM. The content is variable and depends on the manufacturer.

SNMP ID:

1.75.25.48

Telnet path:

Status > **VDSL** > **Advanced**

HIRSCHMANN
A BELDEN BRAND

Addendum
HiLCOS Rel. 9.12

Contents

1 Routing and WAN connections.....3

1.1 Configuring WWAN access.....3

1.2 Switching between mobile profiles or SIM cards.....9

1 Routing and WAN connections

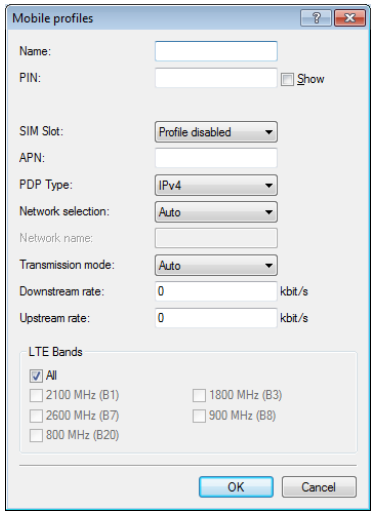
1.1 Configuring WWAN access

The following tutorial shows how you manually configure devices with an internal cellular modem to use access via mobile networks (WWAN). First you either create a mobile profile for your provider or edit an existing profile, and then you assign this profile to the WAN interface of the device.

Alternatively, a simpler and faster way of configuration is available with a Setup Wizard (**Set up Internet access**).

1. In LANconfig, open the configuration dialog for your device and navigate to the section **Interfaces** > **WAN**.
2. Select an existing profile to be edited or add a new profile for your provider in the **Mobile profiles** table.

   In the interests of completeness this tutorial explains the creation of a new profile.



3. Under **Name** type in a unique label for the mobile profile.
4. Under **PIN** enter the 4-digit PIN of the mobile phone SIM card. The device needs this information to operate the mobile modem.

   Important: The SIM card logs every failed attempt with an incorrect PIN. The number of failed attempts remains stored even when the device is temporarily disconnected from the mains. After 3 failed attempts, the SIM card is locked from further access attempts. If this occurs, you usually need the 8-digit PUK or SuperPIN to unlock it.

5. If your device accommodates several SIM cards, use **SIM slot** to select the SIM card that you want to associate with this profile.

   The item **Profile disabled** switches this mobile profile off. This option is useful if you wish to create a profile template only and complete the mobile setup at a later time.

   Note: Only enabled profiles are visible for selection in LANmonitor.

6. Under **APN**, enter the name of the access server for the data services of your mobile provider.
   The APN (access point name) is specific to each mobile phone provider. You will usually find this information in the documentation provided with your mobile phone contract.
7. Under **PDP type** you specify the type of the PDP context for the mobile profile.
   The PDP context describes the support of the address spaces which the backbone of the corresponding cellular network provider offers for connections from the cellular network to the Internet. This can be either IPv4 or IPv6 alone, or can include support for both address spaces (dual stack). Clients that want to use the corresponding cellular network provider must support at least one of the specified address spaces.
8. Set the preferred **Network selection** mode:

   Automatic

   The mobile modem automatically connects to one of the available and permitted mobile phone networks.

   Manual

The mobile modem connects to the specified mobile phone network only.

Note: Manual mobile network selection is especially suitable when the device is in stationary operation and you wish to prevent it from connecting to another undesirable or more expensive mobile phone network.

9. If you have selected manual network selection, enter the exact name of your desired network under **Network name**.
10. Specify the preferred transfer mode within the mobile network under **Transmission mode**:

    Automatic
    Automatic selection of transmission mode

    LTE(4G)+UMTS(3G)
    Combined LTE & UMTS mode

    LTE(4G)+GPRS(2G)
    Combined LTE & GPRS mode

    LTE(4G)
    LTE mode only

    UMTS(3G)+GPRS(2G)
    Combined UMTS & GPRS mode

    UMTS(3G)
    UMTS mode only

    GPRS(2G)
    GPRS mode only

11. Under **Downstream rate** and **Upstream rate** you specify the transfer rates for the mobile phone connection. This is important for the QoS (quality-of-service) feature and the functioning of the firewall.
    If the value is set to `0`, the mobile interface in the corresponding direction is considered to be unlimited and the QoS mechanisms will not take effect.
12. If unfavorable environmental conditions cause the router to constantly switch between two frequency bands, instabilities in the transmission may be the result. The selection under **LTE bands** allows you to control which frequency bands are used by the mobile modem.

    All

All frequency bands are enabled.

2100 MHz (B1)
2.1GHz band is enabled.

1800 MHz (B3)
1.8GHz band is enabled.

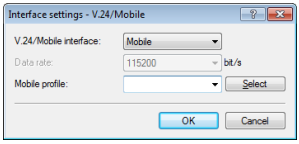
2600 MHz (B7)
2.6GHz band is enabled.

900 MHz (B8)
900MHz band is enabled.

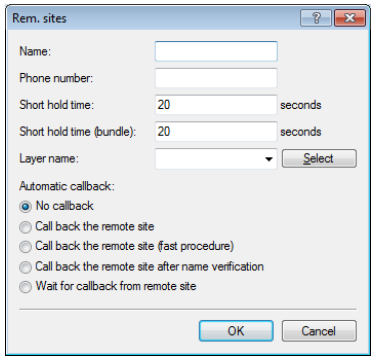
800 MHz (B20)
800MHz band is enabled.

Note: This option applies only to the LTE standard frequency bands. All bands can be used for UMTS and GPRS.

13. Click **OK** to save the settings.
14. In the dialog **Interfaces** > **WAN**, click **Interface settings** and select **V.24/Mobile**.
15. Set the **V.24/Mobile interface** to **Mobile**.
16. Under **Mobile profiles**, select the profile you created earlier for your mobile phone provider.



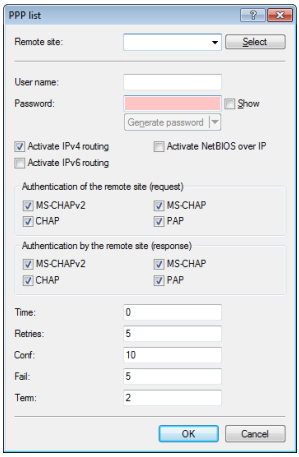
17. Click **OK** to save the settings.
18. In the view **Communication** > **Remote sites**, click **Rem. (Mobile /...)** and add a new profile.



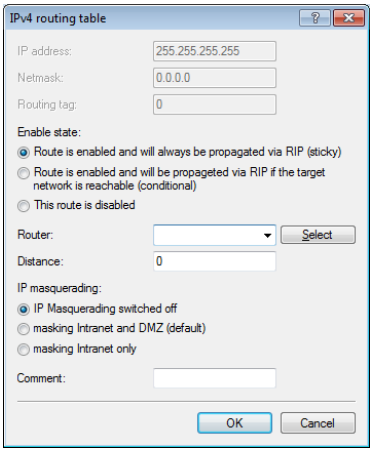
19. Enter a unique name for the profile under **Name**, e.g. `WWAN`.
20. Under **Phone number**, enter the dial-in number of your mobile phone provider. If your provider has not given you a dial-in phone number, enter `*99#`.
21. Under **Short hold time**, enter the time after which the device disconnects from the remote site if no packets are transmitted

    Enter a value in seconds to find a balance between the costs arising from idle time those of connection establishment, for example `300`. A value of `0` causes the device to stay connected until it is broken and terminated. With a value of `9999` the device automatically reconnects every time.

22. For **Layer name** select the presetting `UMTS`.
23. Click **OK** to save the settings.
24. In the view **Communication** > **Protocols**, open the **PPP list** and add a new remote site.



25. Under **Remote site**, select the profile that you created previously, e.g. `WWAN`.
26. Deselect any settings under **Authentication of the remote site (request)**.
27. Click **OK** to save the settings.
28. In the view **IP Router** > **Routing**, click **IPv4 routing table** and add the **Default route** (`255.255.255.255`).



29. Under **Router**, select the profile created earlier under **Rem. sites (Mobile /...)**.
30. Set the **IP masquerading** to **Masking intranet and DMZ (default)**.

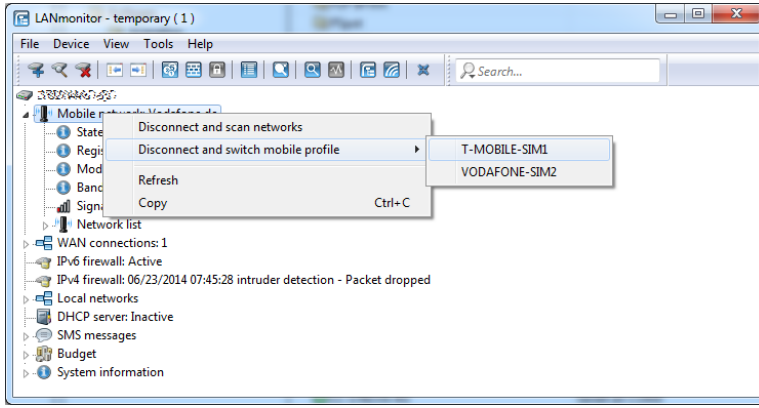
31. Click **OK** to save the settings.
32. Write the changes back to the device.

This concludes the configuration of the WWLAN access.

1.2 Switching between mobile profiles or SIM cards

If you have created different mobile profiles for a SIM card or one mobile profile for several SIM cards, LANmonitor allows you to toggle between these profiles or SIM cards. The following steps show you how to select an alternate profile or an alternate SIM card.

1. Select your device in LANmonitor.
2. On the entry **Mobile network**, open the context menu and select the option **Disconnect and switch mobile profile**.



3. Select the mobile profile that you want to switch to.

The device then disconnects from the mobile network and reconnects using the selected mobile profile.

HIRSCHMANN
A BELDEN BRAND

Addendum
HiLCOS Rel. 10.12

1 Configuration

1.1 Preventing password form fields in the browser from storing passwords

As of HiLCOS 10.12, it is possible to suppress the storage of passwords by your web browser for the WEBconfig login form.

Input dialogs on web pages allow web browsers to store any passwords that are entered. This makes things easier for a user accessing the page again in future. This web browser feature is a vulnerability that malicious software can exploit to read out the confidential form data.

To force the manual input of login passwords each time a page is accessed, open WEBconfig and navigate to **Setup** > **HTTP** > **Disable-Password-Autocompletion** and prevent the storage of passwords with the setting “Yes”.

1.1.1 Additions to the Setup menu

Disable-Password-Autocompletion

This switch controls whether the WEBconfig login dialog allows the browser to save user input to the password form field for subsequent auto-completion.

SNMP ID:

2.21.22

Telnet path:

Setup > **HTTP**

Possible values:

No

The browser may not save the contents of the password form field. The WEBconfig input mask forces the user to enter the password manually.

Yes

The browser saves the input of the password form field and automatically fills-in the field the next time the login dialog is called.

Default:

No

1.2 Support of ChaCha20/Poly1305 for SSH access

As of version 10.12, HiLCOS additionally supports the following cipher algorithms for access via SSH:

- chacha20-poly1305
- aes128-gcm
- aes256-gcm

1.2.1 Additions to the Setup menu

Cipher-Algorithms

The cipher algorithms are used for encrypting and decrypting data. Select one or more of the available algorithms.

SNMP ID:

2.11.28.1

Telnet path:

Setup > **Config** > **SSH**

Possible values:

3des-cbc
3des-ctr
arcfour
arcfour128
arcfour256
blowfish-cbc
blowfish-ctr
aes128-cbc
aes192-cbc
aes256-cbc
aes128-ctr
aes192-ctr
aes256-ctr
chacha20-poly1305
aes128-gcm
aes256-gcm

Default:

3des-cbc

3des-ctr

arcfour

arcfour128

arcfour256

blowfish-cbc

blowfish-ctr

aes128-cbc

aes192-cbc

aes256-cbc

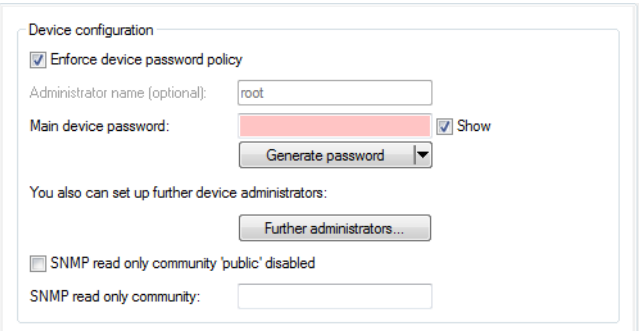
aes128-ctr

aes192-ctr

aes256-ctr

1.3 Enforcing password complexity for device passwords

As of HiLCOS 10.12, you have the option to enforce a predefined password policy for setting device passwords.



The switch **Enforce device password policy**determines the following policies for the main device password and the administrator passwords:

- The length of the password is at least 8 characters.
- The password contains at least 3 of the 4 character classes, i.e. lowercase letters, uppercase letters, numbers, and special characters.

Please note that this feature has no effect on existing passwords. Only when passwords are changed are they checked for their policy compliance.

1.3.1 Additions to the Setup menu

Enforce-Password-Rules

This entry gives you the option to disable or enable the enforcing of password rules.

SNMP ID:

2.11.93

Telnet path:

Setup > **Config**

Possible values:

No

Password rules enforcement is disabled.

Yes

Password rules enforcement is enabled.

Default:

Yes

1.4 Preventing the storage of passwords in WEBconfig

As of HiLCOS 10.12, you have the option to deactivate the auto-completion of password fields.

1.4.1 Additions to the Setup menu

Disable-Password-Autocompletion

This switch controls whether the WEBconfig login dialog allows the browser to save user input to the password form field for subsequent auto-completion.

SNMP ID:

2.21.22

Telnet path:

Setup > **HTTP**

Possible values:

No

The browser may not save the contents of the password form field. The WEBconfig input mask forces the user to enter the password manually.

Yes

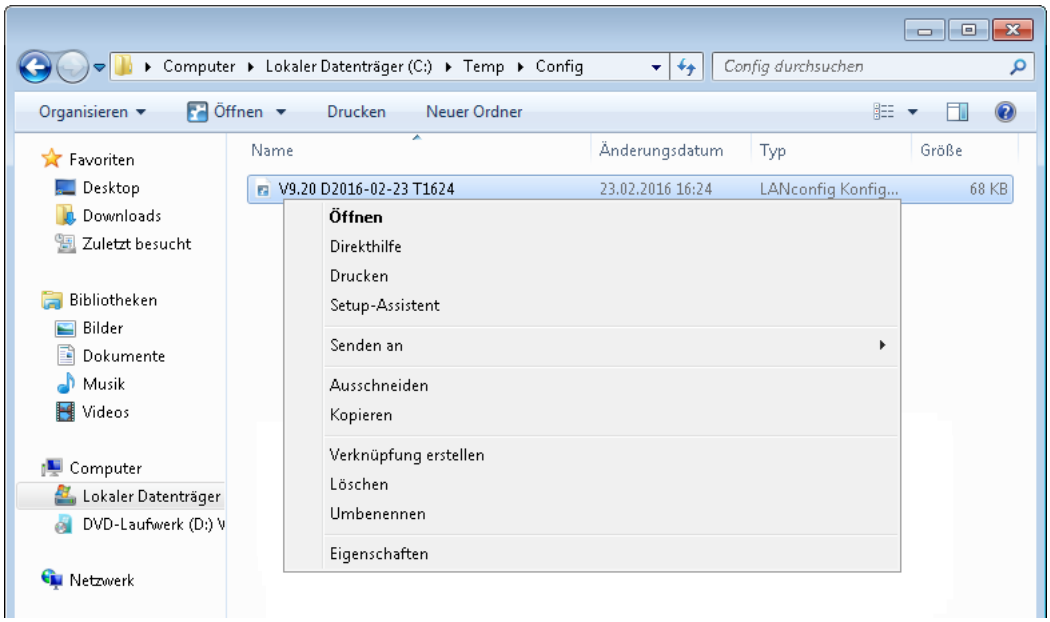
The browser saves the input of the password form field and automatically fills-in the field the next time the login dialog is called.

Default:

No

1.5 LANconfig: Icon for *.LCS files in Windows Explorer

As of HiLCOS 10.12, the Windows Explorer displays *.LCS files with a dedicated icon. The context menu or a double-click on the file opens the LANconfig "What's this" direct help.
The following functions are available from the Windows Explorer context menu:



Open

This menu item opens the configuration in LANconfig.

This item only appears for configuration files with the extension `.lcf`.

What's this

This menu item opens a help text which gives users information about dealing with this file.

Print

This menu item enables you to print the file.

Setup Wizard

This menu item starts the LANconfig Setup Wizard.

This item only appears for configuration files with the extension `.lcf`.

1.6 Importing files by copy & paste on the CLI

From HiLCOS 10.12, your device supports the loading of files into file slots from the console and also by means of a script.

This offers the convenience of using a script to roll-out files together with the configuration or, for example, to import SSH keys and VPN certificates.

- The file format must be of type text or ASCII; binary formats are not supported.
- In the case of certificates, the file format must be PEM-encoded (ASCII/Base64). DER-encoded certificates are not supported.

Syntax of the CLI command **importfile**:

importfile -a <application> [-p <passphrase>] [-n] [-h <hash> -f <fingerprint>] [-c] [-r]

Required parameters:

-a <application>

<application> specifies the storage location and thus the usage for the entered data. For a complete list of the storage locations on your device, enter **importfile -?**.

Optional parameters:

-n

-n starts the non-interactive mode. There are no prompts or other outputs on the CLI. The non-interactive mode is intended for use with scripts.

-p <passphrase>

<passphrase> is the password required to decrypt an entered private key.

-h <hash>

The hash algorithm used to determine the fingerprint of the root CA certificate.

-f <fingerprint>

The fingerprint of the root CA certificate, created with **–h**. The fingerprint can be entered either with or without colons.

-c

Only CA certificates are uploaded.

-r

Uploaded CA certificates replace any existing ones.

CTRL+Z cancels any active input.

Example:

In this example, user input is shown in **bold** and prompts for the user are shown in *italic*. Certificates and other long, multi-line outputs are abbreviated with **[...]** for legibility. At the end of the example you will find explanations for the individual steps.

```
root@test:/
    importfile    -a    VPN2    -p    lancom    -h    SHA512    -f
4F:A7:5E:C9:D4:77:CE:D3:06:4C:79:93:D8:FA:3A:8E:7B:FE:19:61:B2:0C:37:4F:BB:7A:E6:46:36:04:46:EE:F6:DA:97:15:6B:BB:
2D:8F:B6:66:E6:7C:54:1E:B4:02:79:54:D6:DF:1E:9B:27:7C:9C:EA:B8:CB:1B:6D:90:1C

The input can be aborted by pressing CTRL+Z.
Please enter the PEM-encoded (Base64) device certificate, the end of the input will be
detected automatically:
importfile>-----BEGIN CERTIFICATE-----
importfile>MIID9DCCAtwCCQDgaoWRCmWaLjANBgkqhkiG9w0BAQ0FADAkMQswCQYDVQQG[…]
importfile>[…]s7pM5l0L0d0=
importfile>-----END CERTIFICATE-----
Importing device certificate:
        Version: 1 (0x0)
        Serial Number:
            e0:6a:85:91:0a:65:9a:2e
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=OCSP-TEST-CA,C=DE
        Validity
            Not Before: Jul  4 12:34:07 2017 GMT
            Not After : Oct  5 12:34:07 2024 GMT
        Subject: CN=TEST,O=Internet Widgits Pty Ltd,ST=Some-State,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:bb:93:f6:b9:9a:41:b2:3e:30:2b:09:7f:d1:f9:
                    49:54:5a:82:c9:17:10:1f:79:6d:ab:55:df:b8[…]
                   […]2f:0c:8a:69:7b:a9:82:32:f3:ca:9c:02:20:14:
                    bd:8b:0d
                Exponent: 65537 (0x10001)
    Signature Algorithm: sha512WithRSAEncryption
         06:5b:a4:1a:a2:69:c1:bf:6f:b1:d2:6c:b0:21:e1:10:43:[…]
         […]50:e6:a3:1d:f3:15:b7:87:8c:65:2f:25:f6:b3:ba:4c:e6:
         5d:0b:d1:dd

The input can be aborted by pressing CTRL+Z.
Please enter the PEM-encoded (Base64) device private key, the end the input will be detected
 automatically:
importfile>-----BEGIN RSA PRIVATE KEY-----
importfile>Proc-Type: 4,ENCRYPTED
importfile>DEK-Info: AES-128-CBC,8FB95ED0568DA9AE17D7573BC294ACD8
importfile>[…]5Cuf2p798Obhw3isAe04XRwmdLno8ZcPDyB33ZKPjmhUzB0WsdzGdSSq5iYjD
importfile>-----END RSA PRIVATE KEY-----
The private key was read successfully.
The private key matches the device certificate.
The input can be aborted by pressing CTRL+Z.
Please enter the chain of PEM-encoded (Base64) CA certificates.
The input is closed with "endcachain":
importfile>-----BEGIN CERTIFICATE-----
importfile>MIIDGzCCAgOgAwIBAgIJAMlNxBFGQqpoMA0GCSqGSIb3DQEBDQUAMCQxCzAJB[…]
importfile>[…]EUDI9giYt9tnAT8hJfLkkyN/PHSiP+e+vopjSpKuyg==
importfile>-----END CERTIFICATE-----
importfile>endcachain
Importing CA certificate:
        Version: 3 (0x2)
        Serial Number:
            c9:4d:c4:11:46:42:aa:68
    Signature Algorithm: sha512WithRSAEncryption
        Issuer: CN=OCSP-TEST-CA,C=DE
```

```
        Validity
            Not Before: Jun  6 13:56:49 2017 GMT
            Not After : Jun 19 13:56:49 2045 GMT
        Subject: CN=OCSP-TEST-CA,C=DE
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (2048 bit)
                Modulus:
                    00:e9:ba:04:74:7d:78:5a:84:b3:63:cc:ad:4d:[…]
                    […]14:0e:27:c8:8c:5a:00:a3:4c:ed:4f:02:e8:0b:
                    fb:07
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                57:13:BB:94:3B:89:C5:3B:B7:A0:0E:BB:BF:39:05:67:8B:FB:84:30
            X509v3 Authority Key Identifier:
                keyid:57:13:BB:94:3B:89:C5:3B:B7:A0:0E:BB:BF:39:05:67:8B:FB:84:30

            X509v3 Basic Constraints:
                CA:TRUE
    Signature Algorithm: sha512WithRSAEncryption
         c8:cf:3b:97:1a:56:61:13:9c:61:ed:21:23:7a:37:b4:a8:[…]
        […]3f:21:25:f2:e4:93:23:7f:3c:74:a2:3f:e7:be:be:8a:63:
         4a:92:ae:ca

Content of the PKCS12 file: private key: 1, device certificate: 1, CA certificates: 1
root@test:/
```

1. The importfile command is called for the storage location VPN2, so we are dealing with a certificate for use in the VPN. The password for the private key is hirschmann and the root CA certificate can be checked with SHA512 and the specified fingerprint.
2. In the following, the user is prompted to enter the certificate.
3. After entering the certificate, it is then imported.
4. In the following, the user is prompted to enter the private key.
5. Following the input, the key is checked.
6. In the following, the user is prompted to enter the CA certificate chain. The end of the input is not detected automatically. After the last certificate, the end is determined by entering endcachain. Type this command on a new line, because all of the input on a line containing the string **endcachain** is discarded.
7. Following these entries, the CA certificates are imported and the process is completed.

1.7 FirmSafe

1.7.1 Toggling the active firmware via console command

As of HiLCOS 10.12, the current firmware can be switched over to the alternative firmware with a CLI command. The previously inactive firmware is set to "active" and the previously active firmware is set to "inactive". After entering the command, the device automatically executes a restart without further confirmation.

Under **/ Firmware**, enter the command `do switch-firmware`.

The restart is performed automatically.

1.7.2 Additions to the Firmware menu

Switch firmware

This command line is used to switch the active firmware into the inactive state. Correspondingly, the alternative, non-active firmware is switched to the active state.

The device restarts automatically and immediately starts using the alternative firmware. By switching again, you restore the initial state.

SNMP ID:

3.8

Telnet path:

Firmware

Possible values:

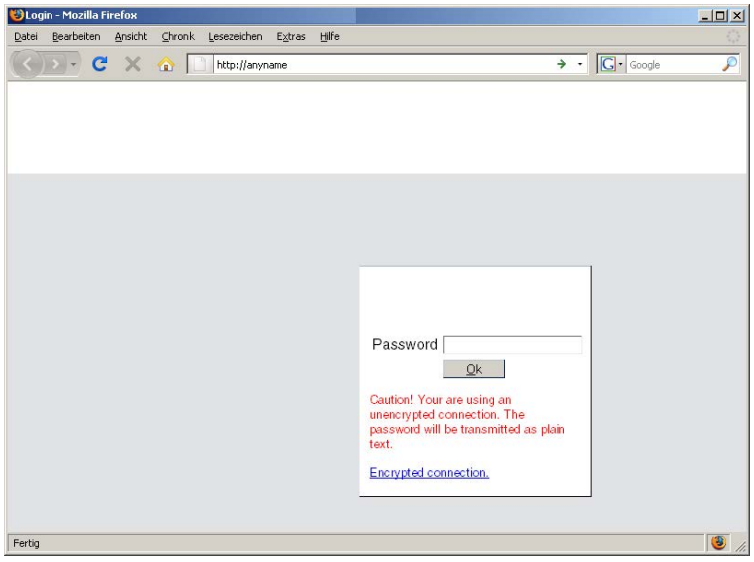
`do Switch-Firmware`

Switch the firmware and restart the device

1.8 Network without a DHCP server

In a network without a DHCP server, unconfigured Hirschmann devices enable their own DHCP server service when switched on and assign IP addresses, information on gateways, etc. to other computers in the LAN (provided they are set to automatic retrieval of IP addresses – auto DHCP). In this constellation, the device can be accessed by every computer with the auto DHCP function enabled with a Web browser under IP address **172.23.56.254**.

With the factory settings and an activated DHCP server, the device forwards all incoming DNS requests to the internal Web server. This means that a connection can easily be made to set up an unconfigured device by entering any name into a Web browser.



If the configuration computer does not retrieve its IP address from the Hirschmann DHCP server, it determines the current IP address of the computer (with **Start** / **Run** / **cmd** and command **ipconfig** at the prompt under Windows 2000 or Windows XP, with **Start** / **Run** / **cmd** and command **winipcfg** at the prompt under Windows Me or Windows 9x or with command **ifconfig** in the console under Linux). In this case, the device can be accessed with address **x.x.x.254** (the "x"s stand for the first three blocks in the IP address of the configuration computer).

1.9 Alternative boot config

1.9.1 Introduction

The way that a Hirschmann device operates is determined by its configuration. The configuration is defined by the user and stored to a special portion of the flash memory that remains intact even when the device is restarted (configuration memory). When shipped, the configuration memory is empty because it does not yet have a user-defined configuration. Once in operation, the configuration memory can be deleted again by carrying out a configuration reset. If a device with

an empty configuration memory is restarted or rebooted, the parameter values are taken from a boot configuration containing default values for the respective model.

A configuration is only written to the configuration memory if at least one parameter has been changed. The full configuration is written to the configuration memory. Even if only the device name is changed, current values for all of the parameters available to the device are stored to the user-defined configuration. Values for unchanged parameters are taken from a boot configuration.

Hirschmann devices can make use of three different boot configurations:

- Hirschmann factory settings: These are the default values for the model as shipped, i.e. the Hirschmann standard. The standard boot configuration is contained in the device's firmware.
- Customer-specific standard settings: These are the customer's own standard settings for the model in question. These are used when the configuration memory is empty but the Hirschmann default settings should not be used. This function provides Hirschmann devices with persistent settings (i.e. remaining available however many times the device is rebooted or reset) that contain customer-specific standard settings for the boot procedure. Customer-specific standard settings are **not** deleted by a configuration reset. Customer-specific standard settings are stored to the first boot memory space.
- Rollout configuration: This configuration is useful for large-scale rollout scenarios where multiple devices need a boot configuration that differs from the Hirschmann default configuration. The rollout configuration is activated by pressing the reset key for a particular length of time. The specialized rollout configuration is stored to the second boot memory space.

1.9.2 Using the boot configuration

When started normally, the Hirschmann devices try to use the available configurations in a set order:

- User-defined configuration (in the configuration memory)
- Customer-specific standard settings (in the first boot memory space)
- Hirschmann factory settings (in firmware)

The customer-specific standard settings are taken automatically and in preference to the Hirschmann factory settings, assuming that the configuration memory is empty.

The rollout configuration is activated with the reset button. The reset button fulfills various functions depending upon how long the button is pressed:

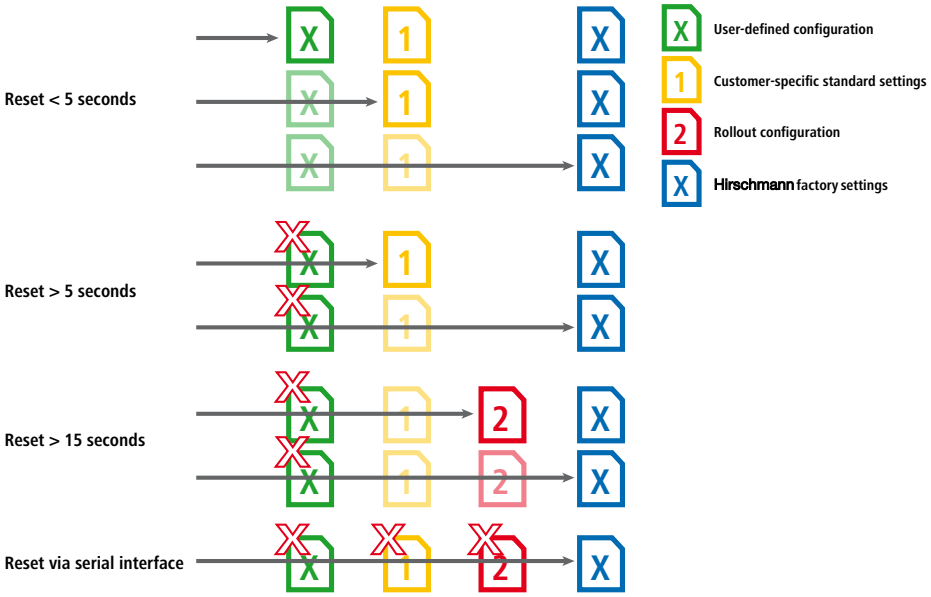
- Less than 5 seconds: Boot (restart), whereby the user-defined configuration is loaded from the configuration memory. If the user-defined configuration is empty, then the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. Similarly, the Hirschmann factory settings are loaded if the first memory space is empty.
- Longer than 5 seconds until the **first** time that all device LEDs light up: Configuration reset (deletes the configuration memory) followed by a restart. In this case the customer-specific standard settings (first memory space) are loaded instead. The loading of the customer-specific standard settings is visible when all LEDs on the device light up briefly in red. The Hirschmann factory settings are loaded if the first memory space is empty.
- Longer than 15 seconds until the **second** time that all device LEDs light up: Activating the rollout configuration and deleting the user-defined configuration After restarting, the rollout configuration is started from the second memory space. The loading of the rollout configuration is visible when all LEDs on the device light up twice briefly in red. The Hirschmann factory settings are loaded if the second memory space is empty.

The rollout configuration is activated directly after restarting if the reset button is pressed for more than 15 seconds. The next time the device is restarted, the normal boot sequence applies again automatically (user-defined configuration, customer-specific standard settings, Hirschmann factory settings).

If the reset button has been deactivated in the configuration (set to 'Ignore' or 'Boot only'), it is impossible to load the rollout configuration.

The following diagram illustrates which configuration is loaded by the different reset procedures, depending on the status of the device. Examples:

- If the button is pressed for less than 5 seconds, the user-defined configuration is loaded. If this is not available, then the customer-specific standard settings are loaded. If this is not available then the Hirschmann factory settings are loaded.
- If the reset button is pressed for more than 15 seconds then the user-defined configuration is loaded. If this is not available then the rollout configuration is loaded. if this is not available then the Hirschmann factory settings are loaded.



1.9.3 Storing and uploading the boot configurations

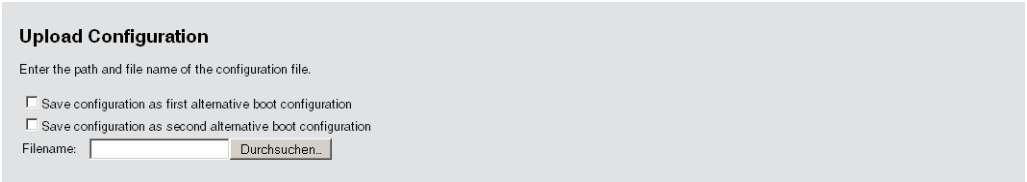
The customer-specific standard settings and the rollout configuration are saved in a compressed format. By means of the command line function, the current device configuration can be saved as customer-specific standard settings or as a rollout configuration. Use the following command for this:

1. `bootconfig -savecurrent [1,2, all]` or `bootconfig -s [1,2, all]`

Entering the appropriate number ensures that either the first boot memory space for the customer-specific standard settings is selected, or the second boot memory space for the rollout configuration. The parameter "all" writes the current configuration to both memory spaces at the same time.

WEBconfig can also be used to upload customer-specific settings or the rollout configuration into the device:

- WEBconfig: HiLCOS menu tree / File management / Upload configuration



Here you select the configuration file to be used and you activate the purpose as either customer-specific standard settings and/or rollout configuration.

1.9.4 Deleting the boot configuration

The alternative and the special boot configurations cannot be deleted with the normal file functions. Use the following command for this:

1. `bootconfig -remove [1,2, all]` or `bootconfig -r [1,2, all]`

Selecting the appropriate number ensures that the corresponding boot memory space is selected. The parameter "all" causes both memory spaces to be deleted at once.

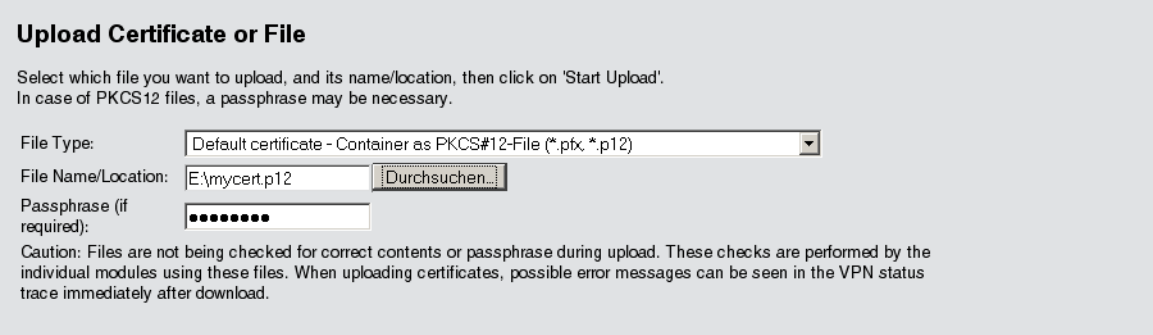
1.9.5 Working with certificates

In order for VPN and SSL/TLS to function after a configuration reset, a standard certificate can be stored to the device as a PKCS#12 container. This standard certificate is only used by the customer-specific standard settings and the rollout configuration.

- If the customer-specific standard settings are loaded, the standard certificate is copied to the normal certificate storage location for VPN and SSL/TLS. This ensures that it remains available even after rebooting.
- If the rollout configuration is loaded, the standard certificate for VPN is used, but it is not copied. This means that in case of a restart (even without a configuration reset) the device has no access to the certificate.

You can upload the standard certificate into the device with WEBconfig.

- WEBconfig: HiLCOS menu tree / File management / Upload certificate or file



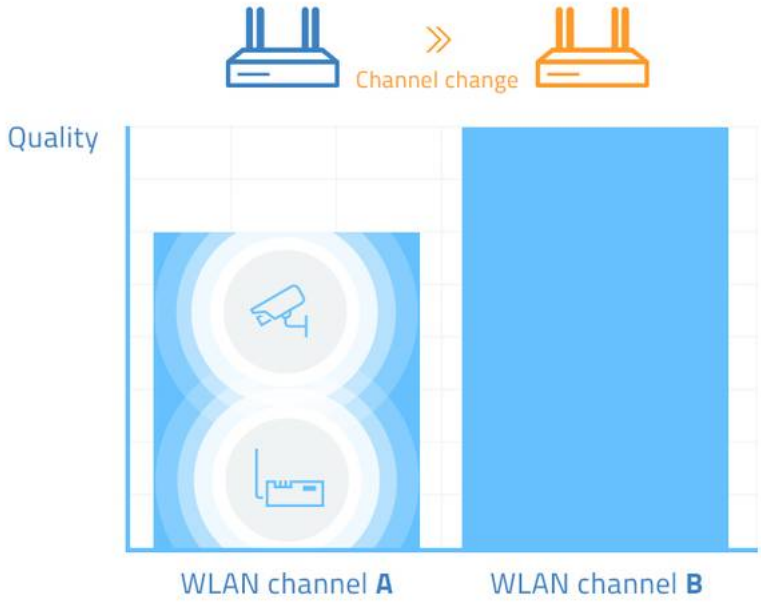
Select the certificate and commence the upload with **Start upload**.

2 WLAN

2.1 Adaptive RF Optimization

Improved WLAN throughput due to dynamic selection of the best WLAN channel by the access point in case of interference.

Choosing a WLAN channel specifies which part of the frequency band is used by an access point for its logical WLANs.
To ensure the flawless operation of a WLAN within range of another access point, each of the access points should be using a separate channel—otherwise the WLANs have to share the medium. For this purpose, Hirschmann access points use the feature Adaptive RF Optimization: The access point permanently scans the radio field for interfering signals. If a threshold is exceeded on the current WLAN channel (by means of the "wireless quality indicators"), the access point automatically switches to a qualitatively better channel. This intelligent feature enables the access point to dynamically adapt to an ever-changing radio field in order to maximize the WLAN's stability.

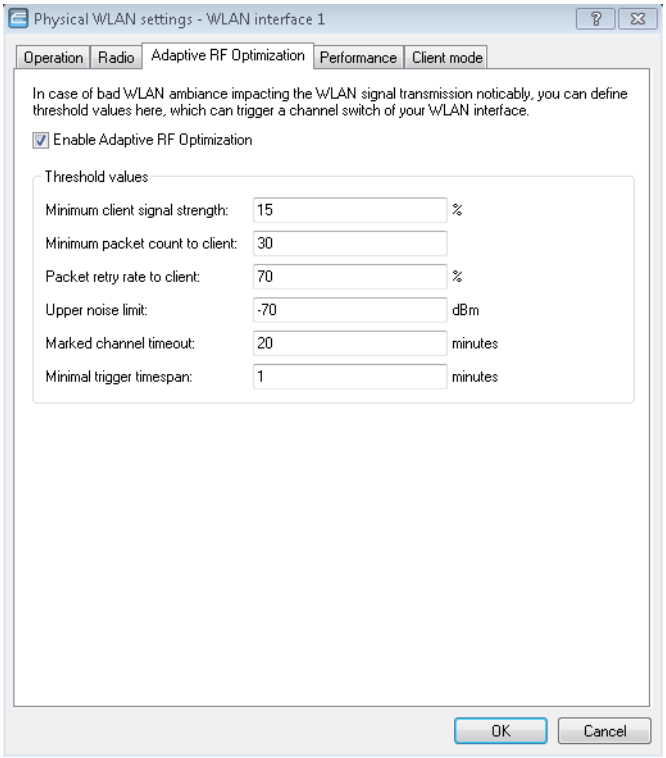


In LANconfig you have the option to manually configure the different thresholds that are used as the basis for an automatic channel change.

2.1.1 Setting up Adaptive RF Optimization with LANconfig

In order to use LANconfig to configure the function Adaptive RF Optimization, it is necessary for the devices that you want to configure to offer the feature "Wireless Quality Indicators". Further information about WQI is available in the reference manual.

To configure Adaptive RF Optimization, open LANconfig and go to **Wireless LAN** > **General**. In the "Interfaces" section, click on **Physical WLAN settings**. Select the WLAN interface you want to configure and go to the tab **Adaptive RF Optimization**.



Enable Adaptive RF Optimization

To enable monitoring of the WLAN radio field via Adaptive RF Optimization, check the box **Enable Adaptive RF Optimization**.

You then configure the thresholds that trigger automatic channel changes.

Minimum client signal strength

Setting for the minimum client signal strength. Clients with a lesser signal strength are not considered at the next evaluation and cannot trigger a channel change. The value is set in % with a default of 15).

Minimum packet count to client

Setting for the minimum number of packets sent to a client (TX). Clients with a lesser signal strength are not considered at the next evaluation and cannot trigger a channel change (default value: 30).

Packet retry rate to client

Setting for the upper limit of packets that are resent to a client. If a client receives a proportion of resent packets that exceeds this percentage value, the device will consider this client the next time the need for a channel change is evaluated. The value is set in % with a default of 70).

Upper noise limit

Setting for the upper limit of acceptable noise on the channel. The value is set in dBm with a default of -70).

Marked channel timeout

If a channel is considered unusable, it will be marked/blocked for the length of time specified here. This value also blocks the channel change trigger in case all channels have been blocked. The value is set in minutes (default value: 20).

Minimal trigger timespan

Here you specify for how long a limit is exceeded continuously before an action is triggered. The timer is reset if no limits are exceeded for a period of 20 seconds. If a limit is exceeded for the entire time span, the current channel is blocked/marked. The value is set in minutes (default value: 1).

For this setting we recommend small single-digit values.

2.1.2 Additions to the Setup menu

Adaptive-RF-Optimization

Adaptive RF Optimization constantly monitors the WLAN environment and evaluates the quality of the network based on the "Wireless Quality Indicators". If the quality drops, the Adaptive RF Optimization triggers a change to a better suited channel.

SNMP ID:

2.23.20.23

Telnet path:

Setup > **Interfaces** > **WLAN**

Ifc

Shows the interface for the Adaptive RF Optimization.

SNMP ID:

2.23.20.23.1

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Operating

Activates or deactivates Adaptive RF Optimization for this interface.

SNMP ID:

2.23.20.23.2

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

No
Yes

Default:

No

Min-Client-Phy-Signal

Setting for the minimum signal strength of clients.

SNMP ID:

2.23.20.23.3

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

Max. 3 characters from `[0-9]`

Default:

15

Min-Client-Tx-Packets

Setting for the minimum number of packets sent to a client.

SNMP ID:

2.23.20.23.4

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

Max. 5 characters from `[0-9]`

Default:

30

Tx-Client-Retry-Ratio-Limit

In this field you specify how quickly a packet is resent to a client.

SNMP ID:

2.23.20.23.5

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

Max. 3 characters from `[0-9]`

Default:

70

Noise-Limit

Setting for the upper limit of acceptable noise on the channel.

SNMP ID:

2.23.20.23.6

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

Max. 6 characters from `[0-9]-`

Default:

-70

Marked-Channel-Timeout

When a channel is considered unusable it is marked/blocked for the time specified here.

SNMP ID:

2.23.20.23.7

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

Max. 5 characters from `[0-9]`

Default:

20

Trigger-Timespan

The trigger timespan set here determines how long a limit is continuously exceeded before an action is triggered.

SNMP ID:

2.23.20.23.8

Telnet path:

Setup > **Interfaces** > **WLAN** > **Adaptive-RF-Optimization**

Possible values:

Max. 5 characters from `[0-9]`

Default:

1

2.2 Managed RF Optimization

As of HiLCOS 10.12, you have the option to allow the APs in your WLAN environment to perform automatic channel selection.

2.2.1 Managed RF Optimization

Automatic channel selection ensures that the devices always operate with the best available channels. Managed RF Optimization allows you to instruct an AP to find the appropriate channel with a simple press of a button. A prerequisite for this is the Inter Access Point Protocol (IAPP), which allows the APs to communicate with one another.

APs use the IAPP protocol to communicate and pass information about the handovers of associated WLAN clients which are roaming. APs regularly send out multicast announcements to inform the devices about the BSSIDs and IP addresses of the other APs. A roaming WLAN client informs a new AP about its former AP. The AP uses the information supplied by the IAPP protocol to inform the former AP to remove the WLAN client from its list of associated clients.

You can initiate channel selection either manually or you can let the devices perform it automatically.

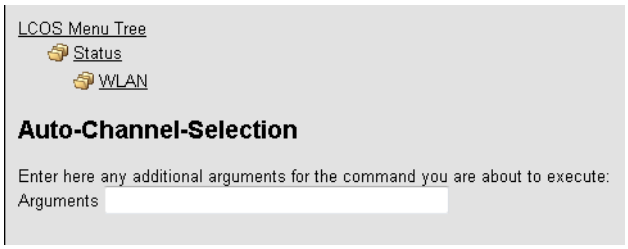
After receiving the command to execute automatic channel selection, each AP performs the following actions:

- The relevant WLAN is disabled.
- The AP sets its priority based on the IAPP table.
- The AP waits for a specified period of time (priority * waiting time (10 seconds)).
- The AP reactivates the relevant WLAN.
- The AP performs an automatic channel selection.

Each AP in the same network searches for the optimal channel in a particular order. This ensures that not all devices commence their channel selection at the same time.

Enabling channel selection via the status menu

To enable channel selection via the status menu, use the HiLCOS menu tree to navigate to **Status** > **WLAN** > **Auto channel selection**.



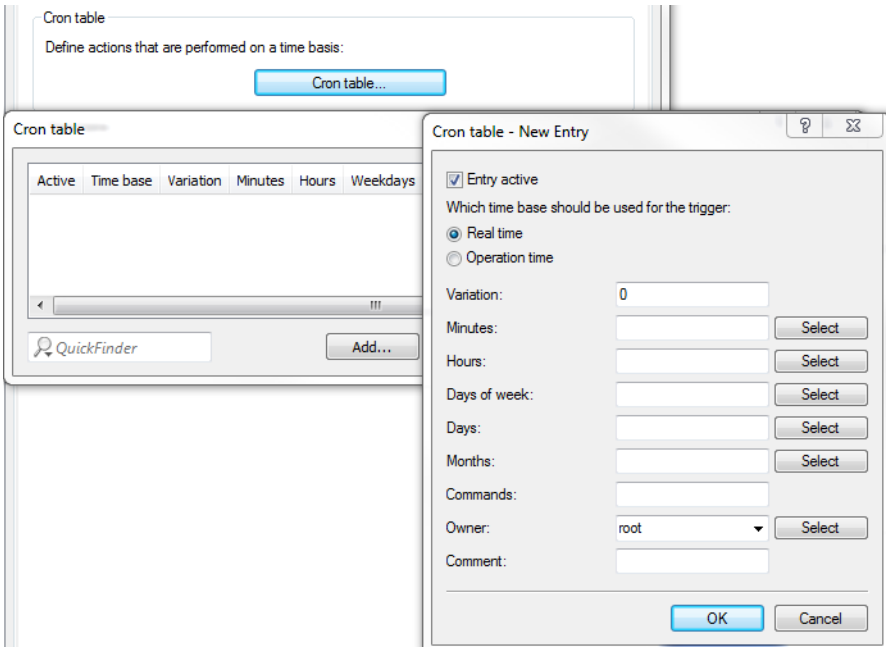
Specify a WLAN interface (e.g. WLAN-1) that should select a new channel and then click **Execute**.

Please note that channel switching only takes place on this specific device!

Enter the parameter "*" in order to prompt all interfaces to search for a new channel.

Setting up Managed RF Optimization with LANconfig

To configure automatic channel selection, open LANconfig and go to **Date & Time** > **General**. In the "Cron table" section, click **Cron table** and add a new entry.



Specify the properties of the new cron job.

Entry active

Activates or deactivates the current entry.

Real time

Select real time as the time base for the cron job.

The real time must be valid, otherwise the commands will not be executed.

Operation time

Select operation time as the time base for the cron job.

If you select operation time, the only fields in the cron table that are evaluated are the hours and minutes.

Variation

This setting is used to generate a random value by which the action is delayed in minutes.

If this value is left at the default setting of "0", the actions are performed at the specified time. There is no variation.

Minutes

Specify the minutes of the time when the command is executed.

Hours

Specify the hours of the time when the command is executed.

Days of week

Specify the weekdays on which the command is executed.

Days

Specify the all of the days of the month on which the command is executed.

Months

Specify the all of the months of a year when the command is executed.

Commands

Enter the command for the channel selection here.

```
do /Status/WLAN/Auto-Channel-Selection [Interface-Name]
```

The following interface names are available: "WLAN-1", "WLAN-2" or "*" for both interfaces.

Owner

By specifying an owner, the action is executed with the associated rights.

Comment

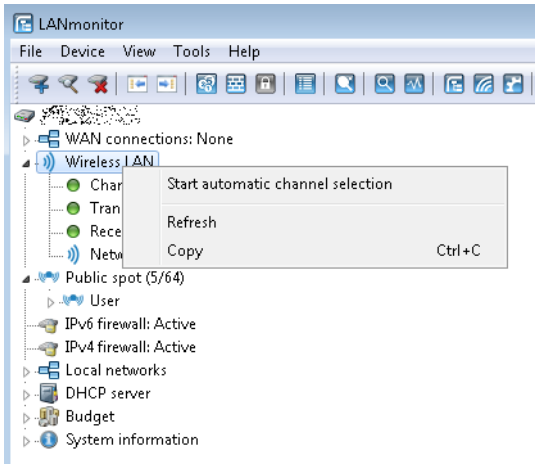
Enter a descriptive comment here.

Please note that channel switching only takes place on this specific device!

For multiple APs within a WLAN environment, channel optimization is best managed by means of a script on the WLC, which is rolled-out to the individual APs on the network.

Manual channel change in LANmonitor

LANmonitor gives you the option to instruct each AP in the network to manually perform a channel change. Go to the **Wireless LAN** view. Right-click with the mouse on the interface that you want to perform a channel change and, in the submenu, select **Perform automatic channel selection**.

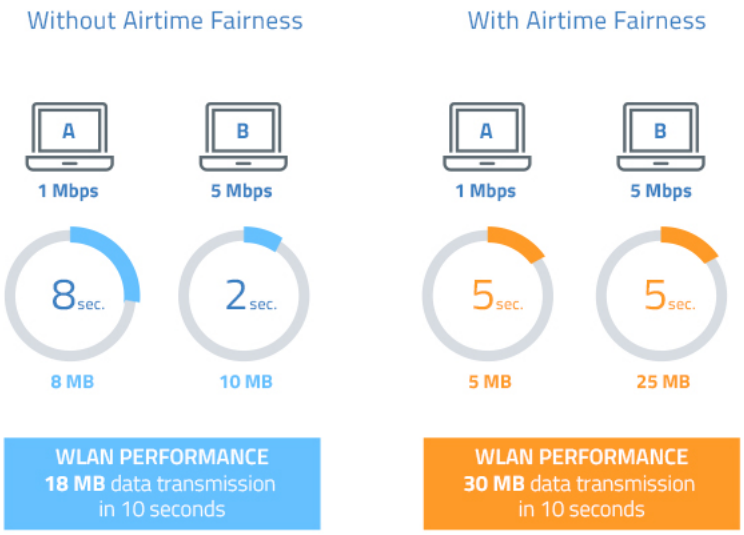


Please notice that you do not receive feedback about the channel change.

2.3 Airtime Fairness

By fairly sharing the WLAN transmission time between all of the active clients, the available bandwidth is used to maximum effect and WLAN performance is improved.

Especially in WLAN scenarios with a high client-density, the devices have to compete for the available bandwidth. Here, the AP offers transmission slots to each of the clients in turn—without any consideration for the necessary transmission times. Legacy clients end up slowing down faster clients, even though the faster ones could complete their data transmission more quickly. The feature "Airtime Fairness" ensures that the available bandwidth is used efficiently. To this end, the WLAN transmission time ("airtimes") is fairly distributed between the active clients. The consequence: Thanks to all clients being provided with the same airtime, faster clients can achieve more data throughput in the same amount of time.

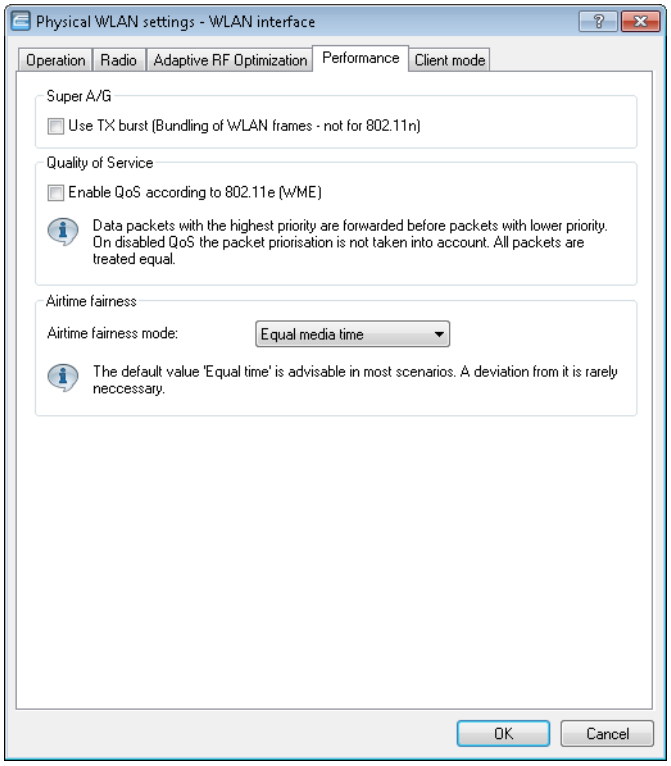


"Airtime" refers to the WLAN transmission time. Airtime Fairness provides WLAN transmission time to all of the active clients according to the mode configured for the Airtime Fairness. This, for example, stops older clients from slowing down more modern clients.

For devices with WLAN modules supporting the IEEE 802.11ac standard, the **Airtime Fairness** feature is automatically enabled in the WLAN module.

2.3.1 Setting up Airtime Fairness with LANconfig

Go to **Wireless LAN** > **General**. In the **Interfaces** section, click on **Physical WLAN settings**. Select the WLAN interface you want to configure, and go to the tab **Performance**.



In the section **Airtime fairness mode** you select the Airtime Fairness operating mode:

Round robin scheduling

Each client receives a time slot for transmission, one after the other.

Equal media time

All clients will receive the same airtime. Clients with a higher data throughput benefit from this setting because they can transmit a greater amount of data to the access point in a given amount of time.

IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

802.11n preferred

This setting prefers clients using IEEE 802.11n. Clients using IEEE 802.11a or IEEE 802.11g only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b only receive 6.25% airtime. The result is that data is sent a lot faster to clients using IEEE 802.11n.

Equal media volume

This setting distributes the airtime between the clients to ensure that all clients will receive the same amount of throughput by the access point. However, slower clients will slow down the other clients.

This setting is only recommended where it is necessary for all clients to receive the same throughput.

2.3.2 Additions to the Setup menu

Airtime-Fairness-Mode

Airtime Fairness is a feature that shares the available bandwidth fairly between all of the active clients. Especially useful in high-density environments, it results in an improvement to WLAN performance. **Airtime Fairness** is activated by default.

SNMP ID:

2.23.20.9.6

Telnet path:

Setup > **Interfaces** > **WLAN** > **Performance**

Possible values:

Round-Robin

Each client in turn receives a time slot for transmission.

Equal-Airtime

All clients will receive the same airtime. Clients with a higher data throughput benefit from this setting because the access point can send more data to the client in the same amount of time.

IEEE 802.11ac WLAN modules already use an algorithm similar to this setting.

Pref.-11n-Airtime

This setting prefers clients that use IEEE 802.11n. Clients using IEEE 802.11a or IEEE 802.11g will only receive 25% of the airtime of an IEEE 802.11n client. Clients using IEEE 802.11b only receive 6.25% airtime. The result is that data is sent much faster to clients using IEEE 802.11n.

Equal-Volume

This setting distributes the airtime between the clients to ensure that all clients receive the same amount of throughput by the access point. However, slower clients will slow down all clients.

This setting is only recommended when it is necessary for all clients to receive the same throughput.

Default:

Equal-Airtime

2.3.3 Additions to the Status menu

Powersave-Retransmits

For each packet deferred by an Airtime Fairness mode the counter increases by 1.

SNMP ID:

1.3.54.29

Telnet path:

Status > **WLAN** > **Errors**

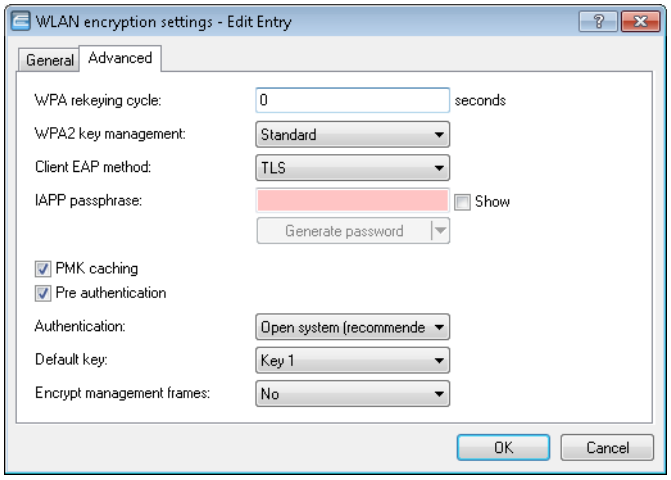
2.4 Encrypted OKC via IAPP

As of HiLCOS 10.12, it is possible to use OKC (opportunistic key caching) in networks that are managed by Industrial HiVision.

2.4.1 Encrypted OKC via IAPP

By setting an IAPP passphrase (PMK-IAPP secret) on an AP, it is possible to transfer the encrypted PMK (pairwise master key) to the other APs and store it there.

In LANconfig, the IAPP passphrase is entered under **Wireless LAN** > **802.11i/WEP** and clicking on **WLAN encryption settings**. Open the configuration dialog box for the appropriate interface and switch to the **Advanced** tab.



2.4.2 Additions to the Setup menu

PMK-IAPP-Secret

Networked APs exchange data about associated WLAN clients by means of the IAPP, so ensuring that the WLAN clients can roam securely in controller-less WLAN networks that are managed by Industrial HiVision.

The AP uses this passphrase to encrypt the PMK and to calculate the mobility domain of the respective WLAN client.

Any value other than 0 automatically triggers an exchange of the master secrets between the relevant APs.

SNMP ID:

2.23.20.3.20

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Special values:

empty

OKC via IAPP is disabled.

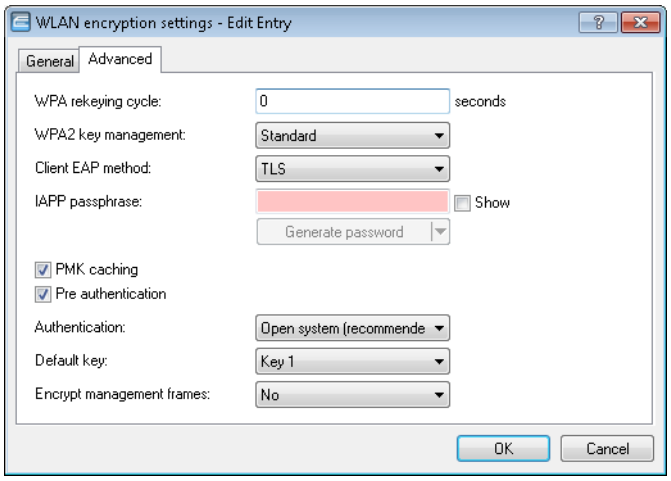
2.5 Fast roaming

As of HiLCOS 10.12, it is possible to operate Fast Roaming (IEEE 802.11r) in networks that are managed by Industrial HiVision.

2.5.1 Fast roaming with IAPP

In order to use fast roaming with IAPP, you need to assign an individual IAPP passphrase in the WLAN encryption settings for each interface. This is used to encrypt the pairwise master keys (PMKs). APs that share a matching IAPP passphrase (PMK-IAPP secret) are able to exchange PMKs between themselves and ensure uninterrupted connections.

In LANconfig, the IAPP passphrase is entered by navigating to **Wireless LAN** > **Encryption** and then clicking on **WLAN encryption settings**. Open the configuration dialog box for the appropriate interface and switch to the **Advanced** tab.



Please note the use of IEEE 802.11r requires **WPA2 key management** in the encryption settings to be set to “Fast roaming”.

2.5.2 Additions to the Setup menu

PMK-IAPP-Secret

Networked APs exchange data about associated WLAN clients by means of the IAPP, so ensuring that the WLAN clients can roam securely in controller-less WLAN networks that are managed by Industrial HiVision.
The AP uses this passphrase to encrypt the PMK and to calculate the mobility domain of the respective WLAN client.
Any value other than 0 automatically triggers an exchange of the master secrets between the relevant APs.

SNMP ID:

2.23.20.3.20

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Special values:

empty

OKC via IAPP is disabled.

2.6 Status counters for failed WPA-PSK/IEEE 802.1X login attempts

As of HiLCOS 10.12, you have the option to display the number of failed login attempts for WPA and IEEE 802.1X.

2.6.1 Status counters for WPA-PSK login attempts

An overview of the number of failed WPA-PSK login attempts is located in the HiLCOS menu tree under **Status** > **WLAN** > **Encryption**.

There is also an overview of successful login attempts, as well as the number of authorizations rejected due to an incorrect passphrase.

Encryption

Interface	Encryption	Method	WPA-Version	WPA1-Session-Keytypes	WPA2-Session-Keytypes	PMK-Caching	Pre-Authentication	OKC	Prot.-Mgmt-Frames	WPA2-Key-Management	WPA-PSK-Num-Success	WPA-PSK-Num-Failures	WPA-PSK-Num-Wrong-Passphrase
WLAN-1	Yes	802.11i-WPA-PSK	WPA1/2	TKIP/AES	TKIP/AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-2	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-3	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-4	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-5	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0
WLAN-1-6	Yes	802.11i-WPA-PSK	WPA1/2	TKIP	AES	Yes	Yes	No	No	Standard	0	0	0

Select an interface in the table (e.g. WLAN-1) to display the information for the selected interface.

Encryption

Interface	WLAN-1
Encryption	Yes
Method	802.11i-WPA-PSK
WPA-Version	WPA1/2
WPA1-Session-Keytypes	TKIP/AES
WPA2-Session-Keytypes	TKIP/AES
PMK-Caching	Yes
Pre-Authentication	Yes
OKC	No
Prot.-Mgmt-Frames	No
WPA2-Key-Management	Standard
WPA-PSK-Num-Success	0
WPA-PSK-Num-Failures	0
WPA-PSK-Num-Wrong-Passphrase	0

2.6.2 Status counters for IEEE 802.1X login attempts

A table showing the number of accepted and rejected connect requests for each logical interface is located in the HiLCOS menu tree under **Status** > **IEEE802.1x** > **Ports**.

The overview also indicates the number of times the authorization limit was reached for each interface.

Ports

Port	Num-Accept	Num-Reject	Num-ReauthMax-reached
LAN-1	0	0	0
LAN-2	0	0	0
LAN-3	0	0	0
LAN-4	0	0	0
WLAN-1	0	0	0
P2P-1-1	0	0	0
P2P-1-2	0	0	0
P2P-1-3	0	0	0
P2P-1-4	0	0	0
P2P-1-5	0	0	0
P2P-1-6	0	0	0
P2P-1-7	0	0	0
P2P-1-8	0	0	0
P2P-1-9	0	0	0
P2P-1-10	0	0	0
P2P-1-11	0	0	0
P2P-1-12	0	0	0
P2P-1-13	0	0	0
P2P-1-14	0	0	0

2.6.3 Additions to the Status menu

Encryption

This table contains information about the encryption on each interface.

SNMP ID:

1.3.64

Telnet path:

Status > **WLAN**

WPA-PSK-Num-Wrong-Passphrase

Displays the number of WPA requests that failed on this interface due to an incorrect passphrase.

SNMP ID:

1.3.64.20

Telnet path:

Status > **WLAN** > **Encryption**

WPA-PSK-Num-Success

Displays the number of successful WPA requests on this interface.

SNMP ID:

1.3.64.21

Telnet path:

Status > **WLAN** > **Encryption**

WPA-PSK-Num-Failures

Displays the number of failed WPA requests on this interface.

SNMP ID:

1.3.64.22

Telnet path:

Status > **WLAN** > **Encryption**

Ports

This table provides an overview of the accepted or rejected connection requests for each logical interface.

SNMP ID:

1.46.3

Telnet path:

Status > **IEEE802.1x**

Port

Displays the name of the interface.

SNMP ID:

1.46.3.1

Telnet path:

Status > **IEEE802.1x** > **Ports**

Num-accept

Displays the number of successful WPA requests on this interface.

SNMP ID:

1.46.3.2

Telnet path:

Status > **IEEE802.1x** > **Ports**

Num-reject

Displays the number of failed WPA requests on this interface.

SNMP ID:

1.46.3.3

Telnet path:

Status > **IEEE802.1x** > **Ports**

Num-ReauthMax-reached

SNMP ID:

1.46.3.4

Telnet path:

Status > **IEEE802.1x** > **Ports**

2.7 Adaptive transmission power

As of HiLCOS 10.12, the failure of any APs on the network can be automatically compensated for by increasing the transmission power of the other APs.

2.7.1 Adaptive transmission power

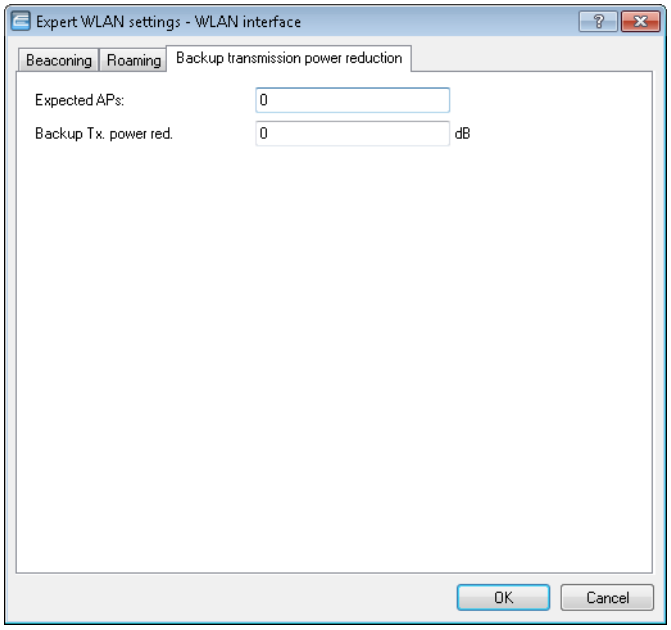
Dynamic transmission power adaptation is an essential feature for WLAN environments with professional backup scenarios. If an AP fails, the remaining access points automatically increase their transmission power to ensure full WLAN coverage at all times.

To do this, specify how many APs operate within a broadcast domain. So long as all of the devices are available, the transmission power reduction configured here applies to all of the APs in this group (e.g. -6 dB). Using IAPP (Inter Access Point Protocol), the APs continually check that the correct number of APs is present on the network.

If an AP fails, the check reveals that the actual number number of APs does not equal the expected number, and so the remaining APs activate the backup transmission power reduction as configured (e.g. 0 dB). As soon as the failed AP is available again, the actual number of APs becomes equal to the expected number of devices. The other APs return their transmission power to the default value.

Setting up Adaptive Transmission Power with LANconfig

To configure this in LANconfig, go to **Wireless LAN** > **General**. In the **Extended settings** section, click the button Expert WLAN settings and, if your AP has multiple WLAN interfaces, select the appropriate one. Go to the **Backup transmission power reduction** tab and enter the number of expected APs and the power reduction.



Expected APs

Specify how many APs operate within a broadcast domain.

Backup TX power red.

Here you specify the transmission power reduction in dB to be applied by the AP if an AP from the configured group is no longer reachable.

The default transmission power reduction is configured under **Wireless LAN** > **General** by clicking the button **Physical WLAN settings** (selecting the WLAN interface, if necessary) and accessing the **Radio** tab.

2.7.2 Additions to the Setup menu

Redundancy settings

In this directory, you configure the dynamic adjustment of transmission power in the event of the failure of an AP a cluster of several APs.

SNMP ID:

2.23.20.24

Telnet path:

Setup > **Interfaces** > **WLAN**

Ifc

The interface that this entry refers to.

SNMP ID:

2.23.20.24.1

Telnet path:

Setup > **Interfaces** > **WLAN** > **Redundancy-Settings**

Other APs expected

Use this item to specify the number of other APs that are located in the AP cluster.

So long as all of the devices are available, the transmission power reduction configured here applies to all of the APs in this group (e.g. -6 dB). Using IAPP (Inter Access Point Protocol), the APs continually check that the correct number of APs is present on the network.

If an AP fails, the check reveals that the actual number number of APs does not equal the expected number, and so the remaining APs activate the backup transmission power reduction as configured (e.g. 0 dB). As soon as the failed AP is available again, the actual number of APs is equal to the number of expected devices. The other APs return their transmission power to the default value.

SNMP ID:

2.23.20.24.2

Telnet path:

Setup > **Interfaces** > **WLAN** > **Redundancy-Settings**

Possible values:

Max. 5 characters from `[0-9]`

Backup transmission power reduction

Here you specify the transmission power reduction in dB to be applied by the AP if an AP from the configured group is no longer reachable.

SNMP ID:

2.23.20.24.3

Telnet path:

Setup > **Interfaces** > **WLAN** > **Redundancy-Settings**

Possible values:

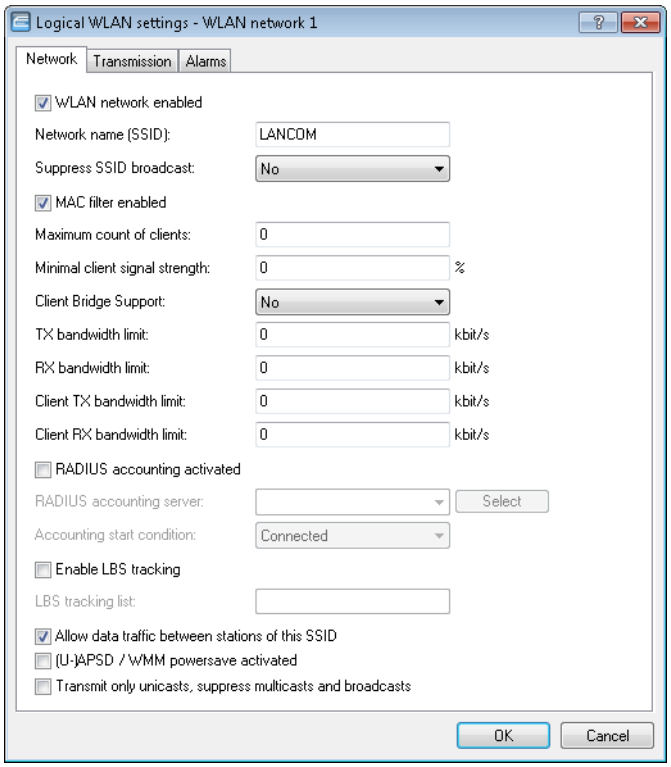
Max. 3 characters from `[0-9]`

2.8 Improved start-up conditions for WLAN RADIUS accounting

As of HiLCOS 10.12, the RADIUS accounting start message is optionally generated only after the client has received a valid IP address. In this case the RADIUS accounting server always receives a valid framed IP address.

In LANconfig, go to the view **Wireless LAN** > **General** > **Logical WLAN settings**. On the tab "Network", enable the check box **RADIUS accounting activated**.

You can now set the accounting start condition with the drop-down menu. The following settings are available.



Accounting-Start-Condition

Normally, the WLAN stack sends a RADIUS "accounting start" message as soon as the WLAN client is connected. Often the WLAN client has no IP address at this time, most likely because one has not yet been issued by the DHCP server. Consequently the `Framed-IP-Address` attribute in the RADIUS accounting message may lack meaningful content.

Connected

Accounting starts when the WLAN client takes on the status "Connected". This is the default setting.

Valid IP address

Accounting starts when the WLAN client receives a valid IP address (IPv4 or IPv6).

Valid IPv4 address

Accounting starts when the WLAN client receives a valid IPv4 address.

Valid IPv6 address

Accounting starts when the WLAN client receives a valid IPv6 address.

APIPA addresses (`169.254.1.0` – `169.254.254.255` and `fe80:`) are not recognized as valid IP addresses.

2.8.1 Additions to the Setup menu

Accounting-Start-Condition

Use this entry to specify when the DHCP server reports the beginning of a billing period to a RADIUS accounting server.

SNMP ID:

2.23.20.1.27

Telnet path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

None

Accounting starts when the WLAN client takes on the status “Connected”.

Valid IP address

Accounting starts when the WLAN client receives a valid IP address (IPv4 or IPv6) from the DHCP server.

Valid IPv4 address

Accounting starts when the WLAN client receives a valid IPv4 address from the DHCP server.

Valid IPv6 address

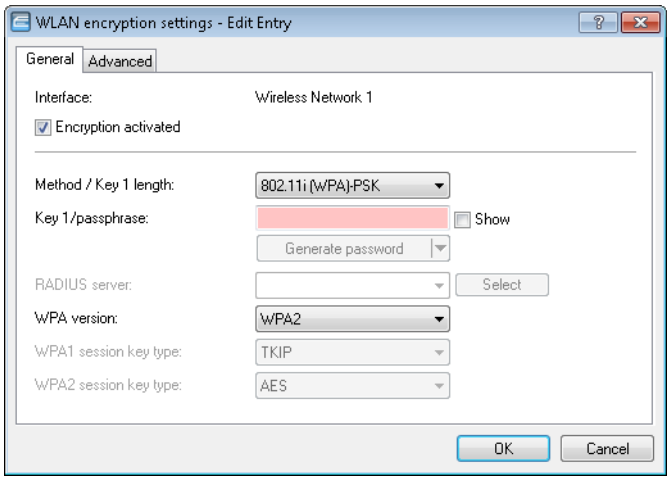
Accounting starts when the WLAN client receives a valid IPv6 address from the DHCP server.

Default:

None

2.9 Selecting a RADIUS server profile for 802.1X authentication

As of HiLCOS 10.12, you have the option of specifying a RADIUS server profile when operating authentication as per the IEEE 802.1X standard.



RADIUS server

If you select an authentication method based on the IEEE 802.1X standard under **Method/Key 1 length**, you specify the profile of a RADIUS server here.

2.9.1 Additions to the Setup menu

RADIUS profile

If you are operating an authentication method based on the IEEE 802.1X standard, you specify the profile of a RADIUS server here.

SNMP ID:

2.23.20.3.21

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

2.10 Configurable data rates per WLAN module

As of HiLCOS 10.12, it is possible to configure the data rates separately for each WLAN module.

2.10.1 Configurable data rates per WLAN module

Some application scenarios may require you to exclude certain data rates, for example where environmental conditions are unfavorable. For this reason it is possible to configure the data rates per SSID or P2P link precisely according to your particular requirements.

In most cases there is no need to change the default settings. Ensure that only WLAN experts adjust these settings, as improper changes may lead to problems with your WLAN network.

By configuring the data rates for each WLAN module, you fix the data rates used by the AP to communicate with its clients (TX) as well as the data rates "announced" by the AP to the client for its communication with the AP (RX).

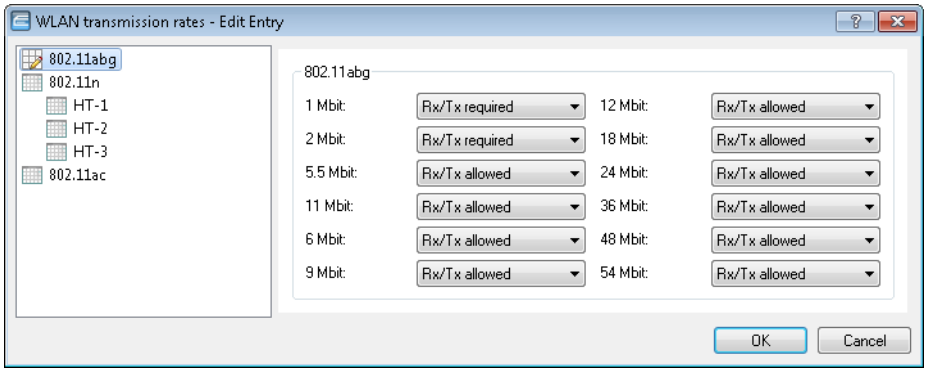
This rate adaptation specifies a minimum and a maximum data rate, and it also allows you to disable certain data rates between these limits.

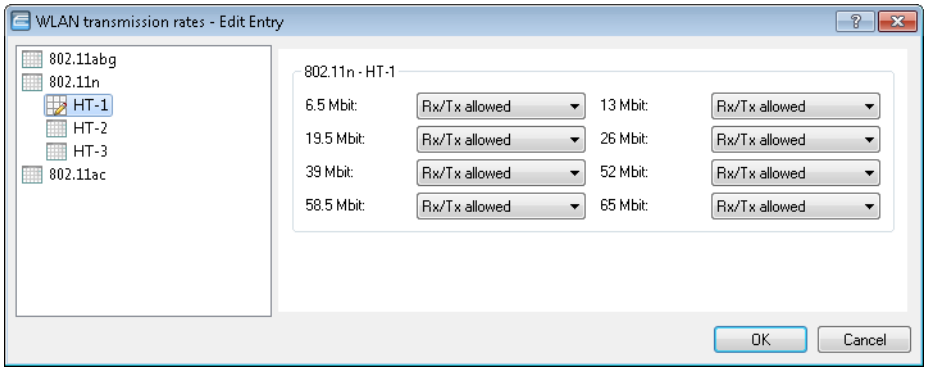
The configuration of data rates is only possible for stand-alone APs. Using this in WLC scenarios requires the use of scripts, which the WLC rolls-out to the APs.

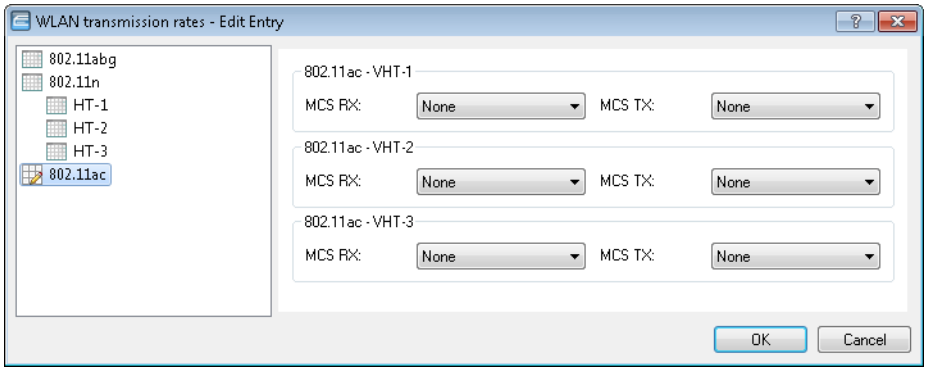
Configuring the data rates with LANconfig

To configure the data rates with LANconfig, switch to the view **Wireless LAN** > **General**, and in the section **Extended settings** open the dialog **WLAN transmission rates**. LANconfig lists the settings for all of the available interfaces. To change the setting for an interface, select its entry and click on **Edit**.

On the left you select the standard that you want to configure.







The configuration can be modified for each of the standards separately

- 802.11abg
- 802.11n
  - HT-1
  - HT-2
  - HT-3
- 802.11ac
  - VHT-1
  - VHT-2
  - VHT-3

Depending on the standard, the following settings are available for each transmission rate and each SSID or P2P link:

Rx/Tx required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx allowed

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx allowed

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Deactivated

The AP does not announce this rate and does not use it to communicate with the client.

MCS-9/8/7

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

None

With 802.11ac modules, the respective stream option is disabled for the corresponding data direction.

2.10.2 Additions to the Setup menu

Rate selection

Some application scenarios may require you to exclude certain data rates, for example where environmental conditions are unfavorable. For this reason it is possible to configure the data rates per SSID or P2P link precisely according to your particular requirements.

In most cases there is no need to change the default settings. Ensure that only WLAN experts adjust these settings, as improper changes may lead to problems with your WLAN network.

By configuring the data rates for each WLAN module, you fix the data rates used by the AP to communicate with its clients (TX) as well as the data rates “announced” by the AP to the client for its communication with the AP (RX).

This rate adaptation specifies a minimum and a maximum data rate, and it also allows certain data rates between these limits to be disabled. This can save airtime under certain circumstances.

The configuration of data rates is only possible for stand-alone APs. Using this in WLC scenarios requires the use of scripts, which the WLC rolls-out to the APs.

In this directory you configure these data rates.

SNMP ID:

2.23.20.25

Telnet path:

Setup > **Interfaces** > **WLAN**

1M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.1

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx-required

2M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.2

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx-required

Ifc

This entry shows which interface is being configured.

SNMP ID:

2.23.20.25.3

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

5.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.4

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

11M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.6

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

6M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.8

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

9M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.9

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

12M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.10

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

18M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.11

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

24M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.12

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

36M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.13

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

48M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.14

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

54M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.15

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-6.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.28

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-13M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.29

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-19.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.30

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-26M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.31

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-39M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.32

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-52M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.33

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-58.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.34

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-1-65M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.35

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-13M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.36

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-26M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.37

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-39M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.38

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-52M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.39

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-78M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.40

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-104M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.41

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-117M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.142

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-2-130M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.43

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-19.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.44

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-39M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.45

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-58.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.46

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-78M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.47

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-117M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.48

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-156M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.49

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is "supported" and "required". The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is "supported". The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is "supported" and "required", but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is "supported", but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-175.5M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.50

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

HT-3-195M

Here you configure how the AP is to handle this data rate for this interface.

SNMP ID:

2.23.20.25.51

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

No

The AP does not announce this rate and does not use it to communicate with the client.

Rx/Tx-required

The AP uses beacons and probe responses to announce to the client that the data rate is “supported” and “required”. The AP also uses this data rate to communicate with the client. If the client does not support a particular rate, the AP will reject a connection request.

Rx/Tx

The AP announces to the client that the rate is “supported”. The AP also uses the rate to communicate with the client. However, the AP also accepts requests from clients that do not support this rate.

Rx-required

The AP announces to the client that the rate is “supported” and “required”, but does not use the rate to communicate with the client.

Rx

The AP announces to the client that the rate is “supported”, but does not use the rate to communicate with the client.

Default:

Rx/Tx

VHT-1-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.105

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-1-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.106

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-2-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.115

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-2-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.116

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-3-Max-Tx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.125

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

VHT-3-Max-Rx-MCS

Here you configure how the AP is to handle this data rate for this interface.

In the case of 802.11ac modules, the data rate per stream option (1, 2 or 3 streams) is restricted to the maximum MCS only.

SNMP ID:

2.23.20.25.126

Telnet path:

Setup > **Interfaces** > **WLAN** > **Rate-Selection**

Possible values:

None
MCS7
MCS8
MCS9

Default:

MCS9

2.11 Maximum length of the AP device name in the WLC config increased to 64 characters

As of HiLCOS 10.12, AP device names in the access point table can be specified using up to 64 characters.

2.11.1 Additions to the Setup menu

Name

Name of the AP in managed mode.

SNMP ID:

2.37.1.4.2

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

2.12 LANconfig: Modified WLAN encryption dialog

In HiLCOS 10.12 the dialog for configuring the WLAN encryption settings has changed.

The WLAN encryption settings in LANconfig are located under **Wireless LAN** > **Encryption**.

2.13 Support for AiRISTA Flow Blink Mode (former Ekahau Blink Mode)

As of HiLCOS 10.12, devices with at least one 11n Wi-Fi module support the AiRISTA Flow Blink Mode.

2.13.1 AiRISTA Flow Blink Mode

Ekahau and their "Real Time Location System" (RTLS) allow you to determine the location of objects and persons within a wireless LAN. This works with special Wi-Fi transmitters known as "Wi-Fi tags" that are located on the device or person's body and which send specially coded Wi-Fi packets. APs located nearby receive these packets, enrich them with additional information (e.g. RSSI), encapsulate them in the "TaZmen Sniffer Protocol" (TZSP) and forward this information to the "Ekahau RTLS Controller" (ERC) installed on the network. The ERC analyzes this data to determine the position of the Wi-Fi tag.

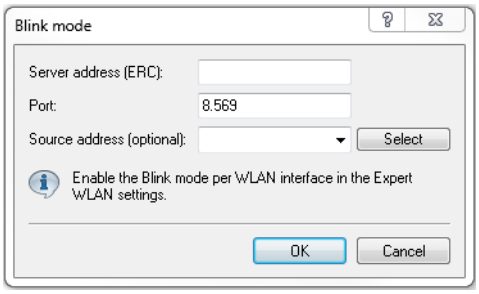
The Wi-Fi tags support three modes for sending the Wi-Fi packets:

- **Associated mode**: In "associated mode" the Wi-Fi tag functions like a Wi-Fi client. It associates with a nearby AP and stays in constant contact with it. While this provides seamless positioning, this mode consumes more power and the battery life of the Wi-Fi tag is reduced. In "associated mode" the Wi-Fi tags use the Ekahau Location Protocol (ELP).
- **Blink mode**: In "blink mode", the Wi-Fi tag transmits short Wi-Fi packets but does not connect to an AP. In "blink mode" the Wi-Fi tags use the "Ekahau Blink Protocol" (EBP).
- **Mixed mode**: In "Mixed mode", the Wi-Fi tags use EBP to send the RSSI and ELP to send status messages to the ERC.

Configuring the AiRISTA Flow Blink Mode with LANconfig

The blink mode only works with 802.11n WLAN modules, not with 802.11ac WLAN modules. Correspondingly, it is not possible to activate the 'blink mode' for 802.11ac WLAN modules in LANconfig. The option is permanently disabled for devices of this type.

To configure access to the RTLS Server (ERC) with LANconfig, open the view **Wireless LAN** > **General** and click the button **Blink mode**.



Server address (ERC)

Enter the address of the ERC. You can enter an IP address or a host name.

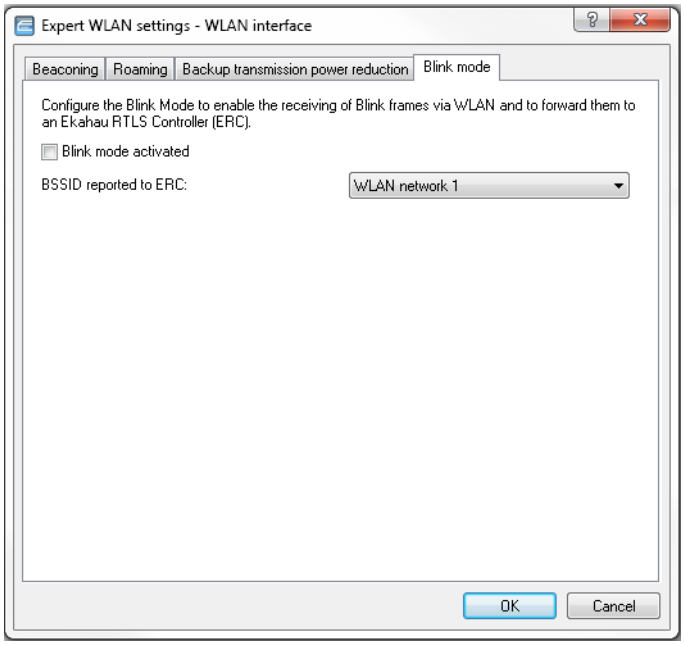
Port

Contains the default UDP port (8569) for communication with the ERC. Change this value only in exceptional cases.

Source address (optional)

Optionally, specify a source address.

To configure the blink mode for each physical WLAN interface, navigate to **Wireless LAN** > **General** and click the button **Expert WLAN settings**. If applicable, select the desired WLAN interface from the drop-down list and switch to the **Blink mode** tab.



Blink mode activated

Enable or disable the blink mode for this interface here.

BSSID reported to ERC

Here you select the logical WLAN interface that the device reports to the ERC.

The ERC "maps" this BSSID to a particular location. For example, if this location were a server room, the ERC knows that Wi-Fi tag "A" is located in the server room as long as the "blink" arrives from the BSSID belonging to the corresponding APs.

2.13.2 Additions to the Setup menu

Blink mode

This menu contains the settings for communications with the RTLS server (Ekahau RTLS Controller, ERC).

SNMP ID:

2.12.131

Telnet path:

Setup > **WLAN**

Server address

Contains the IP address or the DNS name of the RTLS server.

SNMP ID:

2.12.131.1

Telnet path:

Setup > **WLAN** > **Blink-Mode**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~! $%&'()+-,/:;<=>?[\] ^_.`

Default:

empty

Server port

Contains the UDP port number of the RTLS server.

SNMP ID:

2.12.131.2

Telnet path:

Setup > **WLAN** > **Blink-Mode**

Possible values:

Max. 5 characters from `[0-9]`

Default:

8569

Loopback address

Contains the optional source address used by the device instead of the source address that would be automatically selected for this target.

SNMP ID:

2.12.131.3

Telnet path:

Setup > **WLAN** > **Blink-Mode**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]@{|}~! $%&'()+-,/:;<=>?[\] ^_.`

Special values:

Name of the IP networks whose address should be used
"INT"
for the address of the first intranet
"DMZ"
for the address of the first DMZ
LB0 to LBF
for the 16 loopback addresses
Any valid IP address

Default:

empty

Blink mode

In this table, you configure the blink mode for the physical WLAN interfaces.

SNMP ID:

2.23.20.26

Telnet path:

Setup > **Interfaces**

Ifc

Contains the name of the physical WLAN interface.

SNMP ID:

2.23.20.26.1

Telnet path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

WLAN-1
WLAN-2

Operating

Activates or deactivates the blink mode for this physical interface.

SNMP ID:

2.23.20.26.2

Telnet path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

Yes
No

Default:

No

Network

Here you select the logical WLAN interface that the device reports to the ERC.

SNMP ID:

2.23.20.26.3

Telnet path:

Setup > **Interfaces** > **Blink-Mode**

Possible values:

List of the available logical WLAN interfaces 'WLAN-1' to 'WLAN-x'

2.13.3 Additions to the Status menu

Packet transport

This entry contains the packet transport status values.

SNMP ID:

1.3.53

Telnet path:

Status > **WLAN**

2.14 Managing WLAN sessions using RADIUS CoA

As of HiLCOS 10.12, RADIUS CoA (Change of Authorization) allows you to modify the attributes of a current WLAN connection or to terminate the connection using the "disconnect" method.

CoA can be enabled for each WLAN SSID individually. Using the command-line console, the command "`show wlan dynauth`" displays the WLAN sessions currently active on the CoA module

The following WLAN attributes can be modified by RADIUS CoA:

- LCS-TxRateLimit
- LCS-RxRateLimit
- VLAN-ID

The following attributes are required to modify the VLAN ID:

Tunnel-Type=VLAN

This attribute is preset

Tunnel-Medium-Type=IEEE-802

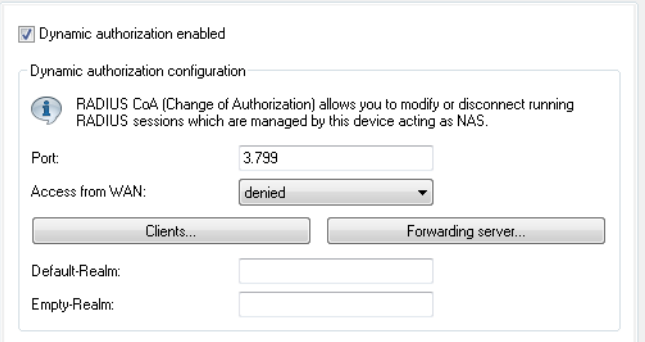
This attribute is preset

Tunnel-Private-Group-Id=42

Specifies a new VLAN ID.

2.14.1 Using LANconfig to configure the management of WLAN sessions using RADIUS CoA

In order to configure dynamic authorization (CoA) with LANconfig, navigate to **RADIUS** > **Dyn. Authorization**.



Dynamic authorization enabled

Activate or deactivate dynamic authorization here.

Port

Contains the default port where CoA messages are received.

Access from WAN

This entry specifies whether messages are accepted from the WAN, via VPN only, or prohibited.

Clients

Enter all of the CoA clients here that are permitted to send messages to the NAS.

Forwarding server

To forward CoA messages, the forwarding servers are specified here.

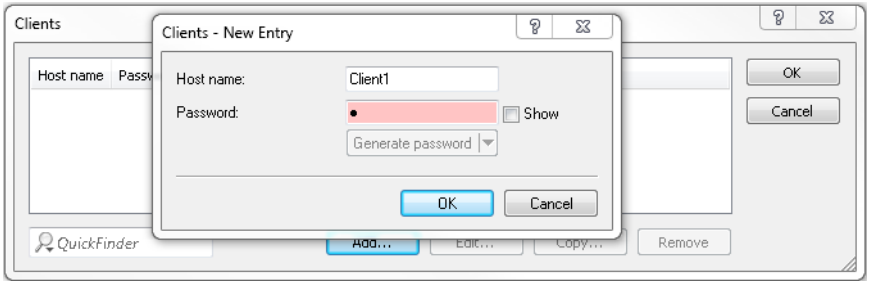
Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

Empty realm

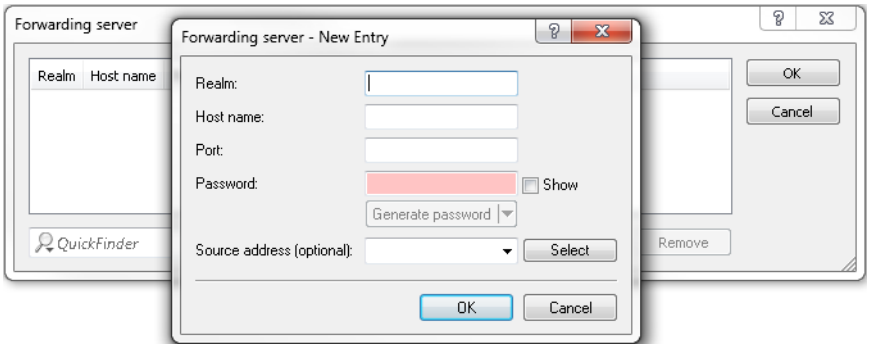
This realm is used when the specified username does not contain a realm.

To add CoA clients for dynamic authorization, click the button **Clients** and add a new entry to the table.



Enter a host name for the client and set a password for the client to access the NAS.

To add new forwarding servers for dynamic authorization, click the button **Forwarding server** and add a new entry to the table.



Realm

Here you enter the realm used by the RADIUS server to identify the forwarding destination.

If applicable, enter any existing forwarding servers that are specified under **RADIUS** > **Server** > **Forwarding** > **Forwarding server**.

Host name

Specify the host name of the forwarding server.

Port

Specify the server port used to forward the requests.

Password

Set a password that is required by the client to access the RADIUS server.

Source address (optional)

Optionally, specify a source address.

Specify which logical WLAN interfaces should use dynamic authorization. You enable or disable them under **Wireless LAN** > **General** > **Logical WLAN settings** with the checkbox **RADIUS CoA activated** for the appropriate interface.

2.14.2 Additions to the Setup menu

Dyn-Auth

This menu contains the settings for dynamic authorization by RADIUS CoA (Change of Authorization). RADIUS CoA is specified in *RFC5176*.

SNMP ID:

2.25.19

Telnet path:

Setup > **RADIUS**

Operating

This entry enables or disables the dynamic authorization by RADIUS.

SNMP ID:

2.25.19.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

No
Yes

Default:

No

Port

This entry specifies the port on which CoA messages are accepted.

SNMP ID:

2.25.19.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 5 characters from `[0-9]`

Default:

3799

WAN access

This entry specifies whether messages are accepted from the LAN, WAN, or VPN.

SNMP ID:

2.25.19.3

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

No
Yes

Default:

No

Clients

All of the CoA clients that send messages to the NAS are entered into this table.

SNMP ID:

2.25.19.4

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

HostName

This entry contains the unique identifier of the client that sends messages to the NAS.

SNMP ID:

2.25.19.4.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Clients**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Secret

This entry specifies the secret required by the client for access to the NAS in the access point.

SNMP ID:

2.25.19.4.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Clients**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Forward-Servers

To forward CoA messages, the forwarding servers are specified here.

SNMP ID:

2.25.19.5

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Realm

This entry contains a string with which the RADIUS server identifies the forwarding destination.

SNMP ID:

2.25.19.5.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

HostName

Here you enter the hostname of the RADIUS server to which the RADIUS client forwards the requests from WLAN clients.

SNMP ID:

2.25.19.5.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Port

This entry contains the port for communications with the forwarding server.

SNMP ID:

2.25.19.5.3

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Secret

This entry specifies the secret required to access the forwarding server.

SNMP ID:

2.25.19.5.4

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Loopback

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

SNMP ID:

2.25.19.5.5

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

SNMP ID:

2.25.19.6

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Empty realm

This realm is used when the specified username does not contain a realm.

SNMP ID:

2.25.19.7

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Radclient

Use the command `do Radclient [...]` to send CoA messages.

The Radclient command is structured as follows:

```
do Radclient <server[:port]> coa/disconnect <secret> <attribute-list>
```

Outputs all known and active RADIUS sessions

Entering the command `show dynauth sessions` on the command line lists the RADIUS sessions that are known to the CoA module. This outputs the session reported by the Public Spot module. The known attributes for this session are shown in the section "Context":

```
Session with MAC-Address: [a3:18:22:0c:ae:df] Context:
[NAS-IP-Address: 192.168.1.254,User-Name: user46909, NAS-Port-Id:
WLC-TUNNEL-1, Framed-IP-Address: 192.168.1.78]
```

The attributes "NAS-IP-Address" and "Username" identify the active session. If you wish to limit the bandwidth for the active session, you enter the Radclient command with these values along with the attributes "LCS-TxRateLimit" and "LCS-RxRateLimit" in combination with the transmission and reception limits in kbps:

do Radclient 192.168.1.254 coa secret
"User-Name=user46909;NAS-IP-Address=192.168.1.254;LCS-TxRateLimit=5000;LCS-RxRateLimit=5000"

Note that the identification attributes and the attributes being modified must be specified with the same rights in the attribute list.

Terminate an active RADIUS session

A running RADIUS session is terminated by using the Radclient command to send a disconnect message:

```
do Radclient 192.168.1.254 disconnect secret
"User-Name=user46909;NAS-IP-Address=192.168.1.254"
```

The Radclient command integrated in HiLCOS is primarily for test purposes. CoA messages are usually sent to the NAS from an external system.

SNMP ID:

2.25.19.8

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Dyn-Auth

This entry enables or disables dynamic authorization by RADIUS CoA on the corresponding interface.

SNMP ID:

2.23.20.1.28

Telnet path:

Setup > **Interfaces** > **WLAN** > **Network**

Possible values:

No
Yes

Default:

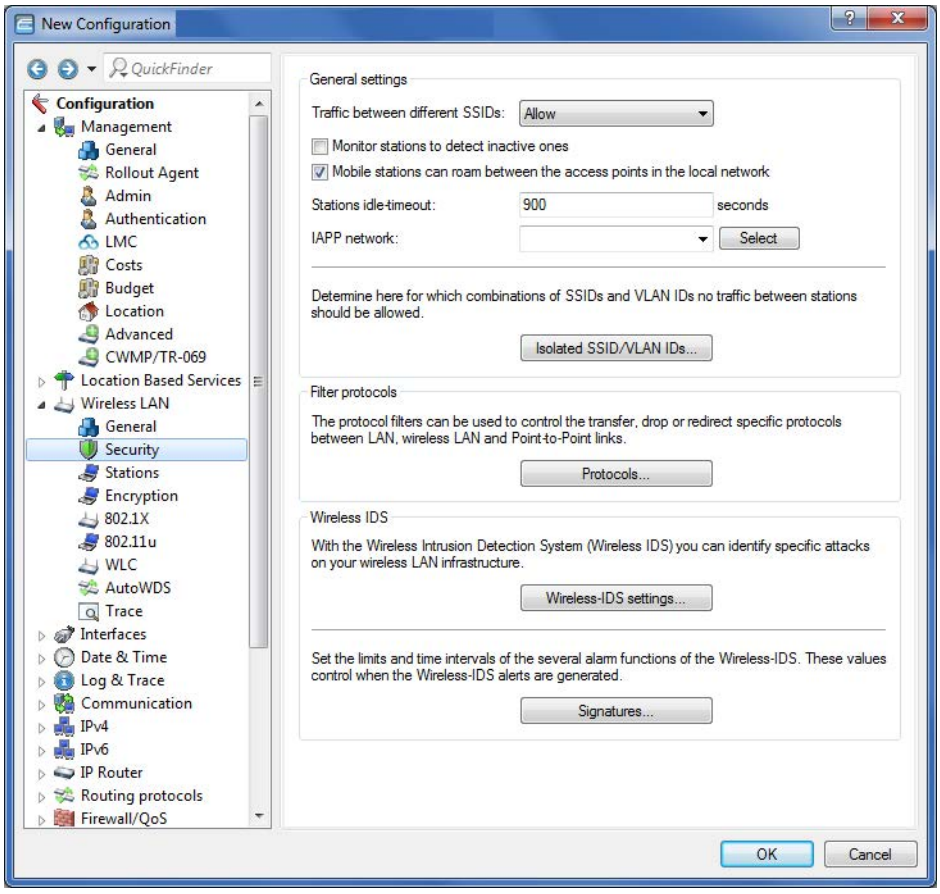
No

2.15 Selectively allowing inter-station traffic for clients on the same VLAN

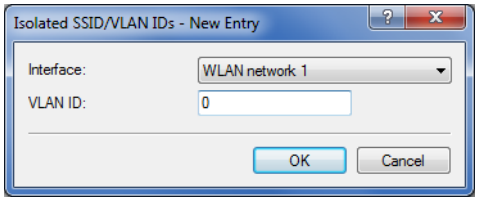
As of HiLCOS 10.12 this feature allows you to map a "collective VLAN" where WLAN clients are unable to communicate with one another. Communication is only possible between WLAN client and AP (hotspot scenario). Outside of this collective VLAN, communication between the clients can be permitted. This works perfectly transparently within a common SSID where the clients are assigned to different VLANs.

2.15.1 Configuration by LANconfig

Navigate to **Wireless LAN** > **Security**.



Add a new entry to the menu **Isolated SSID / VLAN IDs**:



Here you specify the combinations of SSIDs and VLANs between which the traffic between clients is prohibited. This table functions as a blacklist because, generally speaking, we define just a few VLANs where the communication is forbidden, but several where it is allowed.

This mechanism also works when the clients are associated with different APs (although care should be taken to ensure that the table configurations match). A prerequisite for this is that the APs are able to communicate via IAPP.

The table contains the following parameters:

Interface

The list of available WLAN networks.

VLAN-ID

The identification number of the VLAN.

The menu item **Traffic between different SSIDs** must be set to **Allow** in order for this feature to manage the restrictions.

2.15.2 Additions to the Setup menu

VLAN no interstation traffic

This table contains combinations of SSIDs and VLANs for which data exchange between clients should be prohibited.

SNMP ID:

2.12.71

Telnet path:

Setup > **WLAN**

Network

From the list of available SSIDs, select the network for which data exchange between clients should be prohibited.

SNMP ID:

2.12.71.1

Telnet path:

Setup > **WLAN** > **VLAN-No-Interstation-Traffic**

VLAN-ID

Here you specify the VLAN ID for which data exchange between clients should be prohibited.

SNMP ID:

2.12.71.2

Telnet path:

Setup > **WLAN** > **VLAN-No-Interstation-Traffic**

Possible values:

1 … 4094

Default:

0

2.16 Starting an environment scan at a configurable time

Your WLAN's environment can be regularly searched for rogue APs.

As of HiLCOS 10.12, you can configure the times of the automatic environment scan for rogue APs.

Environment scans should be performed at times that minimize interference to normal operations.

This feature allows you to perform the scan of the configured frequency band each day at a predefined time.

In this case, scan refers to:

- Active scanning using probe requests.
- Passive scanning for beacons.

It is not always possible to use active scanning, for example where a 5-GHz channel is not DFS-free. No transmissions are permitted in this case.

The configuration is performed from the command console, shown here with default values as an example:

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Environment-Scan
> ls -a

[1.3.6.1.4.1.2356.11][2.23.20.27]
Ifc      Operating  Hour    Minute  Channel-List
[1]      [2]         [3]    [4]     [5]
=========-------------------------------------------------------------------
WLAN-1    No          3      0
WLAN-2    No          3      0
```

"Hour" and "Minute" are used to set the time at which the daily environment scan is performed. These fields also permit the use of the CRON syntax. The channel list can be used to limit the channels to be scanned (as a comma-separated list). If this list is left empty, all of the channels of the frequency band operating on the module are scanned.

During the scan, the WLAN module spends about three seconds on each channel. The next channel is then scanned. Once all of the configured channels have been scanned, the module returns to normal operating mode.

During the scan the module is not capable of regular WLAN operations, in contrast, for example, to the background scan. However, only one of the two modules can perform an environment scan at any one time, and the other module operates normally.

In addition to the time-controlled activation of the environment scan, it can also be activated permanently. For this purpose, the WLAN module can be switched to the operating mode "Scanner" (see operation mode 7):

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Operational
> l

Ifc       Operating     Operation-Mode  Link-LED-Function     Broken-Link-Detection
==========-------------------------------------------------------------------------
WLAN-1    Yes           Scanner         Normal                No
WLAN-2    Yes           managed-AP      Normal                No
```

```
root@LN-1700Esc:/Setup/Interfaces/WLAN/Operational
> set ?

Possible input for columns in table 'Operational':
[  1] Ifc                   : WLAN-1 (1), WLAN-2 (2)
[  2] Operating             : Yes (0), No (1)
[  3] Operation-Mode        : Access-Point (1), managed-AP (4), Station (0),
                              Probe (5), Scanner (7)
[  4] Link-LED-Function     : Normal (0), Client-Mode-Strength (1), P2P-1-Strength (8))
[  5] Broken-Link-Detection : No (0), LAN-1 (1), LAN-2 (2)
```

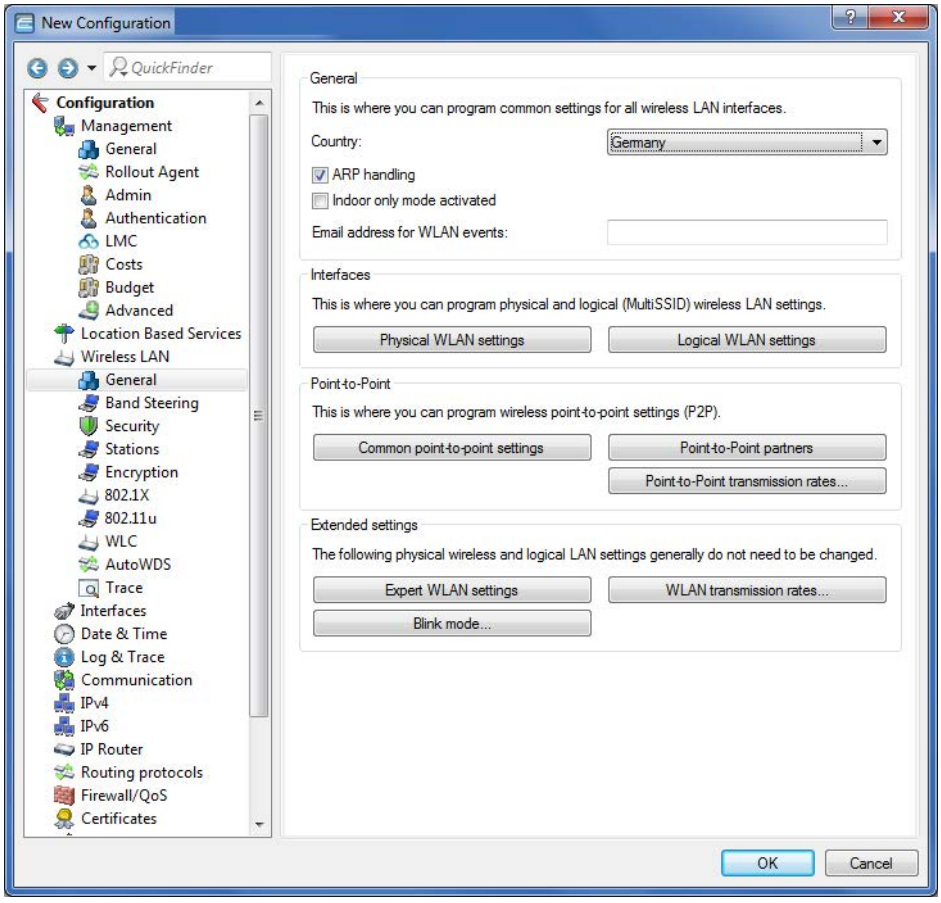
This performs the environment scan as described above: After scanning the configured channels, the scan does not terminate but it starts again from the beginning.

This operating mode allows the use of an AP as a full-time "scanner" AP.

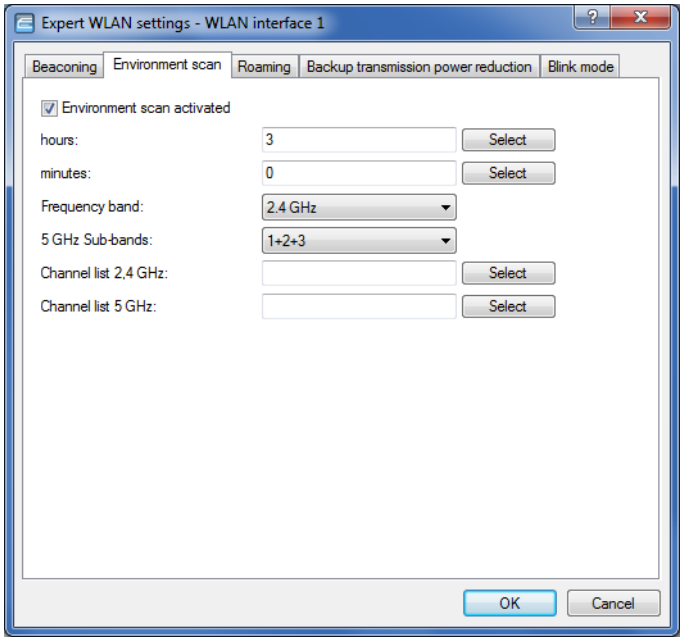
The result of the environment scan can be found in the table **Status** > **WLAN** > **Environment-Scan-Results**.

2.16.1 Configuration by LANconfig

Navigate to **Wireless LAN** > **General** > **Extended settings**.



The parameters for the environment scan are set in the table **Expert WLAN settings** on the tab **Environment scan**.



Environment scan activated

Activates/deactivates the environment scan.

The following parameters are grayed out if the environment scan is disabled.

Hours

Contains the hour value of the time for the environment scan.

Minutes

Contains the minute value of the time for the environment scan.

Frequency band

Contains the frequency bands for the environment scan.

Possible values:

2.4 GHz

Scans the 2.4-GHz frequency band.

5 GHz

Scans the 5-GHz frequency band.

2.4/5 GHz

Scans the 2.4-GHz and 5-GHz frequency bands.

5-GHz subbands

Contains the subbands of the 5-GHz frequency band.

Possible values:

1

2

3

1+2

1+3

2+3

1+2+3

Channel list 2.4 GHz

Specifies the 2.4-GHz channels for the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 2.4-GHz frequency band.

Possible values (multiple selection allowed):

1 to 13

In steps of 1.

Channel list 5GHz

Specifies the 5-GHz channels for the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 5-GHz frequency band.

Possible values (multiple selection allowed):

36 to 64

In steps of 4.

100 to 140

In steps of 4.

2.16.2 Additions to the Setup menu

Starting an environment scan at a configurable time

This table is used to specify the daily time when the frequency band of the corresponding interface is scanned for rogue APs. It is also possible to use the *CRON syntax* for this. The search relies on active scanning with probe requests as well as passive scanning for beacons.

It is not always possible to use active scanning, for example where a 5-GHz channel is not DFS-free.

SNMP ID:

2.23.20.27

Telnet path:

Setup > **Interfaces** > **WLAN**

Ifc

This table contains the available WLAN interfaces.

SNMP ID:

2.23.20.27.1

Telnet path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

1

WLAN-1

2

WLAN-2

Yes

Enables/disables the environment scan.

SNMP ID:

2.23.20.27.2

Telnet path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

0

Not active

1

Active

Default:

0

Hours

Set the hours value for the time of the environment scan here.

SNMP ID:

2.23.20.27.6

Telnet path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

0 … 23

Default:

3

Minutes

Set the minutes value for the time of the environment scan here.

SNMP ID:

2.23.20.27.7

Telnet path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

0 … 59

Default:

0

Frequency band

Here you set the radio band for which your WLAN module performs an environment scan.

SNMP ID:

2.23.20.27.8

Telnet path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

2.4 GHz
Scans the 2.4-GHz frequency band.

5 GHz
Scans the 5-GHz frequency band.

2.4/5 GHz
Scans the 2.4-GHz and 5-GHz frequency bands.

Default:

2.4 GHz

Subbands-5GHz

Here you configure the subbands of your 5-GHz frequency band.

SNMP ID:

2.23.20.27.9

Telnet path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

1+2+3
1+2
1+3
2+3
1
2
3

Default:

1+2+3

Channel-List-2.4 GHz

Here you can limit the 2.4-GHz channels that are subject to the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 2.4-GHz frequency band.

SNMP ID:

2.23.20.27.10

Telnet path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

empty
The environment scan is performed for all channels in the 2.4-GHz frequency band.

1
The environment scan is performed for channel 1 in the 2.4-GHz frequency band.

2
The environment scan is performed for channel 2 in the 2.4-GHz frequency band.

3
The environment scan is performed for channel 3 in the 2.4-GHz frequency band.

4
The environment scan is performed for channel 4 in the 2.4-GHz frequency band.

5
The environment scan is performed for channel 5 in the 2.4-GHz frequency band.

6
The environment scan is performed for channel 6 in the 2.4-GHz frequency band.

7
The environment scan is performed for channel 7 in the 2.4-GHz frequency band.

8
The environment scan is performed for channel 8 in the 2.4-GHz frequency band.

9
The environment scan is performed for channel 9 in the 2.4-GHz frequency band.

10
The environment scan is performed for channel 10 in the 2.4-GHz frequency band.

11
The environment scan is performed for channel 11 in the 2.4-GHz frequency band.

12
The environment scan is performed for channel 12 in the 2.4-GHz frequency band.

13
The environment scan is performed for channel 13 in the 2.4-GHz frequency band.

Channel-List-5 GHz

Here you can limit the 5-GHz channels that are subject to the environment scan.

If you make no entries here, the environmental scan is performed for all channels of the 5-GHz frequency band.

SNMP ID:

2.23.20.27.11

Telnet path:

Setup > **Interfaces** > **WLAN** > **Environment-Scan**

Possible values:

empty
The environment scan is performed for all channels in the 5-GHz frequency band.

36
The environment scan is performed for channel 36 in the 5-GHz frequency band.

40
The environment scan is performed for channel 40 in the 5-GHz frequency band.

44
The environment scan is performed for channel 44 in the 5-GHz frequency band.

48
The environment scan is performed for channel 48 in the 5-GHz frequency band.

52
The environment scan is performed for channel 52 in the 5-GHz frequency band.

56
The environment scan is performed for channel 56 in the 5-GHz frequency band.

60
The environment scan is performed for channel 60 in the 5-GHz frequency band.

64
The environment scan is performed for channel 64 in the 5-GHz frequency band.

100
The environment scan is performed for channel 100 in the 5-GHz frequency band.

104
The environment scan is performed for channel 104 in the 5-GHz frequency band.

108
The environment scan is performed for channel 108 in the 5-GHz frequency band.

112
The environment scan is performed for channel 112 in the 5-GHz frequency band.

116
The environment scan is performed for channel 116 in the 5-GHz frequency band.

120
The environment scan is performed for channel 120 in the 5-GHz frequency band.

124
The environment scan is performed for channel 124 in the 5-GHz frequency band.

128
The environment scan is performed for channel 128 in the 5-GHz frequency band.

132
The environment scan is performed for channel 132 in the 5-GHz frequency band.

136
The environment scan is performed for channel 136 in the 5-GHz frequency band.

140
The environment scan is performed for channel 140 in the 5-GHz frequency band.

2.17 Converting data streams from multicast into unicast

As of HiLCOS 10.12, you can convert multicast data streams to unicast data streams.

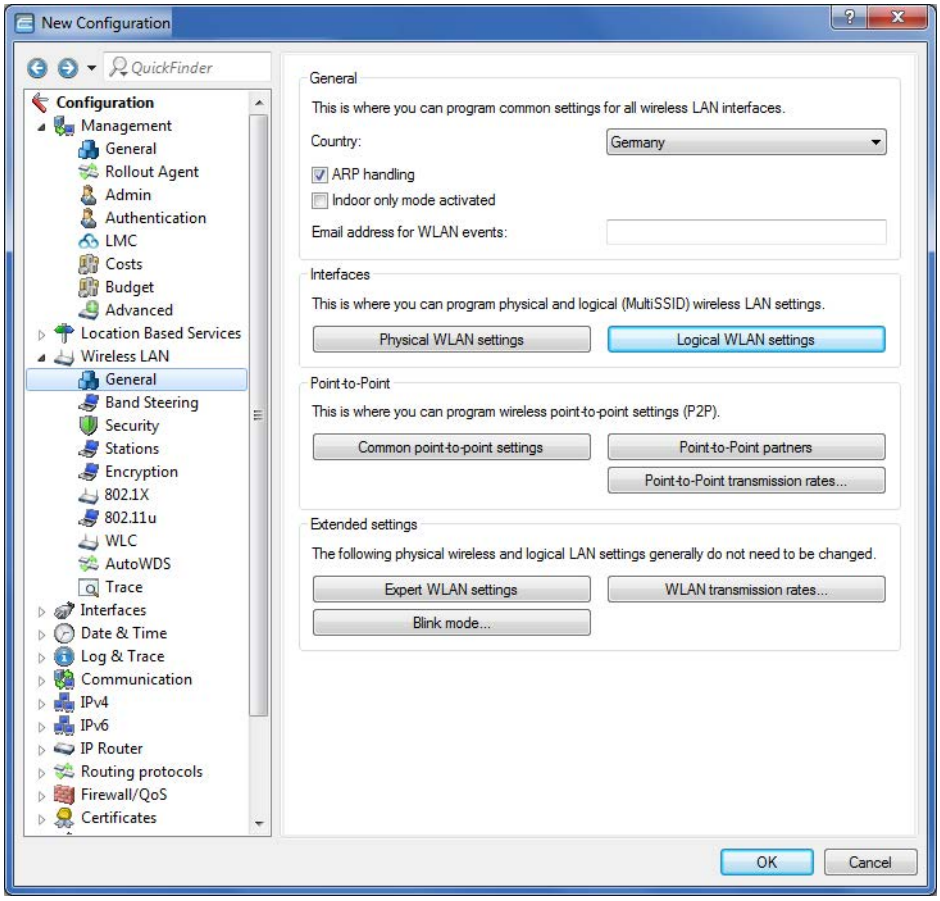
The ability to automatically convert multicast to unicast data streams allows multiple WLAN clients to smoothly stream high-resolution video applications. For applications such as IPTV services, you benefit from better performance and a marked improvement in quality.

After activation of the feature, multicast data streams intended for transmission over WLAN interfaces are converted on the MAC layer or WLAN layer into individual unicast data streams for each client. Although the packets are identical for each client, the fact that they are now part of a unicast means that they can be transmitted at the highest possible data rate supported by the respective client. Even though the packets are now duplicated, in most scenarios the much faster transmission means that significantly less airtime is consumed, which benefits the other transmissions.

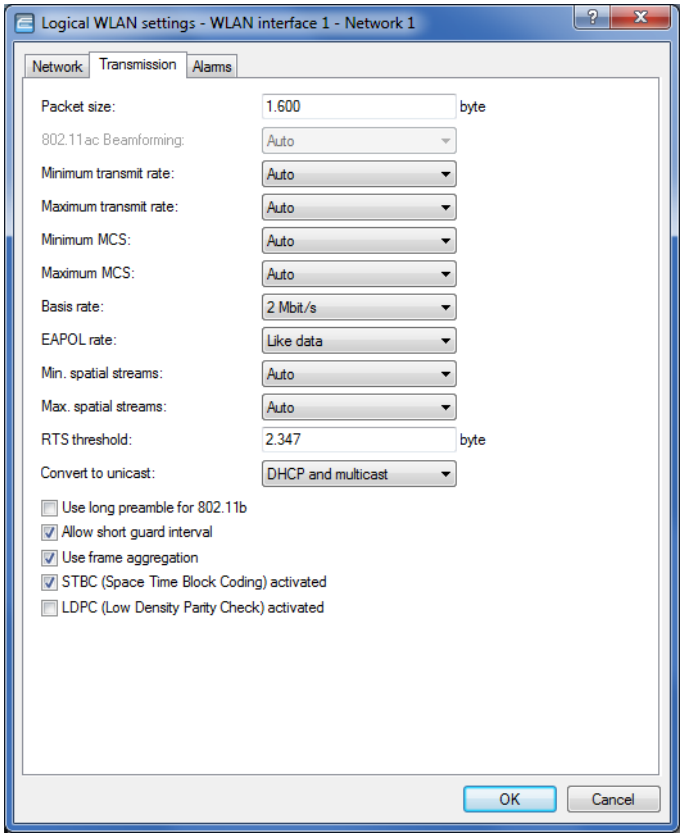
In order for this feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. The device uses IGMP snooping to determine which client should receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

2.17.1 Configuration by LANconfig

The new feature is to be found under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**



after selecting a WLAN interface on the **Transmission** tab.



Convert to unicast

You have the following options for converting data streams to unicast:

None

No data streams are converted to unicast.

DHCP

Response messages sent from the DHCP server as a broadcast are converted into unicasts. This form of message delivery is more reliable because data packets sent as a broadcast have no specific addressee, they do not use optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and they have a low data rate.

Multicast

After activation of the feature, multicast data streams intended for transmission over WLAN interfaces are converted on the MAC layer or WLAN layer into individual unicast data streams for each client.

DHCP and multicast

Converts DHCP and multicast data streams to unicast.

2.17.2 The CLI 'show' command

Using the command `show igmp-snooping` you can see which clients have "subscribed" to which multicast groups. If the feature is activated, a conversion is performed for the members listed here. Here's an example:

```
> show igmp-snooping

Group           | VLAN  | Ports
```

```
=======================================
224.0.0.251     |     1 | WLAN-1


Group           | VLAN  | Member            | Port
=================================================
224.0.0.251     |     1 | a0:18:28:0c:9c:af | WLAN-1
```

2.17.3 Additions to the Setup menu

Convert-to-Unicast

This parameter is used to specify which type of data packets sent in a WLAN as a broadcast are automatically converted into unicast by the device.

SNMP ID:

2.23.20.2.25

Telnet path:

Setup > **Interfaces** > **WLAN** > **Transmission**

Possible values:

0

None

1

DHCP: Response messages sent from the DHCP server as a broadcast are converted into unicasts. This form of message delivery is more reliable because data packets sent as a broadcast have no specific addressee, they do not use optimized transmission techniques such as ARP spoofing or IGMP/MLD snooping, and they have a low data rate.

2

Multicast: In order for this feature to work, it is necessary to enable IGMP snooping on the device and to configure it correctly. The device uses IGMP snooping to determine which client should receive which multicast stream. This ensures that the appropriate target clients or addresses are available for the multicast conversion.

3

DHCP and multicast conversion

Default:

1

3 WLAN Management

3.1 Automatically switch off IAPP if a CAPWAP tunnel exists

As of HiLCOS 10.12, a WLC automatically disables the IAPP on managed APs as soon as a CAPWAP administration tunnel is established between APs and WLC.

3.2 Multiple configurable AutoWDS profiles

As of HiLCOS 10.12 WLCs are able to manage multiple AutoWDS profiles.

3.2.1 Additions to the Setup menu

AutoWDS profiles

This table contains the parameters for the AutoWDS profiles which you assign to the individual APs by means of the WLAN profile in order to implement meshed networks. AutoWDS profiles collect the settings and limits that form the P2P topology and the AutoWDS base networks.

In simple network environments, the use of the preset AutoWDS profile "DEFAULT" is sufficient. If you use several different AutoWDS profiles, the following conditions should be observed:

- APs with different AutoWDS profiles cannot be connected to one other, neither automatically nor manually.
- The maximum number of AutoWDS profiles corresponds to the maximum possible number of WLAN profiles on the WLC.
- The entry for the AutoWDS profile "DEFAULT" cannot be deleted or renamed.
- If two different AutoWDS profiles are used, then the rollout SSIDs must also be different. Similarly, the linking of an AutoWDS profile to a WLAN profile must be unique and unequivocal. If this is not the case, the WLC reports a profile error.
- Each AutoWDS profile uses its own SSID. This reduces the number of SSIDs that are available for the profiles. If an SSID is used multiple times, the WLC reports a profile error.
- There is only one WLC-TUNNEL-AUTOWDS interface on the WLC. The individual rollout SSIDs therefore use the same interface on the WLC as the endpoint. By default, communication between the WLAN clients is disabled during the integration.
- When express integration is enabled, the rollout SSID for unconfigured WLAN clients is initially unimportant. This means that during an express integration, an AP is able to retrieve its configuration from the WLC via an AP with a different AutoWDS profile; however, in this case it only receives its AutoWDS profile and the manually configured topology entries and/or P2P links. The automatic generation of a P2P configuration does not take place if the AutoWDS profiles of the two APs do not match. If only one AutoWDS profile is transferred in this case, the AP falls back to scan mode after the usual time: however, it has by then been assigned its AutoWDS rollout SSID and it then integrates with the corresponding AutoWDS APs (according to its profile).

SNMP ID:

2.37.1.15

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration**

Name

Name of the AutoWDS profile which you reference from other tables.

The entry for the AutoWDS profile "DEFAULT" cannot be deleted or renamed.

SNMP ID:

2.37.1.15.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Max. 15 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Commonprofile

Enter the name of the WLAN profile which the AutoWDS base network is assigned to. All APs operating with this WLAN profile simultaneously deploy the corresponding AutoWDS base network.

Different AutoWDS profiles may not refer to the same WLAN profile.

SNMP ID:

2.37.1.15.2

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **Commonprofiles**.

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

SSID

Enter the name of the logical WLAN network (SSID) that a managed AP uses to deploy the AutoWDS base network. In client mode, unassociated APs use the SSID entered here to receive a configuration from the WLC.

This SSID is reserved exclusively for this AutoWDS profile. The AutoWDS base network cannot be used by other WLAN clients such as smartphones, laptops, etc. These devices require their own SSID within your WLAN infrastructure.

SNMP ID:

2.37.1.15.3

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

AutoWDS-Rollout

AutoWDS-Topology

Name of the AutoWDS profile for which this manual P2P configuration applies.

SNMP ID:

2.37.1.16.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Topology**

Possible values:

Name from **Setup** > **WLAN-Management** > **AP-Configuration** > **AutoWDS-Profiles**

Max. 15 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

3.3 WLC script rollout for certain versions of HiLCOS

As of HiLCOS 10.12, you have the option of specifying WLC-controlled script rollouts for certain versions of HiLCOS. This allows different versions of HiLCOS with their differing configurations to integrate into a common WLAN installation.

3.3.1 Using LANconfig to configure WLC script rollout

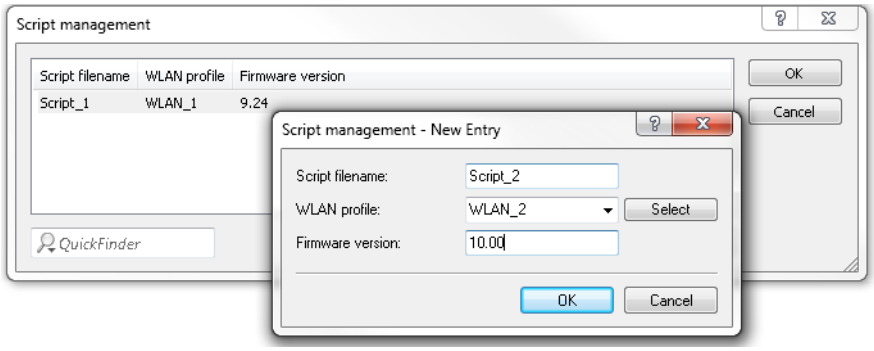
Under certain circumstances, you may need to work with configurations based on different versions of HiLCOS within a single WLAN installation. LANconfig features script management, so that you can rollout scripts with particular firmware versions for your various WLAN profiles.

Please note that it is not possible to assign multiple scripts with different firmware versions to an individual WLAN profile.

In LANconfig, the script management table is located under **WLAN Controller** > **AP Update** > **Script management**.

You specify new scripts for your WLAN profiles by adding new entries to the table.

The dialog in LANconfig has changed as follows:



> **Firmware version**

By specifying a firmware version, you determine the HiLCOS version set in the script that is rolled out.

Please enter the firmware version in the form **xx.yy**, e.g. 10.12

3.3.2 Additions to the Setup menu

Firmware version

Use this item to set the firmware version for which the corresponding script is to be rolled out.

Please enter the firmware version in the form **xx.yy**, e.g. 10.12

SNMP ID:

2.37.27.16.3

Telnet path:

Setup > **WLAN-Management** > **Central-Firmware-Management** > **Script-Management**

Possible values:

Max. 6 characters from `[0-9].`

Default:

empty

3.4 RADIUS

3.4.1 Availability monitoring for external RADIUS servers

As of HiLCOS 10.12, you can use this feature to monitor the availability of a RADIUS server. RADIUS requests are sent at regular intervals to check whether the RADIUS service is functional.

Monitoring can be performed as follows:

- By sending status server requests (DEFAULT). These are specifically used to check the availability of RADIUS services. However, they are not supported by all RADIUS servers (a positive example is FreeRADIUS).
- By sending access requests ("dummy requests"). Only use this method if the server does not support status server requests.

You can create supervision profiles under **Setup** > **RADIUS** > **Supervision-Servers** > **Profiles**. These include the method use to monitor the availability test, the interval (in seconds) after which each check is performed, and the attributes to be attached to an access request (there must be at least one user name for the dummy request; status server requests do not require any additional attributes). The DEFAULT profile contains the following:

```
root@LCS_L452_Office:/Setup/RADIUS/Supervision-Servers/Profiles/DEFAULT
> ls -a
[1.3.6.1.4.1.2356.11][2.25.21.1.1][column][7.68.69.70.65.85.76.84]

[  1] Name              INFO:       DEFAULT
[  2] Type              VALUE:      Status-Server
[  3] Attributes        VALUE:
[  4] Request-Interval  VALUE:      60
```

The following is an example profile for the use of access requests:

```
root@LCS_L452_Office:/Setup/RADIUS/Supervision-Servers/Profiles/DUMMY
> ls -a
[1.3.6.1.4.1.2356.11][2.25.21.1.1][column][5.68.85.77.77.89]

[  1] Name              INFO:       DUMMY
[  2] Type              VALUE:      Dummy-Request
[  3] Attributes        VALUE:      User-name=dummyuser
[  4] Request-Interval  VALUE:      60
```

Here you see that the user name has been set as an attribute. Make sure you the user name is not known to the RADIUS server: This prevents a regular logon to the RADIUS server. The "pseudo-login" attempts by the monitoring system are taken to be failed logins.

You can now reference a profile contained in this table. This is possible for the RADIUS server used for 802.1X. The following is an example entry in the appropriate table:

```
root@LCS_L452_Office:/Setup/IEEE802.1x/RADIUS-Server/FREERADIUS
> ls -a
[1.3.6.1.4.1.2356.11][2.30.3.1][column][10.70.82.69.69.82.65.68.73.85.83]

[  1] Name              INFO:       FREERADIUS
[  8] Host-Name         VALUE:      192.168.1.2
[  3] Port              VALUE:      1812
[  4] Secret            VALUE:      *
[  6] Loopback-Addr.    VALUE:
```

```
[  7] Protocol          VALUE:      RADIUS
[  9] Attribute-Values  VALUE:
[ 10] Sup.-Profile      VALUE:      DEFAULT
[  5] Backup            VALUE:
```

The RADIUS server specified here is monitored using the supervision profile "DEFAULT". If an entry for "Sup.-Profile" does not match with a supervision profile, the DEFAULT profile is used automatically. If "Sup.-Profile" is empty, no monitoring is performed.

The monitored RADIUS servers and their status can be viewed in the following table:

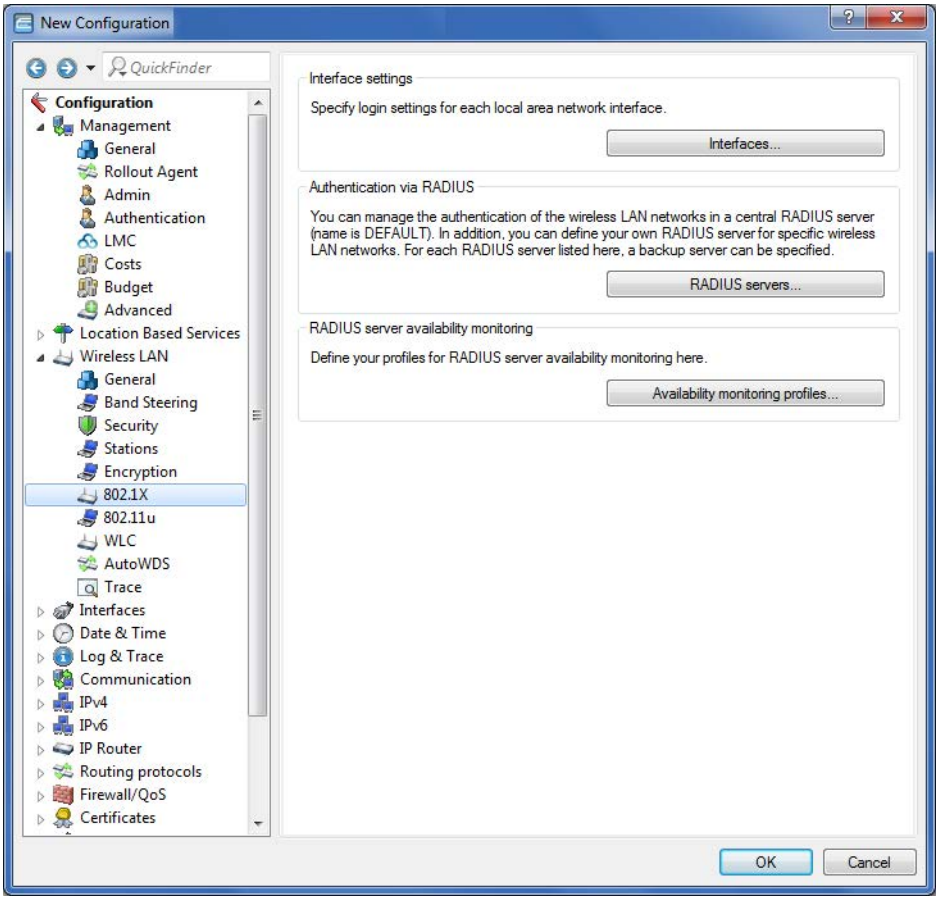
```
root@LCS_L452_Office:/Status/TCP-IP/RADIUS-Supervision-Servers/Servers
> ls -a
[1.3.6.1.4.1.2356.11][1.9.14.1]

Index      Server-Hostname        Port  Loopback-Address  Protocol  State
[1]        [2]                    [3]    [4]              [5]        [6]
==========-----------------------------------------------------------------
1          192.168.1.2            1812                    RADIUS      Up
2          192.168.1.254          1812                    RADIUS      Timeout
```

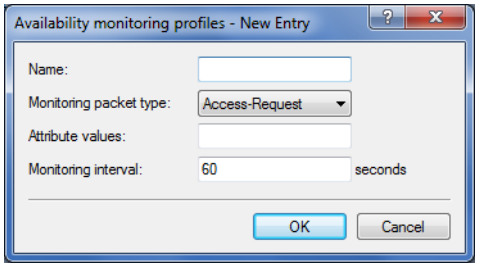
The statistic table is also available under the following path: **Status** > **SLA-Monitor** > **RADIUS** > **Servers**.

Availability monitoring profiles in LANconfig

Navigate to **Wireless LAN** > **802.1X** > **RADIUS server availability monitoring**.



The table **Availability monitoring profiles** provides the following configuration options:



Name

Contains the name of the availability monitoring profile.

Monitoring packet type

Your choices are as follows:

Access request (default)

Only use this type if the server does not support status server requests.

Status server

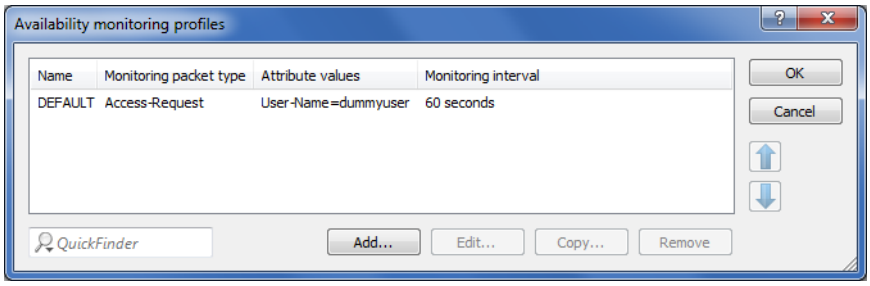
This type is specifically for the availability monitoring of RADIUS services, but it is not supported by all RADIUS servers.

Attribute values

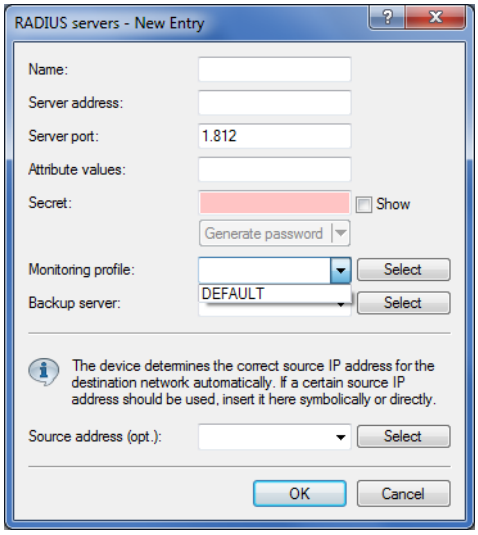
An attribute is only required for access requests. It is not required for status server requests.

Monitoring Interval

The monitoring interval in seconds (default: 60)



The new availability monitoring profile (in this case: DEFAULT) is now also available for use in the **RADIUS server** table:



Additions to the Status menu

Servers

This entry contains the status values for Servers.

SNMP ID:

1.36.2.1

Telnet path:

Status > **SLA-Monitor** > **RADIUS**

Possible values:

0

Unknown

The status of the server is not known either because no request has been sent to it or because no valid response has been received.

1

Up

The server responded to a request with a valid RADIUS response and is therefore assumed to be operational.

2

DNS error

The device cannot resolve the name of the DNS server.

3

Authenticator mismatch

The device received a response from the server, but with a faulty authentication. This indicates a shared-secret mismatch. Note that this status can only occur if, for test purposes, access requests are sent to the server immediately following this type of a mismatch. This is because status server packets contain a message authenticator attribute and are dropped silently in the event of a mismatch. Despite

this, a shared-secret mismatch does not indicate that the server is temporarily unavailable; it rather indicates a permanent mis-configuration.

4

Host unreachable

The server is not accessible via IP.

5

Port unreachable

The server is accessible via IP, but no RADIUS server is using the specified port.

6

Timeout

It is not possible to route the server's IP address.

Additions to the Setup menu

Availability monitoring

In this directory you configure the availability monitoring.

Monitoring is performed by sending status server requests or access requests.

SNMP ID:

2.25.21

Telnet path:

Setup > **RADIUS**

Profiles

Here you create monitoring profiles for the availability of RADIUS servers.

SNMP ID:

2.25.21.1

Telnet path:

Setup > **RADIUS** > **Supervision-Servers**

Name

Enter the name of the availability monitoring profile here.

SNMP ID:

2.25.21.1.1

Telnet path:

Setup > **RADIUS** > **Supervision-Servers** > **Profiles**

Possible values:

Characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

DEFAULT

Type

Here, you specify whether status server or access requests are sent to the RADIUS server for the purpose of availability monitoring.

SNMP ID:

2.25.21.1.2

Telnet path:

Setup > **RADIUS** > **Supervision-Servers** > **Profiles**

Possible values:

Access request
Status server

Default:

Access request

Attributes

If availability monitoring is performed with access requests, you can specify the attributes of the access request here by means of a comma-separated list in the format **Attribute1=value1,Attribute2=value2, etc.**. Accessibility checks by means of an access request require at least the specification of the attribute "User-Name", e.g. **User-Name=dummyuser**.

Status server requests do not require any attributes.

SNMP ID:

2.25.21.1.3

Telnet path:

Setup > **RADIUS** > **Supervision-Servers** > **Profiles**

Possible values:

Characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Request interval

Here you define the interval in seconds used by the RADIUS server to check the availability.

SNMP ID:

2.25.21.1.4

Telnet path:

Setup > **RADIUS** > **Supervision-Servers** > **Profiles**

Possible values:

`[0-9]`

Default:

60

3.5 Coordinated channel selection for Wireless ePaper

As of HiLCOS 10.12, the Wireless ePaper feature offers coordinated channel selection.

This is particularly useful if you operate multiple Wireless ePaper access points at a site.

Each AP requires its own ePaper channel, so collisions or multiple assignments need to be avoided.

For this reason, ePaper APs automatically discover neighboring ePaper APs within a broadcast domain by means of a TCP-based protocol that is transmitted in a multicast group. One of these APs is automatically set as the master AP. The remaining APs become slave APs. If the master AP fails, one of the slave APs is automatically designated as the new master AP.

Each slave AP regularly sends an assessment of its current ePaper channel to the master AP. Based on the assessments from all the slaves, the master decides whether or not a slave needs to change channel.

Each ePaper AP assesses all of the ePaper channels. This takes into account the locally used WLAN channel (which the ePaper channel should not overlap) and whether the ePaper channel is a preferred channel.

Preferred channels are: 3, 5, 8, 9 and 10.

Based on the channel assessments received, the ePaper channels are optimized as follows:

The master AP selects the best of the free channels and assigns it to the ePaper AP with the lowest ePaper AP ID (the master also assigns a channel to itself). This is performed successively for all of the ePaper APs.

Channels are only switched if the evaluation of the competing channel is better by a certain, configurable threshold. This avoids unnecessary channel changes.

If the network contains one or more ePaper APs with a statically assigned ePaper channel, the master can still perform a coordinated channel selection. If this is enabled on an AP with a static channel, the master performing the channel allocation will consider this channel to be already assigned and will not assign it to any other AP.

The status menu of the Wireless ePaper feature has been supplemented with a peer table. This lists the APs involved in channel coordination.

The peer table contains the ePaper AP ID, the role of the AP (slave or master), the channel assessment, and the assigned ePaper channel.

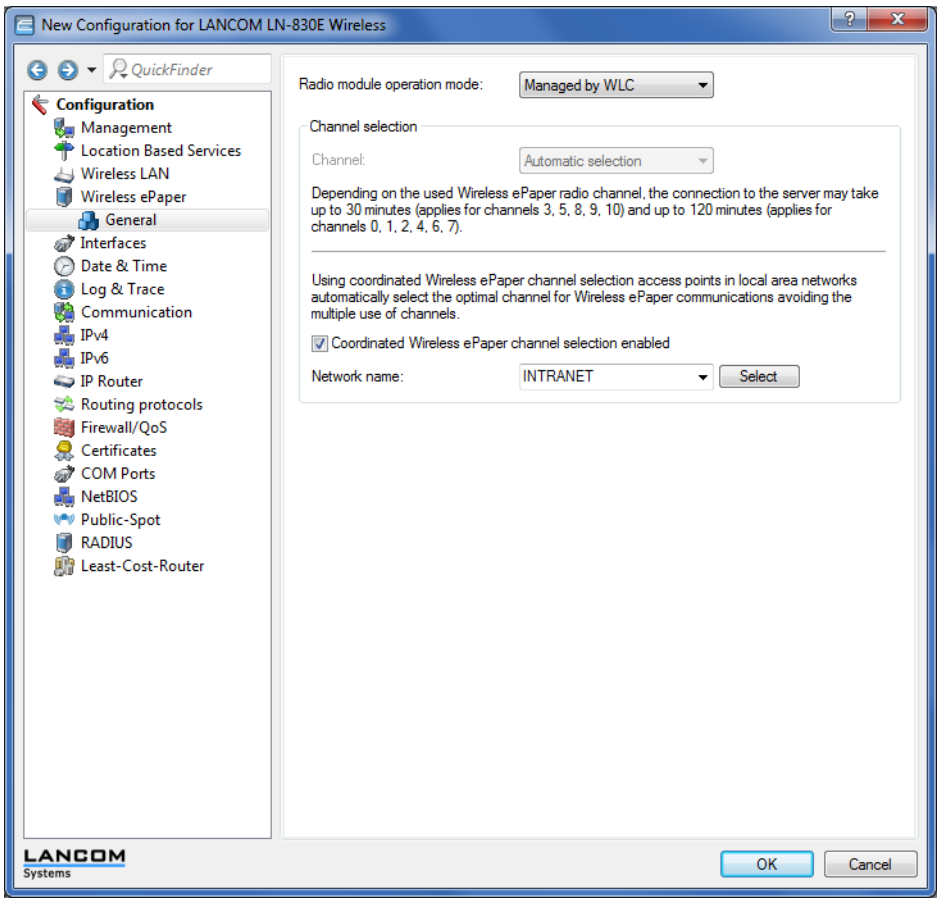
The channel assessment is shown as a list of the ePaper channels 0 to 10 followed by the assessment value. The value range is 0 to 255, a higher value being a better rating.

```
root@LN-830E PM:/Status/Wireless-ePaper
> ls -a Channel-Coordination/Peer-Table/

ID    State    IP-Address    Rtg-Tag  Connected  Assessment  Assignment
===============-------------------------------------------------------
66122  SLAVE  172.16.26.7      1        Yes       0:108|1:096|2:073|3:196
66123  MASTER 172.16.26.6      1        No                  3
66124  SLAVE  172.16.26.8      1        Yes       0:127|1:127|2:127:3:255
```

3.5.1 Activation and configuration in LANconfig

You activate and configure the feature under **Wireless ePaper** > **General**.



1. Activate the coordinated channel selection using the check box **Coordinated Wireless ePaper channel selection enabled**.

   If coordinated channel selection is not activated, the parameter **Network name** is grayed out.

2. Select the network to be used for the access points to communicate with one another from the **Network name** selection list.
3. Confirm your settings by clicking the **OK** button.

3.5.2 Additions to the Status menu

Channel coordination

This menu contains the settings for the coordinated channel assignment.

SNMP ID:

1.88.9

Telnet path:

Status > **Wireless-ePaper**

3.5.3 Additions to the Setup menu

Channel coordination

Prevents collisions on ePaper channels due to APs within range of each other.

SNMP ID:

2.88.4

Telnet path:

Setup > **Wireless-ePaper**

Operating

The coordinated channel selection is activated or deactivated here.

SNMP ID:

2.88.4.1

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0

No

1

Yes

Default:

1

Network

Here you specify the network that the access points are to use to communicate with each other.

SNMP ID:

2.88.4.2

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

16 characters from the following character set `[A-Z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

Announce address

Set the announce address here.

SNMP ID:

2.88.4.3

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

39 characters from the following character set: `[0-9 A-F a-f :.]`

Announce port

Set the announce port here.

SNMP ID:

2.88.4.4

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

Announce interval

Set the announce interval here.

SNMP ID:

2.88.4.5

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

Announce timeout factor

Set the announce timeout factor here.

SNMP ID:

2.88.4.6

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

Announce timeout interval

Set the announce timeout interval here.

SNMP ID:

2.88.4.7

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

Announce master backoff interval

Set the announce master backoff interval here.

SNMP ID:

2.88.4.8

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

3 characters from the following character set: `[0-9]`

Coordination port

Set the coordination port here.

SNMP ID:

2.88.4.9

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

5 characters from the following character set: `[0-9]`

Coordination keep-alive interval

Here you set the coordination keep-alive interval.

SNMP ID:

2.88.4.10

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

Coordination reconnect interval

Here you set the coordination reconnect interval.

SNMP ID:

2.88.4.11

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

10 characters from the following character set: `[0-9]`

Assignment switch threshold

Here you set the assignment switch threshold.

SNMP ID:

2.88.4.12

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

3 characters from the following character set: `[0-9]`

Distance weighting

Here you set the weighting of WLAN distance.

A higher value means a better weighting.

SNMP ID:

2.88.4.13

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0 … 255

Channel weighting

Here you set the weighting of a preferred channel.

A higher value means a better weighting.

SNMP ID:

2.88.4.14

Telnet path:

Setup > **Wireless-ePaper** > **Channel-Coordination**

Possible values:

0 … 255

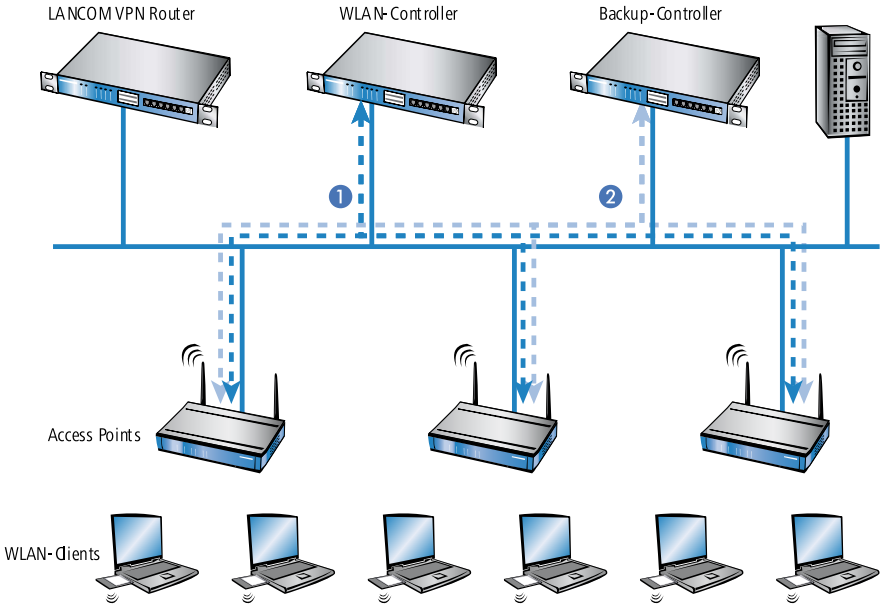
3.6 Backup solutions

Hirschmann WLAN controllers manage a large number of access points, which in turn may have a large number of WLAN clients associated with them. WLAN controllers thus play a crucial role in the functioning of the entire WLAN infrastructure—for which reason the organization of a backup solution in case of temporary WLAN controller failure is in many cases indispensable.

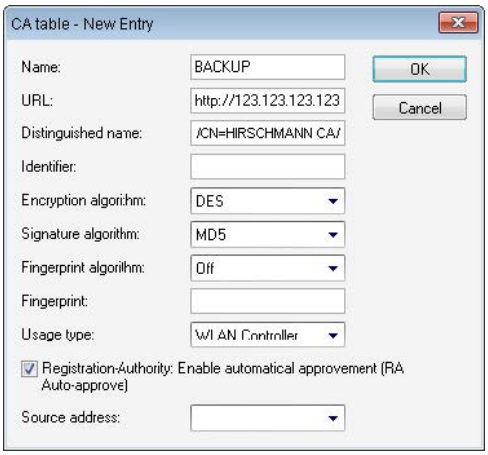
In case of a backup event, a managed access point should connect to an alternative WLAN controller. Because this connection will only function if the certificate in the access point has been authorized by the backup controller, it is essential that all WLAN controllers sharing a backup solution have identical root certificates.

3.6.1 Backup with redundant WLAN controllers

This is worthwhile for backing up a Hirschmann WLAN controller with a second WLAN controller, the aim being to maintain full control over all managed access points at all times. The backup Controller is configured in such a way that it uses SCEP to obtain the necessary certificates from the backed-up primary WLAN controller.

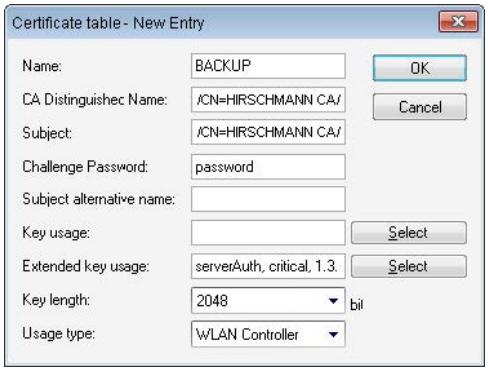


1. Switch off the CA on the backup Controller.
2. In the configuration of the SCEP client in the backup controller, create a new backup in the CA table (in LANconfig under **Certificates** > **SCEP client** > **CA table**). The CA of the primary WLAN controller is entered here:



3. The URL is to be entered as the IP address or the DNS name of the primary WLAN controller followed by the path to the CA `/cgi-bin/pkiclient.exe`. For example `10.1.1.99/cgi-bin/pkiclient.exe`'.
   - **Distinguished name**: Standard name of the CA (/CN=HIRSCHMANN CA/O=Hirschmann Automation and Control GmbH/C=DE) or the name given on the primary Controller
   - Switch on **RA auto approve**
   - **Usage type**: WLAN controller

4. Then create a new entry in the certificate table with the following information:



- **CA distinguished name**: The standard name under which the CA is entered, e.g. /CN=HIRSCHMANN CA/O=Hirschmann Automation and Control GmbH/C=DE
- **Subject**: Specification of the primary WLAN controller's MAC address in the form: /CN=00:a0:57:01:23:45/O=Hirschmann Automation and Control GmbH/C=DE
- **Challenge password**: The general challenge password of the CA on the primary WLAN controller or a password for the Controller specified manually.
- **Extended key usage**: critical,serverAuth,1.3.6.1.5.5.7.3.18
- **Key length**: 2048 bits
- **Usage type**: WLAN controller

5. If a SCEP configuration was previously active on the backup controller, the following actions must be executed under WEBconfig (**HiLCOS Menu Tree** > **Setup** > **Certificates** > **SCEP client**):
   - Clear SCEP file system
   - Update (2x: the first time, the SCEP client retrieves the new CA/RA certificates only; the second time the device certificate is updated)
6. Configure the first WLAN controller **1** according to your requirements with all profiles and the associated AT table. The access points then establish connections to the first WLAN controller. Each access point receives a valid certificate and a configuration for the WLAN module from the WLAN controller.
7. Transfer the configuration from the first WLAN controller **1**, for example using LANconfig, to the backup controller **2**. The profiles and the AP tables with the access point MAC addresses are transferred to the backup controller at the same time. All access points remain logged on to the first WLAN controller.

Should WLAN controller **1** fail, the access points will automatically search for another WLAN controller and they will find the backup controller **2**. Because this has the same root certificate, it is able to check the validity of the access points' certificates. Because the access points are also entered into the backup controller's AP table along with their MAC addresses, the backup controller can fully take over the management of the access points. Changes to the WLAN profiles in the backup controller will directly affect the managed access points.

In this scenario, the access points remain under the management of the backup controller until this itself becomes unavailable or is manually disconnected.

If the access points are set up for standalone operation, they will remain operational while searching for a backup controller and the WLAN clients will remain associated.

3.6.2 Backup with primary and secondary WLAN controllers

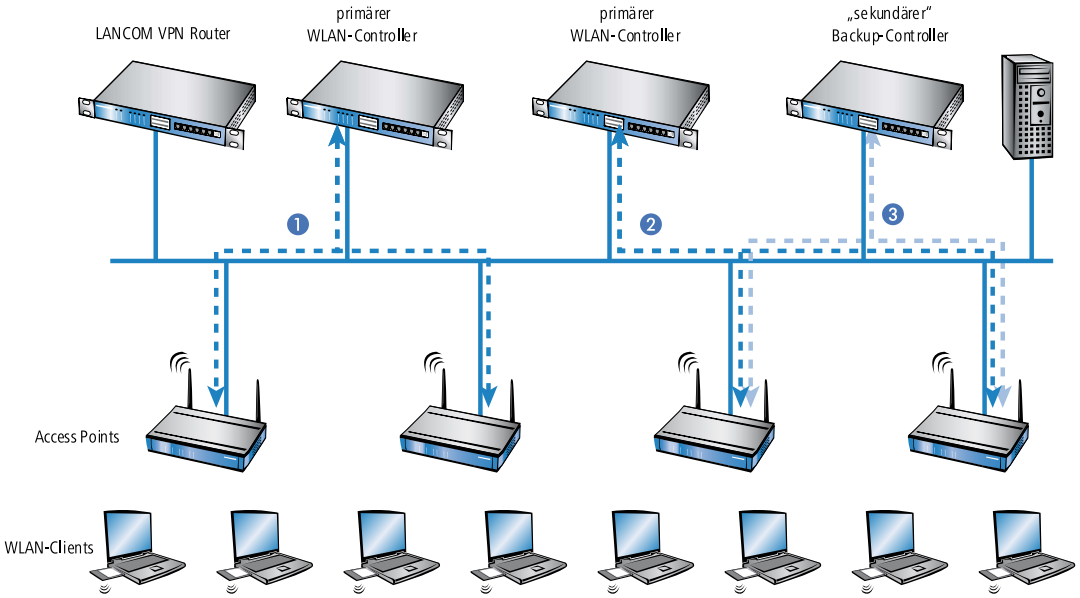
This second type of backup you can provide a larger number of "primary" WLAN controllers with one common "secondary" backup controller. In case a WLAN controller should fail, the access points remain operational but they work with the current configuration of the WLAN modules. As a secondary controller, the backup controller cannot assign any configuration changes to the access points.

3.6.3 Primary and secondary controllers

Connection establishment between an access point and the WLAN controller is always initiated by the access point. A Hirschmann access point in managed mode will search the LAN for a WLAN controller that will provide the configuration. During this search the access point may find various suitable WLAN controllers:

- The WLAN controller can authenticate the **certificate** in the access point and it has a **configuration** stored for the access point's MAC address. A WLAN controller of this type is described as a "primary" WLAN controller.
- A WLAN controller can authenticate the **certificate** of an access point, but it has **neither a configuration** stored for the MAC address of the access point, **nor does it have a default configuration**. A WLAN controller of this type is described as a "secondary" WLAN controller.

This is an example of a backup solution with three WLAN controllers for 50 managed access points: Two of the WLAN controllers each manage 25 access points and the third is available as a backup:



A Hirschmann WLAN controller is now able to accommodate in its AP table five times the maximum number of access points that it can manage by itself. For each five WLAN controllers (identical models), just one additional WLAN controller is sufficient to provide a full backup in case of failure.

1. Set the same time on all of the WLAN controllers **1**, **2** and **3**.
2. Transfer the CA and RA certificates from the first primary WLAN controller **1** to the second primary **2** and to the secondary "backup controller" **3**.
3. Configure the first WLAN controller **1** according to your requirements with the profiles and the associated AP table for one half of the access points. This WLAN controller becomes the primary controller for the access points entered into it.

For a backup solution using a secondary WLAN controller, be sure to set the time for standalone operations such that the access point has time to find a backup controller. This is because the backup controller is not able to provide a new configuration for the access point.

Once the access point has established a backup connection to a secondary WLAN controller, the countdown until expiry of standalone operation is halted. The access point and its WLAN networks remain active as long as it has a connection to a WLAN controller.

1. Configure the second WLAN controller **2** for the other half of the access points, which subsequently treat this WLAN controller as their primary controller.
2. For the backup controller **3** the time and the root certificates are set up only. No further configuration is required.

3. After being started, the access points search for a WLAN controller by emitting a discovery message. In this case, all three Hirschmann WLAN controllers respond to this message—the access points select "their" primary controller for the DTLS connection that follows. One half of the access points decides on WLAN controller **1** and the other half chooses WLAN controller **2**. Because WLAN controller **3** does not function as primary controller for any of the access points, none of the access points log on to it.
4. Should WLAN controller **2** fail, the access points will automatically search for another WLAN controller. They discover the WLAN controllers **1** and **3**, whereby **1** is already under full load with its 25 access points. Backup controller **3** is able to check the validity of the certificates, i.e. it can authenticate the access points and accept them as managed access points. However, because the access points are **not** entered with their MAC numbers into the backup controller's AP table, the backup controller cannot manage the access points any longer; they simply continue to operate with their current WLAN configurations.

If WLAN controller **1** is not under full load, for example because some of "its" access points are switched off, then some of the searching access points could log on here. WLAN controller **1** remains a "secondary" controller for these access points because it does not have their configuration profiles. If in this situation one of the access points with an entry in the AP table of WLAN controller **1** is switched on again, then **1** accepts this reactivated access point and, in exchange, it disconnects one of the backup-event access points.

If the access points are set up for standalone operation they will remain operational while searching for a backup controller, and the WLAN clients can continue to use all of their functions.

3.6.4 Backup connections for dual-SIM services

As of HiLCOS version 10.12, dual-SIM devices also support backup connections if the primary connection is based on a cellular connection. You can also explicitly specify the time until the device returns to the primary connection.

Configuration of the backup connection

The following steps are necessary to define a backup connection:

1. The backup connection requires the appropriate WAN interface to be set up so that the remote site can be reached via this alternative route. If, for example, the ISDN line is to serve as the backup connection, then the remote site is set up as an ISDN remote site (along with the necessary entries in the communications layers and in the PPP list).
2. If the connection to the remote site cannot be checked with LCP requests, the monitoring of the connection should be initiated with an entry in the polling table.
3. Assignment of the new backup connection to the remote site which is to be backed up. This entry is made in the backup table. Dedicated entries in the routing table are not required for a backup connection. The backup connection automatically takes over the source and target networks from the remote site that routes the data under normal operating conditions.

   A remote site can be assigned with multiple backup lines in the backup table. In the case of backup, the system decides which backup line is to be used first:

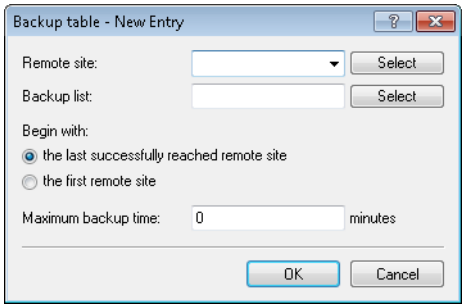
   - The last remote site that was reached successfully
   - The first remote site in the list

The **maximum backup time** specifies the maximum amount of time in minutes that the backup state is maintained. If a time is specified here, the backup connection is disconnected after this time and the backup state is terminated.

For backup scenarios via a cellular connection (multi-SIM), where for technical reasons the cellular module can only maintain one connection at a time, it is only the termination of the backup state that triggers the main connection to attempt to reconnect.

Regardless of the scenario, the backup event occurs again if the main connection cannot be re-established by the time the backup time delay (set elsewhere than this dialog) expires.

The backup table in LANconfig is located under **Communication** > **Call management** under **Backup table**.



Additions to the Setup menu

Fallback minutes

Specifies the maximum amount of time in minutes that the backup state is maintained. If a time is specified here, the backup connection is disconnected after this time and the backup state is terminated.

For backup scenarios via a cellular connection (multi-SIM), where for technical reasons the cellular module can only maintain one connection at a time, it is only the termination of the backup state that triggers the main connection to attempt to reconnect.

Regardless of the scenario, the backup event occurs again if the main connection cannot be re-established by the time the backup time delay (set elsewhere than this dialog) expires.

SNMP ID:

2.2.24.4

Telnet path:

Setup > **WAN** > **Backup-Peers**

Possible values:

Max. 4 characters from `0123456789`

Default:

0

Special values:

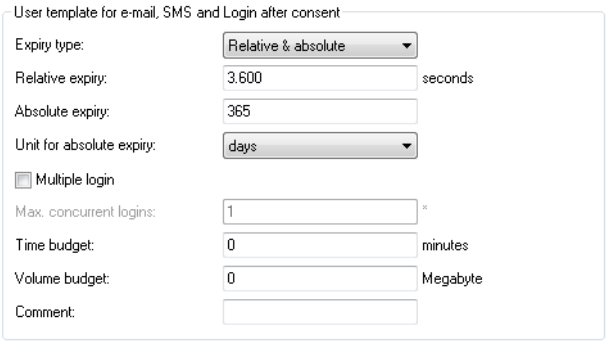
0

The backup connection remains active permanently.

4 Public Spot

4.1 Shorter units for absolute expiry

As of HiLCOS 10.12, Public Spot vouchers can be set with shorter units of time (days, hours, minutes). This is especially useful for scenarios with a high customer frequency in combination with short linger times.
Shorter expiry times for Public Spots are configured in LANconfig under **Public Spot** > **Wizard**.



Unit for absolute expiry

To configure shorter expiry times, use the drop-down menu to select the unit for absolute expiry. Adjust the value for the absolute expiry if necessary.

4.2 Circuit ID as a Public Spot URL-redirect variable

As of HiLCOS 10.12, the redirect variable "%d" enables you to display different welcome pages on authenticated clients, depending on their location.

%d

Enter the URL parameter '%d' as the circuit ID, for example `http://ipaddress/?circuit=%d&nas=%i`. The Public Spot module replaces this variable with the circuit ID that is detected in the client's DHCP request.

This requires "DHCP snooping" to be configured on the AP in such a way that the AP can query the circuit ID in the Public Spot station table of the WLC.

In this way it is possible for the Public Spot welcome page displayed on the clients to be customized by location.

4.3 Creating Public Spot users on a remote Public Spot gateway

As of HiLCOS 10.12, the web API enables you to create Public Spot users on a remote Public Spot gateway.

4.3.1 Creating Public Spot users on a remote Public Spot gateway

With Smart Ticket operating, each user is given a Public Spot account on the RADIUS server of the local Public Spot gateway.

However, where multiple Public Spot gateways are in use but the user accounts should be managed by the RADIUS server of just one gateway, Smart Ticket causes the Public Spot account to be created on this central RADIUS server. To implement this, the remote Public Spot gateway needs to be specified in the HiLCOS menu tree under **Setup** > **Public Spot module** > **Authentication modules**.

If no remote Public Spot gateway is defined, the Public Spot user accounts are created on the local Public Spot gateway.

4.3.2 Additions to the Setup menu

Radius-Server

Use this menu to specify the settings used when Public Spot user accounts are created on the RADIUS server of the remote Public Spot gateway.

SNMP ID:

2.24.41.5

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules**

Provider

Use this entry to specify the RADIUS server profile, which is located in the Public Spot provider table and references the RADIUS server of the remote Public Spot gateway.

SNMP ID:

2.24.41.5.1

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Name

Use this entry to specify which administrator account is used for creating user accounts on the remote Public Spot gateway.

SNMP ID:

2.24.41.5.2

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Password

Use this entry to enter the password for the administrator account specified above.

SNMP ID:

2.24.41.5.3

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Radius-Server**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

4.4 PMS template: Accept GTC

Depending on the configuration, authentication at a Public Spot optionally depends upon the acceptance of the general terms and conditions of use (GTC). In some combinations of login options (e.g. via stored reservation data or SMS authentication) the confirmation of the GTC was not clearly structured until now.

As of HiLCOS 10.12, the appearance of the login page when using a combination of login methods has been redesigned.

4.5 Hiding fields in the setup wizard "Manage Public Spot Account"

As of HiLCOS 10.12 you have the option of permanently hiding table columns in the wizard "Manage Public Spot Account".

4.5.1 Hiding fields in WEBconfig

In the setup wizard "Manage Public Spot Account", the **Show/hide column** button enables you to display or conceal columns of the table. These changes are only temporary. Hidden columns are shown again after a page refresh or in a new session.

If you want to permanently hide specific fields, use the HiLCOS menu tree and navigate to the view **Setup** > **Public Spot module** > **Manage user wizard**. All of the fields are displayed by default. If you hide certain fields, for example to conceal the time budget, they will stay hidden in the wizard itself and also in the drop-down menu behind the button **Show/hide column** after reloading the page.

In order to delete authenticated Public Spot users, the columns "Calling station ID mask" and "Called station ID mask" need to be visible in the wizard. Unauthenticated users can be deleted even if these two columns are hidden.

Please note that hidden fields are not printed out when you press the **Print** button. On the other hand, exporting a CSV file includes all of the data. The **Save as CSV** button can optionally be hidden. To do this, use the HiLCOS menu tree to navigate to the view **Setup** > **Public Spot module** > **Add User Wizard** > **Hide CSV export** . Select "Yes" and save your entry.

Additions to the Setup menu

Show expiry type

This entry gives you the option to hide the "Expiry type" column in the Setup Wizard.

SNMP ID:

2.24.44.12

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Expiry type" column.

No

The Setup Wizard hides the "Expiry type" column.

Default:

Yes

Show abs. expiry

This entry gives you the option to hide the "Absolute expiry" column in the Setup Wizard.

SNMP ID:

2.24.44.13

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "Absolute expiry" column.

No
The Setup Wizard hides the "Absolute expiry" column.

Default:

Yes

Show rel. expiry

This entry gives you the option to hide the "Relative expiry" column in the Setup Wizard.

SNMP ID:

2.24.44.14

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "Relative expiry" column.

No
The Setup Wizard hides the "Relative expiry" column.

Default:

Yes

Show time budget

This entry gives you the option to hide the "Time budget" column in the Setup Wizard.

SNMP ID:

2.24.44.15

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "Time budget" column.

No

The Setup Wizard hides the "Time budget" column.

Default:

Yes

Show volume budget

This entry gives you the option to hide the "Volume budget MByte" column in the Setup Wizard.

SNMP ID:

2.24.44.16

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Volume budget MByte" column.

No

The Setup Wizard hides the "Volume budget MByte" column.

Default:

Yes

Show case sensitive

This entry gives you the option to hide the "Case sensitive" column in the Setup Wizard.

SNMP ID:

2.24.44.17

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Case sensitive" column.

No

The Setup Wizard hides the "Case sensitive" column.

Default:

Yes

Show active

This entry gives you the option to hide the "Show active" column in the Setup Wizard.

SNMP ID:

2.24.44.18

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Show active" column.

No

The Setup Wizard hides the "Show active" column.

Default:

Yes

Show TX limit

This entry gives you the option to hide the "TX limit" (max. transmission bandwidth) column in the Setup Wizard.

SNMP ID:

2.24.44.19

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "TX limit" column.

No

The Setup Wizard hides the "TX limit" column.

Default:

Yes

Show RX limit

This entry gives you the option to hide the "RX limit" (max. receiving bandwidth) column in the Setup Wizard.

SNMP ID:

2.24.44.20

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "RX limit" column.

No

The Setup Wizard hides the "RX limit" column.

Default:

Yes

Show calling station

This entry gives you the option to hide the "Show calling station" column in the Setup Wizard.

SNMP ID:

2.24.44.21

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Show calling station" column.

No

The Setup Wizard hides the "Show calling station" column.

Default:

Yes

Show called station

This entry gives you the option to hide the "Show called station" column in the Setup Wizard.

SNMP ID:

2.24.44.22

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Show called station" column.

No

The Setup Wizard hides the "Show called station" column.

Default:

Yes

Show online time

This entry gives you the option to hide the "Online time" column in the Setup Wizard.

SNMP ID:

2.24.44.23

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes

The Setup Wizard shows the "Online time" column.

No

The Setup Wizard hides the "Online time" column.

Default:

Yes

Show traffic

This entry gives you the option to hide the "Traffic (Rx / Tx Kbyte)" column in the Setup Wizard.

SNMP ID:

2.24.44.24

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "Traffic (Rx / Tx Kbyte)" column.

No
The Setup Wizard hides the "Traffic (Rx / Tx Kbyte)" column.

Default:

Yes

Show status column

This entry gives you the option to hide the "Status" column in the Setup Wizard.

SNMP ID:

2.24.44.25

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "Status" column.

No
The Setup Wizard hides the "Status" column.

Default:

Yes

Show MAC address

This entry gives you the option to hide the "MAC address" column in the Setup Wizard.

SNMP ID:

2.24.44.26

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "MAC address" column.

No
The Setup Wizard hides the "MAC address" column.

Default:

Yes

Show IP address

This entry gives you the option to hide the "IP address" column in the Setup Wizard.

SNMP ID:

2.24.44.27

Telnet path:

Setup > **Public-Spot-Module** > **Manage-User-Wizard**

Possible values:

Yes
The Setup Wizard shows the "IP address" column.

No
The Setup Wizard hides the "IP address" column.

Default:

Yes

4.6 Redirect for HTTPS connections switchable

To minimize the load on Public Spot gateways, HiLCOS 10.12 introduced the option for HTTPS connections from unauthenticated clients to be redirected.

4.6.1 Redirect for HTTPS connections

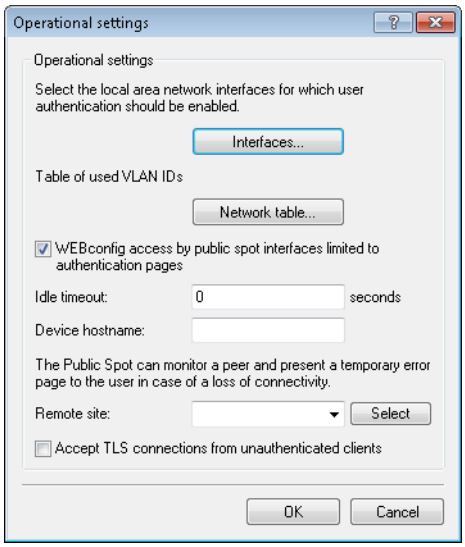
If an unauthenticated client attempts to access an HTTPS website via an interface operated by the Public Spot, the connection request is redirected to the Public Spot gateway itself, which then presents its login page to the user (as is also the case with HTTP). Usually, the user's browser displays a certificate warning, because the name or IP of the requested website is different from the name or IP address of the Public Spot. To prevent this and the increased load on the Public Spot from the HTTPS/TLS connections, this setting allows you to prevent HTTPS connections from being established for unauthenticated clients.

Once the client is authenticated, redirection is stopped and the client can establish any HTTP or HTTPS connection.

Modern clients carry out a "captive portal detection" via HTTP. The client attempts to access a certain URL via HTTP to check for the presence of a login page (from the Public Spot or other solutions). This mechanism is not affected by turning off the HTTPS redirect, since detection is usually via HTTP.

However, if unauthenticated WLAN clients should not perform connect requests over HTTP, this ineffective HTTPS redirect would place unnecessary load on the Public Spot gateway. For this reason it is possible to disable this HTTPS redirect. In this case, the user's browser displays a blank page.

In LANconfig, you configure the HTTPS redirect under **Public Spot** > **Server** > **Operational settings**.



To enable the HTTPS redirect, activate the option **Accept TLS connections from unauthenticated clients**. This option is disabled by default.

4.6.2 Additions to the Setup menu

Redirect TLS connections

Use this option to determine whether the Public Spot redirects HTTPS connections for unauthenticated clients. With this option disabled, unauthenticated clients are unable to establish HTTPS connections.

SNMP ID:

2.24.51

Telnet path:

Setup > **Public-Spot-Module**

Possible values:

No

The Public Spot does not perform HTTPS redirects for unauthenticated WLAN clients.

Yes

The Public Spot performs HTTPS redirects for unauthenticated WLAN clients.

Default:

No

4.7 Printout of bandwidth profile on the voucher

As of HiLCOS 10.12, the voucher printout optionally shows the user-specific bandwidth profile. It is entered into the voucher template with this new template identifier:

BANDWIDTHPROFNAME

Valid for:<pbelem>

This identifier contains the bandwidth profile that the user is associated with.

This identifier is available from HiLCOS 10.12. Templates featuring this identifier are not suitable for HiLCOS versions before 10.12.

RXBANDWIDTH

Valid for:<pbelem>

This identifier contains the maximum reception bandwidth of the bandwidth profile.

This identifier is available from HiLCOS 10.12. Templates featuring this identifier are not suitable for HiLCOS versions before 10.12.

TXBANDWIDTH

Valid for:<pbelem>

This identifier contains the maximum transmission bandwidth of the bandwidth profile.

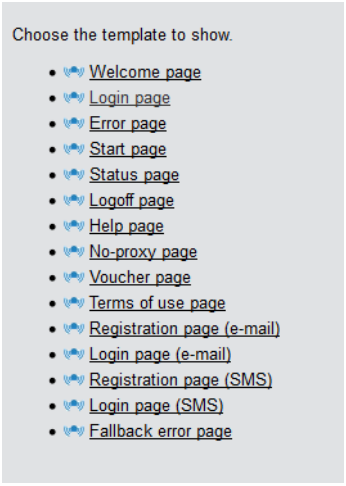
This identifier is available from HiLCOS 10.12. Templates featuring this identifier are not suitable for HiLCOS versions before 10.12.

4.8 Template preview

As of HiLCOS 10.12 you have the option to preview the uploaded Public Spot templates.

4.8.1 Template preview in WEBconfig

You can view the changes to the Public Spot templates in WEBconfig by switching to the view **Extras** > **Public Spot template preview**.

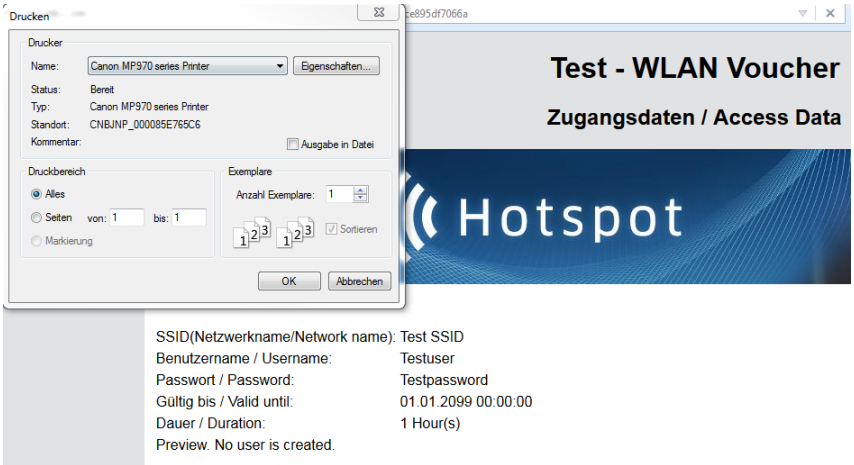


Select a template to display from the list.

The selected template is displayed in the same browser window. Use the "Back" function of your browser to return to WEBconfig.

Some templates contain JavaScript code. This code is executed when the template is invoked. For example, the "Voucher page" template contains code that starts a printout when the page is displayed.

This page contains test data. However, no user is created at this point. This allows you to test the template and print it out.



If a template does not exist or cannot be found, an error message is displayed by WEBconfig.

4.9 Logging DNS requests and responses to external SYSLOG servers

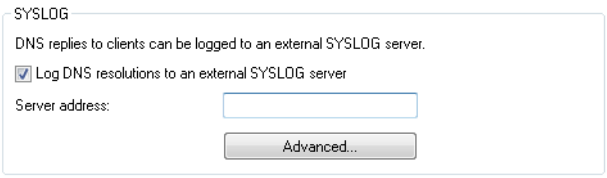
As of HiLCOS 10.12, it is possible to log the DNS requests and responses for the domains that are invoked by clients.

4.9.1 Logging DNS requests and responses to external SYSLOG servers

The DNS server in Hirschmann devices resolves the DNS queries from clients. SYSLOG provides an overview of the clients, the names they requested, and the responses they received.

It is not possible to use the router/AP's own internal SYSLOG. For this reason it is necessary to employ an external SYSLOG server.

DNS logging is configured in LANconfig under **IPv4** > **DNS** in the section **SYSLOG**.



Log the DNS resolutions on an external SYSLOG server

Select this option to enable the DNS logging.

This option is independent of the setting in the SYSLOG module. Even if the SYSLOG module is disabled (setting under **Log & Trace** > **General** in the section **SYSLOG**), DNS logging is carried out nevertheless.

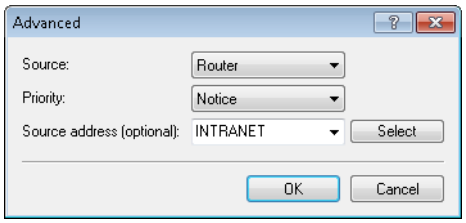
The corresponding SYSLOG message is structured as follows:

```
PACKET_INFO: DNS for <IP address>, TID {Hostname}: Resource-Record
```

Server address

Contains the IP address or the DNS name of the SYSLOG server.

The settings behind the button **Advanced** influence the content of SYSLOG messages.



Source

Contains the log source as displayed in the SYSLOG messages.

Priority

Contains the log level as displayed in the SYSLOG messages.

Source address (optional)

Contains the source address that is shown in the SYSLOG messages.

4.9.2 Additions to the Setup menu

Syslog

Use this directory to configure the SYSLOG logging of DNS requests.

SNMP ID:

2.17.20

Telnet path:

Setup > **DNS**

Log DNS resolutions

This option enables or disables (default setting) the sending of SYSLOG messages in the case of DNS requests.

This switch is independent of the global switch in the SYSLOG module under **Setup** > **SYSLOG** > **Operating**. If you enable this option to log DNS requests, the DNS server in the device sends the corresponding SYSLOG messages to a SYSLOG server even if the global SYSLOG module is disabled.

Each DNS resolution (`ANSWER` record or `ADDITIONAL` record) generates a SYSLOG message with the following structure `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Resource-Record`.

The parameters have the following meanings:

- The `TID` (transaction ID) contains a 4-character hexadecimal code.
- The `{host name}` is only part of the message if the DNS server cannot resolve it without a DNS request (as in the firewall log, as well).
- The `resource record` consists of three parts: The request, the type or class, and the IP resolution (for example `www.mydomain.com STD A resolved to 193.99.144.32`)

SNMP ID:

2.17.20.1

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

No

Disables the logging of DNS requests and responses.

Yes

Enables the logging of DNS requests and responses.

Default:

No

Log server address

The log server address identifies the SYSLOG server by means of its DNS name or an IP address.

The use of the IP addresses `127.0.0.1` and `::1` to force the use of an external server is not permitted.

SNMP ID:

2.17.20.2

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Log source

Contains the log source as displayed in the SYSLOG messages.

SNMP ID:

2.17.20.3

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

System
Login
System time
Console login
Connections
Accounting
Administration
Router

Default:

Router

Log level

Contains the priority that is shown in the SYSLOG messages.

SNMP ID:

2.17.20.4

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

Emergency
Alert
Critical
Error
Warning
Notice
Info
Debug

Default:

Notice

Loopback-Addr.

Here you can optionally specify another address (name or IP) used by your device to identify itself to the SYSLOG server as the sender. By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.

If the source address set here is a loopback address, this will be used **unmasked** even on masked remote clients.

SNMP ID:

2.17.20.5

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Special values:

Name of the IP networks whose address should be used
“INT” for the address of the first Intranet
“DMZ” for the address of the first DMZ
LB0 to LBF for the 16 loopback addresses
Any valid IP address

Facility

The mapping of sources to specific facilities.

SNMP ID:

2.22.3.2

Telnet path:

Setup > **SYSLOG** > **Facility-Mapper**

Possible values:

KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS
UUCP
CRON
AUTHPRIV
SYSTEM0
SYSTEM1
SYSTEM2
SYSTEM3
SYSTEM4
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7

IP address

Contains the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a DNS name.

SNMP ID:

2.22.2.7

Telnet path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

4.10 Protection against brute force attacks

Starting with version 10.12, HiLCOS provides protection against brute-force attacks on the Public Spot.

4.10.1 Protection against brute force attacks

Brute force attacks are the most common type of attack on networks. This method of attack tries out a variety of potential passwords in the shortest possible time, until the right one is found. One form of protection against brute-force attacks is to react to one or more successive failed attempts by delaying the time until the entry is allowed to be attempted again.

Configure the protection against brute-force attacks in LANconfig under **Public Spot** > **Server** in the section **Brute force protection**.

Lock after

Specify how many unsuccessful attempts are permitted before the entry lock takes effect.

Lock duration

Specify for how long the entry lock is to apply.

You can use the console to display the current status of the brute-force protection with the command `show pbbruteprotector`:

`show pbbruteprotector`

Shows all of the MAC addresses that are associated with the Public Spot.

`show pbbruteprotector [MAC address[ MAC address [ ...]]]`

Specifying one or more space-separated MAC addresses shows the status of all of the respective MAC addresses.

MAC addresses are specified in the format `11:22:33:44:55:66`, `11-22-33-44-55-66` or `112233445566`.

4.10.2 Additions to the Setup menu

Brute force protection

This menu contains the settings for the brute-force protection used by the Public Spot.

SNMP ID:

2.24.49

Telnet path:

Setup > **Public-Spot-Module**

Max. login tries

Specify how many unsuccessful attempts are permitted before the login block takes effect.

SNMP ID:

2.24.49.1

Telnet path:

Setup > **Public-Spot-Module** > **Brute-Force-Protection**

Possible values:

Max. 3 characters from `[0-9]`

Default:

10

Blocking time in minutes

Specify how long the login block of the brute-force protection applies.

SNMP ID:

2.24.49.2

Telnet path:

Setup > **Public-Spot-Module** > **Brute-Force-Protection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

60

Unblocking check in seconds

Specify the interval after which the AP checks for the expiry of a login block for a MAC address.

SNMP ID:

2.24.49.3

Telnet path:

Setup > **Public-Spot-Module** > **Brute-Force-Protection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

60

Unblock

Use this action to remove the login block on a MAC address. Enter the parameters as one or more space-separated MAC addresses.

MAC addresses are specified in the format `11:22:33:44:55:66`, `11-22-33-44-55-66` or `112233445566`.

SNMP ID:

2.24.49.4

Telnet path:

Setup > **Public-Spot-Module** > **Brute-Force-Protection**

4.11 Additional memory locations for your own Public Spot template images

As of HiLCOS 10.12, additional memory locations are available for your own Public Spot template images.

4.11.1 Embedding graphics in user-created template pages

Images for your vouchers can now be uploaded into the device because a further five images slots (voucher image 1 to voucher image 5) are now available for your pages. These images are permanently stored in the flash memory of the device.

How to transfer the images into the device is described in the section *Custom header images for variable screen widths*. When uploading, set the **Certificate type** to "Public Spot - voucher image 1" to "Public Spot - voucher image 5".

Modify the HTML template of the relevant voucher (e.g. with a text editor such as Notepad++) and reference the uploaded images by including the following in the template: `<img src="/images/voucherimg1">` to `<img src="/images/voucherimg5">`. How to set up a custom template page is described in the section *Setting up a customized template page*.

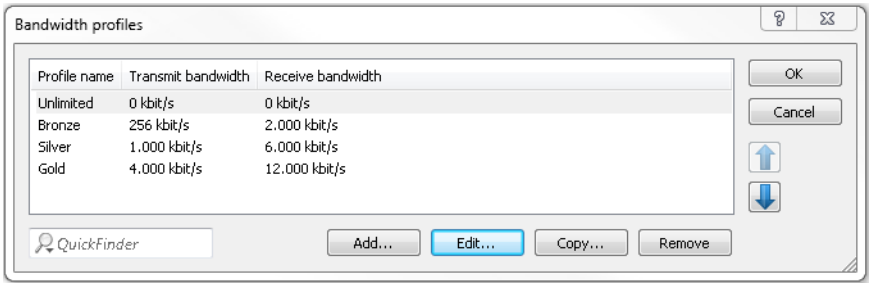
4.11.2 Predefined bandwidth profiles

As of HiLCOS 10.12 you have the option of using predefined bandwidth profiles in the wizard **Create Public Spot account**.

Using the window **Public-Spot** > **Wizard** > **Bandwidth profiles**, you have the ability to set up profiles that limit the available bandwidth (uplink and downlink) for Public Spot users. You can select a predefined profile or create your own bandwidth profiles that meet your needs. These profiles can be assigned to new users when access is created for the Public Spot by calling the Setup-Wizard **Create Public Spot account** in WEBconfig.

Integrating predefined bandwidth profiles

From the four predefined profiles, select the bandwidth profile that closest meets your requirements:



Unlimited

No restriction in the transmit and receive bandwidth.

These values refer to the transmit bandwidth (TX) and receive bandwidth (RX) from the perspective of the client.

Bronze

The transmit (TX) bandwidth is 256 kbps, the receive (RX) bandwidth is 2 Mbps.

Silver

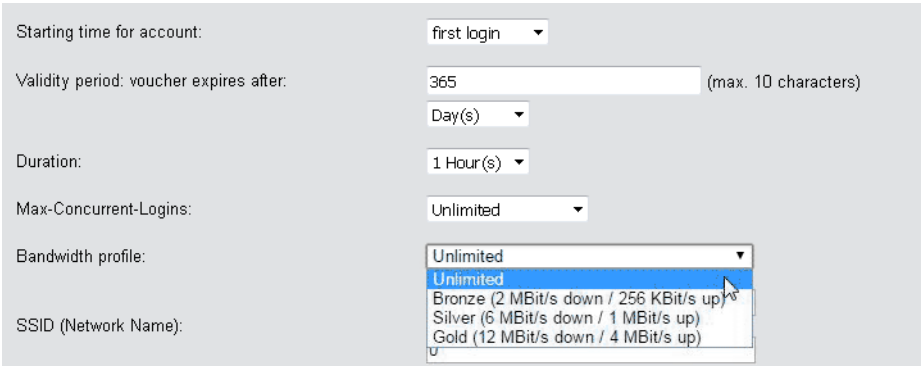
The transmit (TX) bandwidth is 1 Mbps, the receive (RX) bandwidth is 6 Mbps.

Gold

The transmit (TX) bandwidth is 4 Mbps, the receive (RX) bandwidth is 12 Mbps.

You have the option of customizing the predefined entries to meet your requirements. Select the profile for editing and click the button **Edit**. Alternatively, you can create your own profiles.

The selection dialog in WEBconfig has changed as follows:



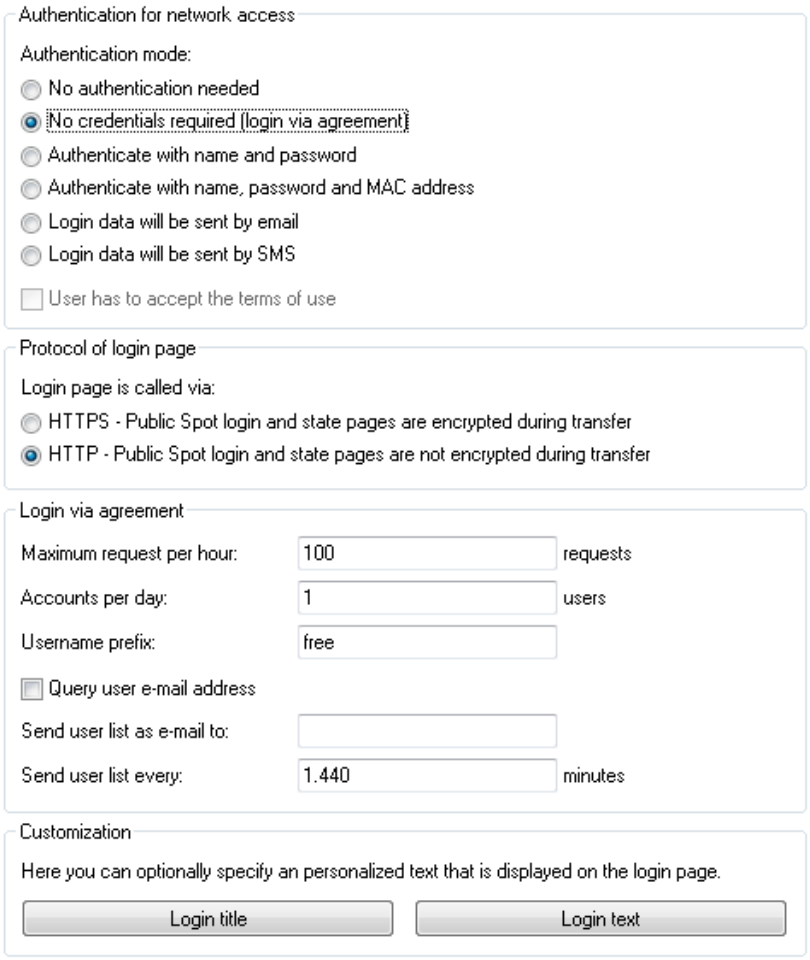
4.12 Requesting the user e-mail address upon "login via agreement"

As of HiLCOS 10.12, you can optionally require users who wish to authenticate at your Public Spot to enter an e-mail address.

4.12.1 Configuring an address request with LANconfig

Users wishing to authenticate at your Public Spot can optionally be required to register themselves first by entering an e-mail address. The network access authentication setting is located in the dialog **Public Spot** > **Authentication** in the section "Login via agreement".

Changes to the dialog are as follows:



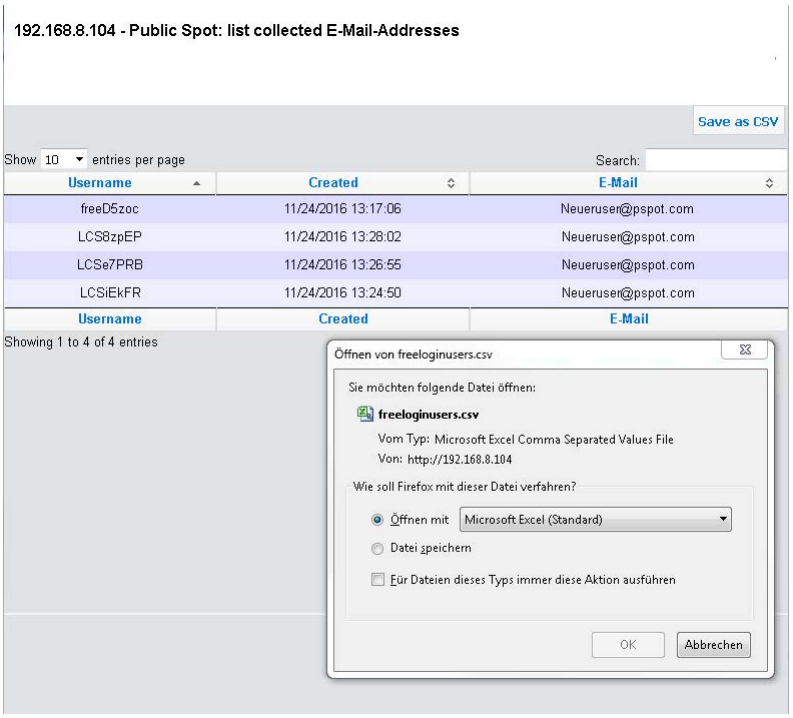
- **Query user e-mail address**: Enable this check box in order to query the user's e-mail address as a requirement for using the Public Spot. The device automatically enters the e-mail address specified here into the comments box of

the newly created RADIUS user. Once a day a list of all of the available addresses is stored in the flash memory of the device. This list is boot persistent.

- **Send user list as e-mail to**: Enter the e-mail address where the address list is to be sent. Only new entries that have been added since the last submission are sent. The address list is transmitted as a CSV file.
- **Send user list every**: This sets the interval at which the updated address list is sent to the specified e-mail address. This value is specified in minutes.

The Setup Wizard **Public Spot: list collected e-mail-addresses** in WEBconfig allows you to view the registered addresses and to export them as a CSV file.

Please note that this wizard is only visible when the "Query user e-mail address" option is enabled. It may be necessary to login to the device again.



4.12.2 Additions to the Setup menu

Require e-mail

This entry allows you to specify whether the e-mail address of the user should be requested.

SNMP ID:

2.24.41.4.4

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

No
Yes

Default:

No

E-Mail-List-Recipient

This entry contains the e-mail address to which the list of requested e-mail addresses is sent.

If you have already set the recipient e-mail address in LANconfig, it will be shown here.

SNMP ID:

2.24.41.4.7

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **Login-via-agreement**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

4.12.3 Additions to the Status menu

Free login

This menu enables you to see or delete users of the authentication mode "Login via agreement".

SNMP ID:

1.44.17

Telnet path:

Status > **Public-Spot**

Users

This entry displays all of the active users of the authentication mode "Login via agreement".

SNMP ID:

1.44.17.1

Telnet path:

Status > **Public-Spot** > **Free-Login**

Possible values:

User name
Displays the name of the created user.

Created
The time when the user was created.

E-mail
Displays the e-mail address entered for the created user

This field contains information only if the option "Query user e-mail address" is enabled.

Delete user

This menu enables you to delete users of the authentication mode "Login via agreement".

SNMP ID:

1.44.17.2

Telnet path:

Status > **Public-Spot** > **Free-Login**

4.13 Configuring the headline of the Public Spot login page

As of HiLCOS 10.12, you have the option of adding a headline to the login page of your Public Spot.

You can enter the title of your login page in six different languages. The available languages are English, German, French, Italian, Spanish and Dutch. The language used for the title of your Public Spot login page depends on the browser language set by the user.

4.13.1 Customized text or login title for the login page

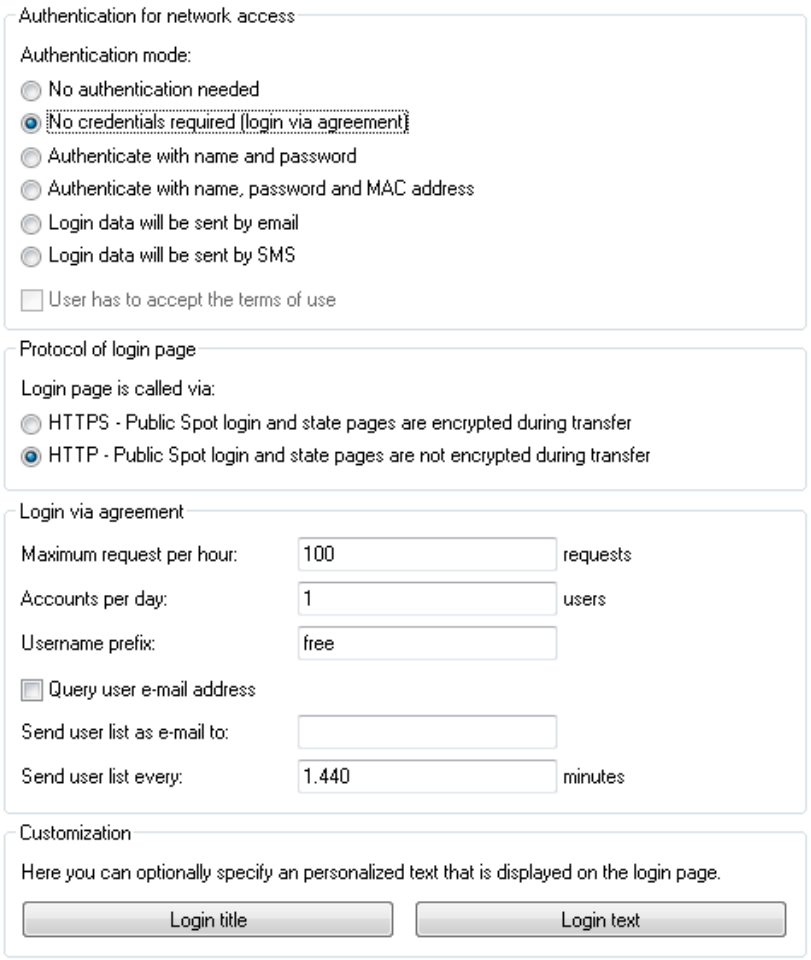
The Public Spot module gives you the option to specify customized **login text** and a **login title**, which appear on the login page in the box of the login form. The title and the text can be entered for a number of languages (English, German, French, Italian, Spanish and Dutch). The language displayed by the device depends on the language settings of the user's Web browser. If no customized login text or title is specified for a language, then the device falls back to the English login text (if available).

Please note that the login text and the login title are separate items.

Carry out the following steps to set up customized text or title on the login page.

1. In LANconfig, open the configuration dialog for the device.

2. Navigate to the dialog **Public Spot** > **Authentication**, click on the button **Login text** or **Login title** and select a language.



3. In the dialog that opens, enter the text that your Public Spot should display to users. You can enter an HTML string with max. 254 characters composed of:

   ```
   [Leerzeichen][0-9][A-Z[a-z] @{|}~!$%&amp;'()+-,/:;&lt;=>?[\]^_.#*
   ```

   LANconfig automatically transforms umlauts into their respective equivalents (ü to ue; ß to ss; etc.). To type umlauts, use their HTML equivalents (such as `ü` for ü), because the text is directly embedded in the Web page. You can also use HTML tags to structure and format the text. Example:

   ```
   Welcome!<br/><i>Please complete this form.</i>)
   ```

4. Click **OK** to complete your entries and load the configuration back to the device.

Once the configuration has been written successfully, the new login text and login title appears the next time the Public Spot page is called.

4.13.2 Additions to the Setup menu

Login instructions

This menu is used to set a login title for your Public Spot page. You can define the title in six languages (English, German, French, Italian, Spanish and Dutch).

SNMP ID:

2.24.61

Telnet path:

Setup > **Public-Spot-Module**

Language

This entry displays the language selected for the login title.

SNMP ID:

2.24.61.1

Telnet path:

Setup > **Public-Spot-Module** > **Login-Instructions**

Contents

Enter the login title for your Public Spot here.

SNMP ID:

2.24.61.1

Telnet path:

Setup > **Public-Spot-Module** > **Login-Instructions**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

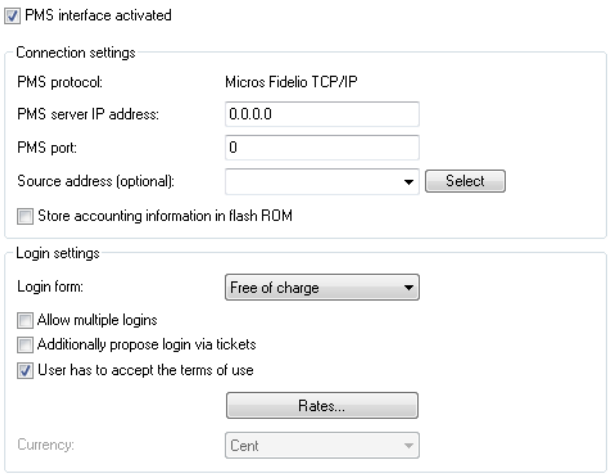
4.14 Confirmation of the terms of use on the PMS-login page

As of HiLCOS 10.12, you have the option of requiring your users to accept the terms and conditions of use of your Public Spot on the PMS-login page.

4.14.1 Using LANconfig to configure confirmation of the terms of use on the PMS-login page

In LANconfig, navigate to **Public-Spot** > **PMS interface**, go to the "Login settings" section, and activate the checkbox **User has to accept the terms of use**.

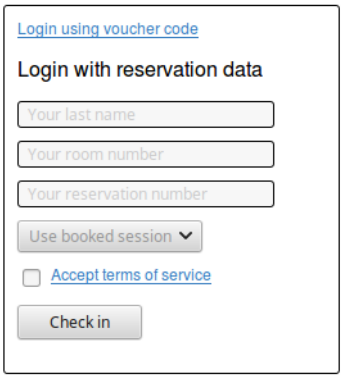
Please note that using this option requires the PMS interface to be enabled.



The dialog for the PMS interface has changed as follows:

- **User has to accept the terms of use**: Enable this checkbox in order for hotel guests to accept the terms and conditions for the use of your hotspot.

With the option enabled, the PMS-login page displays the checkbox for confirming the terms of use.



4.14.2 Additions to the Setup menu

User-Must-Accept-GTC

With this setting you enable or disable the confirmation of the terms of use on the PMS-login page.

SNMP ID:

2.64.11.14

Telnet path:

Setup > **PMS-Interface** > **Login-Form**

Possible values:

No

The user is not prompted to accept the terms of use.

Yes

The user is prompted to accept the terms of use.

Default:

No

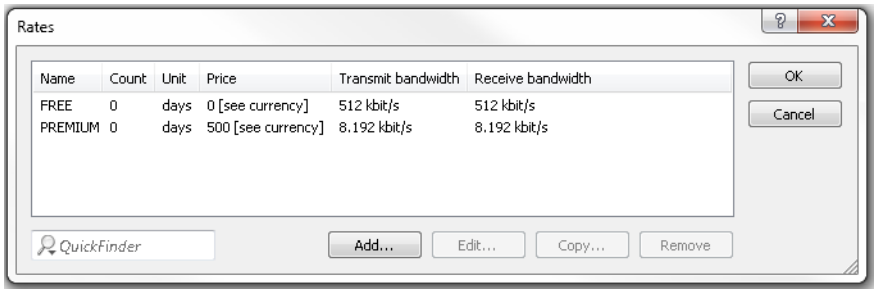
4.15 Tx and Rx bandwidths configurable for rates in the PMS module

As of HiLCOS 10.12, you have the option to limit the transmit and receive bandwidths for each of the rates configured in the PMS module, and to give each rate an appropriate name (e.g. "Free" and "Premium"). When choosing a rate on the Public Spot login page, users see the rates along with their configured names.

If rates are already entered in the configuration at the time of a firmware update, these are automatically given a name according to the pattern **Rate_1** to **Rate_n**.

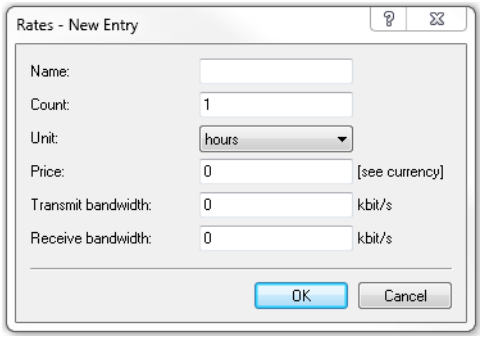
4.15.1 Using LANconfig to configure Tx and Rx bandwidths for rates in the PMS module

To configure the rates in the PMS interface of your device, go to the menu **Public-Spot** > **PMS-Interface** > **Rates**.



You can edit existing rates or add new entries to the table. Changes to the dialog are as follows:

- **Rates**: If you offer fee-based Internet access, this table is used to manage the tariff rates for the accounting.



- **Name**: Specify a descriptive name for the rate here.
- **Count**: Enter the rate for the time quota, for example, `1`. Combined with the unit, this is the value shown in the screenshot above, e.g., 1 hour.
- **Unit**: Select the unit for the time quota from the list. Possible values are: `Minutes`, `Hours`, `Days`
- **Price** Enter the amount charged for the time quota. In combination with the currency selected in the Login settings, the value amounts to 50 cents, for example.
- **TX bandwidth**: Here you specify the maximum transmit bandwidth for this rate.
- **RX bandwidth**: Here you specify the maximum receive bandwidth for this rate.

A temporary logout from the Public Spot does not change the expiry time of a purchased time quota. It is not possible to "pause" a previously purchased time credit in order to restart it at a later point in time. The countdown starts as of the purchase of the time credit regardless of the login status.

4.15.2 Additions to the Setup menu

Name

Use this entry to specify a name for this rate.

SNMP ID:

2.64.15.4

Telnet path:

Setup > **PMS-Interface** > **Rate**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Tx bandwidth

Use this entry to restrict the transmit (Tx) bandwidth.

SNMP ID:

2.64.15.5

Telnet path:

Setup > **PMS-Interface** > **Rate**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The value "0" disables the restriction of the transmit bandwidth.

Rx bandwidth

Use this entry to restrict the receive (Rx) bandwidth.

SNMP ID:

2.64.15.6

Telnet path:

Setup > **PMS-Interface** > **Rate**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

The value "0" disables the restriction of the receive bandwidth.

4.16 Support for RADIUS CoA

As of HiLCOS 10.12, the Public Spot module optionally accepts RADIUS CoA commands.

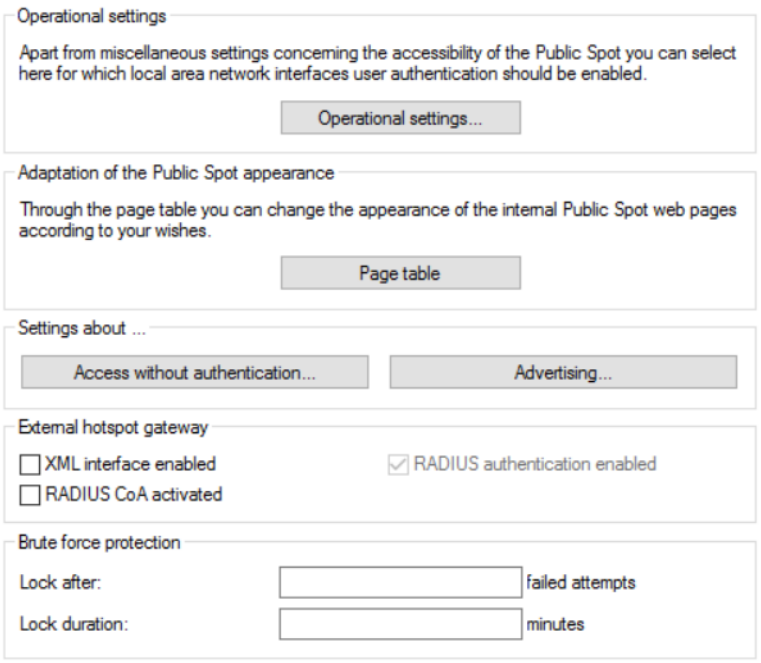
4.16.1 Enabling the acceptance of RADIUS CoA requests by the Public Spot

- The following steps assume that you have a functioning Public Spot that can be connected to an external hotspot gateway.
- The external hotspot gateway is located either in a freely accessible network provided by the Public Spot, or its address is included in the list of free hosts.

As an alternative to an XML-based `RADIUS_COA_REQUEST` via the XML interface, the Public Spot can also receive CoA requests by means of the RADIUS protocol from an external hotspot gateway or from an external RADIUS server. You have also have the option to use both forms of command transmission in parallel.

The following section explains how you enable RADIUS-CoA support as per RFC3576 in the Public Spot.

1. In LANconfig, open the device configuration and navigate to **Public Spot** > **Server**.



2. Set a checkmark under **RADIUS CoA activated**.
3. Now write the configuration back to the device.

From now on, the Public Spot processes any RADIUS CoA requests received from an external hotspot gateway.

4.16.2 Additions to the Setup menu

Accept CoA

As an alternative to an XML-based `RADIUS_COA_REQUEST` via the XML interface, the Public Spot can also receive CoA requests by means of the RADIUS protocol from an external hotspot gateway or from an external RADIUS server. You have also have the option to use both forms of command transmission in parallel.

With this entry you enable or disable the dynamic authorization of Public Spot users by means of RADIUS CoA via an external hotspot gateway.

SNMP ID:

2.24.55

Telnet path:

Setup > **Public-Spot-Module**

Possible values:

No

Dynamic authorization disabled. If there is a change to the RADIUS connection attributes, authorized users remain unaffected until their session expires.

Yes

Dynamic authorization enabled. The external gateway is able to modify the connection attributes of authorized users, or to disconnect existing sessions.

Default:

No

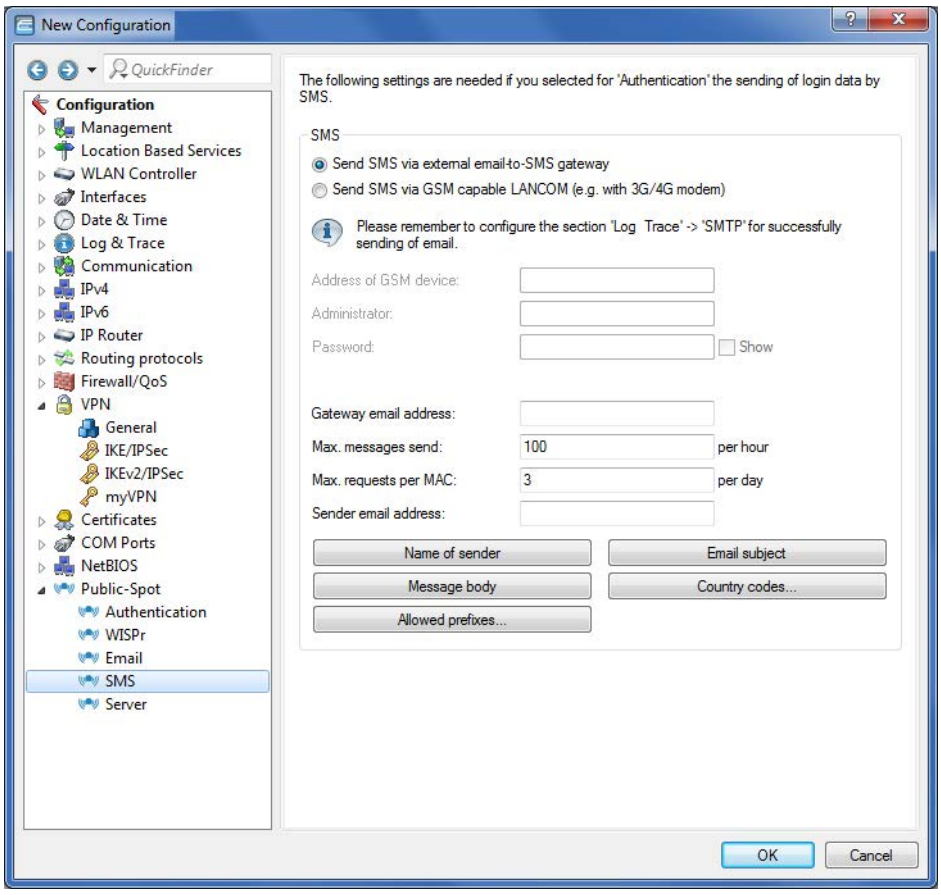
4.17 Independent user authentication (Smart Ticket)

4.17.1 Restricting the allowed country codes when using SmartTicket via SMS

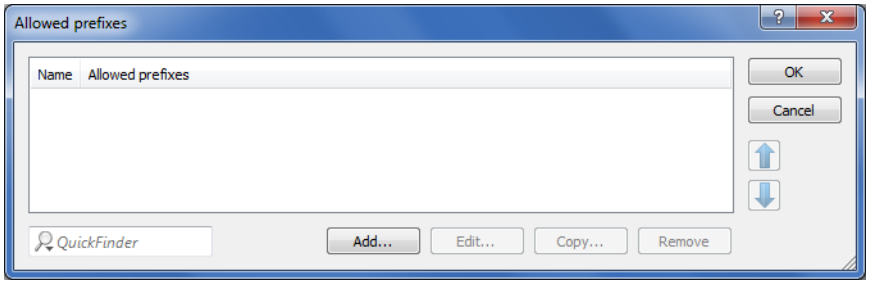
As of HiLCOS 10.12 you have the option to restrict the permitted area codes for each country.

Restricting the permitted area codes prevents SMS messages from being sent to expensive premium or service call numbers.

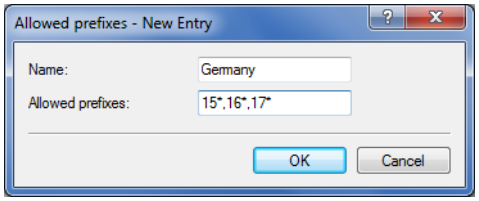
This avoids unnecessarily high costs when operating authorization by SMS.



1. Click the button **Allowed prefixes**.



2. Click **Add**.



3. Enter the name for the country into the **Name** input box.
4. You can limit the transmission of SMS text messages to certain area codes for each country by entering the permissible codes followed by a '*' into a comma-separated list. An example for German mobile phone providers: `15*, 16*, 17*`.

If you do not make an entry for a country in this table, all country codes will be allowed. Beforehand, an entry must have been created for this country in the Allowed-Country-Codes table.

4.17.2 Additions to the Setup menu

Restricting the allowed country codes when using SmartTicket via SMS

In this table you specify the permitted country codes for the option SmartTicket via SMS. Each country requires an entry in the Allowed-Country-Codes table.

SNMP ID:

2.24.41.2.26

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication**

Country name

This is where you enter the name of the allowed country (e.g., Germany or DE) for which access to certain area dialing codes is to be restricted.

Beforehand, an entry must have been created for this country in the Allowed-Country-Codes table.

SNMP ID:

2.24.41.2.26.1

Telnet path:

Setup > **Public-Spot-Module** > **Authentication-Modules** > **e-mail2Sms-Authentication** > **Allowed-Prefixes**

Possible values:

Max. 150 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

Germany

5 VPN

5.1 IKEv2 support

As of HiLCOS 10.12, HiLCOS supports IKEv2.

5.1.1 Functions of the VPN module

This section lists all of the functions and properties of the HiLCOS VPN module. Experts of the VPN sector are offered a highly compressed summary of the performance of the function. Understanding the terminology requires a sound knowledge of the technical fundamentals of VPN. However, for commissioning and normal operation of the VPN, this information is non-essential.

- VPN tunnel via leased lines, switched connections and IP networks
- Dynamic VPN: Public IP addresses can be static or dynamic (establishing a connection with remote sites using dynamic IP addresses requires ISDN)
- VPN in accordance with IPSec standard
- IPSec protocols ESP, AH and IPCOMP in tunnel mode
- Hash algorithms:
  - HMAC-MD5-96, hash length 128 bits
  - HMAC-SHA-1-96, hash length 160 bits
  - HMAC-SHA-1-256, hash length 256 bits
  - HMAC-SHA-1-384, hash length 384 bits
  - HMAC-SHA-1-512, hash length 512 bits
- Compression with “Deflate” (ZLIB)
- Key management as per ISAKMP (IKEv1, IKEv2)
- Symmetrical encryption methods
  - AES, key lengths of 128, 192 and 256 bits
  - Triple-DES (3DES), key length 168 bit
  - Blowfish, key length 128 - 448 bits
  - CAST, key length 128 bits
  - DES, key length 56 bits
- IKEv1 main and aggressive mode
- IKEv1/IKEv2 config mode
- IKEv1 with pre-shared keys and IKEv2
- IKEv1 and IKEv2 with RSA signature and digital certificates (X.509)
- Key exchange via Oakley, Diffie-Hellman algorithm with key lengths 768 bits, 1024 bits, 1536 bits, 2048 bits, 3072 bits and 4096 bits (well-known groups 1, 2, 5, 14, 15 and 16)

5.1.2 IKEv2

Hirschmann devices are capable of VPN with IKEv1 and IKEv2.

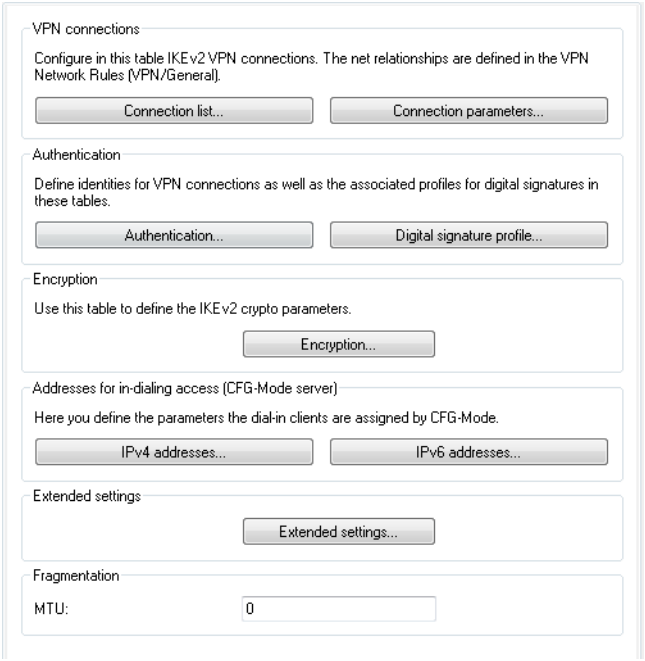
IKEv2 facilitates a fast and secure establishment of VPN tunnels. For the first time it is now possible to operate encrypted networking between IPv6-based sites and IPv4-based sites by means of the mixed mode.

Manually configuring a VPN connection that uses IKEv1 is complex and error prone. Consequently, many IPSec implementations have incompatible configurations, which causes the VPN connections between the devices to fail. The IKEv2 configuration in HiLCOS gives administrators a reliable method of setting up a configuration that matches that of the remote station. For example, administrators have a choice of several Diffie-Hellman groups. At the same time, the revised user interface presents recommended default values for many of the configuration parameters. The simplified configuration with IKEv2 eliminates sources of error, which results in a lower administrative overhead. Further, VPN connection establishment with IKEv2 offers better performance, because IKEv2 only exchanges 4 packets when negotiating a VPN tunnel (one REQUEST per VPN partner and one REPLY), rather than the 6 required by IKEv1 in the "aggressive/quick mode" or 12 in "main mode". The standard of security is just as high with IKEv2 as with IKEv1.

Operating IKEv2 supports *RFC 7296*, *RFC 7427* and, in the IKEv2 client mode, *RFC 5685*.

5.1.3 Configuring IKEv2 with LANconfig

IKEv2 is configured under **VPN** > **IKEv2/IPSec**.



VPN connections

In this section, you configure the IKEv2 VPN connections and the connection parameters.

Authentication

This table is used to define the identities for your VPN connections.

Digital signature profile

This table is used to specify the authentication methods for your VPN connections.

Encryption

This table is used to set the encryption parameters.

Addresses for dial-in access (CFG mode server)

Use this table to specify the parameters that the device CFG mode assigns to the dial-in clients.

Extended settings

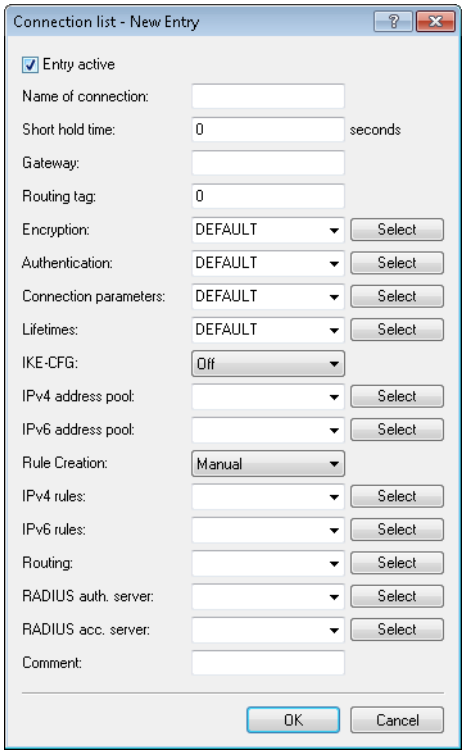
This section is used to configure the settings for the authentication of other remote identities, the IKEv2 rekeying parameters, and the prefixes for IKEv2 routing.

In order to configure an IKEv2 connection, you first need to make an entry in the **Connection list**. HiLCOS contains default entries in order to minimize the effort of configuration. Most of these entries contain default parameters with common settings for strong encryption algorithms, dead-peer-detection, and lifetimes. All you need to do is specify the address of the VPN remote peer, the authentication parameters (under **Authentication**), and the VPN rules (under **VPN** > **General** > **Network rules**).

The console command `show vpn` displays whether the VPN connection was established successfully.

Connection list

In this table, you configure the IKEv2 connections to VPN partners.



Entry active

Enables or disables the connection to this VPN peer.

Name of connection

Contains the name of the connection to the remote station.

Short hold time

Specifies the hold time in seconds for which the device stays connected if there is no data flow.

Gateway

Contains the address (IPv4, IPv6 or FQDN) of the VPN partner.

Routing tag

Contains the routing tag for this VPN connection.

Encryption

Specifies the encryption used for the VPN connection. The corresponding entry is located in the **Encryption** table.

Authentication

Specifies the authentication method used for the VPN connection. The corresponding entry is located in the **Authentication** table.

Connection parameters

Specifies the general parameters used for the VPN connection. The corresponding entry is located in the **Connection parameters** table.

Validity period

Specifies the lifetime of the key used for the VPN connection. The corresponding entry is located in the **Extended settings** > **Lifetimes** table.

IKE-CFG

Specifies the IKEv2 config mode of this connection for RAS dial-ins.

Possible values are:

- Off: IKEv2 config mode is disabled
- Server: The router distributes configuration parameters (such as addresses or the DNS server) to VPN clients. The parameters to be distributed are configured in the IPv4 or IPv6 address pool.
- Client: The router requests the server for configuration parameters (e.g. addresses or the DNS server).

IPv4 address pool

IPv4 addresses and DNS server for dial-in access in the IKE CFG mode Server.

IPv6 address pool

IPv6 addresses and DNS server for dial-in access in the IKE CFG mode Server.

Rule creation

Specifies how VPN rules are created.

Possible values:

Automatic

The local intranet serves as the source network (private IP address range that the local VPN gateway itself belongs to). For automatically generated VPN rules, the target networks are those network ranges that have a remote VPN gateway set as their router.

When two simple local networks are connected, the automatic VPN can interpret the necessary network relationships from the IP address range in its own LAN and from the entry for the remote LAN in the IP routing table.

Manual

Rules are created for the network relationships in the same way as rules are defined manually for IPv4 or IPv6.

IPv4-Rules

Specifies which IPv4 rules apply to this VPN connection.

The IPv4 rules are located in the table **VPN** > **Network rules**.

IPv6-Rules

Specifies which IPv6 rules apply to this VPN connection.

The IPv6 rules are located in the table **VPN** > **Network rules**.

Routing

Specifies the routes that the remote site should transmit dynamically via IKE-CFG mode. This function is only available in the IKEv2 CFG mode for the client and server.

The routes for IPv4 and IPv6 connections are located in the **Extended settings** > **IPv4 routing/IPv6 routing** tables.

RADIUS auth. server

Specifies the RADIUS server for the VPN peer authorization. You configure the RADIUS server for IKEv2 under **VPN** > **IKEv2/IPSec** under **Extended settings**.

RADIUS auth. server

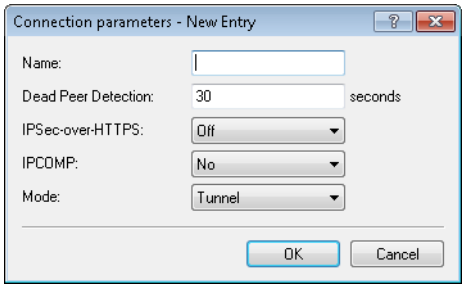
Specifies the RADIUS server for the VPN peer accounting. You configure the RADIUS server for IKEv2 under **VPN** > **IKEv2/IPSec** under **Extended settings**.

Comment

Enter a descriptive comment here.

Connection parameters

Use this table to specify the parameters of IKEv2 VPN connections that are not included in the SA negotiation. An entry named "DEFAULT" is provided with common settings.



Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** in the "Connection parameters" field.

Dead peer detection

Contains the time in seconds after which the device disconnects from the remote peer if there is a loss of contact.

IPSec-over-HTTPS

Specifies whether the connection uses IKEv2 over HTTPS.

IPCOMP

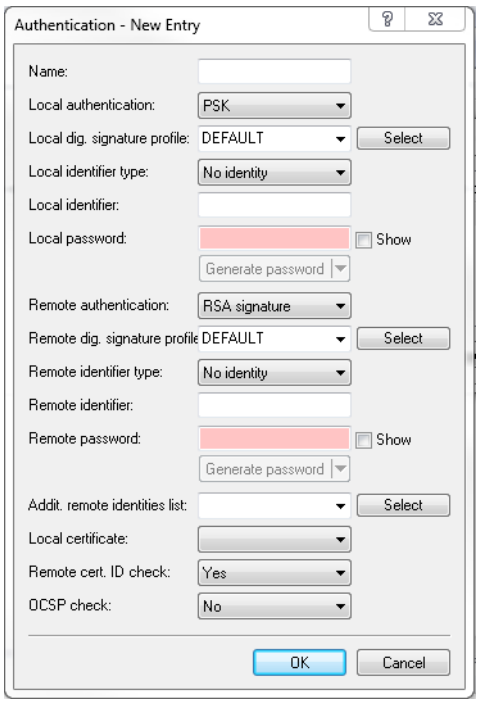
Specifies whether the devices transmit compressed IKEv2 data packets.

Mode

Specifies the mode of transmission.

Authentication

In this table, you configure the parameters for IKEv2 authentication of the local and at least one remote identifier.



Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** in the "Authentication" field.

Local authentication

Sets the authentication method for the local identity. Possible values are:

- PSK: Pre-shared key:
- RSA-Signature: Use of digital certificates with private RSA key and RSA signature scheme
- Digital signature: Use of configurable authentication methods with digital certificates as per *RFC 7427*. This procedure is an extensible and flexible authentication technique that allows padding and hash algorithms to be configured freely.

The device uses the authentication method configured here when connecting to the remote site. The method must match with a corresponding configuration at the remote site.

It is possible to use different authentication methods for the local and remote authentication. For example, the headquarters can identify itself by RSA signature, while branch offices or clients use PSK authentication.

Local digital signature profile

The profile name of the local digital signature profile that is used.

Local identifier type

Displays the ID type of the local identity. The device interprets the entry under "Local identifier" accordingly. Possible entries are:

- No identity: No identity is transmitted.
- IPv4 address: The device uses an IPv4 address as a local ID.
- IPv6 address: The device uses an IPv6 address as a local ID.
- Domain name (FQDN): The device uses a domain name as a local ID.

- E-mail address (FQUN): The device uses an e-mail address as a local ID.
- ASN.1 Distinguished Name: The device uses a distinguished name as a local ID (e.g. “CN=client01.example.com,O=test,C=DE”).
- Key ID (group name): The device uses the group name as a local ID. You can set any group name.

Local identifier

Contains the local identity. The significance of this entry depends on the setting under “Local identifier type”.

Local password

Contains the password of the local identity. The device uses this password to authenticate at the remote site. The local and remote password can be identical or different.

Remote authentication

Sets the authentication method for the remote identity. Possible values are:

- PSK: Pre-shared key:
- RSA-Signature: Use of digital certificates with private RSA key and RSA signature scheme
- Digital signature: Use of configurable authentication methods with digital certificates as per *RFC 7427*. This procedure is an extensible and flexible authentication technique that allows padding and hash algorithms to be configured freely.

The device uses the authentication method configured here when connecting to the remote site. The method must match with a corresponding configuration at the remote site.

It is possible to use different authentication methods for the local and remote authentication. For example, the headquarters can identify itself by RSA signature, while branch offices or clients use PSK authentication.

Remote digital signature profile

The profile name of the remote digital signature profile.

Remote identifier type

Displays the ID type that the device expects from the remote identifier. The device interprets the entry under “Remote identifier” accordingly. Possible entries are:

- No identity: The device accepts any ID from the remote device. The device to ignores entries in the “Remote identifier” field.
- IPv4 address: The device expects an IPv4 address as the remote ID.
- IPv6 address: The device expects an IPv6 address as the remote ID.
- Domain name (FQDN): The device expects a domain name as the remote ID.
- E-mail address (FQUN): The device expects an e-mail address as the remote ID.
- ASN.1 Distinguished Name: The device expects a distinguished name as a remote ID (e.g. “CN=client01.example.com,O=test,C=DE”).
- Key ID (group name): The device expects the group name as the remote ID.

Remote identifier

Contains the remote identity. The significance of this entry depends on the setting under “Remote identifier type”.

Remote password

Contains the password of the remote identity.

Addit. remote identities list

Redundant VPN scenarios allow the use of alternative remote identities.

Here you configure additional remote identities from the table **Extended settings** > **Identity list**.

Local certificate

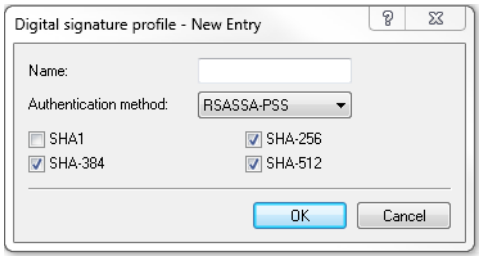
Displays the local certificate.

Remote certificate check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

Digital signature profile

In this table, you configure the parameters for IKEv2 authentication of the local and at least one remote identifier.



Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** in the "Authentication" field.

Authentication method

Sets the authentication method for the digital signature. Possible values are:

- RSASSA-PSS: RSA with improved probabilistic signature schema as per version 2.1 of PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1_5: RSA according to the older version of the signature schema as per version 1.5 of PKCS #1 (probabilistic signature scheme with appendix)

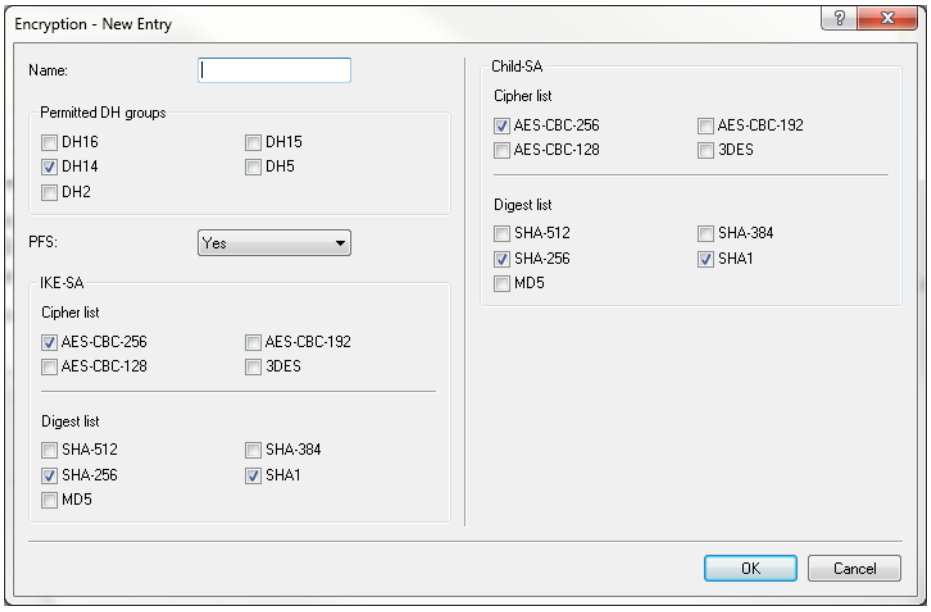
You also specify the secure hash algorithms (SHA) to be used.

Encryption

This table is used to configure the encryption parameters. An entry named "DEFAULT" is provided with common settings.

Multiple parameters can be selected. The device propagates these parameter lists in the IKE protocol and in CHILD SAs. The two VPN partners agree to use one of the algorithms in the propagated lists. While they are establishing the first IKE SA, the VPN partners agree to use the highest of the mutually propagated DH groups. The VPN partners use this DH group when they renew the IKE SAs, or when they create or renew the CHILD SAs (if PFS is enabled).

A connection will be established between the VPN partners if there are sets of encryption parameters that agree at both ends. If none of the parameters match, no connection can be established.



Name

Contains the unique name of this entry. You assign this name to the connections in the **Connection list** by selecting it from the "Encryption" field.

Permitted DH groups

Contains the selection of Diffie-Hellman groups used by the VPN partners to create a key for exchanging data. The higher the DH group selected, the more complex is the key that is generated. The following groups are currently supported:

- DH-2 (1024-bit modulus)
- DH-5 (1536-bit modulus)
- DH-14 (2048-bit modulus)
- DH-15 (3072-bit modulus)
- DH-16 (4096-bit modulus)

PFS

Specifies whether perfect forward secrecy (PFS) is enabled.

Cipher list

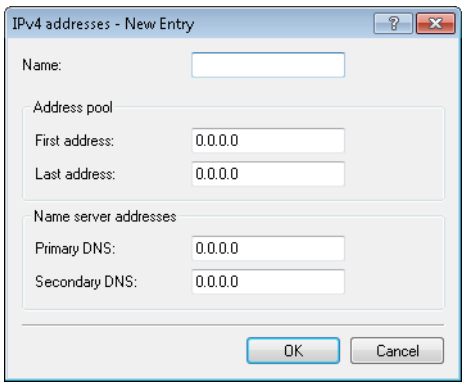
Specifies which encryption algorithms are enabled.

Digest list

Specifies which hash algorithms are enabled.

IPv4 addresses

Use this table to configure the IPv4 parameters that the device CFG mode assigns to the VPN clients.



Name

Contains the name of the interface for the dial-in access.

Address pool

First address

Here you enter the first IPv4 address of the pool of addresses that you want to provide to VPN clients.

End address

Here you enter the last IPv4 address of the pool of addresses that you want to provide to VPN clients.

Name server addresses

DNS default

Contains the primary DNS address.

DNS backup

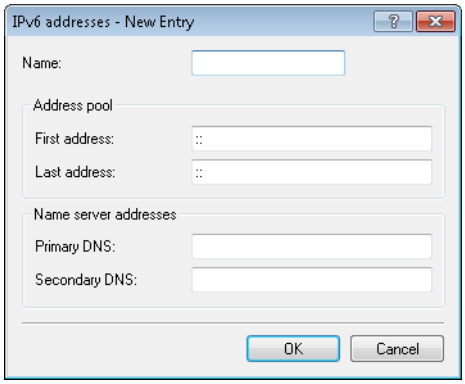
Contains the secondary DNS address.

IPv6 addresses

If the device operates as a “CFG-mode server”, it uses the IKEv2 configuration payload to assign an address from a local address pool to clients. Also, it can assign up to two DNS servers to the client.

To operate this, you use the VPN connection list to enable the CFG mode “Server” on the server and the CFG mode “Client” on the client.

Use this table to configure the IPv6 parameters that the device in the CFG mode “Server” assigns to VPN clients.



Name

Contains the name of the interface for the dial-in access.

Address pool

First address

Here you enter the first IPv6 address of the pool of addresses that you want to provide to VPN clients.

End address

Here you enter the last IPv6 address of the pool of addresses that you want to provide to VPN clients.

Name server addresses

DNS default

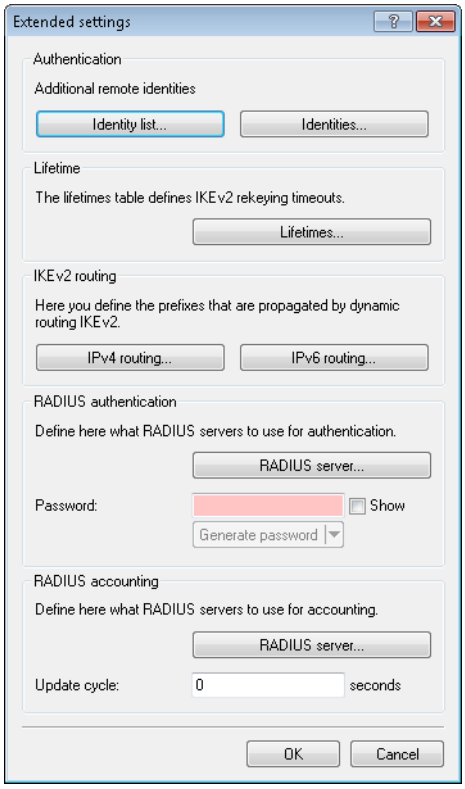
Contains the primary DNS address.

DNS backup

Contains the secondary DNS address.

Extended settings

Use this dialog to configure the settings for the authentication of other remote identities, the IKEv2 rekeying parameters, the prefixes for IKEv2 routing, and the RADIUS server for IKEv2.

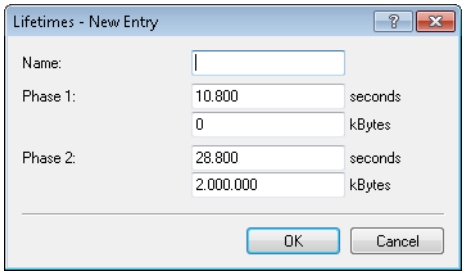


Lifetimes

Use this table to specify the IKEv2 rekeying parameters. An entry named "DEFAULT" is provided with common settings.

Depending on the phase, the device discriminates according to time or the amount of transmitting data. The parameter that reaches its limit first triggers the renewal of the corresponding IKEv2 key.

The value "0" means that the device sets no limit on the corresponding key.



Name

Contains the unique name of this entry.

Phase 1:

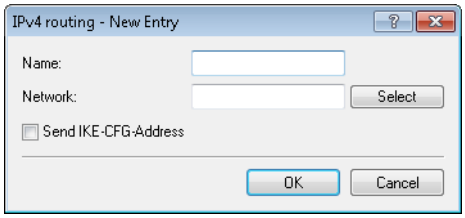
Contains the time in seconds or the data volume in kilobytes until the IKE SA key is renewed.

Phase 2:

Contains the time in seconds or the data volume in kilobytes until the CHILD SA key is renewed.

IPv4 routing

Use this table to configure the IPv4 networks that the device propagates via dynamic routing as per IKEv2.



Name

Contains the unique name of this entry.

Network

Contains the comma-separated list of IP subnets.

Networks are entered in the following available formats:

- IP address
- IP address/IP mask
- IP address/prefix length
- IP interface name

The IP subnets are configured under **IPv4** > **General** in the section **Own addresses**.

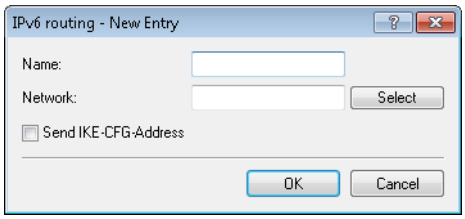
Send IKE-CFG address

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server).

This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. Hirschmann routers generate the necessary routes automatically.

IPv6 routing

Use this table to configure the IPv6 networks that the device propagates via dynamic routing as per IKEv2.



Name

Contains the unique name of this entry.

Network

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IPv6 address
- IPv6 address/prefix length
- IPv6 interface name

The IP subnets are configured under **IPv6** > **General** in the section **IPv6 networks**.

Send IKE-CFG address

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server).

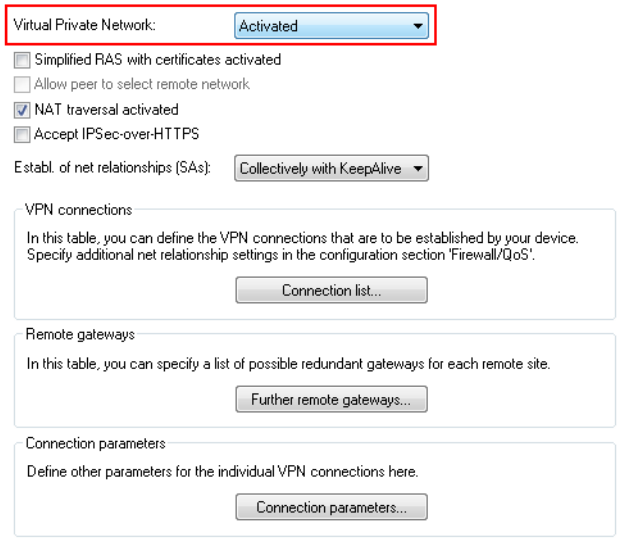
This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. Hirschmann routers generate the necessary routes automatically.

5.1.4 Tutorial: Setting up IKEv2 under LANconfig

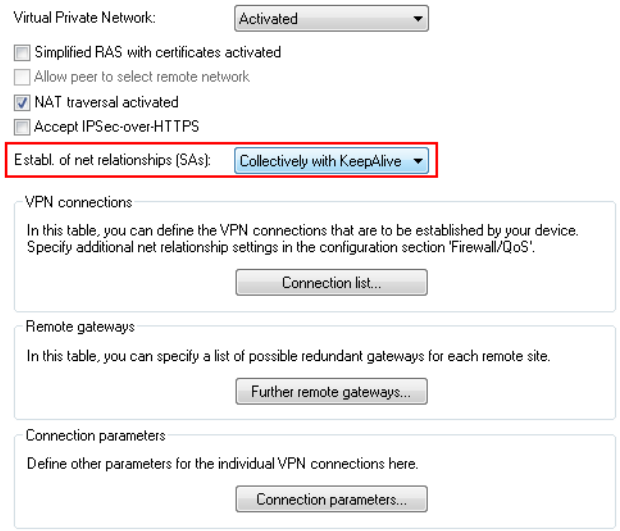
Initial situation: Two Hirschmann routers are connected via a WAN link. The requirement is to establish a secure VPN connection between them by means of IKEv2/IPSec VPN.

We assume that a WAN connection exists between the two devices.

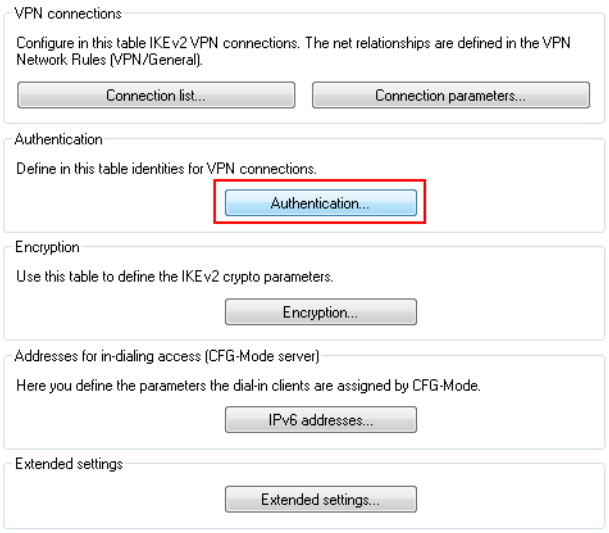
1. **Enabling VPN**: For both of the routers, open the menu item **VPN** > **General** and, under **Virtual Private Network**, select the option **Activated**. This enables VPN on that specific device.



2. **Configuration of the establishment of net relations (SAs)**: In order for net relations to be established correctly and according to the same schema, on each of the routers you should navigate to **Establishment of net relations (SAs)** and enable the option **Collectively with KeepAlive**.

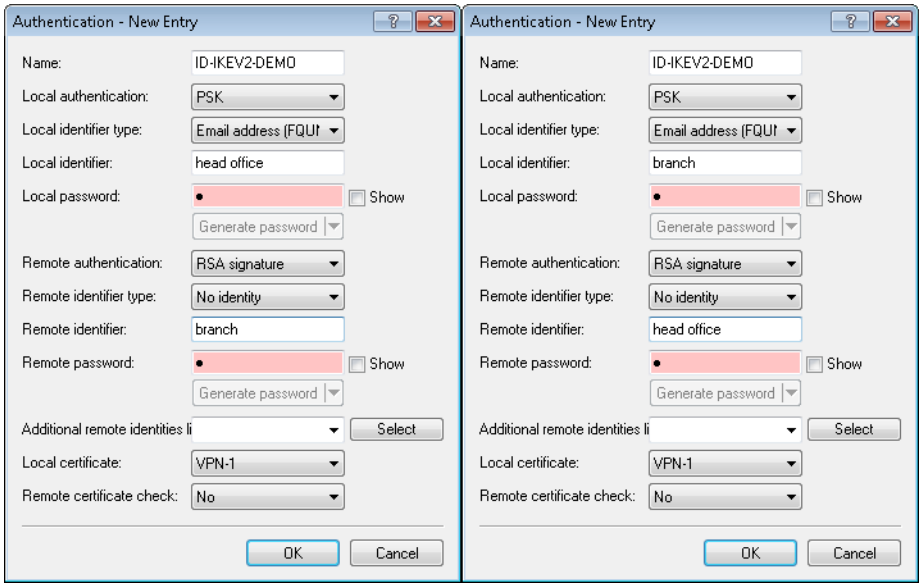


3. **Configuring the authentication**: Specify the type of authentication for the VPN connection. To do this, open the menu item **VPN** > **IKEv2/IPSec** and click the button **Authentication**.



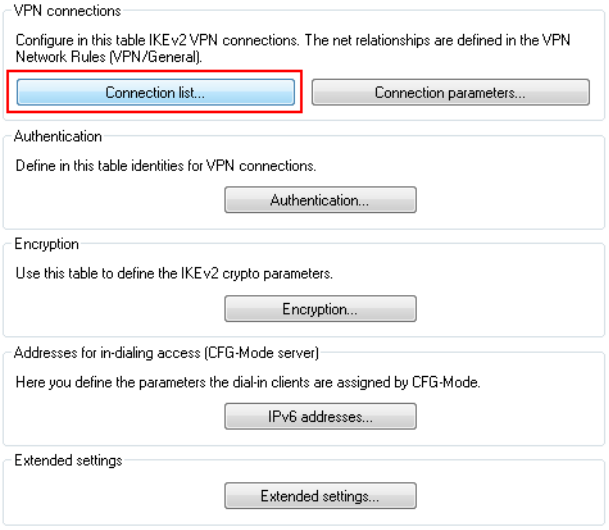
4. Click on the **Add** button to configure a new authentication type. Enter the information for the authentication of the VPN connection into the configuration window.

The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.



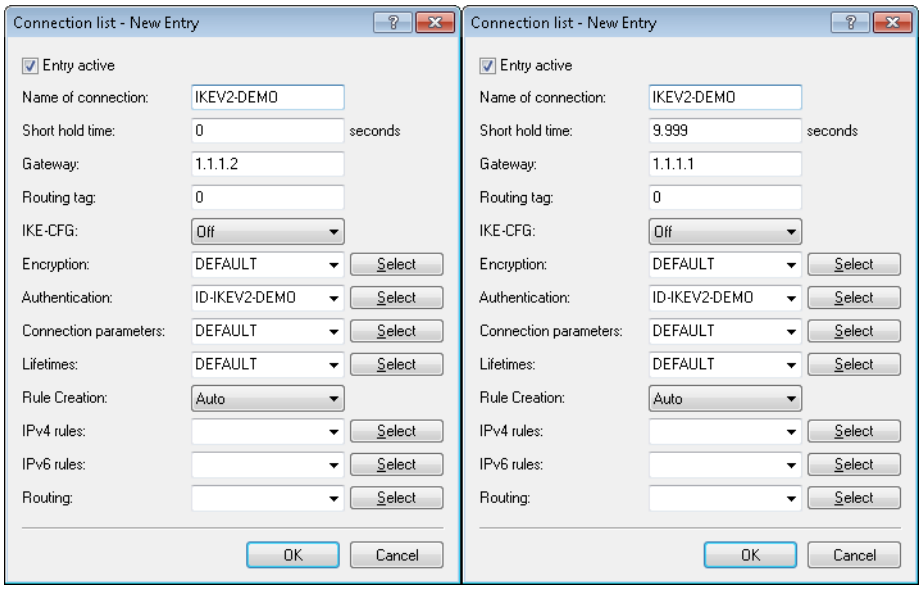
Parameter	Description
Name	Enter the name for the authentication here. In this example, **ID-IKEV2-DEMO** was entered on both devices. This entry is used later in the VPN connection list.
Local authentication	Select the authentication type used on this router. This example uses authentication by pre-shared key (PSK).
Local identifier type	Select the identifier type used on this router. In this example, the identity type was set to **E-mail address (FQUN)**.
Local identifier	Set the local identifier. In this example, the local identifier was set to **Main** on the 1781AW and **Branch** on the 1781VA-4G.
Local password	The pre-shared key required to successfully authenticate at this router.
Remote authentication	Select the authentication type used by the remote router. On the 1781AW, this entry corresponds to the entry for “Local authentication” on the 1781VA-4G.
Remote identifier type	Select the type of the remote identifier (used by the remote router). On the 1781AW, this entry corresponds to the entry for Local identifier on the 1781VA-4G.
Remote identifier	Enter the identifier of the remote station. On the 1781AW, this entry corresponds to the entry for “Local identifier” on the 1781VA-4G.
Remote password	The pre-shared key required to successfully authenticate at the remote station. On the 1781AW, this entry corresponds to the entry for Local password on the 1781VA-4G.

5. **Configuring the Connection list:** Configure the connection lists on each individual router. To carry out the configuration, open the menu item **VPN** > **IKEv2/IPSec** and click the button **Connection list**.



6. Create a new VPN connection by clicking the button **Add**.

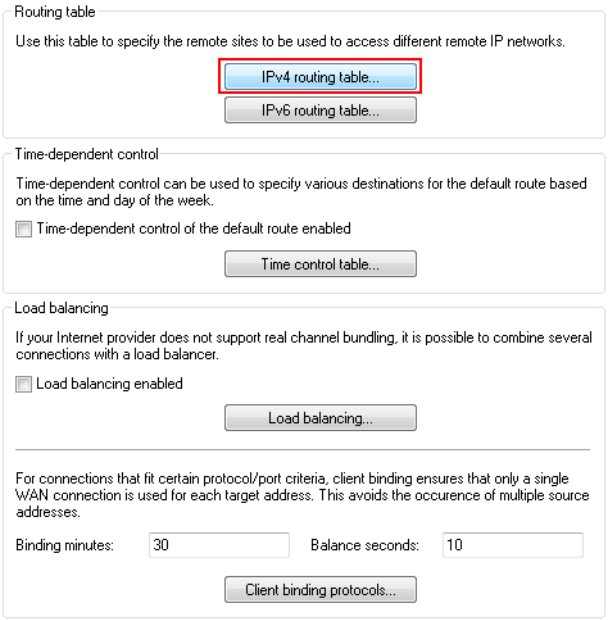
The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.



Parameter	Description
Entry active	Set a check mark in the check box to activate the connection.
Name of connection	Enter a name for the VPN connection. This name is used later in the routing table.
Short hold time	Specify the short-hold time in seconds for the VPN connection. In this example, the value for the 1781AW is set to **0**. This means that this router will not actively establish the VPN

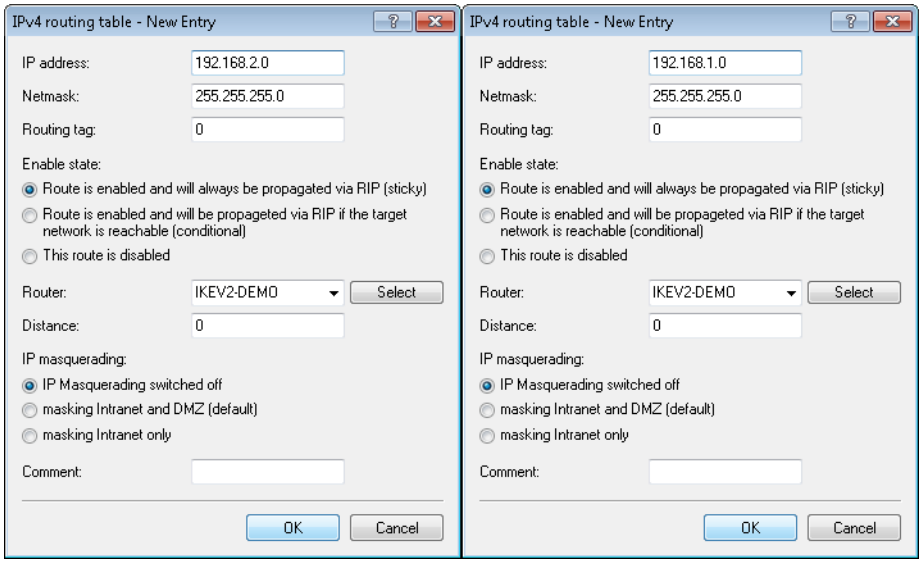
Parameter	Description
	connection. The value for the 1781VA-4G is set to **9999**. This value means that the router will not actively disconnect and, in case the connection is lost, it reconnects immediately.
Gateway	Specify the IP address of the remote station. In this example, the IP address of the WAN interface of the 1781AW is `1.1.1.1` and that of the 1781VA-4G is `1.1.1.2`.
Authentication	Select the authentication. The entry here corresponds to the name of the authentication that you set in **step 3**.

7. **Configuring the Routing table:** Configuring the routes here ensures that packets can be sent from the router through the VPN tunnel to the VPN remote station. To do this, open the menu item **IP router** > **Routing** and click the button **IPv4 routing table**.



8. Create an additional route by clicking the button **Add**. Information about the route is entered into the configuration window for each router.

The screenshots below show the configurations for both devices for direct comparison side by side. Here we only describe the configuration parameters that differ from the default values.



Parameter	Description
IP address	Enter the IP network to be accessed via the VPN tunnel. In this example, the IP network `192.168.2.0` should be accessed from the 1781AW and the IP network `192.168.1.0` should be accessed from the 1781VA-4G.
Netmask	Specify the netmask of the IP network named above.
Enable state	Select the option **Route is enabled and will always be propagated by RIP**. This activates the entry and makes it available for use.
Router	For the router, enter the name of the VPN connection that you entered in **step 4**.
IP masquerading	Select **IP masquerading switched off** so that the router does not conceal the other network behind its own IP address.

9. Write the respective configurations back to the two devices.
10. Use LANmonitor to check the VPN connection. LANmonitor displays the status of the VPN connection.

5.1.5 Additions to the Setup menu

IKEv2

In this directory you configure the IKEv2 parameters.

SNMP ID:

2.19.36

Telnet path:

Setup > **VPN**

remote sites

In this table, you configure the IKEv2 connections to VPN partners.

The console command `show vpn` shows whether the connection is successful.

SNMP ID:

2.19.36.1

Telnet path:

Setup > **VPN** > **IKEv2**

Peer

Contains the name of the connection to the remote station.

Subsequently, this name appears in the routing table.

SNMP ID:

2.19.36.1.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

Active

Specifies whether the VPN peer is enabled.

SNMP ID:

2.19.36.1.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Yes

The VPN connection is enabled.

No

The VPN connection is disabled.

Default:

Yes

SH time

Specifies the hold time in seconds for which the device stays connected if there is no data flow.

SNMP ID:

2.19.36.1.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 4 characters from `[0-9]`

Default:

0

0 … 9999

Special values:

0

The device does not actively establish a connection, but waits for data packets to arrive.

9999

Keepalive: The device establishes a permanent connection.

Remote gateway

Contains the address (IPv4, IPv6 or FQDN) of the VPN partner.

SNMP ID:

2.19.36.1.4

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 40 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Rtg-Tag

Contains the routing tag for this VPN connection.

SNMP ID:

2.19.36.1.5

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Encryption

Specifies the encryption method used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Encryption**.

SNMP ID:

2.19.36.1.6

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

Authentication

Specifies the authentication method used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**.

SNMP ID:

2.19.36.1.7

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

General

Specifies the general parameters used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **General**.

SNMP ID:

2.19.36.1.8

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

Lifetimes

Specifies the lifetimes of the key used for the VPN connection. The corresponding entry is located in the table **Setup** > **VPN** > **IKEv2** > **Lifetimes**.

SNMP ID:

2.19.36.1.9

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

IKE-CFG

Specifies the IKEv2 config mode of this connection for RAS dial-ins.

SNMP ID:

2.19.36.1.10

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Off

RAS services are disabled.

Client
The device works as a RAS client and dials-in to a server.

Servers
The device works as a server. RAS clients can dial-in to it.

Default:

Off

Rule creation

Specifies how VPN rules are created.

SNMP ID:

2.19.36.1.11

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Auto
The device creates the VPN rules automatically.

Manual
The device uses manually created rules.

Default:

Auto

IPv4-Rules

Specifies which IPv4 rules apply to this VPN connection.

The IPv4 rules are located in the table **Setup** > **VPN** > **Networks** > **IPv4-Rule-Lists**.

SNMP ID:

2.19.36.1.12

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

Default:

empty

IPv6-Rules

Specifies which IPv6 rules apply to this VPN connection.

The IPv6 rules are located in the table **Setup** > **VPN** > **Networks** > **IPv6-Rule-Lists**.

SNMP ID:

2.19.36.1.13

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

Default:

empty

Comment

Enter a comment about this entry.

SNMP ID:

2.19.36.1.17

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

IPv4-CFG-Pool

Use this entry to specify an IPv4 address pool for the IKEv2 peer.

SNMP ID:

2.19.36.1.18

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

IPv6-CFG-Pool

Use this entry to specify an IPv6 address pool for the IKEv2 peer.

SNMP ID:

2.19.36.1.19

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Encryption

Use this table to configure the parameters for the IKEv2 encryption.

SNMP ID:

2.19.36.2

Telnet path:

Setup > **VPN** > **IKEv2**

Name

Contains the name of this configuration.

SNMP ID:

2.19.36.2.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

DH-Groups

Contains the selection of Diffie-Hellman groups.

SNMP ID:

2.19.36.2.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

DH16
DH15
DH14
DH5
DH2

Default:

DH14

PFS

Specifies whether perfect forward secrecy (PFS) is enabled.

SNMP ID:

2.19.36.2.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

Yes
No

Default:

Yes

IKE-SA cipher list

Specifies which encryption algorithms are enabled.

SNMP ID:

2.19.36.2.4

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES

Default:

AES-CBC-256

IKE-SA-Integ-Alg-List

Specifies which hash algorithms are enabled.

SNMP ID:

2.19.36.2.5

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

SHA-512
SHA-384
SHA-256
SHA1
MD5

Default:

SHA-256

SHA1

Child-SA-Cipher-List

Specifies which encryption algorithms are enabled in the Child-SA.

SNMP ID:

2.19.36.2.6

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES

Default:

AES-CBC-256

Child-SA-Integ-Alg-List

Specifies which hash algorithms are enabled in the Child-SA.

SNMP ID:

2.19.36.2.7

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

SHA-512
SHA-384
SHA-256
SHA1
MD5

Default:

SHA-256

SHA1

Auth

Use this menu to configure the parameters for the IKEv2 authentication.

SNMP ID:

2.19.36.3

Telnet path:

Setup > **VPN** > **IKEv2**

Parameter

Use this table to configure the local and a corresponding remote identity for the IKEv2 authentication.

SNMP ID:

2.19.36.3.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth**

Name

Contains the name of this entry.

SNMP ID:

2.19.36.3.1.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

Local-Auth

Sets the authentication method for the local identity.

SNMP ID:

2.19.36.3.1.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

RSA-Signature
Authentication by RSA signature.

PSK
Authentication by pre-shared key (PSK).

Digital signature
Use of configurable authentication methods with digital certificates as per *RFC 7427*.

Default:

PSK

Local-ID-Type

Displays the ID type of the local identity. The device interprets the entry under **Local-ID** accordingly.

SNMP ID:

2.19.36.3.1.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

No-Identity
The ID is the local gateway address.

If this option is selected, the entry under **Local-ID** has no effect.

IPv4 address
IPv6 address
Domain name
E-mail address
Distinguished name
Key ID

Default:

E-mail address

Local-ID

Contains the local identity. The significance of this entry depends on the setting under **Local-ID-Type**.

SNMP ID:

2.19.36.3.1.4

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Local-Password

Contains the password of the local identity.

SNMP ID:

2.19.36.3.1.5

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Remote-Auth

Sets the authentication method for the remote identity.

SNMP ID:

2.19.36.3.1.6

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

RSA-Signature
Authentication by RSA signature.

PSK
Authentication by pre-shared key (PSK).

Digital signature
Use of configurable authentication methods with digital certificates as per *RFC 7427*.

Default:

PSK

Remote-ID-Type

Displays the ID type of the remote identity. The device interprets the entry under **Remote-ID** accordingly.

SNMP ID:

2.19.36.3.1.7

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

No-Identity
The device accepts all connections from remote IDs.

If this option is selected, the entry under **Remote-ID** has no effect.

IPv4 address
IPv6 address
Domain name
E-mail address
Distinguished name
Key ID

Default:

E-mail address

Remote-ID

Contains the remote identity. The significance of this entry depends on the setting under **Remote-ID-Type**.

SNMP ID:

2.19.36.3.1.8

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Remote-Password

Contains the password of the remote identity.

SNMP ID:

2.19.36.3.1.9

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Local-Certificate

Contains the local VPN certificate used by the device for outbound connections.

The corresponding VPN certificates “VPN1” to “VPN9” are configured under **Setup** > **Certificates** > **SCEP-Client** > **Certificates**.

SNMP ID:

2.19.36.3.1.11

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Remote-Cert-ID-Check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

SNMP ID:

2.19.36.3.1.12

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Yes

The device checks that the remote identity exists in the certificate.

No

The device does not check that the remote identity exists in the certificate.

Default:

Yes

Local-Dig-Sig-Profile

Contains the profile name of the local digital signature profile being used.

SNMP ID:

2.19.36.3.1.13

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Remote-Dig-Sig-Profile

Contains the profile name of the remote digital signature profile.

SNMP ID:

2.19.36.3.1.14

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

OCSP-Check

With this setting you enable the real-time check of a X.509 certificate via OCSP, which checks the validity of the remote station's certificate. In order to use the OCSP check for individual VPN connections, you must first enable the global OCSP client for VPN connections and then create profile lists of the valid certificate authorities used by the device to perform the real-time check.

SNMP ID:

2.19.36.3.1.15

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Yes
No

Default:

No

General

Use this table to configure the general IKEv2 parameters.

SNMP ID:

2.19.36.4

Telnet path:

Setup > **VPN** > **IKEv2**

Name

Contains the name of this entry.

SNMP ID:

2.19.36.4.1

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

DPD-Inact-Timeout

Contains the time in seconds after which the device disconnects from the remote peer if there is a loss of contact.

SNMP ID:

2.19.36.4.2

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Max. 4 characters from `[0-9]`

Default:

30

SSL-Encaps.

Specifies whether the connection uses IKEv2 over HTTPS.

SNMP ID:

2.19.36.4.4

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Yes
No

Default:

No

IPCOMP

Specifies whether the devices transmit compressed IKEv2 data packets.

SNMP ID:

2.19.36.4.5

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Yes
No

Default:

No

Encaps-Mode

Specifies the mode of transmission.

SNMP ID:

2.19.36.4.6

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Tunnel

Default:

Tunnel

Lifetimes

Use this table to configure the lifetimes of the IKEv2 keys.

SNMP ID:

2.19.36.5

Telnet path:

Setup > **VPN** > **IKEv2**

Name

Contains the name of this entry.

SNMP ID:

2.19.36.5.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

IKE-SA-Sec

Contains the time in seconds until the IKE SA key is renewed.

SNMP ID:

2.19.36.5.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

Max. 10 characters from `[0-9]`

Default:

108000

Special values:

0

No key renewal.

IKE-SA-KB

Contains the data volume in kilobytes until the IKE SA key is renewed.

SNMP ID:

2.19.36.5.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

No key renewal.

Child-SA-Sec

Contains the time in seconds until the CHILD SA key is renewed.

SNMP ID:

2.19.36.5.4

Telnet path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

Max. 10 characters from `[0-9]`

Default:

28800

Special values:

0

No key renewal.

Child-SA-KB

Contains the data volume in kilobytes until the CHILD SA key is renewed.

SNMP ID:

2.19.36.5.5

Telnet path:

Setup > **VPN** > **IKEv2** > **Lifetimes**

Possible values:

Max. 10 characters from `[0-9]`

Default:

2000000

Special values:

0

No key renewal.

IKE-CFG

When configuring VPN dial-in connections, there is as an alternative to fixed IP addresses for the remote sites that dial in, in that a pool of IP addresses can be made available to them. To this end, the IKE-CFG mode “Server” is specified for the entries in the connection list.

Use this menu to configure the address pool that the device in CFG mode “Server” passes to the clients.

SNMP ID:

2.19.36.7

Telnet path:

Setup > **VPN** > **IKEv2**

IPv4

In this table, you configure the IPv4 addresses of the address pool for the IKEv2-CFG mode “Server”.

SNMP ID:

2.19.36.7.1

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

Name

Contains the name of the IPv4 address pool.

SNMP ID:

2.19.36.7.1.1

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Start-Address-Pool

Here you enter the first IPv4 address of the pool of addresses that you want to provide to dial-in clients.

SNMP ID:

2.19.36.7.1.2

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 15 characters from `[0-9]./`

Default:

empty

End-Address-Pool

Here you enter the last IPv4 address of the pool of addresses that you want to provide to dial-in clients.

SNMP ID:

2.19.36.7.1.3

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 15 characters from `[0-9]./`

Default:

empty

Primary-DNS

Specify here the address of a name server to which DNS requests are to be forwarded.

SNMP ID:

2.19.36.7.1.4

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 15 characters from `[0-9].`

Default:

0.0.0.0

Secondary-DNS

Here you specify the address of an alternative name server, to which the DNS requests are redirected if the connection to the first name server is broken.

SNMP ID:

2.19.36.7.1.5

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv4**

Possible values:

Max. 15 characters from `[0-9].`

Default:

empty

IPv6

In this table, you configure the IPv6 addresses of the address pool for the IKEv2-CFG mode “Server”.

SNMP ID:

2.19.36.7.2

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

Name

Contains the name of the IPv6 address pool.

SNMP ID:

2.19.36.7.2.1

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Start-Address-Pool

Here you enter the first IPv6 address of the pool of addresses that you want to provide to dial-in clients.

SNMP ID:

2.19.36.7.2.2

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

End-Address-Pool

Here you enter the last IPv6 address of the pool of addresses that you want to provide to dial-in clients.

SNMP ID:

2.19.36.7.2.3

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Primary-DNS

Specify here the address of a name server to which DNS requests are to be forwarded.

SNMP ID:

2.19.36.7.2.4

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Secondary-DNS

Here you specify the address of an alternative name server, to which the DNS requests are redirected if the connection to the first name server is broken.

SNMP ID:

2.19.36.7.2.5

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

5.2 IKEv2 fragmentation support

As of HiLCOS 10.12, HiLCOS supports IKEv2 fragmentation.

5.2.1 IKEv2 fragmentation

The fragmentation of data packets is controlled by the maximum transmission unit (MTU). The MTU is the maximum size that a packet may have in order to be sent as payload over a channel. The two communication partners negotiate this during connection establishment in order to optimize data transmission by avoiding any additional fragmentation of the data packets.

In HiLCOS, IKEv2 fragmentation is enabled automatically. You can manually specify a maximum MTU if you wish.

To do this in LANconfig, go to **VPN** > **IKEv2/IPSec**.

Enter the maximum IP packet length/size in bytes into the **MTU** field in the **Fragmentation** section. Smaller values lead to greater fragmentation of the payload data.

5.2.2 Additions to the Setup menu

MTU

This entry contains the maximum transmission unit (MTU) for IKEv2.

SNMP ID:

2.19.36.8

Telnet path:

Setup > **VPN** > **IKEv2**

Possible values:

Max. 5 characters from `[0-9]`

0 … 65535

Default:

0

Special values:

0

The MTU setting is disabled. The two IKEv2 endpoints negotiate the MTU between themselves.

5.3 RADIUS support for IKEv2

As of HiLCOS 10.12, RADIUS supports the IKEv2 protocol for authorization and accounting.

5.3.1 RADIUS support for IKEv2

HiLCOS enables the configuration of IKEv2 for authorization and accounting of VPN peers to be performed by an external RADIUS server.

In medium- to large-scale VPN scenarios, the tables for VPN configurations are generally rather large and complex. If multiple VPN gateways are operated for redundancy, it is important to ensure that the configuration is identical on all VPN gateways.

Operating a central RADIUS server allows the configuration of the VPN parameters on the VPN gateways to be almost completely outsourced to one or more RADIUS servers. When a device receives an incoming connection from a VPN peer, the device attempts to authenticate the incoming connection via RADIUS and to retrieve other necessary connection parameters, such as VPN network relationships, CFG-mode address or DNS server, from the RADIUS server.

The VPN configuration may be either completely or only partially retrieved from the RADIUS server, in which case it is combined with parameters stored locally. This mechanism works for incoming connections only.

Optional RADIUS accounting allows information about VPN connections to be stored centrally on a RADIUS server. This information may consist of the duration of the connection to the client, the time when the connection is established, or the transmitted data volume.

The RADIUS server is configured in LANconfig under **VPN** > **IKEv2/IPSec** > **Extended settings**.

RADIUS authorization

When authenticating a VPN peer, the Hirschmann gateway transmits the following RADIUS attributes to the RADIUS server in the `Access-Request`:

ID :	Name	Meaning
1	User name	The remote ID of the VPN peers sent in the AUTH negotiation with the Hirschmann gateway.
2	User-Password	The dummy password as configured in LANconfig under **VPN** > **IKEv2/IPSec** > **Extended settings** > **Password**.
4	NAS-IP-Address	Specifies the IPv4 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute “95” instead (see below).
6	Service type	The service type is always “Outbound (5)” or “Dialout-Framed-User”.
31	Calling-Station-Id	Specifies the identifier (as an IPv4 or IPv6 address) of the calling station (e.g. the VPN client).

ID :	Name	Meaning
95	NAS-IPv6-Address	Specifies the IPv6 address of the gateway that is requesting access for a user. In the case of an IPv4 connection, the gateway transmits the attribute “4” instead (see above).

Of the attributes contained in the `Access-Accept` response from the RADIUS server, the Hirschmann gateway evaluates the following, in part vendor-specific attributes:

ID :	Name	Meaning
8	Framed-IP-Address	IPv4 address for the client (in IKE CFG-mode “Server”).
22	Framed-Route	IPv4 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client).
39	Tunnel-Password	Sets the passwords on the local and remote identity to the same value when using synchronous PSKs.
88	Framed-Pool	Name of the IPv4 address pool from which the client retrieves its IP address and the DNS server. The values in “Framed-IP-Address” and “LCS-DNS-Server-IPv4-Address” take precedence over this attribute.
99	Framed-IPv6-Route	IPv6 routes that should be entered into the routing table on the VPN gateway in the direction of the client (next-hop client).
168	Framed-IPv6-Address	IPv6 address for the client (in IKE CFG-mode “Server”).
169	DNS-Server-IPv6-Address	IPv6 DNS server for the client (in IKE CFG-mode “Server”).
172	Stateful-IPv6-Address-Pool	Name of the IPv6 address pool (in IKE CFG-mode “Server”).
LANCOM 19	LCS-IKEv2-Local-Password	Local IKEv2 PSK
LANCOM 20	LCS-IKEv2-Remote-Password	Remote IKEv2 PSK
LANCOM 21	LCS-DNS-Server-IPv4-Address	IPv4 DNS server for the client (in IKE CFG-mode “Server”).
LANCOM 22	LCS-VPN-IPv4-Rule	Contains the IPv4 network rules (examples below)
LANCOM 23	LCS-VPN-IPv6-Rule	Contains the IPv6 network rules (examples below)
LANCOM 24	LCS-Routing-Tag	Routing tag to be configured for the client (IPv4/IPv6).
LANCOM 25	LCS-IKEv2-IPv4-Route	Routes in prefix notation (e.g. “192.168.1.0/24”) that the Hirschmann gateway transfers to the client via `INTERNAL_IP4_SUBNET`. Multiple attributes can be analyzed.
LANCOM 26	LCS-IKEv2-IPv6-Route	Routes in prefix notation (e.g. “2001:db8::/64”) that the Hirschmann gateway transfers to the client via `INTERNAL_IP6_SUBNET`. Multiple attributes can be analyzed.

Examples of network rules

The format for a network rule on the RADIUS server takes the form `<local networks> * <remote networks>`.

The entries for `<local networks>` and `<remote networks>`are comma-separated lists.

Example 1: `10.1.1.0/24,10.2.0.0/16 * 172.32.0.0/12`

The result is the following network rules:

- 10.2.0.0/255.255.0.0 <-> 172.16.200.0/255.255.255.255
- 10.1.1.0/255.255.255.0 <-> 172.16.200.0/255.255.255.255

Example 2: 10.1.1.0/24 * 0.0.0.0/0

This results in the following network rule:

- 10.1.1.0/255.255.255.0 <-> 0.0.0.0/0.0.0.0

Here, 0.0.0.0/0 means "ANY", i.e. any network. 0.0.0.0/32 can be used to restrict a CFG-mode client to its own (as yet unknown) config-mode address. This address could come from an address pool on the device or from the RADIUS server.

Example 3: 2001:db8:1::/48 * 2001:db8:6::/48

RADIUS accounting

The Hirschmann gateway counts the transmitted data packets and octets and sends this information as regular Accounting-Request messages to the RADIUS accounting server. The RADIUS server answers this message with an Accounting-Response message.

The Accounting-Request messages have the following status types:

Home

As soon as a VPN peer contacts the Hirschmann gateway, the gateway starts an accounting session via IKEv2 and sends a Start status message with the appropriate RADIUS attributes to the RADIUS accounting server.

Interim-Update

During an ongoing accounting session, the gateway sends Interim-Update status messages at specified time intervals to that RADIUS accounting server, which gave a valid response to the Start status message. The gateway ignores any backup servers that may have been configured.

Stop

After the end of a session, the Hirschmann gateway sends a Stop status message to the RADIUS accounting server. This message is also sent only to that RADIUS accounting server, which gave a valid response to the Start status message. The gateway ignores any backup servers that may have been configured.

In the Access-Request message, the gateway transmits the following RADIUS attributes to the RADIUS server:

ID :	Name	Meaning	Status-Type
1	User name	The remote ID of the VPN peers sent in the AUTH negotiation with the Hirschmann gateway.	■ Home ■ Interim-Update ■ Stop
4	NAS-IP-Address	Specifies the IPv4 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute "95" instead (see below).	■ Home ■ Interim-Update ■ Stop
8	Framed-IP-Address	IP4 address of the VPN client.	■ Home ■ Interim-Update ■ Stop
31	Calling-Station-Id	Specifies the identifier (as an IPv4 or IPv6 address) of the calling station (e.g. the VPN client).	■ Home ■ Interim-Update ■ Stop
32	NAS identifier	The device name of the gateway.	■ Home

ID :	Name	Meaning	Status-Type
			■ Interim-Update ■ Stop
40	Acct-Status-Type	Contains the status type “Start” (1).	■ Home
40	Acct-Status-Type	Contains the status type “Interim-Update” (3).	■ Interim-Update
40	Acct-Status-Type	Contains the status type “Stop” (2).	■ Stop
42	Acct-Input-Octets	Contains the number of octets received from the direction of the VPN peer. The value refers to the decrypted data, starting with the IP header.	■ Interim-Update ■ Stop
43	Acct-Output-Octets	Contains the number of octets sent to the VPN peer. The value refers to the decrypted data, starting with the IP header.	■ Interim-Update ■ Stop
44	Acct-Session-Id	The name of the VPN peer and the timestamp at the start of the session form the unique session ID.	■ Home ■ Interim-Update ■ Stop
46	Acct-Session-Time	Contains the elapsed time in seconds since the start of the session.	■ Interim-Update ■ Stop
47	Acct-Input-Packets	Contains the current number of data packets received from the direction of the VPN peer.	■ Interim-Update ■ Stop
48	Acct-Output-Packets	Contains the current number of data packets sent to the VPN peer.	■ Interim-Update ■ Stop
49	Acct-Terminate-Cause	Contains the reason for terminating the session.	■ Stop
52	Acct-Input-Gigawords	Contains the number of gigawords received from the direction of the VPN peer. The value refers to the decrypted data, starting with the IP header.	■ Interim-Update ■ Stop
53	Acct-Input-Gigawords	Contains the number of gigawords sent to the VPN peer. The value refers to the decrypted data, starting with the IP header.	■ Interim-Update ■ Stop
95	NAS-IPv6-Address	Specifies the IPv6 address of the gateway that is requesting access for a user. In the case of an IPv6 connection, the gateway transmits the attribute “4” instead (see above).	■ Home ■ Interim-Update ■ Stop
168	Framed-IPv6-Address	IP6 address of the VPN client.	■ Home ■ Interim-Update ■ Stop

RADIUS authentication

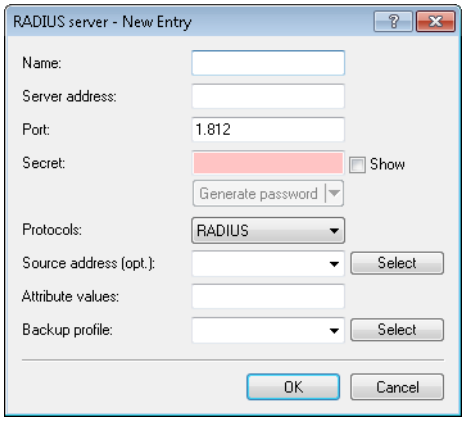
In the **RADIUS authentication** section you configure the settings for the RADIUS server used for VPN client authentication.

In the **Password** field you set the password that the RADIUS server receives as a user password in the access-request attribute.

The RADIUS server usually associates this password directly with a VPN peer for network access authorization. With IKEv2 however, the requesting VPN peer is authorized not by the RADIUS server, but instead by the Hirschmann gateway after this receives the corresponding authorization in the `access-accept` message from the RADIUS server.

Accordingly, you enter a dummy password at this point.

Just click on **RADIUS server** to open the configuration dialog of the RADIUS server.



Name

Specify an identifier for this entry.

Server address

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

Port

Specify the UDP port of the RADIUS server. The value “1812” is preset as the default value.

Secret

This entry contains the shared secret used to authorize the Hirschmann gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

Protocols

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

Source address (optional)

Enter the loopback address of the device, where applicable.

Attribute values

HiLCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Backup profile

From the list of RADIUS server profiles, select a profile as the backup server.

The RADIUS server configured is selected in the connection list under **VPN** > **IKEv2/IPSec** > **Connection list** in the **RADIUS auth. server** field.

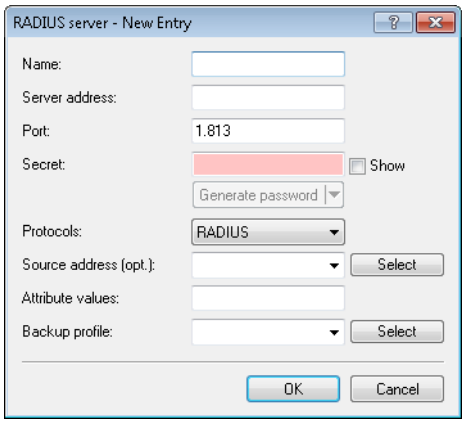
RADIUS accounting

In the **RADIUS accounting** section you configure the settings for the RADIUS server used for VPN client accounting.

Just click on **RADIUS server** to open the configuration dialog of the RADIUS server.

The **Update cycle** field is used to set the time in seconds between two successive interim-update messages. The device randomly inserts a tolerance of ±10% to keep the update messages of parallel accounting sessions separate from one another.

Just click on **RADIUS server** to open the configuration dialog of the RADIUS server.



Name

Specify an identifier for this entry.

Server address

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

Port

Specify the UDP port of the RADIUS server. The value “1813” is preset as the default value.

Secret

This entry contains the shared secret used to authorize the Hirschmann gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

Protocols

From the drop-down menu, choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

Source address (optional)

Enter the loopback address of the device, where applicable.

Attribute values

HiLCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Backup profile

From the list of RADIUS server profiles, select a profile as the backup server.

The RADIUS server configured is selected in the connection list under **VPN** > **IKEv2/IPSec** > **Connection list** in the **RADIUS acc. server** field.

5.3.2 Additions to the Setup menu

RADIUS authorization

Here you specify the RADIUS server that performs the authorization.

Here you select an entry from the table under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**.

If you do not specify a RADIUS server for authorization, the device uses the local IKEv2 configuration.

SNMP ID:

2.19.36.1.15

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

RADIUS accounting

Use this entry to specify the RADIUS server that is to be used for the accounting.

Here you select an entry from the table under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**.

If you do not specify a RADIUS server, no accounting takes place for this VPN peer.

SNMP ID:

2.19.36.1.16

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

RADIUS

This menu contains the RADIUS configuration for IKEv2.

SNMP ID:

2.19.36.9

Telnet path:

Setup > **VPN** > **IKEv2**

Authorization

This menu contains the configuration for the RADIUS authorization via IKEv2.

SNMP ID:

2.19.36.9.1

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS**

Servers

This table contains the server configuration for the RADIUS authorization under IKEv2.

SNMP ID:

2.19.36.9.1.1

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization**

Name

Specify an identifier for this entry.

SNMP ID:

2.19.36.9.1.1.1

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Server host name

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

SNMP ID:

2.19.36.9.1.1.2

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default:

empty

Port

Specify the UDP port of the RADIUS server.

SNMP ID:

2.19.36.9.1.1.3

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

Max. 5 characters from `[0-9]`

Default:

1812

Secret

This entry contains the shared secret used to authorize the Hirschmann gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

SNMP ID:

2.19.36.9.1.1.4

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Protocol

Choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

SNMP ID:

2.19.36.9.1.1.6

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

Loopback address

This entry contains the loopback address of the Hirschmann gateway that sent the request to the RADIUS server.

SNMP ID:

2.19.36.9.1.1.7

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Attribute-Values

HiLCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

SNMP ID:

2.19.36.9.1.1.8

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Backup

To specify the backup server here, enter the name of an alternative RADIUS server from the list of already configured RADIUS servers.

SNMP ID:

2.19.36.9.1.1.9

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Password

Here you set the password that the RADIUS server receives as a user password in the access-request attribute.

The RADIUS server usually associates this password directly with a VPN peer for network access authorization. With IKEv2 however, the requesting VPN peer is authorized not by the RADIUS server, but instead by the Hirschmann gateway after this receives the corresponding authorization in the `access-accept` message from the RADIUS server.

Accordingly, you enter a dummy password at this point.

SNMP ID:

2.19.36.9.1.2

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Authorization**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Accounting

This menu contains the configuration for the RADIUS accounting via IKEv2.

SNMP ID:

2.19.36.9.2

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS**

Server

This table contains the server configuration for the RADIUS accounting under IKEv2.

SNMP ID:

2.19.36.9.2.1

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting**

Name

Specify an identifier for this entry.

SNMP ID:

2.19.36.9.2.1.1

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Server host name

Specify the host name for the RADIUS server (IPv4, IPv6 or DNS address).

SNMP ID:

2.19.36.9.2.1.2

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default:

empty

Port

Specify the UDP port of the RADIUS server.

SNMP ID:

2.19.36.9.2.1.3

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

Max. 5 characters from `[0-9]`

Default:

1813

Secret

This entry contains the shared secret used to authorize the Hirschmann gateway at the RADIUS server.

Confirm the secret by entering it again into the field that follows.

SNMP ID:

2.19.36.9.2.1.4

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Protocol

Choose between the standard RADIUS protocol and the secure RADSEC protocol for RADIUS requests.

SNMP ID:

2.19.36.9.2.1.5

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

RADIUS
RADSEC

Default:

RADIUS

Loopback address

This entry contains the loopback address of the Hirschmann gateway that sent the request to the RADIUS server.

SNMP ID:

2.19.36.9.2.1.6

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Attribute-Values

HiLCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

SNMP ID:

2.19.36.9.2.1.7

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Backup

To specify the backup server here, enter the name of an alternative RADIUS server from the list of already configured RADIUS servers.

SNMP ID:

2.19.36.9.2.1.8

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Interim-Interval

Set the time in seconds between two successive interim-update messages. The device randomly inserts a tolerance of ±10% to keep the update messages of parallel accounting sessions separate from one another.

SNMP ID:

2.19.36.9.2.2

Telnet path:

Setup > **VPN** > **IKEv2** > **RADIUS** > **Accounting**

Possible values:

Max. 10 characters from `[0-9]`

0 … 4294967295

Default:

0

Special values:

0

The transmission of interim-update messages is disabled.

Create-Routes-For-RAS-SAs

Specifies whether routes should be generated automatically from the VPN rules for dial-in (RAS) clients operating as CFG-mode servers. Disabling automatic route generation is useful when the routes are to be created by means of a routing protocol.

SNMP ID:

2.19.36.10

Telnet path:

Setup > **VPN** > **IKEv2**

Possible values:

No

No routes are generated for RAS SAs.

Yes

Routes are generated for RAS SAs.

Default:

Yes

Extended parameters

This table contains extended parameters for IKEv2 remote stations.

SNMP ID:

2.19.36.11

Telnet path:

Setup > **VPN** > **IKEv2**

Name

Name of the remote device.

SNMP ID:

2.19.36.11.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Extended-Parameters**

Possible values:

Max. 254 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

PRF-as-Sig-Hash

Specifies whether to use the PRF (pseudo-random function) of the IKEv2 negotiation as a signature hash with the RSA signature. This function should be used for compatibility with third-party products only. The setting must be configured identically at both ends of the VPN connection.

SNMP ID:

2.19.36.11.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Extended-Parameters**

Possible values:

Yes
No

Default:

No

5.3.3 Additions to the Status menu

RADIUS

This menu contains status values for all of the current VPN peers being managed by a RADIUS server (authorization and accounting).

SNMP ID:

1.26.39

Telnet path:

Status > **VPN**

Authorization

This directory contains the status values for all of the current VPN peers that were authorized by a RADIUS server.

A new VPN peer appears in this table after the first access request at a RADIUS server. The entry for a VPN peer is removed from the table as soon as its IKE SA (phase 1) is deleted.

SNMP ID:

1.26.39.1

Telnet path:

Status > **VPN** > **RADIUS**

Peer

This entry shows the name of the remote station.

SNMP ID:

1.26.39.1.1

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Remote-ID

This entry shows the remote ID of the VPN peer as forwarded by the device to the RADIUS server.

SNMP ID:

1.26.39.1.2

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Local-Gateway

This entry contains the IPv4 or IPv6 address of the Hirschmann gateway that the VPN peer sent its VPN request to. The Hirschmann gateway transmits this address as the RADIUS attribute "NAS-IP-Address" or "NAS-IPv6-Address" in the access request sent to the RADIUS server.

SNMP ID:

1.26.39.1.3

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Remote gateway

This entry contains the IPv4 or IPv6 address from which the VPN peer sent its VPN request to the Hirschmann gateway. The Hirschmann gateway transmits this address as the RADIUS attribute "Calling-Station-Id" in the access request sent to the RADIUS server.

SNMP ID:

1.26.39.1.4

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

State

Displays the status of the VPN peer. The following states are possible:

Running

The "Access-Request" was sent to the RADIUS server but there was no response yet.

Succeeded

The “Access-Accept” message was received from the RADIUS server.

Failed

The “Access-Request” to the RADIUS server or the configured backup RADIUS server failed.

SNMP ID:

1.26.39.1.5

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Server-Hostname

Displays the host name of the requested RADIUS server if this has answered a request. The entry corresponds to the configuration under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Authorization** > **Server**.

SNMP ID:

1.26.39.1.6

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

CFG-IPv4-Address

Displays the value reported by the RADIUS server in the RADIUS attribute “Framed-IP-Address”. If the RADIUS server does not return a value, this entry remains blank.

SNMP ID:

1.26.39.1.7

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

CFG-IPv4-DNS-Server

Displays a comma-separated list of IPv4 DNS servers reported by the RADIUS server in the vendor-specific RADIUS attribute “LCS-DNS-Server-IPv4-Address”. This entry remains blank if the VPN peer is in the “running” or “failed” state, or if the RADIUS server did not return a corresponding value in the “Access-Accept” message.

SNMP ID:

1.26.39.1.8

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

CFG-IPv4-Pool

Displays the framed IPv4 address pool reported by the RADIUS server. If the RADIUS server does not return a value, this entry remains blank.

SNMP ID:

1.26.39.1.9

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

CFG-IPv6-Address

Displays the value reported by the RADIUS server in the RADIUS attribute "Framed-IPv6-Address". If the RADIUS server does not return a value, this entry remains blank.

SNMP ID:

1.26.39.1.10

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

CFG-IPv6-DNS-Server

Displays a comma-separated list of IPv6 DNS servers reported by the RADIUS server in the vendor-specific RADIUS attribute "LCS-DNS-Server-IPv6-Address". This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

SNMP ID:

1.26.39.1.11

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

CFG-IPv6-Pool

Displays the framed IPv6 address pool reported by the RADIUS server. If the RADIUS server does not return a value, this entry remains blank.

SNMP ID:

1.26.39.1.12

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Rtg-Tag

This entry contains the IPv4 or IPv6 routing tag reported by the RADIUS server in the "Access-Accept" message (with the vendor-specific RADIUS attribute "LCS-Routing-Tag").

SNMP ID:

1.26.39.1.13

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Framed-IPv4-Routes

This entry contains a comma-separated list of IPv4 prefixes reported by the RADIUS server in the "Access-Accept" message by means of the RADIUS attribute "Framed-Route".

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

SNMP ID:

1.26.39.1.14

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Framed-IPv6-Routes

This entry contains a comma-separated list of IPv6 prefixes reported by the RADIUS server in the "Access-Accept" message in the RADIUS attribute "Framed-IPv6-Route".

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

SNMP ID:

1.26.39.1.15

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

IKE-IPv4-Routes

This entry contains a comma-separated list of IPv4 prefixes reported by the RADIUS server in the "Access-Accept" message by means of the vendor-specific RADIUS attribute "LCS-IKEv2-IPv4-Route".

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

SNMP ID:

1.26.39.1.16

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

IKE-IPv6-Routes

This entry contains a comma-separated list of IPv6 prefixes reported by the RADIUS server in the "Access-Accept" message by means of the vendor-specific RADIUS attribute "LCS-IKEv2-IPv6-Route".

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

SNMP ID:

1.26.39.1.17

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Other attributes

This entry contains a comma-separated or space-separated list of additional attributes transferred by the RADIUS server in the "Access-Accept" message.

This entry remains blank if the VPN peer is in the "running" or "failed" state, or if the RADIUS server did not return a corresponding value in the "Access-Accept" message.

Possible values are:

Local password

The content of the attributes "LCS-IKEv2-Local-Password" or "Tunnel-Password".

Remote password

The content of the attributes "LCS-IKEv2-Remote-Password" or "Tunnel-Password".

IPv4-Rule

Content of the attribute "LCS-VPN-IPv4-Rule".

IPv6-Rule

Content of the attribute "LCS-VPN-IPv6-Rule".

SNMP ID:

1.26.39.1.18

Telnet path:

Status > **VPN** > **RADIUS** > **Authorization**

Accounting

This directory contains the status values for all of the current VPN peers whose accounting is handled by a RADIUS server.

SNMP ID:

1.26.39.2

Telnet path:

Status > **VPN** > **RADIUS**

Peer

This entry shows the name of the remote station.

SNMP ID:

1.26.39.2.1

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Session-ID

The name of the VPN peer and the timestamp at the start of the session form the unique session ID.

SNMP ID:

1.26.39.2.2

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Remote-ID

This entry shows the remote ID of the VPN peer as forwarded by the device to the RADIUS server.

SNMP ID:

1.26.39.2.3

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Local-Gateway

This entry contains the IPv4 or IPv6 address of the Hirschmann gateway that the VPN peer sent its VPN request to. The Hirschmann gateway transmits this address as the RADIUS attribute “NAS-IP-Address” or “NAS-IPv6-Address” in the access request sent to the RADIUS server.

SNMP ID:

1.26.39.2.4

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Remote gateway

This entry contains the IPv4 or IPv6 address from which the VPN peer sent its VPN request to the Hirschmann gateway. The Hirschmann gateway transmits this address as the RADIUS attribute "Calling-Station-Id" in the access request sent to the RADIUS server.

SNMP ID:

1.26.39.2.5

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

CFG-IPv4-Address

Displays the value reported by the RADIUS server in the RADIUS attribute "Framed-IP-Address". If the RADIUS server does not return a value, this entry remains blank.

SNMP ID:

1.26.39.2.6

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

CFG-IPv6-Address

Displays the value reported by the RADIUS server in the RADIUS attribute "Framed-IPv6-Address". If the RADIUS server does not return a value, this entry remains blank.

SNMP ID:

1.26.39.2.7

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

State

Displays the status of the VPN peer. The following states are possible:

Starting

There was no “Accounting-Response” message from the RADIUS server.

Start-Failed

IKE did not transfer a valid “Start” message, or the VPN peer did not receive a valid “Accounting-Response” message from the RADIUS server.

Running

The VPN peer received a valid “Accounting-Response” message and the last interim update was successful.

Update-Failed

The last interim update was not successful.

SNMP ID:

1.26.39.2.8

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Server host name

Displays the host name of the requested RADIUS server if this has answered a request. The entry corresponds to the configuration under **Setup** > **VPN** > **IKEv2** > **RADIUS** > **Accounting** > **Server**.

SNMP ID:

1.26.39.2.9

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Session-Time

Displays the elapsed time in seconds since the start of the session.

SNMP ID:

1.26.39.2.10

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Input-Octets

Shows the number of octets received from the direction of the VPN peer. The value refers to the decrypted data, starting with the IP header.

SNMP ID:

1.26.39.2.11

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Output-Octets

Shows the number of octets sent to the VPN peer. The value refers to the decrypted data, starting with the IP header.

SNMP ID:

1.26.39.2.12

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Input-Packets

Shows the current number of data packets received from the direction of the VPN peer.

SNMP ID:

1.26.39.2.13

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

Output-Packets

Shows the current number of data packets sent to the VPN peer.

SNMP ID:

1.26.39.2.14

Telnet path:

Status > **VPN** > **RADIUS** > **Accounting**

5.4 IKEv2 routing support

As of version 10.12, HiLCOS supports the following functions for IKEv2-Config-Exchange

- CFG_Request
- CFG_Reply
- CFG_Set
- CFG_Ack

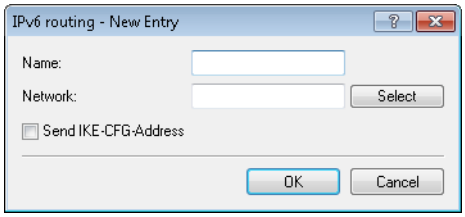
Configuring the prefixes for dynamic routing via IKEv2 in LANconfig is done under **VPN** > **IKEv2/IPSec** > **Extended settings** in the **IKEv2 routing** section.

5.4.1 IPv4 routing

IKEv2 routing uses an IKEv2 tunnel to propagate local networks or to learn about remote networks.

5.4.2 IPv6 routing

Use this table to configure the IPv6 networks that the device propagates via dynamic routing as per IKEv2.



Name

Contains the unique name of this entry.

Network

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IPv6 address
- IPv6 address/prefix length
- IPv6 interface name

The IP subnets are configured under **IPv6** > **General** in the section **IPv6 networks**.

Send IKE-CFG address

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server).

This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. Hirschmann routers generate the necessary routes automatically.

5.4.3 Additions to the Setup menu

Routing

Specifies the route used for the VPN connection.

The routes for IPv4 and IPv6 connections are located in the menu **Setup** > **VPN** > **IKEv2** > **Routing**.

SNMP ID:

2.19.36.1.14

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Routing

Use this menu to configure the routing table for the IKEv2 routing.

The routing tables specify IPv4/IPv6 routes used by the VPN connections if there is no corresponding route in the IPv4/IPv6 router.

SNMP ID:

2.19.36.6

Telnet path:

Setup > **VPN** > **IKEv2**

IPv4

Use this table to configure the IPv4 tables for the IKEv2 routing.

SNMP ID:

2.19.36.6.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Routing**

Name

Contains the name of this entry.

SNMP ID:

2.19.36.6.1.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

Networks

Contains the comma-separated list of IPv4 subnets.

Networks are entered in the following available formats:

- IP address
- IP address/IP mask
- IP address/prefix
- IP interface name

SNMP ID:

2.19.36.6.1.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Send-IKE-CFG-Addr

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server). This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. Hirschmann routers generate the necessary routes automatically.

SNMP ID:

2.19.36.6.1.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv4**

Possible values:

No

The IPv4 address is not sent

Yes

The IPv4 address will be sent

Default:

Yes

IPv6

Use this table to configure the IPv6 tables for the IKEv2 routing.

SNMP ID:

2.19.36.6.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Routing**

Name

Contains the name of this entry.

SNMP ID:

2.19.36.6.2.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

Networks

Contains the comma-separated list of IPv6 subnets.

Networks are entered in the following available formats:

- IP address
- IP address/IP mask
- IP address/prefix
- IP interface name

SNMP ID:

2.19.36.6.2.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Send-IKE-CFG-Addr

As a client, the device sends the retrieved CFG-mode address to the VPN peer (server). This option is required only if the remote site does not automatically create a routing entry for assigned IP addresses. Hirschmann routers generate the necessary routes automatically.

SNMP ID:

2.19.36.6.2.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Routing** > **IPv6**

Possible values:

No
The IPv6 address is not sent

Yes
The IPv6 address will be sent

Default:

Yes

5.5 "Match Remote Identity" for IKEv2

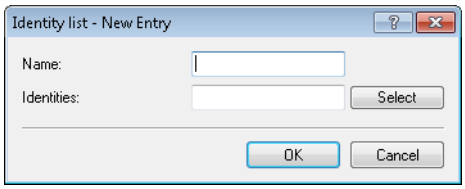
HiLCOS as of version 10.12 supports the configuration of multiple remote identities for IKEv2 connections. These identities can then be allocated to a VPN remote station.

The additional remote identities are configured in LANconfig under **VPN** > **IKEv2/IPSec** > **Extended settings** in the **Authentication** section.

The allocation of an additional remote identity to a VPN connection is done under **VPN** > **IKEv2/IPSec** > **Authentication** in the **Additional remote identities** section.

5.5.1 Identity list

Use this table to collect other remote identities into a group.



Name

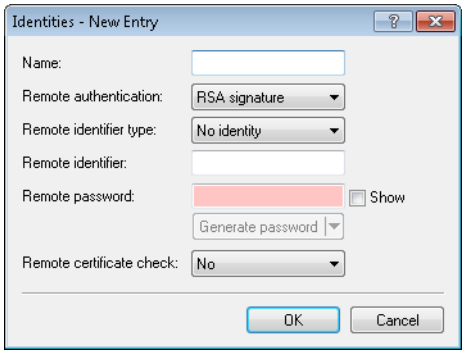
Contains the unique name of this entry.

Identity

Lists the other identities that are collected into this group. Configure the identities under **Identities**.

5.5.2 Identities

Use this table to configure additional remote identities. You select this name when grouping remote identities in the **Identity list**.



Name

Contains the unique name of this entry.

Remote authentication

Sets the authentication method for the remote identity.

Remote identifier type

Displays the ID type that the device expects from the remote identifier. The device interprets the entry under "Remote identifier" accordingly. Possible entries are:

- No identity: The device accepts any ID from the remote device. The device to ignores entries in the "Remote identifier" field.
- IPv4 address: The device expects an IPv4 address as the remote ID.
- IPv6 address: The device expects an IPv6 address as the remote ID.
- Domain name (FQDN): The device expects a domain name as the remote ID.
- E-mail address (FQUN): The device expects an e-mail address as the remote ID.
- ASN.1 Distinguished Name: The device expects a distinguished name as the remote ID.
- Key ID (group name): The device expects the group name as the remote ID.

Remote identifier

Contains the remote identity. The significance of this entry depends on the setting under "Remote identifier type".

Remote password

Contains the password of the remote identity.

Remote certificate check

This option determines whether the device checks that the specified remote identity is included in the received certificate.

5.5.3 Additions to the Setup menu

Addit.-Remote-ID-List

Contains additional remote identities as specified in the table **Setup** > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**.

SNMP ID:

2.19.36.3.1.10

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Addit.-Remote-ID-List

Use this table to configure lists of additional remote identities.

SNMP ID:

2.19.36.3.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth**

Name

Sets the name of the ID list.

SNMP ID:

2.19.36.3.2.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Addit.-Remote-IDs

Contains the remote identities that you want to collect into this list. The IDs are located in the table **Addit.-Remote-IDs**.

Specify several IDs by separating them with a space character.

SNMP ID:

2.19.36.3.2.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-ID-List**

Possible values:

Max. 254 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Addit.-Remote-IDs

Use this table to configure additional remote identities.

SNMP ID:

2.19.36.3.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth**

Name

Contains the name of this remote identity.

SNMP ID:

2.19.36.3.3.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Remote-Auth

Sets the authentication method for the remote identity.

SNMP ID:

2.19.36.3.3.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

RSA-Signature
Authentication by RSA signature.

PSK
Authentication by pre-shared key (PSK).

Digital signature
Use of configurable authentication methods with digital certificates as per *RFC 7427*.

Default:

PSK

Remote-ID-Type

Displays the ID type of the remote identity. The device interprets the entry under **Remote-ID** accordingly.

SNMP ID:

2.19.36.3.3.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

No-Identity
The device accepts all connections from remote IDs.

IPv4 address
IPv6 address
Domain name
E-mail address
Distinguished name
Key ID

Default:

E-mail address

Remote-ID

Contains the remote identity. The significance of this entry depends on the setting under **Remote-ID-Type**.

SNMP ID:

2.19.36.3.3.4

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Remote-Password

Contains the password of the remote identity.

SNMP ID:

2.19.36.3.3.5

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Remote-Cert-ID-Check

This function checks whether the specified remote ID is also included in the certificate that was used by the peer to establish the connection.

SNMP ID:

2.19.36.3.3.6

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

Yes
No

Default:

Yes

Digital-Signature-Profiles

Use this table to configure the profiles of the digital signature.

SNMP ID:

2.19.36.3.4

Telnet path:

Setup > **VPN** > **IKEv2**

Name

Name of the profile.

SNMP ID:

2.19.36.3.4.1

Telnet path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

Auth-Method

Sets the authentication method for the digital signature.

SNMP ID:

2.19.36.3.4.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

RSASSA-PSS
RSASSA-PKCS1-v1_5

Default:

RSASSA-PSS

Hash algorithms

Sets the hash algorithms for the digital signature.

SNMP ID:

2.19.36.3.4.3

Telnet path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

SHA-512, SHA-384, SHA-256, SHA1

Default:

SHA-512, SHA-384, SHA-256, SHA1

5.6 Redirect mechanism for IKEv2

As of HiLCOS 10.12, HiLCOS supports the redirect mechanism as per RFC 5685 for VPN connections that use IKEv2. This is initially supported as a client only. This allows an IKEv2 server to redirect a client to a different gateway.

5.7 VPN via IPv6 connections with IKEv1

As of HiLCOS 10.12, current VPN devices support IKEv1 for VPN connections over IPv6.

5.8 VPN network rules for IPv4 and IPv6

As of HiLCOS 10.12, current VPN devices allow the flexible configuration of network rules for VPN connections over IPv4 and IPv6.

5.8.1 Additions to the Setup menu

Networks

In this directory, you configure the VPN network rules for IPv4 and IPv6 connections.

SNMP ID:

2.19.35

Telnet path:

Setup > **VPN**

IPv4-Rules

In this table, you configure the VPN network rules for IPv4 connections.

SNMP ID:

2.19.35.1

Telnet path:

Setup > **VPN** > **Networks**

Name

Contains the name of this rule.

SNMP ID:

2.19.35.1.1

Telnet path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

Max. 31 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Local-Networks

Contains the local networks to which this rule applies.

The following entries are valid:

- Name of the IP networks whose addresses should be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses.
- Any valid IP address.

Specify multiple networks by separating them with a space character.

SNMP ID:

2.19.35.1.2

Telnet path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

Remote-Networks

Contains the remote networks to which this rule applies.

The following entries are valid:

- Name of the IP networks whose addresses should be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ
- LB0 to LBF for the 16 loopback addresses.
- Any valid IP address.

Specify multiple networks by separating them with a space character.

SNMP ID:

2.19.35.1.3

Telnet path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. `

Default:

empty

IPv4-Rule-Lists

In this table, you collect the VPN network rules for IPv4 connections into a rule list.

SNMP ID:

2.19.35.2

Telnet path:

Setup > **VPN** > **Networks**

Name

Contains the name of this rule list.

SNMP ID:

2.19.35.2.1

Telnet path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

Max. 31 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Rules

Contains the rules that you want to collect into this rule list.

Specify several rules by separating them with a space character.

SNMP ID:

2.19.35.2.2

Telnet path:

Setup > **VPN** > **Networks** > **IPv4-Rules**

Possible values:

Max. 127 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

Default:

empty

IPv6-Rules

In this table, you configure the VPN network rules for IPv6 connections.

SNMP ID:

2.19.35.3

Telnet path:

Setup > **VPN** > **Networks**

Name

Contains the name of this rule.

SNMP ID:

2.19.35.3.1

Telnet path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

Max. 31 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Local-Networks

Contains the local networks to which this rule applies.

Specify multiple networks by separating them with a space character.

SNMP ID:

2.19.35.3.2

Telnet path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

Remote-Networks

Contains the remote networks to which this rule applies.

Specify multiple networks by separating them with a space character.

SNMP ID:

2.19.35.3.3

Telnet path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

Max. 127 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_. ``

Default:

empty

IPv6-Rule-Lists

In this table, you collect the VPN network rules for IPv6 connections into a rule list.

SNMP ID:

2.19.35.4

Telnet path:

Setup > **VPN** > **Networks**

Name

Contains the name of this rule list.

SNMP ID:

2.19.35.4.1

Telnet path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

Max. 31 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Rules

Contains the rules that you want to collect into this rule list.

Specify several rules by separating them with a space character.

SNMP ID:

2.19.35.4.2

Telnet path:

Setup > **VPN** > **Networks** > **IPv6-Rules**

Possible values:

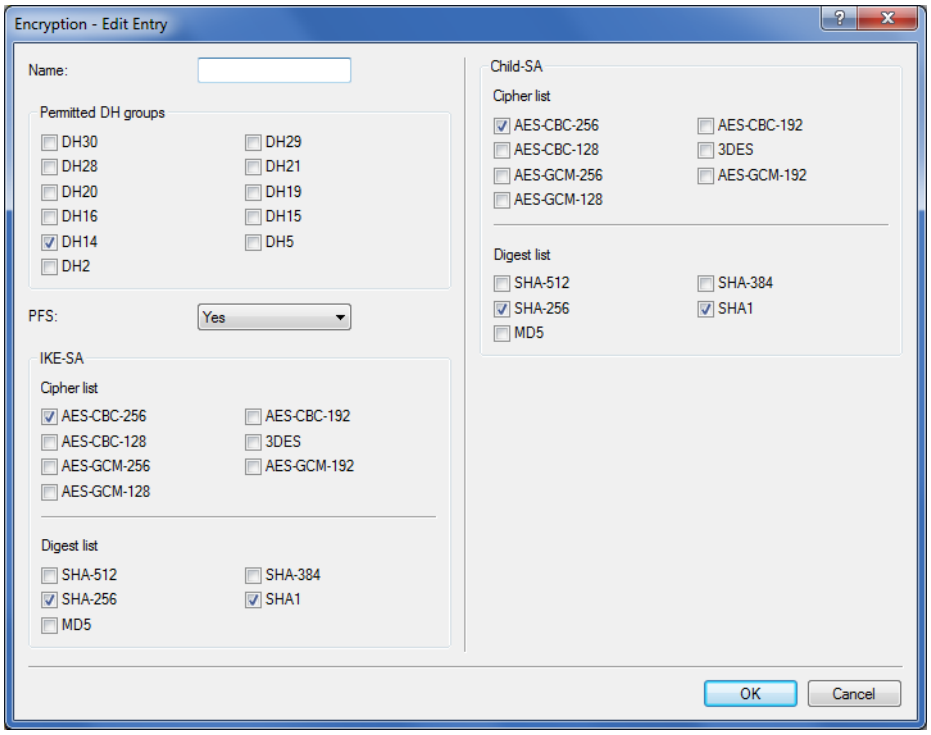
Max. 127 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_ .`

Default:

empty

5.9 Addition to the IKEv2 encryption algorithms

As of HiLCOS 10.12, an additional encryption algorithm is supported: GCM (Galois/Counter Mode).
This algorithm is particularly efficient and provides a noticeable increase in performance.
Also, new groups are available for the Diffie-Hellmann key exchange, namely DH-19 to DH-21 as per RFC5903 as well as DH-28 to DH-30 as per RFC 6954.



The new groups for the Diffie-Hellmann key exchange:

- DH-19 (256-bit random ECP group)
- DH-20 (384-bit random ECP group)
- DH-21 (521-bit random ECP group)
- DH-28 (brainpoolP256r1)
- DH-29 (brainpoolP384r1)
- DH-30 (brainpoolP512r1)

Variants of the newly added Galois/Counter Mode encryption algorithm:

- AES-GCM-128
- AES-GCM-192
- AES-GCM-256

5.9.1 Additions to the Setup menu

DH-Groups

Contains the selection of Diffie-Hellman groups.

SNMP ID:

2.19.36.2.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

DH30
(as of HiLCOS 10.12)
DH29
(as of HiLCOS 10.12)
DH28
(as of HiLCOS 10.12)
DH21
(as of HiLCOS 10.12)
DH20
(as of HiLCOS 10.12)
DH19
(as of HiLCOS 10.12)
DH16
DH15
DH14
DH5
DH2

Default:

DH14

IKE-SA cipher list

Specifies which encryption algorithms are enabled. As of version 10.12, HiLCOS also supports AES-GCM (Galois/Counter Mode).

SNMP ID:

2.19.36.2.4

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256
(as of HiLCOS version 10.12)
AES-GCM-192
(as of HiLCOS version 10.12)
AES-GCM-128
(as of HiLCOS version 10.12)

Default:

AES-CBC-256

AES-GCM-256

Child-SA cipher list

Specifies which encryption algorithms are enabled in the Child-SA. As of version 10.12, HiLCOS also supports AES-GCM (Galois/Counter Mode).

SNMP ID:

2.19.36.2.6

Telnet path:

Setup > **VPN** > **IKEv2** > **Encryption**

Possible values:

AES-CBC-256
AES-CBC-192
AES-CBC-128
3DES
AES-GCM-256
(as of HiLCOS version 10.12)
AES-GCM-192
(as of HiLCOS version 10.12)
AES-GCM-128
(as of HiLCOS version 10.12)

Default:

AES-CBC-256

AES-GCM-256

5.10 IKEv2 load balancer

HiLCOS 10.12 saw the introduction of the IKEv2 load balancer. This allows the operation of any number of VPN nodes while balancing the number of incoming VPN connections according to their load.

The IKEv2 load balancer allows the distribution of incoming IKEv2 connections to other gateways depending on the current load or number of VPN tunnels. The IKEv2 redirect mechanism is used to achieve this.

Larger-scale VPN scenarios generally operate with redundant VPN gateways. Often, the gateways are are not used evenly, and some gateways are reserved for backup events. The result is a non-uniform resource load across the installation.

With multiple VPN gateways in operation, all of them need to be configured on all of the clients. Particularly when a new VPN gateway is installed, it has to be subsequently configured on all of the clients. With the redirect mechanism (RFC 5685), IKEv2 offers an enhancement that enables a VPN gateway to redirect a client to another gateway.

The IKEv2 redirect mechanism in combination with VRRP provides a highly available IKEv2 load balancer that is suitable for enterprise scenarios.

In the first step, a VRRP group is activated on all participating VPN gateways. The virtual VRRP IP address is at the same time the master IP address of the IKEv2 load balancer cluster. The VPN gateways now exchange information about their load and their availability by means of regular status messages via multicast. If the master goes down, another VPN gateway is automatically set as the master.

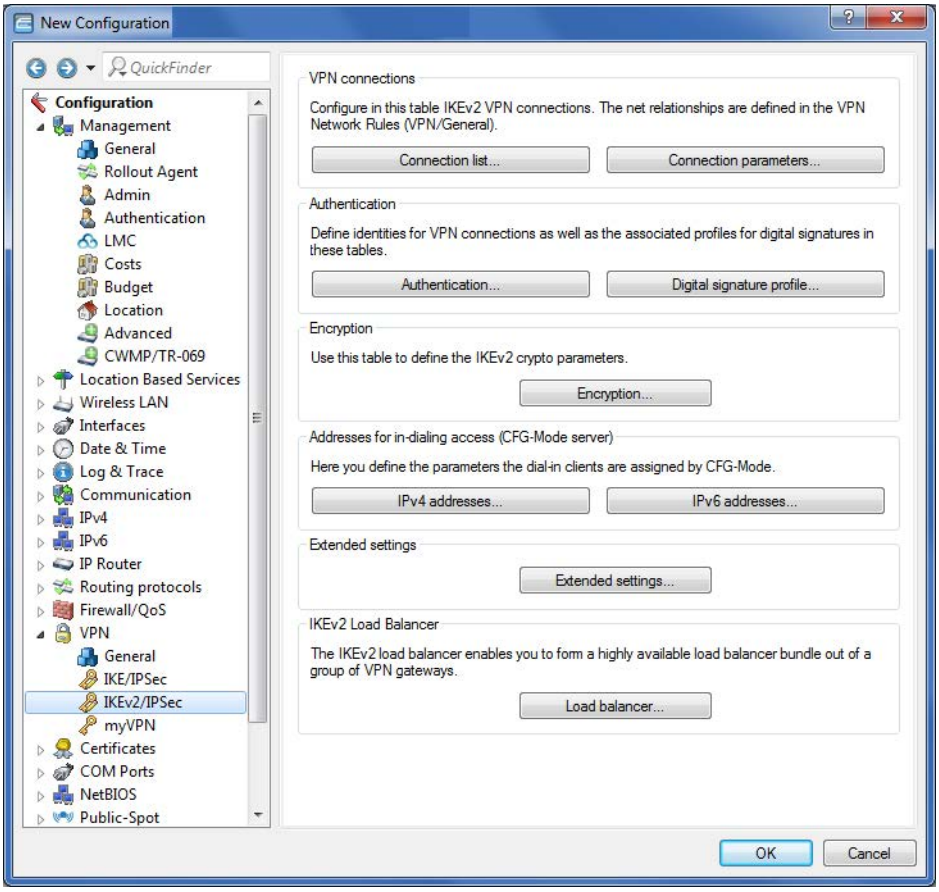
The only information the clients need is the master IP address. If a client establishes a VPN connection to this IP address, the master gateway checks the load of the VPN gateways and redirects the client to the gateway with the least load. The master gateway sends a redirect either in the IKE_SA_INIT response or in the IKE Auth phase. The redirect depends on the availability of free VPN tunnels of the participating gateways. The VPN client is directed to the VPN gateway with the lowest number of active tunnels.

The virtual gateway address is only used for the initial contact before the subsequent redirect. The client then establishes the actual VPN tunnel to a different gateway address.

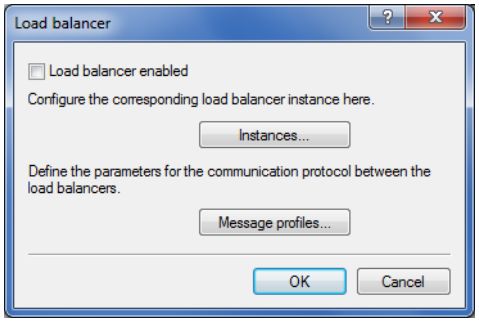
The following limiting conditions must be observed:

- VRRP is required for the automatic selection of the master gateway.
- The VPN gateways involved must have a common layer-2 connection for the VRRP and the exchange of status messages via multicast.
- VRRP is currently supported on LAN interfaces only.
- An upstream router (redundant, if necessary) is required for WAN access.
- The client must support IKEv2 gateway redirect as per RFC 5685 (currently applies to Hirschmann routers and the Hirschmann Advanced VPN Client on Windows).

In **LANconfig** you configure the IKEv2 load balancer under **VPN** > **IKEv2/IPSec** > **IKEv2 load balancer**



in the menu **Load balancer**,

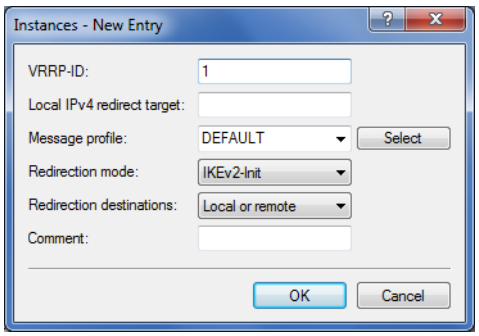


Load balancer enabled

activates the IKEv2 load balancer.

5.10.1 Instances

Load balancer instances are configured in the **Instances** table.



VRRP-ID

VRRP-ID (router ID) to be used for this IKEv2 load balancer instance. VRRP must be activated on this device and configured for this VRRP ID.

Possible values:

0 to 255

Default: 1

Local IPv4 redirect target

IPv4 address or FQDN on which the device is to receive VPN tunnels. A VPN client is forwarded to this address by the master in the load-balancer cluster.

This is not the virtual VRRP-IP address.

Message profile

Message profile to use for this instance. The message profile contains the parameters for the status log used by the device to communicate its status information to the load balancer cluster.

Default: DEFAULT.

Redirection mode

Specifies at which phase of the IKEv2 negotiation the VPN gateway redirects clients to another gateway.

This parameter only takes effect if the device is VRRP master.

Possible values:

IKEv2-Init (default)

The redirect message is sent in the IKE_SA_INIT response from the VPN gateway.

IKEv2-Auth

The redirect message is sent in the IKE_AUTH phase after the client has identified itself to the VPN gateway.

Redirection destinations

Specifies the destination to which the VPN client is redirected.

The parameter only takes effect if the device is VRRP master.

Possible values:

Local or remote

Clients are redirected to the device's own IP address and also to other remote gateways in the cluster.

Remote only

Clients are only redirected to other VPN gateways. This results in VPN clients being evenly distributed between all gateways except for the master gateway.

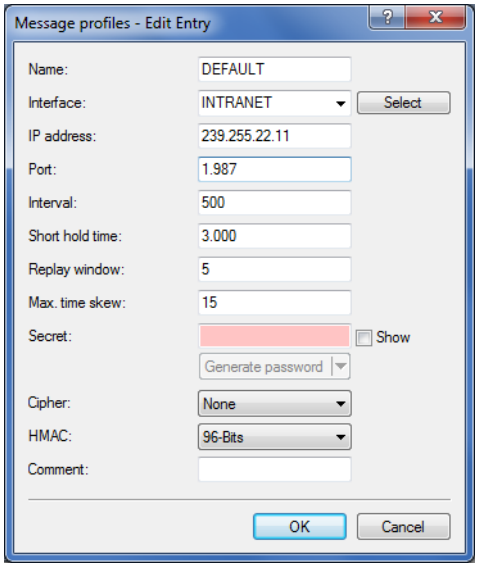
This can be used to configure scenarios in which the load balancer master only distributes the clients, but does not terminate any VPN tunnels itself.

Comment

Enter a descriptive comment for this entry.

5.10.2 Message profiles

The **Message profiles** table contains the parameters for the status log used by the VPN gateways to communicate their status information to the load balancer cluster.



Name

Unique name for this profile

Interface

Interface used by the IKEv2 load balancer to exchange status messages with other VPN gateways in the cluster.

Possible values:

Entries from the IPv4 networks table

IP address

Specifies the multicast IP address used by the IKEv2 load balancer to communicate on the local network.

Default: 239.255.22.11

Port

Specifies the port used by the IKEv2 load balancer to communicate on the local network.

Default: 1987

Interval

Interval (in milliseconds), in which status messages are exchanged between the IKEv2 load balancers.

Possible values:

0 to 65535

Default: 500

Short hold time

Specifies the time in milliseconds following the last status message, after which the other IKEv2 load balancers flag the device as disabled.

The short hold time must be greater than the interval. A recommended value is at least three times the **Interval** parameter.

Possible values:

0 to 65535

Default: 3000

Replay window

Size of the replay window (the number of messages) for IKEv2 load-balancer status messages. Messages that fall outside the replay window are dropped.

Possible values:

1 to 9

Default: 5

0

Disables the replay detection.

Max. time skew

Maximum permitted time deviation (in seconds) of the time stamps in status messages from the IKEv2 load balancer. Messages with a higher skew are dropped.

Possible values:

0 to 255

Default: 15

Secret

Shared secret for the load balancer communication log.

The secret must be the same on all of the VPN gateways in a cluster.

Possible values:

Up to 32 random characters

Cipher

Specifies the encryption algorithm used for the status messages from the IKEv2 load balancers.

Possible values:

None (default)

AES-128-GCM

AES-192-GCM

AES-256-GCM

HMAC

Specifies the signaling algorithm used for the status messages from the IKEv2 load balancers.

Possible values:

None

96 bits (default)

128 bits

Comment

Enter a descriptive comment for this entry.

5.10.3 Show commands via CLI

`show vlb-status`: Displays the status of the individual gateways in the cluster.

5.10.4 Trace commands

The available trace commands are listed in the following:

- VLB-Status
- VLB-Packet

5.10.5 Additions to the Setup menu

IKEv2 load balancer

Configures the IKEv2 load balancer.

SNMP ID:

2.19.50

Telnet path:

Setup > **VPN**

Operating

Activates/deactivates the IKEv2 load balancer.

SNMP ID:

2.19.50.1

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer**

Possible values:

Yes

Activates the IKEv2 load balancer.

No

Deactivates the IKEv2 load balancer.

Default:

No

Instances

Load balancer instances are configured in the **Instances** table.

SNMP ID:

2.19.50.2

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer**

VRRP-ID

VRRP-ID (router ID) to be used for this IKEv2 load balancer instance. VRRP must be activated on this device and configured for this VRRP ID.

SNMP ID:

2.19.50.2.1

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

0 … 255

Default:

1

Local IPv4 redirect target

IPv4 address or FQDN on which the device is to receive VPN tunnels. A VPN client is forwarded to this address by the master in the load-balancer cluster.

This is not the virtual VRRP-IP address.

SNMP ID:

2.19.50.2.2

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Message profile

Message profile to use for this instance. The message profile contains the parameters for the status log used by the device to communicate its status information to the load balancer cluster.

SNMP ID:

2.19.50.2.4

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Default:

DEFAULT

Redirection mode

Specifies at which phase of the IKEv2 negotiation the VPN gateway redirects clients to another gateway.

This parameter only takes effect if the device is VRRP master.

SNMP ID:

2.19.50.2.5

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

IKEv2-Init

The redirect message is sent in the IKE_SA_INIT response from the VPN gateway.

IKEv2-Auth

The redirect message is sent in the IKE_AUTH phase after the client has identified itself to the VPN gateway.

Default:

IKEv2-Init

Redirection destinations

Specifies the destination to which the VPN client is redirected.

The parameter only takes effect if the device is VRRP master.

This can be used to configure scenarios in which the load balancer master only distributes the clients, but does not terminate any VPN tunnels itself.

SNMP ID:

2.19.50.2.6

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

Local or remote

Clients are redirected to the device's own IP address and also to other remote gateways in the cluster.

Remote only

Clients are only redirected to other VPN gateways. This results in VPN clients being evenly distributed between all gateways except for the master gateway.

Comment

Contains a comment about this instance.

SNMP ID:

2.19.50.2.7

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Message profiles

The **Message profiles** table contains the parameters for the status log used by the VPN gateways to communicate their status information to the load balancer cluster.

SNMP ID:

2.19.50.3

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer**

Name

Unique name for this profile

SNMP ID:

2.19.50.3.1

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Interface

Interface used by the IKEv2 load balancer to exchange status messages with other VPN gateways in the cluster.

SNMP ID:

2.19.50.3.2

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

Entries from the IPv4 networks table

IP address

Specifies the multicast IP address used by the IKEv2 load balancer to communicate on the local network.

SNMP ID:

2.19.50.3.3

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

IPv4 address `[0-9.]`

Default:

239.255.22.11

Port

Specifies the port used by the IKEv2 load balancer to communicate on the local network.

SNMP ID:

2.19.50.3.4

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 65535

Default:

1987

Interval

Interval (in milliseconds), in which status messages are exchanged between the IKEv2 load balancers.

SNMP ID:

2.19.50.3.5

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 65535

Default:

500

Short hold time

Specifies the time in milliseconds following the last status message, after which the other IKEv2 load balancers flag the device as disabled.

The short hold time must be greater than the interval. A recommended value is at least three times the **Interval** parameter.

SNMP ID:

2.19.50.3.6

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 65535

Default:

3000

Replay window

Size of the replay window (the number of messages) for IKEv2 load-balancer status messages. Messages that fall outside the replay window are dropped.

SNMP ID:

2.19.50.3.7

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 9

Default:

5

Special values:

0

Disables the replay detection.

Max. time skew

Maximum permitted time deviation (in seconds) of the time stamps in status messages from the IKEv2 load balancer. Messages with a higher skew are dropped.

SNMP ID:

2.19.50.3.8

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

0 … 255

Default:

15

Key

Shared secret for the load balancer communication log.

The secret must be the same on all of the VPN gateways in a cluster.

SNMP ID:

2.19.50.3.9

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

32 characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Cipher

Specifies the encryption algorithm used for the status messages from the IKEv2 load balancers.

SNMP ID:

2.19.50.3.10

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

None
AES-128-GCM
AES-192-GCM
AES-256-GCM

Default:

None

HMAC

Specifies the signaling algorithm used for the status messages from the IKEv2 load balancers.

SNMP ID:

2.19.50.3.11

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Message-Profiles**

Possible values:

None
96 bits
128 bits

Default:

96 bits

Comment

Contains a comment about this message profile.

SNMP ID:

2.19.50.3.12

Telnet path:

Setup > **VPN** > **IKEv2 Load Balancer** > **Instances**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

5.11 Flexible identity comparison for PSK connections

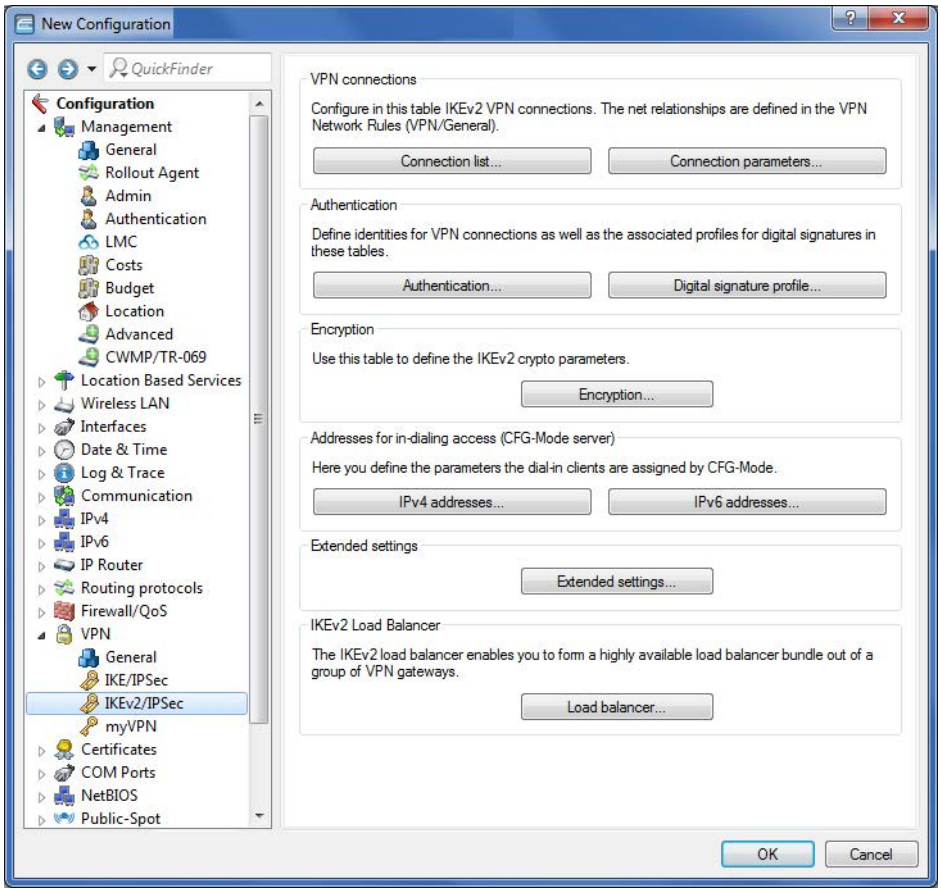
With HiLCOS 10.12 the flexible identity comparison now includes PSK connections (IKEv2). Until now, identity comparison was only possible for certificate-based VPN connections (distinguished name).

Support of "wildcard globbing" is now available for IKEv2 identities. Here '?' stands for exactly one character and '*' for any number characters, including zero.

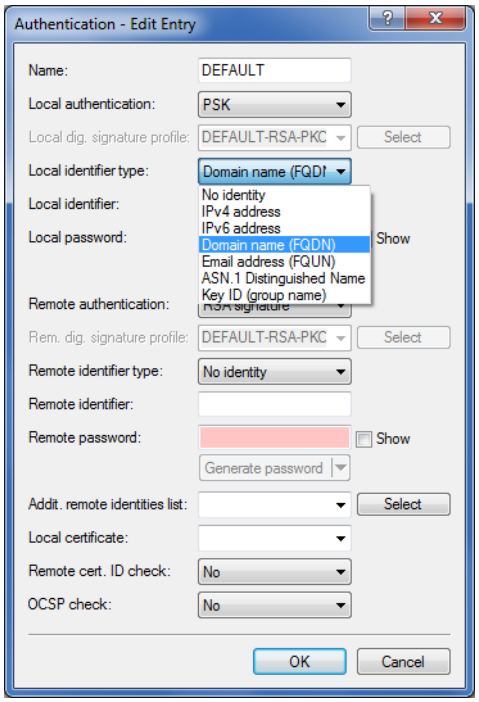
This feature makes it easier to configure your VPN, since in principle all you need for inbound IKEv2 connections is a single entry.

The prerequisite is that all inbound connections use a particular syntax and that flexible comparison is enabled.

Flexible identity comparison is configured in **LANconfig** under **VPN** > **IKEv2/IPSec** > **Authentication** and clicking the **Authentication** button.



Flexible identity comparison for PSK connections supports the two identity types **FQUN** and **FQDN**.



Please note that all parameters are case-sensitive.

On the command line, you can access the parameters with the path **Setup** > **VPN** > **IKEv2** > **Auth** > **Parameter**.

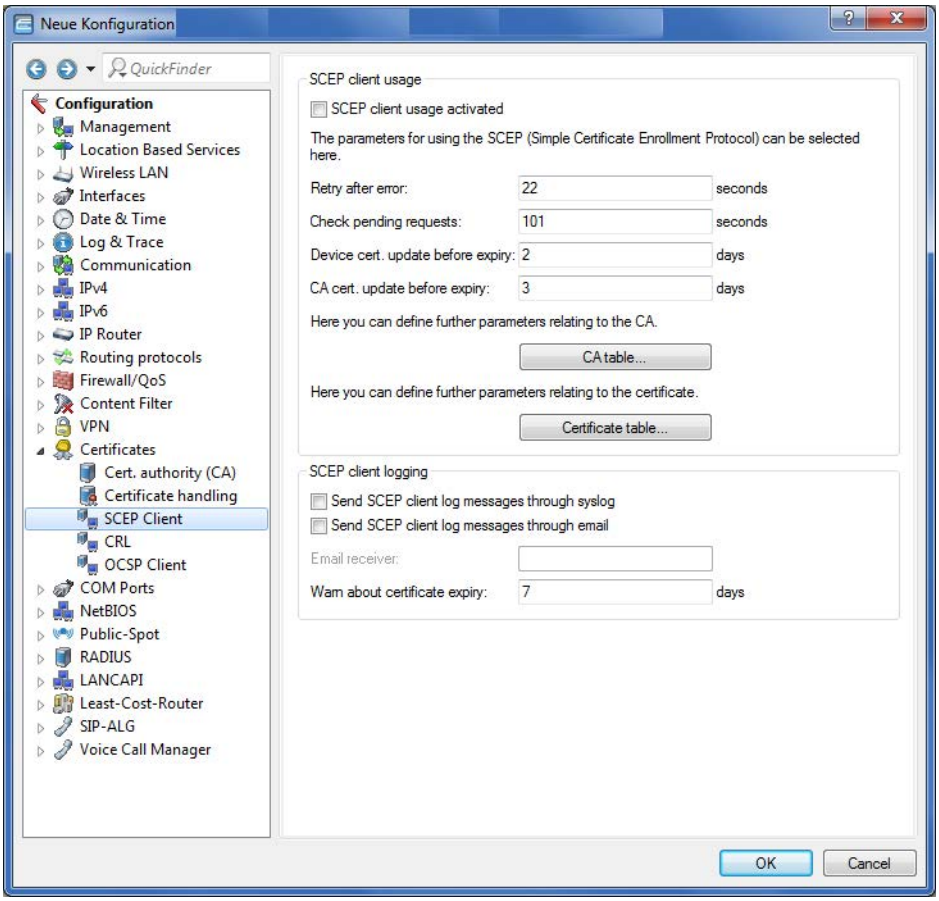
5.12 SCEP client logging

As of HiLCOS 10.12 you have the option to send an e-mail or SYSLOG message informing you that the certificate has expired after an unsuccessful request for certificate renewal.

You can also issue a warning message in advance. In this way you can ensure that there is enough time to update the certificate before it expires.

5.12.1 Configuration by LANconfig

You configure the new feature under **Certificates** > **SCEP client** > **SCEP client logging**.



The new parameters:

Send SCEP client log messages through syslog

Enables/disables log message transmission via SYSLOG.

Send SCEP client log messages through email

Enables/disables log message transmission via e-mail.

This requires that you enter an e-mail address in the corresponding input box.

Email receiver

E-mail address to receive the log message.

To make an entry, you first have to activate the option **Send SCEP client log messages through email**.

Warn about certificate expiry

Time interval in days before certificate expiry.

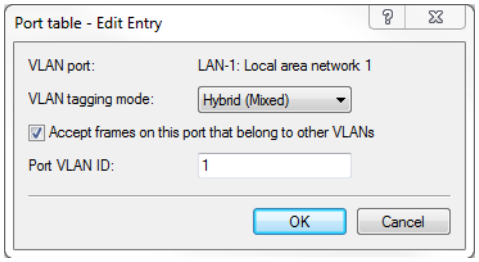
6 Virtual LANs (VLAN)

6.1 VLAN-tagging mode "ingress mixed" removed

As of HiLCOS 10.12, the VLAN-tagging mode "ingress mixed" in the VLAN port table is deprecated.
This tagging mode is now automatically converted to "Hybrid (mixed)" mode. The default value for new configurations is also the mode "Hybrid (mixed)".

6.1.1 The port table

The port table is used to configure each of the device's ports that are used in the VLAN. The table has an entry for each of the device's ports with the following values.



LANconfig: Interfaces / VLAN / Port table

WEBconfig: HiLCOS menu tree / Setup / VLAN / Port-Table

- **Port**: The name of the port; this cannot be edited
- **Tagging mode**

  Controls the processing and assignment of VLAN tags at this port.

  - Access (never): Outbound packets are not given a VLAN tag at this port. Incoming packets are treated as though they have no VLAN tag. If incoming packets have a VLAN tag, it is ignored and treated as though it were part of the packet's payload. Incoming packets are always assigned to the VLAN defined for this port.
  - Trunk (always): Outgoing packets at this port are always assigned with a VLAN tag, irrespective of whether they belong to the VLAN defined for this port or not. Incoming packets must have a VLAN tag, otherwise they are dropped.
  - Hybrid (mixed): Allows mixed operation of packets with and without VLAN tags at the port. Packets without a VLAN tag are assigned to the VLAN defined for this port. Outgoing packets are given a VLAN tag unless they belong to the VLAN defined for this port.
  - Default: Hybrid (mixed)

- **Allow all VLANs (allows packets from other VLANs to enter this port)**

  This option defines whether tagged data packets with any VLAN ID should be accepted, even if the port is not a "member" of this VLAN.

- **Port VLAN-ID**

  This port ID has two functions:

  - Untagged packets received at this port in "Hybrid (mixed)" mode are assigned to this VLAN, as are all ingress packets received in "Access (never)" mode.

- In the "Hybrid (mixed)" mode, this value determines whether outgoing packets receive a VLAN tag or not: Packets assigned to the VLAN defined for this port receive **no** VLAN tag; all others are given a VLAN tag.

7 Routing and WAN connections

7.1 Route monitor

As of HiLCOS 10.12, a route monitor checks the network connections to a specified prefix. This prefix is learned, for example as the result of a dynamic routing protocol such as BGP.

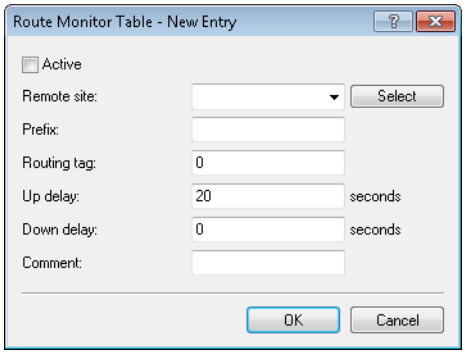
In case of a faulty connection, the route monitor opens a backup connection, if required.

The route monitor observes the connections to the networks of different providers and establishes a backup connection in case of failure. The monitoring makes use of a trigger prefix, which providers supply in their routing protocol, for example with the Border Gateway Protocol (BGP). As soon as a route to a provider's network becomes unavailable, the route monitor declares the relevant trigger prefix to be invalid for its network and opens a backup connection to the provider's network.

7.1.1 Configuring the route monitor with LANconfig

To activate the route monitor, switch to the view **Communication** > **Call management** and check the option **Route monitor active**.

To configure the route monitor, open the **Route monitor table**.



Operating

Specifies whether this backup connection is enabled.

Remote site

Contains the name of the backup remote station.

Prefix

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

Routing tag

Contains the routing tag of the prefix being monitored.

Up delay

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

Down delay

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

The value "0" causes the device to disconnect from the backup peer immediately after the prefix arrives (no delay).

Comment

Comment on this entry.

7.1.2 Additions to the Setup menu

Route monitor

In this directory, you configure the route monitor.

SNMP ID:

2.93.2

Telnet path:

Setup > **Routing-protocols**

Monitor table

In this table, you configure the route monitor.

SNMP ID:

2.93.2.1

Telnet path:

Setup > **Routing-protocols** > **Route-monitor**

Backup peer

Contains the name of the backup remote station.

SNMP ID:

2.93.2.1.1

Telnet path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Prefix

Contains the prefix (IPv4 or IPv6 address) to be observed by the route monitor.

SNMP ID:

2.93.2.1.2

Telnet path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:./`

Default:

empty

Rtg-Tag

Contains the routing tag of the prefix being monitored.

SNMP ID:

2.93.2.1.3

Telnet path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Up delay

Should the prefix fail to arrive, the device waits for this delay in seconds before it connects to the backup peer.

SNMP ID:

2.93.2.1.4

Telnet path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 10 characters from `[0-9]`

Default:

20

Down delay

Once the prefix arrives, the device waits for the delay in seconds specified here before it disconnects from the backup peer.

SNMP ID:

2.93.2.1.5

Telnet path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Special values:

0

No delay: The device immediately closes the connection to the backup peer when the prefix arrives.

Operating

Specifies whether this backup connection is enabled.

SNMP ID:

2.93.2.1.6

Telnet path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Yes

The backup connection is enabled.

No

The backup connection is disabled.

Default:

No

Comment

Comment on this entry.

SNMP ID:

2.93.2.1.7

Telnet path:

Setup > **Routing-protocols** > **Route-monitor** > **Monitor-table**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Operating

This action is used to enable or disable the route monitor.

SNMP ID:

2.93.2.2

Telnet path:

Setup > **Routing-protocols** > **Route-monitor**

Possible values:

No
The route monitor is disabled.

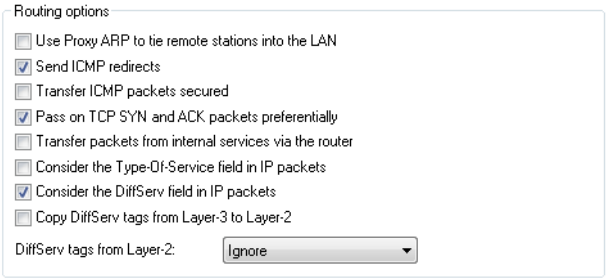
Yes
The route monitor is enabled.

Default:

No

7.2 DiffServ field enabled by default

As of HiLCOS 10.12, the routing method observes the DiffServ field in IP packets by default.



Consider the DiffServ field in IP packets

If the router considers the DiffServ field in IP packets, it applies preferential transmission according to the standardized DSCP (DiffServ code point) AFxx (Assured Forwarding) for secured transmission and EF (Expedited Forwarding). All other IP packets will be transmitted normally. This option is enabled by default.

This option cannot be used in combination with ToS since the DiffServ field replaces the ToS field within the IP packet.

For more information about DiffServ, see the chapter *Quality-of-Service*.

7.2.1 Additions to the Setup menu

Routing method

Controls the analysis of ToS or DiffServ fields.

SNMP ID:

2.8.7.1

Telnet path:

Setup > **IP-Router** > **Routing-Method**

Possible values:

Normal
The TOS/DiffServ field is ignored.

Type of service
The TOS/DiffServ field is regarded as a TOS field; the bits "low delay" and "high reliability" will be evaluated.

DiffServ
The TOS/DiffServ field is regarded as a DiffServ field and evaluated as follows.

- **CSx (including CS0 = BE):** Normal transmission
- **AFxx:** Secure transmission
- **EF:** Preferred transmission

Default:

DiffServ

7.3 iPerf-compliant server/client

As of HiLCOS 10.12, HiLCOS features the tool "iPerf" for performance measurements over network routes. It performs bandwidth measurements either one-way or two-way. Iperf can be started directly from any Hirschmann device. The Hirschmann device is able to act as a client and as a server (UDP/TCP). The HiLCOS implementation is based on iPerf2.

iPerf can be configured either via LANconfig or via the command-line console.

7.3.1 Bandwidth measurements with iPerf

Measurements of network performance determine values such as the throughput, latency, jitter and error rates over a network connection. The measured values are used, among other things, for network optimization, error detection and troubleshooting, and for assessing the performance of network infrastructures.

iPerf has become established as a free program for generating and evaluating data streams over data connections. An iPerf server daemon receives TCP and UDP streams and measures the throughput for the corresponding applications along with the latency, jitter, packet loss and packet reordering over UDP connections.

To conduct a bandwidth measurement between two hosts, you start the iPerf server on one device and the iPerf client on the other one. The iPerf client then connects to the iPerf server. The server and client exchange data packets for a certain time or a certain amount of data and generate statistics about this. These statistics provide information about the quality of the connection between the two devices.

When measuring the quality of the TCP connection, the iPerf client transmits completely filled TCP data packets at the fastest speed possible. The average data rate of successful data transfer (“goodput”) is the result of what the iPerf server received correctly.

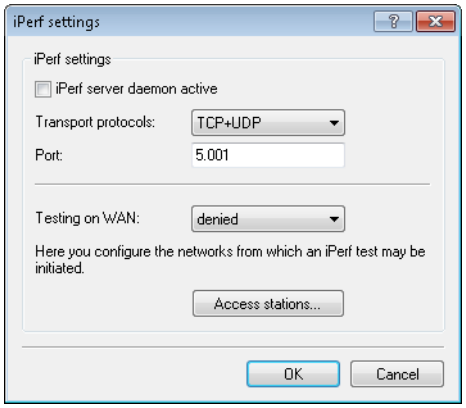
When measuring UDP connection quality, the iPerf client transmits data over a specified bandwidth (1 Mbps by default), although this is without flow or performance control. The “goodput” relates to the maximum bandwidth with which the client's transmission buffer remains permanently filled without data packets being lost.

Hirschmann devices include an Iperf2-compatible feature that directly measures the network performance between network nodes such as routers, VPN gateways, and APs. This makes it easier to measure the data throughput over WAN connections or WLAN point-to-point links, for example.

Measurements can be carried out between two Hirschmann devices or between a Hirschmann device and another iPerf2 instance.

7.3.2 Setting up iPerf with LANconfig

In LANconfig, you configure iPerf under **Log & Trace** > **General** and clicking on **iPerf settings**.



iPerf server daemon active

Activates or deactivates the iPerf server daemon.

Rather than setting up the iPerf server to run permanently at this point, you can optionally start a one-off test by accessing the command-line console via SSH and starting a temporary iPerf server.

Transport protocols

Here you set which transport protocols are to be measured for bandwidth.

Port

This port is used for communications between the iPerf client and server (“5001” by default).

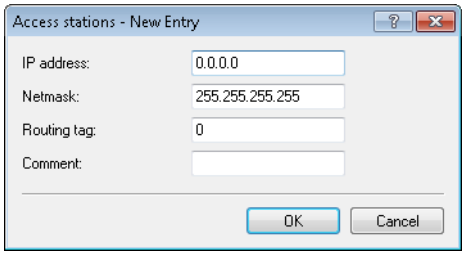
Testing on WAN

Here you determine whether measurements are also permitted over a WAN connection.

Depending on the provider contract, additional connection charges may arise from measurements over WAN connections.

Access stations

In order restrict iPerf access to certain stations only, enter the connection data into this table.



IP address

Enter the IPv4 address of the remote station.

Netmask

Enter the netmask of the remote station.

Routing tag

Enter the routing tag that specifies the connection to the remote station.

Comment

Enter a descriptive comment for this entry.

7.3.3 Temporary iPerf server and client

If you configure iPerf with LANconfig, the iPerf function remains permanently active. You can optionally start a temporary iPerf daemon, which remains active for just one test, by using SSH to connect to the command-line console.

To do this, start a terminal program (e.g. PuTTY) and open a connection to the device where you want to perform the iPerf test. Use the console command `iperf` and the appropriate option switches to start the temporary iPerf daemon. The following examples illustrate some standard commands.

More information about the option switches for `iperf` is available in the section *Commands for the console*.

Running the iPerf server in TCP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s
[Iperf-TCP-Server|1526] Now listening on port 5001
```

Press the Enter button again or close the console window to stop the iPerf server.

Running the iPerf server in UDP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -s -u
[Iperf-UDP-Server|1524] Now listening on port 5001
```

Press the Enter button again or close the console window to stop the iPerf server.

Running the iPerf client in UDP mode

```
root@device:/Setup/Iperf/Server-Daemon
> iperf -u -c 172.16.30.23
WARN: Using default UPD bandwidth limitation of 1 MBit/s
WARN: Using default UDP payload length of 1472 bytes (for matching Ethernet MTU
via IPv4)
[Iperf-UDP-Client|2100] Connecting to server...
[Iperf-UDP-Client|2100] Connection established to 172.16.30.23:5001

root@device:/
>
```

Press the Enter key to exit the test.

```
[Iperf-UDP-Client|2100] Connection closed actively
[Iperf-UDP-Client|2100] Sent 1249728 bytes within 10s (10000ms) -> 0 Mbit/s (999
 Kbit/s)
[Iperf-UDP-Client|2100] Server reports 1249728 bytes received within 9s (9985ms)
 -> 1 Mbit/s (1001 Kbit/s)
[Iperf-UDP-Client|2100] Server received 849 packets (0 lost / 0 out-of-order) with
 62us jitter

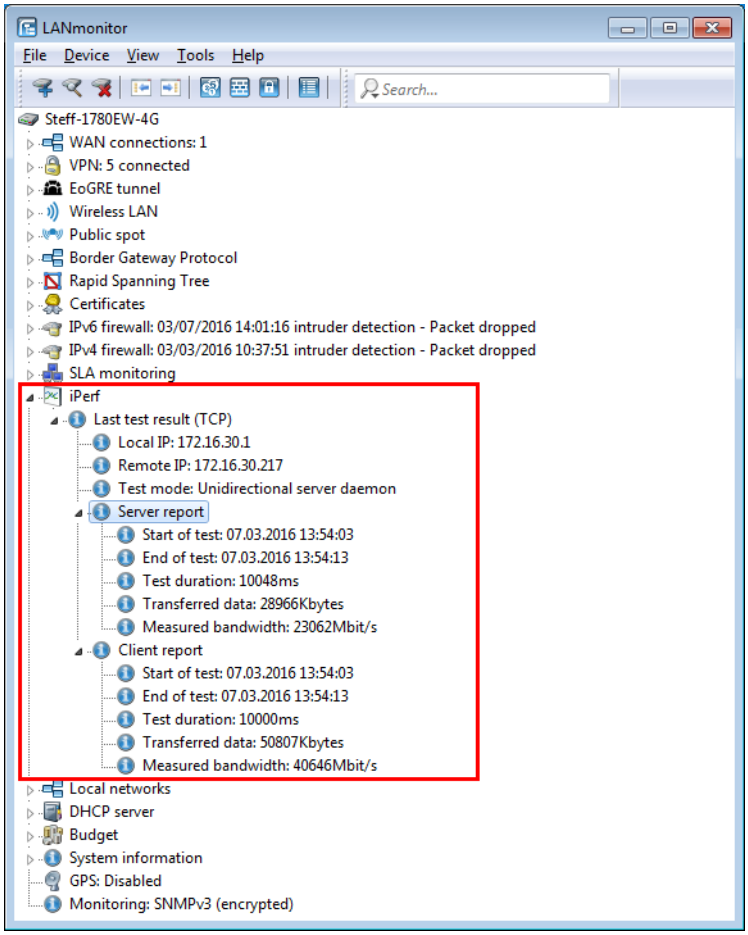
root@device:/
>
```

7.3.4 Analyzing iPerf results with LANmonitor

Hirschmann devices include an Iperf2-compatible feature that directly measures the network performance between network nodes such as routers, VPN gateways, and APs. This makes it easier to measure the data throughput over WAN connections or WLAN point-to-point links, for example.

For more information on iPerf, see the section *Bandwidth measurements with iPerf*.

The last iPerf test result can also be viewed in LANmonitor under "iPerf". In this case it is unimportant whether the device initiated a connection or was contacted externally. The connection type "Test mode" displays the mode accordingly:



LANmonitor displays the test results stored in the device under **Status** > **Iperf** > **Last results**.

7.3.5 iPerf commands on the command line

Table 2: Overview of iPerf options

Command	Description
`iperf [-s|-c <Host>] [-u] [-p <Port>] [-B <Interface>] [-c] [-b [<Bandw>/]<Bandw>[kKmM]] [-l <Length>] [-t <Time>] [-d] [-r] [-L <Port>] [-h]`	Starts iPerf on the device in order to perform a bandwidth measurement with an iPerf2 remote station. Possible arguments are: ■ **Client/server** □ `-u, --udp`: Uses UDP instead of TCP. □ `-p, --port <Port>`: Connects with or expects data packets on this port (default: 5001). □ `-B, --bind <Interface>`: Permits the connection only via the specified interface (IP address or interface name). ■ **Server specific** □ `-s, --server`: Starts iPerf in server mode and waits for an iPerf client to contact it.

Command	Description
	■ **Client specific** ▫ `-c, --client <Host>`: Starts iPerf in client mode and connects with the iPerf server <Host> (IP address or DNS name). ▫ `-b, --bandwidth [<Bandw>/]<Bandw>{kKmM}`: Limit the [down]/up-stream bandwidth when analyzing a UDP connection. This Is specified as kilobytes (kK) or megabytes (mM) per second (default: 1 Mbps). ▫ `-l, --len <Length>`: Sets the length of the UDP data packets. ▫ `-t, --time <Time>`: Sets the duration of the connection in seconds (default: 10 seconds). ▫ `-d, --dualtest`: The test is bidirectional: the iPerf server and client send and receive at the same time. ▫ `-r, --tradeoff`: The test is sequential: the iPerf server and client send and receive one after the other. ▫ `-L, --listenport <Port>`: Specifies the port where the device in bidirectional mode expects to receive data packets from the remote iPerf server (default: 5001). ■ **Miscellaneous** ▫ `-h, --help`: Outputs the help text.

7.3.6 Additions to the Setup menu

Iperf

iPerf measures the throughput for TCP and UDP applications, as well as latency, jitter, packet loss or packet reordering for UDP connections.

Use this menu to configure the iPerf settings.

SNMP ID:

2.96

Telnet path:

Setup

Server daemon

This menu contains the configuration for the iPerf server daemon.

SNMP ID:

2.96.1

Telnet path:

Setup > **Iperf**

Operating

This entry is used to enable or disable the iPerf server daemon.

SNMP ID:

2.96.1.1

Telnet path:

Setup > **Iperf** > **Server-Daemon**

Possible values:

No

The iPerf server daemon is not active.

Yes

The iPerf server daemon is active.

Default:

No

Transport

Use this entry to set the transfer protocol used by the iPerf server daemon.

SNMP ID:

2.96.1.2

Telnet path:

Setup > **Iperf** > **Server-Daemon**

Possible values:

UDP
TCP

Default:

UDP

Port

Here you specify a port on which the iPerf server expects packets to arrive.

SNMP ID:

2.96.1.3

Telnet path:

Setup > **Iperf** > **Server-Daemon**

Possible values:

Max. 5 characters from `[0-9]`

Default:

5001

IPv4-WAN-Access

Here you determine whether measurements are also permitted over a WAN connection.

Depending on the provider contract, additional connection charges may arise from measurements over WAN connections.

SNMP ID:

2.96.2

Telnet path:

Setup > **Iperf**

Possible values:

No

Bandwidth measurements are not permitted over a WAN connection.

VPN

The bandwidth measurements are permitted over a WAN connection, but only if it is protected by a VPN tunnel.

Yes

Bandwidth measurements are also permitted over a WAN connection.

Default:

No

IPv4-Access-List

In order restrict iPerf access to certain stations only, enter the connection data into this table.

SNMP ID:

2.96.3

Telnet path:

Setup > **Iperf**

IP address

Enter the IPv4 address of the remote station.

SNMP ID:

2.96.3.1

Telnet path:

Setup > **Iperf** > **IPv4-Access-List**

Possible values:

Max. 15 characters from `[0-9].`

Default:

empty

Netmask

Enter the netmask of the remote station.

SNMP ID:

2.96.3.2

Telnet path:

Setup > **Iperf** > **IPv4-Access-List**

Possible values:

Max. 15 characters from `[0-9].`

Default:

255,255,255,255

Rtg-Tag

Enter the routing tag that specifies the connection to the remote station.

SNMP ID:

2.96.3.3

Telnet path:

Setup > **Iperf** > **IPv4-Access-List**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Comment

Enter a descriptive comment for this entry.

SNMP ID:

2.96.3.4

Telnet path:

Setup > **Iperf** > **IPv4-Access-List**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

7.3.7 Additions to the Status menu

Iperf

Measurements of network performance determine values such as the throughput, latency, jitter and error rates over a network connection. The measured values are used, among other things, for network optimization, error detection and troubleshooting, and for assessing the performance of network infrastructures. Measurements can be performed automatically, periodically or manually on demand.

Iperf has become established as free software for generating and evaluating data streams over data connections. Iperf measures the throughput for TCP and UDP applications, as well as latency, jitter, packet loss and packet reordering for UDP connections.

Hirschmann devices include an iPerf-compatible feature that directly measures the network performance between network nodes such as routers, VPN gateways, and APs. This makes it easier to measure the data throughput over WAN connections or WLAN point-to-point links, for example.

This directory contains an overview of WAN bandwidth measurements.

SNMP ID:

1.96

Telnet path:

Status

Last-Results

This menu contains the tables with the results of WAN bandwidth measurements for TCP and UDP.

SNMP ID:

1.96.1

Telnet path:

Status > **Iperf**

UDP

This menu contains the table with the results of WAN bandwidth measurements for UDP.

In order to analyze the measurements on the client side as well, the iPerf server sends the data back to the iPerf client. These data appear in separate columns of the table.

SNMP ID:

1.96.1.1

Telnet path:

Status > **Iperf** > **Last-Results**

Index

This column contains the sequential number of each entry.

SNMP ID:

1.96.1.1.1

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Local-IP

This column contains the local IP of the measured interface.

SNMP ID:

1.96.1.1.2

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-IP

This column contains the remote IP of the measured interface.

SNMP ID:

1.96.1.1.3

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Mode

This column contains the mode of the measured interface.

SNMP ID:

1.96.1.1.4

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Connections

This column contains the current connections at the measured interface.

SNMP ID:

1.96.1.1.5

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Start

This column contains the time when the iPerf server started.

SNMP ID:

1.96.1.1.6

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Stop

This column contains the time when the iPerf server stopped.

SNMP ID:

1.96.1.1.7

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Duration-ms

This column contains the transmission time of data packets from the server to the client in milliseconds.

SNMP ID:

1.96.1.1.8

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Bytes

This column contains the number of bytes that the server transmitted during the connection.

SNMP ID:

1.96.1.1.9

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Bandwidth-kbps

This column contains the server bandwidth during the connection.

SNMP ID:

1.96.1.1.10

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Packets

This column contains the number of data packets that the server transmitted during the connection.

SNMP ID:

1.96.1.1.11

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Lost-Packets

To detect the loss or reordering of a data packet, the client inserts a sequence ID in the header of every data packet it receives before it returns it to the server.

This column contains the difference between the number of data packets that the server sent and the number the client reported as received.

SNMP ID:

1.96.1.1.12

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Out-Of-Order-Packets

To detect the loss or reordering of a data packet, the client inserts a sequence ID in the header of every data packet it receives before it returns it to the server.

This column contains the number of data packets that the server sent and that were reported by the client as being received in a different order.

SNMP ID:

1.96.1.1.13

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Jitter-us

The client inserts a timestamp into the header of every packet it sends, so enabling the server to measure the latency of this data transfer.

This column contains the latency of the data packets in microseconds.

SNMP ID:

1.96.1.1.14

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Server-Error

Should an error occur, this column contains the error reported by the server during the connection.

SNMP ID:

1.96.1.1.15

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Start

This column contains the time when the iPerf client started.

SNMP ID:

1.96.1.1.16

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Stop

This column contains the time when the iPerf client stopped.

SNMP ID:

1.96.1.1.17

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Duration-ms

This column contains the transmission time of data packets from the client to the server in milliseconds.

SNMP ID:

1.96.1.1.18

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Bytes

This column contains the quantity of data packets in bytes that the client received during the connection.

SNMP ID:

1.96.1.1.19

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Bandwidth-kbps

This column contains the client bandwidth during the connection.

SNMP ID:

1.96.1.1.20

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Packets

This column contains the quantity of data packets that the client received during the connection.

SNMP ID:

1.96.1.1.21

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Client-Error

Should an error occur, this column contains the error reported by the client during the connection.

SNMP ID:

1.96.1.1.22

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Duration-ms

This column contains the transmission time of data packets in milliseconds that the server reported back to the client.

This value appears only when the device is in the iPerf-client mode.

SNMP ID:

1.96.1.1.23

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Bytes

This column contains the number of bytes that the server reported to the client.

This value appears only when the device is in the iPerf-client mode.

SNMP ID:

1.96.1.1.24

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Bandwidth-kbps

This column contains the server bandwidth during the connection that the server reported back to the client.

This value appears only when the device is in the iPerf-client mode.

SNMP ID:

1.96.1.1.25

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Packets

This column contains the number of data packets that the server reports to the client as being sent.

This value appears only when the device is in the iPerf-client mode.

SNMP ID:

1.96.1.1.26

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Lost-Packets

To detect the loss or reordering of a data packet, the client inserts a sequence ID in the header of every data packet it receives before it returns it to the server.

The server uses this to find the difference between the number of data packets that it sent and the number the client reports as received.

This column contains the value that the server reports to the client.

This value appears only when the device is in the iPerf-client mode.

SNMP ID:

1.96.1.1.27

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Out-Of-Order-Packets

To detect the loss or reordering of a data packet, the client inserts a sequence ID in the header of every data packet it receives before it returns it to the server.

The server uses this to calculate the number of data packets that the it sent and that were reported by the client as being received in a different order.

This column contains the value that the server reports to the client.

This value appears only when the device is in the iPerf-client mode.

SNMP ID:

1.96.1.1.28

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

Remote-Server-Jitter-us

The client inserts a timestamp into the header of every packet it sends, so enabling the server to measure the latency of this data transfer.

The server uses this to calculate the latency of the data packets in microseconds.

This column contains the value that the server reports to the client.

This value appears only when the device is in the iPerf-client mode.

SNMP ID:

1.96.1.1.29

Telnet path:

Status > **Iperf** > **Last-Results** > **UDP**

TCP

This menu contains the table with the results of WAN bandwidth measurements for TCP.

SNMP ID:

1.96.1.2

Telnet path:

Status > **Iperf** > **Last-Results**

Index

This column contains the sequential number of each entry.

SNMP ID:

1.96.1.2.1

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Local-IP

This column contains the local IP of the measured interface.

SNMP ID:

1.96.1.2.2

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Remote-IP

This column contains the remote IP of the measured interface.

SNMP ID:

1.96.1.2.3

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Mode

This column contains the mode of the measured interface.

SNMP ID:

1.96.1.2.4

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Connections

This column contains the current connections at the measured interface.

SNMP ID:

1.96.1.2.5

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Start

This column contains the time when the iPerf server started.

SNMP ID:

1.96.1.2.6

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Stop

This column contains the time when the iPerf server stopped.

SNMP ID:

1.96.1.2.7

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Duration-ms

This column contains the transmission time of data packets from the server to the client in milliseconds.

SNMP ID:

1.96.1.2.8

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Bytes

This column contains the number of bytes that the server transmitted during the connection.

SNMP ID:

1.96.1.2.9

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Bandwidth-kbps

This column contains the server bandwidth during the connection.

SNMP ID:

1.96.1.2.10

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Server-Error

Should an error occur, this column contains the error reported by the server during the connection.

SNMP ID:

1.96.1.2.11

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Start

This column contains the time when the iPerf client started.

SNMP ID:

1.96.1.2.12

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Stop

This column contains the time when the iPerf client stopped.

SNMP ID:

1.96.1.2.13

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Duration-ms

This column contains the transmission time of data packets from the client to the server in milliseconds.

SNMP ID:

1.96.1.2.14

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Bytes

This column contains the quantity of data packets in bytes that the client received during the connection.

SNMP ID:

1.96.1.2.15

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Bandwidth-kbps

This column contains the client bandwidth during the connection.

SNMP ID:

1.96.1.2.16

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

Client-Error

Should an error occur, this column contains the error reported by the client during the connection.

SNMP ID:

1.96.1.2.17

Telnet path:

Status > **Iperf** > **Last-Results** > **TCP**

7.4 SLA monitor

As of HiLCOS 10.12, an SLA monitor checks the network connections and the available services. The device performs this by sending data packets over the Internet Control Message Protocol (ICMP) and using ping commands, among other things, to query the accessibility of remote stations.

Information about packet transmission times and the number of lost packets can be inspected via SYSLOG or LANmonitor.

7.4.1 SLA monitoring

SLA monitoring is used to monitor the connections to remote stations within a network infrastructure. Ping tests to specified targets provide information about peer availability, packet transmission times and the number of lost packets. You can optionally define alerts that are issued when certain threshold values are exceeded, and to output these with SYSLOG or LANmonitor. The history of past checks is also stored, so helping administrators to stay up to date about the quality of the connections.

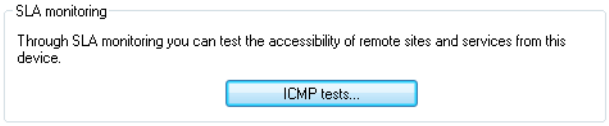
A corresponding SYSLOG client or daemon is required to receive the SYSLOG messages. Logging under UNIX/Linux is generally performed by the SYSLOG daemon that is set up as standard in these operating systems. The daemon either establishes contact with the console or writes its log to an appropriate SYSLOG file.

Under Linux, the file `/etc/syslog.conf` contains a definition of which facilities should be written to which log file. Please check your daemon's configuration to see if it explicitly listens to network connections.

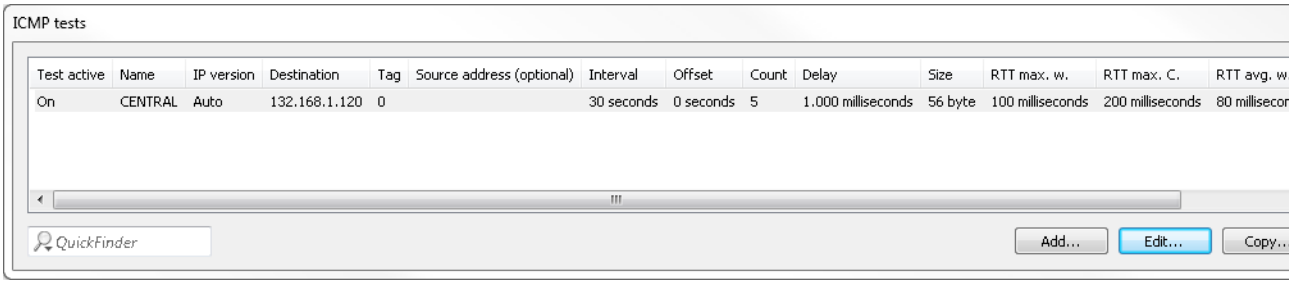
Windows does not provide a corresponding system function. You require special software to provide the functionality of a SYSLOG daemon.

7.4.2 Configuring SLA monitoring with LANconfig

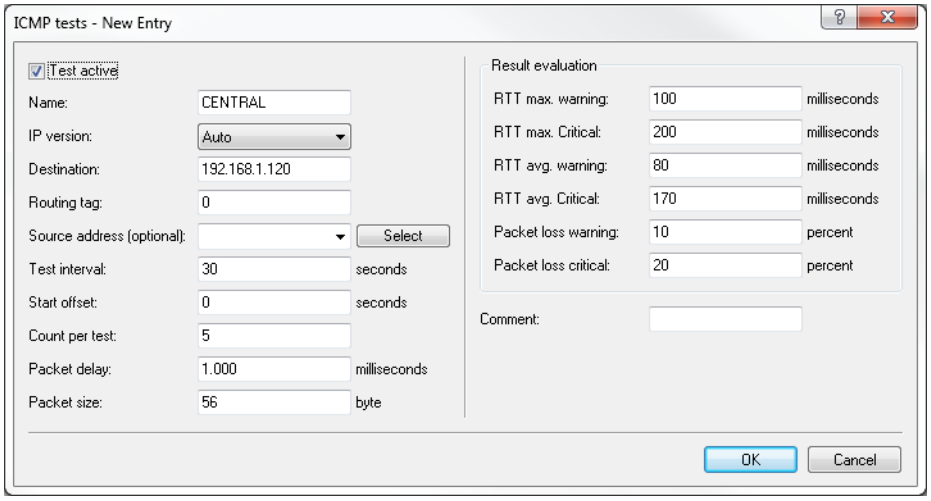
For configuration with LANconfig, the SLA monitor is located under **Log & Trace** > **General** on the **SLA monitoring** pane.



Click the button **ICMP tests**, add new queries and set guideline values for the connection tests.



Click the **Add** button, or select an existing entry and click **Edit**.



Test active

With this check box enabled, the device uses the specified settings for the connectivity test.

Name

Name of connection

IP version

Specifies the use of IPv4 or IPv6.

The setting "Auto" is selected by default.

Destination

Specifies the destination for testing (ICMP/PING destination).

Routing tag

Specify a routing tag if a particular route is to be used.

Source address (optional)

You can optionally configure a source address if you want to use a specific network as the source interface.

Test Interval:

Specifies the time interval in which the device sends ICMP packets (**default: 30 seconds**).

Start offset

Set a delay time before ICMP packets are sent.

Count per test

Specifies how many ICMP packets are sent per test (**default: 5**).

Packet delay

Set a delay before packets are sent.

Packet size

Sets the packet size for the ICMP message.

Result evaluation

In this section, you specify the threshold limits for packet handling.

RTT max. warning

Specify a maximum packet transmission time (**R**ound **T**rip **T**ime). A warning message is generated if an ICMP packet takes longer than the transmission time specified here.

RTT max. critical

An error message is generated if an ICMP packet takes longer than the transmission time specified here.

RTT avg. warning

Specify an average packet transmission time here. A warning message is generated if the average number of ICMP packets takes longer than the transmission time specified here.

RTT avg. critical

Specify an average packet transmission time here. An error message is generated if the average number of ICMP packets takes longer than the transmission time specified here.

Packet loss warning

A warning message is generated if the percentage of lost packets reaches the value specified here.

Packet loss critical

An error message is generated if the percentage of lost packets reaches the value specified here.

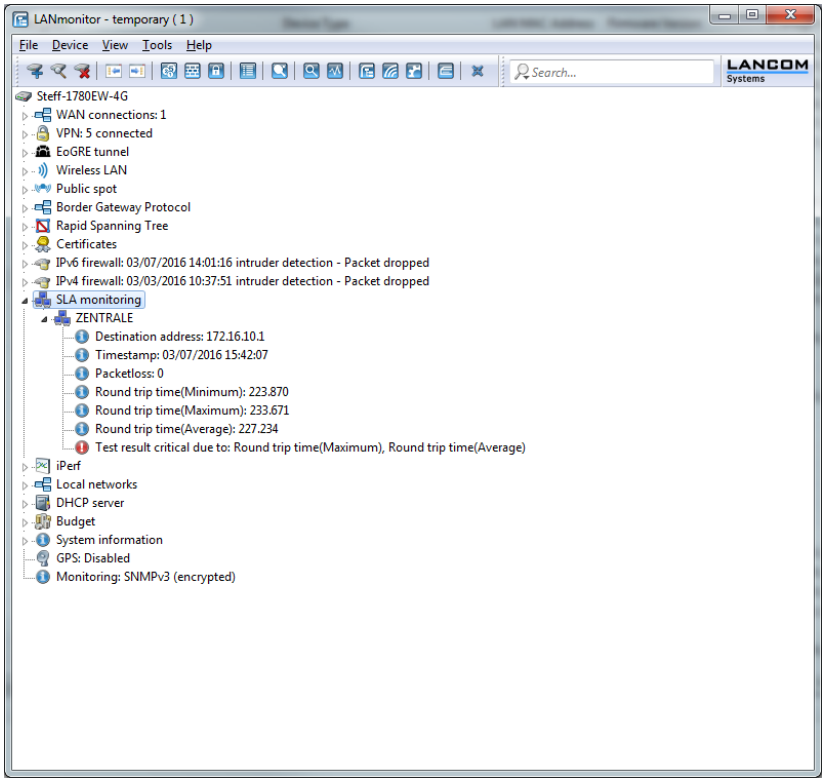
Comment

Enter a descriptive comment for this entry.

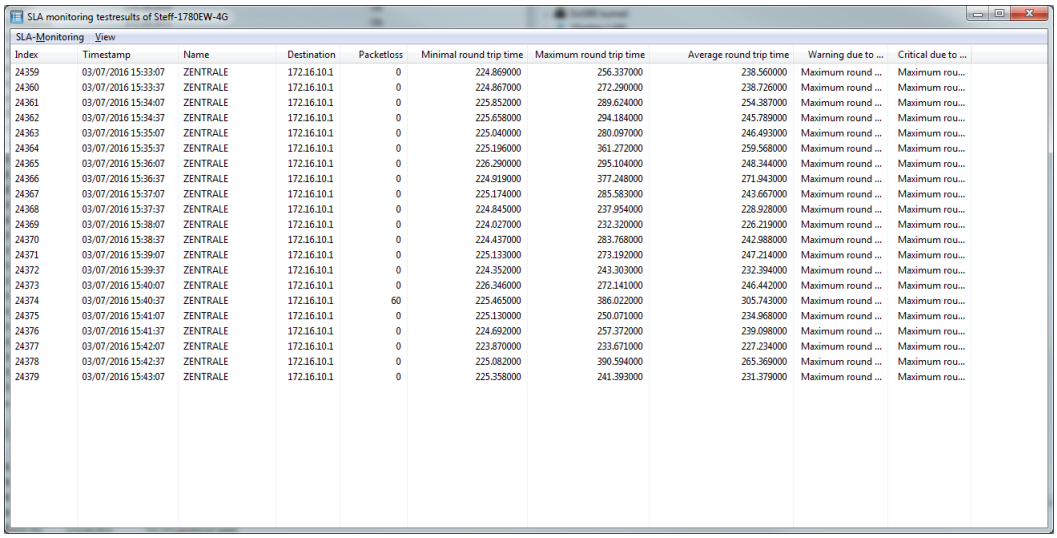
7.4.3 Displaying the SLA monitoring results in LANmonitor

LANmonitor displays the configured tests under **SLA monitoring**.

It shows the results of the most recently collected information from the connection test.



You also have the option to display the history of the connection tests. Click with the right mouse button on the entry **SLA monitoring**. In the following dialog, select **SLA monitoring history**.



Index	Timestamp	Name	Destination	Packetloss	Minimal round trip time	Maximum round trip time	Average round trip time	Warning due to ...	Critical due to ...
24359	03/07/2016 15:33:07	ZENTRALE	172.16.10.1	0	224.869000	256.337000	238.560000	Maximum round ...	Maximum rou...
24360	03/07/2016 15:33:37	ZENTRALE	172.16.10.1	0	224.867000	272.290000	238.726000	Maximum round ...	Maximum rou...
24361	03/07/2016 15:34:07	ZENTRALE	172.16.10.1	0	225.852000	289.624000	254.387000	Maximum round ...	Maximum rou...
24362	03/07/2016 15:34:37	ZENTRALE	172.16.10.1	0	225.658000	294.184000	245.789000	Maximum round ...	Maximum rou...
24363	03/07/2016 15:35:07	ZENTRALE	172.16.10.1	0	225.040000	280.097000	246.493000	Maximum round ...	Maximum rou...
24364	03/07/2016 15:35:37	ZENTRALE	172.16.10.1	0	225.196000	361.272000	259.568000	Maximum round ...	Maximum rou...
24365	03/07/2016 15:36:07	ZENTRALE	172.16.10.1	0	226.290000	295.104000	248.344000	Maximum round ...	Maximum rou...
24366	03/07/2016 15:36:37	ZENTRALE	172.16.10.1	0	224.919000	377.248000	271.943000	Maximum round ...	Maximum rou...
24367	03/07/2016 15:37:07	ZENTRALE	172.16.10.1	0	225.174000	285.583000	243.667000	Maximum round ...	Maximum rou...
24368	03/07/2016 15:37:37	ZENTRALE	172.16.10.1	0	224.845000	237.954000	228.928000	Maximum round ...	Maximum rou...
24369	03/07/2016 15:38:07	ZENTRALE	172.16.10.1	0	224.027000	232.320000	226.219000	Maximum round ...	Maximum rou...
24370	03/07/2016 15:38:37	ZENTRALE	172.16.10.1	0	224.437000	283.768000	242.988000	Maximum round ...	Maximum rou...
24371	03/07/2016 15:39:07	ZENTRALE	172.16.10.1	0	225.133000	273.192000	247.214000	Maximum round ...	Maximum rou...
24372	03/07/2016 15:39:37	ZENTRALE	172.16.10.1	0	224.352000	243.303000	232.394000	Maximum round ...	Maximum rou...
24373	03/07/2016 15:40:07	ZENTRALE	172.16.10.1	0	226.346000	272.141000	246.442000	Maximum round ...	Maximum rou...
24374	03/07/2016 15:40:37	ZENTRALE	172.16.10.1	60	225.465000	386.022000	305.743000	Maximum round ...	Maximum rou...
24375	03/07/2016 15:41:07	ZENTRALE	172.16.10.1	0	225.130000	250.071000	234.968000	Maximum round ...	Maximum rou...
24376	03/07/2016 15:41:37	ZENTRALE	172.16.10.1	0	224.692000	257.372000	239.098000	Maximum round ...	Maximum rou...
24377	03/07/2016 15:42:07	ZENTRALE	172.16.10.1	0	223.870000	233.671000	227.234000	Maximum round ...	Maximum rou...
24378	03/07/2016 15:42:37	ZENTRALE	172.16.10.1	0	225.082000	390.594000	265.369000	Maximum round ...	Maximum rou...
24379	03/07/2016 15:43:07	ZENTRALE	172.16.10.1	0	225.358000	241.393000	231.379000	Maximum round ...	Maximum rou...

7.4.4 Additions to the Status menu

SLA monitor

This menu contains the status values for the SLA monitor.

SNMP ID:

1.36

Telnet path:

Status

ICMP

This menu contains the history log and the recent results of the ICMP.

SNMP ID:

1.36.1

Telnet path:

Status > **SLA-Monitor**

History log

This entry contains the history table.

SNMP ID:

1.36.1.1

Telnet path:

Status > **SLA-Monitor** > **ICMP**

Index

Consecutive numbering of entries.

SNMP ID:

1.36.1.1.1

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

Timestamp

Exact time when the entry was created.

SNMP ID:

1.36.1.1.2

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

Name

Name of the ICMP configuration.

SNMP ID:

1.36.1.1.3

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

Destination

This entry contains the destination of the check.

SNMP ID:

1.36.1.1.4

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

Pkt-Loss-Percent

This entry shows the number of lost data packets in percent.

SNMP ID:

1.36.1.1.5

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

RTT-Min

This entry shows the minimum round-trip time of the ICMP packets.

SNMP ID:

1.36.1.1.6

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

RTT-Max

This entry shows the maximum round-trip time of the ICMP packets.

SNMP ID:

1.36.1.1.7

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

RTT-Avg

This entry shows the average round-trip time of the ICMP packets.

SNMP ID:

1.36.1.1.8

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

Warning

This entry contains the number of reported warnings.

SNMP ID:

1.36.1.1.9

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

Critical

This entry contains the number of reported errors.

SNMP ID:

1.36.1.1.10

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **History-Log**

Last-Result

This entry contains the table with the results of the last check.

SNMP ID:

1.36.1.2

Telnet path:

Status > **SLA-Monitor** > **ICMP**

Name

Name of the ICMP configuration.

SNMP ID:

1.36.1.2.1

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

Destination

This entry contains the destination of the last check.

SNMP ID:

1.36.1.2.2

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

Timestamp

Exact time when the entry was created.

SNMP ID:

1.36.1.2.3

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

Pkt-Loss-Percent

This entry shows the number of lost data packets in percent.

SNMP ID:

1.36.1.2.4

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

RTT-Min

This entry shows the minimum round-trip time of the ICMP packets.

SNMP ID:

1.36.1.2.5

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

RTT-Max

This entry shows the maximum round-trip time of the ICMP packets.

SNMP ID:

1.36.1.2.6

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

RTT-Avg

This entry shows the average round-trip time of the ICMP packets.

SNMP ID:

1.36.1.2.7

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

Warning

This entry contains the number of reported warnings.

SNMP ID:

1.36.1.2.8

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

Critical

This entry contains the number of reported errors.

SNMP ID:

1.36.1.2.9

Telnet path:

Status > **SLA-Monitor** > **ICMP** > **Last-Result**

Delete-Values

This entry give you the option to delete all values.

SNMP ID:

1.36.1.3

Telnet path:

Status > **SLA-Monitor** > **ICMP**

7.4.5 Additions to the Setup menu

SLA monitor

This menu contains the settings for the SLA monitor.

SNMP ID:

2.45

Telnet path:

Setup

ICMP

This menu is used to configure the Internet Control Message Protocol (ICMP).

SNMP ID:

2.45.1

Telnet path:

Setup > **SLA-Monitor**

Name

Contains the name of the ICMP configuration.

SNMP ID:

2.45.1.1

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Active

This entry controls whether the ICMP profile is actually used.

SNMP ID:

2.45.1.2

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Yes
No

Default:

Yes

Destination

Set an IPv4 address to which the ICMP sends diagnostic and error messages.

SNMP ID:

2.45.1.3

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 40 characters from `[0-9].`

Default:

0.0.0.0

Rtg-Tag

Enter the routing tag for setting the route to the relevant remote gateway.

SNMP ID:

2.45.1.4

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Loopback address

The device sees this address as its own address, which is also available even if a physical interface is disabled, for example.

SNMP ID:

2.45.1.5

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 56 characters from `[0-9]`

Default:

empty

Interval

The interval in seconds in which the ICMP sends diagnostic or error messages to the specified destination.

SNMP ID:

2.45.1.6

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 6 characters from `[0-9]`

Default:

30

Start offset

Here you specify a startup delay for the ICMP transmissions in milliseconds.

SNMP ID:

2.45.1.7

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Count

Set the number of ICMP packets to be transmitted at the same time.

SNMP ID:

2.45.1.8

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 3 characters from `[0-9]`

Default:

5

Packet delay

Sets delay before the ICMP packets are transmitted. Delay in milliseconds.

SNMP ID:

2.45.1.9

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

1000

Packet size

Sets the packet size for ICMP messages. The value is set in bytes.

SNMP ID:

2.45.1.10

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 5 characters from `[0-9]`

Default:

56

Warn-Lvl-RTT-Max

Maximum allowable packet round-trip time before the SLA monitor emits a warning.

SNMP ID:

2.45.1.11

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

100

Crit-Lvl-RTT-Max

Maximum allowable packet round-trip time before the SLA monitor reports an error.

SNMP ID:

2.45.1.12

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

200

Warn-Lvl-RTT-Avg

Average packet round-trip time before the SLA monitor emits a warning.

SNMP ID:

2.45.1.13

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

80

Crit-Lvl-RTT-Avg

Average packet round-trip time before the SLA monitor reports an error.

SNMP ID:

2.45.1.14

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

170

Warn-Lvl-Pkt-Loss-Percent

Number of lost data packets in percent before a warning is issued.

SNMP ID:

2.45.1.15

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 3 characters from `[0-9]`

Default:

10

Crit-Lvl-Pkt-Loss-Percent

Number of lost data packets in percent before an error message is issued.

SNMP ID:

2.45.1.16

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 3 characters from `[0-9]`

Default:

20

IP-Version

Specifies the IP standard used for the Internet Control Message Protocol.

SNMP ID:

2.45.1.17

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Auto
IPv4
IPv6

Default:

Auto

Comment

Comment about this ICMP configuration.

SNMP ID:

2.45.1.19

Telnet path:

Setup > **SLA-Monitor** > **ICMP**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Event count

Number of events to be logged by the SLA monitor.

SNMP ID:

2.45.2

Telnet path:

Setup > **SLA-Monitor**

Possible values:

Max. 3 characters from `[0-9]`

Default:

100

Startup delay

Delay time in milliseconds before monitoring is started.

SNMP ID:

2.45.3

Telnet path:

Setup > **SLA-Monitor**

Possible values:

Max. 3 characters from `[0-9]`

Default:

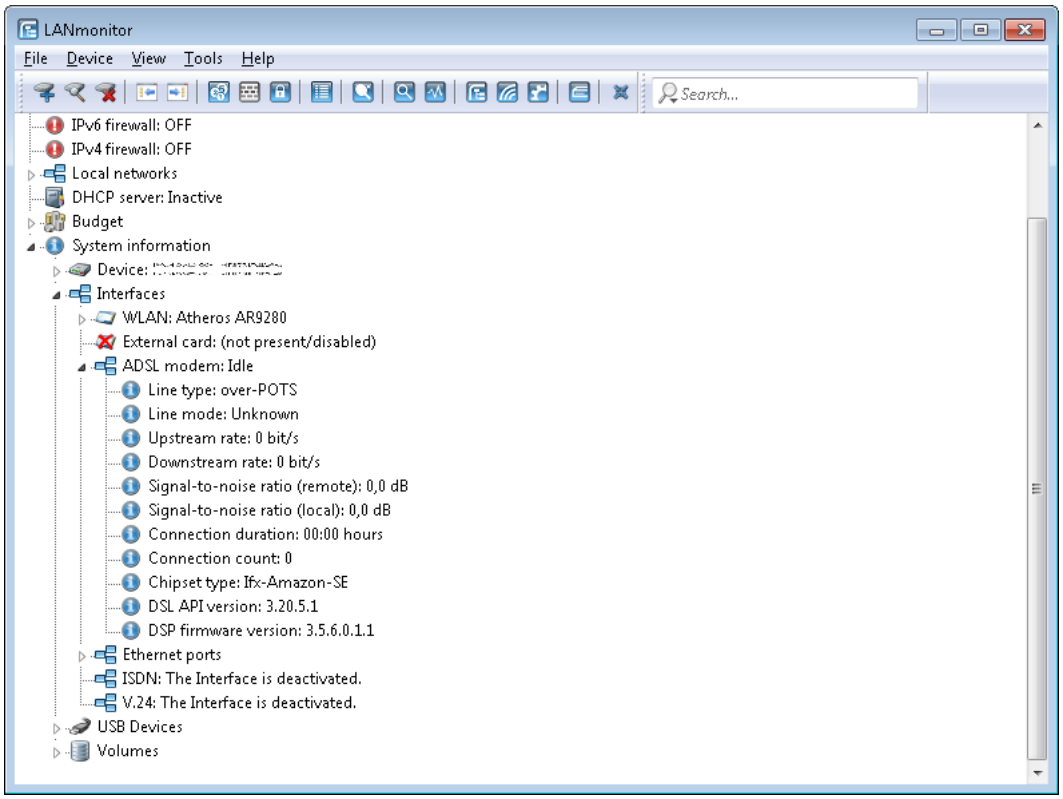
10

7.5 Additional DSL-modem status values

As of version 10.12, HiLCOS provides additional status values for DSL connections, i.e. the duration and number of connections.

7.5.1 Read out DSL modem status values with LANmonitor

LANmonitor can be used to read out the status values for each registered device with an ADSL/VDSL modem in the section **System information** > **Interfaces** > **ADSL modem: <Status>**.



7.5.2 Additions to the Status menu

Connection count

This entry contains the number of DSL connections since the last system reboot.

SNMP ID:

1.75.53

Telnet path:

Status > **VDSL**

Connection duration

This entry contains the duration of the DSL connection since the last synchronization.

SNMP ID:

1.75.54

Telnet path:

Status > **VDSL**

Connection count

This entry contains the number of DSL connections since the last system reboot.

SNMP ID:

1.75.25.53

Telnet path:

Status > **VDSL** > **Advanced**

Connection duration

This entry contains the duration of the DSL connection since the last synchronization.

SNMP ID:

1.75.25.54

Telnet path:

Status > **VDSL** > **Advanced**

7.6 Displaying the mobile/cellular standards

As of HiLCOS 10.12, LANconfig displays the names of mobile/cellular standards along with the corresponding generation numbers:

- GPRS: 2G
- GSM: 2G
- EDGE: 2.5G
- UMTS: 3G
- HSPA: 3.5G
- HSDPA: 3.5G
- HSUPA: 3.5G
- HSPA+: 3.5G
- LTE: 4G

7.6.1 Additions to the Setup menu

Mode

Select the mobile networking transmission mode here.

SNMP ID:

2.23.41.1.6

Telnet path:

Setup > **Interfaces** > **Mobile** > **Profiles**

Possible values:

Auto
Automatic selection of transmission mode

3G
UMTS operation only

2G
GPRS operation only

3G-2G
Combined UMTS-GPRS operation

4G
LTE operation only

4G-3G
Combined LTE-UMTS operation

4G-2G
Combined LTE-GPRS operation

Default:

Auto

7.6.2 Additions to the Status menu

Mode

This entry shows the mobile/cellular mode.

SNMP ID:

1.49.9.3

Telnet path:

Status > **Modem-Mobile** > **Network-List**

Possible values:

Unknown
2G
3G
4G

Mode

This entry contains the mobile/cellular mode.

SNMP ID:

1.49.12

Telnet path:

Status > **Modem-Mobile**

Possible values:

Unknown
UMTS(3G)
GPRS(2G)
GSM(2G)
EDGE(2.5G)
HSDPA(3.5G)
HSUPA(3.5G)
HSPA+(3.5G)
LTE(4G)
HSPA(3.5G)

Default:

Unknown

Mode

This entry contains the status values for Mode.

SNMP ID:

1.49.16.5

Telnet path:

Status > **Modem-Mobile** > **History**

Possible values:

Unknown
UMTS(3G)
GPRS(2G)
GSM(2G)
EDGE(2.5G)
HSDPA(3.5G)
HSUPA(3.5G)
HSPA+(3.5G)
LTE(4G)
HSPA(3.5G)

Default:

Unknown

AcT

This entry contains the status values for AcT.

SNMP ID:

1.49.47.5

Telnet path:

Status > **Modem-Mobile** > **Network-List**

Possible values:

Unknown
2G
3G
4G

7.7 Editable VLAN assignment per Internet service provider

Specify the VLANs that should be checked, along with VLAN 0, by entering additional VLAN IDs per Internet service provider. Some Internet service providers use specific VLANs for specific Internet connections, and these need to be configured in the device. This setting facilitates the detection of the Internet service provider and the assignment of the appropriate VLAN. As a basis for this check, HiLCOS identifies the Internet service provider by means of the user name stored in the PPP list under **Communication** > **Protocols**.

7.7.1 Additions to the Setup menu

VLANs

This menu contains the editable configuration of VLAN assignments for different Internet service providers.

SNMP ID:

2.2.60

Telnet path:

Setup > **WAN**

Provider list

This table contains the Internet service providers for whom VLANs should be checked in addition to VLAN 0. For this check, HiLCOS uses the "User name" entry in the PPP list under **Communication** > **Protocols**.

SNMP ID:

2.2.60.1

Telnet path:

Setup > **WAN** > **VLANs**

Providers

Here you enter the user name specified under **Communication** > **Protocols** > **PPP list** in order to identify Internet service providers that require the checking of additional VLANs.

"*" is defined as a wild card for this field so that, for example, entering "`*@t-online.de`" causes the setting to be applied to all PPP list entries that end with @t-online.de.

SNMP ID:

2.2.60.1.1

Telnet path:

Setup > **WAN** > **VLANs** > **Provider-List**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

VLAN-IDs

Here you specify the VLANs that are to be checked in addition to VLAN 0. The checking of additional VLANs only takes place if the entry under *Provider* matches the user name in the PPP list.

You have the option of specifying a single VLAN or multiple comma-separated VLANs.

SNMP ID:

2.2.60.1.2

Telnet path:

Setup > **WAN** > **VLANs** > **Provider-List**

Possible values:

Max. 64 characters from `[0-9]-,`

Default:

empty

7.8 Manually configuring VDSL/ADSL bandwidth

As of HiLCOS 10.12, the bandwidth for devices with an integrated ADSL/VDSL modem can be set manually at the interface.

7.8.1 Configuring bandwidth with LANconfig

To configure the upstream and downstream transmission speeds in LANconfig, navigate to **Interfaces** > **WAN** and click the **Interface settings** button.

VDSL and ADSL interfaces

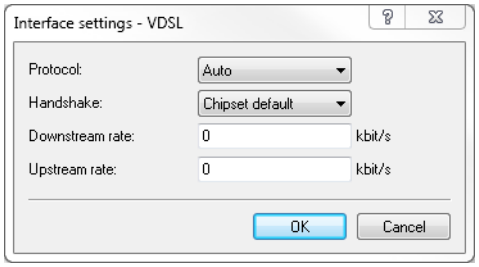
In order for Quality of Service to function properly, you need to know the actual bandwidth of the WAN connection. Sometimes, the bandwidth negotiated by the DSL modem may not agree with the actual data transfer rate. In this case, it is necessary to manually correct the speed of DSL connection to the actual value.

This only applies to devices with an integrated ADSL/VDSL modem.

Example:

The bandwidth negotiated during the DSL synchronization is 100 Mbps. In fact, the actual available bandwidth is a transmission speed of just 50 Mbps.

Settings for devices with an integrated VDSL modem



Protocol

Select the protocol used by your DSL connection. Your Internet provider will be able to provide this information.

The following options are available:

Automatic

Automatic selection of the operating mode

VDSL2 (G.993.2)

Operating mode VDSL2 for transmission rates of up to 100 Mbps upstream and downstream.

ADSL

Operating mode ADSL with up to 8 Mbps downstream and 0.6 Mbps upstream

ADSL2+ (G.992.5)

Operating mode ADSL2+ with up to 24 Mbps downstream and 1 Mbps upstream

ADSL2 (G.992.3)

Operating mode ADSL2 with up to 12 Mbps downstream and 1.2 Mbps upstream

ADSL1 (G.992.1/G.DMT)

Operating mode ADSL (G.DMT) with up to 8 Mbps downstream and 1 Mbps upstream

ADSL2+ (Annex J)

Operating mode All Digital ADSL2+ with up to 24 Mbps downstream and 3.5 Mbps upstream

ADSL2 (Annex J)

Operating mode All Digital Mode ADSL2+ with up to 12 Mbps downstream and 3.5 Mbps upstream

Off

The interface is not active.

Handshake

Select from the following handshake methods for this interface:

Chipset-default

The handshake is carried out according to the default for the chipset in the device.

V43 if needed

The V43 carrier set is used for the handshake if required.

V43 enabled

The carrier set V43 is enabled for the handshake.

V43 disabled

The carrier set V43 is disabled for the handshake.

Downstream rate

Specify the downstream rate (RX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

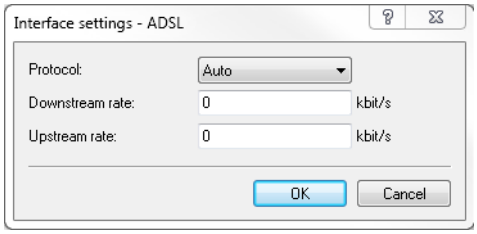
If the default value is "0", the value used is negotiated automatically.

Upstream rate

Specify the upstream rate (TX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is "0", the value used is negotiated automatically.

Settings for devices with an integrated ADSL modem



Protocol

Select the protocol used by your DSL connection. Your Internet provider will be able to provide this information.

The following options are available:

Automatic

Automatic selection of the operating mode

ADSL1 (autom. Annex A/B)

Operating mode ADSL over POTS/ISDN for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (autom. Annex A/B)

Operating mode ADSL2 over POTS/ISDN for transmission rates up to 12 Mbps downstream and 1 Mbps upstream.

ADSL2+ (autom. Annex A/B)

Operating mode ADSL2+ over POTS/ISDN for transmission rates up to 24 Mbps downstream and 1 Mbps upstream.

Auto-POTS (autom. Annex A/I/L/M)

Operating mode ADSL over POTS for transmission rates from 10 to 24 Mbps downstream and up to 3.5 Mbps upstream.

ADSL1 (Annex A)

Operating mode ADSL over POTS for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex A)

Operating mode ADSL2 over POTS with up to 12 Mbps downstream and 1 Mbps upstream

ADSL2+ (Annex A)

Operating mode ADSL2+ over POTS with up to 24 Mbps downstream and 1 Mbps upstream

ADSL2 (Annex I)

Operating mode All Digital Mode ADSL2+ with up to 12 Mbps downstream and 3.2 Mbps upstream

ADSL2+ (Annex I)

Operating mode All Digital ADSL2+ with up to 24 Mbps downstream and 3.2 Mbps upstream

ADSL2 (Annex L)

Operating mode RE-ADSL2 with up to 6 Mbps downstream and 1.2 Mbps upstream

ADSL2 (Annex M)

Operating mode ADSL2 with up to 24 Mbps downstream and 3.5 Mbps upstream

ADSL2+ (Annex M)

Operating mode ADSL2+ with up to 24 Mbps downstream and 3.7 Mbps upstream

Auto-ISDN (autom. Annex B/J)

Operating mode ADSL over ISDN for transmission rates from 10 to 24 Mbps downstream and up to 3.5 Mbps upstream.

ADSL1 (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 10 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 12 Mbps downstream and 1 Mbps upstream.

ADSL2+ (Annex B)

Operating mode ADSL over ISDN for transmission rates up to 24 Mbps downstream and 1 Mbps upstream.

ADSL2 (Annex J)

Operating mode ADSL over ISDN for transmission rates up to 12 Mbps downstream and 3.5 Mbps upstream.

ADSL2+ (Annex J)

Operating mode ADSL over ISDN for transmission rates up to 24 Mbps downstream and 3.5 Mbps upstream.

Off

The interface is not active.

Downstream rate

Specify the downstream rate (RX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is "0", the value used is negotiated automatically.

Upstream rate

Specify the upstream rate (TX). The actual bandwidth corresponds to the minimum of the negotiated value and the value set here.

If the default value is "0", the value used is negotiated automatically.

7.8.2 Additions to the Setup menu

Upstream rate

This item allows you to set the gross upstream rate for this port. The data rate entered here (kbps) limits the outgoing data streams from the device.

SNMP ID:

2.23.6.16

Telnet path:

Setup > **Interfaces** > **ADSL-Interface**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Special values:

0

The value used is negotiated automatically.

Downstream rate

The downstream rate is measured in kilobits and includes everything arriving at the router over the WAN interface. For example, on a connection with guaranteed 768 kbps downstream, the upstream rate negotiated by the modem is 864 kbps. This still includes an overhead typical for this type of connection, which results from the modem using ATM as the transport protocol. If we adjust the 864 kbps to allow for the overhead that results from the structure of an ATM cell (48 bytes of payload for a cell length of 53 bytes), we arrive at 864 * 48/53 = 792 kbps gross downstream rate, which is transferred from the modem to the router over Ethernet. If data rates negotiated by the modem are unknown, it is possible to multiply the guaranteed data rates by 56/55 to approximate the gross data rates.

SNMP ID:

2.23.6.18

Telnet path:

Setup > **Interfaces** > **ADSL-Interface**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Special values:

0

The value used is negotiated automatically.

Upstream rate

This item allows you to set the gross upstream rate for this port. The data rate entered here (kbps) limits the outgoing data streams from the device.

SNMP ID:

2.23.8.16

Telnet path:

Setup > **Interfaces** > **VDSL**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Special values:

0

The value used is negotiated automatically.

Downstream rate

The downstream rate is measured in kilobits and includes everything arriving at the router over the WAN interface. For example, on a connection with guaranteed 768 kbps downstream, the upstream rate negotiated by the modem is 864 kbps. This still includes an overhead typical for this type of connection, which results from the modem using ATM as the transport protocol. If we adjust the 864 kbps to allow for the overhead that results from the structure of an ATM cell (48 bytes of payload for a cell length of 53 bytes), we arrive at 864 * 48/53 = 792 kbps gross downstream rate, which is transferred from the modem to the router over Ethernet. If data rates negotiated by the modem are unknown, it is possible to multiply the guaranteed data rates by 56/55 to approximate the gross data rates.

SNMP ID:

2.23.8.18

Telnet path:

Setup > **Interfaces** > **VDSL**

Possible values:

Max. 6 characters from `[0-9]`

Default:

0

Special values:

0

The value used is negotiated automatically.

7.9 The Bonjour proxy

As of version 10.12, HiLCOS provides a Bonjour proxy.

Apple Bonjour allows devices to discover and operate certain approved services automatically and without prior configuration. This procedure is also known as "Zero Configuration Networking" (ZeroConf).

The most popular services include, among others:

- Printer services (with or without Apple Airprint support)
- File services (folder or file shares)
- Apple Airplay
- iTunes

7.9.1 Bonjour basics

Bonjour exchanges information by means of individual multicast DNS packets (mDNS) according to *RFC 6762* and DNS-based service discovery (DNS-SD) according to *RFC 6763*. The clients exchange Bonjour information via the multicast address `224.0.0.251` (IPv4) or `ff02::fb` (IPv6) on port 5353. Bonjour packets are not routed (multicast packet, TTL = 1), which limits their use to the current local area network.

Please note that the Bonjour proxy only serves to aid the discovery of Bonjour services. The actual routing between the communicating parties requires a separate configuration or restriction by means of, for example, routing or firewall entries.

It is often impractical to provide all services on a single network. This is why larger networks are often divided into several subnets. However, Bonjour is unable to operate in this situation.

Example application with two networks

At a school, students use a dedicated IP network to access the WLAN. In parallel to this, the local printer is made available on a second internal IP network. In principal, the appropriate routing and restrictions would make it possible for students to use their smartphones to access the local internal printer. However, because mDNS is only defined as link-local, Bonjour is unable to help students to discover the printer with their smartphones. The Hirschmann Bonjour proxy mediates between two networks, which enables students to discover printers in other networks.

Basically, there are two ways of realizing such a scenario:

Multicast routing

A router forwards the search queries and service advertisements between the two networks.

This option causes unnecessary traffic, which makes it rather inefficient.

Caching of services

The router stores discovered mDNS service advertisements in its local cache. A router that receives an mDNS query then responds on behalf of the original service. Before processing the advertisement and before transmitting anything from the cache, the router checks its policies to see whether the service is approved or blocked. The policies are used to control which services are approved for discovery and between which networks.

Please note that reading out the mDNS cache content with the SNMP protocol is not supported.

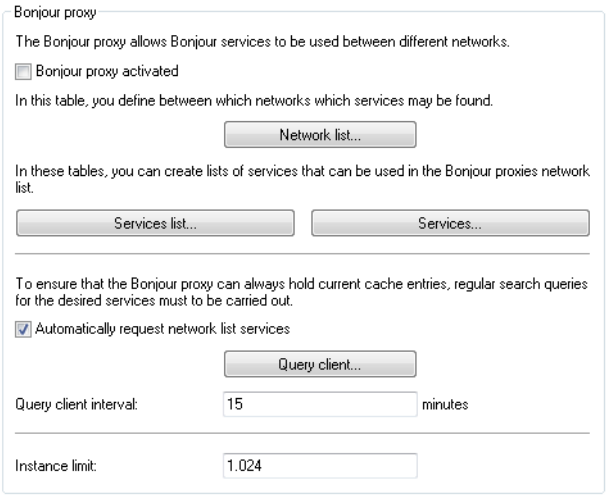
The Bonjour proxy supports an mDNS query client, which at set time intervals queries an interface about the services of interest. This query keeps the cache entries for approved services up to date. In order for the cache to be up-to-date at all times, it is useful to enable automatic searches for services that are permanently available (e.g. print services).

If no automatic queries about frequently used services are configured, the Bonjour proxy may be unable to respond to the corresponding queries even though the services are approved.

Bonjour proxies only operate on logical LAN / WLAN interfaces or on logical networks with an IP address. WAN interfaces / remote stations or tunnels (except for WLC L3 tunnels) and VLANs without address binding are not supported.

7.9.2 Configuration with LANconfig

The Bonjour proxy is configured with LANconfig under **IP router** > **Bonjour**.



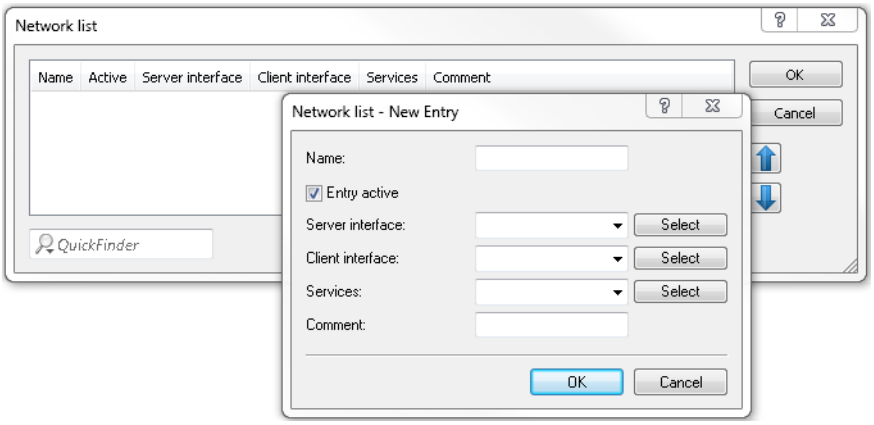
The following settings are available:

Bonjour proxy activated

Use this checkbox to enable or disable the Bonjour proxy.

Network list

Use this table to specify the networks between which Bonjour services may be discovered. To function properly, the networks or interfaces need to be configured with an IPv4 or IPv6 address. This table offers you the following options:



Name

Specify a unique name for this table entry.

Entry active

Enable or disable this table entry.

Server interface

Set the name of the IPv4 network or IPv6 interface that is used to provide the Bonjour services (e.g. print services).

Client interface

IPv4 network name or IPv6 interface name to be used for Bonjour clients to discover services on the server network

Services

This references an entry in the list of services. Clients are only able to find services contained in this list. Non-listed services are rejected.

If this box is left empty, all services are allowed.

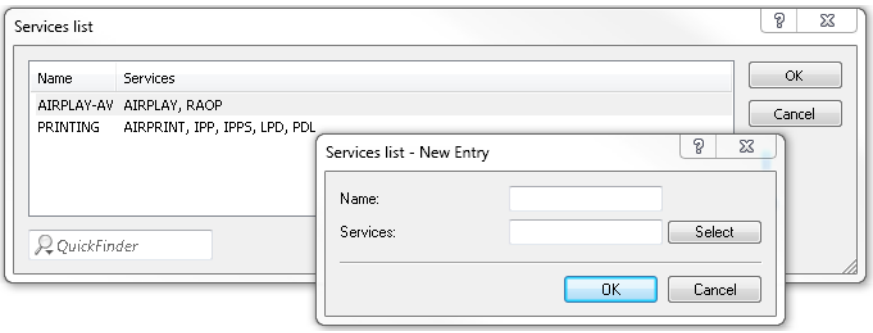
Comment

Enter a comment about this table entry.

Services list

In this table, create a list of Bonjour service types that are available for use in the Bonjour network list.

The following settings are available:



Name

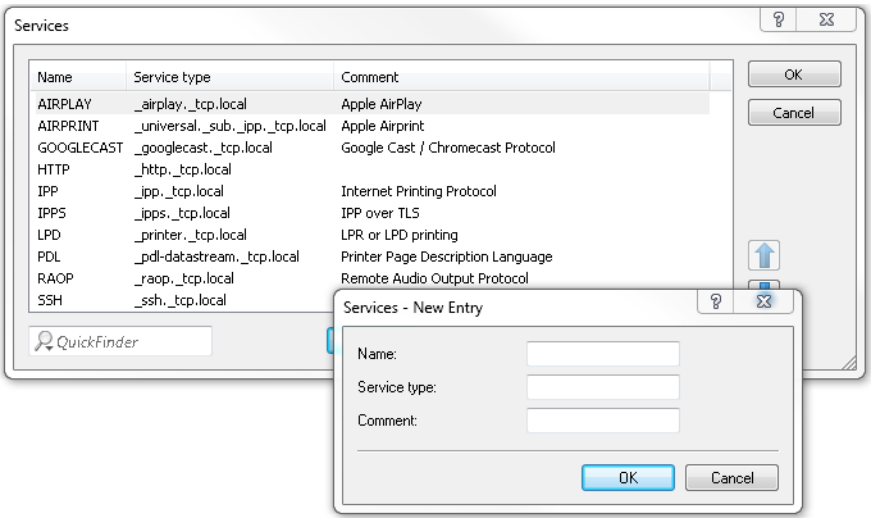
Specify a unique name for this table entry.

Services

Enter a comma-separated list of services that are to be available for use in the **Services** table.

Services

This table is used to specify the Bonjour service types that can be used in the services list. Additional settings are available as follows:



Name

Specify a unique name for this table entry.

Service type

Specify the Bonjour service type as a DNS SRV record, e.g. with `_http._tcp.local`.

Comment

Enter a comment about this table entry.

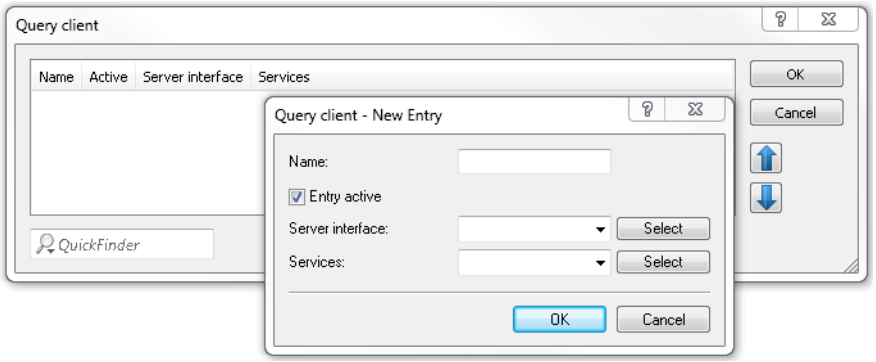
Automatically request network list services

With this item enabled, the device sends regular queries about which services (as specified in the network list) are available from the corresponding server interface. This option is enabled by default. This setting is also recommended.

If this setting is disabled, you need to manually enter the services to be queried into the **Query client** table.

Query client

To keep the Bonjour proxy services cache up-to-date all times, you need to configure regular queries about the desired services. The query client regularly contacts the configured service types for information about their availability.



Name

Specify a unique name for the corresponding entry.

Entry active

Activates or deactivates this table entry.

Server interface

Set an IPv4 network name or an IPv6 interface name that is to offer the Bonjour services (e.g. print services) and which will regularly be used by the router to make the queries.

Services

This references an entry in the list of services. These services are regularly queried by the router at the server interface. This entry may not be empty.

Query client interval

Set the interval in minutes in which the query client updates the Bonjour services configured in the **Query client** table. 15 minutes are defined by default.

Instance limit

Specify the maximum number of service instances that the Bonjour proxy stores at the same time.

7.9.3 Additions to the Setup menu

Bonjour proxy

This menu contains the settings for the Bonjour proxy. The Bonjour proxy allows Bonjour services to be discovered across network boundaries.

SNMP ID:

2.104

Telnet path:

Setup

Operating

This entry is used to enable or disable the Bonjour proxy.

SNMP ID:

2.104.1

Telnet path:

Setup > **Bonjour-Proxy**

Possible values:

No
Yes

Default:

No

Query client interval

Set the interval in minutes in which the query client requests the Bonjour services configured in the **Query client** table.

SNMP ID:

2.104.2

Telnet path:

Setup > **Bonjour-Proxy**

Possible values:

0 … 999 Minutes

Default:

15

Special values:

0

Network list

Use this table to specify the networks between which Bonjour services may be discovered.

SNMP ID:

2.104.3

Telnet path:

Setup > **Bonjour-Proxy**

Name

Specify a unique name for this table entry.

SNMP ID:

2.104.3.1

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Active

This entry is used to enable or disable the Bonjour proxy for the corresponding combination of client and server network.

SNMP ID:

2.104.3.2

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

No
Yes

Default:

No

Server interface

Set the name of the IPv4 network or IPv6 interface that is used to provide the Bonjour services (e.g. print services).

SNMP ID:

2.104.3.3

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Client interface

IPv4 network name or IPv6 interface name to be used for Bonjour clients to discover services on the server network

SNMP ID:

2.104.3.4

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Services

This references an entry in the list of services. Clients are only able to find services contained in this list. Non-listed services are rejected.

If this box is left empty, all services are allowed.

SNMP ID:

2.104.3.5

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Comment

Enter a comment about this entry.

SNMP ID:

2.104.3.6

Telnet path:

Setup > **Bonjour-Proxy** > **Network-List**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Service list

In this table, create a list of Bonjour service types that are available for use in the Bonjour network list.

SNMP ID:

2.104.4

Telnet path:

Setup > **Bonjour-Proxy**

Name

Enter a name for this list here.

SNMP ID:

2.104.4.1

Telnet path:

Setup > **Bonjour-Proxy** > **Service-List**

Possible values:

Max. 36 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Services

This table is used to specify the Bonjour service types that can be used in the services list.

Specify multiple services with a comma-separated list.

SNMP ID:

2.104.4.2

Telnet path:

Setup > **Bonjour-Proxy** > **Service-List**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Services

This table lists the default services for communicating between networks. You can extend the table according to your needs.

SNMP ID:

2.104.5

Telnet path:

Setup > **Bonjour-Proxy**

Name

Enter the service name here (e.g. "HTTP").

SNMP ID:

2.104.5.1

Telnet path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Service type

Specify the service type here (e.g. `_http._tcp.local`).

SNMP ID:

2.104.5.2

Telnet path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Comment

Enter a comment about this service.

SNMP ID:

2.104.5.6

Telnet path:

Setup > **Bonjour-Proxy** > **Services**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Query client

The table lists the services that should be requested by the router at regular intervals.

SNMP ID:

2.104.6

Telnet path:

Setup > **Bonjour-Proxy**

Name

Specify a unique name for the corresponding entry.

SNMP ID:

2.104.6.1

Telnet path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Active

Enable or disable this entry.

SNMP ID:

2.104.6.2

Telnet path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

No
Yes

Default:

No

Server interface

Here you specify the server interface to be used for the client query.

SNMP ID:

2.104.6.3

Telnet path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Services

Here you specify which services should be requested.

SNMP ID:

2.104.6.4

Telnet path:

Setup > **Bonjour-Proxy** > **Query-Client**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Instance limit

Specify the maximum number of service instances that the Bonjour proxy stores at the same time.

SNMP ID:

2.104.7

Telnet path:

Setup > **Bonjour-Proxy**

Possible values:

0 … 4294967295

Default:

1024

Auto-query services

Activate the checkbox if the Query Client should periodically query the configured service types for their availability.

SNMP ID:

2.104.8

Telnet path:

Setup > **Bonjour-Proxy**

Possible values:

No
Yes

Default:

Yes

7.9.4 Additions to the Status menu

Bonjour proxy

This menu contains the current values of the Bonjour proxy.

SNMP ID:

1.104

Telnet path:

Status

Instance count

This value shows the current number of cached instances of the service.

SNMP ID:

1.104.1

Telnet path:

Status > **Bonjour-Proxy**

MDNS cache

This table contains the cache information of the multicast domain name system (mDNS).

SNMP ID:

1.104.2

Telnet path:

Status > **Bonjour-Proxy**

Service propagation

This table contains information about the propagated services.

SNMP ID:

1.104.3

Telnet path:

Status > **Bonjour-Proxy**

Clear cache

This command clears the current mDNS cache content.

SNMP ID:

1.104.4

Telnet path:

Status > **Bonjour-Proxy**

7.10 OSPF

As of version 10.12, HiLCOS features OSPF.

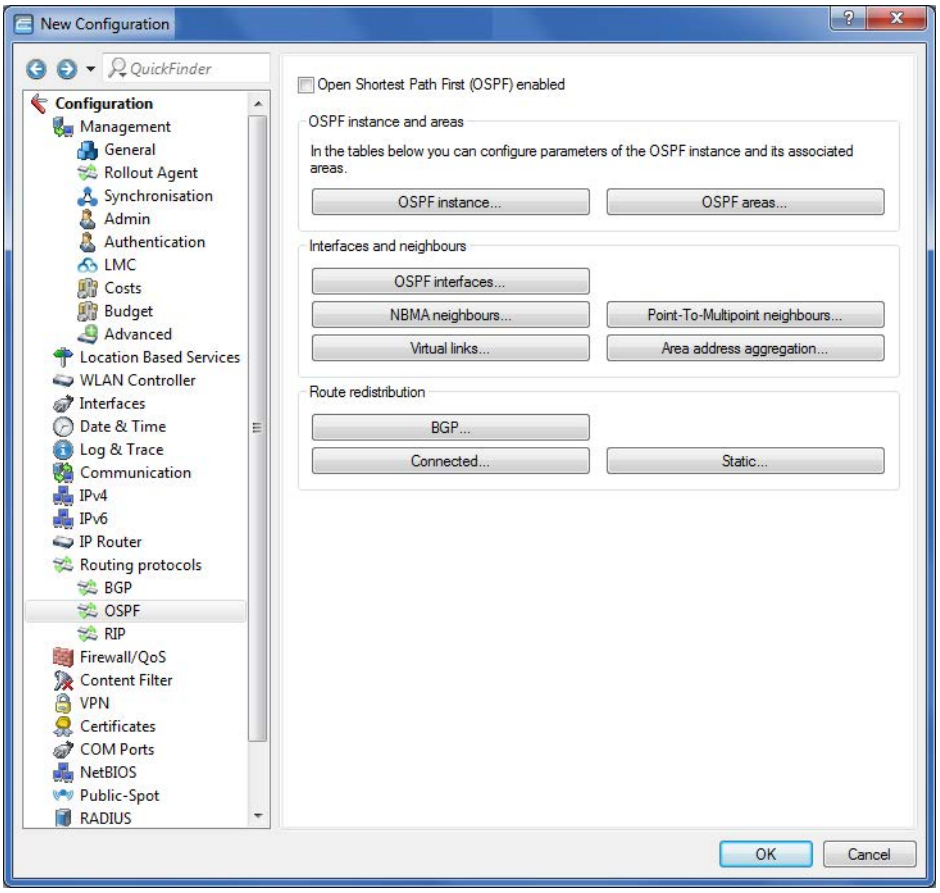
Open Shortest Path First (OSPF) is a link-state routing protocol as per RFC 2328. It belongs to the category **Interior Gateway Protocols** (IGP). This involves routers regularly exchanging link-status information via link-state advertisements (LSA). The routers use multicast to automatically discover one another on the local network. OSPF is generally used for the exchange of internal routing information in large networks (LANs).

Each router has an identical copy of the database (link state database, LSDB), which routers use to determine the best routes (Shortest Path First, SPF) using the Dijkstra algorithm.

In contrast, BGP is one of the **Exterior Gateway Protocols** (EGP) and is typically used to route between autonomous systems or within VPNs.

7.10.1 Setting up OSPF with LANconfig

In order to configure OSPF with LANconfig, navigate to the **Routing protocols** > **OSPF** menu.



Open Shortest Path First (OSPF) enabled

To activate the OSPF function, set a check mark for **Open Shortest Path First (OSPF) enabled**.

OSPF instance

The table **OSPF instance** defines the OSPF instances on this device. It is possible for a device to operate multiple OSPF instances in parallel. Each instance corresponds to an autonomous system or an OSPF domain.

OSPF areas

The table **OSPF areas** is used to define the parameters of the OSPF areas.

OSPF interfaces

This table specifies the interfaces on which OSPF is to operate.

NBMA neighbors

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. A default router is selected for this network type.

The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.

Point-to-multipoint neighbors

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network. If no default router is selected, multicast is used for communications instead.

Virtual links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.

Area address aggregation

In order to reduce the number of entries in the routing tables, IP addresses can be grouped by address aggregation at area borders that transition from non-backbone areas to the backbone area. The corresponding subnet is advertised as a summary LSA.

BGP

Routes learned dynamically from BGP sources or protocols can be distributed by OSPF.

Connected

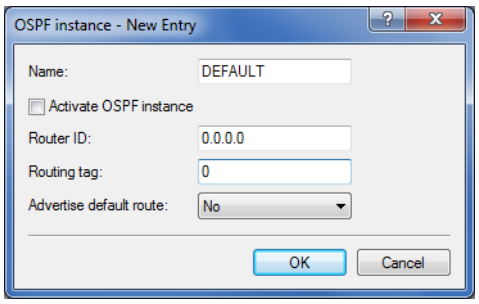
Connected routes, i.e. routes that the operating system automatically enters into the routing table, can be redistributed by OSPF.

Static

Static routes, i.e. routes that the user manually enters into the routing table, can be redistributed by OSPF.

OSPF instance

You configure the OSPF instance of the device under **OSPF instance**.



Name

Contains the name of the OSPF instance.

Activate OSPF instance

Activates or deactivates this OSPF instance.

Router ID

Contains the 32-bit router ID (represented as an IPv4 address) of this particular OSPF instance. The router ID uniquely identifies this router within an OSPF domain.

Routing tag

Contains the routing tag assigned to this instance.

Advertise default route

Specifies whether this router should advertise or propagate the default route in this instance.

Possible values:

No (Default)

The router does not advertise a default route.

Yes

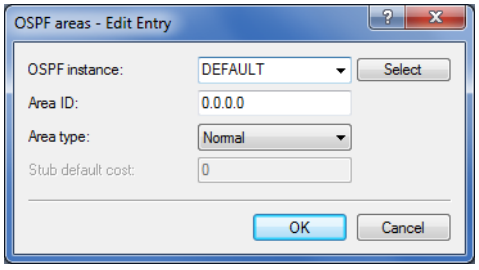
The router always advertises the default route, regardless of whether the default route exists in its routing table.

Dynamic

The router only advertises the default route if this is also available in its routing table.

OSPF areas

The parameters for the OSPF area are configured under **OSPF areas ...**.



OSPF instance

Contains the name of the OSPF instance.

Area ID

The area ID (displayed as an IPv4 address) identifies the area.

If this instance is to be the backbone area, the value to be used is 0.0.0.0.

Area type

Specifies the type of the area.

Possible values:

Normal (default)

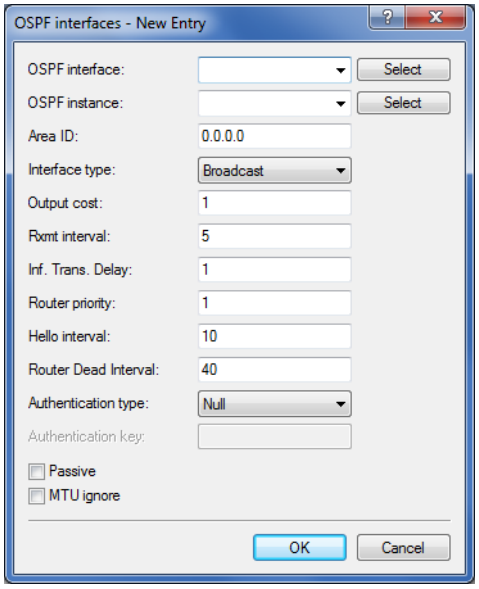
Stub

Stub default cost

If the area is configured as a stub area and the router itself is an area border router, the parameter **Stub default cost** indicates the cost of the default summary LSA that this router should advertise in this area.

OSPF interfaces

Defines the interfaces on which OSPF should be operated.



OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

OSPF instance

Contains the name of the OSPF instance.

Area ID

Identifies the area by means of an IPv4 address.

Port type

Defines the interface type.

Possible values:

Broadcast

Ethernet-based network; a default router is selected and multicast is used for communication.

Point-to-point

Network consisting of two routers only (e.g. GRE tunnel) or Ethernet via P2P link; no default router is selected and multicast is used for communication.

Point-to-multipoint

Network as hub-and-spoke topology; a default router is selected and multicast is used for communication.

Non-Broadcast Multi-Access (NBMA)

Point-to-multipoint networks that do not support broadcast or multicast; a default router is selected and unicast is used for communication; the neighbors are configured manually.

Output cost

Specifies the cost to send a packet on this interface, shown in the link-state metric. The advertisement is implemented in router LSA messages as a link cost for this interface.

The value must always be greater than zero.

Retransmit interval

Contains the number of seconds between retransmissions.

Transmit delay

Contains the estimated number of seconds required to transfer a link-state update packet over this interface.

Router priority

Defines the priority of this router on this interface when set as the designated router (DR). The router with the highest priority is set as the default router.

The value 0 prevents the router from becoming default router on this interface.

Hello interval

Contains the interval in seconds in which the router sends Hello packets from this interface.

Router Dead Interval

Specifies the elapsed time in seconds during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

This value must be greater than the Hello interval.

Authentication type

Contains the authentication method to use for this interface.

Possible values:

Null

Simple password

Cryptographic MD5

Authentication key

Contains the authentication key for this network.

In this case the authentication type **Null** may not be selected.

Passive

Defines whether OSPF should work actively or passively on this interface.

Possible values:

Yes

No routing updates or hello packets are sent from this router on this interface. Similarly, no incoming OSPF messages are processed either. However, the corresponding route or network of this interface is still inserted into the LSDB and so is advertised on other interfaces.

No (Default)

MTU ignore

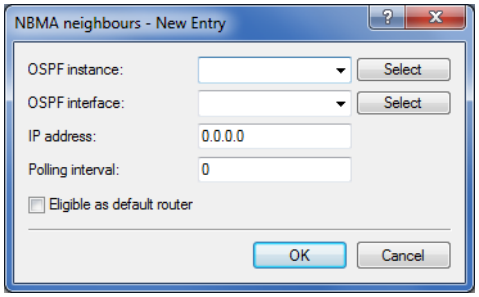
Disables the MTU value check in database description packets.

This allows routers to establish a full neighbor relationship even if the MTU of the corresponding interfaces is not uniform.

NBMA neighbors

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. Initially, a default router is selected for this purpose.

The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.



OSPF instance

Contains the name of the OSPF instance.

OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

IP address

Contains the IPv4 address of the neighboring router (router at the remote end).

Polling interval

Contains the interval in which Hello messages are sent to this router.

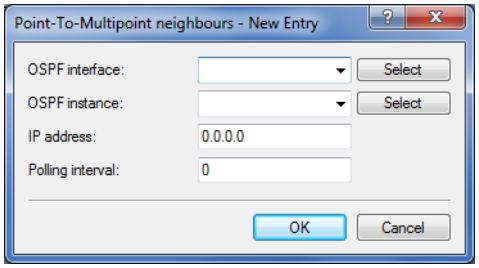
The value zero disables the transmission of Hello messages.

Eligible as default router

Specifies whether the local device itself is selectable as default router.

Point-to-multipoint neighbors

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network. No default router is selected and multicast is used for communications.



OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

OSPF instance

Contains the name of the OSPF instance.

IP address

Contains the IPv4 address of the neighboring router (router at the remote end).

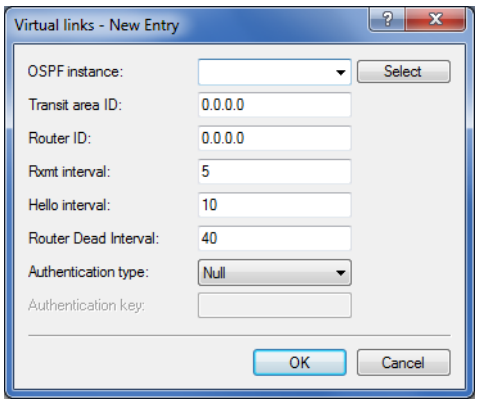
Polling interval

Contains the interval in which Hello messages are sent to this router.

The value zero disables the transmission of Hello messages.

Virtual links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.



OSPF instance

Contains the name of the OSPF instance.

Transit area ID

Contains the area ID, defined as an IPv4 address.

Router ID

Contains the router ID of the router at the remote end of the virtual link as an IPv4 address.

Retransmit interval

Contains the number of seconds between retransmissions.

Hello interval

Specifies the interval in seconds that the router sends Hello packets from this interface.

Router Dead Interval

Specifies the elapsed time in seconds during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

This value must be greater than the Hello interval.

Authentication type

Contains the authentication method to use for this interface.

Possible values:

Null

Simple password

Cryptographic MD5

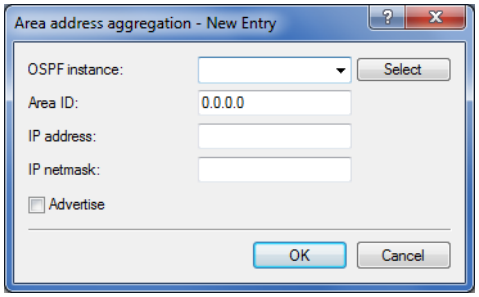
Authentication key

Contains the authentication key for this network.

In this case the authentication type **Null** may not be selected.

Area address aggregation

In order to reduce the number of entries in the routing tables, IP addresses can be grouped by address aggregation at area borders that transition from non-backbone areas to the backbone area. The corresponding subnet is advertised as a summary LSA.



OSPF instance

Contains the name of the OSPF instance.

Area ID

Identifies the area by means of an IPv4 address.

If this instance is to be the backbone area, the value to be used is 0.0.0.0.

IP address

Contains the IPv4 address.

IP netmask

Contains the IPv4 subnet mask.

Advertise

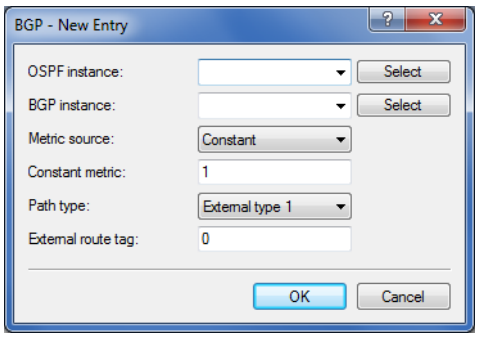
Enables or disables the advertisement of this address aggregation.

Route redistribution

Routes can be redistributed from other route sources or protocols by means of OSPF. For this purpose, routes of the corresponding type are read out from the routing table and redistributed by OSPF.

BGP

The distribution of routes learned dynamically from the Border Gateway Protocol is configured under **BGP**.



OSPF instance

Contains the name of the OSPF instance.

BGP instance

Contains the name of the BGP instance.

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The "Local preference" value of the BGP prefix is used or imported.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.

In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

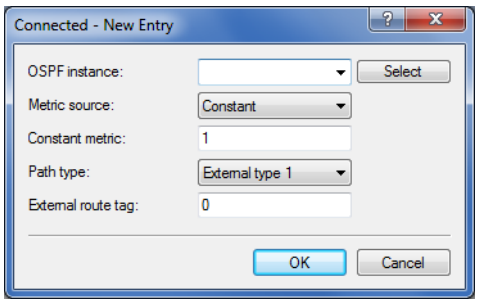
External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

Connected

The redistribution of routes that are automatically set by the operating system is configured under **Static**.



OSPF instance

Contains the name of the OSPF instance.

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The value is set automatically.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.

In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

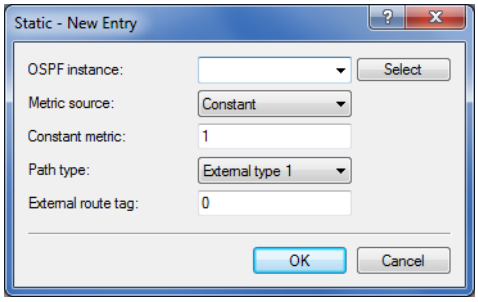
External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

Static

The redistribution of static routes, i.e. routes that the user manually enters into the routing table, is configured under **Static**.



OSPF instance

Contains the name of the OSPF instance.

Metric source

Specifies which source is used to set the OSPF metric.

Possible values:

Constant

A user-defined constant metric is used.

Protocol

The value is set automatically.

Constant metric

If the metric source is set to "Constant", the OSPF metric of the imported routes is set to the value Constant metric.

Path type

Specifies the type assigned to the routes imported into OSPF.

Possible values:

External type 1

The OSPF metric is formed from the redistribution metric or constant metric + the total path metric used to reach this ASBR.

In the OSPF routing algorithm of routers, type 1 routes are generally preferred over type 2 routes.

External type 2

The OSPF metric is formed from the redistribution metric and/or the constant metric.

External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

7.10.2 Show commands via CLI

The the available show commands are listed in the following:

- **show ospf-config**

  Displays a summary of the configured OSPF instances.

- **show ospf-database**

  Displays the OSPF database.

- **show ospf-graph**

  Displays the OSPF areas as a graphical representation in Graphviz format.

- **show ospf-neighbor**

  Displays information about OSPF neighbors.

- **show ospf-rib**

  Displays information about the OSPF Routing Information Base.

7.10.3 Additions to the Setup menu

OSPF

This directory enables you to configure the device for the Open Shortest Path First protocol.

SNMP ID:

2.93.3.

Telnet path:

Setup > **Routing-Protocols**

OSPF instance

This table is used to configure the OSPF instances.

SNMP ID:

2.93.3.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

Name

This parameter contains the name of the OSPF instance.

SNMP ID:

2.93.3.1.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Activate OSPF instance

Activates or deactivates this OSPF instance

SNMP ID:

2.93.3.1.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

0

Disabled

1

Activated

Default:

0

Router ID

The 32-bit router ID of this particular OSPF instance. The router ID uniquely identifies this router within an OSPF domain.

SNMP ID:

2.93.3.1.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

Routing tag

Contains the routing tag assigned to this instance.

SNMP ID:

2.93.3.1.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

0 … 65535

Advertise default route

Specifies whether this router should advertise or propagate the default route in this instance.

SNMP ID:

2.93.3.1.5

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Instance**

Possible values:

No

The router does not advertise a default route.

Yes

The router always advertises the default route, regardless of whether the default route exists in its routing table.

Dynamic

The router only advertises the default route if this is also available in its routing table.

Default:

No

OSPF areas

This table is used to configure the OSPF areas.

SNMP ID:

2.93.3.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF instance

This parameter contains the name of the OSPF instance.

SNMP ID:

2.93.3.2.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Area ID

The area ID (displayed as an IPv4 address) identifies the area.

SNMP ID:

2.93.3.2.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

Possible values:

IPv4 address `[0-9.]`

Special values:

0.0.0.0

Designates this instance as the backbone area.

Area type

This parameter describes the type of the area.

SNMP ID:

2.93.3.2.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

Possible values:

Normal
Stub

Default:

Normal

Stub default cost

If the area is configured as a stub area and the router itself is an area border router, the parameter **Stub default cost** indicates the cost of the default summary LSA that this router should advertise in this area.

SNMP ID:

2.93.3.2.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Areas**

Possible values:

0 … 4294967295

Area address aggregation

This table is used to configure the area address aggregation.

SNMP ID:

2.93.3.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF instance

This parameter contains the name of the OSPF instance.

SNMP ID:

2.93.3.3.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Area ID

Contains the ID of the area.

SNMP ID:

2.93.3.3.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

IP address

This parameter contains the IPv4 address.

SNMP ID:

2.93.3.3.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

IP netmask

This parameter contains the IPv4 subnet mask.

SNMP ID:

2.93.3.3.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

IPv4 netmask `[0-9.]`

Advertise

Enables or disables the advertisement of this address aggregation.

SNMP ID:

2.93.3.3.5

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Area-Address-Aggregation**

Possible values:

No

Advertising disabled

Yes

Advertising enabled

Default:

No

OSPF interfaces

Specifies the interfaces on which OSPF is operated.

SNMP ID:

2.93.3.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

SNMP ID:

2.93.3.4.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **OSPF-Interfaces**

Possible values:

Characters from the following character set: `[a-z A-Z 0-9 .]`

OSPF instance

This parameter contains the name of the OSPF instance.

SNMP ID:

2.93.3.4.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Area ID

Contains the ID of the area.

SNMP ID:

2.93.3.4.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

Interface type

Contains the interface type.

SNMP ID:

2.93.3.4.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

Broadcast

Ethernet-based network; a default router is selected and multicast is used for communication.

Point-to-point

Network consisting of two routers only (e.g. GRE tunnel) or Ethernet via P2P link; no default router is selected and multicast is used for communication.

Point-to-multipoint

Network as hub-and-spoke topology; a default router is selected and multicast is used for communication.

Non-Broadcast Multi- Access (NBMA)

Point-to-multipoint networks that do not support broadcast or multicast; a default router is selected and unicast is used for communication. All neighbors must be configured manually.

Default:

Broadcast

Output cost

Specifies the cost to send a packet on this interface, shown in the link-state metric. The advertisement is implemented in router LSA messages as a link cost for this interface.

SNMP ID:

2.93.3.4.5

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

Retransmit interval

Contains the number of seconds between retransmissions.

SNMP ID:

2.93.3.4.6

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

Transmit delay

Contains the estimated number of seconds required to transfer a link-state update packet over this interface.

SNMP ID:

2.93.3.4.7

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

Router priority

The priority of this router on this interface when it is set as default router (DR). The router with the highest priority is set as the default router.

SNMP ID:

2.93.3.4.8

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 255

Special values:

0

The value 0 prevents the router from becoming default router on this interface.

Hello interval

The interval in seconds in which the router sends Hello packets from this interface.

SNMP ID:

2.93.3.4.9

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

Router Dead Interval

Contains the elapsed time during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

This value must be greater than the Hello interval.

SNMP ID:

2.93.3.4.10

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

0 … 4294967295

Authentication type

Authentication method used for this interface.

SNMP ID:

2.93.3.4.11

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

Null
Simple password
Cryptographic MD5

Default:

Null

Authentication key

Authentication key for this network in the case that the authentication type **Null** is used.

SNMP ID:

2.93.3.4.12

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

16 characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

Passive

Defines whether OSPF works actively or passively on this interface.

SNMP ID:

2.93.3.4.13

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Interfaces**

Possible values:

No
Yes

No routing updates or hello packets are sent from this router on this interface. Similarly, no incoming OSPF messages are processed either. However, the corresponding route or network of this interface is still inserted into the LSDB and so is advertised on other interfaces.

Default:

No

MTU ignore

Disables the MTU value check in database description packets. This allows routers to establish a full neighbor relationship even if the MTU of the corresponding interfaces is not uniform.

SNMP ID:

2.93.3.4.14

Telnet path:

Possible values:

No
Yes

Default:

No

Virtual links

This table is used to define virtual links (also referred to as transit area). In principle, OSPF requires all areas to be directly connected to the backbone area. Virtual links can be used in cases where this is not possible. A virtual link uses a non-backbone area to connect a router to the backbone area.

SNMP ID:

2.93.3.5

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.5.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Transit area ID

Defines the area ID of the transit area.

SNMP ID:

2.93.3.5.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

Router ID

Defines the router ID of the router at the remote end of the virtual link.

SNMP ID:

2.93.3.5.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

Retransmit interval

Contains the number of seconds between retransmissions.

SNMP ID:

2.93.3.5.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

0 … 4294967295

Hello interval

The interval in seconds in which the router sends Hello packets from this interface.

SNMP ID:

2.93.3.5.5

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

0 … 4294967295

Router Dead Interval

Contains the elapsed time during which at least one hello packet must be received from a neighbor before the router declares that neighbor as down.

This value must be greater than the Hello interval.

SNMP ID:

2.93.3.5.6

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

0 … 4294967295

Authentication type

Authentication method used for this interface.

SNMP ID:

2.93.3.5.7

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

Null
Simple password
Cryptographic MD5

Default:

Null

Authentication key

Authentication key for this network in the case that the authentication type **Null** is used.

SNMP ID:

2.93.3.5.8

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Virtual-Links**

Possible values:

16 characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

NBMA neighbors

The neighbors of your non-broadcast multi-access network are configured in the **NBMA neighbors** menu.

Non-broadcast multi-access networks are networks containing multiple routers, but where broadcast is not supported. In this type of network, OSPF emulates operations in a broadcast network. A default router is selected for this network type.

The communication takes place not by multicast, but by unicast. Neighborhood connections must be configured manually, as the routers are unable to discover one another automatically by multicast.

SNMP ID:

2.93.3.6

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.6.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

SNMP ID:

2.93.3.6.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

Characters from the following character set: `[a-z A-Z 0-9 .]`

IP address

Contains the IPv4 address of the neighbor router at the remote end.

SNMP ID:

2.93.3.6.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

Request interval

Defines the interval in which Hello messages are sent to this router.

SNMP ID:

2.93.3.6.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

0 … 4294967295

Special values:

0

Disables the transmission of Hello messages.

Eligible as default router

Specifies whether the local device itself is selectable as default router.

SNMP ID:

2.93.3.6.5

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **NBMA-Neighbors**

Possible values:

No
Yes

Default:

No

Point-to-multipoint neighbors

This table is used to configure your point-to-multipoint neighbors.

In a point-to-multipoint network, all neighbors are treated as if point-to-point neighbors were directly connected via a non-broadcast network.

If no default router is selected, multicast is used for communications instead.

SNMP ID:

2.93.3.7

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.7.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

Possible values:

16 characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()#*+-,/:;?[\]^_.&<=>]`

OSPF interface

Contains the interface (IPv4 network or WAN remote station) on which OSPF is to be activated.

SNMP ID:

2.93.3.7.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

Possible values:

Characters from the following character set: `[a-z A-Z 0-9 .]`

IP address

Contains the IPv4 address of the neighbor router at the remote end.

SNMP ID:

2.93.3.7.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

Possible values:

IPv4 address `[0-9.]`

Default:

0.0.0.0

Request interval

Defines the interval in which Hello messages are sent to this router.

SNMP ID:

2.93.3.7.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Point-to-MultiPoint-Neighbors**

Possible values:

0 … 4294967295

Special values:

0

Disables the transmission of Hello messages.

BGP

in the **BGP** menu you configure the redistribution of routes that were learned dynamically from the Border Gateway Protocol.

SNMP ID:

2.93.3.8

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.8.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **BGP**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

BGP instance

Contains the name of the BGP instance.

SNMP ID:

2.93.3.8.2

Telnet path:

Routing-Protocols > **OSPF** > **BGP**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Metric source

Specifies which source is used to set the OSPF metric.

SNMP ID:

2.93.3.8.3

Telnet path:

Routing-Protocols > **OSPF** > **BGP**

Possible values:

Constant

Uses a user-defined constant metric.

Protocol

Uses the "local preference" value of the BGP prefix.

Default:

Constant

Constant metric

Contains the constant for the OSPF metric of the imported routes.

The metric source must first have been set to **Constant**.

SNMP ID:

2.93.3.8.4

Telnet path:

Routing-Protocols > **OSPF** > **BGP**

Possible values:

0 … 4294967295

Path type

Specifies the type of routes that were imported into OSPF.

SNMP ID:

2.93.3.8.5

Telnet path:

Routing-Protocols > **OSPF** > **BGP**

Possible values:

External type 1

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External type 2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

SNMP ID:

2.93.3.8.6

Telnet path:

Routing-Protocols > **OSPF** > **BGP**

Possible values:

0 … 4294967295

Connected

Routes that are automatically entered into the routing table by the operating system are configured under **Connected**.

SNMP ID:

2.93.3.9

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.9.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Connected**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Metric source

Specifies which source is used to set the OSPF metric.

SNMP ID:

2.93.3.9.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Connected**

Possible values:

Constant

Uses a user-defined constant metric.

Protocol

Uses a value set automatically.

Default:

Constant

Constant metric

Contains the constant for the OSPF metric of the imported routes.

The metric source must first have been set to **Constant**.

SNMP ID:

2.93.3.9.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Connected**

Possible values:

0 … 4294967295

Path type

Specifies the type of routes that were imported into OSPF.

SNMP ID:

2.93.3.9.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Connected**

Possible values:

External type 1

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External type 2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

SNMP ID:

2.93.3.9.5

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Connected**

Possible values:

0 … 4294967295

Static

Routes that the user manually enters into the routing table are configured in the menu **Static**.

SNMP ID:

2.93.3.10

Telnet path:

Setup > **Routing-Protocols** > **OSPF**

OSPF instance

Contains the name of the OSPF instance.

SNMP ID:

2.93.3.10.1

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Static**

Possible values:

Characters from the following character set `[A-Z a-z 0-9 @{|}~!$%'()+-,/:;?[\]^_.&<=>]`

Metric source

Specifies which source is used to set the OSPF metric.

SNMP ID:

2.93.3.10.2

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Static**

Possible values:

Constant

Uses a user-defined constant metric.

Protocol

Uses a value set automatically.

Default:

Constant

Constant metric

Contains the constant for the OSPF metric of the imported routes.

The metric source must first have been set to **Constant**.

SNMP ID:

2.93.3.10.3

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Static**

Possible values:

0 … 4294967295

Path type

Specifies the type of routes that were imported into OSPF.

SNMP ID:

2.93.3.10.4

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Static**

Possible values:

External type 1

In the OSPF routing algorithm, this type is given preference over external type 2.

The OSPF metric is formed as follows:

Redistribution metric or constant metric + the total path metric used to reach this ASBR.

External type 2

The OSPF metric is formed as follows:

Redistribution metric or constant metric.

External route tag

Specifies which external route tag the routes are imported with.

The value is not processed by OSPF itself.

SNMP ID:

2.93.3.10.5

Telnet path:

Setup > **Routing-Protocols** > **OSPF** > **Static**

Possible values:

0 … 4294967295

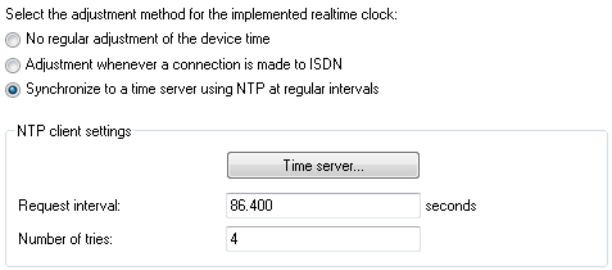
8 IPv6

8.1 IPv6 support for (S)NTP client and server

HiLCOS 10.12 supports IPv6 for the (S)NTP client and server.

8.1.1 Configuring the time server under LANconfig

In order for a device to broadcast the current time on the network, go to **Date & Time** > **Synchronization** and enable the regular synchronization with a time server.



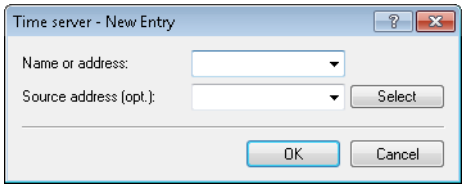
Request interval

Specify the time interval in seconds after which the internal clock of the device is re-synchronized with the specified time server (NTP).

Number of tries

Enter the number of times that the device should try to synchronize with the time server. By setting this value to zero, the device attempts to connect until it achieves a valid synchronization.

Then go to the section **NTP settings** and, under **Time server**, configure the settings for synchronizing the time with the server.



Name or address

Specify a time server (NTP) here for the device to synchronize with. The time server should be accessible via one of the available interfaces.

An address can be specified as a FQDN, IPv4 or IPv6 address. If the DNS name resolution returns an IPv6 address for the time server, the device will use this IPv6 address preferentially.

If you specify more than one time server in the list, you set the order in which they are queried in the overview of entries.

Source address (optional)

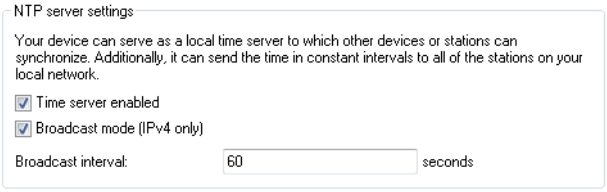
Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address. If you have configured loopback addresses, specify them here as the respective source address.

If the source address set here is a loopback address, then the device will use this unmasked even for remote stations that are masked.

The device accepts addresses in various input formats:

- Name of the IP network (ARF network), whose address should be used.
- "INT" for the address of the first intranet.
- "DMZ" for the address of the first DMZ (caution: If there is an interface called "DMZ", then the device takes its address).
- LB0 ... LBF for one of the 16 loopback addresses or its name
- Any valid IPv4 or IPv6 address

With these settings, the device initially retrieves the time from the public time servers for its own use only. To broadcast the current time to other devices in the LAN, go to **Date & Time** > **Synchronization** and, in the section **NTP server settings**, enable the time server on the device.



Time server enabled

Enable this option if the device is to work as a time server on the network.

Broadcast mode (IPv4 only)

If the device should regularly operate as a time server and send the current time to all stations in the network, enable the “send mode” here.

The send mode of the device only supports IPv4 addresses.

Broadcast interval

Specify the time interval in seconds after which the time server broadcasts the current time to the accessible stations on the network.

8.1.2 Additions to the Setup menu

BC-Mode

If the device should regularly operate as a time server and send the current time to all stations in the network, enable the “send mode” here.

The send mode of the device only supports IPv4 addresses.

SNMP ID:

2.26.3

Telnet path:

Setup > **NTP**

Possible values:

No

The send mode is disabled.

Yes

The send mode is enabled.

Default:

No

RQ-Address

Specify a time server (NTP) here for the device to synchronize with. The time server should be accessible via one of the available interfaces.

An address can be specified as a FQDN, IPv4 or IPv6 address. If the DNS name resolution returns an IPv6 address for the time server, the device will use this IPv6 address preferentially.

SNMP ID:

2.26.11.1

Telnet path:

Setup > **NTP** > **RQ-Address**

Possible values:

Max. 31 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Loopback-Addr.

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address. If you have configured loopback addresses, specify them here as the respective source address.

If the source address set here is a loopback address, then the device will use this unmasked even for remote stations that are masked.

The device accepts addresses in various input formats:

- Name of the IP network (ARF network), whose address should be used.
- "INT" for the address of the first intranet.

- "DMZ" for the address of the first DMZ (caution: If there is an interface called "DMZ", then the device takes its address).
- LB0 ... LBF for one of the 16 loopback addresses or its name
- Any valid IPv4 or IPv6 address

SNMP ID:

2.26.11.2

Telnet path:

Setup > **NTP** > **RQ-Address**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

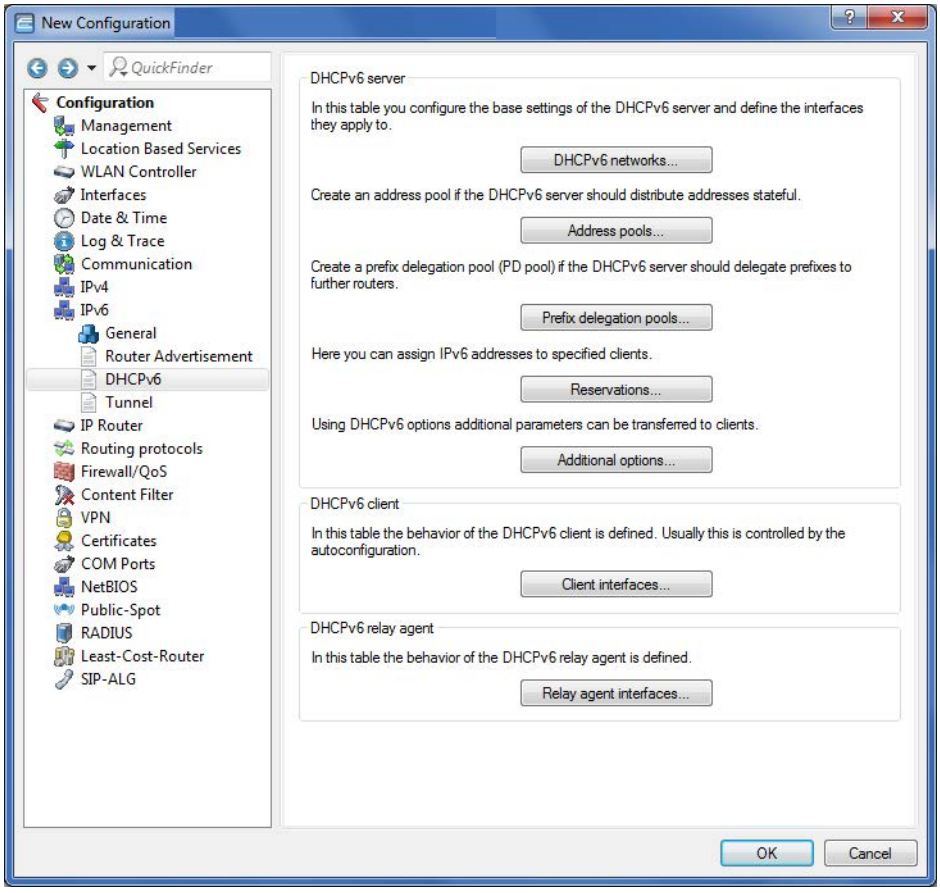
empty

8.2 Support for SNTP option in the DHCPv6 client

From HiLCOS 10.12, the DHCPv6 client is able to request a list of SNTP (Simple Network Time Protocol) servers from the DHCPv6 server.

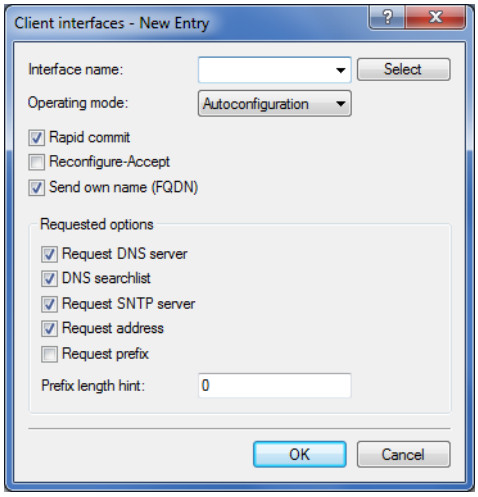
8.2.1 Configuration by LANconfig

1. Start LANconfig and open the configuration dialog for your device.
2. Navigate to **IPv6** > **DHCPv6** > **DHCPv6 server**.



3. Click the button **Client interfaces**.

4. Click the button **Add** to create a new entry or **Edit** to modify an existing entry.



5. Activate **Request SNTP server** in order to enable the new SNTP feature.

8.2.2 Additions to the Setup menu

Request SNTP

Specify whether the DHCPv6 client requests a list of SNTP (Simple Network Time Protocol) servers from the DHCPv6 server.

This requires regular synchronization with a timeserver.

SNMP ID:

2.70.3.2.1.10

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

0

No

1

Yes

Default:

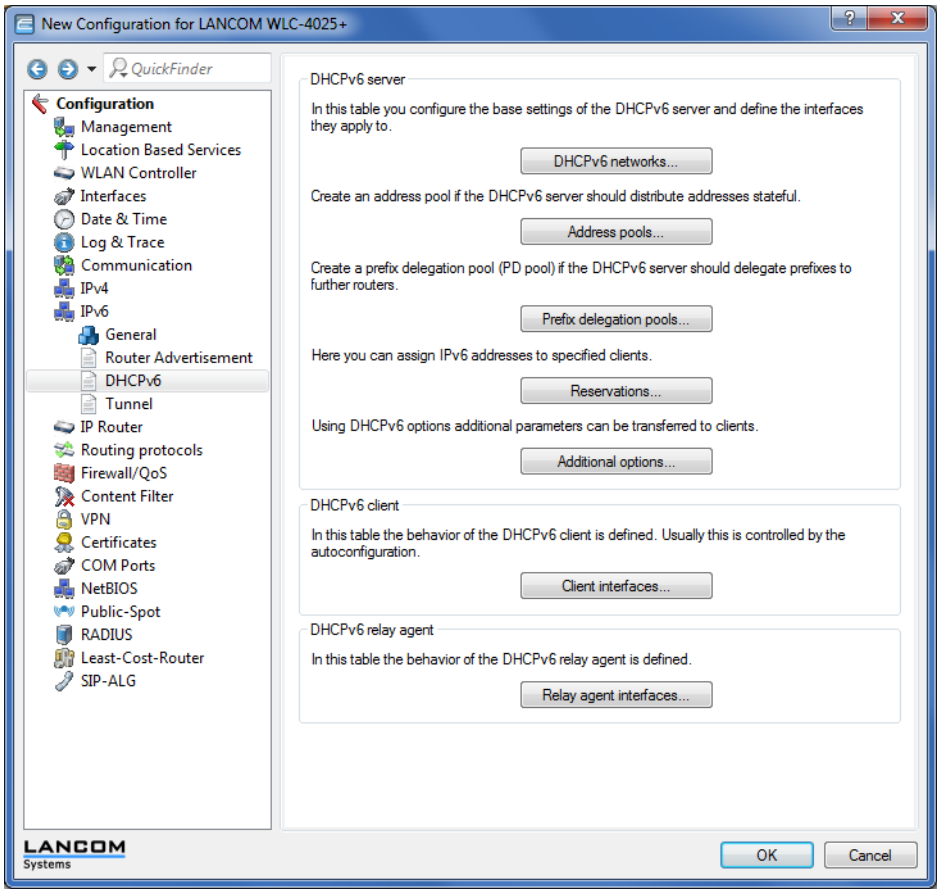
0

8.3 Support of prefix hint in the DHCPv6 client

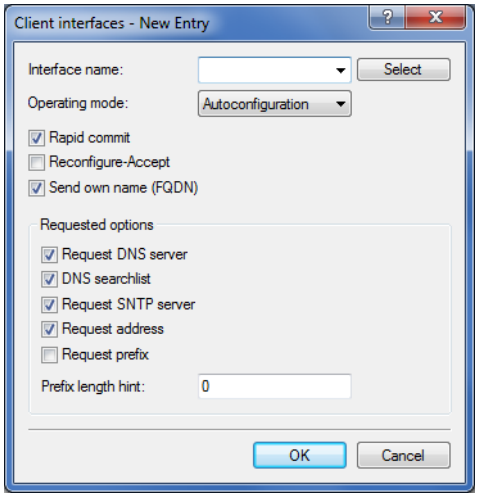
As of HiLCOS 10.12, the DHCPv6 client can request the DHCPv6 server for the necessary prefix length, e.g. 56 or 48 bits. The server can then assign the prefix to the client with the required length.

8.3.1 Configuration by LANconfig

1. Start LANconfig and open the configuration dialog for your device.
2. Navigate to **IPv6** > **DHCPv6** > **DHCPv6 server**.



3. Click the button **Client interfaces**.
4. Click the button **Add** to create a new entry or **Edit** to modify an existing entry.



5. Enter the required prefix length into the input field **Prefix length hint**.

> In order to send the desired prefix length to the DHCPv6 server, you must first enable Request prefix. Enter a three-digit number.

8.3.2 Additions to the Setup menu

PD hint

Here you specify whether the DHCPv6 client requests a desired prefix length from the DHCPv6 server.

SNMP ID:

2.70.3.2.1.11

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Client** > **Interface-List**

Possible values:

Three characters from the following character set: `[0-9]`

8.4 Transmitting the IPv6 LAN prefix with the action table

The action table offers two new variables as of HiLCOS 10.12.

A number of dynamic DNS providers, such as feste-ip.net and dynv6.com, are able to form fully-fledged Global Unicast Addresses (GUAs), which are accessible from the Internet, by combining the IPv6 LAN prefix transmitted by the router and the host identifiers of the LAN clients that are known to the provider. All the provider has to do is to append the host identifier to the transmitted LAN prefix. This GUA is then available from the provider as a AAAA record in the DNS. This allows you to make your IPv6-enabled LAN devices available at a fixed host name from anywhere in the world, even if the IPv6 prefix changes after a forced re-connection.

In order for the LAN clients to be accessible from the outside, the IPv6 firewall of the Hirschmann router needs to be configured with the appropriate exceptions. By default, no connections are permitted from the outside to the LAN.

Table 1: The following variables are available for use in the action table:

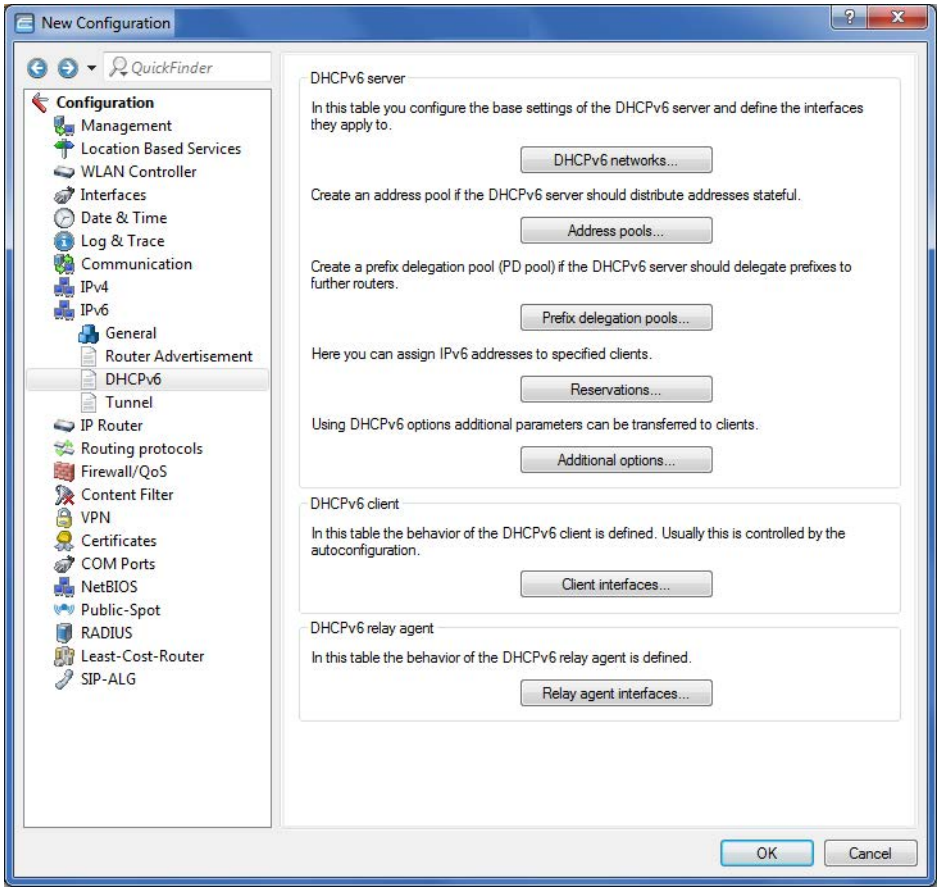
Variable	Meaning
%x	The current IPv6 LAN prefix as a string in the format "fd00:0:0:1::/64"
%y	The current IPv6 LAN address of the device as a string in the format "fd00::1:2a0:57ff:fa1b:9d7b"

8.5 DHCPv6 options

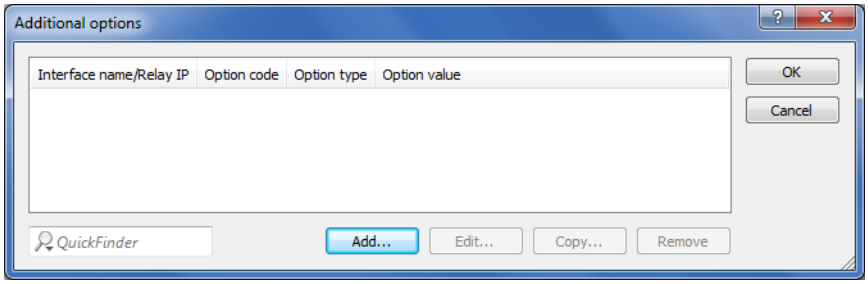
As of HiLCOS 10.12, the DHCPv6 server is able to assign DHCPv6 options to its DHCPv6 clients.

8.5.1 Configuration by LANconfig

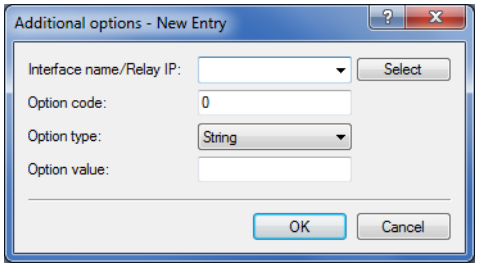
1. Navigate to the configuration menu **IPv6** > **DHCPv6** > **DHCPv6 server**.



2. Click the button **Additional options**.



3. Click on **Edit** or **Add** as as necessary.



4. From the selection list **Interface name/Relay IP**, select the name of the IPv6 interface or the remote IPv6 address of a relay agent for which the DHCPv6 server should distribute the additional option.

Note: In order for this option to be delivered to clients, the request sent by a client must must also contain the corresponding option code.

5. Enter the code of the DHCPv6 option into the **Option code** input box.
6. Use the selection list **Option type** to set the type of the DHCPv6 option.

A number of types are available here:

- **String**: Accepts the characters as a string.
- All other types use comma- and space-delimited lists; empty list elements are ignored; a list may be empty and results in an option of length 0.
- **Integer types** are decimal, octal with a leading 0, and hexadecimal with a leading 0x; capitalization is ignored. The value range for Integer8 is from -128 to 127; for Integer16 from -32768 to 32767; and for Integer32 from -2147483648 to 2147483647. A leading + or - sign is generally allowed.
- **IPv6Address** accepts IPv6 addresses (case insensitive) in all permissible notations, including the mixed IPv4/IPv6 notation of mapped V4 addresses (e.g., ::ffff:1.2.3.4).
- **Domain-List** accepts all strings that produce labels of maximum 63 characters in length. Empty labels are allowed but are ignored. A domain always ends with the empty label 0.
- **Hexdump** expects each block to have hex numbers only, without a leading 0x. It fills each block with a leading 0 for an even length and ends with the block **bigendian**.

7. The input field **Option value** is for the content of the DHCPv6 option, formatted according to the option type.
8. To accept the configuration, click the button **OK**.

8.5.2 Additions to the Setup menu

Additional options

This is the **Additional options** table for the DHCP server.

In order for this option to be delivered to clients, the request sent by a client must must contain the corresponding option code.

SNMP ID:

2.70.3.1.8

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Server**

Interface-Name-or-Relay

Here you choose the name of the IPv6 interface or the remote IPv6 address of a relay agent for which the DHCPv6 server should distribute the additional option

SNMP ID:

2.70.3.1.8.1

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

Possible values:

Characters from the following character set:
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Option code

Enter the code of your DHCPv6 option here.

SNMP ID:

2.70.3.1.8.2

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

Possible values:

0 … 65535

Default:

0

Option type

Select the type of your DHCPv6 option here.

SNMP ID:

2.70.3.1.8.3

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

Possible values:

String

The characters are accepted as a string. Please note: All other types use comma- and space-delimited lists; empty list elements are ignored; a list may be empty and results in an option of length 0.

Integer8

An 8-bit integer from -128 to 127 optionally decimal, octal with prefix '0', or hexadecimal with prefix '0x'.

Integer16

A 16-bit integer from -32768 to 32767.

Integer32

A 32-bit integer from -2147483648 to 2147483647.

IPv6 address

IPv6 addresses (case insensitive) in all permissible notations, including the mixed IPv4/IPv6 notation of mapped V4 addresses, such as ::ffff:1.2.3.4.

Domain list

All strings that produce labels of maximum 63 characters in length. Empty labels are allowed but are ignored. A domain always ends with the empty label 0.

Hexdump

Expects each block to have hex numbers only, without a leading 0x. Each block is filled with a leading 0 for an even length. The block is taken as **bigendian**.

Option value

Enter the contents of your DHCPv6 option here. The content must be formatted according to the selected option type.

SNMP ID:

2.70.3.1.8.4

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Additional-Options**

Possible values:

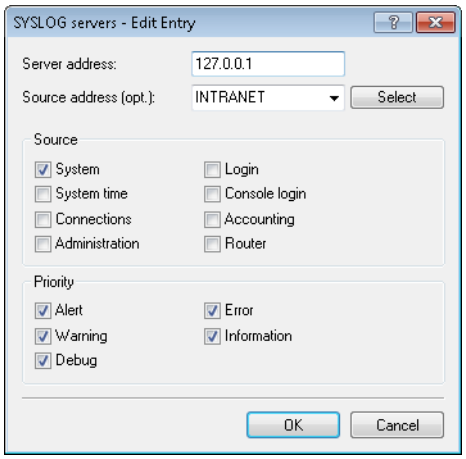
Depending on the option type, characters from:

```
[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`
```

9 Diagnosis

9.1 Specifying the SYSLOG server address as an IPv6 address or DNS name

As of HiLCOS 10.12, the addresses of a SYSLOG server can be entered in the form of an IPv6 address or a DNS name.



Server address

Used to set the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a host name.

9.2 IPv6 support for LCOScap

As of HiLCOS 10.12, LCOScap also supports IPv6 connections.

The LCOScap client is able to connect to the device via IPv4 or IPv6.

9.3 Layer-7 application detection

As of HiLCOS 10.12, layer-7 application detection allows you to identify bandwidth-intensive services on your network. When a client establishes a connection over a tracked interface, layer-7 application detection begins analyzing and recording the traffic volumes.

The results of the recording and the usage statistics depend on the configuration that was specified for this connection.

Layer-7 application detection monitors the destination port of an application. If a connection Is detected arriving at port 80 or 443 (HTTP or HTTPS), the connection establishment is further analyzed. If a different destination port is used, the application is identified according to the applications entered into the "Port-based tracking" list.

If the establishment of an HTTP/HTTPS connection is detected, this connection is subjected to deeper analysis. For HTTP connections, the application detection additionally extracts the destination host from the destination URL in the HTTP GET request.

The only part to be used is the host; additional parts of the URL are truncated

If an HTTPS connection is detected, the layer-7 application detection attempts to identify the destination host in the following sequence:

- Server name indication from the TLS "Client Hello"
- Common name from the transmitted TLS server certificate
- Reverse DNS request to the server IP address

For HTTP and HTTPS connections, the destination host name found is compared with the "HTTP/HTTPS tracking" list. This list contains the most widely used Web services/applications, including the components of their host names.

If neither the service nor the connection appear in the list, i.e. the application cannot be identified, then it is classified as a general HTTP or HTTPS service on the port.

Allocation in this way requires the "Port-based tracking" list to include the entries HTTP and HTTPS.

If the destination service is known for every connection on a tracked interface, the combination with the connecting client makes is possible to track the connection and to determine which client caused what amount of traffic to / from a service.

The values found are available from the corresponding tables in the HiLCOS menu tree under **Status** > **Layer-7-App-Detection**.

Layer-7 application detection can be operated either centrally or decentrally on your network. Both options prevent traffic being listed multiple times:

Central

Layer-7 application detection is enabled on a central router in the LAN, and it is disabled on all other Hirschmann devices.

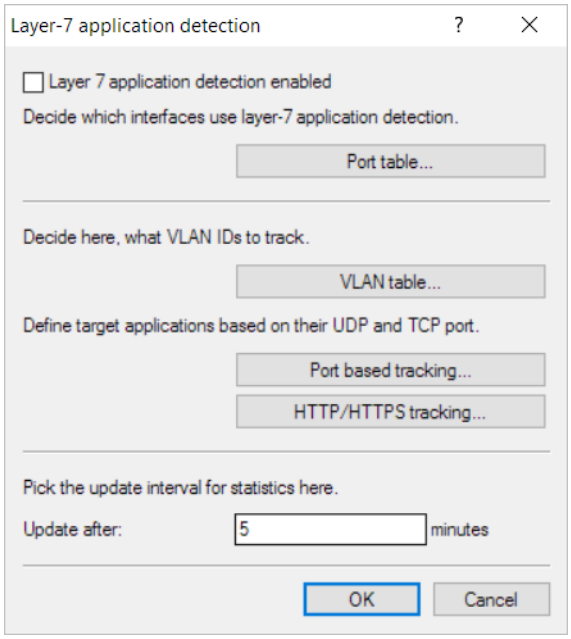
Decentral

Layer-7 application detection is enabled only on the final bridges in the LAN, e.g. on access points or Hirschmann routers with the clients connected directly to their LAN interfaces.

To avoid distorted results, the traffic should pass through just one single device or bridge running the layer-7 application detection.

9.3.1 Configuring layer-7 application detection with LANconfig

In LANconfig, you enable and configure layer-7 application detection under **Firewall/QoS** > **General** > **Layer-7 application detection**.



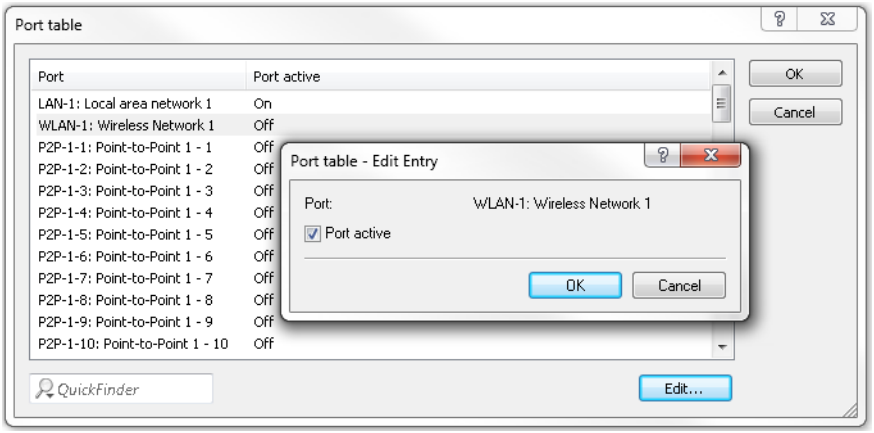
Use this dialog to specify the following parameters:

Layer-7 application detection enabled

This entry is used to enable or disable layer-7 application detection.

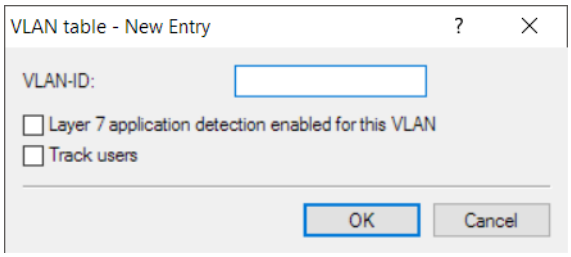
Port table

Here you specify the ports that are to be tracked by layer-7 application detection. Enable or disable the available ports correspondingly.



VLAN table

Here you specify the VLAN IDs to be monitored and you determine the extent to which the layer-7 application detection collects traffic information.

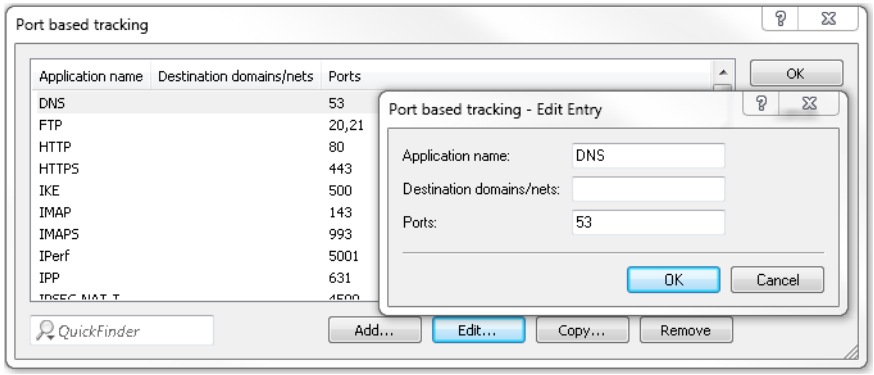


- **Layer-7 application detection enabled for this VLAN**: The device tracks general and application-specific data.
- **Track users:** The device tracks user-specific data (user or client name and MAC address) in the specified VLAN.

In order for layer-7 application discovery to be active in the VLAN, the data must collect application-specific data at the least.

Port-based tracking

Here you select the applications to be tracked. Optionally you can chose default applications or you can specify your own applications. You also specify the destination domains or the destination networks of the application. Extend the list according to your needs.

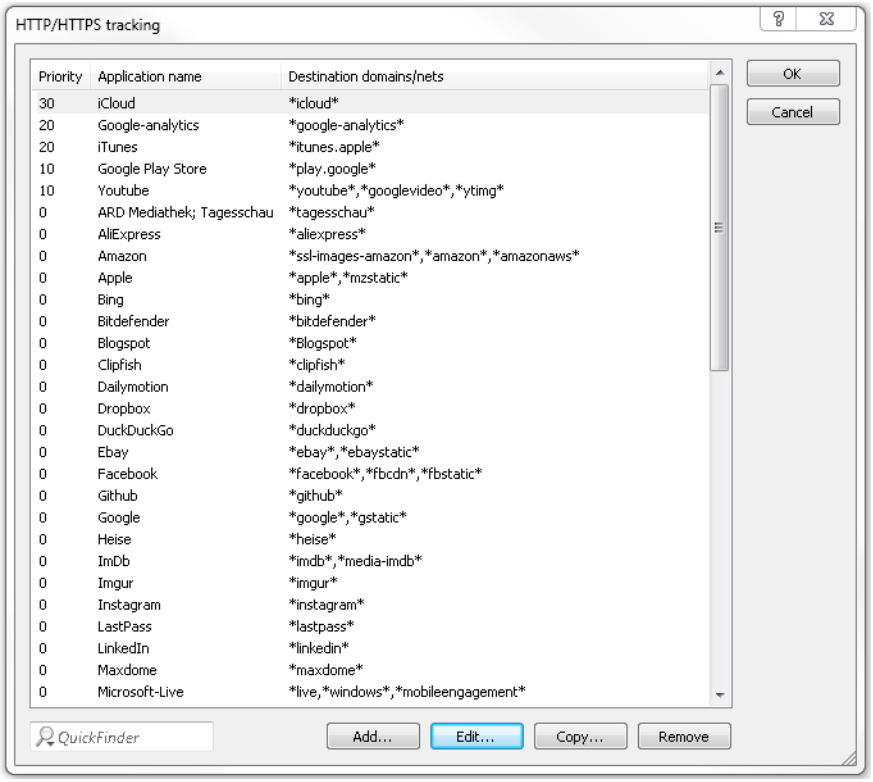


You can specify several destination domains, destination networks or ports by using a comma-separated list in CIDR notation (classless inter-domain routing). You have the option of using IPv4 or IPv6 destination networks.

HTTP/HTTPS tracking

Use this table to specify which HTTP/HTTPS services are tracked. You should additionally specify parts of the application's host name.

Use wildcards ("*" for multiple characters or "?" for exactly one character) to define the parts of the host name.



Multiple host-name parts can be specified in a comma-separated list.

By specifying the priority you have the additional option of setting the order in which services are evaluated if certain host-name parts appear in multiple entries (e.g. *google).

Update after

Specify an interval in minutes for updating the usage statistics.

9.3.2 Additions to the Setup menu

Layer-7 app detection

This menu is used to configure layer-7 application detection.

SNMP ID:

2.101

Telnet path:

Setup

Operating

This entry is used to enable or disable layer-7 application detection.

SNMP ID:

2.101.1

Telnet path:

Setup > **Layer-7-App-Detection**

Possible values:

No
Yes

Default:

No

IP port applications

Set the target ports for the layer-7 application detection, or add new entries to the table.

SNMP ID:

2.101.2

Telnet path:

Setup > **Layer-7-App-Detection**

Application name

Specify a unique name for this application.

SNMP ID:

2.101.2.1

Telnet path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Targets

Define targets for this application.

Specify multiple targets with a comma-separated list.

SNMP ID:

2.101.2.2

Telnet path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Ports

Specify the ports to be tracked.

SNMP ID:

2.101.2.3

Telnet path:

Setup > **Layer-7-App-Detection** > **IP-Port-Applications**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Port table

Here you activate or deactivate the ports to be tracked by layer-7 application detection.

The contents of the table are device dependent.

SNMP ID:

2.101.4

Telnet path:

Setup > **Layer-7-App-Detection**

Port

This entry contains the name of the port selected from the table.

SNMP ID:

2.101.4.2

Telnet path:

Setup > **Layer-7-App-Detection** > **Port-Table**

Traffic tracking

This entry is used to enable or disable the tracking of traffic for this port.

SNMP ID:

2.101.4.3

Telnet path:

Setup > **Layer-7-App-Detection** > **Port-Table**

Possible values:

No
Yes

Default:

No

Status-Update-In-Minute

This entry sets an interval in minutes when the usage statistics are updated.

SNMP ID:

2.101.5

Telnet path:

Setup > **Layer-7-App-Detection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

60

Max queue length

This entry specifies the maximum queue length for the usage statistics.

SNMP ID:

2.101.6

Telnet path:

Setup > **Layer-7-App-Detection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

10000

Reset statistics

This entry deletes the usage statistics of the layer-7 application detection.

SNMP ID:

2.101.7

Telnet path:

Setup > **Layer-7-App-Detection**

HTTP-HTTPS tracking

In this menu, specify the entries for the tracking of HTTP / HTTPS connections.

SNMP ID:

2.101.8

Telnet path:

Setup > **Layer-7-App-Detection**

Application name

Name for the tracking of HTTP / HTTPS connections (e.g. youtube).

SNMP ID:

2.101.8.1

Telnet path:

Setup > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Targets

Here you specify the targets for the tracking of HTTP / HTTPS connections (e.g. youtube).

Specify multiple targets in a comma-separated list (e.g. youtube, googlevideo, ytimg)

SNMP ID:

2.101.8.2

Telnet path:

Setup > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Prio

Set the priority of HTTP/HTTPS tracking by the layer-7 application detection.

SNMP ID:

2.101.8.3

Telnet path:

Setup > **Layer-7-App-Detection** > **HTTP-HTTPS-Tracking**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

VLAN

Here you specify the VLAN IDs to be monitored and you determine the extent to which the layer-7 application detection collects traffic information.

In order for layer-7 application discovery to be active in the VLAN, the data must collect application-specific data at the least.

SNMP ID:

2.101.11

Telnet path:

Setup > **Layer-7-App-Detection**

VLAN-ID

Use this entry to specify a VLAN ID.

SNMP ID:

2.101.11.1

Telnet path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

0 … 65535

Default:

0

Track user

With this entry you enable or disable the collection of user-specific data (user or client name and MAC address).

SNMP ID:

2.101.11.2

Telnet path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

No
Yes

Default:

No

Tracking active

This entry is used to enable or disable the collection of general or application-specific data.

SNMP ID:

2.101.11.3

Telnet path:

Setup > **Layer-7-App-Detection** > **VLAN**

Possible values:

No
Yes

Default:

No

Save-In-Min

Specify the interval in minutes for storing the usage statistics of the layer-7 application detection.

SNMP ID:

2.101.12

Telnet path:

Setup > **Layer-7-App-Detection**

Possible values:

Max. 5 characters from `[0-9]`

Default:

3600

9.3.3 Additions to the Status menu

Layer-7 app detection

This menu gives you information about the applications being tracked by the layer-7 application detection.

SNMP ID:

1.95

Telnet path:

Status

Applications

This table displays how much traffic each client generated to/from a service. The content of this table is regularly saved boot-persistent.

The table shows the name of the user or client in as far as this can be detected. The first attempt is to set the "User name" to the 802.1X user name. If 802.1X is not used, the client host name identified using DHCP snooping will be shown.

In addition, the column "PSpot-Users" shows the user name of the logged-on Public Spot users.

Public Spot user names are only displayed if the Public Spot module is active on the same device as that running the layer-7 application detection.

SNMP ID:

1.95.1

Telnet path:

Status > **Layer-7-App-Detection**

Total traffic per application

This table displays the traffic as grouped by application.

SNMP ID:

1.95.2

Telnet path:

Status > **Layer-7-App-Detection**

Total traffic per user

This table displays the traffic as grouped by user.

The table shows the name of the user or client in as far as this can be detected. The first attempt is to set the "User name" to the 802.1X user name. If 802.1X is not used, the client host name identified using DHCP snooping will be shown.

In addition, the column "PSpot-Users" shows the user name of the logged-on Public Spot users.

Public Spot user names are only displayed if the Public Spot module is active on the same device as that running the layer-7 application detection.

SNMP ID:

1.95.3

Telnet path:

Status > **Layer-7-App-Detection**

HTTP-HTTPS hit list

This table displays the hits for the HTTP/HTTPS connection tracking.

SNMP ID:

1.95.4

Telnet path:

Status > **Layer-7-App-Detection**

Operating

This entry indicates whether the layer-7 application detection is enabled or disabled.

SNMP ID:

1.95.5

Telnet path:

Status > **Layer-7-App-Detection**

Reset statistics

This entry deletes the usage statistics of the layer-7 application detection.

SNMP ID:

1.95.6

Telnet path:

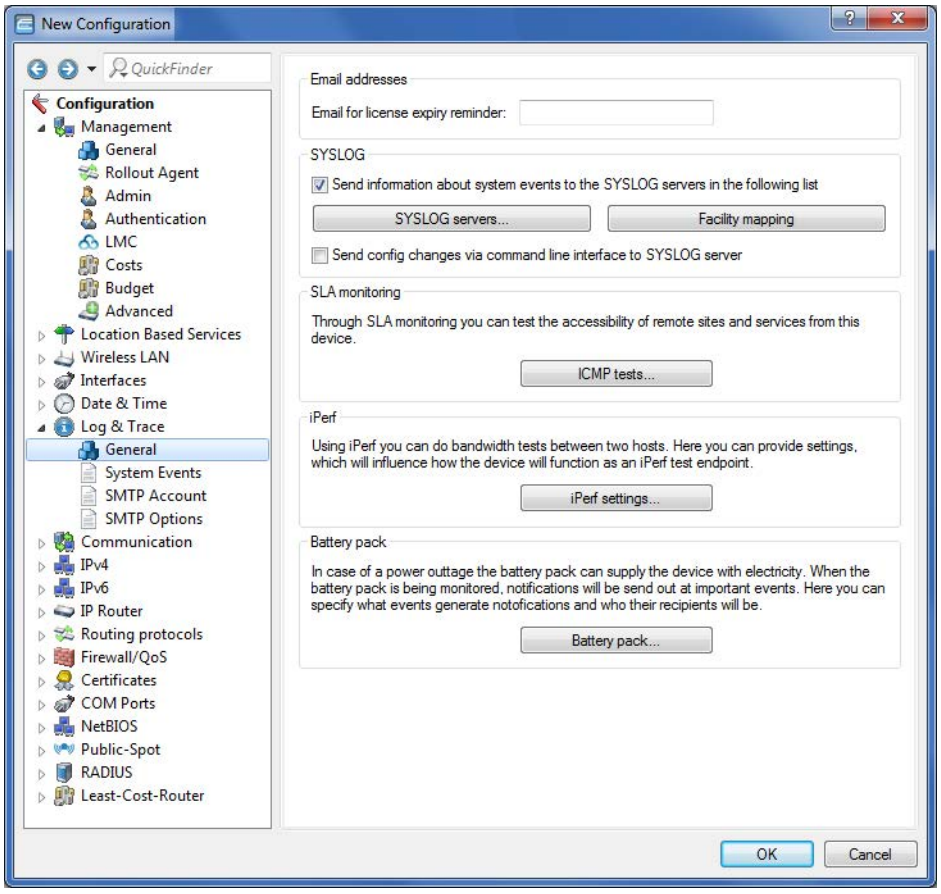
Status > **Layer-7-App-Detection**

9.4 SYSLOG messaging via TCP

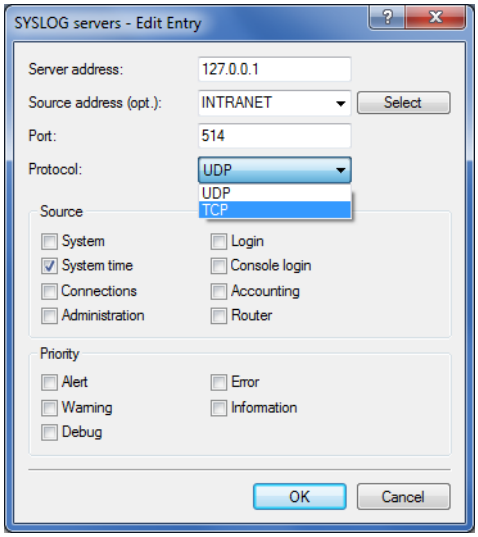
As of HiLCOS 10.12, the SYSLOG client can also send messages to a SYSLOG server via TCP.
During TCP transmission, every data packet is checked to see that it arrived at the destination address completely and unmodified.

9.4.1 Configuration by LANconfig

1. Start LANconfig and open the configuration dialog for your device.



2. Change to the dialog **Log & Trace** > **General** and open the table **SYSLOG servers**.



3. Set the **Port** input field to 514.
4. From the selection list **Protocol** select TCP.

9.4.2 Additions to the Setup menu

Port

This entry contains the port used for SYSLOG.

SNMP ID:

2.22.2.8

Telnet path:

Setup > **SYSLOG** > **Server**

Possible values:

514

TCP/UDP

Default:

514

Protocol

This entry contains the protocol used for SYSLOG.

SNMP ID:

2.22.2.9

Telnet path:

Setup > **SYSLOG** > **Server**

Possible values:

TCP
UDP

Default:

UDP

9.5 IPv4/IPv6 traffic accounting

As of HiLCOS 10.12, layer-7 application detection captures IPv4 and IPv6 traffic separately.

There is no need to switch on this feature separately. With layer-7 application detection is active, both IPv4 and IPv6 applications are automatically resolved separately.

Layer-7 application detection logs details about the traffic transmitted over the relevant interface.

This is presented in the following status table:

```
root@LN-1700Esc:/Status/Layer-7-App-Detection/Total-Traffic-per-Protocol
> ls -a

[1.3.6.1.4.1.2356.11][1.95.8]
Protocol-Name  Tx-KBytes  Rx-KBytes  Tx-KBytes-Curr.-Day  Rx-KBytes-Curr.-Day
[1]            [2]        [3]        [4]                  [5]
===============-------------------------------------------------------------
IPv4            522        259        522                  259
IPv6            2696       18         2696                 18
```

The inbound (RX) and the outbound (TX) traffic are listed separately for IPv4 and IPv6 in kBytes.

9.5.1 Additions to the Status menu

Total traffic per protocol

This table presents inbound and outbound IPv4 / IPv6 traffic in kBytes.

SNMP ID:

1.95.8

Telnet path:

Status > **Layer-7-App-Detection**

Possible values:

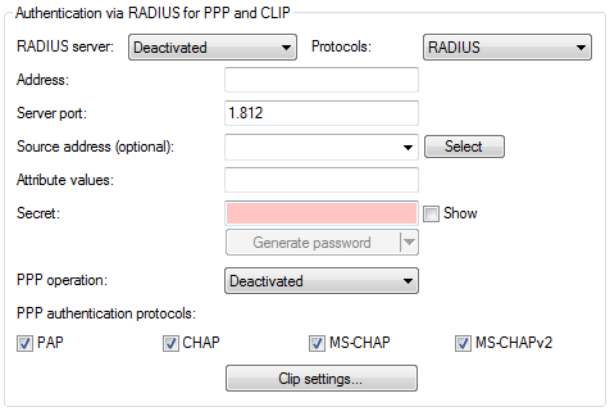
0 … 4294967295

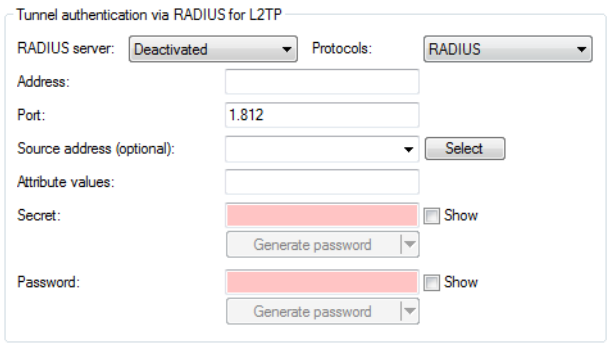
10 RADIUS

10.1 User-definable attributes in the RADIUS client

As of HiLCOS 10.12, LANconfig provides the option to independently configure all of the RADIUS attributes for the communications with RADIUS servers.

In LANconfig, you configure the attributes under **Communication** > **RADIUS** in the sections **Authentication via RADIUS for PPP and clip** and **Tunnel authentication via RADIUS for L2TP**.





Attribute values

HiLCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

10.2 Automatic clean-up of access information on the RADIUS server

As of HiLCOS 10.12, the function "Auto-Cleanup-Accounting-Totals" is enabled by default.

10.2.1 Additions to the Setup menu

Auto-Cleanup-Accounting-Totals

Closed accounting sessions are deleted if the function "RADIUS cleanup user table" has removed the related RADIUS account.

SNMP ID:

2.25.10.18

Telnet path:

Setup > **RADIUS** > **Server**

Possible values:

No

Accounting information is not automatically deleted.

Yes

Accounting information is deleted automatically.

Default:

Yes

10.3 Vendor-specific RADIUS attribute "LCS-Routing-Tag"

As of HiLCOS 10.12, the RADIUS client supports the vendor-specific RADIUS attribute "LCS-Routing-Tag" for PPTP, L2TP, and PPPoE.

10.4 Dynamic authorization by RADIUS CoA (Change of Authorization)

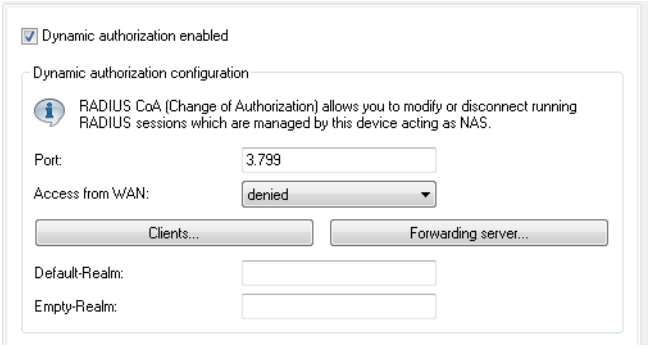
As of HiLCOS 10.12, it is possible to use CoA messages to modify current RADIUS sessions.

If you operate an external hotspot server, it is possible to change the attributes of Public Spot sessions after the user has authenticated. This is achieved with dynamic authorization by means of RADIUS CoA (Change of Authorization). See also the section "Dynamic authorization by RADIUS CoA (Change of Authorization)" in the RADIUS chapter.

In HiLCOS 10.12, this function is implemented for the Public Spot only.

10.4.1 Configuring dynamic authorization with LANconfig

In order to configure dynamic authorization (CoA) with LANconfig, navigate to **RADIUS** > **Dyn. Authorization**.



Dynamic authorization enabled

Activate or deactivate dynamic authorization here.

Port

Contains the default port where CoA messages are received.

Access from WAN

This entry specifies whether messages are accepted from the WAN, via VPN only, or prohibited.

Clients

Enter all of the CoA clients here that are permitted to send messages to the NAS.

Forwarding server

To forward CoA messages, the forwarding servers are specified here.

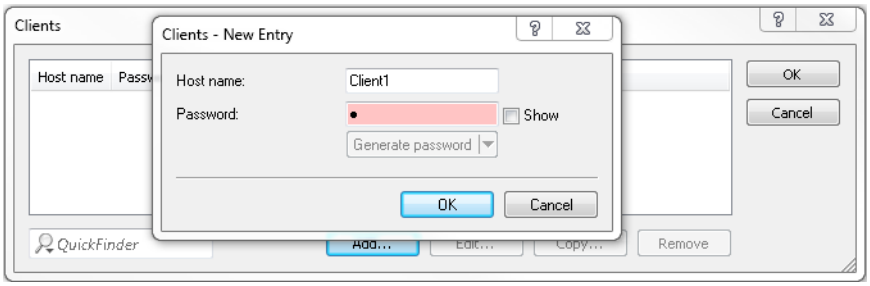
Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

Empty realm

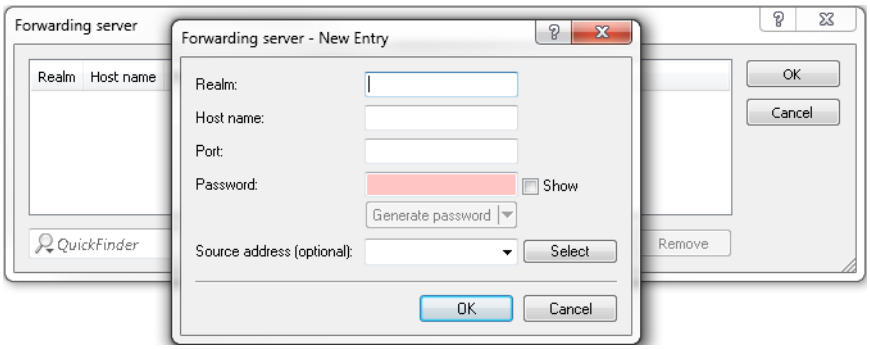
This realm is used when the specified username does not contain a realm.

To add CoA clients for dynamic authorization, click the button **Clients** and add a new entry to the table.



Enter a host name for the client and set a password for the client to access the NAS.

To add new forwarding servers for dynamic authorization, click the button **Forwarding server** and add a new entry to the table.



Realm

Here you enter the realm used by the RADIUS server to identify the forwarding destination.

If applicable, enter any existing forwarding servers that are specified under **RADIUS** > **Server** > **Forwarding** > **Forwarding server**.

Host name

Specify the host name of the forwarding server.

Port

Specify the server port used to forward the requests.

Password

Set a password that is required by the client to access the RADIUS server.

Source address (optional)

Optionally, specify a source address.

Additions to the Setup menu

Dyn-Auth

This menu contains the settings for dynamic authorization by RADIUS CoA (Change of Authorization). RADIUS CoA is specified in *RFC5176* .

SNMP ID:

2.25.19

Telnet path:

Setup > **RADIUS**

Operating

This entry enables or disables the dynamic authorization by RADIUS.

SNMP ID:

2.25.19.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

No
Yes

Default:

No

Port

This entry specifies the port on which CoA messages are accepted.

SNMP ID:

2.25.19.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 5 characters from `[0-9]`

Default:

3799

WAN access

This entry specifies whether messages are accepted from the LAN, WAN, or VPN.

SNMP ID:

2.25.19.3

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

No
Yes

Default:

No

Clients

All of the CoA clients that send messages to the NAS are entered into this table.

SNMP ID:

2.25.19.4

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

HostName

This entry contains the unique identifier of the client that sends messages to the NAS.

SNMP ID:

2.25.19.4.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Clients**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Secret

This entry specifies the secret required by the client for access to the NAS in the access point.

SNMP ID:

2.25.19.4.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Clients**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Forward-Servers

To forward CoA messages, the forwarding servers are specified here.

SNMP ID:

2.25.19.5

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Realm

This entry contains a string with which the RADIUS server identifies the forwarding destination.

SNMP ID:

2.25.19.5.1

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

HostName

Here you enter the hostname of the RADIUS server to which the RADIUS client forwards the requests from WLAN clients.

SNMP ID:

2.25.19.5.2

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Port

This entry contains the port for communications with the forwarding server.

SNMP ID:

2.25.19.5.3

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 10 characters from `[0-9]`

Default:

0

Secret

This entry specifies the secret required to access the forwarding server.

SNMP ID:

2.25.19.5.4

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Loopback

Here you have the option to configure a sender address for the device to use in place of the one that would otherwise be used automatically for this target address.

SNMP ID:

2.25.19.5.5

Telnet path:

Setup > **RADIUS** > **Dyn-Auth** > **Forward-Servers**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Default realm

This realm is used if the supplied username uses an unknown realm that is not in the list of forwarding servers.

SNMP ID:

2.25.19.6

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Empty realm

This realm is used when the specified username does not contain a realm.

SNMP ID:

2.25.19.7

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Radclient

Use the command `do Radclient [...]` to send CoA messages.

The Radclient command is structured as follows:

```
do Radclient <server[:port]> coa/disconnect <secret> <attribute-list>
```

Outputs all known and active RADIUS sessions

Entering the command `show dynauth sessions` on the command line lists the RADIUS sessions that are known to the CoA module. This outputs the session reported by the Public Spot module. The known attributes for this session are shown in the section "Context":

```
Session with MAC-Address: [a3:18:22:0c:ae:df] Context:
[NAS-IP-Address: 192.168.1.254,User-Name: user46909, NAS-Port-Id:
WLC-TUNNEL-1, Framed-IP-Address: 192.168.1.78]
```

The attributes "NAS-IP-Address" and "Username" identify the active session. If you wish to limit the bandwidth for the active session, you enter the Radclient command with these values along with the attributes "LCS-TxRateLimit" and "LCS-RxRateLimit" in combination with the transmission and reception limits in kbps:

do Radclient 192.168.1.254 coa secret
"User-Name=user46909;NAS-IP-Address=192.168.1.254;LCS-TxRateLimit=5000;LCS-RxRateLimit=5000"

Note that the identification attributes and the attributes being modified must be specified with the same rights in the attribute list.

Terminate an active RADIUS session

A running RADIUS session is terminated by using the Radclient command to send a disconnect message:

```
do Radclient 192.168.1.254 disconnect secret
"User-Name=user46909;NAS-IP-Address=192.168.1.254"
```

The Radclient command integrated in HiLCOS is primarily for test purposes. CoA messages are usually sent to the NAS from an external system.

SNMP ID:

2.25.19.8

Telnet path:

Setup > **RADIUS** > **Dyn-Auth**

10.5 Support of tunnel-password and LCS-routing-tag attributes

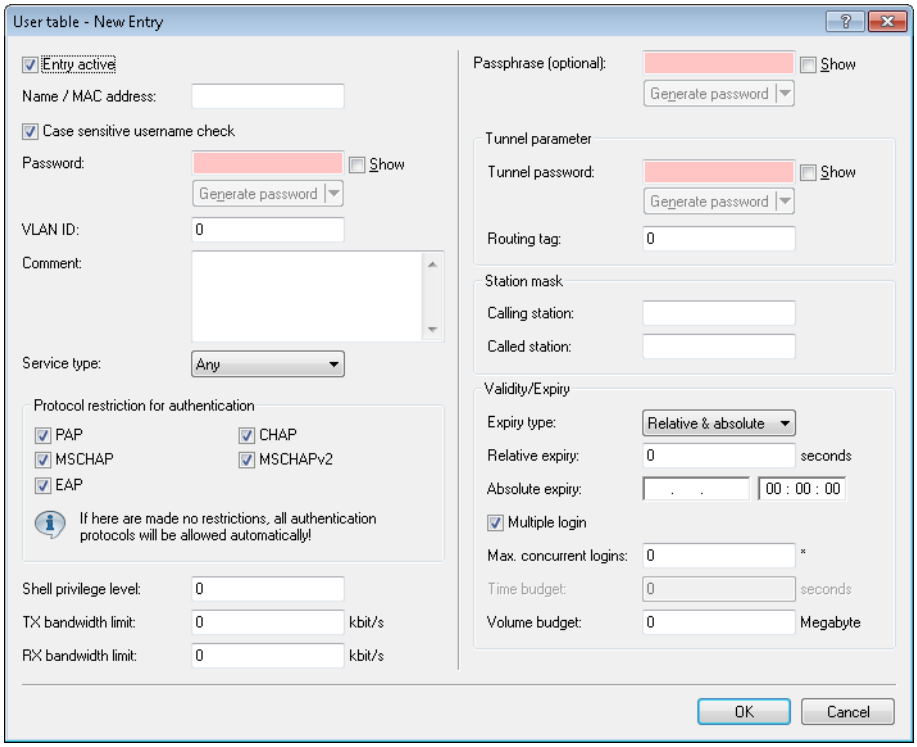
As of HiLCOS 10.12, Hirschmann RADIUS servers support the attributes "Tunnel-Password" and "LCS-Routing-Tag", which you can specify for each user account.

This helps an organization to store user data on a central RADIUS server and to minimize the effort required for the configuration of VPN scenarios.

10.5.1 Using LANconfig to configure Tunnel-Password and Routing-Tag attributes

In LANconfig, specify the attributes of "Tunnel-Password" and "Routing-Tag" under **RADIUS** > **Server** > **User table**.

Add a new entry to the table or edit an existing entry.



In the "Tunnel parameter" section, set values for the corresponding attributes:

Tunnel-Password

Here you enter the password used by the corresponding user to authenticate for a VPN connection via IKEv2 or L2TP.

Routing tag

Specify the routing tag to be used for the connection.

10.5.2 Additions to the Setup menu

Tunnel-Password

This entry sets the connection password for each user.

SNMP ID:

2.25.10.7.23

Telnet path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

LCS-Routing-Tag

Specify the routing tag for this connection.

SNMP ID:

2.25.10.7.24

Telnet path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

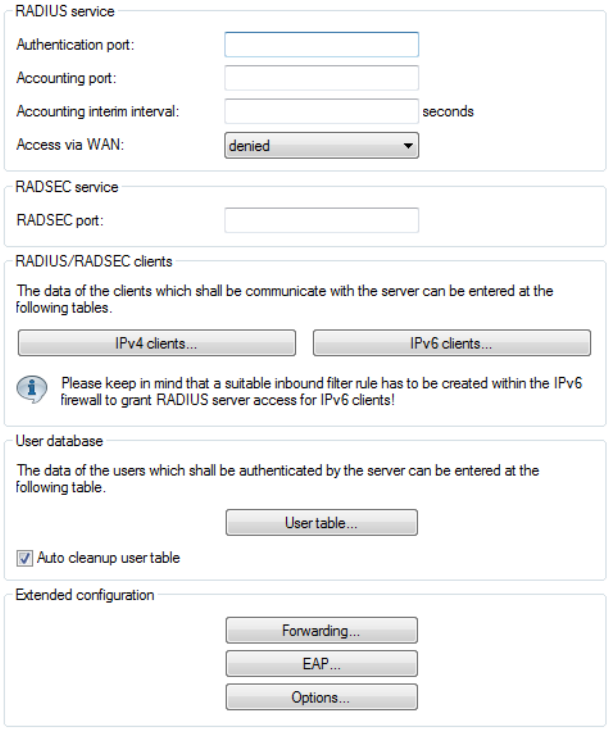
Max. 5 characters from `[0-9]`

Default:

0

10.6 Restricting WAN access to the RADIUS server

As of version 10.12, HiLCOS allows the restriction of access from the IPv4 network.



WAN access to the RADIUS server

Here you specify how the RADIUS server can be accessed from the WAN.

Applies only to traffic from the IPv4 network. Traffic from the IPv6 network is controlled by the integrated firewall. By default, the IPv6 firewall prohibits access to the RADIUS server from the WAN.

10.6.1 Additions to the Setup menu

IPv4-WAN-Access

Here you specify how the RADIUS server can be accessed from the WAN.

Applies only to traffic from the IPv4 network. Traffic from the IPv6 network is controlled by the integrated firewall. By default, the IPv6 firewall prohibits access to the RADIUS server from the WAN.

SNMP ID:

2.25.10.22

Telnet path:

Setup > **RADIUS** > **Server**

Possible values:

No

The RADIUS server rejects WAN traffic from the IPv4 network.

Yes

The RADIUS server accepts WAN traffic from the IPv4 network.

VPN

The RADIUS server accepts only WAN traffic from the IPv4 network that arrives at the device over a VPN connection.

Default:

No

11 Interface bundling with LACP

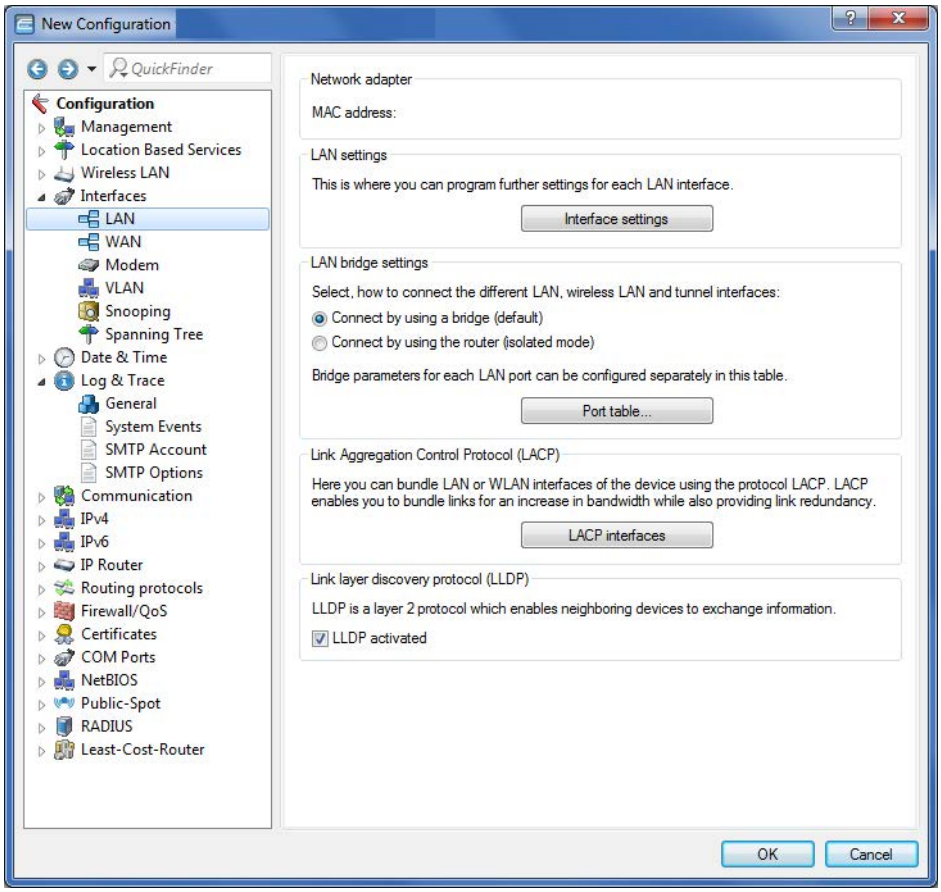
Significant improvements in terms of failover reliability and performance come with HiLCOS 10.12 and the new support for the standard LACP (Link Aggregation Control Protocol). LACP allows you to bundle Ethernet ports into a virtual link. Physical Ethernet connections can be combined to form a single logical connection, which greatly increases the speed of data transmission and makes optimal use of the available bandwidth.

For example, 11ac Wave 2 (4x4 MIMO) achieves a data throughput greater than 1 Gbps net per AP.

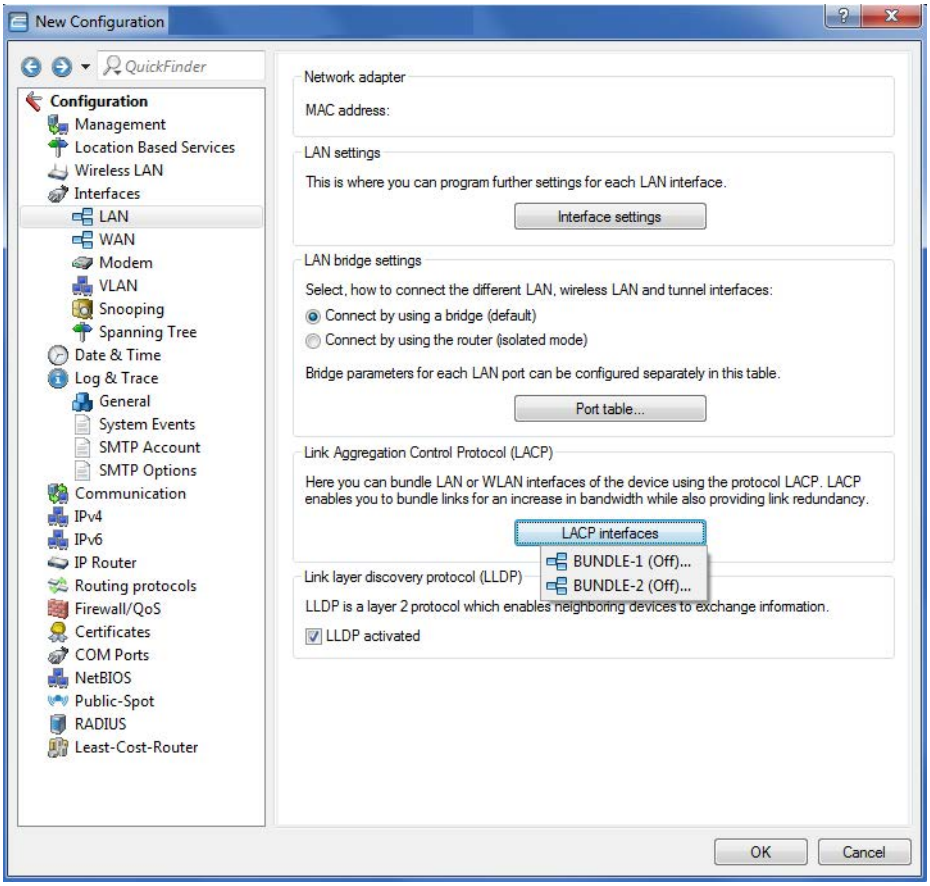
Along with a real performance gain in the network, LACP is also an ideal redundancy option because, even if a physical connection fails, data traffic is still transmitted on the other line.

11.1 Configuring the LACP interfaces

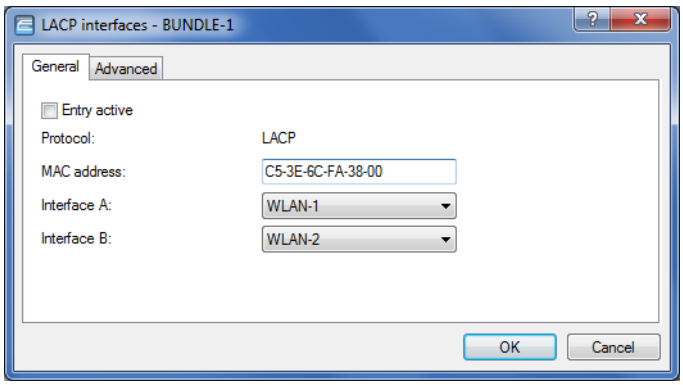
In LANconfig, you configure LACP interfaces under **Interfaces** > **LAN** in the section **Link Aggregation Control Protocol (LACP)**.



1. Click the button **LACP interfaces** to access the list of available bundles.



2. Choose a bundle.



3. Enter the MAC address of the device into the input field **MAC address**.

> The MAC address is used to identify the LACP partner within the LAG. If this is left empty or set to 0, the LAN MAC address of the device is set automatically. The MAC address does not necessarily have to belong to an interface of the bundle. In case of a configuration reset, the system-wide MAC address is entered here as the default.

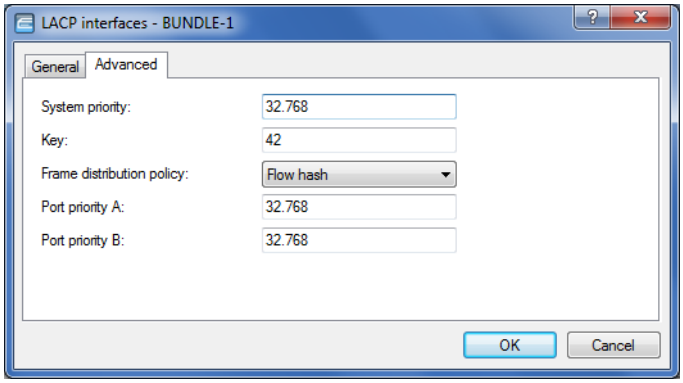
4. Select the first interface from the selection menu **Interface A**.
5. Select the second interface from the selection menu **Interface B**.
6. Activate the bundle by checking the checkbox **Entry active**.

> The remaining steps are optional.

The default settings are suitable for most common applications.

Further customizations to the configuration should only be performed by an experienced network technician.

7. Further configuration options are available on the **Advanced** tab.



8. In the **System priority** input field, enter a multiple of 4,096. The default value is 32,768.
9. Enter a value for the **Key**.

The key is a number from 1 to 54 and is used to identify the bundle.

10. Select an entry from the drop-down menu **Frame distribution policy**. The default setting for most scenarios is Flow hash.
11. In the **Port priority A** input field, enter a multiple of 4,096. The default value is 32,768.
12. In the **Port priority B** input field, enter a multiple of 4,096. The default value is 32,768.

11.1.1 Additions to the Setup menu

LACP

This menu is used to configure the Link Aggregation Control Protocol (LACP).

SNMP ID:

2.4.13.12

Telnet path:

Setup > **LAN** > **Interface-Bundling**

Interfaces

Select an interface bundle here.

SNMP ID:

2.4.13.12.1

Telnet path:

Setup > **LAN** > **Interface-Bundling** > **LACP**

Possible values:

BUNDLE-1
Interface bundle 1
BUNDLE-2
Interface bundle 2

Interface

Use this menu to access the advanced features.

SNMP ID:

2.4.13.12.1.1

Telnet path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

General
Contains previously known features of the interface bundling.
Advanced
Contains new features of the interface bundling.

Default:

General

System-Priority

Set the system priority here.

SNMP ID:

2.4.13.12.1.2

Telnet path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

Multiples of 4096 `[0-9]`

Default:

32768

Key

Here, you assign a number as an identifier for the bundle.

SNMP ID:

2.4.13.12.1.3

Telnet path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

1 … 54

Default:

42

Frame distribution policy

Outbound packets from the transmitting end are distributed to the individual interfaces within the link aggregation group (LAG) according to the frame distribution policy.

SNMP ID:

2.4.13.12.1.4

Telnet path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

VLAN

Outbound packets are distributed to the individual links of the LAG according to their VLAN tags.

Flow hash

For outbound packets, a flow hash is formed from the IP addresses and the TCP/UDP ports. The flow hash determines how the packets are distributed to the individual links of the LAG.

Source MAC

Outbound packets are distributed to the individual links of the LAG according to their source MAC address.

Destination MAC

Outbound packets are distributed to the individual links of the LAG according to their destination MAC address.

Source-dest. MAC

Outbound packets are distributed to the individual links of the LAG according to their source MAC address and destination MAC address.

Default:

Flow hash

Port priority A

Here you set the status values for port priority A.

SNMP ID:

2.4.13.12.1.5

Telnet path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

Multiples of 4096 `[0-9]`

Default:

32768

Port priority B

Here you set the status values for port priority A.

SNMP ID:

2.4.13.12.1.6

Telnet path:

Setup > **LAN** > **Interface-Bundling** > **LACP** > **Interfaces**

Possible values:

Multiples of 4096 `[0-9]`

Default:

32768

12 Other Services

A single device offers a range of services for the PCs on the LAN. These are essential functions for use by the workstations. In particular these are:

- Automatic address management with DHCP
- Name administration of computers and networks by DNS
- Network traffic logging with SYSLOG
- Charging
- Office communications with LANCAPI
- Time server

12.1 DHCP snooping: New variable for LAN MAC address

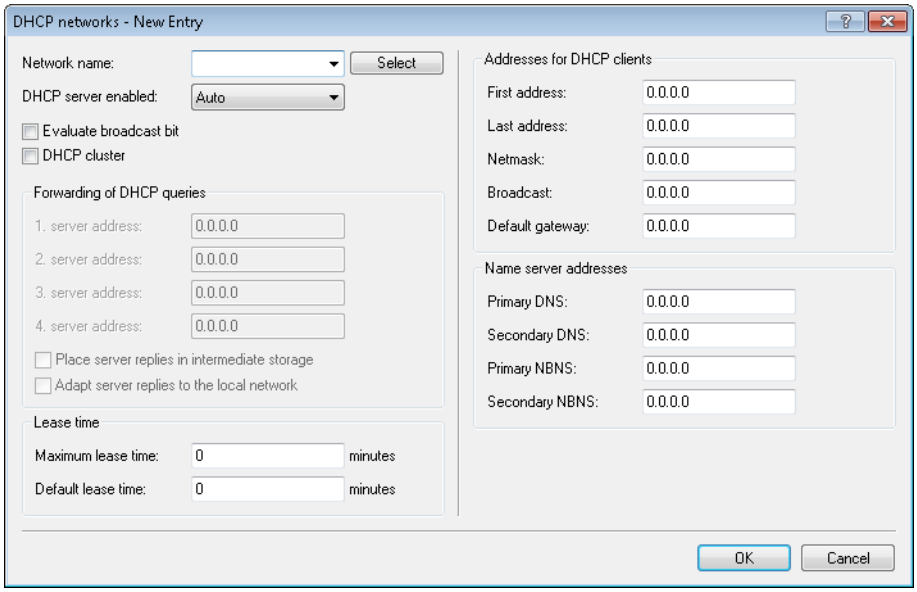
As of HiLCOS 10.12, a dedicated variable is available for the LAN MAC address. This MAC address applies system-wide and also appears in the SysInfo and in LANconfig.

- `%r`: Inserts the interface-independent (i.e. valid throughout the system) MAC address of the device that received the DHCP request.

12.2 DHCP lease time per network

As of HiLCOS 10.12 it is possible to give each DHCP network its own lease time.

Carry out the configuration in LANconfig under **IPv4** > **DHCPv4** and click on **DHCP networks**.



Lease time of address assignments

In addition to the global default lease time configured under **IPv4** > **DHCPv4**, it is possible to configure a lease time specifically for this DHCP network only.

Maximum lease time

Here you specify the maximum lease time that a client may request.

Default lease time

If a client requests IP-address data without specifying any particular lease time, the lease time set here is assigned to it.

12.2.1 Additions to the Setup menu

Max.-Lease

In addition to the global maximum lease time configured under **Setup** > **DHCP**, it is possible to configure a maximum lease time specifically for this DHCP network only.

Here you specify the maximum lease time that a client may request.

SNMP ID:

2.10.20.20

Telnet path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Special values:

0

There is no limit on the lease time that the DHCP client may request.

Def.-Lease

In addition to the global default lease time configured under **Setup** > **DHCP**, it is possible to configure a default lease time specifically for this DHCP network only.

If a client requests IP-address data without specifying any particular lease time, the lease time set here is assigned to it.

SNMP ID:

2.10.20.21

Telnet path:

Setup > **DHCP** > **Network-List**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

Special values:

0

There is no limit on the lease time that can be assigned to the DHCP client.

12.3 DHCP lease RADIUS accounting

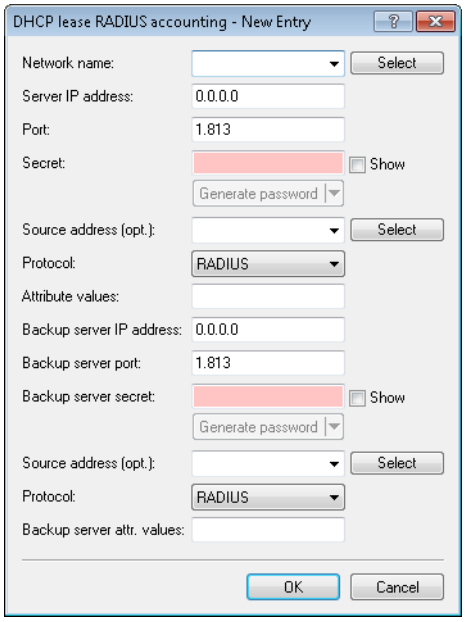
As of HiLCOS 10.12, HiLCOS supports DHCP RADIUS accounting.

12.3.1 DHCP lease RADIUS accounting

If RADIUS accounting is enabled and the DHCP server assigns an IP address to a DHCP client, the server sends a RADIUS `accounting start` to the relevant accounting server (or the backup RADIUS server). If the DHCP lease expires because no extension was requested, the DHCP server sends a `RADIUS accounting stop`. In between these two events, the DHCP server regularly sends the RADIUS server a `RADIUS accounting interim update` in a configurable interval.

To enable or disable RADIUS accounting for the DHCP server, go to **IPv4** > **DHCPv4** and click on the option **Activate DHCP lease RADIUS accounting**.

The input box **Accounting interim interval** configures the interval for the RADIUS interim updates. You configure the RADIUS accounting server and the corresponding backup server by clicking on **DHCP lease RADIUS accounting**.



Network name

Select here the name of the network for which RADIUS accounting messages are to be sent.

Server IP address

Enter the IP address or the DNS name of the RADIUS server (IPv4 or IPv6).

Port

Enter the TCP port used by the RADIUS server to receive accounting information. That is usually the port “1813”.

Key

Enter the key (shared secret) for access to the RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

Source address (optional)

By default, the RADIUS server sends its replies back to the IP address of your device without having to enter it here. By entering an optional alternative loopback address, you change the source address and route used by the device to connect to the RADIUS server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

Protocol

Use this entry to specify the protocol used by the DHCP server to communicate with the RADIUS accounting server.

Attribute values

HiLCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

Backup server IP address

Enter the IP address or the DNS name of the backup RADIUS server.

Backup server port

Enter the TCP port used by the backup RADIUS server to receive accounting information. That is usually the port "1813".

Backup server secret

Enter the key (shared secret) for access to the backup RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

Source address (optional)

Here you optionally specify an alternative source address that the DHCP server transfers to the backup RADIUS server.

Protocol

Use this entry to specify the protocol that the DHCP server uses for the RADIUS accounting server.

Backup server attr. values

Here you specify any additional attribute values for the RADIUS communication with the backup server.

12.3.2 Additions to the Setup menu

RADIUS accounting

If RADIUS accounting is enabled and the DHCP server assigns an IP address to a DHCP client, the server sends a `RADIUS accounting start` to the relevant accounting server (or the backup RADIUS server). If the DHCP lease expires because no extension was requested, the DHCP server sends a `RADIUS accounting stop`. In between these two events, the DHCP server regularly sends the RADIUS server a `RADIUS accounting interim update` in a configurable interval.

This menu contains the settings for the DHCP lease RADIUS accounting.

SNMP ID:

2.10.23

Telnet path:

Setup > **DHCP**

Operating

Enables or disables the RADIUS accounting on this DHCP network.

SNMP ID:

2.10.23.1

Telnet path:

Setup > **DHCP** > **RADIUS-Accounting**

Possible values:

No

RADIUS accounting is disabled for this network.

Yes

RADIUS accounting is enabled for this network.

Default:

No

Interim Interval

Here you specify the time interval in seconds after which the DHCP server sends a `RADIUS interim update` to the accounting server.

SNMP ID:

2.10.23.2

Telnet path:

Setup > **DHCP** > **RADIUS-Accounting**

Possible values:

Max. 10 characters from `[0-9]`

Network list

This table contains the IP networks for the RADIUS accounting.

SNMP-ID:

2.10.23.20

Pfad Telnet:

Setup > **DHCP** > **RADIUS-Accounting**

Network name

Contains the name of the network.

SNMP-ID:

2.10.23.20.1

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Server host name

Enter the host name of the RADIUS accounting server here.

SNMP-ID:

2.10.23.20.2

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Accnt.-Port

Enter the TCP port used by the RADIUS server to receive accounting information. That is usually the port „1813".

SNMP-ID:

2.10.23.20.3

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 5 characters from `[0-9]`

Default-Wert:

1813

Secret

Enter the key (shared secret) for access to the RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

SNMP-ID:

2.10.23.20.4

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Loopback address

By default, the RADIUS server sends its replies back to the IP address of your device without having to enter it here. By entering an optional alternative loopback address, you change the source address and route used by the device to connect to the RADIUS server. This can be useful, for example, when the server is available over different paths and it should use a specific path for its reply message.

SNMP-ID:

2.10.23.20.5

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Protocol

Use this entry to specify the protocol used to communicate with the RADIUS accounting server.

SNMP-ID:

2.10.23.20.6

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

Attribute-Values

HiLCOS facilitates the configuration of the RADIUS attributes used to communicate with a RADIUS server (for authentication and accounting).

The attributes are specified in a semicolon-separated list of attribute numbers or names along with a corresponding value in the form `<Attribute_1>=<Value_1>;<Attribute_2>=<Value_2>`.

As the number of characters is limited, the name can abbreviated. The abbreviation must be unique, however. Examples:

- `NAS-Port=1234` is not allowed, because the attribute is not unique (`NAS-Port`, `NAS-Port-Id` or `NAS-Port-Type`).
- `NAS-Id=ABCD` is allowed, because the attribute is unique (`NAS-Identifier`).

Attribute values can be used to specify names or RFC-compliant numbers. For the device , the specifications `Service-Type=Framed` and `Service-Type=2` are identical.

Specifying a value in quotation marks (`"<Value>"`) allows you to specify special characters such as spaces, semicolons or equals signs. The quotation mark requires a leading backslash (`\"`), as does the backslash itself (`\\`).

The following variables are permitted as values:

%n

Device name

%e

Serial number of the device

%%

Percent sign

%{name}

Original name of the attribute as transferred by the RADIUS application. This allows attributes to be set with the original RADIUS attributes, for example: `Called-Station-Id=%{NAS-Identifier}` sets the attribute `Called-Station-Id` to the value with the attribute `NAS-Identifier`.

SNMP-ID:

2.10.23.20.7

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Backup server hostname

Enter the host name of the backup server here.

SNMP-ID:

2.10.23.20.12

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Default-Wert:

leer

Backup-Accnt.-Port

Here you enter the backup port used by the backup RADIUS accounting server.

SNMP-ID:

2.10.23.20.13

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 5 characters from `[0-9]`

Default-Wert:

0

Backup secret

Enter the key (shared secret) for access to the backup RADIUS accounting server here. Ensure that this key is consistent with that in the accounting server.

SNMP-ID:

2.10.23.20.14

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

Backup-Loopback-Address

Specify a loopback address for the backup RADIUS accounting server.

SNMP-ID:

2.10.23.20.15

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default-Wert:

leer

Backup-Protocol

Use this entry to specify the protocol used to communicate with the backup RADIUS accounting server.

SNMP-ID:

2.10.23.20.16

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

RADIUS
RADSEC

Default-Wert:

RADIUS

Backup attribute values

Here you specify the attribute values for the backup RADIUS accounting server.

SNMP-ID:

2.10.23.20.17

Pfad Telnet:

Setup > **DHCP** > > **RADIUS-Accounting** > **Network-List**

Mögliche Werte:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default-Wert:

leer

12.4 SNMPv3 support

With version 10.12, HiLCOS now supports SNMPv3 to provide the following versions of SNMP:

- SNMPv1
- SNMPv2c
- SNMPv3

12.4.1 Simple Network Management Protocol (SNMP)

The Simple Network Management Protocol (SNMP) enables devices on a network to be monitored and configured from a central instance. Since the initial release of SNMPv1 in 1988, it has continued to evolve with the versions SNMPv2 and SNMPv3 to meet the needs of increasingly complex network infrastructures and the demands for user-friendliness, security and flexibility.

The protocol SNMP (simple network management protocol) meets the highest standards for convenient management and monitoring of a network. It allows for the early detection of problems and errors on a network and offers support in eliminating them. The simple network management protocol allows a central instance to monitor and configure the devices on a network from, and it regulates the communication between the monitored devices and the monitoring station. This means that parameters such as the status of the device, CPU utilization, the temperature of a device, its connection status, errors, and others can be monitored and analyzed with LANmonitor or LSM. The administrator benefits from active support with network management and is helped to detect problems at an early stage. The latest SNMPv3 version of the protocol, in contrast to the previous versions SNMPv1 and SNMPv2, now enables encrypted data communication between the network and its management system, which provides a crucial security factor. By offering different user accounts for authentication, the integrated user administration provides optimal control over access to the configurations. You have precise control over the rights to the different levels of access that administrators receive, and the network is optimally protected.

SNMP components

The typical SNMP architecture consists of three components:

SNMP manager

The SNMP manager sends SNMP requests to the SNMP agent and evaluates the SNMP responses from it. The LCMS tools LANconfig and LANmonitor are SNMP managers of this type. Hirschmann devices comply with the standards SNMPv1, SNMPv2, and SNMPv3, so it is possible to use an alternative SNMP administration and management software.

SNMP agent

The SNMP agent is a module that is active on the managed device. When it receives a request from the SNMP manager, it retrieves the requested status data from the MIB in the device and returns this information to the SNMP manager as an "SNMP response". Depending on the configuration, an SNMP agent that detects certain changes of state in the managed device can independently act to send an "SNMP trap" to the SNMP manager. It is also possible to send a notification to the device administrator by means of a SYSLOG message or an e-mail.

Managed device

The status of this device is stored in its Management Information Base (MIB). When requested by the SNMP agent, the device reads out this information and returns it to the SNMP agent.

By default, SNMP requests and SNMP responses are exchanged between the SNMP manager and SNMP agent by the User Datagram Protocol (UDP) on port 161. SNMP traps are transmitted with the UDP via port 162 by default.

SNMP versions

The differences between the various versions of SNMP can be summarized as follows:

SNMPv1

Version 1 was launched in 1988 and has long been regarded as the de facto standard for network management. In SNMPv1, the SNMP manager authenticates at the SNMP agent by means of a community string, which must be identical on both components. The security of this is very limited, as the community strings are transmitted in cleartext. The increase in demands for secure network communication necessitated a revision of version 1.

SNMPv2

After 1993, the main improvements in version 2 were to its user-friendliness. Numerous intermediate steps and the repeated rejection of concepts eventually led to the version SNMPv2c. This version allows large amounts of data to be requested via a `GetBulkRequest` command and also the communication between SNMP managers. However, the exchange of the community strings was still as cleartext as with version 1.

SNMPv3

From 1999, version 3 finally met the by then much-needed security requirements. Among other things, the communication was encrypted and the communication partners first had to authenticate and authorize themselves. Also, the structure of SNMP became more modular so that improvements, for example in encryption technologies, can be incorporated into SNMPv3, without having to completely redesign the standard.

HiLCOS supports the following SNMP versions:

- SNMPv1
- SNMPv2c
- SNMPv3

SNMPv3 basics

The SNMP protocol structure has changed significantly with version 3. SNMPv3 is now divided into a number of modules with clearly defined interfaces that communicate with one another. The three main elements in SNMPv3 are "Message Processing and Dispatch (MPD)", "User-based Security Model (USM)" and "View-based Access Control Mechanism (VACM)".

MPD

The MPD module is responsible for the processing and dispatch of inbound and outbound SNMP messages.

USM

The USM module manages security features that ensure the authentication of the users and the encryption and integrity of the data. SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in HiLCOS primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly.

VACM

VACM ensures that the sender of an SNMP request is entitled to receive the requested information. The associated access permissions are found in the following settings and parameters:

SNMPv3-Views

"SNMPv3-Views" collect together the content, status messages, and actions of the Management Information Base (MIB) that are permitted to receive or execute an SNMP request. These views can be single values, but also complete paths of the MIB. This content is specified by the OIDs of the MIB entries.

In this way, a successfully authenticated sender of an SNMP request only has access to that data specified in the applicable SNMPv3 views.

SNMPv3-Groups

"SNMPv3-Groups" collect users with the same permissions into a specific group.

Security-Levels

"Security levels" relate to the exchange of SNMP messages. The following levels can be selected:

NoAuth-NoPriv

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

Auth-Priv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Context

"Context" is used to distinguish the various SNMP entities.

Setting up SNMP with LANconfig

In LANconfig you configure SNMP under **Management** > **Admin** in the section **SNMP** and by clicking on **SNMP settings**.

Protocol versions

Here you enable the SNMP versions supported by the device for SNMP requests and SNMP traps.

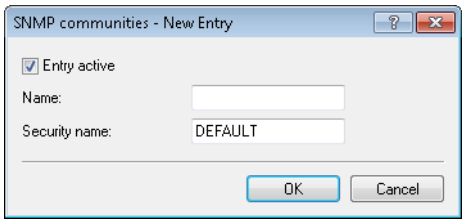
SNMPv3 access settings for administrators

Enable this option if registered administrators should also have access via SNMPv3.

SNMP communities

SNMP agents and SNMP managers belong to SNMP communities. These communities collect certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

This configuration is relevant for the SNMP versions v1 and v2c only.



The SNMP community `public` is set up by default, and this provides unrestricted SNMP read access.

Entry active

Activates or deactivates this SNMP community.

Name

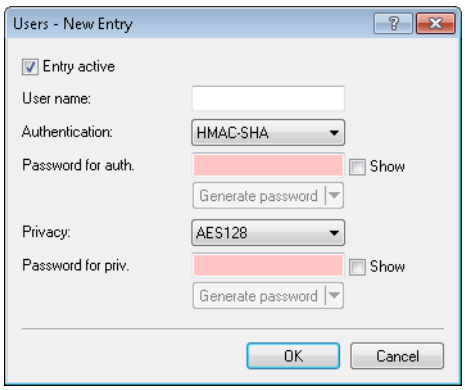
Enter a descriptive name for this SNMP community.

Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

Users

Individual users can be granted access to the device in addition to the administrators registered on it. Here you configure the authentication and encryption settings for these users when operating SNMPv3.



Entry active

Activates or deactivates this user.

User name

Enter a descriptive name for this user.

Authentication

Specify the method that the user is required to use to authenticate at the SNMP agent. The following options are available:

None

Authentication of the user is not necessary.

HMAC-MD5

Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA (default)

Authentication is performed using the hash algorithm HMAC-SHA-96 (hash length 160 bits).

Password for auth.

Enter the user password necessary for authentication here and repeat it in the box below.

Encryption

Specify which encryption method is used for encrypted communication with the user. The following options are available:

None

Communication is not encrypted.

DES

Encryption is performed with DES (key length 56 bits).

AES128 (default)

Encryption is performed with AES128 (key length 128 bits)

AES192

Encryption is performed with AES192 (key length 192 bits)

AES256

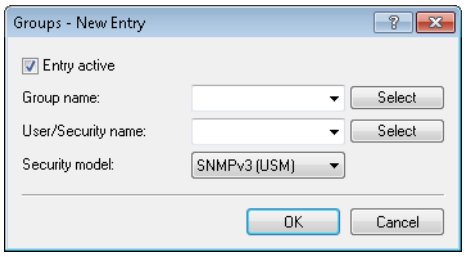
Encryption is performed with AES256 (key length 256 bits)

Password for priv.

Enter the user password required by the encryption here and repeat it in the box below.

Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users. By default, the configuration is set up for SNMP access via LANmonitor.



Entry active

Activates or deactivates this group.

Group name

Enter a descriptive name for this group. You will use this name when you go on to configure the access rights.

User/security name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

Security model

SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in HiLCOS primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly. Select one of the following entries accordingly:

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

SNMPv2

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level "NoAuthNoPriv".

SNMPv3 (USM)

Data is transmitted by SNMPv3. Users can authenticate and communicate according to the following security levels:

NoAuthNoPriv

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

AuthNoPriv

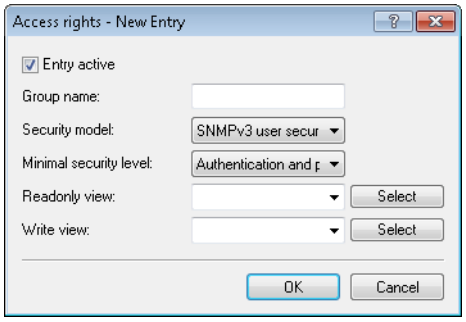
The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is not encrypted.

AuthPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is encrypted by DES or AES algorithms.

Access rights

This table brings together the different configurations for access rights, security models, and views.



Entry active

Activates or deactivates this entry.

Group name

Here you select the name of a group that is to receive these assess rights.

Security model

Activate the appropriate security model here.

Minimal security level

Specify the minimum security level for access and data transfer.

Read-only view

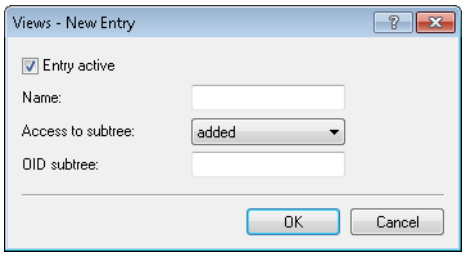
Set the view of the MIB entries for which this group is to receive read rights.

Write view

Set the view of the MIB entries for which this group is to receive write rights.

Views

Here you collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with the corresponding access rights.



Entry active

Activates or deactivates this view.

Name

Give the view a descriptive name here.

Access to subtree

Here you decide whether the OID subtrees specified in the following are “added” or “removed” from the view.

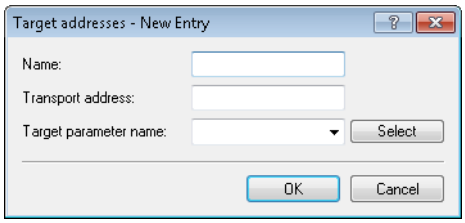
OID subtree

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in this view.

The OIDs are taken from the device MIB, which you can download with WEBconfig under **Extras** > **Get Device SNMP MIB**.

Target addresses

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.



Name

Give the entry a descriptive name here.

Transport address

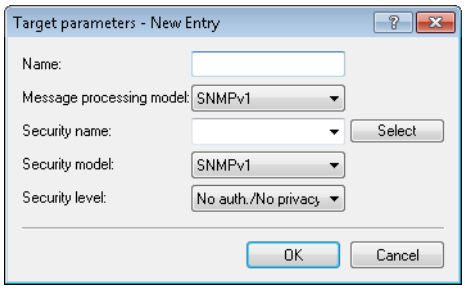
Configure the address of the recipient here.

Target parameter name

Here you select the desired entry from the list of recipient parameters.

Target parameter name

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.



Name

Give the entry a descriptive name here.

Message processing model

Here you specify the protocol for which the SNMP agent structures the message.

Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

Security model

Activate the appropriate security model here.

Security level

Set the security level that applies for the recipient to receive the SNMP trap.

No authentication/No privacy

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

Authentication/No privacy

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

Authentication and privacy

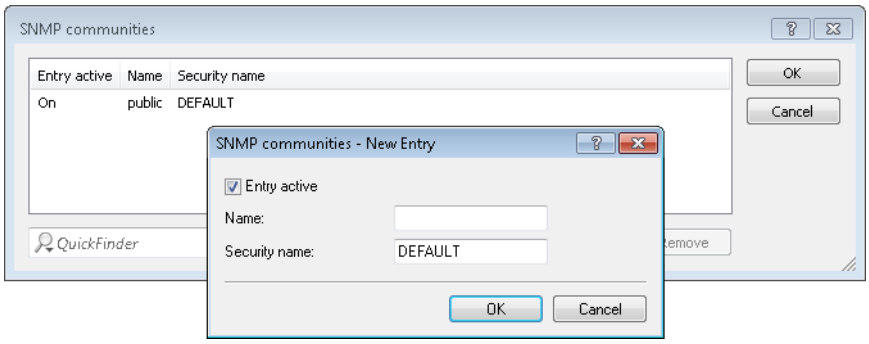
SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

12.4.2 Configuring SNMP read-only access

Administrators of networks with SNMP management systems can precisely control the access rights to various access levels. SNMP of the versions v1 and v2 do this by encoding the access credentials as part of a "community". Authentication is optionally handled

- by the `public` community (unlimited SNMP read access),
- by a master password (limited SNMP read access), or
- a combination of user name and password, separated by a colon (limited SNMP read access)

. By default, your device answers all SNMP requests that it receives from LANmonitor or another SNMP management system with the community `public`. Because this represents a potential security risk, especially with external access, LANconfig gives you the option define your own communities under **Management** > **Admin** and clicking **SNMP settings** and **SNMP communities**.



For SNMPv1 or SNMPv2c, you force the entry of login data for SNMP read-only access by disabling the `public` community in the list of the SNMP communities. This setting only allows information about the state of the device, current connections, reports, etc., to be read out via SNMP after the user authenticates at the device. Authorization can be conducted either with the administrator-account access credentials or an access account created for the individual SNMP community.

Disabling the community `public` has no effect on accessing for other communities created here. An individual SNMP read-only community always provides an alternative access path that is not tied to an administrator account.

SNMP write access is reserved exclusively for administrators with the appropriate permissions.

For more information about SNMP, see the chapter *Simple Network Management Protocol (SNMP)*

12.4.3 Additions to the Setup menu

Communities

SNMP agents and SNMP managers belong to SNMP communities. These communities collect certain SNMP hosts into groups, in part so that it is easier to manage them. On the other hand, SNMP communities offer a certain degree of security because an SNMP agent only accepts SNMP requests from participants in a community that it knows.

This table is used to configure the SNMP communities.

The SNMP community `public` is set up by default, and this provides unrestricted SNMP read access.

SNMP ID:

2.9.27

Telnet path:

Setup > **SNMP**

Name

Enter a descriptive name for this SNMP community.

SNMP ID:

2.9.27.1

Telnet path:

Setup > **SNMP** > **Communities**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Security-Name

Here you enter the name for the access policy that specifies the access rights for all community members.

SNMP ID:

2.9.27.3

Telnet path:

Setup > **SNMP** > **Communities**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Status

This entry is used to enable or disable this SNMP community.

SNMP ID:

2.9.27.8

Telnet path:

Setup > **SNMP** > **Communities**

Possible values:

Active

The community is enabled.

Inactive

The community is disabled.

Default:

Active

Groups

By configuring SNMP groups, it is easy to manage and assign the authentication and access rights of multiple users. By default, the configuration is set up for SNMP access via LANmonitor.

SNMP ID:

2.9.28

Telnet path:

Setup > **SNMP**

Security-Model

SNMPv3 introduced the principle of the "security model", so that the SNMP configuration in HiLCOS primarily uses the security model "SNMPv3". However, for compatibility reasons it may be necessary to also take the versions SNMPv2c or even SNMPv1 into account, and to select these as the "security model" accordingly.

You select a security model here as is appropriate.

SNMP ID:

2.9.28.1

Telnet path:

Setup > **SNMP** > **Groups**

Possible values:

SNMPv1

Data is transmitted by SNMPv1. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “NoAuthNoPriv”.

SNMPv2

Data is transmitted by SNMPv2c. Users are authenticated by the community string in the SNMP message only. Communication is not encrypted. This corresponds to the security level “NoAuthNoPriv”.

SNMPv3(USM)

Data is transmitted by SNMPv3. Users can authenticate and communicate according to the following security levels:

NoAuthNoPriv

The authentication is performed by the specification and evaluation of the user name only. Data communication is not encrypted.

AuthNoPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is not encrypted.

AuthPriv

The authentication is performed with the hash algorithm HMAC-MD5 or HMAC-SHA. Data communication is encrypted by DES or AES algorithms.

Default:

SNMPv3(USM)

Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

SNMP ID:

2.9.28.2

Telnet path:

Setup > **SNMP** > **Groups**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Group-Name

Enter a descriptive name for this group. You will use this name when you go on to configure the access rights.

SNMP ID:

2.9.28.3

Telnet path:

Setup > **SNMP** > **Groups**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Status

Activates or deactivates this group configuration.

SNMP ID:

2.9.28.5

Telnet path:

Setup > **SNMP** > **Groups**

Possible values:

Active
Down

Default:

Active

Access

This table brings together the different configurations for access rights, security models, and views.

SNMP ID:

2.9.29

Telnet path:

Setup > **SNMP**

Group-Name

Here you select the name of a group that is to receive these assess rights.

SNMP ID:

2.9.29.1

Telnet path:

Setup > **SNMP** > **Access**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Security model

Activate the appropriate security model here.

SNMP ID:

2.9.29.3

Telnet path:

Setup > **SNMP** > **Access**

Possible values:

Any
Any model is accepted.

SNMPv1
SNMPv1 is used.

SNMPv2
SNMPv2c is used.

SNMPv3(USM)
SNMPv3 is used.

Default:

Any

Read-View-Name

Set the view of the MIB entries for which this group is to receive read rights.

SNMP ID:

2.9.29.5

Telnet path:

Setup > **SNMP** > **Access**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Write-View-Name

Set the view of the MIB entries for which this group is to receive write rights.

SNMP ID:

2.9.29.6

Telnet path:

Setup > **SNMP** > **SNMPv3-Accesses**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Notify-View-Name

Set the view of the MIB entries for which this group is to receive notify rights.

SNMP ID:

2.9.29.7

Telnet path:

Setup > **SNMP** > **Access**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_.`

Default:

empty

Status

Activates or deactivates this entry.

SNMP ID:

2.9.29.9

Telnet path:

Setup > **SNMP** > **Access**

Possible values:

Active
Down

Default:

Active

Min-Security-Level

Specify the minimum security level for access and data transfer.

SNMP ID:

2.9.29.10

Telnet path:

Setup > **SNMP** > **Access**

Possible values:

NoAuth-NoPriv

The SNMP request is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

Auth-Priv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Default:

Auth-Priv

Views

This table is used to collect the different values or even entire branches of the device MIB, which each user is entitled to view or change in keeping with their corresponding access rights.

SNMP ID:

2.9.30

Telnet path:

Setup > **SNMP**

View-Name

Give the view a descriptive name here.

SNMP ID:

2.9.30.1

Telnet path:

Setup > **SNMP** > **Views**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

OID-Subtree

Use a comma-separated list of the relevant OIDs to decide which values and actions from the MIB are included in this view.

The OIDs are taken from the device MIB, which you can download with WEBconfig under **Extras** > **Get Device SNMP MIB**.

SNMP ID:

2.9.30.2

Telnet path:

Setup > **SNMP** > **Views**

Possible values:

Max. 128 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Type

Here you decide whether the OID subtrees specified in the following are “Included” or “Excluded” from the view.

SNMP ID:

2.9.30.4

Telnet path:

Setup > **SNMP** > **Views**

Possible values:

Included

This setting outputs MIB values.

Excluded

This setting blocks the output of MIB values.

Default:

Included

Status

Activates or deactivates this view.

SNMP ID:

2.9.30.6

Telnet path:

Setup > **SNMP** > **Views**

Possible values:

Active
Down

Default:

Active

SNMPv3-Users

This menu contains the user configuration.

SNMP ID:

2.9.32

Telnet path:

Setup > **SNMP**

User name

Specify the SNMPv3 user name here.

SNMP ID:

2.9.32.2

Telnet path:

Setup > **SNMP** > **SNMPv3-Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Authentication-Protocol

Specify the method that the user is required to use to authenticate at the SNMP agent.

SNMP ID:

2.9.32.5

Telnet path:

Setup > **SNMP** > **Users**

Possible values:

None

Authentication of the user is not necessary.

HMAC-MD5

Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA

Authentication is performed using the hash algorithm HMAC-SHA-96 (hash length 160 bits).

Default:

HMAC-SHA

Authentication-Password

Enter the user password necessary for authentication here and repeat it in the box below.

SNMP ID:

2.9.32.6

Telnet path:

Setup > **SNMP** > **Users**

Possible values:

Max. 40 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Privacy-Protocol

Specify which encryption method is used for encrypted communication with the user.

SNMP ID:

2.9.32.8

Telnet path:

Setup > **SNMP** > **SNMPv3-Users**

Possible values:

None

Communication is not encrypted.

DES

Encryption is performed with DES (key length 56 bits).

AES128

Encryption is performed with AES128 (key length 128 bits).

AES192

Encryption is performed with AES192 (key length 192 bits).

AES256

Encryption is performed with AES256 (key length 256 bits)

Default:

AES128

Privacy-Password

Enter the user password required by the encryption here and repeat it in the box below.

SNMP ID:

2.9.32.9

Telnet path:

Setup > **SNMP** > **Users**

Possible values:

Max. 40 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Status

Activates or deactivates this user.

SNMP ID:

2.9.32.13

Telnet path:

Setup > **SNMP** > **Users**

Possible values:

Active
Down

Default:

Active

SNMPv3-Notifiers

This menu contains the table with the SNMPv3 notifications.

SNMP ID:

2.9.33

Telnet path:

Setup > **SNMP**

Notify-Name

Enter a name for this notifier here.

SNMP ID:

2.9.33.1

Telnet path:

Setup > **SNMP** > **SNMPv3-Notifiers**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Notify-Tag

Enter the notifier tag here.

SNMP ID:

2.9.33.2

Telnet path:

Setup > **SNMP** > **SNMPv3-Notifiers**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Notify-Type

Contains the notification types.

SNMP ID:

2.9.33.3

Telnet path:

Setup > **SNMP** > **SNMPv3-Notifiers**

Possible values:

NOTIFICATION-TRAP

Default:

NOTIFICATION-TRAP

Target-Address

The list of target addresses is used to configure the addresses of the recipients to whom the SNMP agent sends the SNMP traps.

SNMP ID:

2.9.34

Telnet path:

Setup > **SNMP**

Target-Address-Name

Specify the target address name here.

SNMP ID:

2.9.34.1

Telnet path:

Setup > **SNMP** > **Target-Address**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Target-Transport-Address

Contains the IP address which the SNMP traps are sent to.

SNMP ID:

2.9.34.3

Telnet path:

Setup > **SNMP** > **Target-Address**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Target-Tag-List

Contains a tag list for defining target addresses for specific tasks.

SNMP ID:

2.9.34.6

Telnet path:

Setup > **SNMP** > **Target-Address**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Parameters-Name

Here you select the desired entry from the list of recipient parameters.

SNMP ID:

2.9.34.7

Telnet path:

Setup > **SNMP** > **Target-Address**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Target-Params

In this table you configure how the SNMP agent handles the SNMP traps that it sends to the recipient.

SNMP ID:

2.9.35

Telnet path:

Setup > **SNMP**

Name

Give the entry a descriptive name here.

SNMP ID:

2.9.35.1

Telnet path:

Setup > **SNMP** > **Target-Params**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Message-Processing-Model

Here you specify the protocol for which the SNMP agent structures the message.

SNMP ID:

2.9.35.2

Telnet path:

Setup > **SNMP** > **Target-Params**

Possible values:

SNMPv1
SNMPv2c
SNMPv3

Default:

SNMPv3

Security model

Use this entry to specify the security model.

SNMP ID:

2.9.35.3

Telnet path:

Setup > **SNMP** > **Target-Params**

Possible values:

SNMPv1
SNMPv2
SNMPv3(USM)

Default:

SNMPv3(USM)

Security-Name

Here you select a security name you assigned to an SNMP community. It is also possible to specify the name of an existing configured user.

SNMP ID:

2.9.35.4

Telnet path:

Setup > **SNMP** > **Target-Params**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Security-Level

Set the security level that applies for the recipient to receive the SNMP trap.

SNMP ID:

2.9.35.5

Telnet path:

Setup > **SNMP** > **Target-Params**

Possible values:

NoAuth-NoPriv

The SNMP message is valid without the use of specific authentication methods. Authentication merely requires the user to belong to an SNMP community (for SNMPv1 and SNMPv2c) or to specify a valid user name (for SNMPv3). Data transfer is not encrypted.

Auth-NoPriv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, but data transfer is not encrypted.

Auth-Priv

SNMP requests are only processed following authentication by means of the HMAC-MD5 or HMAC-SHA algorithm, and data transfer is encrypted by the DES or AES algorithm.

Default:

NoAuth-NoPriv

Notification-Server-Enable

This entry specifies whether the server notification is enabled or disabled.

SNMP ID:

2.9.36

Telnet path:

Setup > **SNMP**

Possible values:

No

Server notification is disabled.

Yes

Server notification is enabled.

Default:

No

Admitted-Protocols

Here you enable the SNMP versions supported by the device for SNMP requests and SNMP traps.

SNMP ID:

2.9.37

Telnet path:

Setup > **SNMP**

Possible values:

SNMPv1
SNMPv2
SNMPv3

Default:

SNMPv1

SNMPv2

SNMPv3

Allow admins

Enable this option if registered administrators should also have access via SNMPv3.

SNMP-ID:

2.9.38

Pfad Telnet:

Setup > **SNMP**

Mögliche Werte:

No
Yes

Default-Wert:

Yes

SNMPv3-Admin-Authentication

Sets the authorization method for administrators.

This value cannot be modified.

SNMP ID:

2.9.39

Telnet path:

Setup > **SNMP**

Possible values:

AUTH-HMAC-SHA

Default:

AUTH-HMAC-SHA

SNMPv3-Admin-Privacy

Specifies the encryption settings for administrators.

This value cannot be modified.

SNMP ID:

2.9.40

Telnet path:

Setup > **SNMP**

Possible values:

AES256

Default:

AES256

Operating

This entry enables or disables SNMP traps. Clear the checkbox to disable SNMP traps.

SNMP ID:

2.9.41

Telnet path:

Setup > **SNMP**

Possible values:

No
Yes

Default:

Yes

12.5 Logging DNS queries with SYSLOG

As of HiLCOS 10.12, the DNS server on the device sends DNS responses to the clients and also as SYSLOG messages to a SYSLOG server.

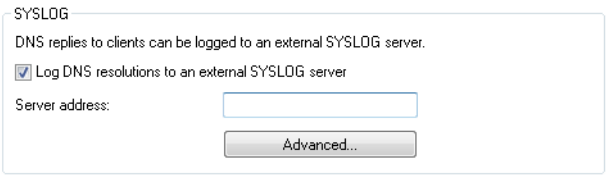
With the move to HiLCOS 10.12, HiLCOS converts existing table entries into the new form. In case you downdate to an earlier HiLCOS version, any changes you make with HiLCOS 10.12 will be lost (e.g. entries for IP addresses). As long as the device configuration remains unchanged since you updated to HiLCOS 10.12, it is possible to downdate to an earlier HiLCOS version without losing data.

12.5.1 Logging DNS queries with SYSLOG

In order to document the requests from the clients to the DNS server in the device, this option allows the server to additionally send its responses to clients as SYSLOG messages to a SYSLOG server on a continual basis.

Please be aware that recording DNS requests must be performed in accordance with the applicable data privacy regulations in your country.

In LANconfig, you configure the documentation of DNS requests under **IPv4** > **DNS** in the section **SYSLOG**.



Log the DNS resolutions on an external SYSLOG server

This option enables or disables (default setting) the sending of SYSLOG messages in the case of DNS requests.

This switch is independent of the global switch in the SYSLOG module under **Log & Trace** > **General** > **SYSLOG**. Thus, if you enable this option to log DNS requests, the DNS server sends the corresponding SYSLOG messages to a SYSLOG server even if the global SYSLOG module is disabled.

Each DNS resolution (`ANSWER` record or `ADDITIONAL` record) generates a SYSLOG message with the following structure `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Resource-Record`.

The parameters have the following meanings:

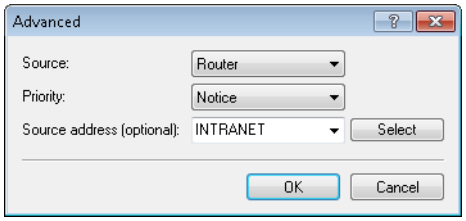
- The `TID` (transaction ID) contains a 4-character hexadecimal code.
- The `{host name}` is only part of the message if the DNS server cannot resolve it without a DNS request (as in the firewall log, as well).
- The `resource record` consists of three parts: The request, the type or class, and the IP resolution (for example `www.mydomain.com STD A resolved to 193.99.144.32`)

Server address

Enter the address of the SYSLOG server. You can enter an IPv4/IPv6 address or a DNS name.

The use of the IP addresses `127.0.0.1` and `::1` to force the use of an external server is not permitted.

To configure the SYSLOG message, click on **Advanced**.



Source

Here you select which source is entered in the SYSLOG messages.

Priority

Here you select the source that is entered in the SYSLOG messages.

Source address (optional)

Here you can optionally specify another address (name or IP) used by your device to identify itself to the SYSLOG server as the sender. By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.

If the source address set here is a loopback address, this will be used **unmasked** even on masked remote clients.

For more information on SYSLOG and the available settings, see the section *The SYSLOG module*.

12.5.2 Additions to the Setup menu

Syslog

Use this directory to configure the SYSLOG logging of DNS requests.

SNMP ID:

2.17.20

Telnet path:

Setup > **DNS**

Log DNS resolutions

This option enables or disables (default setting) the sending of SYSLOG messages in the case of DNS requests.

This switch is independent of the global switch in the SYSLOG module under **Setup** > **SYSLOG** > **Operating**. If you enable this option to log DNS requests, the DNS server in the device sends the corresponding SYSLOG messages to a SYSLOG server even if the global SYSLOG module is disabled.

Each DNS resolution (`ANSWER` record or `ADDITIONAL` record) generates a SYSLOG message with the following structure `PACKET_INFO: DNS for IP-Address, TID {Hostname}: Resource-Record`.

The parameters have the following meanings:

- The `TID` (transaction ID) contains a 4-character hexadecimal code.
- The `{host name}` is only part of the message if the DNS server cannot resolve it without a DNS request (as in the firewall log, as well).
- The `resource record` consists of three parts: The request, the type or class, and the IP resolution (for example `www.mydomain.com STD A resolved to 193.99.144.32`)

SNMP ID:

2.17.20.1

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

No

Disables the logging of DNS requests and responses.

Yes

Enables the logging of DNS requests and responses.

Default:

No

Log server address

The log server address identifies the SYSLOG server by means of its DNS name or an IP address.

The use of the IP addresses `127.0.0.1` and `::1` to force the use of an external server is not permitted.

SNMP ID:

2.17.20.2

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Log source

Contains the log source as displayed in the SYSLOG messages.

SNMP ID:

2.17.20.3

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

System
Login
System time
Console login
Connections
Accounting
Administration
Router

Default:

Router

Log level

Contains the priority that is shown in the SYSLOG messages.

SNMP ID:

2.17.20.4

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

Emergency
Alert
Critical
Error
Warning
Notice
Info
Debug

Default:

Notice

Loopback-Addr.

Here you can optionally specify another address (name or IP) used by your device to identify itself to the SYSLOG server as the sender. By default, your device sends its IP address from the corresponding ARF context, without you having to enter it here. By entering an optional loopback address you change the source address and route that your device uses to contact the remote site. This can be useful, for example, if your device is available over different paths and the remote site should use a specific path for its reply message.

If the source address set here is a loopback address, this will be used **unmasked** even on masked remote clients.

SNMP ID:

2.17.20.5

Telnet path:

Setup > **DNS** > **Syslog**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Special values:

Name of the IP networks whose address should be used
“INT” for the address of the first Intranet
“DMZ” for the address of the first DMZ
LB0 to LBF for the 16 loopback addresses
Any valid IP address

Source

Here you select which source is entered in the SYSLOG messages.

SNMP ID:

2.22.2.3

Telnet path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

None
System
Login
System time
Console login
Connections
Accounting
Administration
Router

Default:

None

Level

Here you select the source that is entered in the SYSLOG messages. Multiple entries can be selected.

SNMP ID:

2.22.2.4

Telnet path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

None
Alert
Error
Warning
Info
Debug

Default:

None

IP address

Contains the IP address of the SYSLOG server. This can be specified as an IPv4 or IPv6 address, or as a DNS name.

SNMP ID:

2.22.2.7

Telnet path:

Setup > **SYSLOG** > **SYSLOG table**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9].-:%`

Facility

The mapping of sources to specific facilities.

SNMP ID:

2.22.3.2

Telnet path:

Setup > **SYSLOG** > **Facility-Mapper**

Possible values:

KERN
USER
MAIL
DAEMON
AUTH
SYSLOG
LPR
NEWS
UUCP
CRON
AUTHPRIV
SYSTEM0
SYSTEM1
SYSTEM2
SYSTEM3
SYSTEM4
LOCAL0
LOCAL1
LOCAL2
LOCAL3
LOCAL4
LOCAL5
LOCAL6
LOCAL7

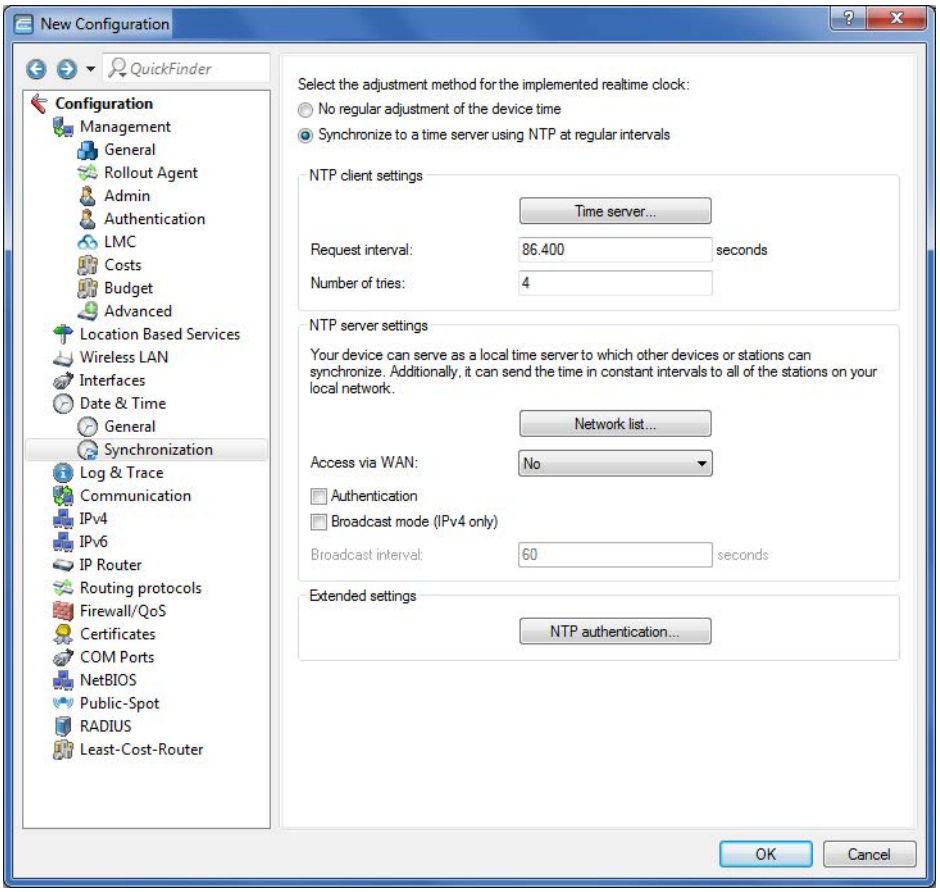
12.6 Time server for the local network

Additional features are available as of HiLCOS 10.12:

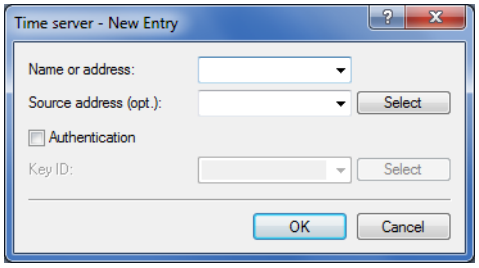
- The NTP server can be activated for each ARF network.
- NTP servers and NTP clients support MD5 authentication.
- Access to the NTP server from the WAN can be enabled or disabled.

12.6.1 Configuration by LANconfig

You configure the new features under **Date & Time** > **Synchronization**.



In the section **NTP client settings**, the **Time server** menu contains two additional parameters.



Authentication

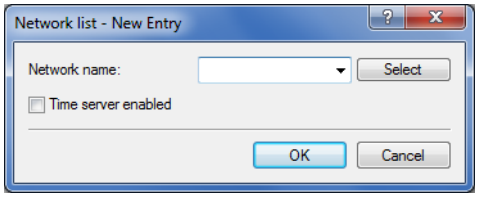
Enables or disables MD5 authentication by the client.

Key-ID

Identifies the key used by the client for MD5 authentication.

New in the section **NTP server settings**:

You can configure the list of networks to which your device forwards the current time under **Network list**.



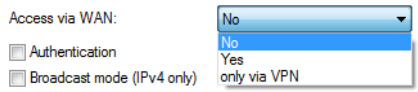
Network name

Specifies the name of the network.

Time server enabled

Determines whether the time server function of your device is activated for the selected network.

WAN access is configured with the selection list **Access via WAN**.



Options:

No

Access to the NTP server from the WAN is disabled.

Yes

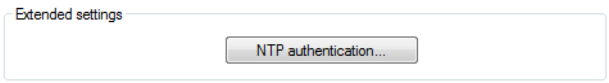
Access from the WAN to the NTP server is possible via unmasked connections, but is in principle not possible with WAN masked connections.

Only via VPN

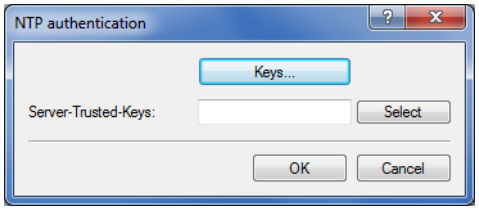
VPN access to the NTP server is enabled.

MD5 authentication support is enabled with **Authentication**.

New section **Extended settings**:

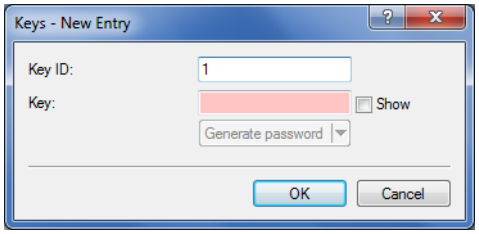


Configure the list of server trusted keys under **NTP authentication**.



The available keys are listed under **Server trusted keys** and are set with the **Select** button.

Keys are edited or added under **Keys**.



12.6.2 Additions to the Setup menu

Authentication

Enables or disables MD5 authentication for the client.

SNMP ID:

2.26.11.3

Telnet path:

Setup > **NTP** > **RQ-Address**

Possible values:

No

Disabled

Yes

Enabled

Default:

No

Key-ID

Identifies the key ID used for the client for MD5 authentication.

SNMP ID:

2.26.11.4

Telnet path:

Setup > **NTP** > **RQ-Address**

Possible values:

1 … 65535

Authentication

Enables or disables MD5 authentication for the server.

SNMP ID:

2.26.13

Telnet path:

Setup > **NTP**

Possible values:

No

Disabled

Yes

Enabled

Default:

No

Key

Configures the table **Authentication-Keys**.

SNMP ID:

2.26.14

Telnet path:

Setup > **NTP**

Key-ID

Identifies the key ID used for the server for MD5 authentication.

SNMP ID:

2.26.14.1

Telnet path:

Setup > **NTP** > **Authentication-Keys**

Possible values:

1 … 65535

Key

This entry contains the value of the key.

SNMP ID:

2.26.14.2

Telnet path:

Setup > **NTP** > **Authentication-Keys**

Possible values:

64 characters from `[A-Z@{|}~!$%&'()+-,/:;<=>?[\]^_.0-9]`

Server-Trusted-Keys

Contains the list of trusted keys (comma-separated list of key numbers).

SNMP ID:

2.26.15

Telnet path:

Setup > **NTP**

Possible values:

Max. 63 characters from `[0-9,]`

Network list

This list contains the networks that your device uses as a time server.

SNMP ID:

2.26.16

Telnet path:

Setup > **NTP**

Network name

Defines the name of the network on which the NTP server is to be activated.

SNMP ID:

2.26.16.1

Telnet path:

Setup > **NTP** > **Networklist**

Possible values:

Entries from Setup/TCP-IP/Networklist: Characters from
`[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Server-Operating

Defines whether the NTP server is enabled on the selected network.

SNMP ID:

2.26.16.2

Telnet path:

Setup > **NTP** > **Networklist**

Possible values:

No
Disabled

Yes
Enabled

Default:

No

Server-WAN-Access

Configures WAN access to your device.

SNMP ID:

2.26.17

Telnet path:

Setup > **NTP**

Possible values:

No

Disables access to the NTP server from the WAN.

Yes

Access from the WAN to the NTP server is possible via unmasked connections, but is in principle not possible with masked connections.

VPN

VPN access to the NTP server is enabled.

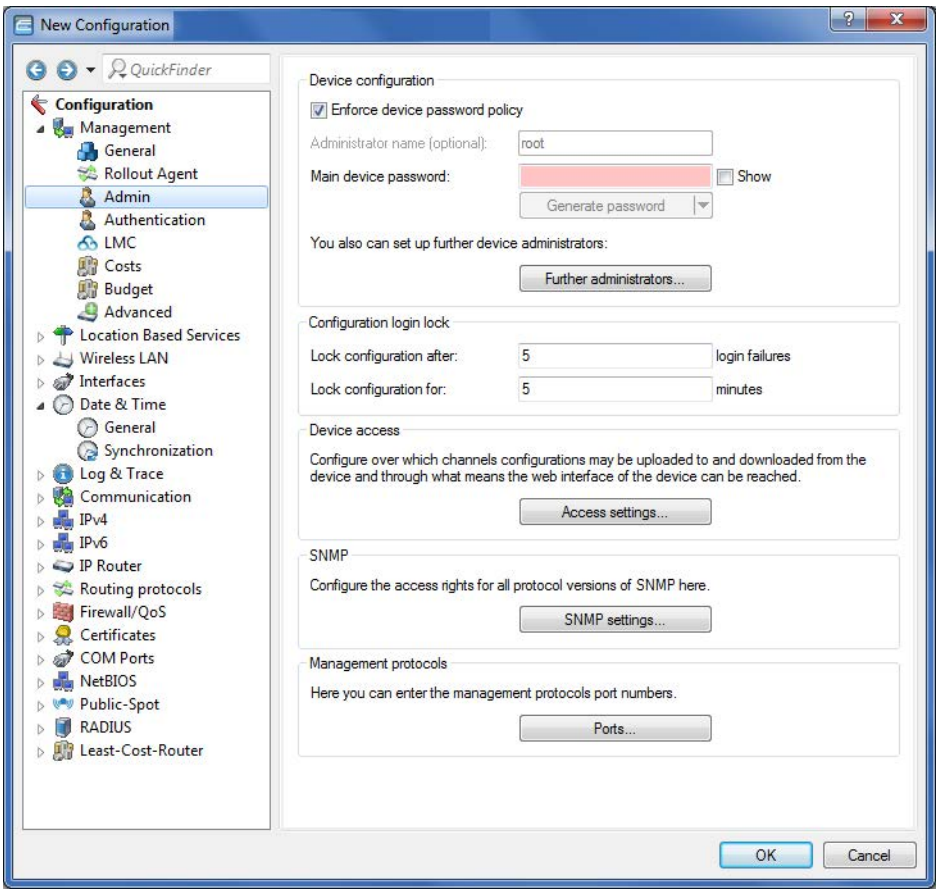
12.7 Simple Network Management Protocol (SNMP)

As of HiLCOS 10.12, SNMPv3 users can make use of additional authentication algorithms.

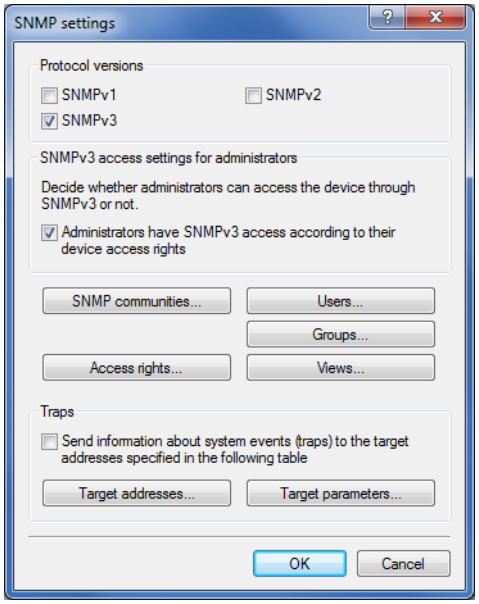
This means a further improvement to security.

12.7.1 Setting up SNMP with LANconfig

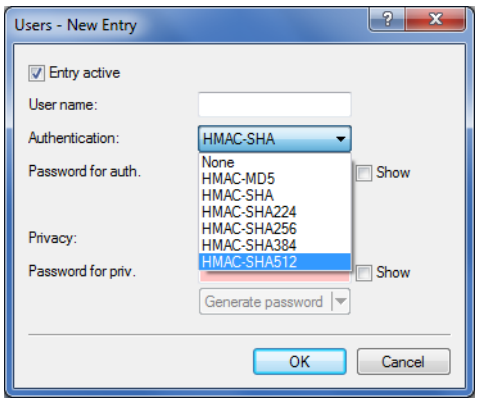
You configure the new features under **Management** > **Admin** > **SNMP**



in the menu **SNMP settings**.



The **Users** menu contains the **Authentication** selection list.



The new authentication algorithms:

HMAC-SHA224

Authentication is performed using the hash algorithm HMAC-SHA-224 (hash length 224 bits).

HMAC-SHA256

Authentication is performed using the hash algorithm HMAC-SHA-256 (hash length 256 bits).

HMAC-SHA384

Authentication is performed using the hash algorithm HMAC-SHA-384 (hash length 384 bits).

HMAC-SHA512

Authentication is performed using the hash algorithm HMAC-SHA-512 (hash length 512 bits).

12.7.2 Additions to the Setup menu

Authentication-Protocol

Specify the method that the user is required to use to authenticate at the SNMP agent.

As of HiLCOS 10.12, you can use hash algorithms with a hash length of 224 bits and more.

SNMP ID:

2.9.32.5

Telnet path:

Setup > **SNMP** > **Users**

Possible values:

None

Authentication of the user is not necessary.

HMAC-MD5

Authentication is performed using the hash algorithm HMAC-MD5-96 (hash length 128 bits).

HMAC-SHA

Authentication is performed using the hash algorithm HMAC-SHA-96 (hash length 160 bits).

HMAC-SHA224

Authentication is performed using the hash algorithm HMAC-SHA-224 (hash length 224 bits).

HMAC-SHA256

Authentication is performed using the hash algorithm HMAC-SHA-256 (hash length 256 bits).

HMAC-SHA384

Authentication is performed using the hash algorithm HMAC-SHA-384 (hash length 384 bits).

HMAC-SHA512

Authentication is performed using the hash algorithm HMAC-SHA-512 (hash length 512 bits).

Default:

HMAC-SHA

13 Appendix

13.1 CRON syntax

A CRON job consists of six fields:

```
minute    hour    day of month    month    day of week    command
```

The asterisk '*' serves as a placeholder for all permitted characters.

Here are some examples of performing regular restarts with the use of CRON:

Every day at 13:30h:

```
30        13        *         *         *        restart
```

Every day 30 minutes past each hour:

```
30        *         *         *         *        restart
```

Every 30 minutes every day:

```
*/30      *         *         *         *        restart
```

Every Saturday at 20:15h:

```
15        20        *         *         6        restart
```

Sundays is selected either with '0' or '7'.

At 00:00h on the first day of the month

```
0         0         1         *         *        restart
```

HIRSCHMANN
A BELDEN BRAND

Addendum
HiLCOS Rel. 10.32

1 Addendum to HiLCOS Rel. 10.32.....5

2 Configuration..... 5

2.1 Configuration software.....5

2.1.1 Automatic redirection of WEBconfig access to HTTPS.....5

2.1.2 Commands for the CLI..... 6

2.1.3 WEBconfig with TLS 1.3.....8

2.1.4 Commands for the CLI.....8

2.2 Managing rights for different administrators.....10

2.2.2 Improved protection of the device configuration against unwanted changes..... 10

3 Routing and WAN connections.....11

3.1 Advanced Routing and Forwarding (ARF).....11

3.1.1 Routing tags for DNS forwarding..... 11

3.2 Locator / ID Separation Protocol (LISP).....13

3.2.1 Configuration.....14

3.2.2 LISP tutorial.....20

3.2.3 Additions to the Setup menu.....23

3.3 Route redistribution of LISP and RIP routes in BGP.....40

3.3.1 Additions to the Setup menu.....41

3.4 BGP: Setting administrative distance by policy.....43

3.4.1 Additions to the Setup menu.....43

3.5 DSLoL for WLAN routers.....43

3.6 Filter list for redistribution in BGP.....45

3.6.1 Additions to the Setup menu.....47

3.7 BGP: Switch for default route propagation.....51

3.7.1 Additions to the Setup menu.....51

4 IPv6.....52

4.1 IPv6 WAN interface.....52

4.1.1 Additions to the Setup menu.....52

4.2 DHCPv6.....56

4.2.1 DHCPv6 server..... 56

5 Firewall.....59

5.1 WAN policy-based NAT.....59

5.1.1 Configuring policy-based NAT with firewall rules.....59

5.2 SD-WAN application routing / Layer-7 application control.....63

5.2.1 Configuration.....64

5.2.2 Additions to the Setup menu.....66

6 Wireless LAN – WLAN....70
6.1 WLAN encryption settings moved to the logical WLAN settings....70
6.2 WPA3 (Wi-Fi Protected Access 3)....70
6.2.1 WPA3-Personal....71
6.2.2 WPA3-Enterprise....71
6.2.3 WPA3 device support....72
6.2.4 Additions to the Setup menu....73
6.3 Enhanced Open....75
6.3.1 Enhanced Open Transitional mode....76
6.3.2 Additions to the Setup menu....77
6.4 Enhanced Passphrase Security (LEPS)....78
6.4.1 Enhanced Passphrase Security User (LEPS-U)....79
6.4.2 Enhanced Passphrase Security MAC (LEPS-MAC)....81
6.4.3 Additions to the Setup menu....82
6.5 Client Management....91
6.5.1 Configuration of Client Management....92
6.5.2 Additions to the Setup menu....95
6.6 Return to the original 5 GHz channel when preference is configured....105
6.7 Reduction of sensitivity for received packets....105
6.7.1 Additions to the Setup menu....106
6.8 Separate switch to enable e-mail notification....108
6.8.1 Additions to the Setup menu....109
6.9 IEEE 802.11k Roaming Targets....109
6.9.1 Additions to the Setup menu....110
6.10 Setting target EIRP....111
6.10.1 Additions to the Setup menu....112

7 WLAN management....114
7.1 WLC features in the Hirschmann BAT-Controller Virtual....114
7.2 New mode for antenna gain....114
7.2.1 Additions to the Setup menu....115

8 Virtual Private Networks – VPN....117
8.1 OCSP server....117
8.1.1 Configuring the OCSP server....117
8.1.2 Additions to the Setup menu....119
8.2 Layer-3 Ethernet tunnel with Layer-2 Tunneling Protocol version 3 (L2TPv3)....123
8.2.1 Configuring a WLAN scenario for bridging payload data to the central site....125
8.2.2 Additions to the Setup menu....128

8.3 IKEv2....130
8.3.1 Configuring IKEv2 with LANconfig....130
8.3.2 Elliptic Curve Digital Signature Algorithm (ECDSA)....134
8.3.3 IKEv2 configuration payload with a specified source for prefix delegation....135
8.3.4 Split DNS....136
8.3.5 IKEv2 fragmentation....137
8.3.6 8.3.6 IKEv2 password rules....137
8.3.7 Additions to the Setup menu....137

9 Public Spot....146

9.1 Setting up a secure hotspot with Enhanced Open....146
9.2 User list removed....147

10 RADIUS....148

10.1 Importing and exporting RADIUS user data by CSV file....148
10.1.1 Exporting RADIUS user data by CSV file....148
10.1.2 Importing RADIUS user data by CSV file....148
10.2 User-defined attributes for RADIUS users in the RADIUS server....150
10.2.1 Additions to the Setup menu....150

11 Other services....152

11.1 Automatic IP address administration with DHCP....152
11.1.1 Configuring DHCPv4 parameters with LANconfig....152
11.2 DHCP server – suppress ARP request....160
11.2.1 Additions to the Setup menu....160
11.3 Simple Network Management Protocol (SNMP)....161
11.3.1 SNMPv3 Password Rules....161
11.3.2 Additions to the Setup menu....161
11.4 TACACS+....29
11.4.1 Configuring the TACACS+ server 162

12 Quality of Service....164

12.1 Configurable DSCP tags for internal Hirschmann services....164
12.1.1 Additions to the Setup menu....164

1 Addendum to HiLCOS Rel. 10.32

This document describes the changes and enhancements in HiLCOS Rel. 10.32 since the previous release.

2 Configuration

2.1 Configuration software

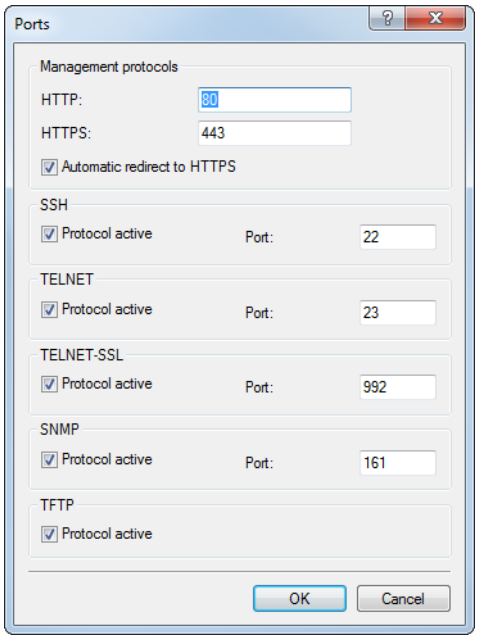
2.1.1 Automatic redirection of WEBconfig access to HTTPS

From HiLCOS Rel. 10.32, unencrypted connection requests received by WEBconfig are automatically switched to encrypted HTTPS connections.

This improves the security when the user wishes to configure the device via WEBconfig and enters the IP address or name into the browser address bar. The browser would normally establish an unencrypted HTTP connection.

The usual way to establish an encrypted HTTPS connection is to explicitly enter the prefix `https://` into the browser. This change makes it easier to enter the address and, at the same time, confidential data such as the login password or the configuration itself are secured by the encrypted connection.

This feature is always switched on in new configurations. Existing configurations will not be changed automatically. In these cases you can enable the function under **Management** > **Admin** > **Management protocols** > **Ports** > **Automatic redirect to HTTPS**.



Additions to the Setup menu

Automatic-Redirect-to-HTTPS

This switch determines whether the WEBconfig login dialog receiving an unencrypted connection request automatically switches to an encrypted HTTPS connection. This is always switched on in new configurations. Existing configurations will not be changed.

SNMP ID:

2.21.24

Telnet path:

Setup > **HTTP**

Possible values:

No

WEBconfig does not automatically switch to an encrypted connection upon receiving an unencrypted connection request.

Yes

WEBconfig automatically switches to an encrypted connection upon receiving an unencrypted connection request.

Default:

Yes

2.1.2 Commands for the CLI

As of HiLCOS Rel. 10.32 your device supports the new commands or options as follows.

Table 1: Overview of new commands available at the command line

Command	Description
`find <term>`	Looks for the search <term> and outputs all menu items containing it.
`lig [[-i <instance>] | [-m <server>]] [-id <num>] destination-eid [-retries <num>] [-rtg-tag <num>] [-source-eid <num>]`	LIG (Locator/ID Separation Protocol Internet Groper) is a command-line tool specified in RFC 6835 to query LISP mappings on a map resolver. Possible arguments are: › `-i <instance>`: Name of the LISP instance used for the destination query › `-m <server>`: LISP map server used for the destination query › `-id <num>`: LISP Instance ID [0-16777215] used for the destination query › `destination-eid`: Requested destination EID › `-retries <num>`: LISP retries to the map server [0-10] › `-rtg-tag <num>`: Routing tag used › `-source-eid <num>`: Source EID used Example: `lig -i LISP-INST 172.16.200.1`
`readscript [-n] [-d] [-i] [-c] [-m] [-h] [-s <password>] [-o]`	The readscript command generates a text dump of all commands and parameters required to configure the device in its current state. The following option switch is new: › `-o`: Replaces the passwords with a "*" to obfuscate them in the text output. **Access rights**: Supervisor-Read
`show admin-distance`	Shows the administrative (routing) distance of all internal applications or routing protocols. **Access rights**: Supervisor-Read, Local-Admin-Read
`show ip-addresses`	Displays all IPv4 and IPv6 addresses for the device for the LAN and WAN interfaces, along with advanced status information. **Access rights**: Supervisor-Read, Local-Admin-Read

Command	Description
`show ipv4-addresses`	Displays all IPv4 addresses for the device for the LAN and WAN interfaces, along with advanced status information. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp instance`	Displays status information about all configured LISP instances. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp instance [instance]`	Displays status information about the LISP instance named [instance]. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp map-cache`	Displays status information about the map cache entries available for all instances. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp map-cache [instance]`	Displays status information about the map cache entries for the instance named [instance]. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp registrations`	Displays status information about the EIDs/RLOCs of all instances registered with the map server. **Access rights**: Supervisor-Read, Local-Admin-Read
`show lisp registrations [instance]`	Displays status information about the EIDs/RLOCs of the instance named [instance] registered with the map server. **Access rights**: Supervisor-Read, Local-Admin-Read
`show VLAN`	Other HiLCOS modules can at runtime instruct the VLAN module to add further VLANs and VLAN memberships to the static configuration. This is used by CAPWAP or WLAN/802.1X, for example. The `show` command now displays this with the new option `VLAN`. **Access rights**: Supervisor-Read, Local-Admin-Read
`ssldefaults [-y]`	This command resets the SSL / TLS settings in all submenus of the current configuration to the default values after a security prompt. In HiLCOS, each module comes with its own submenu for SSL / TLS settings. This provides a way to reset all settings in these various submenus to the current secure default settings. The parameter `-y` ensures that the security prompt is automatically answered so that the command can be used non-interactively in scripts.

2.1.3 WEBconfig with TLS 1.3

As of HiLCOS 10.32 your device supports TLS 1.3 for accessing WEBconfig. TLS 1.3 represents the latest advancement of the TLS standard and offers, for example, the exclusive use of state-of-the-art cipher suites and Perfect Forward Secrecy to provide improved security compared to previous versions.

An HiLCOS update automatically supplements the configuration with TLS 1.3 support for WEBconfig. If necessary, remove older methods that should no longer be available for WEBconfig.

Additions to the Setup menu

Versions

This bitmask specifies which versions of the protocol are allowed.

SNMP ID:

2.21.40.3

Telnet path:

Setup > **HTTP** > **SSL**

Possible values:

SSLv3
TLSv1
TLSv1.1
TLSv1.2
TLSv1.3

Default:

TLSv1.2

TLSv1.3

2.1.4 Commands for the CLI

As of HiLCOS 10.32 your device supports the following new commands and

options. **Table 1: Overview of all new commands on the CLI**

Command	Description
`clear`	Clears the current CLI output. All previously entered commands can be viewed by means of the log.

New ping command options

As of HiLCOS 10.32 your device supports the following new parameters for the ping

Parameter	Meaning
`-b`	Do not stop pinging when a PacketTooBig (DF) is received, to ensure you have "Path MTU Discovery".
`[-x x]`	Atomic fragments: (n)ever, (f)orce, (a)utomatic
`%scope`	Name of the interface used to send the packet when link-local addresses are used as the destination.
`%scope@rtg-tag`	Name of the interface used to send the packet when link-local addresses are used as the destination, with additional specification of the routing tag.
`%%interface`	Name of the destination interface. The packet is sent directly to the interface without taking the routing table into account.
`@rtg-tag`	Routing tag used to send the packet.

2.2 Managing rights for different administrators

2.2.1 Improved protection of the device configuration against unwanted changes

From HiLCOS 10.32, access to the table **Configuration** > **Management** > **Admin** > **Further administrators** is only possible for the root administrator. This is no longer possible for other administrators configured in this table, even if their 'Access rights' are configured as "All".

On the CLI, this change means that the table is no longer visible to other administrators. Reading out the file with "readscript" is also no longer possible. If another administrator tries to access the table with a script, the corresponding script lines are not executed and a "Script Error" is issued.

The cron table works with the user configured for it, meaning that if the commands "loadconfig/loadscript" are executed via the cron table, they will only be able to read the configuration completely if they are run with the root administrator.

The table is still displayed in LANconfig, but it is shown as empty if accessed by another administrator. Changes are not written back to the device.

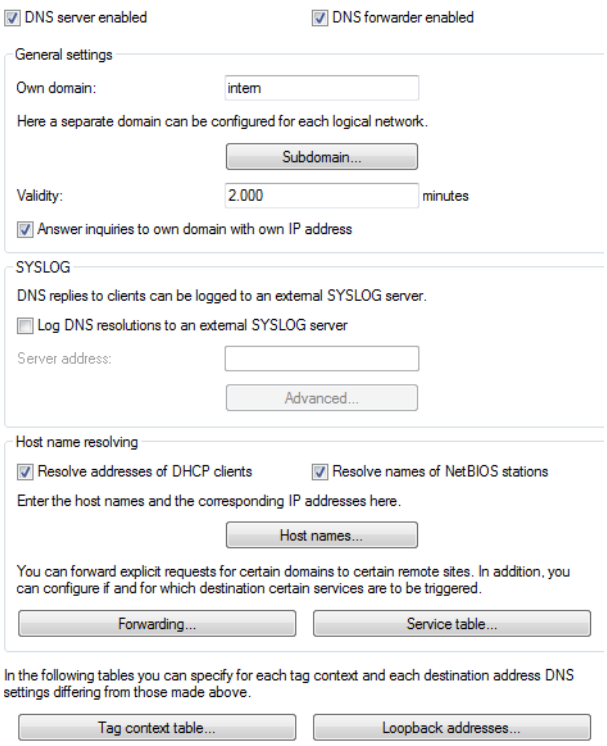
SNMP access (read/write) to this table has been deprecated as a part of this feature.

3 Routing and WAN connections

3.1 Advanced Routing and Forwarding (ARF)

3.1.1 Routing tags for DNS forwarding

With DNS forwarding, it is possible to set up multiple forwarding definitions (especially general wildcard definitions with "*") that are independent of one another by marking them with unique routing tags. Depending on the routing context of the requesting client, the router considers only those forwarding entries that are correspondingly tagged and any general entries that are marked with "0".

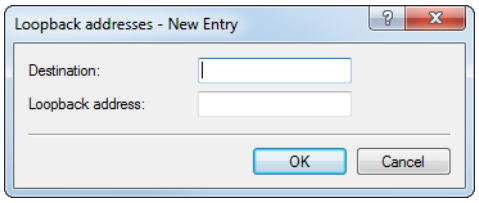


From HiLCOS 10.32, each destination for DNS forwarding can be given a specific loopback address.

Loopback addresses

LANconfig allows loopback addresses to be specified for every remote site under **IPv4** > **DNS** > **Loopback addresses**. Consequently, there is an adjustable sender address for DNS forwarding. Each loopback address consists of exactly one

remote site and loopback address. Since only one remote site can be entered per loopback address, two entries are required here if the DNS Destinations have been configured with two remote sites for one domain.



The following options are possible for each loopback address:

Destination

The remote site for a loopback address. This is either an interface name, an IPv4 or IPv6 address. A routing tag can be added after an "@". The remote site must also be in the DNS Destinations table.

Source address

The loopback address for a specific remote site. This is either an interface name, an IPv4 or IPv6 address or a known loopback address.

Additions to the Setup menu

Loopback-Addresses

This table allows you to store loopback addresses for each remote site. This means that there is an adjustable sender address for DNS forwarding. Each loopback address consists of exactly one remote site and loopback address. The remote site must also be in the DNS Destinations table. Since only one remote site can be entered per loopback address, two entries are required here if the DNS Destinations have been configured with two remote sites for one domain.

SNMP ID:

2.17.17

Telnet path:

Setup > **DNS**

Destination

The remote site as part of a loopback address. This is either an interface name, an IPv4 or IPv6 address. A routing tag can be added after an @. The remote site must also be in the DNS Destinations table.

SNMP ID:

2.17.17.1

Telnet path:

Setup > **DNS** > **Loopback-Addresses**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Loopback address

The loopback address for a specific remote site. This is either an interface name, an IPv4 or IPv6 address or a known loopback address.

SNMP ID:

2.17.17.2

Telnet path:

Setup > **DNS** > **Loopback-Addresses**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

3.2 Locator / ID Separation Protocol (LISP)

As of version 10.32, HiLCOS features LISP.

The Locator/ID Separation Protocol (LISP) as per RFC 6830 is a new routing architecture that splits an IP address into two entities: The routing locator (RLOC) and the endpoint identifier (EID). The goal is to achieve a highly scalable routing architecture with integrated routing, tunneling and overlay protocols.

Conventional routing protocols such as RIP, OSPF or BGP work according to the "push principle" and proactively distribute their best routes to their neighbors. This architecture is of limited scalability, as the ever larger BGP tables and routing tables increasingly become a challenge.

LISP works according to the "pull principle" and works much like the Domain Name System (DNS). LISP routers register their networks, referred to as endpoint identifiers (EIDs), at a central instance called a map server or map resolver. Along with the EID, they also register their global (WAN) address, called the routing locator (RLOC). This keeps the information about the location (locator) separate from the identity (ID).

If a router wants to transfer data to a remote LISP network, first the LISP map resolver is queried for the mappings between the requested EID prefix and the routing locator. In the next step, a data tunnel is established between the two LISP routers.

LISP currently does not provide encryption of the data tunnel and, when used in insecure networks such as the Internet, it is typically combined with VPN. Application scenarios for LISP are multi-VPNs.

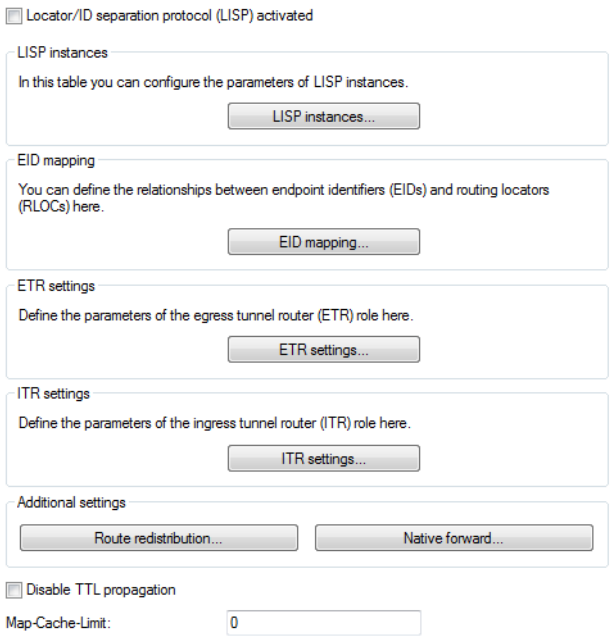
HiLCOS 10.32 supports the following roles:

- Ingress tunnel router (ITR)
- Egress tunnel router (ETR)

The role of the map server/map resolver is currently not supported.

3.2.1 Configuration

LISP routing is configured in LANconfig under **Routing protocols** > **LISP**. The switch **Locator/ID separation protocol (LISP) activated** is used to switch this routing protocol on or off.



Disable TTL propagation

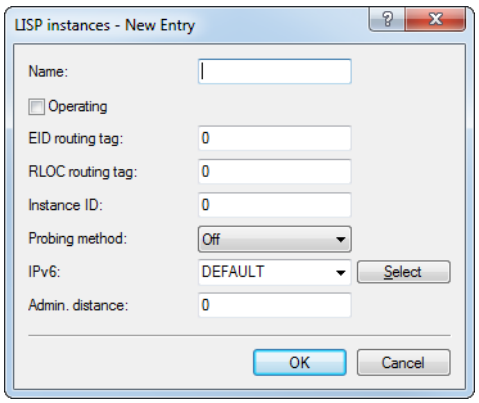
When enabled, the ITR does not copy the Time-To-Live (TTL) from the outer to the inner header. As a result, a client running traceroute sees the LISP tunnel as a hop. If disabled, traceroute shows all of the hops between ITR and ETR.

Map-Cache-Limit

Defines the maximum number of map-cache entries across all LISP instances. After reaching the limit, new entries are rejected. Only after older entries in the map cache have become invalid will new entries be accepted. 0 means there is no restriction.

LISP instances

This table contains the global configuration of the LISP instances on the device.



Name

Specifies a unique name for a LISP instance. This name is referenced in other LISP tables.

Entry active

Activates or deactivates this LISP instance.

EID routing tag

Routing tag of the endpoint identifier (EID) of this instance.

RLOC routing tag

Routing tag of the routing locator (RLOC) of this instance.

Instance ID

LISP instance ID as a numeric tag from RFC 8060 (LISP Canonical Address Format (LCAF)) for the segmentation of networks with ARF.

Probing method

Specifies the method used to periodically check the accessibility of the RLOCs for map cache entries. Available methods:

- Off: The availability of the RLOCs is not checked periodically.
- RLOC probing: The availability of the RLOCs is periodically checked by LISP RLOC messages.

IPv6

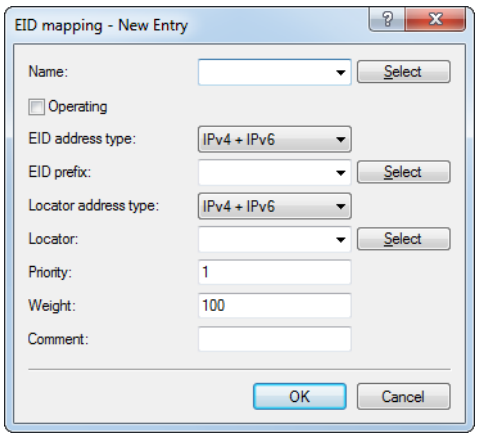
Name of the IPv6 WAN profile from the IPv6 WAN interface table. An entry is required if IPv6 EIDs are used.

Administrative distance

The administrative distance of this LISP instance.

EID mapping

This table specifies the mapping of EIDs to RLOCs to be registered with the map server.



Name

References the name of the LISP instance.

Operating

Activates or deactivates this EID mapping.

EID address type

Protocol version of the EID prefix when referencing the EID prefix via an interface or network name. Possible values:

- **IPv4**: Only the IPv4 prefix of the referenced interface is used.
- **IPv6**: Only the IPv6 prefix of the referenced interface is used.
- **IPv4+IPv6**: Both the IPv4 prefix and the IPv6 prefix of the referenced interface are used.

EID prefix

EID prefix of the EID mapping. Possible values are an IPv4 network name or an IPv6 interface, e.g. INTRANET, or a named loopback address.

Locator address type

Protocol version of the RLOC when referencing the EID prefix via an interface name. Possible values:

- **IPv4**: Only the IPv4 address is used as the RLOC of the referenced interface.
- **IPv6**: Only the IPv6 address is used as the RLOC of the referenced interface.
- **IPv4+IPv6**: Both the IPv4 address and the IPv6 address are used as the RLOC of the referenced interface.

Locator

RLOC of the EID mapping. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

Priority

The priority of the EID mapping. Default: 1.

Weight

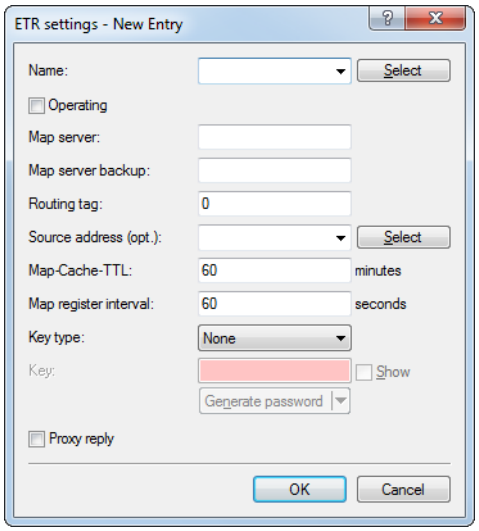
The weight of the EID mapping. Default: 100.

Comment

Enter a descriptive comment for this entry.

ETR settings

This table specifies the parameters for the role as Egress Tunnel Router (ETR).



Name

References the name of the LISP instance.

Operating

Activates or deactivates these ETR settings.

Map-Server

IPv4 or IPv6 address of the LISP map server

Map-Server-Backup

IPv4 or IPv6 address of the LISP backup map server. The LISP registration is sent in parallel both to the primary map server and to the backup map server.

Routing tag

Routing tag to be used to access the map server.

Source address (opt.)

Contains the sender address as the named interface that is used with the map server in LISP communication.

Map-Cache-TTL

Time-to-live of the EID mappings in minutes registered with the map server.

Map register interval

Registration interval in seconds in which map registrations are sent to the map server.

Key type

Algorithm used for authentication at the map server. Possible values:

- None
- HMAC-SHA-1-96
- HMAC-SHA-256-128

Key

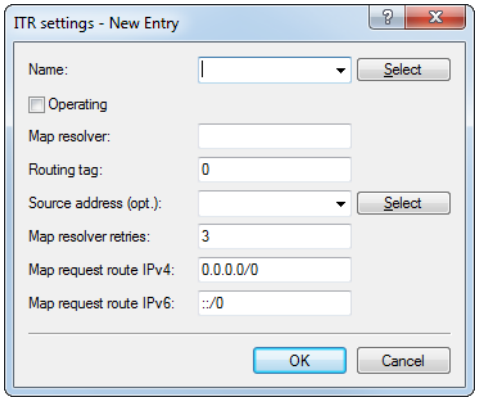
Key or password used to register the EID mapping on the map server.

Proxy-Reply

Determines whether the proxy reply bit is set in map registrations. In this case, the map server acts as a proxy and responds to map requests on behalf of the ETR.

ITR settings

This table specifies the parameters for the role as Ingress Tunnel Router (ITR).



Name

References the name of the LISP instance.

Operating

Activates or deactivates these ITR settings.

Map-Resolver

IPv4 or IPv6 address of the LISP map resolver.

Routing tag

Routing tag used to access the map resolver.

Source address (opt.)

Contains the sender address as the named interface that is used with the map resolver in LISP communication.

Map-Resolver-Retries

Number of retries for map requests to the map resolver. Default: 3

Map-Request-Route-IPv4

Specifies the IPv4 route or prefix for the LISP map requests.

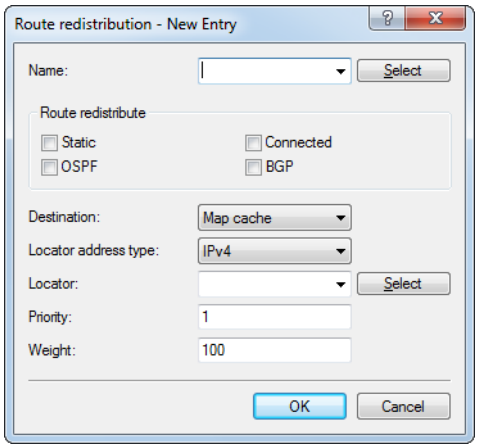
Map-Request-Route-IPv6

Specifies the IPv6 route or prefix for the LISP map requests.

Route redistribution

The redistribution of routes allows routes from the routing table to be imported into the LISP map cache. Map requests are performed for these routes.

Route redistribution also allows routes to be imported from the routing table and dynamically registered to the map server as an EID prefix.



Name

References the name of the LISP instance.

Route redistribute

Specifies the route sources of the imported routes.

- **Static**: The device imports static routes from the routing table into the LISP map cache or into the EID table as an EID prefix.
- **Connected**: From directly connected networks, the device imports information from the routing table into the LISP map cache or into the EID table as an EID prefix.
- **OSPF**: The device imports OSPF routes from the routing table into the LISP map cache or into the EID table as an EID prefix.
- **BGP**: The device imports BGP routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

Destination

Specifies the destination of routes imported to LISP. Possible values:

- **Map cache**: Imports the routes into the map cache. LISP performs map requests for these routes.

- **EID table**: Import the routes into the LISP EID table. These routes are registered with the map server as an EID prefix with the configured RLOC.

Locator address type

Protocol version of the RLOC when referencing the EID prefix via an interface name. Possible values:

- **IPv4**: Only the IPv4 address is used as the RLOC of the referenced interface.
- **IPv6**: Only the IPv6 address is used as the RLOC of the referenced interface.
- **IPv4+IPv6**: Both the IPv4 address and the IPv6 address are used as the RLOC of the referenced interface.

Locator

Specifies the RLOC used to register the imported EID prefixes with the map server. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

Priority

The priority. Default: 1

Weight

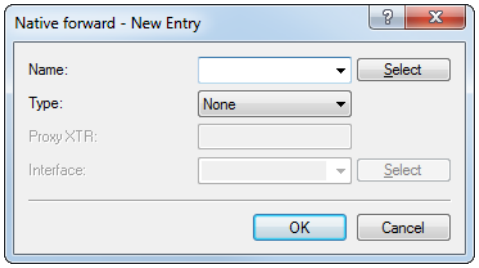
The weight. Default: 100

Native forward

If LISP networks are to communicate with non-LISP networks, proxy routers can be used. These roles are referred to as proxy ingress tunnel routers (proxy ITRs) and proxy egress tunnel routers (proxy ETRs).

If a LISP router receives a negative response from the map resolver, i.e. there is no mapping between the requested EID and an RLOC, the LISP router can either send the associated packets to a proxy xTR (packet with LISP header) or send it via another local interface (packet without LISP header).

HiLCOS only supports scenarios where PITR and PETR functions are operated on the same router.



Name

References the name of the LISP instance.

Type

Defines how to send packets to non-LISP networks.

- **None**: Packets to non-LISP networks are not forwarded but dropped
- **Proxy XTR**: Packets to non-LISP networks are sent to a ProxyXTR
- **Interface**: Packets to non-LISP networks are sent via a local interface

Proxy XTR

IPv4 or IPv6 address of the proxy XTR used to send packets to non-LISP networks.

Interface

Name of the interface used to send packets to non-LISP networks.

3.2.2 LISP tutorial

In this tutorial we will configure a LISP network on the basis of an ARF network that is named INTRANET and uses tag 1. This involves registering the network prefix as an EID prefix with the MAP server 1.1.1.1. Registration is performed via the WAN remote site INTERNET (default route), which uses tag 0. The IP address of the INTERNET remote site can be dynamic or static. This address is registered as an RLOC address with the MAP server.

Data from the INTRANET should be sent to the LISP tunnel. For this purpose, the router requesting an unknown destination sends a map request to the MAP resolver 1.1.1.1.

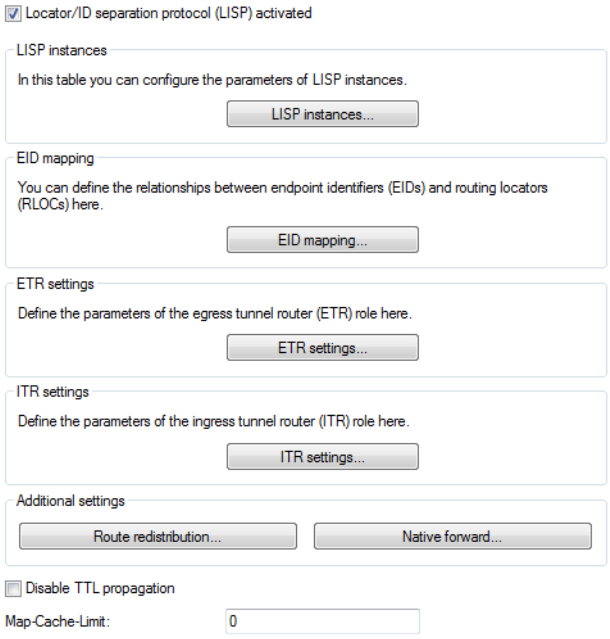
If the map resolver returns a positive mapping, LISP automatically establishes a dynamic tunnel to the remote LISP router and enters the corresponding routes into the routing table.

If the map resolver returns a negative mapping, i.e. the destination prefix is unknown or is not registered on the map server/resolver, then the packet can optionally be sent directly over the INTERNET remote site, without using a tunnel (native forward).

LISP routes do not have to be configured manually. LISP automatically creates routes and later deletes them.

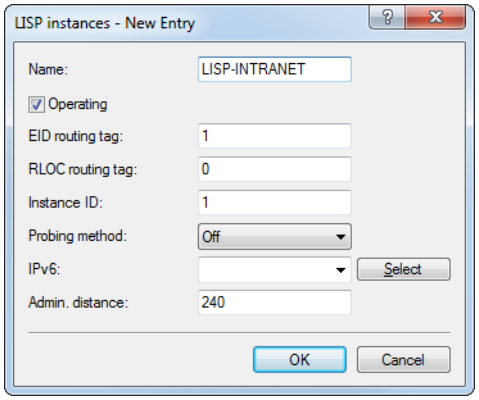
As a matter of principle, entries for the routing tags have to be created manually in the WAN tag table.

1. First, enable the LISP protocol under **Routing protocols** > **LISP** > **Locator/ID separation protocol (LISP) activated**.

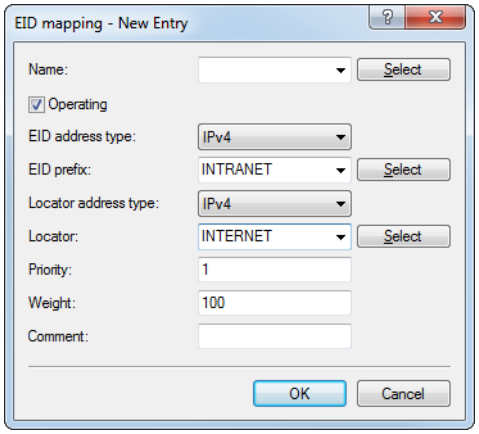


2. Create a new entry in the table of LISP instances. Do this by navigating to **Routing protocols** > **LISP** > **LISP instances** and then click on **Add**.
   a) Give this LISP instance a **Name**, e.g. LISP-INTRANET.
   b) Enable the entry **Operating**.
   c) Set the **EID routing tag** to 1.
   d) Set the **RLOC routing tag** to the value of the tag of the WAN remote site INTERNET, in this case 0.
   e) Set the **Instance ID** to the value created on the LISP map server, in this case 1 like the tag of the INTRANET.

f) Under **IPv6** you can remove the entry **DEFAULT**, as we are only considering IPv4 here.

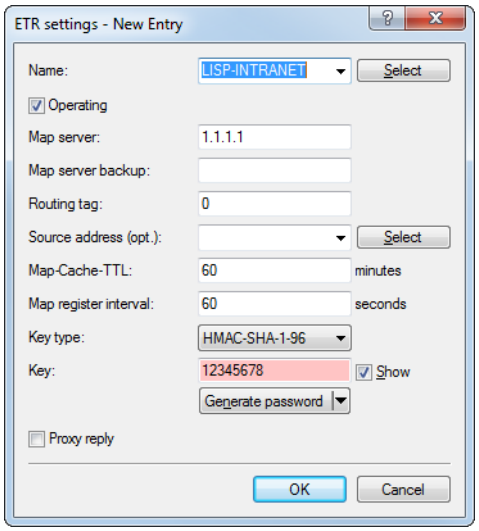


3. Create a new entry in the EID mapping table, which is used to link the EID prefix and the locator. Do this by navigating to **Routing protocols** > **LISP** > **EID mapping** and then click on **Add**.
   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
   b) Enable the entry **Operating**.
   c) Set both the **EID address type** and the **Locator address type** to IPv4.
   d) Set the **EID prefix** to INTRANET.
   e) Set the **Locator** to INTERNET.

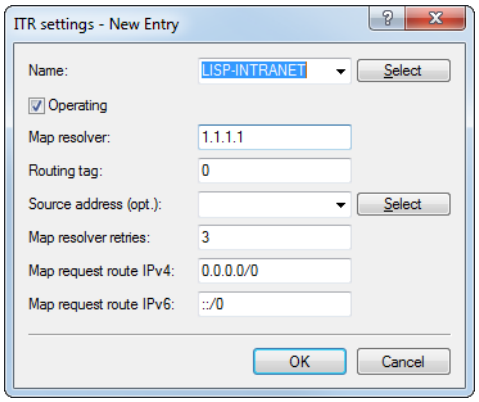


4. In the ETR settings table, create a new entry containing the parameters for communication with the map server. Do this by navigating to **Routing protocols** > **LISP** > **ETR settings** and then click on **Add**.
   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
   b) Enable the entry **Operating**.
   c) Set the **Map server** to 1.1.1.1.
   d) Set the **Routing tag** to 0.

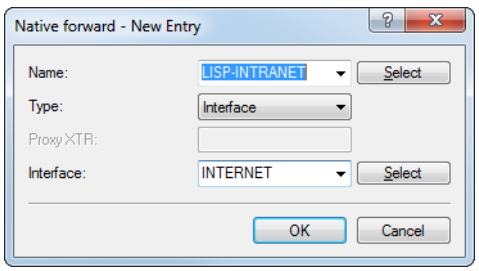
e) Set the **Key type** and the **Key** for connecting to the map server. These must match the type and password configured on the map server. In this example we take HMAC-SHA-1-96 and 12345678.



5. In the ITR settings table, create a new entry containing the parameters for communications with the map resolver. Do this by navigating to **Routing protocols** > **LISP** > **ITR settings** and then click on **Add**.
   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
   b) Enable the entry **Operating**.
   c) Set the **Map resolver** to 1.1.1.1.
   d) Set the **Routing tag** to 0.



6. Optional: Packets to destinations that are not LISP networks can be sent directly via a local interface, i.e. without using the LISP tunnel. In our example, the interface to be used is INTERNET. Create a new entry in the Native forward table. Do this by navigating to **Routing protocols** > **LISP** > **Native forward** and then click on **Add**.
   a) Set the **Name** to the LISP instance created previously, in this case LISP-INTRANET.
   b) Set the **Type** to **Interface**.
   c) Set the **Interface** to INTERNET.



7. Navigate to **Communication** > **Remote sites** > **WAN tag table**, click on **Add** and create an entry for the LISP instance with the instance ID of 1 that you just created.

   For each LISP instance, an entry with the corresponding interface tag for the EID/ARF network must be created in the WAN tag table.

   Do this by creating each entry with the name for the remote site set to LISP-<LISP instance ID>*. The name of each remote site is formed from the keyword LISP supplemented by the corresponding LISP instance ID (in hexadecimal form) and the wildcard *. This unequivocally assigns the incoming traffic from the LISP tunnel to the EID/ARF network.

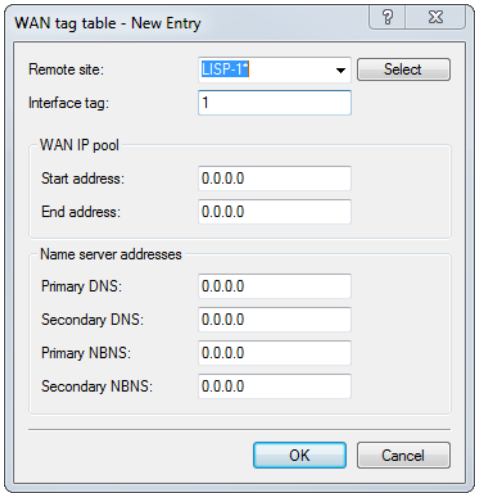
   The instance ID must be specified in hexadecimal without a leading 0x.

   Representation: LISP-<LISP instance ID>*

   Examples:

   - For LISP instance 1: LISP-1*
   - For LISP instance 15: LISP-F*

   a) Fill out the **Remote site** field as described above, i.e. the LISP instance with instance ID 1 takes the value "LISP-1*".
   b) Set the **Interface tag** to 1.



That's it!

3.2.3 Additions to the Setup menu

LISP

Settings for Locator / ID Separation Protocol (LISP).

SNMP ID:

2.93.4

Telnet path:

Setup > **Routing-Protocols**

Instances

This table contains the global configuration of the LISP instances on the device.

SNMP ID:

2.93.4.1

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

Specifies a unique name for a LISP instance. This name is referenced in other LISP tables.

SNMP ID:

2.93.4.1.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Operating

Activates or deactivates this LISP instance.

SNMP ID:

2.93.4.1.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

No
Yes

EID-Rtg-Tag

Routing tag of the endpoint identifier (EID) of this instance.

SNMP ID:

2.93.4.1.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

RLOC-Rtg-Tag

Routing tag of the routing locator (RLOC) of this instance.

SNMP ID:

2.93.4.1.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

Instance-ID

LISP instance ID as a numeric tag from RFC 8060 (LISP Canonical Address Format (LCAF)) for the segmentation of networks with ARF.

SNMP ID:

2.93.4.1.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 10 characters from `[0-9]`

Probing-Method

Specifies the method used to periodically check the accessibility of the RLOCs for map cache entries.

SNMP ID:

2.93.4.1.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Off

The availability of the RLOCs is not checked periodically.

RLOC-Probing

The availability of the RLOCs is periodically checked by LISP RLOC messages.

IPv6

Name of the IPv6 WAN profile from the IPv6 WAN interface table. An entry is required if IPv6 EIDs are used.

SNMP ID:

2.93.4.1.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

600

Admin-Distance

Administrative routing distance.

SNMP ID:

2.93.4.1.9

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Instances**

Possible values:

Max. 3 characters from `[0-9]`

Default:

240

EID-Mapping

This table specifies the mapping of EIDs to RLOCs to be registered with the map server.

SNMP ID:

2.93.4.2

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.2.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

EID-Address-Type

This bitmask specifies the protocol version of the EID prefix when referencing the EID prefix via an interface or network name.

SNMP ID:

2.93.4.2.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

IPv4
IPv6

EID-Prefix

EID prefix of the EID mapping. Possible values are an IPv4 network name or an IPv6 interface, e.g. INTRANET, or a named loopback address.

SNMP ID:

2.93.4.2.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 43 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Locator-Address-Type

This bitmask specifies the protocol version of the RLOC when referencing the EID prefix via an interface name.

SNMP ID:

2.93.4.2.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

IPv4
IPv6

Locator

RLOC of the EID mapping. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

SNMP ID:

2.93.4.2.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Operating

SNMP ID:

2.93.4.2.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

No
Yes

Priority

The priority of the EID mapping.

SNMP ID:

2.93.4.2.7

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

Weight

The weight of the EID mapping.

SNMP ID:

2.93.4.2.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 3 characters from `[0-9]`

Default:

100

Comment

Enter a descriptive comment for this entry.

SNMP ID:

2.93.4.2.9

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 25 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

ITR-Settings

This table specifies the parameters for the role as Ingress Tunnel Router (ITR).

SNMP ID:

2.93.4.3

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.3.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Map-Resolver

IPv4 or IPv6 address of the LISP map resolver.

SNMP ID:

2.93.4.3.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Operating

Activates or deactivates these ITR settings.

SNMP ID:

2.93.4.3.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

No
Yes

Loopback address

Contains the sender address as the named interface that is used with the map resolver in LISP communication.

SNMP ID:

2.93.4.3.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Rtg-Tag

Routing tag used to access the map resolver.

SNMP ID:

2.93.4.3.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Map-Resolver-Retries

Number of retries for map requests to the map resolver.

SNMP ID:

2.93.4.3.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 3 characters from `[0-9]`

Default:

3

Map-Request-Route-IPv4

Specifies the IPv4 route or prefix for the LISP map requests.

SNMP ID:

2.93.4.3.7

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 18 characters from `[A-F][a-f][0-9]:.`

Map-Request-Route-IPv6

Specifies the IPv6 route or prefix for the LISP map requests.

SNMP ID:

2.93.4.3.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ITR-Settings**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:.`

ETR-Settings

This table specifies the parameters for the role as Egress Tunnel Router (ETR).

SNMP ID:

2.93.4.4

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.4.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Map-Server

IPv4 or IPv6 address of the LISP map server

SNMP ID:

2.93.4.4.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Operating

Activates or deactivates these ETR settings.

SNMP ID:

2.93.4.4.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

No
Yes

Loopback address

Contains the sender address as the named interface that is used with the map server in LISP communication.

SNMP ID:

2.93.4.4.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Rtg-Tag

Routing tag to be used to access the map server.

SNMP ID:

2.93.4.4.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Map-Cache-TTL-Minutes

Time-to-live of the EID mappings in minutes registered with the map server.

SNMP ID:

2.93.4.4.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Map-Register-Interval-Seconds

Registration interval in seconds in which map registrations are sent to the map server.

SNMP ID:

2.93.4.4.7

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 10 characters from `[0-9]`

Key-Type

Algorithm used for authentication at the map server.

SNMP ID:

2.93.4.4.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

None
HMAC-SHA-1-96
HMAC-SHA-256-128

Key

Key or password used to register the EID mapping on the map server.

SNMP ID:

2.93.4.4.9

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 24 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Proxy-Reply

Determines whether the proxy reply bit is set in map registrations. In this case, the map server acts as a proxy and responds to map requests on behalf of the ETR.

SNMP ID:

2.93.4.4.10

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

No
Yes

Map-Server-Backup

IPv4 or IPv6 address of the LISP backup map server. The LISP registration is sent in parallel both to the primary map server and to the backup map server.

SNMP ID:

2.93.4.4.11

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **ETR-Settings**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Operating

This item switches the routing protocol Locator / ID Separation Protocol (LISP) on or off.

SNMP ID:

2.93.4.5

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

No
Yes

Default:

No

Disable-TTL-Propagation

With this switch enabled, the ITR does not copy the Time-To-Live (TTL) from the outer to the inner header. As a result, a client running traceroute sees the LISP tunnel as a hop. If disabled, traceroute shows all of the hops between ITR and ETR.

SNMP ID:

2.93.4.7

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

No
Yes

Default:

No

Map-Cache-Limit

Defines the maximum number of map-cache entries across all LISP instances. After reaching the limit, new entries are rejected. Only after older entries in the map cache have become invalid will new entries be accepted. 0 means there is no restriction.

SNMP ID:

2.93.4.8

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Possible values:

Max. 4 characters from `[0-9]`

Default:

0

Native-Forward

SNMP ID:

2.93.4.9

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.9.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Type

SNMP ID:

2.93.4.9.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

None
ProxyXTR
Interface

Proxy-XTR

SNMP ID:

2.93.4.9.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

Max. 43 characters from `[A-F][a-f][0-9]:.`

Interface

SNMP ID:

2.93.4.9.5

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Native-Forward**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Redistribution

The redistribution of routes allows routes from the routing table to be imported into the LISP map cache. Map requests are performed for these routes.

Route redistribution also allows routes to be imported from the routing table and dynamically registered to the map server as an EID prefix.

SNMP ID:

2.93.4.10

Telnet path:

Setup > **Routing-Protocols** > **LISP**

Name

References the name of the LISP instance.

SNMP ID:

2.93.4.10.1

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 24 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Source

This bitmask specifies the route sources of the imported routes.

SNMP ID:

2.93.4.10.2

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Connected

From directly connected networks, the device imports information from the routing table into the LISP map cache or into the EID table as an EID prefix.

Static

The device imports static routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

OSPF

The device imports OSPF routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

BGP

The device imports BGP routes from the routing table into the LISP map cache or into the EID table as an EID prefix.

Destination

Specifies the destination of routes imported to LISP.

SNMP ID:

2.93.4.10.3

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Map-Cache

Imports the routes into the map cache. LISP performs map requests for these routes.

Eid-Table

Import the routes into the LISP EID table. These routes are registered with the map server as an EID prefix with the configured RLOC.

Locator

Specifies the RLOC used to register the imported EID prefixes with the map server. Possible values are named remote sites, IPv6 WAN interfaces, or loopback interfaces.

SNMP ID:

2.93.4.10.4

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 39 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Priority

The priority.

SNMP ID:

2.93.4.10.6

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **Redistribution**

Possible values:

Max. 3 characters from `[0-9]`

Default:

1

Weight

The weight of the EID mapping.

SNMP ID:

2.93.4.2.8

Telnet path:

Setup > **Routing-Protocols** > **LISP** > **EID-Mapping**

Possible values:

Max. 3 characters from `[0-9]`

Default:

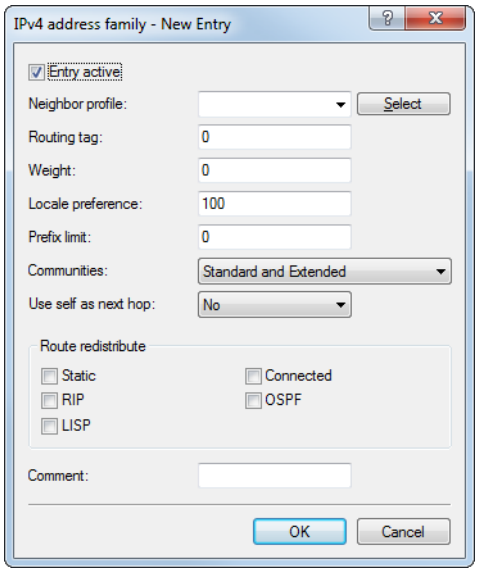
100

3.3 Route redistribution of LISP and RIP routes in BGP

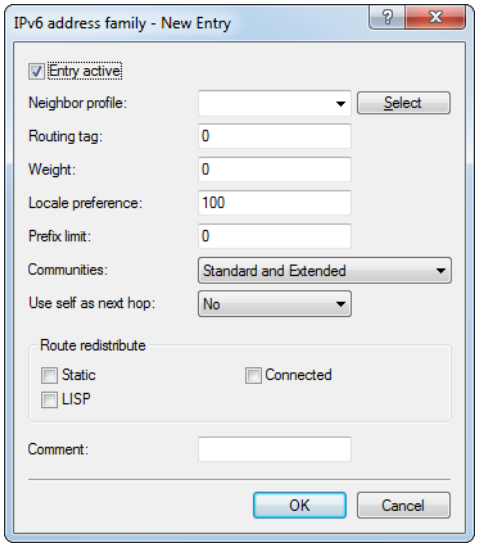
As of HiLCOS 10.32, route redistribution allows LISP and RIP routes be redistributed according to BGP. For this purpose, routes of the corresponding type are read out from the routing table and redistributed by BGP.

The redistribution of RIP routes is only supported for IPv4 routes.

There are two new switches for these features. In LANconfig, these are located under **Routing protocols** > **BGP** > **IPv4 address family**



and **Routing protocols** > **BGP** > **IPv6 address family**, respectively.



If the LISP option is selected, the device distributes LISP routes from the routing table to the BGP neighbors. With the RIP option selected, the device distributes RIP routes from the routing table to the BGP neighbors.

3.3.1 Additions to the Setup menu

Route redistribute

Specifies whether the device forwards certain routes to BGP neighbors of this profile.

If no option is selected, the device does not redistribute any routes to the BGP neighbors of this neighbor profile (default setting).

SNMP ID:

2.93.1.4.1.9

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Static

The device distributes static routes from the routing table to the BGP neighbors.

Connected

The device redistributes routes from the networks that it is directly connected to to the BGP neighbors.

RIP

The device redistributes RIP routes from the routing table to the BGP neighbors.

OSPF

The device distributes OSPF routes from the routing table to the BGP neighbors.

LISP

The device distributes LISP routes from the routing table to the BGP neighbors.

Route redistribute

Specifies whether the device forwards certain routes to BGP neighbors of this profile.

If no option is selected, the device does not redistribute any routes to the BGP neighbors of this neighbor profile (default setting).

SNMP ID:

2.93.1.4.2.9

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Static

The device distributes static routes from the routing table to the BGP neighbors.

Connected

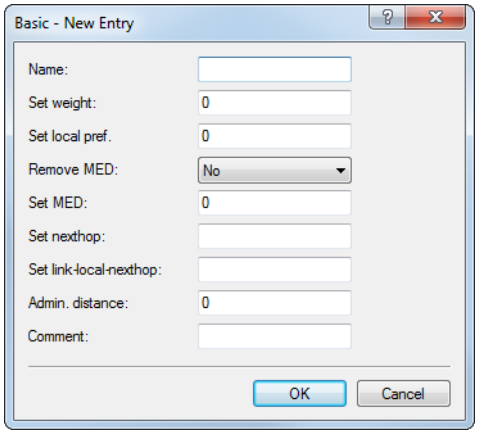
The device redistributes routes from the networks that it is directly connected to to the BGP neighbors.

LISP

The device distributes LISP routes from the routing table to the BGP neighbors.

3.4 BGP: Setting administrative distance by policy

In relation to BGP, the parameter **Admin. distance** under **Routing protocols** > **BGP** > **BGP policy** > **Basic** specifies the "administrative distance" entered into the routing table for the received prefixes.



The list of fixed "administrative distances" for the various system services and routing protocols can be displayed on the command line by `show admin-distance`.

3.4.1 Additions to the Setup menu

Set-Admin-Distance

This parameter specifies the "administrative distance" given to prefixes received in the BGP when they are entered into the routing table. The list of fixed "administrative distances" for the various system services and routing protocols can be displayed on the CLI by show admin-distance.

SNMP ID:

2.93.1.5.2.1.9

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Policy** > **Overrides** > **Basic**

Possible values:

Max. 3 characters from `[0–9]`

3.5 DSLoL for WLAN routers

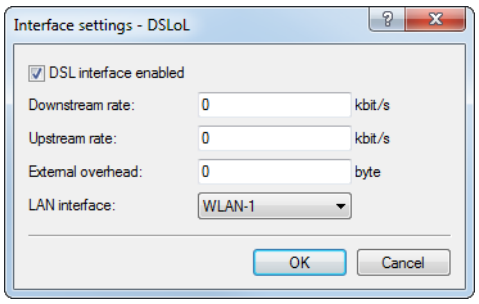
IPv4 addresses can only be masked ("NAT") on WAN connections. If you want to masquerade in the direction of a LAN or WLAN interface, then the corresponding LAN or WLAN interface must be declared as a DSL port in order for it to establish a WAN connection (typically by IPoE or DHCPoE).

Until HiLCOS10.12, this was only possible for access points. From HiLCOS10.32, DSLoL is also available for WLAN routers.

An example scenario for DSLoL:

A WLAN router should be used to connect to the Internet primarily over WLAN. This is done using the WLAN client mode. If the WLAN is not available, the Internet connection should instead be established via LTE/4G as a backup. For this

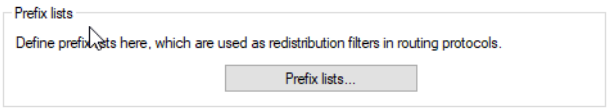
purpose, an LTE/4G connection is configured as usual, and the other WLAN-based Internet connection is set up by operating DSLoL on the WLAN interface. This is done in LANconfig under **Interfaces** > **WAN** > **Interface settings** > **DSLoL** by selecting the option **DSL interface enabled** and then setting the **LAN interface** to the WLAN that was earlier set up as the WLAN client.

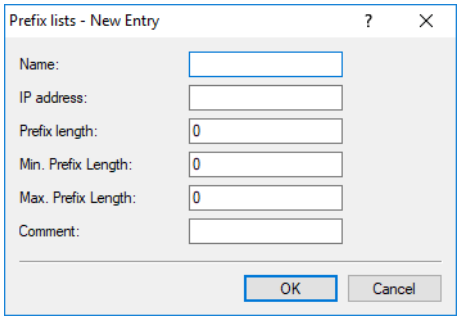


The LTE/4G connection is now configured as a backup for the WLAN/DSLoL Internet connection.

3.6 Filter list for redistribution in BGP

Filter lists can be used to allow or reject certain prefixes during redistribution by the BGP. To do this, create the prefix filter list under **IP router** > **General** > **Prefix lists**.





Name

Give this entry a name here.

IP address

Specify the IPv4 or IPv6 address of the network here.

Prefix length

Contains the netmask or prefix length of the network. This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address. The prefix length must exactly match this value unless **Min. prefix length** and **Max. prefix length** are set to values not equal to zero.

If the value is "0", the prefix for this rule is a match if it comes from same IP address family as that specified under **IP address**.

Min. prefix length

Here you specify the minimum prefix length value required for the prefix to match.

Max. prefix length

Here you specify the maximum prefix length value required for the prefix to match.

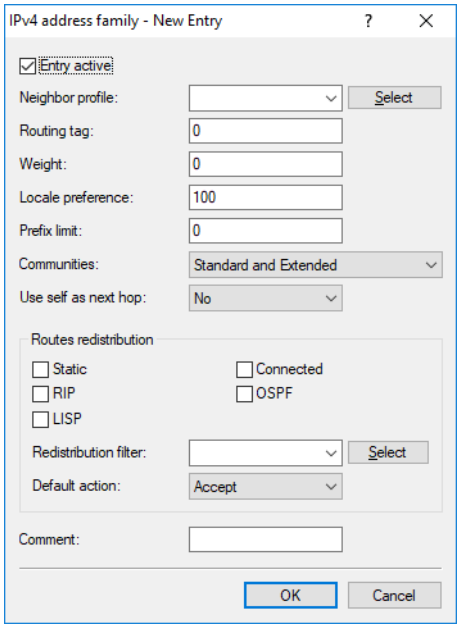
Comment

Comment on this entry.

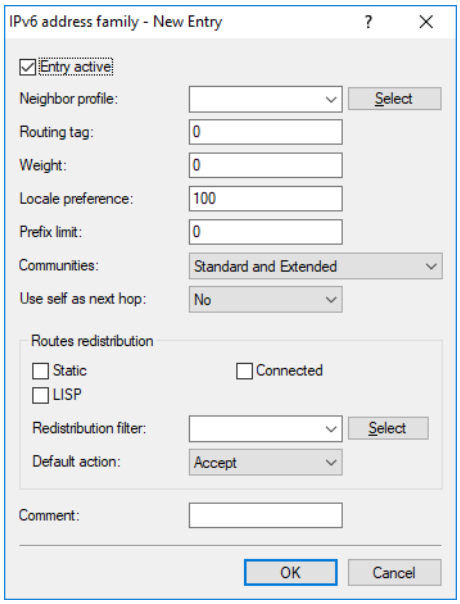
Using prefix lists with BGP

These **prefix lists** can be referenced for the IPv4 and IPv6 address families of the BGP protocol, and you can specify whether these prefix lists should be allowed or rejected

Routing protocols > **BGP** > **IPv4 address family**



Routing protocols > **BGP** > **IPv6 address family**



Redistribution filter

Name of the prefix-filter list.

Default action

Defines the default handling of prefixes that are not configured in the prefix list. Possible values:

Accept

Deny

3.6.1 Additions to the Setup menu

Redistribution-Filter

Name of the prefix filter list from 2.93.5.1 .

SNMP ID:

2.93.1.4.1.11

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

SNMP ID:

2.93.1.4.1.12

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv4**

Possible values:

Allow
Reject

Default:

Allow

Redistribution-Filter

Name of the prefix filter list from 2.93.5.1 .

SNMP ID:

2.93.1.4.2.11

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

Default-Action

Defines the default handling of prefixes that are configured in the prefix list.

SNMP ID:

2.93.1.4.2.12

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Addressfamily** > **IPv6**

Possible values:

Allow
Reject

Default:

Allow

Filter

Filter lists can be used to allow or reject certain prefixes during redistribution by the BGP.

SNMP ID:

2.93.5

Telnet path:

Setup > **Routing-Protocols**

Prefix-List

Here you specify a prefix list that can be referenced by BGP.

SNMP ID:

2.93.5.1

Telnet path:

Setup > **Routing-Protocols** > **Filter**

Name

Contains the name of this entry.

SNMP ID:

2.93.5.1.1

Telnet path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]-_`

Default:

empty

IP-Address

Contains the IPv4 or IPv6 address of the network.

SNMP ID:

2.93.5.1.2

Telnet path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 39 characters from `[A-F][a-f][0-9]:.`

Default:

empty

Prefix-Length

Contains the netmask or prefix length of the network. This entry specifies how many most-significant bits (MSB) of the prefix must match to the IP address. The prefix length must exactly match this value unless **Length-min** and **Length-max** are set to values not equal to zero.

If the value is "0", the prefix for this rule is a match if it comes from same IP address family as that specified under **IP address**.

SNMP ID:

2.93.5.1.3

Telnet path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

Length-Min

Specifies the minimum prefix length value required for the prefix to match.

SNMP ID:

2.93.5.1.4

Telnet path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

Length-Max

Specifies the maximum prefix length value required for the prefix to match.

SNMP ID:

2.93.5.1.5

Telnet path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

Comment

Comment on this entry.

SNMP ID:

2.93.5.1.6

Telnet path:

Setup > **Routing-Protocols** > **Filter** > **Prefix-List**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

3.7 BGP: Switch for default route propagation

As of Addendum HiLCOS Rel. 10.32 your device has the option to handle default routes like normal routes with BGP.

3.7.1 Additions to the Setup menu

Send-Default-Route

This switch determines the behavior of the propagation of default routes.

SNMP ID:

2.93.1.3.11

Telnet path:

Setup > **Routing-Protocols** > **BGP** > **Neighbor-Profiles**

Possible values:

Yes

In BGP phase 3 (determining routes for redistribution), default routes are treated as normal routes.

No

Default routes are ignored if they are not sourced from the static BGP routes table (see 2.93.1.6.1 IPv4 or 2.93.1.6.2 IPv6).

Default:

No

4 IPv6

4.1 IPv6 WAN interface

The configuration logic of the IPv6 WAN interfaces has been changed. There is now a DEFAULT entry under **IPv6** > **General** > **WAN interfaces**. It is automatically selected for every remote station if you do not create another entry and select it at the remote site. For all remote stations, the configuration now has a new parameter **IPv6**, which allows you to select the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

An entry in the WAN interfaces table can be referenced multiple times by remote sites.

4.1.1 Additions to the Setup menu

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.2.8

Telnet path:

Setup > **WAN** > **Dialup-Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.19.19

Telnet path:

Setup > **WAN** > **DSL-Broadband-Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.21.9

Telnet path:

Setup > **WAN** > **PPTP-peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.37.5

Telnet path:

Setup > **WAN** > **L2TP-Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.2.51.11

Telnet path:

Setup > **WAN** > **GRE-Tunnel**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.19.9.20

Telnet path:

Setup > **VPN** > **VPN-Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

IPv6

This entry specifies the name of the IPv6 WAN interface. Leaving this entry blank causes IPv6 to be disabled for this interface.

SNMP ID:

2.19.36.1.21

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

DEFAULT

Interface name

Give a name to the device IPv6 WAN interface here. This name is specified at the remote site. It is preset with a default entry. This is selected automatically if nothing is explicitly specified at the remote site. Leaving this entry blank causes IPv6 to be disabled for this interface.

An entry in the WAN interfaces table can be referenced multiple times by remote sites.

SNMP ID:

2.70.7.1

Telnet path:

Setup > **IPv6** > **WAN-Interfaces**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

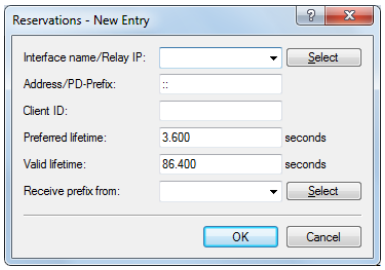
DEFAULT

4.2 DHCPv6

4.2.1 DHCPv6 server

Enhancements for client reservations in the DHCPv6 server

As of HiLCOS 10.32, the parameter **Client ID** has been replaced by the two new parameters **Identifier** and **Identifier type**. This means that the DHCPv6 server can now assign client addresses or prefixes on the basis of the DUID, MAC address, interface ID (as per RFC 3315) or remote ID (as per RFC 4649). The corresponding settings in LANconfig are made under **IPv6** > **DHCPv6** > **Reservations**:



Identifier type

This type specifies how the **Identifier** is to be interpreted.

Client ID

The identifier specifies the client DUID, e.g. 0003000100a057000001.

MAC address

The identifier specifies a MAC address, e.g. 00a057000001. If the client communicates directly with the server, the MAC address is taken from the DHCPv6 packet. If relay agents are used, it is taken from the client link-layer address option (code 79, RFC 6939) in the relay-forward message from the relay agent that is closest to the client.

Interface ID

The identifier specifies the interface ID from the interface-ID option (code 18) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Remote ID

The identifier specifies the remote ID from the remote-ID option (code 37, RFC 4649) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Identifier

Unique identifier for the DHCPv6 client. The type used for identification is configured by the parameter Identifier type.

Possible formats:

- Specification as a client DUID, e.g. 0003000100a057000001
- Specification as a MAC address, e.g. 00a057000001
- Specification as an interface ID or remote ID, e.g. “INTRANET”

Additions to the Setup menu

Identifier

Unique identifier for the DHCPv6 client. The type used for identification is configured by the parameter Identifier type.

Possible formats:

- Specification as a client DUID, e.g. 0003000100a057000001
- Specification as a MAC address, e.g. 00a057000001
- Specification as an interface ID or remote ID, e.g. INTRANET

SNMP ID:

2.70.3.1.6.3

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

A hex string with max. 127 characters `[a-z][0-9]:-`

Default:

empty

Identifier-Type

This type specifies how the identifier in 2.70.3.1.6.3 is to be interpreted.

SNMP ID:

2.70.3.1.6.8

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Client-ID

The identifier specifies the client DUID, e.g. 0003000100a057000001.

Mac-Address

The identifier specifies a MAC address, e.g. 00a057000001. If the client communicates directly with the server, the MAC address is taken from the DHCPv6 packet. If relay agents are used, it is taken from the client link-layer address option (code 79, RFC 6939) in the relay-forward message from the relay agent that is closest to the client.

Interface-ID

The identifier specifies the interface ID from the interface-ID option (code 18) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Remote-ID

The identifier specifies the remote ID from the remote-ID option (code 37, RFC 4649) in the relay-forward message from the relay agent that is closest to the client. This only works with one relay agent.

Comment

Enter a descriptive comment for this entry.

SNMP ID:

2.70.3.1.6.9

Telnet path:

Setup > **IPv6** > **DHCPv6** > **Server** > **Reservations**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

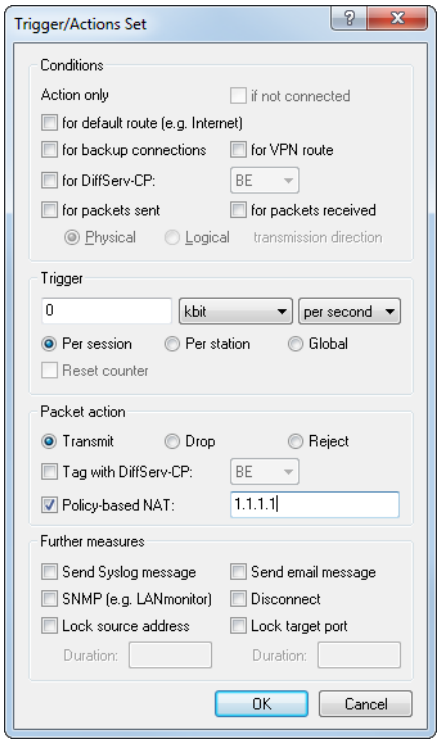
5 Firewall

5.1 WAN policy-based NAT

From HiLCOS 10.32 it is possible to use WAN policy-based NAT.

WAN policy-based NAT allows address translation (masking) of connections based on firewall rules. You can now configure which of the WAN-IPv4 addresses assigned by the provider is to be used to mask internal addresses. This is ideal for scenarios where a provider assigns multiple static IPv4 addresses, e.g. for operating mail servers and web servers with different WAN addresses.

For this purpose, the firewall features the new packet option **Policy-based NAT** under **Firewall/QoS** > **IPv4 Rules** > **Action objects**. This action can be used together with the option **Transmit** and allows masking or NAT behind a specified IPv4 address.



The parameter must be entered as a fixed IP address. Dynamic IP addresses are not supported.

NAT is only possible if a WAN interface is involved. NAT between two LAN interfaces is not supported.

The CLI under (`/Setup/IP-Router/Firewall/Action-Table`) provides the variable `%Y` as an action.

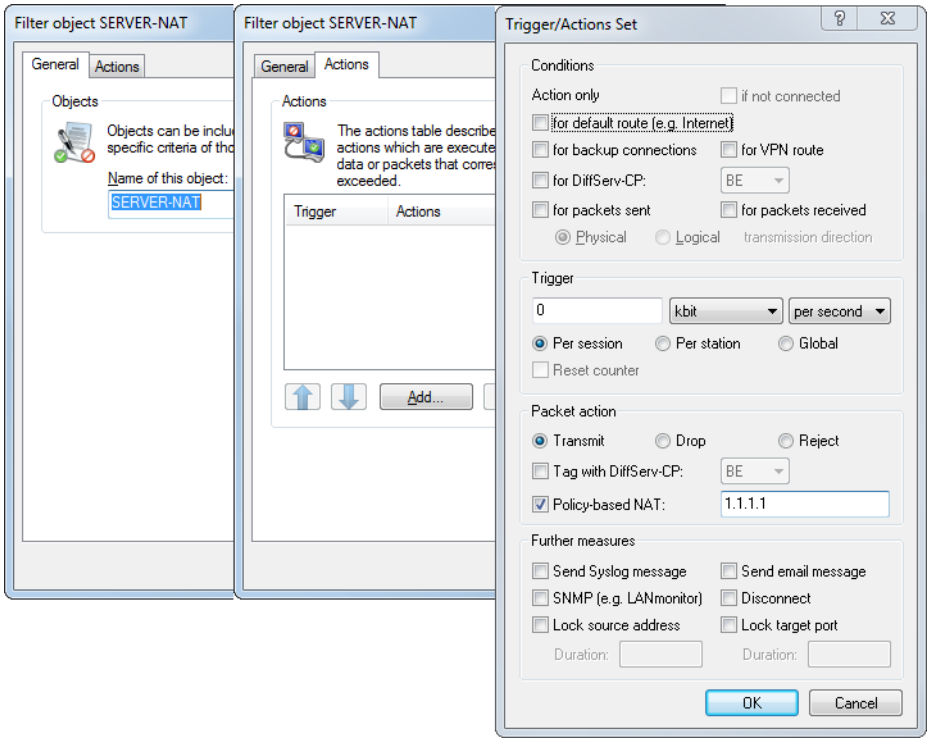
5.1.1 Configuring policy-based NAT with firewall rules

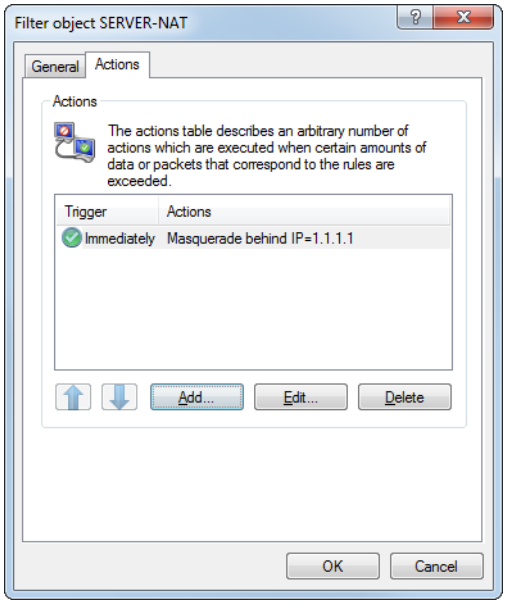
The following example configures an IPv4 network (intranet) with the subnet 192.168.80.0/24. The Internet provider has assigned a number of public IP addresses. Internet access has been set up using the Setup Wizard. Clients on the intranet are automatically masked behind the public IP address that was created with the Wizard.

Now we want to mask a server with the internal IP address 192.168.80.21 behind the public IP address 1.1.1.1.

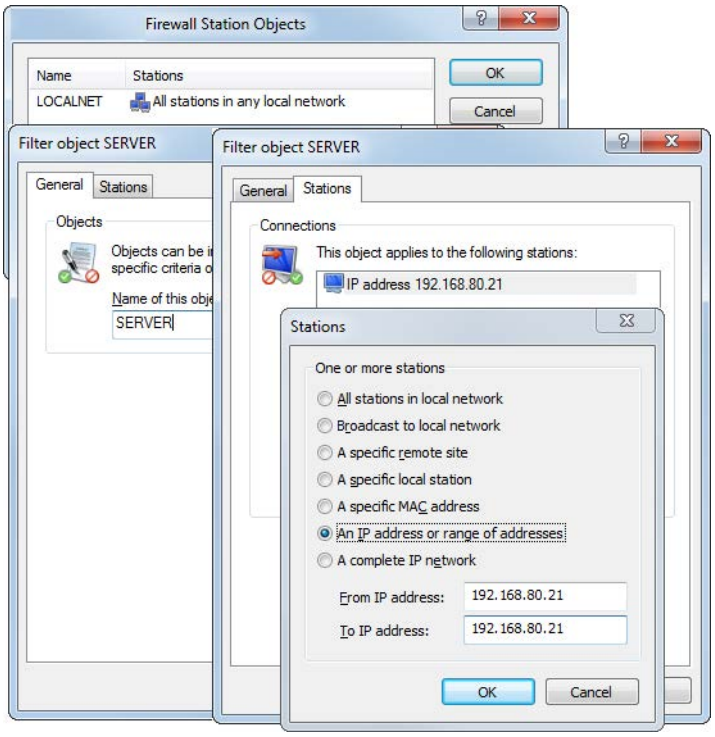
The “return direction” of the masking, i.e. the server’s accessibility from the outside, is realized by a port-forwarding entry, which is not part of this example.

1. Create a new action object in the firewall under **Firewall/QoS** > **IPv4 rules** > **Action objects**. Under Action, set the packet action to **Transmit** and the **Policy-based NAT** to 1.1.1.1.

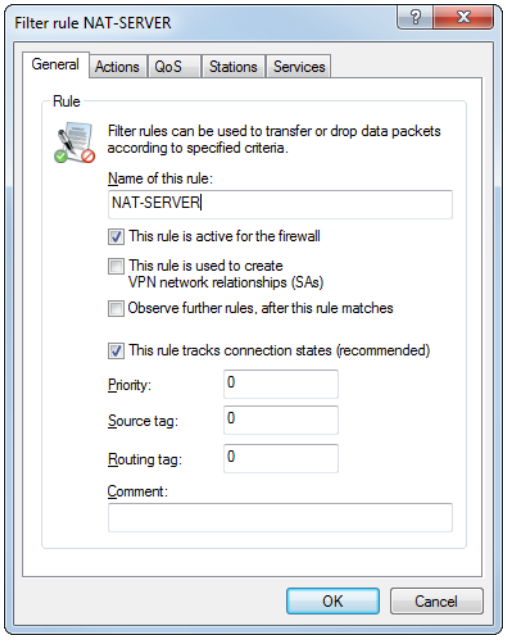




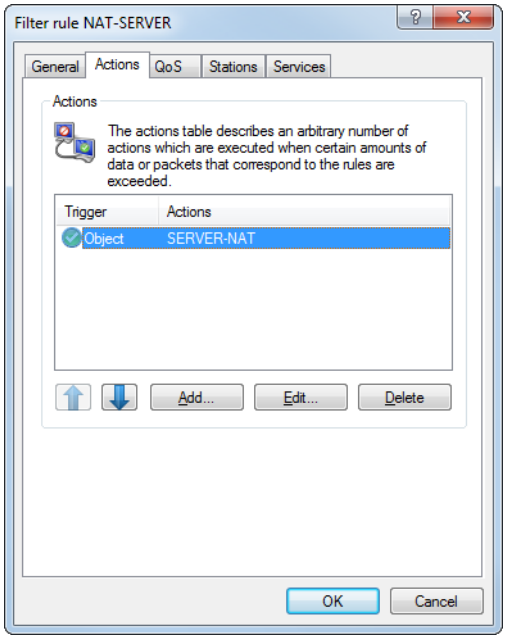
2. Under **Firewall/QoS** > **IPv4 rules** > **Station objects** create a new station object defined for the IP address 192.168.80.21.



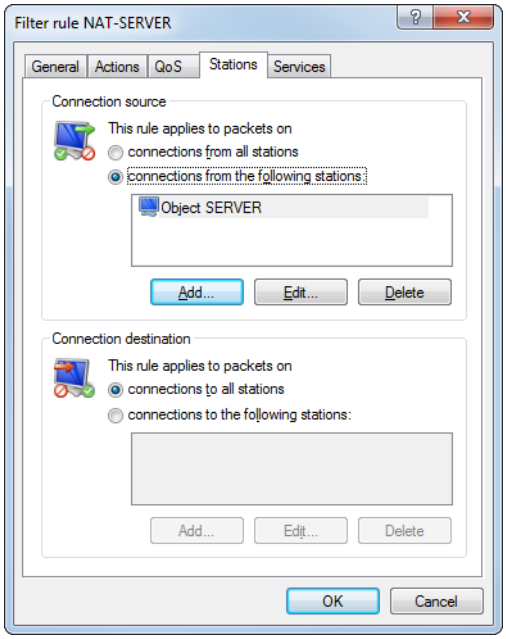
3. Next, go to **Firewall/QoS** > **IPv4 rules** > **Firewall rules** and create a filter rule.

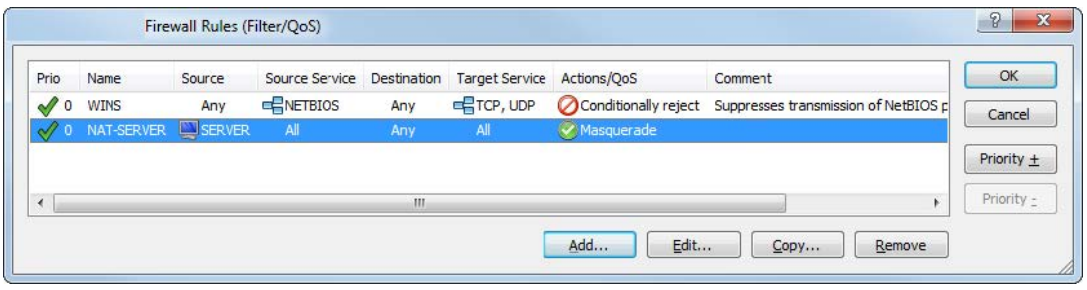


4. In this filter rule, go to **Actions** and select the new action "SERVER-NAT" that was defined above.



5. Then go to **Stations** and use the newly created station object. If necessary. you can also specify the Internet line under **Connection destination**.





5.2 SD-WAN application routing / Layer-7 application control

You can benefit from significant performance gains by operating modern business applications in the cloud (e.g. Microsoft Office 365, AWS, etc). Application routing uses rules to direct trusted applications from the branch office directly to the Internet. This relieves the load on the VPN connection to the main office and also on the Internet connection at the main office.

Microsoft explicitly recommends this mode for Office 365. Because these web-based services often have no fixed IP address, they can only be recognized by DNS names. For this purpose, the corresponding DNS targets can be created in the firewall with an appropriate wildcard expression. These packets are marked with a different routing tag so that the router directs them straight to the Internet. As an alternative, layer-7 application control can be implemented in the firewall. This gives you full control over how applications operate on your network. By defining rules for DNS-based applications, you decide which Internet applications are allowed, blocked, limited or prioritized.

If a user now invokes one of these DNS targets in his or her browser, the computer sends a DNS request for this domain. The DNS forwarder in the router then forwards this request to the Internet Service Provider. When the response arrives the router stores the returned IP address, and from that moment on this resolution is available in the firewall. The response then continues on to the computer that made the original request. This allows the browser to open the connection to the returned IP address. The firewall recognizes the previously learned IP address and can assign a routing tag correspondingly. Other defined firewall actions can also be applied to this destination, such as allow, block, limit, or prioritize.

Because the firewall remembers the exact DNS address that the user uses for the domain, this mechanism will also work if the domain name resolves to many different IP addresses or to IP addresses that change over time.

Recommendations

The router must operate as a DNS server or DNS forwarder on the network, i.e. clients on the local network must use the router as the DNS server. In addition, clients need to be prevented from using DNS-over-TLS and DNS-over-HTTPS (also in the browser) directly with external DNS servers.

This can be done as follows:

- The DHCP server has to communicate the IP address of the router as a DNS server (set by default by the Internet wizard)
- Firewall rules have to be set up that prevent the direct use of external DNS servers, e.g. by blocking the outgoing port 53 (UDP) for clients on the source network
- Firewall rules have to be set up that prevent the direct use of external DNS servers that support DNS-over-TLS, e.g. by blocking the outgoing port 853 (TCP) for clients on the source network
- Disable DNS-over-HTTPS (DoH) in the browser

Notes on how to synchronize the firewall's DNS database:

Since the firewall learns its information from the DNS requests of the clients, in certain situations the DNS database will be incomplete. This can happen in the following situations:

- A new firewall rule is added, but the client still has a cached DNS entry
- The router was recently restarted, and the client still has a cached DNS entry

Helpful in these cases are emptying the DNS cache on the client, rebooting the client, or a time-out of the DNS record on the client.

The router's own services, such as ping, are not handled by the firewall rules. By sending a ping to a full DNS name (without wildcard expressions), the generation of rule resolutions (DNS to IP addresses) can be performed on-demand either from the CLI (once) or by a cron job.

Different DNS names that resolve to the same IP address cannot be distinguished. In this case, the first rule that references one of these DNS names will apply. That should not be a problem for large service providers. However, it could occur with small websites hosted by the same vendor.

show fw-dns-destinations

This new parameter for the CLI command `show` accepts an optional space-separated list of names of DNS destinations. It lists all DNS destinations or the ones specified in the parameter list sequentially. For each destination, it displays the counter from **Status** > **Firewall** > **DNS-Database** > **Destination-Usage** followed by the list of wildcard expressions. For each wildcard expression, it shows the currently resolved addresses and the data records that are a direct or indirect match.

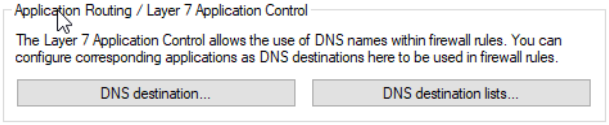
Trace

For application-based routing, there is the new parameter `FW-DNS` for the trace command. It can monitor changes to the firewall database of DNS destinations:

- If a DNS packet arrives, it outputs the packet along with the affected wildcard expressions and destinations.
- If the TTL (time-to-live) of an entry expires, it outputs the associated record along with the relevant wildcard expressions and destinations.
- If one of the two firewalls registers or de-registers a DNS destination because its configuration has changed.
- If there is a change to the table **Set up** > **Firewall** > **DNS-Destinations** or **Set up** > **Firewall** > **DNS-Destination-List**.

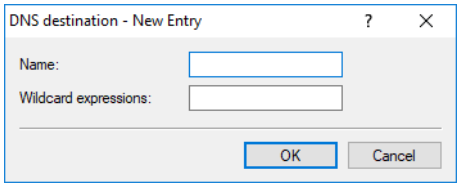
5.2.1 Configuration

Settings for the application-based routing or the Layer%#160;7 application control are located under **Firewall/QoS** > **General** > **Application Routing / Layer 7 Application Control**.



DNS-Destinations

In LANconfig, you specify the names and wildcard expressions for the DNS destinations that you want to treat separately in the firewall under **Firewall/QoS** > **General** > **Application-based routing** > **DNS destinations**.



Name

The name for this DNS destination. This name is used to reference this object.

Wildcard expressions

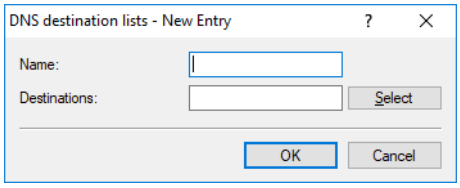
Contains a comma-separated or space-separated list of wildcard expressions. The expressions can contain any number of ? (any character) and * (several arbitrary characters), e.g. "*.hirschmann.*". The input is limited to 252 characters. If you need more DNS wildcard expressions for a service, then you can group multiple DNS destinations into one referenced object in the **DNS destinations list**.

Unicode characters for internationalized domain names can be entered as follows:

- UTF-8: Here, one to four bytes must be entered individually as '\x' followed by two hexadecimal digits.
- UTF-16: Here, one or two double bytes must be entered as '\u' followed by four hexadecimal digits.
- UTF-32: Here, the value must be entered as '\U' followed by eight hexadecimal digits.

DNS destination list

In LANconfig, specify the DNS destinations that you want to reference as one object in the firewall under **Firewall/QoS** > **General** > **Application-based routing** > **DNS destinations list**.



Name

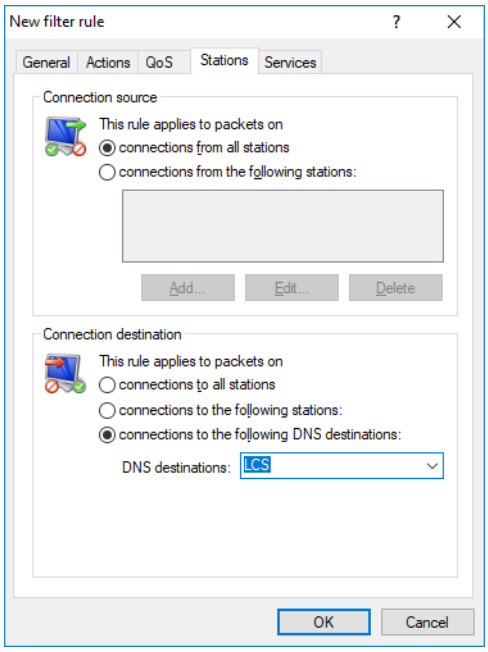
Name of the list of DNS destinations

Targets

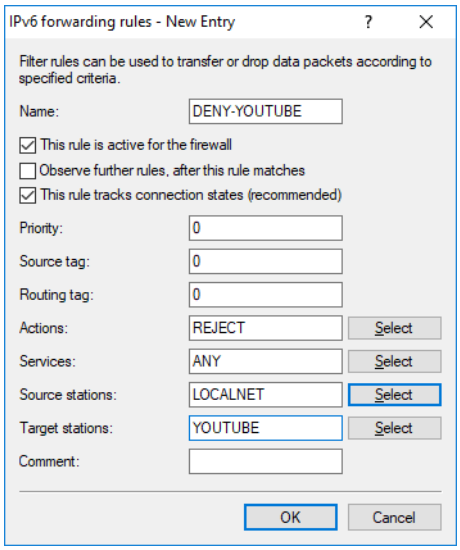
Contains a comma-separated or space-separated list of names of the DNS destinations.

Referencing in firewall rules

In **Firewall / Qos** > **IPv4-Rules** > **Rules** you can create a new filter rule and, then, go to the **Stations** tab and select from the configured DNS destinations under **Connections to the following DNS destinations**.



In **Firewall / Qos** > **IPv6 Rules** > **IPv6 forwarding rules**you can create a new rule. Entries from the **DNS destinations** or **DNS destination list** tables can be used as **Target stations**.



5.2.2 Additions to the Setup menu

DSCP-support

If you set this parameter to Yes, then the DiffServ field in the IPv6-packet header is observed and evaluated as follows:

- **CSx (including CS0 = BE)**: Normal transmission
- **AFxx**: Secure transmission
- **EF**: Preferred transmission

SNMP ID:

2.70.5.25

Telnet path:

Setup > **IPv6** > **Firewall**

Possible values:

No
Yes

Default:

No

Firewall

Firewall settings

SNMP ID:

2.110

Setup

DNS-Destinations

As of HiLCOS 10.32 DNS names can be used in the firewall. DNS names can be defined in full, e.g. "www.hirschmann.de", or as a wildcard expression, e.g. "*hirschmann*". These objects can be used in firewall rules as destinations. Layer-7 (web) applications can be blocked, allowed, limited, prioritized, or redirected to another routing context.
Further information and recommendations are available in the Reference Manual under the Firewall section.

SNMP ID:

2.110.1

Telnet path:

Setup > **Firewall**

Name

The name for this DNS destination. This name is used to reference this object.

SNMP ID:

2.110.1.1

Telnet path:

Setup > **Firewall** > **DNS-Destinations**

Possible values:

Max. 36 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Wildcard-Expressions

Contains a comma-separated or space-separated list of wildcard expressions. The expressions can contain any number of ? (any character) and * (several arbitrary characters), e.g. "*.hirschmann.*". The input is limited to 252 characters. If you need more DNS wildcard expressions for a service, then you can group multiple DNS destinations into one referenced object in the **DNS destinations list**.

Unicode characters for internationalized domain names can be entered as follows:

- UTF-8: Here, one to four bytes must be entered individually as '\x' followed by two hexadecimal digits.
- UTF-16: Here, one or two double bytes must be entered as '\u' followed by four hexadecimal digits.
- UTF-32: Here, the value must be entered as '\U' followed by eight hexadecimal digits.

SNMP ID:

2.110.1.2

Telnet path:

Setup > **Firewall** > **DNS-Destinations**

Possible values:

Max. 252 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

DNS-Destination-List

In the DNS destination list, you can group multiple DNS destinations into one referenced object.

SNMP ID:

2.110.2

Telnet path:

Setup > **Firewall**

Name

The name for this DNS destination list. This name is used to reference this object.

SNMP ID:

2.110.2.1

Telnet path:

Setup > **Firewall** > **DNS-Destination-List**

Possible values:

Max. 36 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Targets

Contains a comma-separated or space-separated list of names of the DNS destinations.

SNMP ID:

2.110.2.2

Telnet path:

Setup > **Firewall** > **DNS-Destination-List**

Possible values:

Max. 252 characters from `[A-Z][0-9]#@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

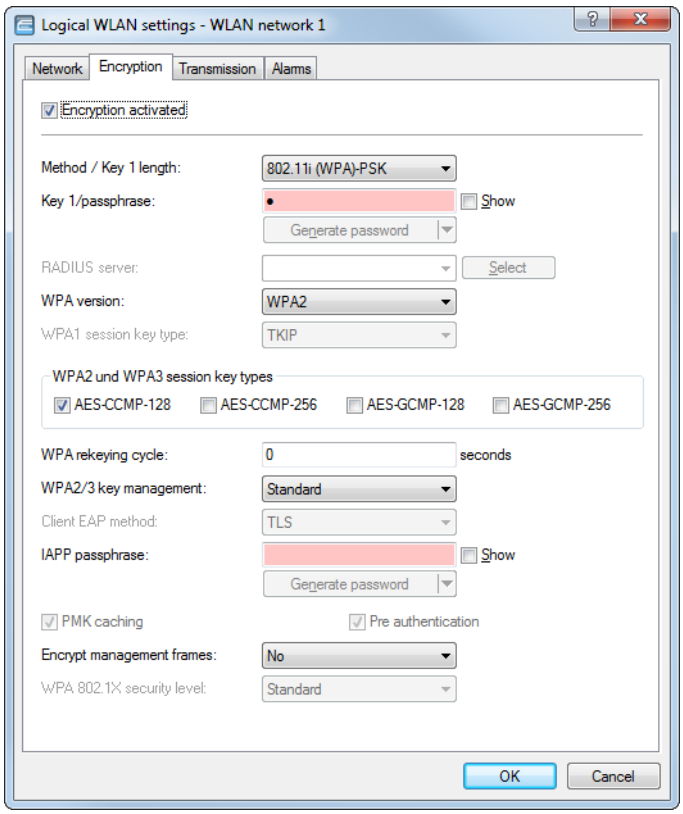
empty

6 Wireless LAN – WLAN

6.1 WLAN encryption settings moved to the logical WLAN settings

To simplify the task of configuration, the WLAN encryption settings now appear as an additional tab in the dialog for the Logical WLAN settings. When configuring an SSID, it is no longer necessary to switch back and forth between the logical WLAN settings dialog and the WLAN encryption settings dialog.

The logical WLAN settings are to be found under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**.

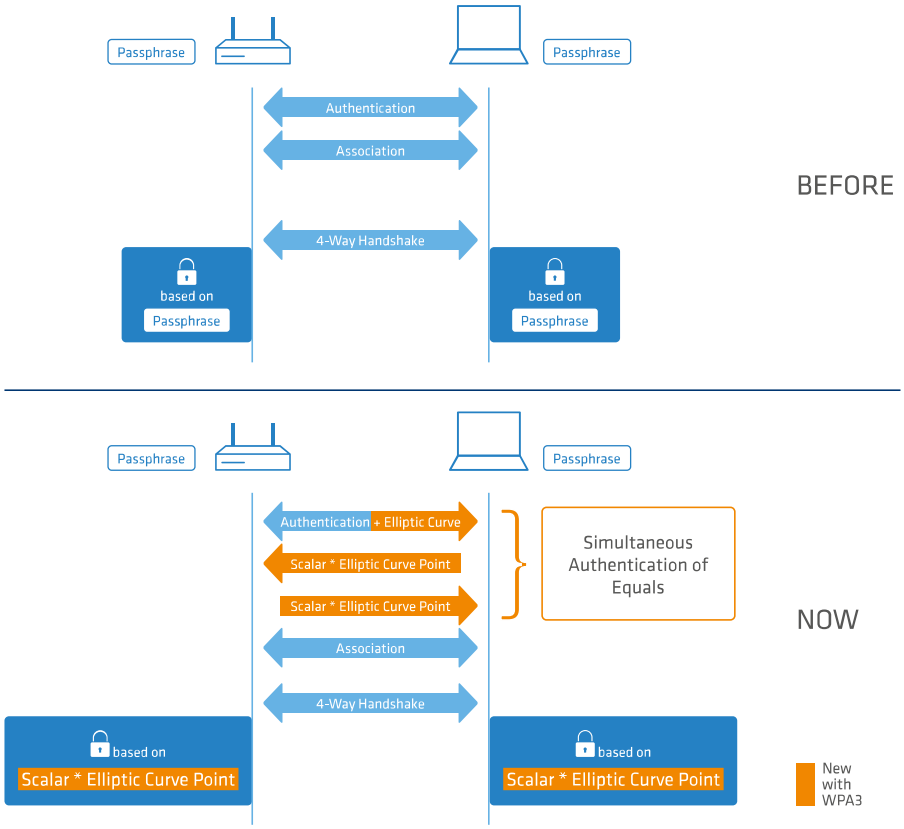


6.2 WPA3 (Wi-Fi Protected Access 3)

Compared to the predecessor standard WPA2 introduced by the Wi-Fi Alliance in 2004, the WPA3 standard introduced in 2018 offers improved security by combining various security methods. Like WPA2, WPA3 also exists in the versions WPA3-Personal and WPA3-Enterprise.

WPA3-Personal uses the Simultaneous Authentication of Equals (SAE) authentication method, which only requires a password for authentication but which prevents brute-force and dictionary attacks. Furthermore, for the first time this

method offers forward secrecy, i.e. captured WPA3-secured traffic cannot be decrypted subsequently after the attacker gains knowledge of the pre-shared key.



Also available with WPA3 is the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Both variants now require the use of protected management frames (PMF) according to IEEE 802.11w. PMF prevents attackers from computing the WLAN password from captured material gained by using fake management frames to force a disassociation and then eavesdropping the re-authentication.

6.2.1 WPA3-Personal

The WLAN encryption settings under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**. now offer the new WPA versions **WPA3** and **WPA2/3**.

With **WPA3** selected, only WLAN clients that support WPA3-Personal will be able to login. This configuration enforces authentication with the Simultaneous Authentication of Equals (SAE). Similarly, this SSID enforces the use of PMF (Protected Management Frames as per 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

6.2.2 WPA3-Enterprise

WPA3-Enterprise does not fundamentally change or replace the protocols defined in WPA2-Enterprise. Rather, it set out policies to ensure greater consistency in the application of these protocols and to assure the desired level of security.

The WLAN encryption settings under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**. now offer the new WPA versions **WPA3** and **WPA2/3**.

By selecting **WPA3**, only WLAN clients that support WPA3-Enterprise will be able to log in. This SSID enforces the use of PMF (Protected Management Frames as per 802.11w), a mandatory part of WPA3.

By selecting **WPA2/3**, these two versions of WPA are offered in parallel. This option allows clients that only support WPA2 to operate in parallel with clients that already support WPA3. For WPA3-compatible WLAN clients, this configuration enforces the use of PMF; for WPA2-compatible WLAN clients, PMF is offered as an option for backwards compatibility.

Suite B cryptography

Also available is the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments. Suite B ensures that all links in the encryption chain match with one another. Suite B forms classes of bit lengths for hashed, symmetric, and asymmetric encryption in order to provide suitable levels of protection. For example, an SHA-2 hash with 256 bits matches AES with 128 bits. Where Suite B is operated, the support of all other combinations is expressly excluded. Consequently, the encryption chain consists of links of equal strength.

Further information on CNSA Suite B can be found at the following link: *CNSA algorithm suite factsheet*

The switch **WPA 802.1X security level** under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings** is used to enable the optional Suite B encryption. With “Suite B 192 bits” support enabled, the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-256 is also enforced.

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

With “Suite B 128 bits” support enabled, the following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Other cipher suites can no longer be used. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP-128 is also enforced.

Because the session key types AES-GCMP-128 and AES-GCMP-256 are not supported by all WLAN modules, the use of Suite B cryptography may be limited or impossible, depending on the device type.

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

6.2.4 Additions to the Setup menu

WPA-Version

Data in this logical WLAN will be encrypted with this WPA version.

SNMP ID:

2.23.20.3.9

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

WPA1
WPA2
WPA1/2
WPA2/3
WPA3
WPA1/2/3

Default:

WPA2

SAE-Groups

The authentication method SAE (Simultaneous Authentication of Equals) uses elliptic curves. Further information is available from the *Standards for Efficient Cryptography Group*.

SNMP ID:

2.23.20.3.26

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

secp256r1
secp384r1
secp521r1
secp192r1
secp224r1

Default:

secp256r1

secp384r1

secp521r1

WPA2-3-Session-Keytypes

From Addendum HiLCOS Rel. 10.32 this setting replaces the value 2.23.20.3.13 **WPA2-Session-Keytypes**.

Here you select the methods that users should be offered to generate the WPA session or group keys. The following Advanced Encryption Standard (AES) methods can be offered.

SNMP ID:

2.23.20.3.27

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

AES-CCMP-128
AES-CCMP-256
AES-GCMP-128
AES-GCMP-256

Default:

AES-CCMP-128

WPA 802.1X security level

Setting the 802.1X security level. WPA3 features the support of CNSA Suite B cryptography, which is an optional part of WPA3-Enterprise for high-security environments.

Operating CNSA Suite B cryptography requires the use of certain cipher suites. Also enforced are a minimum key length of 3072 bits for the RSA and Diffie-Hellman key exchange, as well as 384 bits for the ECDSA and ECDHE key exchange. The session key type AES-GCMP128 is also enforced with "Suite B 128 bits".

If these cipher suites are not supported by the WLAN clients or the remaining infrastructure (e.g. the RADIUS server), then no connection is possible!

SNMP ID:

2.23.20.3.28

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

Default

Suite-B 128-bit

Enabled "Suite B 128 bits". The following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Suite-B 128-bit

Enabled "Suite B 192 bits". The following EAP cipher suites are enforced:

- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

Default:

Default

6.3 Enhanced Open

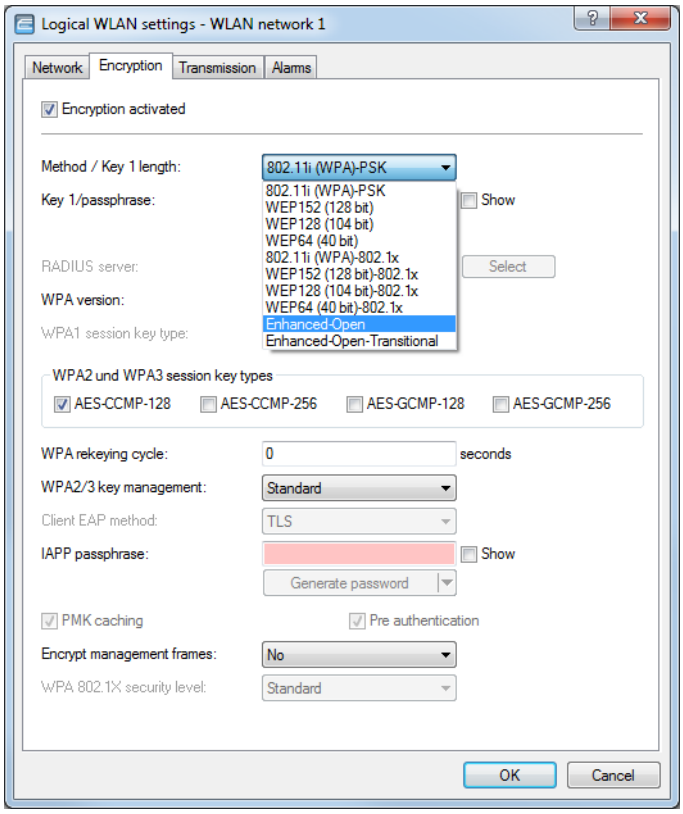
Until now, hotspots were mainly operated without encryption, meaning that the data transmitted over the wireless interface was open to inspection. Also, the widespread practice of securing a hotspot with WPA2-PSK and publicly posting the shared key provides limited security. Since WPA2-PSK does not provide Perfect Forward Secrecy, an attacker who knows the key can use it to decrypt recordings of data traffic. The Enhanced Open method minimizes these risks. Clients that support this method use encrypted communication to prevent other users in the same radio cell from eavesdropping on their communications. The threat of a man-in-the-middle attack remains, but the risk is much lower than when using an unencrypted open hotspot.

Public Spot with Enhanced Open

To use Enhanced Open with the Public Spot, see chapter "9.1 Setting up a secure hotspot with Enhanced Open".

Configuration

Enhanced Open is set as the WLAN encryption method under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**. That is all you need to do to encrypt communications for clients that support this method.



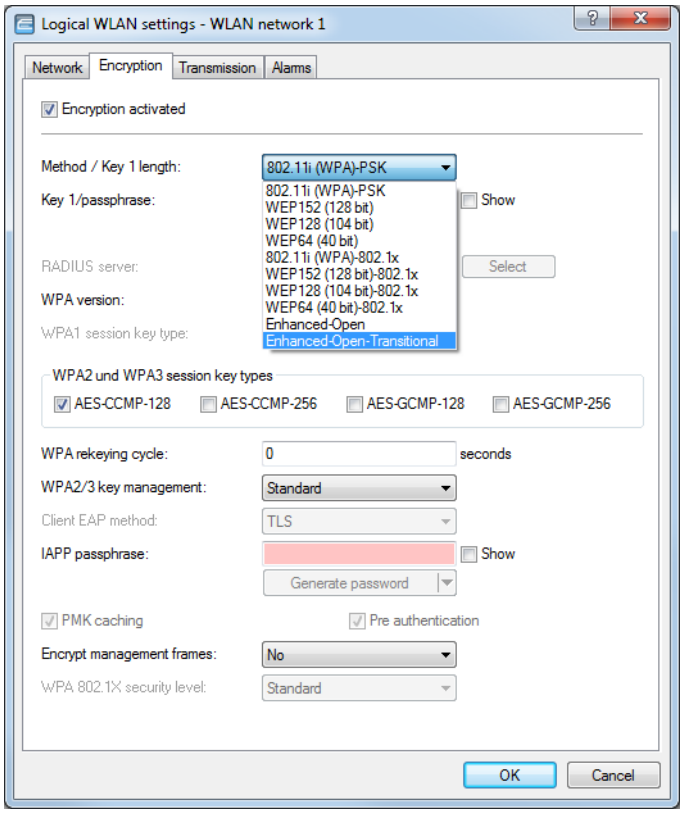
6.3.1 Enhanced Open Transitional mode

The Enhanced Open Transitional mode allows connections to clients that support Enhanced Open and also to those that do not yet support Enhanced Open. With the transitional mode in operation, the regular Enhanced Open SSID is operated in parallel to an unencrypted/open SSID with the same name and otherwise identical settings.

A prerequisite for this is that at least one other SSID is available and unused on the selected radio module. Depending on the device, a total of 15 or 16 SSIDs are available per radio module. If no SSID is available, both the Enhanced Open Transitional SSID and the actual Enhanced Open SSID will not be activated.

Configuration

The Enhanced Open Transitional mode is set as the WLAN encryption method under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**.



6.3.2 Additions to the Setup menu

Method

Selects the encryption method and, for WEP, the key length that is to be used to encrypt data packets on the WLAN.

Please consider that not all wireless cards support all encryption methods.

SNMP ID:

2.23.20.3.4

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

802.11i-WPA-PSK
WEP-128-Bits
WEP-104-Bits
WEP-40-Bits
802.11i-WPA-802.1X
WEP-128-Bits-802.1X
WEP-104-Bits-802.1X
WEP-40-Bits-802.1X
Enhanced-Open
Enhanced-Open-Transitional

Default:

802.11i-WPA-PSK

Enhanced-Open-Groups

The authentication method Enhanced Open uses elliptic curves.

SNMP ID:

2.23.20.3.22

Telnet path:

Setup > **Interfaces** > **WLAN** > **Encryption**

Possible values:

secp256r1
secp384r1
secp521r1

Default:

secp256r1

secp384r1

secp521r1

6.4 Enhanced Passphrase Security (LEPS)

The encryption method WPA2 protects data traffic in the WLAN from "interception". The required passphrase is easily handled as a central key; a RADIUS server such as that for 802.1X installations is not required.

Nevertheless, the tap-proof WPA2 method still has some weaknesses:

- One passphrase applies **globally** for **all** WLAN clients
- The passphrase may fall into unauthorized hands if treated carelessly

› A “leaked” passphrase then offers any attacker free access to the wireless network

This means in practice that: Should the passphrase “go missing” or if an employee with knowledge of the passphrase leaves the company, then the passphrase in the access point needs to be changed in the interests of security—in every WLAN client, too. As this is not always possible, an improvement would be to have an individual passphrase for each user in the WLAN instead of a global passphrase for all WLAN clients. In the case mentioned above, the situation of an employee leaving the company requires merely his “personal” passphrase to be deleted; all others remain valid and confidential.

LEPS provides two efficient methods that makes use of the simple configuration of IEEE 802.11i with passphrase, but that avoid the potential security loopholes that come with global passphrases.

LEPS-U (Enhanced Passphrase Security User) assigns an individual password for the SSID to each individual client or to entire groups. LEPS-MAC (Enhanced Passphrase Security MAC) additionally authenticates the clients by their MAC address, which is ideal for secure enterprise networks.

6.4.1 Enhanced Passphrase Security User (LEPS-U)

Enhanced Passphrase Security Users (LEPS-U) allows a set of passphrases to be configured and assigned to individual users or groups. This avoids having one global passphrase for an SSID. Instead, there are several passphrases, which can then be distributed individually.

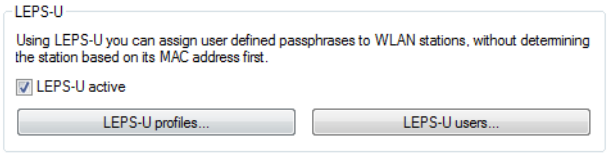
This is useful for onboarding devices into the network. For example, a network operator “onboarding” multiple WLAN devices into different areas of the network does not want to configure each specific device; instead this should done by the users of the devices themselves. In this case, users are given a preshared key for the company WLAN for use with their own devices. The preshared key is used to map each user to a VLAN, thus automatically assigning them to a specific network. The configuration of LEPS-U takes place on the infrastructure side only, which assures full compatibility to third-party products.

The security issue presented by global passphrases is fundamentally remedied by LEPS-U. Each user is assigned their own individual passphrase. If a passphrase assigned to a user should “get lost” or an employee with knowledge of their passphrase leaves the company, then only the passphrase of that user needs to be changed or deleted. All other passphrases remain valid and confidential.

For technical reasons, LEPS-U is only compatible with WPA version WPA2.

Configuration

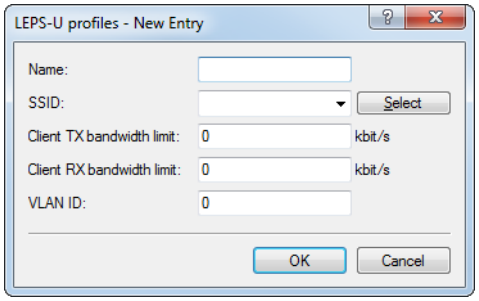
The **LEPS-U profiles** and **LEPS-U users** are configured in LANconfig under **Wireless LAN** > **Stations/LEPS** > **LEPS-U**. The switch **LEPS-U active** enables the LEPS-U feature.



When configured in LEPS-U, each user who should be able to authenticate client devices on the WLAN receives an individual passphrase. This is done with LEPS-U profiles, which avoids having to repeat all of the settings for every new user. You then create the LEPS-U users with their individual passphrases and link them to one of the LEPS-U profiles created previously.

LEPS-U profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users.



Name

Enter a unique name for the LEPS-U profile here.

SSID

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

Client TX bandwidth limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

Client RX bandwidth limit

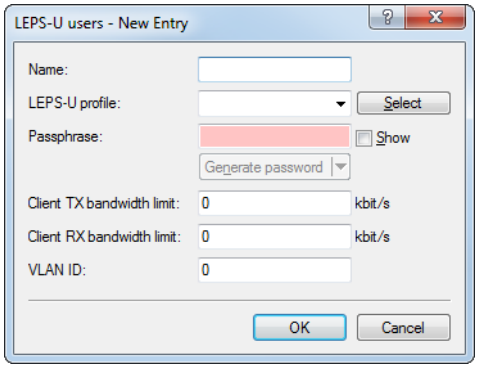
Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

VLAN-ID

Here you specify which VLAN ID is assigned to a LEPS-U user who is connected to this profile.

LEPS-U users

Create individual LEPS-U users here. Each LEPS-U user must be linked with a previously created profile and assigned an individual WPA passphrase. Any client can then use this passphrase to authenticate at the SSID specified in the corresponding profile. The passphrase identifies the user, who is assigned to the VLAN specified in this table. If no VLAN is specified here, the user is assigned to the VLAN configured in the profile. Settings for the individual user thus take priority over settings in the profile.



Name

Enter a unique name for the LEPS-U user here.

LEPS-U profiles

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

Passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

Client TX bandwidth limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

Client RX bandwidth limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

VLAN-ID

Here you specify which VLAN ID is assigned to the LEPS-U user. If no VLAN-ID is configured here, the VLAN-ID configured in the LEPS-U profile (if any) applies. If a VLAN-ID is configured in both the LEPS-U profile and for the LEPS-U user, the VLAN-ID configured for the LEPS-U user applies.

6.4.2 Enhanced Passphrase Security MAC (LEPS-MAC)

LEPS-MAC uses an additional column in the ACL (access-control list) to assign an **individual** passphrase consisting of any 8 to 63 ASCII characters to each MAC address. Authentication at the access point is only possible with the correct combination of passphrase and MAC address.

This combination makes the spoofing of the MAC addresses futile—and LEPS-MAC thus shuts out a potential attack on the ACL. If WPA2 is used for encryption, the MAC address can indeed be intercepted—but this method never transmits the passphrase over wireless. This greatly increases the difficulty of attacking the WLAN as the combination of MAC address and passphrase requires both to be known before an encryption can be negotiated.

LEPS-MAC can be used both locally in the device and centrally managed by a RADIUS server. LEPS-MAC works with all WLAN client adapters available on the market without any modification. Full compatibility to third-party products is assured as LEPS-MAC only involves configuration in the access point.

Compared to LEPS-U, the administrative overhead is slightly higher because the MAC address has to be entered for each device.

Configuration

The configuration of LEPS-MAC involves the assignment of an individual passphrase to the MAC address of each client that is approved for the WLAN. This is done either with an entry in the list under **Wireless LAN** > **Stations/LEPS** > **LEPS-MAC** > **Station rules** or in the RADIUS server. One entry is generated per MAC address—from the point of view of the RADIUS server, the MAC address is therefore a user. It is also necessary to activate the MAC filter under **Wireless LAN** > **General** > **Interfaces** > **Logical WLAN settings**, i.e. data will be transmitted for the WLAN clients entered here.

The passphrase can be a string of 8 to 64 characters. We recommend that the passphrases consist of a random string at least 32 characters long.

If you are storing client-specific passphrases in the user table of a RADIUS server, a LAN-based device can serve as the central RADIUS server and take advantage of LEPS-MAC.

6.4.3 Additions to the Setup menu

LEPS-U

Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

SNMP ID:

2.12.133

Telnet path:

Setup > **WLAN**

Operating

Switches LEPS-U on or off. When switched off, LEPS-U users are ignored during WLAN client authentication.

SNMP ID:

2.12.133.1

Telnet path:

Setup > **WLAN** > **LEPS-U**

Possible values:

No
Yes

Default:

No

Profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users. You can overwrite the profile values for any particular user with individual values.

SNMP ID:

2.12.133.2

Telnet path:

Setup > **WLAN** > **LEPS-U**

Name

Enter a unique name for the LEPS-U profile here.

SNMP ID:

2.12.133.2.1

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Network name

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.12.133.2.2

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

SNMP ID:

2.12.133.2.3

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

SNMP ID:

2.12.133.2.4

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

VLAN-ID

Here you specify which VLAN ID is assigned to a LEPS-U user who is connected to this profile.

SNMP ID:

2.12.133.2.5

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Profiles**

Possible values:

Max. 4 characters from `[0-9]`

Users

Create individual LEPS-U users here. Every LEPS-U user must be connected to a profile that was created previously.

SNMP ID:

2.12.133.3

Telnet path:

Setup > **WLAN** > **LEPS-U**

Name

Enter a unique name for the LEPS-U user here.

SNMP ID:

2.12.133.3.1

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Profile

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.12.133.3.2

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

WPA passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

SNMP ID:

2.12.133.3.3

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

SNMP ID:

2.12.133.3.4

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

SNMP ID:

2.12.133.3.5

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

VLAN-ID

Here you specify which VLAN ID is assigned to the LEPS-U user. If no VLAN-ID is configured here, the VLAN-ID configured in the LEPS-U profile (if any) applies. If a VLAN-ID is configured in both the LEPS-U profile and for the LEPS-U user, the VLAN-ID configured for the LEPS-U user applies.

SNMP ID:

2.12.133.3.6

Telnet path:

Setup > **WLAN** > **LEPS-U** > **Users**

Possible values:

Max. 4 characters from `[0-9]`

LEPS-U

Enhanced Passphrase Security User (LEPS-U) lets you assign custom passphrases to WLAN stations without having to pre-register stations by their MAC address.

SNMP ID:

2.37.1.25

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration**

Profiles

Configure LEPS-U profiles here and link them to an SSID. You can then assign the LEPS-U profiles to the LEPS-U users. You can overwrite the profile values for any particular user with individual values.

SNMP ID:

2.37.1.25.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U**

Name

Enter a unique name for the LEPS-U profile here.

SNMP ID:

2.37.1.25.1.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Network profile

Here you select the SSID or, in the case of a WLC, the logical WLAN network for which the LEPS-U profile is valid. The only users who can authenticate at the SSID or, in the case of a WLC, at the logical WLAN network are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.37.1.25.1.2

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients.

SNMP ID:

2.37.1.25.1.3

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients.

SNMP ID:

2.37.1.25.1.4

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

VLAN-ID

Here you specify which VLAN ID is assigned to a LEPS-U user who is connected to this profile.

SNMP ID:

2.37.1.25.1.5

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Profiles**

Possible values:

Max. 4 characters from `[0-9]`

Users

Create individual LEPS-U users here. Every LEPS-U user must be connected to a profile that was created previously.

SNMP ID:

2.37.1.25.2

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U**

Name

Enter a unique name for the LEPS-U user here.

SNMP ID:

2.37.1.25.2.1

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Profile

Select the profile for which the LEPS-U user is valid. The only users who can authenticate at the SSID are those who are connected to it via the LEPS-U profile.

SNMP ID:

2.37.1.25.2.2

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

WPA passphrase

Here you can specify the passphrase to be used by LEPS-U users to authenticate at the WLAN.

SNMP ID:

2.37.1.25.2.3

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 63 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Per-Client-Tx-Limit

Here you can set a transmission bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

SNMP ID:

2.37.1.25.2.4

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

Per-Client-Rx-Limit

Here you can set a reception bandwidth limit in kbps for authenticating WLAN clients. If no limit is configured here, the limitation configured in the LEPS-U profile (if any) applies. If a limit is configured in both the LEPS-U profile and for the LEPS-U user, the limit configured for the LEPS-U user applies.

SNMP ID:

2.37.1.25.2.5

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 9 characters from `[0-9]`

Special values:

0

No limit.

VLAN-ID

Here you specify which VLAN ID is assigned to the LEPS-U user. If no VLAN-ID is configured here, the VLAN-ID configured in the LEPS-U profile (if any) applies. If a VLAN-ID is configured in both the LEPS-U profile and for the LEPS-U user, the VLAN-ID configured for the LEPS-U user applies.

SNMP ID:

2.37.1.25.2.6

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **LEPS-U** > **Users**

Possible values:

Max. 4 characters from `[0-9]`

6.5 Client Management

With Client Management, Wi-Fi clients are steered to the best available access point and frequency band. This feature improves the quality of wireless networks of all sizes. The popular band steering and client steering, which so far were separate features, have now been combined and even operate without a WLAN controller.

Compared to the previous client steering feature supported by WLCs, Client Management operates independently and without a WLC. The access points communicate with one another using the protocol IAPP.

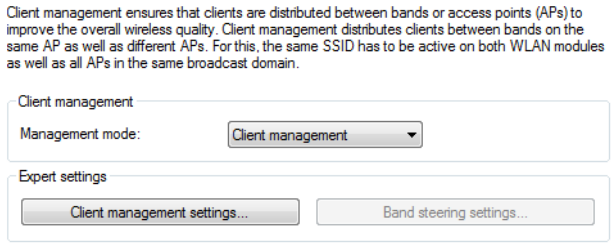
For the access points to communicate with one another, they need to be able to exchange IAPP messages. IAPP messages are transmitted by multicast. If necessary, the infrastructure—and switches in particular—requires exemptions to be created for IGMP snooping or other filtering mechanisms. IAPP uses the multicast group 224.0.1.76.

Hirschmann switches in the default setting are already set up correctly for Client Management.

In this way Client Management ensures that clients are evenly distributed across the frequency bands and access points to optimize overall WLAN performance. A requirement for this is that the WLAN modules and access points in a broadcast domain all transmit on the same SSID.

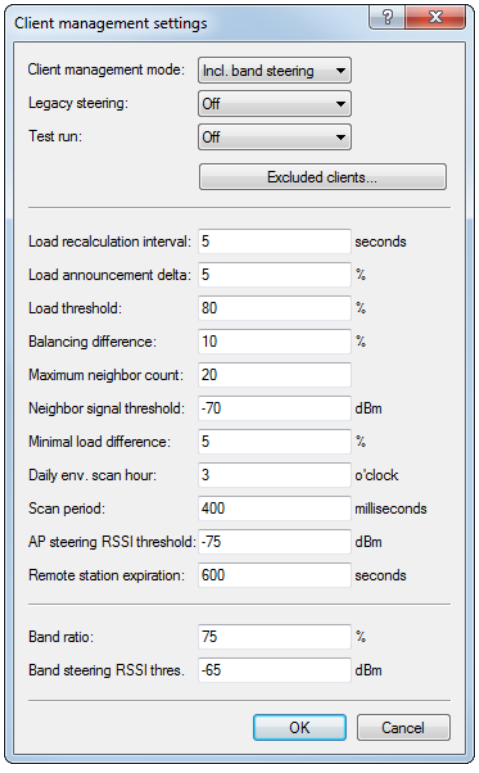
6.5.1 Configuration of Client Management

Client Management is switched on and off under **Wireless LAN** > **Client Management** > **Client Management** > **Management mode**. For new installations, this is turned on by default and usually does not require any special settings. As an alternative for access points with multiple WLAN modules, **AP-based band steering** can also be activated.



Expert settings

The settings for Client Management are configured under **Wireless LAN** > **Client Management** > **Expert settings** > **Client Management**. The default settings are ideal for operating Client Management in offices and school environments.



Client Management mode

Access points with multiple WLAN modules can operate Client Management with and without band steering.

Default setting:with band steering

Legacy steering

Configures whether clients that do not fully support 802.11v are also directed to other access points by Client Management. Even with legacy steering activated, Client Management first steers the 802.11v-capable clients to other access points; only then does it steer the clients that do not support 802.11v. Legacy steering forcibly disconnects these clients from the WLAN. The AP prevents the client from re-associating with it for a certain period, so that the client itself selects another access point. Compared to clients steered with 802.11v, this can lead to a poorer user experience, although this depends mainly on the behavior of the legacy clients.

Default setting: Off

Test run

Operates the Client Management in test mode: Environment scans are performed and steering decisions are made by the system and recorded to the syslog, but no actual client steering takes place. Use the test run to test the behavior of Client Management without actually making changes to your network.

Default setting: Off

Excluded clients

In many environments, there are certain clients that are known to be unresponsive. Imagine a hospital with custom VoIP phones that are unable to properly handle dropped calls and that tend to stick to a certain access point. To avoid having to switch off Client Management completely, you can exclude these clients from client steering.

Use the table to configure the MAC addresses of the clients that are to be excluded from client steering. The wildcard character `*` can be used, which stands for any characters. However, this must not be used as the only character of a MAC address. Possible entries are, for example `01:23:45:12:34:56`, `01:*:56` or `01:23:*`.

Load recalculation interval

Configures the interval at which the load on the AP is calculated and decisions are made to steer the clients. Increase the value to reduce the load on the network. Decrease the value to steer clients faster. Values < 2 seconds are not recommended as this negatively impacts network performance. Values > 10 seconds are not recommended as client steering does not happen in time. We recommend that you use the default value.

Default value: 5 seconds

Load announcement delta

Configures the percentage change in current load at which an access point communicates the load to other access points outside of the regular announcement interval. Increase the value in installations with many mobile clients. Decrease the value in installations with fewer moving clients. The default setting has been chosen for office and school environments. Note that this value should be lower than the value configured for the balancing difference to avoid miscalculations.

Default value: 5 %

Load threshold

Configures the load threshold at which the access point starts steering regardless of the load threshold of the neighbor access points. Increase the value in low-quality/high-density scenarios such as stadiums. Decrease the value in high-quality/high-throughput scenarios such as offices/schools.

Default value: 80 %

Balancing difference

Configures the load difference between access points at which clients are steered to the access point with the lesser load. High values lead to less balanced installations, low values lead to more steering of the clients. Increase the value if excessive client steering is happening. Decrease the value to achieve maximum balancing across the installation. The default setting has been chosen for office and school environments.

Default value: 10 %

Maximum neighbor count

Configures the number of neighbor access points that Client Management on this access point takes into consideration. In high-density scenarios, a lower number can be advantageous as clients are predominantly steered to nearby access points and less management communication is required between the access points. Values < 4 are not recommended, as there are not enough available access points for useful steering decisions. Values > 72 are not supported due to limitations of the 802.11 protocol.

Default value: 20 APs

Neighbor signal threshold

Configures the signal strength that an AP must display in order to be classified as a neighbor access point. Increase the value for high-density scenarios (for example: -60, -50). Decrease the value for scenarios where widespread coverage is required (e.g. -80, -90).

Default value: -70 dBm

Minimum load difference

Configures the minimum load difference between neighboring access points for steering to be performed between these access points. Steering is only performed when the configured load threshold is exceeded. To avoid miscalculation, the minimum load difference should not exceed the value for balancing difference. Increase the value for less steering in the installation. Decrease the value for more steering in the installation.

Default value: 5 %

Daily env. scan hour

Configures the time (00-23) at which the daily environment scan is performed as required by Client Management. The exact time of the scan is spread over a 30-minute window to minimize conflicts between concurrent environment scans. The environment scan takes about 15 seconds. No WLAN data is exchanged while the WLAN module is scanning.

Default value: 03:00 hours

Scan period

Configures the length of the environment scan used to identify neighbor access points. The scan period should be 2 to 2.5 times the configured beacon interval; the default value is suitable for the default beacon interval. This value can be configured from 200 ms to 1000 ms.

Default value: 400 ms

AP steering RSSI threshold

The signal strength that a client must have on a remote access point in order to be steered to it.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to access points with a poor signal quality. Clients may even refuse to be steered to an access point with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the access points they are being steered to.

The default value is ideal for office environments.

Default value: -75 dBm

Remote station expiration

Time for which an access point remembers the information about the clients of a neighboring access point. This information is used to speed up the steering decisions. The default value suits office environments with a relatively static set-up and few moving clients. Set lower values in environments with larger numbers of moving clients or with clients that connect for a short time only. Values that are too high lead to incorrect steering if the information of the cache no longer applies.

Default value: 600 seconds

Band ratio

Configures the intended distribution of clients between the radio bands. The configured ratio specifies what proportion of clients should be steered to the 5-GHz band.

Default value: 75 %

Band steering RSSI threshold

Configures the signal strength (RSSI) that a client "displays" on the other radio band in order to be steered there. The default setting is suitable for office environments.

Default value: -65 dBm

6.5.2 Additions to the Setup menu

Client Steering

This is where you specify the settings for the Client Management and the WLAN Band Steering for WLAN clients registered at the access point.

SNMP ID:

2.12.87

Telnet path:

Setup > **WLAN**

Operating

This option enables WLAN Band Steering or Client Management in the access point.

SNMP ID:

2.12.87.1

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Client Management

Enables Client Management in the access point. The percentage settings given below refer to the maximum load of an access point. This is set to 80 clients and cannot be changed.

Radio-Band

Enables WLAN band steering in the access point.

No

Switches this feature off. With this setting, these features are managed by a WLC, for example.

Default:

No

Dry-Run

Client Management performs a test run. The scans are performed, decisions are calculated and logged, but not executed.

SNMP ID:

2.12.87.6

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

No
Yes

Default:

No

Load-Recalculation-Interval

Interval in seconds, after which the load of the access point is calculated in Client Management. This results in the decision as to whether clients should be steered. If yes, then steering also takes place within this interval.

A higher value reduces the network load and has a limited positive effect in very large networks. A lower value leads to faster client steering. However, you should not go below 2 or above 10 seconds.

SNMP ID:

2.12.87.7

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Special values:

0

This value disables the delay.

Default:

5

Load-Announcement-Delta

If Client Management detects a change in load that exceeds the specified percentage value, then messages outside of the usual interval report this load to the neighboring access points that were discovered by scan. The value should be increased in environments with many moving devices. The default of 5% (4 clients) is suitable for environments with few moving devices, e.g. in offices or classrooms.

SNMP ID:

2.12.87.8

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0–9]`

Default:

5

Load-Threshold

Percentage load threshold at which Client Management on an access point attempts to steer devices associated with it, irrespective of the load on neighboring access points. Increase the value in difficult environments with poor transmission quality or a high density of associated devices. In optimal environments with a high transmission quality and high throughput, such as in offices or classrooms, the load threshold can be reduced. The default of 80% (64 clients) lies between these extremes.

SNMP ID:

2.12.87.9

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0–9]`

Default:

80

Balancing-Difference

Relating to Client Management, this is the percentage difference in load between two neighboring access points, at which point the access point with the higher load attempts to steer clients to the access point with a lower load. A high value leads to an unbalanced scenario, while a low value leads to more steering attempts. If too many steering attempts

are observed, this value should be increased. If a balanced scenario is a priority, then you have to reduce this value. The default of 10% (8 clients) difference should be suitable an office or classroom environment.

SNMP ID:

2.12.87.10

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 10 characters from `[0-9]`

Default:

10

Maximum-Neighbor-Count

Relating to Client Management, this is the number of neighboring access points taken into account for client steering and for the exchange of information between the access points. High-density environments benefit from a lower value, as clients can be steered to nearby access points with reduced communication between the access points. As a minimum you should consider 4 access points. The maximum is 72 access points, which is a limitation of the 802.11 protocol. Increasing the value to more than the default value of 20 produces no significant improvements.

SNMP ID:

2.12.87.11

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Default:

20

Neighbor-Signal-Threshold

Signal strength in dBm at which Client Management classifies an access point as a neighbor. Lower values (-80, -90) are useful for networks that cover a wider area. Higher values (-60, -50) are useful in high-density environments.

SNMP ID:

2.12.87.12

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 4 characters from `-[0-9]`

Default:

-70

Legacy-Steering

Normally, Client Management only attempts to steer clients to a different access point that correctly supports the 802.11v protocol. If you set this parameter to "Yes" then steering is attempted for every client. During a steering event, the client is denied access to the access point for a period. The intention is to force it to switch to another access point. From the user's perspective, the WLAN simply appears to be gone for a while.

SNMP ID:

2.12.87.13

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

No
Yes

Default:

No

Minimal-Load-Difference

Relating to Client Management, this is the minimum percentage load difference between access points at which client steering takes place. Only applies if the load threshold is exceeded. Should not be set to a larger value than "Balancing-Difference" as the calculations could be incorrect. Also, no lower than 2%, otherwise there is a risk that a client is moved back and forth between two access points.

A low value results in more steering events in high-load environments. This may be useful in environments where the clients are relatively stationary. A high value results in fewer steering events, which is useful in environments with high loads and numerous mobile clients.

SNMP ID:

2.12.87.14

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Default:

5

Daily-Env-Scan-Hour

Time at which an environment scan is performed when Client Management is enabled. The scan is performed at random within a 30-minute time window to minimize the chance of access points conflicting. A scan takes about 15 seconds with "Scan-Period" in the default setting. The access point is unavailable to clients throughout the scan, so the least possible number of clients should be active at the selected time. The default is 3 o'clock in the morning.

SNMP ID:

2.12.87.15

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

0 … 23

Default:

3

Scan-Period

Time in milliseconds that the client-management environment scan searches for other access points on a given channel. This should be 2 to 2.5 times your own beacon interval. The default value works with a common beacon interval. Higher values are only necessary with higher beacon intervals, although this increases the risk of scan conflicts when the access point is starting or during the nightly scans.

SNMP ID:

2.12.87.16

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

200 … 1000

Default:

400

AP-Steering-RSSI-Threshold

The signal strength in dBm that a client must have on a remote access point in order to be directed to it by Client Management.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to access points with a poor signal quality. Clients may even refuse to be steered to an access point with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the access points they are being steered to.

The default value is ideal for office environments.

SNMP ID:

2.12.87.17

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 4 characters from `-[0-9]`

Default:

-75

Remote-Station-Expiration

Time in seconds for which an access point remembers the information about the clients of a neighboring access point. This information is used to speed up the steering decisions made by the Client Management. The default value suits office environments with a relatively static set-up and few moving clients. Set lower values in environments with larger numbers of moving clients or with clients that connect for a short time only. Values that are too high lead to incorrect steering if the information of the cache no longer applies.

SNMP ID:

2.12.87.18

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 5 characters from `[0-9]`

Default:

600

Blacklist-Clients

In many environments, there are certain clients that are known to be unresponsive. Imagine a hospital with custom VoIP phones that are unable to properly handle dropped calls and that tend to stick to a certain access point. To avoid having to switch off Client Management completely, you can exclude these clients from client steering. Either explicitly or via wildcards. This provides the best user experience for compatible clients without affecting incompatible clients.

SNMP ID:

2.12.87.19

Telnet path:

Setup > **WLAN** > **Client-Steering**

MAC address

The MAC addresses of the clients to be excluded from client steering. The wildcard character `*` can be used, which stands for any characters. However, this must not be used as the only character of a MAC address. Possible entries are, for example `01:23:45:12:34:56`, `01:*:56` or `01:23:*`.

SNMP ID:

2.12.87.19.1

Telnet path:

Setup > **WLAN** > **Client-Steering** > **Blacklist-Clients**

Possible values:

Max. 20 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Start-Environment-Scan

This action manually starts the Client Management environment scan. This can be used if new access points have been added and they are not yet visible in the table of neighboring access points. Start the action using `do Start-Environment-Scan`.

SNMP ID:

2.12.87.20

Telnet path:

Setup > **WLAN** > **Client-Steering**

Client Management mode

Client Management operating mode. You can choose either to steer the clients between access points only or to additionally use band steering, which optimizes the frequency bands used by each access point.

SNMP ID:

2.12.87.21

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

AP-Steering
AP+Band-Steering

Default:

AP+Band-Steering

Band-Ratio

Ratio of distribution between bands in percent. This is used for the band-steering feature of Client Management.

The ratio indicates how many 5-GHz clients are able to connect to this access point. If more clients are connected at 5 GHz, clients are steered to 2.4 GHz. If more clients are connected at 2.4 GHz, clients are steered to 5 GHz.

Decrease the percentage if you are working with a channel width of 20 MHz in the 5-GHz band and your 2.4-GHz spectrum is free, i.e. there are few conflicting SSIDs and few other users such as Bluetooth. Choose a higher ratio if your 2.4-GHz band is full.

SNMP ID:

2.12.87.22

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 3 characters from `[0-9]`

Default:

75

Band-Steering-RSSI-Threshold

Signal strength in dBm that a client must have on the other band in order for it to be steered. This is used for the band-steering feature of Client Management.

A higher signal threshold reduces the number of potentially steerable clients, thus limiting the options available to the Client Management. At the same time this would be useful in environments with high quality demands, for example where VoIP is heavily used. This requires very good signal coverage and a higher density of access points.

A lower signal threshold increases the number of potentially steerable clients, although there is a risk that clients could be assigned to a band with a poor signal quality. Clients may even refuse to be steered to a band with a poorer signal quality. This is a help in environments with coverage over a large area. Values below -80 dBm produce poor results, as the likelihood increases that clients cannot connect to the band.

The default value is ideal for office environments.

SNMP ID:

2.12.87.23

Telnet path:

Setup > **WLAN** > **Client-Steering**

Possible values:

Max. 4 characters from `-[0-9]`

Default:

-65

Roaming-Targets

With Client Management enabled, the table under `/Status/WLAN/Roaming-Targets` is filled out automatically. The targets added manually to this table are also included into the list of neighbors by an 802.11k advertisement, even if they are out of range. The number of automatically added roaming targets is limited by *2.12.87.11 Maximum-Neighbor-Count*.

SNMP ID:

2.12.132

Telnet path:

Setup > **WLAN**

Name

Enter the name for the roaming target here.

SNMP ID:

2.12.132.1

Telnet path:

Setup > **WLAN** > **Roaming-Target**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

6.6 Return to the original 5 GHz channel when preference is configured

From HiLCOS 10.32, devices with WLAN module support the return to the original 5 GHz channel if a preference is configured. This feature allows you to keep to a channel plan as far as possible, even for installations that do not use indoor-only mode and may therefore be affected by channel changes due to radar detection.

If a WLAN channel or the WLAN channel list is configured for a WLAN module operated at 5 GHz and not in indoor-only mode, the channels entered there are preferred. Only if the channels set there have been blocked by radar detection will they be deviated from.

With the feature described here, the access point will attempt to switch back to the set channel after the DFS lock time has elapsed. If this channel is still not available, a channel configured in the channel list will be used. The DFS lock time takes effect as soon as a channel has been locked due to radar detection and is usually 30 minutes.

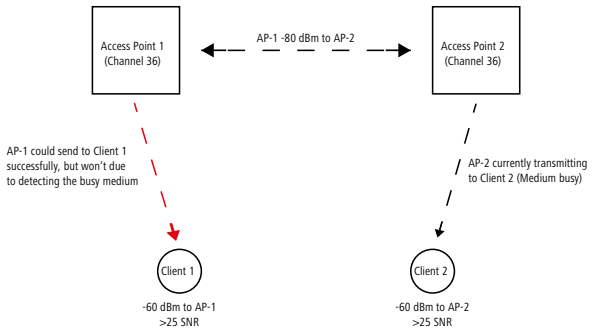
If no dedicated channel is configured for the WLAN module (channel list empty and radio channel "0" or "Automatic"), the previous behavior does not change. If a channel change is triggered by radar detection, the new channel is retained and not changed back to the last channel used.

This preference helps to be able to use fixed channel schemes in 5 GHz, since the full capacity of the network can be used faster after DFS events.

There is no configuration possibility. If you configure a WLAN channel or WLAN channel list for a WLAN module that is operated at 5 GHz and is not in indoor-only mode, this feature is automatically active.

6.7 Reduction of sensitivity for received packets

In high-density scenarios such as stadiums, exhibition halls or auditoriums, it is inevitable that access points that use the same channel will use the medium to a high capacity. This can result in a situation where the access points withhold their transmissions to the clients because the channel is recognized more often as busy.



An access point can be set artificially "deaf" by reducing the reception sensitivity from HiLCOS 10.32 onwards. This means that transmissions further away from the access point are "overheard" and the channel is detected more often as "free". In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer "heard". This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

You set the reduction via the console in value **Setup** > **Interfaces** > **WLAN** > **Radio-Settings** > **Rx-Packet-Sens.-Reduction**. The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

For WLAN controllers, this setting can also be made via the console in the profile of an access point. Under **Setup** > **WLAN-Management** > **AP-configuration** > **Accesspoints** adjust the values **Module-1-Rx-Packet-Sens.-Reduction** resp. **Module-2-Rx-Packet-Sens.-Reduction** accordingly.

This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

6.7.1 Additions to the Setup menu

Rx-Packet-Sens.-Reduction

An access point can be set artificially "deaf" by reducing the reception sensitivity. This means that transmissions further away from the access point are "overheard" and the channel is detected more often as "free". In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer "heard". This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

SNMP ID:

2.23.20.8.35

Telnet path:

Setup > **Interfaces** > **WLAN** > **Radio-Settings**

Possible values:

0 … 20

Module-1-Rx-Packet-Sens.-Reduction

An access point can be set artificially "deaf" by reducing the reception sensitivity. This means that transmissions further away from the access point are "overheard" and the channel is detected more often as "free". In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer "heard". This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

SNMP ID:

2.37.1.4.37

Telnet path:

Setup > **WLAN-Management** > **AP-configuration** > **Accesspoints**

Possible values:

0 … 20

Module-2-Rx-Packet-Sens.-Reduction

An access point can be set artificially "deaf" by reducing the reception sensitivity. This means that transmissions further away from the access point are "overheard" and the channel is detected more often as "free". In simplified terms, more simultaneous transmissions on the same channel are possible. On the one hand, this increases the overall throughput of a system, but on the other hand, the interference on the client side also increases.

Because a client does not know anything about the artificial hearing loss, it continues to receive the desired signals from its access point as well as the signals from other access points on the same channel. Only if the signal-to-noise ratio (SNR) remains good, the the additional transmissions will be received properly by the client thanks to this feature. Another side effect of the clients' ignorance is that a value set too high can reverse the effect. Since the access point cannot distinguish between transmissions from its own clients and from other devices—both access points and clients—only what is above the set threshold is heard—no matter from whom it comes. It may happen that the transmission of a connected client from the access point is no longer "heard". This results in an asymmetrical connection, the client may still receive the access point properly and therefore assumes a good connection, while the access point does not notice anything from the client anymore and ignores it. It is recommendable to set the reduction so that there is no discrimination against clients.

The value range from 0-20 corresponds to a minimum reception strength in the range from -95 dBm (0) to -75 dBm (20). In principle, Wi-Fi radio modules are subject to manufacturing variations. As a result, the real reception strength can deviate slightly.

This feature is for experts! As already mentioned in the description, instead of adding value, it can also have the opposite effect and disrupt transmissions on the access point side. On the one hand, the reduction should be configured with a buffer to the usual RSSI values of the clients on the access point side. On the other hand, the retries and Wi-Fi quality indices must be observed. If these deteriorate significantly after increasing this value, this indicates that the value is too high.

SNMP ID:

2.37.1.4.38

Telnet path:

Setup > **WLAN-Management** > **AP-configuration** > **Accesspoints**

Possible values:

0 … 20

6.8 Separate switch to enable e-mail notification

Previously, e-mail notifications were sent whenever an e-mail address was present in the corresponding field of the configuration. This implicit behavior has now been replaced by an additional operating mode switch that controls the sending of notifications.

You can find the new switch under **Wireless LAN** > **General**. **Send e-mails** controls whether notifications are sent to the e-mail address specified in **E-Mail address for WLAN events**.

6.8.1 Additions to the Setup menu

Mail-Address

Information about events in the WLAN is sent to this e-mail address if this is enabled with the 2.12.141 switch.

An SMTP account must be set up to make use of the e-mail function.

SNMP ID:

2.12.41

Telnet path:

Setup > **WLAN**

Possible values:

Max. 254 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

empty

Send-Mails

Determines whether notifications about WLAN events are sent to the e-mail address specified in 2.12.41 .

SNMP ID:

2.12.141

Telnet path:

Setup > **WLAN**

Possible values:

No
Yes

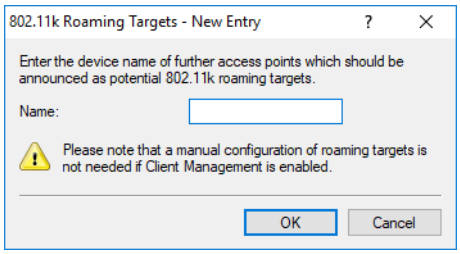
Default:

No

6.9 IEEE 802.11k Roaming Targets

The IEEE 802.11k standard describes a way to inform WLAN clients about potential roaming targets, i.e. additional access points of the same SSID that are within range. This information is sent to the client in the "Neighbor Report" as defined for the standard. 802.11k has so far been used as part of the client management, so it does not need to be configured separately. In some cases or in special scenarios, it may be necessary to dispense with automatic client management and to use the sub-feature 802.11k separately.

You can find the new table under **Wireless LAN** > **General** > **Extended settings** > **802.11k Roaming Targets**. Enter the potential roaming targets here.



6.9.1 Additions to the Setup menu

Roaming-Targets

With Client Management enabled, the table under /Status/WLAN/Roaming-Targets is filled out automatically. Additionally, any targets added manually to this table are also included in the list of neighbors in an 802.11k advertisement, even if they are out of range. The number of automatically added roaming targets is limited by "Maximum-Neighbor-Count" (see 2.12.87.11).

SNMP ID:

2.12.132

Telnet path:

Setup > **WLAN**

Name

As a part of client management, the names of the roaming targets for this access point are entered here after an environment scan. This is a part of the standard IEEE 802.11k. This standard describes a way to inform WLAN clients about potential roaming targets, i.e. additional access points of the same SSID that are within range. This information is sent to the WLAN client in the “Neighbor Report” as defined for the standard.

Client management makes these entries automatically. In some cases or in special scenarios, it may be necessary to dispense with automatic client management and to use the sub-feature 802.11k separately. In this case, you enter the device names of the potential roaming targets here, i.e. other access points of the same SSID.

The device name is used so that further required information about the potential roaming target (e.g. the channel number) can be communicated via IAAP. For this reason it is necessary for the participating access points to communicate with one another via IAPP.

Depending on the scenario, it may be desirable for a dual-radio access point to communicate its own, second WLAN module as a potential roaming target. In this case, the device’s own name can also be entered into the table.

SNMP ID:

2.12.132.1

Telnet path:

Setup > **WLAN** > **Roaming-Target**

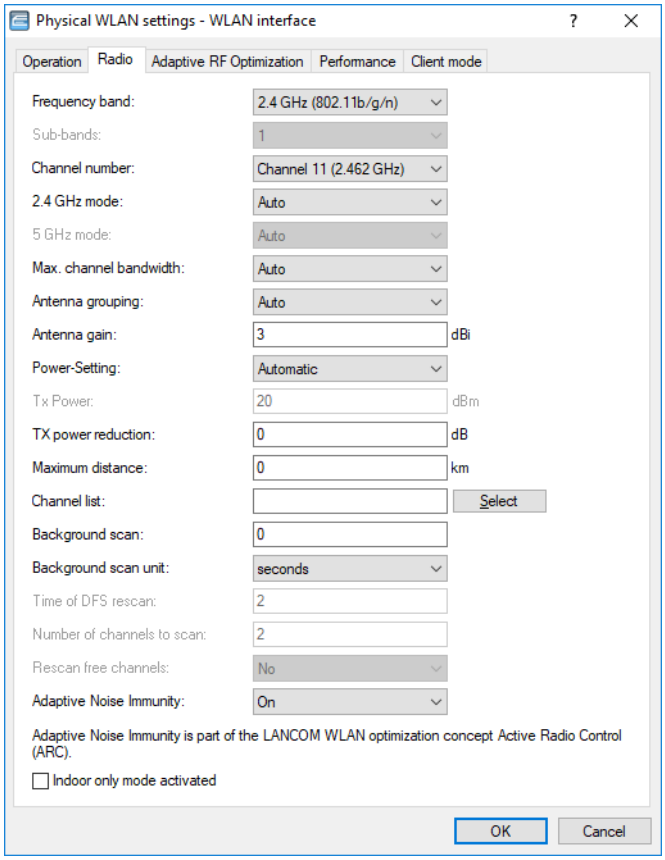
Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

6.10 Setting target EIRP

In versions before HiLCOS 10.32, the current WLAN transmission power could be reduced by a fixed, configured value. This made it possible to adapt the WLAN cell size to the requirements of any particular scenario. This method reaches its limits in the case of a professional WLAN where a value has been set for the actual maximum wireless transmission power and, at the same time, clients should automatically change between the channels of the different 5-GHz subbands. For example, higher transmission powers are permitted in the 5-GHz subband 2 than in subband 1. The fixed reduction in transmission power would be applied to the higher transmission power in subband 2 and also to the lower transmission power permitted in subband 1. This would result in cells of different sizes, depending on the subband selected. As of HiLCOS 10.32, the actual maximum transmission power can be set as an absolute value, which means that the cell size is always the same, irrespective of the maximum permitted transmission power.

Configure this in LANconfig under **Wireless LAN** > **General** > **Physical WLAN settings** > **Radio** using the fields **Power setting** and **Tx Power**.



The **Automatic** mode describes the previous behavior, whereas **Manual** allows an absolute value in dBm to be specified in the field **Tx power**.

Under no circumstances will the access point exceed the legal limits for transmission power. These are always respected automatically, regardless of the settings made here.

6.10.1 Additions to the Setup menu

Power-Setting

In versions before HiLCOS 10.32, the current WLAN transmission power could be reduced by a fixed, configured value. This made it possible to adapt the WLAN cell size to the requirements of any particular scenario. This method reaches its limits in the case of a professional WLAN where a value has been set for the actual maximum wireless transmission power and, at the same time, clients should automatically change between the channels of the different 5-GHz subbands. For example, higher transmission powers are permitted in the 5-GHz subband 2 than in subband 1. The fixed reduction in transmission power would be applied to the higher transmission power in subband 2 and also to the lower transmission power permitted in subband 1. This would result in cells of different sizes, depending on the subband selected. As of HiLCOS 10.32, the actual maximum transmission power can be set as an absolute value, which means that the cell size is always the same, irrespective of the maximum permitted transmission power.

Under no circumstances will the access point exceed the legal limits for transmission power. These are always respected automatically, regardless of the settings made here.

SNMP ID:

2.23.20.8.33

Telnet path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Automatic

The maximum permitted transmission power that can be realized by the hardware of the access point is used.

Manual

The desired transmission power is to be set in dBm in the EIRP field.

If the hardware of the access point is not capable of the desired transmission power, the maximum possible value is set automatically. The actual value can be checked in LANmonitor or on the CLI by means of the command `show wlan`.

Default:

Automatic

EIRP

With the setting for WLAN transmission power in 2.23.20.8.33 is set to manual, the value set here is taken in dBm.

SNMP ID:

2.23.20.8.34

Telnet path:

Setup > **Interfaces** > **WLAN** > **Radio-settings**

Possible values:

Max. 4 characters from `[0-9]-`

7 WLAN management

7.1 WLC features in the Hirschmann BAT-Controller Virtual

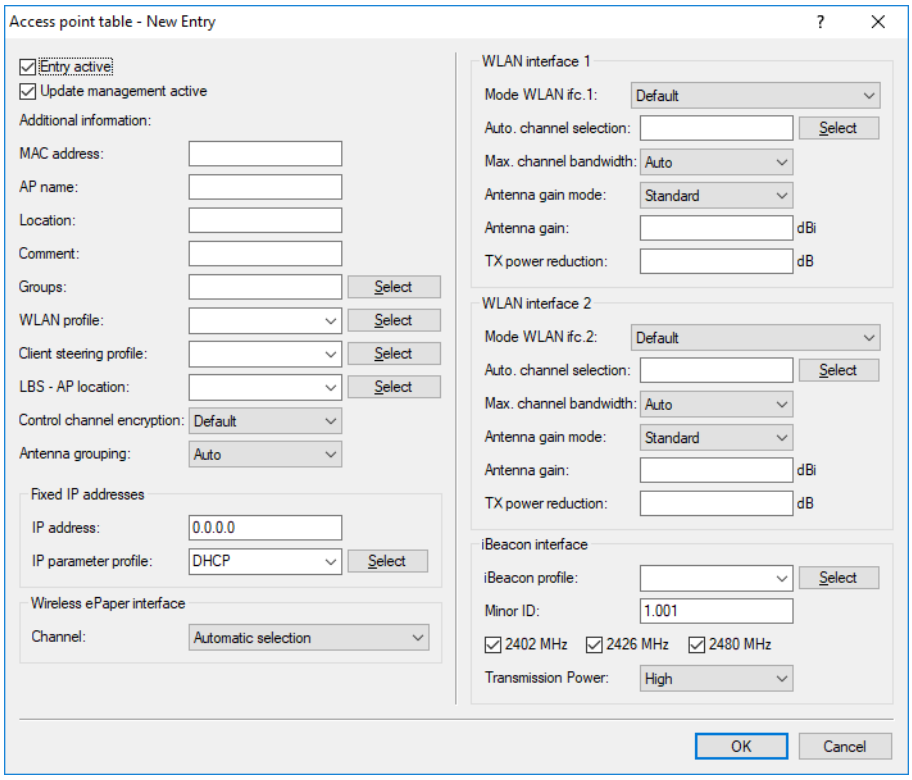
You decide which role your BAT-Controller Virtual should play: VPN gateway or WLAN controller. The BAT-Controller Virtual supports the role of a virtual WLC (vWLC), which means it is capable of managing access points. This fully virtualizes the functions of a WLAN controller on virtualization platforms such as VMWare ESXi or Microsoft Hyper-V. The number of managed access points depends on the license category.

Product	VPN licenses	AP licenses
BAT-Controller Virtual 100	100	100
BAT-Controller Virtual 200	200	200
BAT-Controller Virtual 1000	1000	1000

7.2 New mode for antenna gain

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. As of HiLCOS 10.32, there is a configuration option, that the standard antenna gain of a managed access point can be transmitted to the WLAN controller and is used there automatically. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.32. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

This is configured in LANconfig under **WLAN Controller** > **AP Configuration** > **Access point table** using the fields **Antenna gain mode** for each WLAN interface.



Antenna gain mode

Possible values:

Standard

The antenna gain value preset in the access point is used.

Userdefined

The value entered in the field **Antenna gain** is used.

7.2.1 Additions to the Setup menu

Module-1-Ant-Gain-Mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. As of HiLCOS 10.32, there is a configuration option, that the standard antenna gain of a managed access point can be transmitted to the WLAN controller and is used there automatically. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.32. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

SNMP ID:

2.37.1.4.35

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Standard
The antenna gain value preset in the access point is used.

User defined
The value for **Module-1-Ant-Gain** is used.

Default:

Standard

Module-2-Ant-Gain-Mode

Until now, access points commissioned with a WLAN controller have been set up with an antenna gain of 3 dBi per module, as this is the most suitable value for most indoor access points equipped with standard antennas. As of HiLCOS 10.32, there is a configuration option, that the standard antenna gain of a managed access point can be transmitted to the WLAN controller and is used there automatically. This feature only works if both the access point and the WLAN controller have at least the firmware version 10.32. This setting for the antenna gain mode prevents you from having to manually correct some of the access points after a rollout.

SNMP ID:

2.37.1.4.36

Telnet path:

Setup > **WLAN-Management** > **AP-Configuration** > **Accesspoints**

Possible values:

Standard
The antenna gain value preset in the access point is used.

User defined
The value for **Module-2-Ant-Gain** is used.

Default:

Standard

8 Virtual Private Networks – VPN

8.1 OCSP server

As of HiLCOS 10.32, Hirschmann devices support a server/responder for the Online Certificate Status Protocol (OCSP).

The Online Certificate Status Protocol (OCSP) is a procedure defined in RFC 6960 for checking the validity of a certificate at a central instance. Unlike certificate revocation lists (CRLs), the full CRL does not need to be downloaded periodically; instead, an on-demand OCSP request is made to the OCSP server when the connection is established, which ensures that the information about the validity of the certificate is always up-to-date. Only a small amount of data is transmitted since only the validity information for a certificate is sent. Compared to the CRL-based method, the validity information is always up-to-date and verification is faster.

The OCSP server can only be used in conjunction with a certification authority (CA) on the same device (Smart Certificate). The OCSP server is not able to provide validity information for certificates from other CAs.

In order for the OCSP server to be used to generate certificates per Smart Certificate, it must be assigned a certificate and a new entry is required in the profile for certificate creation in order to identify the OCSP server.

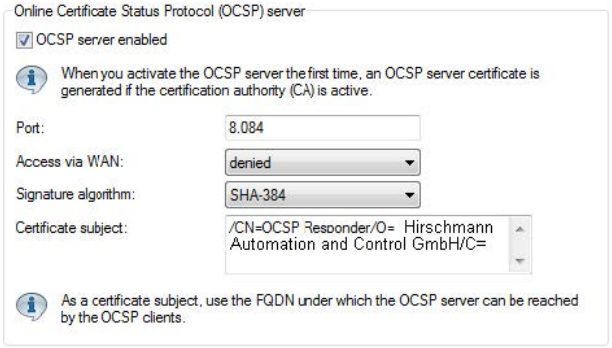
8.1.1 Configuring the OCSP server

Take the following steps to configure the OCSP server:

1. Enable the OCSP server under **Certificates** > **OCSP** > **Online Certificate Status Protocol (OCSP) server** > **OCSP server enabled**.
2. Assign a certificate to the OCSP server.

   Operating the OCSP server requires it to receive a certificate from the CA whose certificates it should provide information about. This certificate is used to sign the OCSP responses.

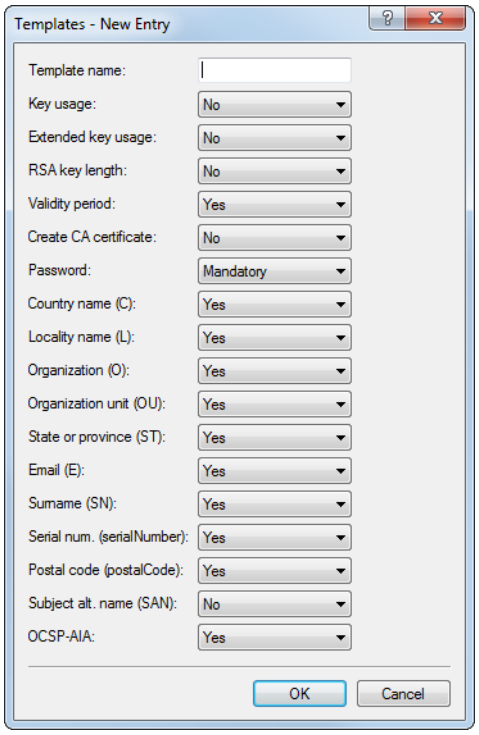
   For this purpose, go to **Certificates** > **OCSP** > **Online Certificate Status Protocol (OCSP) server** and configure the **Certificate subject** for the OCSP server. When the server is activated for the first time, this information is used to automatically generate the certificate for the OCSP server.



   In the certificate subject, enter CN as the FQDN where OCSP clients can reach the OCSP server.

3. Provide information about the OCSP server to the Smart Certificate preconfiguration
   a) Under **Certificates** > **Certificate handling** > **CA web interface** > **Templates**, you can specify that when Smart Certificate CA generates a certificate, the field "OCSP-AIA" (Authority Information Access) is available for

configuration. If you use the "Default" template, this is automatically the case. If you use a custom template, then set the field “OCSP-AIA” to Yes.

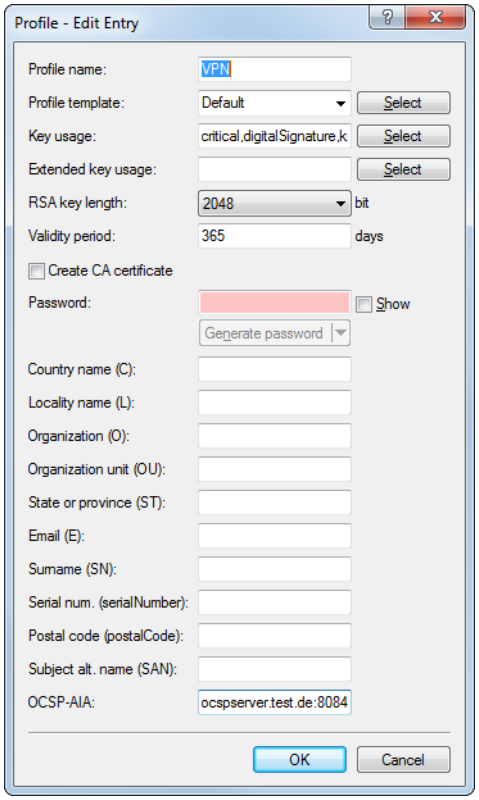


b) Under **Certificates** > **Certificate handling** > **CA web interface** > **Profile** you set a default value for the field OCSP-AIA in the desired Smart Certificate profile.

This step is optional. If you do not specify a default value here, you must manually specify a value when creating a certificate.

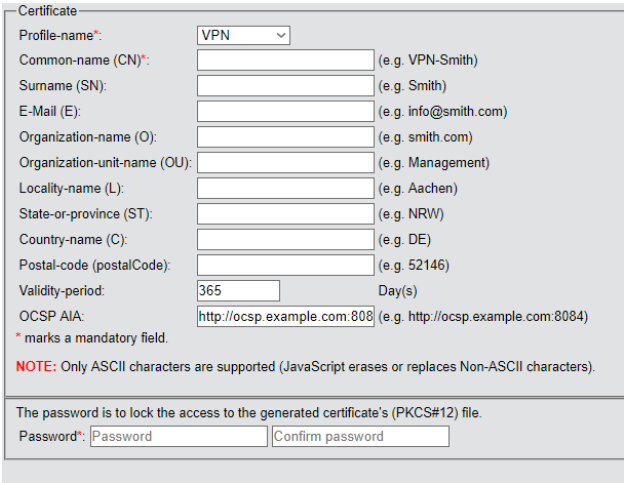
Configure the name or IP address where the OCSP server is available to the OCSP clients. This was already used earlier when generating the OCSP server certificate. Also add the port number where the OCSP server can be reached. The default setting is port 8084.

In the example, the default value for the profile "VPN" is adapted to "ocspserver.test.de:8084":



This concludes the configuration of the OCSP server.

If you now use Smart Certificate in WEBconfig to generate a certificate , the OCSP AIA is automatically added to it, so enabling the client to contact the OCSP server for a validity check during connection establishment.



The OCSP server refers to its internal certificate list to check the validity. All in all, the Smart Certificate web interface offers a convenient way to withdraw or validate the certificates.

8.1.2 Additions to the Setup menu

OCSP-AIA

Enter the name or IP address where OCSP clients can reach the OCSP server.

SNMP ID:

2.39.2.14.1.19

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Profiles**

Possible values:

Max. 254 characters from `[A-Z][0-9]@{|}~!$%&'()+-/:;<=>?[\]^_.`

Default:

empty

OCSP-AIA

When creating a certificate using Smart Certificate, the field "OCSP AIA" (OCSP Authority Information Access) can be displayed.

SNMP ID:

2.39.2.14.2.18

Telnet path:

Setup > **Certificates** > **SCEP-CA** > **Web-Interface** > **Template**

Possible values:

Yes

The field is visible and can be changed by the user.

No

The field is invisible, the value entered is considered to be a default value.

Mandatory

The field is visible, the user must enter a value.

Fixed

The field is visible, but cannot be changed by the user.

Default:

Yes

OCSP server

This table contains the settings for the OCSP server.

SNMP ID:

2.39.7

Telnet path:

Setup > **Certificates**

Operating

Turn the OCSP server on or off here.

SNMP ID:

2.39.7.1

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Yes
No

Default:

No

Port

The port used by the OCSP server.

SNMP ID:

2.39.7.2

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Max. 5 characters from `[0-9]`

Default:

8084

Certificate-Subject

Operating the OCSP server requires it to receive a certificate from the certification authority (CA) whose certificates it should provide information about. This certificate is used to sign the OCSP responses. Here you enter the name or IP address where OCSP clients can contact the OCSP server, e.g.

```
/CN=ocspresponder.example.test/O=Hirschmann Automation and Control GmbH/C=DE
```

In the certificate subject, enter CN as the FQDN where OCSP clients can reach the OCSP server.

SNMP ID:

2.39.7.3

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

/CN=ocspresponder.example.test/O=Hirschmann Automation and Control GmbH/C=DE

WAN access

This setting determines if and how the OCSP server can be reached from the WAN.

SNMP ID:

2.39.7.4

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

Yes
No
Over-VPN

Default:

No

Signature-Algo

The algorithm used to generate the certificate used by the OCSP server.

SNMP ID:

2.39.7.5

Telnet path:

Setup > **Certificates** > **OCSP-Server**

Possible values:

SHA1
SHA-256
SHA-384
SHA-512

Default:

SHA-256

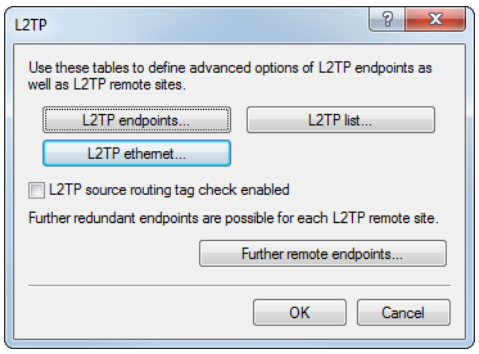
8.2 Layer-3 Ethernet tunnel with Layer-2 Tunneling Protocol version 3 (L2TPv3)

With L2TPv3, Ethernet traffic (layer 2) is tunneled over UDP. This allows LANs to be connected across network and site boundaries.

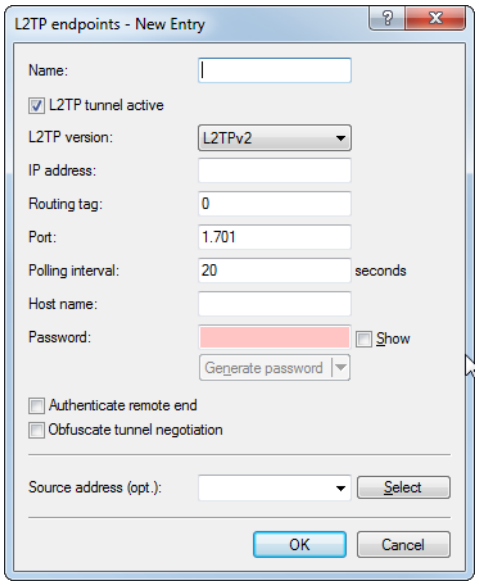
This is particularly useful for bridging WLAN traffic on access points to a central concentrator by means of an L2TPv3 Ethernet tunnel. Without L2TPv3, this would require the use of a WLAN controller operating CAPWAP layer-3 tunnels. L2TPv3 does not require WLAN controllers and this allows WLAN traffic to be bridged through tunnels to the central site.

From HiLCOS 10.32, layer-3 Ethernet tunnels can be configured to use L2TPv3. This is configured in the L2TP endpoints table, available since version 2 of the protocol, and in the new L2TP Ethernet table. For a corresponding scenario, see *Configuring a WLAN scenario for bridging payload data to the central site*.

With LANconfig, you configure L2TP under **Communication** > **Remote sites** > **L2TP**.



For version 3, the configuration of the L2TP endpoints table under **L2TP endpoints** was enhanced with the following parameters:



L2TP tunnel active

Enables the configured L2TP tunnel.

L2TP version

The L2TP protocol version used, either version 2 or 3.

Ethernet tunnels are only possible with version 3. In this case, be sure to set the protocol “L2TPv3” here.

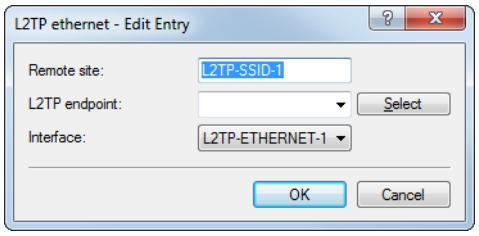
L2TPv3 in the HiLCOS is always encapsulated in UDP. This allows transmissions to pass through NAT gateways without problem.

If you specify an IP address or a host name, an attempt is made to establish a connection. If the corresponding field is left blank, no connection is established, but connections can be accepted. Configured properties such as the station name or password are checked by the remote site when the connection is established.

A number of implicit dependencies during the connection establishment and authentication are not directly apparent, so we will enlarge on these here:

- The host name transmitted by the remote site is checked to see whether it corresponds to a configured L2TP endpoint. The host name is configured in the L2TP endpoint table of the remote site under **Host name**. If this field is left blank, the device name is used for authentication instead.
- If this is the case, the connection is established using the configuration for the corresponding L2TP endpoint.
- If not, the L2TP endpoints table is checked to see if it contains a “wildcard” entry. This is an entry that contains no host/station name or routing tag. The connection is established using the configuration of the “wildcard” entry.
- If authentication is activated for the corresponding entry in the L2TP endpoints table, authentication is carried out based on the configured password.
- If the password field is empty and authentication is switched on, a RADIUS authentication is carried out.
- If authentication is turned off, a “wildcard” entry accepts any incoming tunnel accordingly.

Under **L2TP Ethernet** you link L2TPv3 sessions with one of the 16 L2TP virtual Ethernet interfaces. The L2TP virtual Ethernet interfaces can then be used elsewhere in the configuration, e.g. in the LAN bridge for linking to WLAN or LAN interfaces.



Remote site

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

L2TP endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint. If connections are to be accepted only, and not actively established from this end, leaving this field blank allows any sessions to be accepted. Of course, these still need "to run" via an accepted/established endpoint from the L2TP endpoints table. This can be useful in scenarios where not every endpoint on the receiving side should be configured separately.

Interface

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

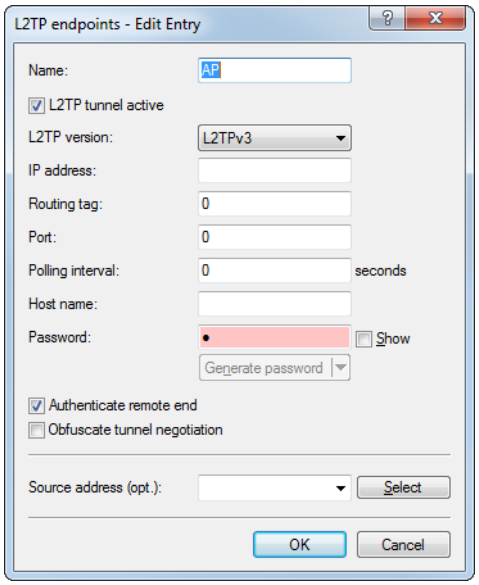
8.2.1 Configuring a WLAN scenario for bridging payload data to the central site

This is an example of how L2TPv3 is used in a scenario where several access points use bridging to transfer their payload data to a central router (referred to here as the "concentrator"), where the data are made available via a separate Ethernet port.

Before HiLCOS 10.32, this scenario would have required a WLAN controller.

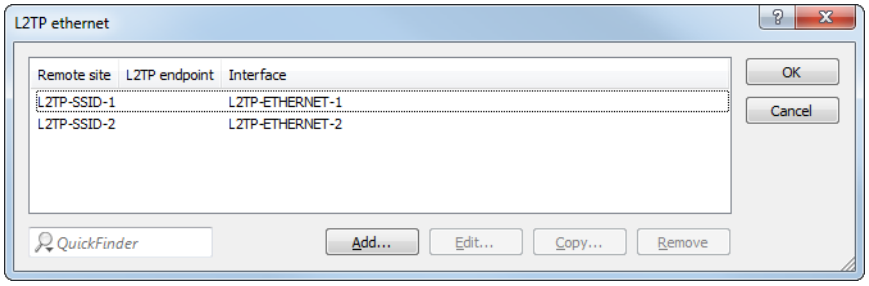
1. Prepare the WLAN configuration on the access points. To enable roaming, SSID names and encryption settings should be configured identically on each AP.
2. Now configure the concentrator, which is to accept the L2TPv3 Ethernet sessions from the individual access points.
   a) Under **Communication** > **Remote sites** > **L2TP** in the L2TP endpoints table, create an entry "DEFAULT". Enter a descriptive name for the new entry. Set the **L2TP version** to "L2TPv3". Do not specify an **IP address**. Set a

password to increase security and enable the "Authenticate remote end" option to use the password for authentication during connection establishment. Leave the remaining settings at their default values.



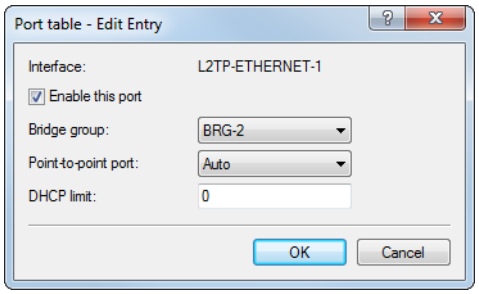
The **IP address** is empty. This is then a "wildcard" entry that can accept connections from any remote site.

b) Under **Communication** > **Remote sites** > **L2TP** in the L2TP Ethernet table, create a new entry. Use **Remote site** to set a name for the Ethernet tunnel, e.g. the name of the SSID to which the tunnel on the access points is to be linked. Leave the field **L2TP endpoint** empty so that any (authenticated) sessions can be accepted. This method avoids having to create an entry for each individual access point in the L2TP endpoint table: The wildcard entry created in the previous step is used instead. Under **Interface** you now configure the virtual interface to which the L2TP Ethernet tunnel is to be connected. If the access points operate multiple SSIDs that are to be bridged to the central site, use this table to create an entry for each SSID, each with a unique name under **Remote site**.



In our scenario, the payload data of all connected access points are routed to the virtual interface configured here. Furthermore, the payload data of all access points connected to this virtual interface are bridged to one another—rather like the WLAN controller-based layer-3 tunneling technique.

c) Under **Interfaces** > **LAN** > **LAN bridge settings** > **Port table**, link the virtual L2TP interface selected earlier to a LAN interface where you set the same bridge group. Repeat this for any additional L2TP virtual interfaces for additional SSIDs.

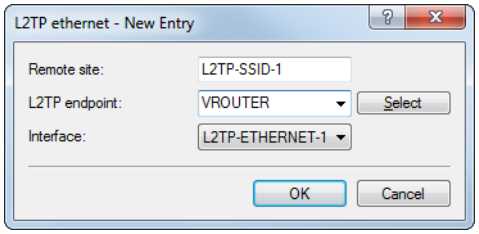


d) This concludes the configuration of the concentrator.

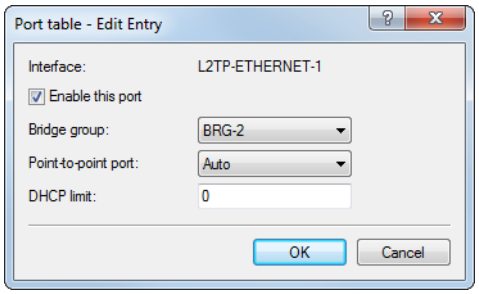
3. The following example shows how to configure an access point to transfer payload data to the concentrator.

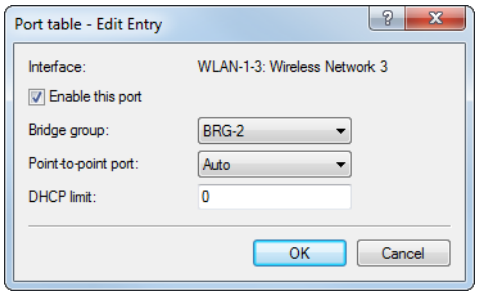
a) Under **Communication** > **Remote sites** > **L2TP**, create a new entry in the L2TP endpoints table. Enter a descriptive name for the new entry. Set the **L2TP version** to "L2TPv3". Enter the IP address or host name where the access point contacts the concentrator. Enter the password you set when configuring the concentrator and select "Authenticate remote end" to use the password for authentication. Leave the remaining settings at their default values.

b) Under **Communication** > **Remote sites** > **L2TP** in the L2TP Ethernet table, create a new entry. Under **Remote site**, enter a name that identifies the Ethernet tunnel. This must be the same as the name given to this Ethernet tunnel on the concentrator. In the field **L2TP endpoint**, select the L2TP endpoint table entry that was created in the previous step. This endpoint is then used to establish the Ethernet tunnel. Under **Interface** you now configure the virtual interface to which the L2TP Ethernet tunnel is to be connected.



c) Under **Interfaces** > **LAN** > **LAN bridge settings** > **Port table**, link the virtual L2TP interface selected earlier to a WLAN interface by setting the same bridge group. Repeat this for any additional L2TP virtual interfaces for additional SSIDs.





d) Carry out the configuration described here for the other access points. Once the configuration has been completed in this way, the identical configuration can be used on all of the access points and no further adaptations are necessary for the individual APs.

8.2.2 Additions to the Setup menu

Version

The L2TP protocol version used for this L2TP endpoint, either version 2 or 3.

Ethernet tunnels are only possible with version 3. In this case, be sure to set the protocol “L2TPv3” here.

SNMP ID:

2.2.35.11

Telnet path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

L2TPv2

Layer 2 Tunneling Protocol Version 2

L2TPv3

Layer 2 Tunneling Protocol Version 3

Operating

This L2TP endpoint is enabled or disabled.

SNMP ID:

2.2.35.12

Telnet path:

Setup > **WAN** > **L2TP-Endpoints**

Possible values:

No

L2TP endpoint is disabled.

Yes

L2TP endpoint is enabled.

L2TP-Ethernet

This table is used to link L2TPv3 sessions with one of the 16 L2TP virtual Ethernet interfaces. The L2TP virtual Ethernet interfaces can then be used elsewhere in the configuration, e.g. in the LAN bridge for linking to WLAN or LAN interfaces.

SNMP ID:

2.2.39

Telnet path:

Setup > **WAN**

Remote-End

Here you configure the name used to assign the Ethernet tunnel to the remote site. For each Ethernet tunnel, this name must be identical at both ends.

SNMP ID:

2.2.39.1

Telnet path:

Setup > **WAN** > **L2TP-Ethernet**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

L2TP endpoint

Here you configure the name of the L2TP endpoint configured in the L2TP endpoints table. This causes an Ethernet tunnel session to be established via this endpoint. If connections are to be accepted only, and not actively established from this

end, leaving this field blank allows any sessions to be accepted. Of course, these still need "to run" via an accepted/established endpoint from the L2TP endpoints table. This can be useful in scenarios where not every endpoint on the receiving side should be configured separately.

SNMP ID:

2.2.39.2

Telnet path:

Setup > **WAN** > **L2TP-Ethernet**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Interface

The virtual L2TP Ethernet interface to be used for the L2TPv3 session.

SNMP ID:

2.2.39.3

Telnet path:

Setup > **WAN** > **L2TP-Ethernet**

Possible values:

L2TP-ETHERNET-1 … L2TP-ETHERNET-16

16 virtual L2TP Ethernet interfaces

8.3 IKEv2

8.3.1 Configuring IKEv2 with LANconfig

IKEv2 is configured under **VPN** > **IKEv2/IPSec**.

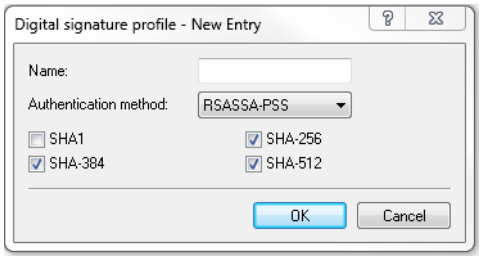
Digital signature profile

This table is used to specify the authentication methods for your VPN connections.

Digital signature profile

From HiLCOS 10.32, devices that are set to use the older RSASSA-PKCS1-v1_5 to negotiate with remote sites now also support the newer RSASSA PSS.

Use this table to configure the parameters for the IKEv2 authentication.



Name

Contains the unique name of this entry. You can assign this name in three different places. In the section **Authentication** in the fields **Local dig.signature profile** and **Rem. dig.signature profile**, and under **Extended settings** > **Authentification** > **Identities** > **Rem. dig.signature profile**.

Authentication method

Sets the authentication method for the digital signature. Possible values are:

- RSASSA-PSS: RSA with improved probabilistic signature schema as per version 2.1 of PKCS #1 (probabilistic signature scheme with appendix)
- RSASSA-PKCS1-v1_5: RSA according to the older version of the signature schema as per version 1.5 of PKCS #1 (probabilistic signature scheme with appendix)

If RSASSA-PKCS1-v1_5 is selected, a check is made to see whether the remote site also supports the superior RSASSA-PSS method and switches to it if necessary. If RSASSA-PSS is selected, then a fallback to the older RSASSA-PKCS1-v1_5 is not provided.

You also specify the secure hash algorithms (SHA) to be used.

Additions to the Setup menu

Auth-Method

Sets the authentication method for the digital signature.

If RSASSA-PKCS1-v1_5 is selected, a check is made to see whether the remote site also supports the superior RSASSA-PSS method and switches to it if necessary. If RSASSA-PSS is selected, then a fallback to the older RSASSA-PKCS1-v1_5 is not provided.

SNMP ID:

2.19.36.3.4.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Digital-Signature-Profiles**

Possible values:

RSASSA-PSS
RSASSA-PKCS1-v1_5

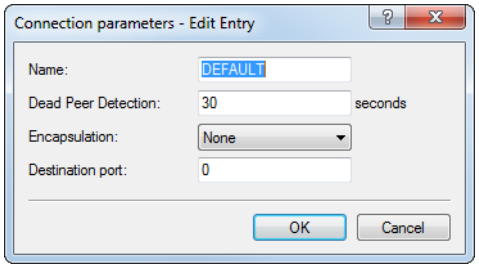
Default:

RSASSA-PSS

Connection parameters

From HiLCOS 10.32, the new parameters **Encapsulation** and **Destination port** are located in the table **VPN** > **IKEv2/IPSec** > **VPN connections** > **Connection parameters**.

Use this table to specify the parameters of IKEv2 VPN connections that are not included in the SA negotiation. An entry named "DEFAULT" is provided with common settings.



Encapsulation

In some scenarios, using the normal VPN port 500 is not an option, such as when firewalls are in the way. SSL or UDP can be set here. Use this in combination to configure any **Destination port**. The IKEv2 tunnel is established either with port 4500 for UDP or with the port set for the **Destination port**. If the destination port is set to 500, this will be ignored and port 4500 is used instead. For SSL, the tunnel is established either with port 443 or with the setting for the destination port. If the destination port is set to 500 or 4500, this will be ignored and port 443 is used instead. If set to "None", the port 500 is taken and the setting in **Destination port** is ignored.

The configurable port can be used for scenarios where a Hirschmann router already accepts VPN tunnels on the standard ports. A port forwarding rule would allow these ports to be forwarded to any destination.

Destination port

Here you can specify that the destination port depends on the setting in **Encapsulation**. If the setting is different from 500, UDP encapsulation is performed automatically.

Additions to the Setup menu

Encapsulation

In some scenarios, using the normal VPN port 500 is not an option, such as when firewalls are in the way. You can set the ports 443 or 4500 instead. Use this in combination to configure any **Destination-Port**. If the setting is different from 500, UDP encapsulation is performed automatically. The configurable port can be used for scenarios where a Hirschmann router already accepts VPN tunnels on the standard ports. A port forwarding rule would allow these ports to be forwarded to any destination.

Incoming VPN tunnels continue to be accepted on the default ports 443, 500 and 4500. These cannot be freely configured.

SNMP ID:

2.19.36.4.7

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

UDP

The IKEv2 tunnel is established either with port 4500 or with the setting for the destination port. If the destination port is set to 500, this will be ignored and port 4500 is used instead.

SSL

The IKEv2 tunnel is established either with port 443 or with the setting for the destination port. If the destination port is set to 500 or 4500, this will be ignored and port 443 is used instead.

None

The IKEv2 tunnel is established with port 500. The setting for the destination port is ignored.

Default:

None

Destination-Port

Here you can specify the destination port for the IKEv2 connection depending on the setting in **Encapsulation**. If the setting is different from 500, UDP encapsulation is performed automatically.

SNMP ID:

2.19.36.4.8

Telnet path:

Setup > **VPN** > **IKEv2** > **General**

Possible values:

Max. 5 characters from `[0-9]`

Default:

0

8.3.2 Elliptic Curve Digital Signature Algorithm (ECDSA)

As of HiLCOS 10.32, IKEv2 now supports Elliptic Curve Digital Signature Algorithm (ECDSA) as per RFC 4754 in addition to the authentication methods RSA Signature and Digital Signature.

ECDSA signatures are generally smaller than RSA signatures with comparable cryptographic strength. ECDSA keys and certificates also have significantly smaller file sizes than RSA-based keys and certificates. Furthermore, ECDSA operations are generally faster on most devices. The following methods are supported in IKEv2:

- ECDSA with SHA-256 on the P-256 curve
- ECDSA with SHA-384 on the P-384 curve
- ECDSA with SHA-512 on the P-521 curve

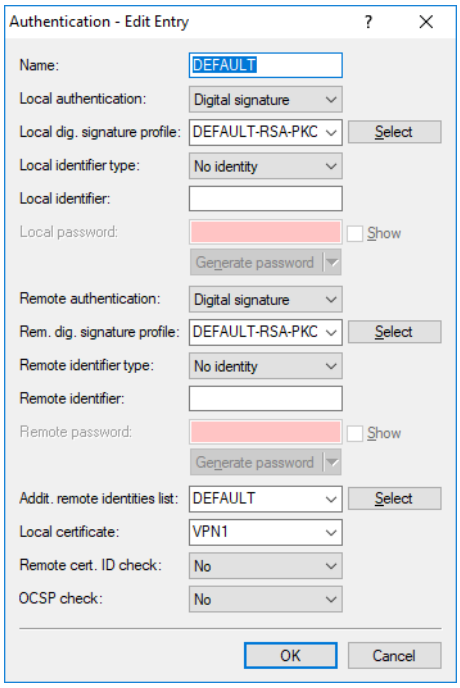
When using OpenSSL to generate certificates, the following predefined curves must be used as parameters for ECDSA in IKEv2:

- prime256v1 with ECDSA-256
- secp384r1 with ECDSA-384
- secp521r1 with ECDSA-512

The following restrictions apply when using ECDSA:

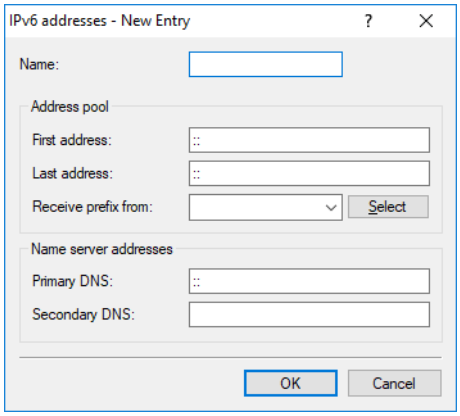
- The negotiation of ECDSA within the Digital Signature method is not supported.
- ECDSA-based certificates currently cannot be generated by the HiLCOS's own CA. Similarly, it is not possible
  to obtain certificates automatically by means of SCEP. ECDSA certificates must be generated using an external application such as OpenSSL or XCA and then loaded into the device.

In LANconfig under **VPN** > **IKEv2/IPSec** > **Authentication**, you can now select these methods for both **Local authentication** and **Remote authentication**.



8.3.3 IKEv2 configuration payload with a specified source for prefix delegation

As of HiLCOS 10.32 , the IKEv2 configuration payload supports the specification of a source for prefix delegation. In LANconfig, the configuration is located under **VPN** > **IKEv2/IPSec** > **IPv6 addresses**.



Address pool

Receive prefix from

With this parameter you can assign addresses to the VPN clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then set the parameter **First address** to the value "::1" in the **Last address** to "::9". In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g.,"/48" or "/56", you must take subnetting for the logical network into account in the address.

Example:

- Assigned provider prefix: 2001:db8:abcd:aa::/56
- /64 as the prefix of the logical network (subnet ID 1): 2001:db8:abcd:aa01::/64
- First address: 0:0:0:0001::1
- Last address: 0:0:0:0001::9

Currently no Neighbor Discovery Proxy is supported for IPv6. For this reason, the address range of the pool must not overlap with address ranges or prefixes that are already used for other networks on the router.

8.3.4 Split DNS

With VPN split tunneling, only those applications that are supposed to reach endpoints behind the VPN tunnel are sent through the VPN tunnel. All other traffic is sent directly to the Internet and not through the VPN tunnel. The IP networks which should be accessible through the tunnel are defined by VPN rules.

Split DNS allows DNS to resolve specific internal domains (e.g. "*.company.com") to a VPN tunnel, while other DNS requests are sent to a public DNS server. When establishing a connection, the IKE Config Mode server dynamically assigns one or more split-DNS domains to the client by means of the attribute INTERNAL_DNS_DOMAIN. The client enters the received domain list into its local DNS forwarding list. The client must support this attribute.

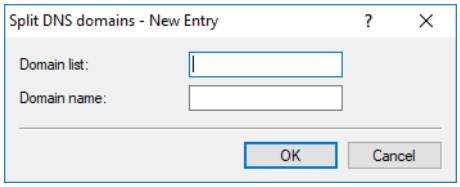
Split DNS for IKEv2 is supported by Hirschmann VPN routers in the role IKE Config Mode client and server. For site-to-site VPN connections, dynamic split-DNS assignment is not supported by the IKE protocol. Instead, the appropriate VPN endpoints have to be configured by means of static DNS forwarding.

The split-DNS configuration is assigned in the IKEv2 connection list when the CFG mode is set to "Server" and the split DNS profile has been selected.

In LANconfig you first specify the required domains under **VPN** > **IKEv2/IPSec** > **Split DNS domains** and assign these to a profile under **VPN** > **IKEv2/IPSec** > **Split DNS profiles**. This profile can then be selected in the **Connection list** under IKE config mode when **IKE-CFG** is set to **Server**.

Split DNS domains

In LANconfig, the split DNS domains are configured under **VPN** > **IKEv2/IPSec** > **Split DNS domains**.



Domain list

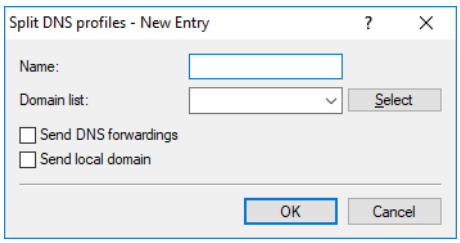
Enter a name for the domain lists.

Domain name

Split-DNS domain name that the VPN gateway should send to VPN clients, e.g. "company.internal". Multiple domain names can be configured by multiple entries with the same identifier from the domain list.

Split DNS profile

In LANconfig, the split DNS profiles are configured under **VPN** > **IKEv2/IPSec** > **Split DNS profiles**.



Name

Enter a name for this profile.

Domain list

Name of the list of split-DNS domains that the VPN gateway should send to VPN clients.

Send DNS forwardings

Here you set whether the VPN gateway should send its locally configured DNS forwardings to VPN clients.

Send local domain

Set whether the VPN gateway should send its own locally configured domain to VPN clients.

8.3.5 IKEv2 fragmentation

HiLCOS 10.32 supports IKEv2 fragmentation according to RFC 7383. This enables the VPN router to fragment IKEv2 messages by itself, which is more efficient than having IKE-packet fragmentation performed by the transport network. Two methods of IKEv2 fragmentation are supported:

- Manufacturer-specific fragmentation, compatible with third-party manufacturers
- Fragmentation as per RFC 7383

The device sets the best method automatically. If a VPN remote site supports both methods, fragmentation as per RFC 7383 is preferred.

8.3.6 IKEv2 password rules

HiLCOS 10.32 supports enforcing password rules for pre-shared keys. Navigate to **VPN** > **IKEv2/IPSec** > **Extended settings** and set the option **Enforce Preshared Key rules**. The following rules then apply for Pre-Shared Keys (PSK) with IKEv2:

- The length of the password must be at least 32 characters.
- The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

These rules do not apply to PSK managed and obtained by a RADIUS server.

8.3.7 Additions to the Setup menu

Split-DNS-Profile

Name of the Split DNS profile. The split DNS profile is only active if **IKE-CFG** is set to the value **Server**.

SNMP ID:

2.19.36.1.22

Telnet path:

Setup > **VPN** > **IKEv2** > **Peers**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Local-Auth

Sets the authentication method for the local identity.

SNMP ID:

2.19.36.3.1.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

RSA-Signature
Authentication by RSA signature.

PSK
Authentication by pre-shared key (PSK).

Digital signature
Use of configurable authentication methods with digital certificates as per RFC 7427.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-256 on the P-256 curve.

ECDSA-384
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-384 on the P-384 curve.

ECDSA-521
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-512 on the P-521 curve.

Default:

PSK

Remote-Auth

Sets the authentication method for the remote identity.

SNMP ID:

2.19.36.3.1.6

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Parameter**

Possible values:

RSA-Signature
Authentication by RSA signature.

PSK
Authentication by pre-shared key (PSK).

Digital signature
Use of configurable authentication methods with digital certificates as per RFC 7427.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-256 on the P-256 curve.

ECDSA-384
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-384 on the P-384 curve.

ECDSA-521
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-512 on the P-521 curve.

Default:

PSK

Remote-Auth

Sets the authentication method for the remote identity.

SNMP ID:

2.19.36.3.3.2

Telnet path:

Setup > **VPN** > **IKEv2** > **Auth** > **Addit.-Remote-IDs**

Possible values:

RSA-Signature
Authentication by RSA signature.

PSK
Authentication by pre-shared key (PSK).

Digital signature
Use of configurable authentication methods with digital certificates as per RFC 7427.

ECDSA-256
Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-256 on the P-256 curve.

ECDSA-384

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-384 on the P-384 curve.

ECDSA-521

Elliptic Curve Digital Signature Algorithm (ECDSA) according to RFC 4754 with SHA-512 on the P-521 curve.

Default:

PSK

PD-Source

With this parameter you can assign addresses to the VPN clients from the prefix that the router retrieved from the WAN interface via DHCPv6 prefix delegation. Select the desired WAN interface here. For example, if the provider assigned the prefix "2001:db8::/64", you can then set the parameter "First address" to the value "::1" in the "Last address" to "::9". In combination with the prefix "2001:db8::/64" as delegated by the provider, the clients receive addresses from the pool "2001:db8::1" to "2001:db8::9". If the provider prefix is greater than "/64", e.g.,"/48" or "/56", you must take subnetting for the logical network into account in the address.

Example:

- Assigned provider prefix: 2001:db8:abcd:aa::/56
- /64 as the prefix of the logical network (subnet ID 1): 2001:db8:abcd:aa01::/64
- First address: 0:0:0:0001::1
- Last address: 0:0:0:0001::9

SNMP ID:

2.19.36.7.2.6

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **IPv6**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Split-DNS

With VPN split tunneling, only those applications that are supposed to reach endpoints behind the VPN tunnel are sent through the VPN tunnel. All other traffic is sent directly to the Internet and not through the VPN tunnel. The IP networks which should be accessible through the tunnel are defined by VPN rules.

Split DNS allows DNS to resolve specific internal domains (e.g. "*.company.com") to a VPN tunnel, while other DNS requests are sent to a public DNS server. When establishing a connection, the IKE Config Mode server dynamically assigns one or more split-DNS domains to the client by means of the attribute INTERNAL_DNS_DOMAIN. The client enters the received domain list into its local DNS forwarding list. The client must support this attribute.

Split DNS for IKEv2 is supported by Hirschmann VPN routers in the role IKE Config Mode client and server. For site-to-site VPN connections, dynamic split-DNS assignment is not supported by the IKE protocol. Instead, the appropriate VPN endpoints have to be configured by means of static DNS forwarding.

SNMP ID:

2.19.36.7.3

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG**

Domain-Lists

Here you specify the domain lists for split DNS.

SNMP ID:

2.19.36.7.3.1

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS**

Domain-name

Split-DNS domain name that the VPN gateway should send to VPN clients, e.g. “company.internal”. Multiple domain names can be configured by multiple entries with the same identifier from the domain list.

SNMP ID:

2.19.36.7.3.1.1

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Domain-Lists**

Possible values:

Max. 64 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Domain-List

Enter a name for the domain lists.

SNMP ID:

2.19.36.7.3.1.3

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Domain-Lists**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Profiles

Here you set the profiles for split DNS.

SNMP ID:

2.19.36.7.3.4

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS**

Name

Enter a name for this profile.

SNMP ID:

2.19.36.7.3.4.1

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Send-DNS-Forwardings

Here you set whether the VPN gateway should send its locally configured DNS forwardings to VPN clients.

SNMP ID:

2.19.36.7.3.4.2

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

Possible values:

No
Yes

Default:

No

Send-local-Domain

Set whether the VPN gateway should send its own locally configured domain to VPN clients.

SNMP ID:

2.19.36.7.3.4.3

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

Possible values:

No
Yes

Default:

No

Domain-List

Name of the list of split-DNS domains that the VPN gateway should send to VPN clients.

SNMP ID:

2.19.36.7.3.4.4

Telnet path:

Setup > **VPN** > **IKEv2** > **IKE-CFG** > **Split-DNS** > **Profiles**

Possible values:

Max. 16 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[\]^_.`

Default:

empty

Cookie-Challenge

IKEv2 offers cookie notification, a challenge-response procedure that the IKEv2 responder can trigger if it has too many half-open IKEv2 connections. This makes the responder more resistant to DDoS attacks.

Cookie notification has been implemented to improve the compatibility with third-party VPN-enabled devices. It must be enabled on both VPN participants in order for a VPN connection to be established.

The IKEv2 cookie notification prevents the establishment of excessive numbers of half-open VPN connections and the attack on VPN-gateway resources (DDOS) that they cause. With cookie notification enabled, the responder only reacts to incoming VPN connections if the remote site is verified as reachable.

Enabling the IKEv2 cookie challenge adds two additional IKE messages to the VPN connection setup.

The switch activates the Cookie Challenge on the responder or gateway side.

On the initiator side, the cookie challenge is done automatically if the other side requests it. The switch has no effect on the initiator side or on the client side.

Please note that both initiator and responder must support the cookie challenge feature. If the remote site does not support cookie challenge, the VPN tunnel cannot be established. Hirschmann VPN routers at both ends must have at least HiLCOS 10.32.

SNMP ID:

2.19.36.12

Telnet path:

Setup > **VPN** > **IKEv2**

Possible values:

Off
Always

Default:

Off

Enforce-Pre-Shared-Key-Rules

This entry gives you the option to disable or enable the enforcing of password rules. The following rules then apply for Pre-Shared Keys (PSK) with IKEv2:

- The length of the password must be at least 32 characters.
- The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

These rules do not apply to PSK managed and obtained by a RADIUS server.

SNMP ID:

2.19.36.14

Telnet path:

Setup > **VPN** > **IKEv2**

Possible values:

No
Password rules enforcement is disabled.

Yes
Password rules enforcement is enabled.

Default:

No

RSA-Padding-Method

Specifies the RSA padding method for certificates issued by the SCEP-CA.

SNMP ID:

2.39.2.15

Telnet path:

Setup > **Certificates** > **SCEP-CA**

Possible values:

PKCS1
Certificate padding is performed with the RSASSA-PKCS1-v1_5 method.

PSS
Certificate padding is performed with the RSASSA-PSS method

Default:

PKCS1

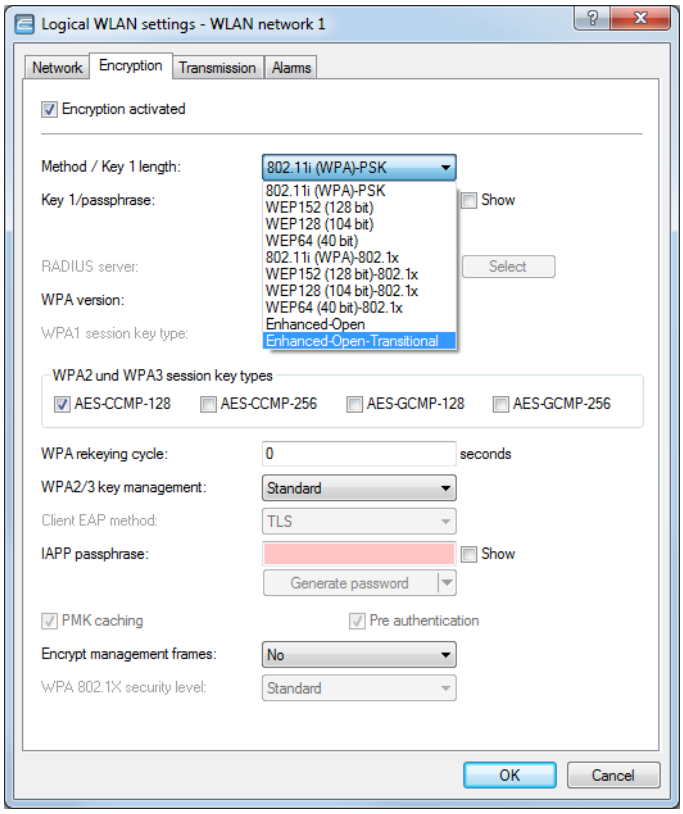
9 Public Spot

9.1 Setting up a secure hotspot with Enhanced Open

Enhanced Open for the first time provides a way to offer a secure, yet easy-to-use hotspot.

Enhanced Open has been combined with the Public Spot option.

The WLAN to be used for the hotspot is set up in the usual way with the exception that the encryption method is set to **Enhanced Open Transitional**:



Not only is entering a key not required, it is not even possible: A client enabled for Enhanced Open establishes an encrypted connection to the access point without any key having to be entered. To the user, it is just like using an unencrypted, open WLAN: There is no need to enter any previously communicated key as with WPA2-PSK.

The Transitional mode allows an SSID to be used concurrently by clients that support Enhanced Open as well as by clients that do not yet support Enhanced Open. For the latter clients, no encryption is used at all and the SSID works like an open, unencrypted SSID. Once Enhanced Open has become more widespread, you can switch from Transitional mode to regular Enhanced Open mode.

After this, you can proceed as usual with the configuration of the Public Spot module. Since the Public Spot module is independent of the encryption settings of the WLAN interfaces, all of the functions of the Public Spot module can be used without restriction in conjunction with Enhanced Open.

In summary, Enhanced Open is ideal for hotspot operation as it provides a higher level of security than the open hotspots used in the past. The optional Transitional mode ensures that even clients that do not yet support Enhanced Open can be connected in a way that is transparent to the user.

9.2 User list removed

The former user list for the Public Spot (LANconfig: **Configuration** > **Public Spot** > **Users** > **User list**) has been deprecated. The preferred way to configure Public Spot users is to use the internal RADIUS server, so this old table is no longer required. If there are still entries in the user list at the time of the upgrade, they will be automatically converted to RADIUS users. These converted users can be identified as such by an entry in the comment field (e.g. “moved by root”).

An entry of the same name that already exists in the RADIUS user table at this time will be overwritten.

10 RADIUS

10.1 Importing and exporting RADIUS user data by CSV file

The internal RADIUS server is basically a user database. Here we describe an easy way to import and export the user entries. This is particularly relevant for Public Spots, where users are generated in large numbers by an external system. For LEPS-MAC, too, this is an easy way to import the data. The format used for the data exchange is csv (comma separated values), whereby a semicolon serves as the default separator of the individual data fields.

10.1.1 Exporting RADIUS user data by CSV file

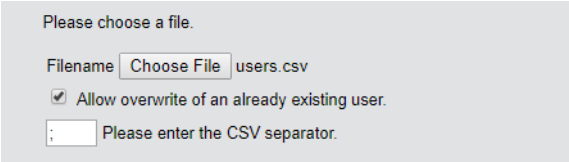
To export the user data of the RADIUS server via WEBconfig, proceed as follows.

Click on **Extras** > **Export RADIUS users**.
The user data is downloaded as the file `users.csv`. The semicolon is the separator; the first row contains the identifiers of the database fields.

10.1.2 Importing RADIUS user data by CSV file

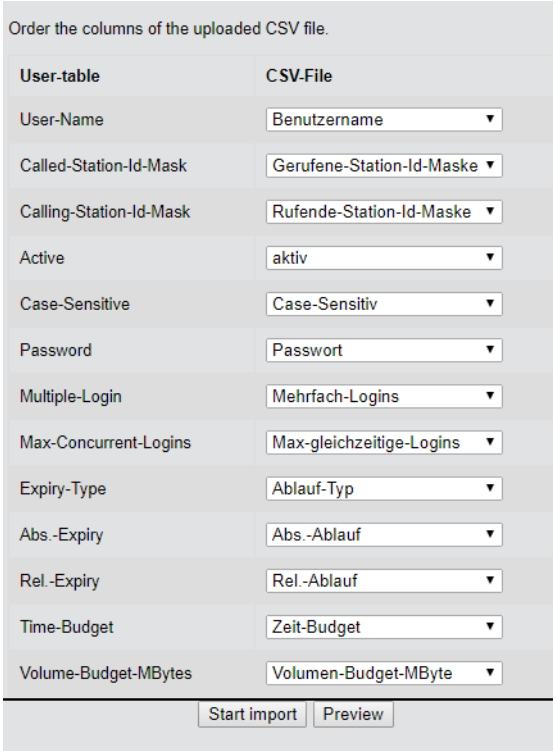
To import the user data of the RADIUS server via WEBconfig, proceed as follows.

1. Generate a file with the required header for the user data by performing an export of the user data as described in *Exporting RADIUS user data by CSV file* in the chapter above.
2. Create a CSV import file with a header containing the correct database field identifiers determined in the previous step. The import file does not have to contain all the columns.
3. Navigate to the menu item **Extras** > **Import RADIUS users**.
4. Use **Choose file** to select the CSV file to be imported.
5. Enter the CSV separator. By default this is already preset to ";".



6. Start the upload.

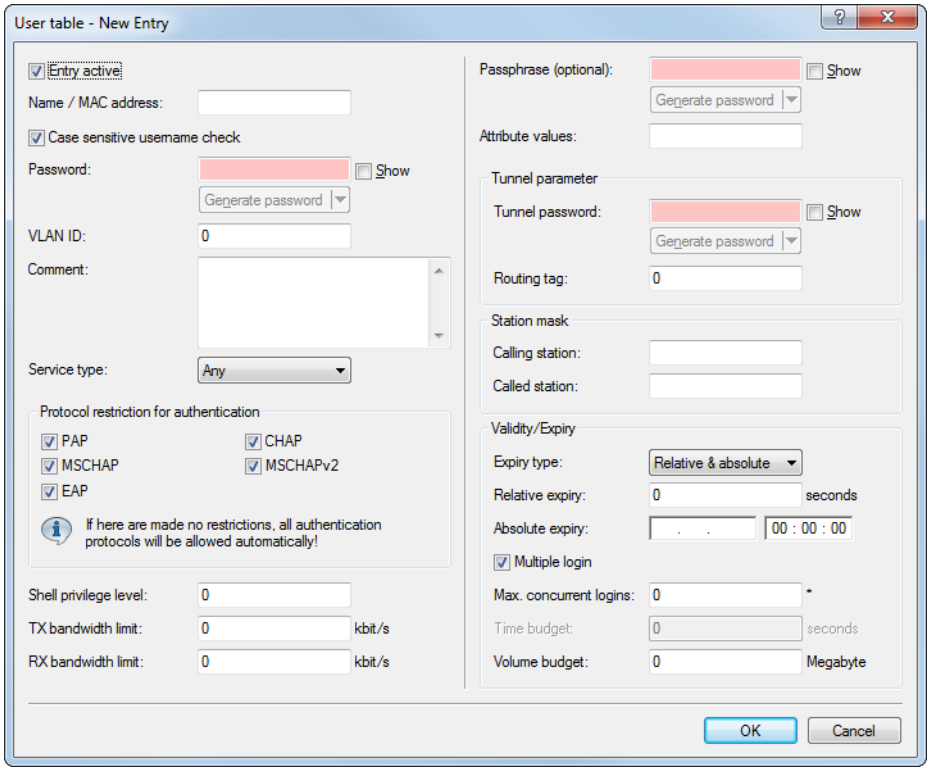
7. Now check that the columns detected in the CSV file are correctly aligned with the supported columns. You can adjust the alignment in this dialog. No adjustment should be necessary if you used the column names from the previously exported CSV file.



8. Click **Start import** to complete the process and accept the user data.

10.2 User-defined attributes for RADIUS users in the RADIUS server

The RADIUS user database under **RADIUS** > **Server** > **User table** now features the parameter **Attribute values**, which can be used to add vendor-specific attributes.



Attribute values

Along with the user-management attributes supported by the Hirschmann RADIUS server, there is a vast array of vendor-specific attributes (VSAs). These attributes can be freely configured for RADIUS users as a comma-separated list of attributes and values in the form <Attribute_1>=<Value_1>,<Attribute_2>=<Value_2> ...

10.2.1 Additions to the Setup menu

Attribute-Values

User-defined attributes for RADIUS users in the RADIUS server.

Along with the user-management attributes supported by the Hirschmann RADIUS server, there is a vast array of vendor-specific attributes (VSAs). These attributes can be freely configured for RADIUS users here.

SNMP ID:

2.25.10.7.25

Telnet path:

Setup > **RADIUS** > **Server** > **Users**

Possible values:

Comma-separated list of attributes and values in the form
<Attribute_1>=<Value_1>,<Attribute_2>=<Value_2> ...

Max. 251 characters from `[A-Z][a-z][0-9]#@{|}~!"$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

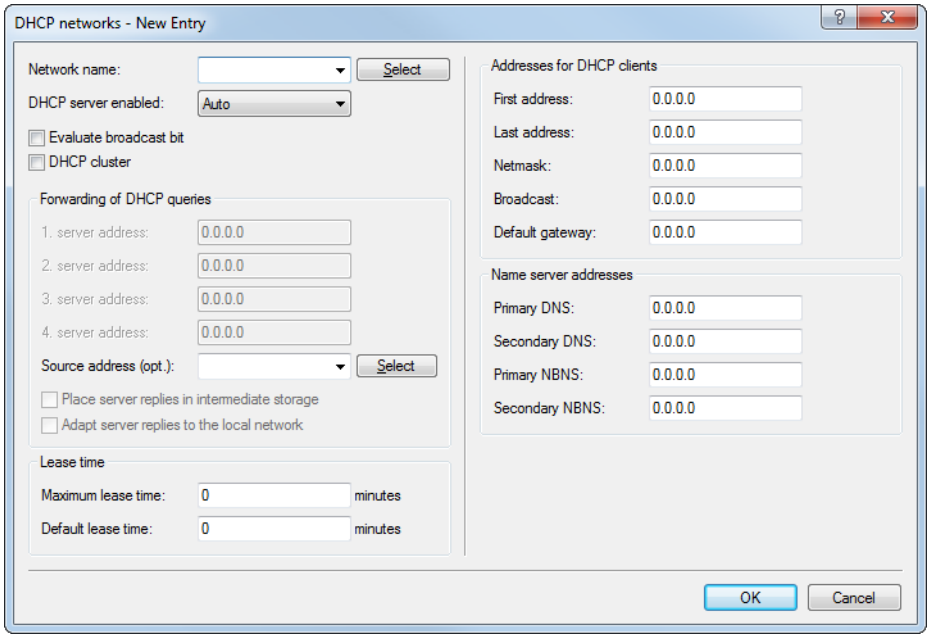
11 Other services

11.1 Automatic IP address administration with DHCP

11.1.1 Configuring DHCPv4 parameters with LANconfig

Source address for DHCP relay agent

In the DHCP network table (LANconfig: **IPv4** > **DHCPv4** > **DHCP networks**) there is a new option for assigning an optional source address to a relay agent.



Source address (optional)

Here you assign an optional source address to a relay agent. This address (the name of an ARF network, named loopback address) is used to forward client messages.

Additions to the Setup menu

Loopback address

Here you assign a loopback address to a relay agent. The loopback address (the name of an ARF network, named loopback address) is used to forward client messages.

SNMP ID:

2.10.20.22

Telnet path:

Setup > **DHCP**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. `

Default:

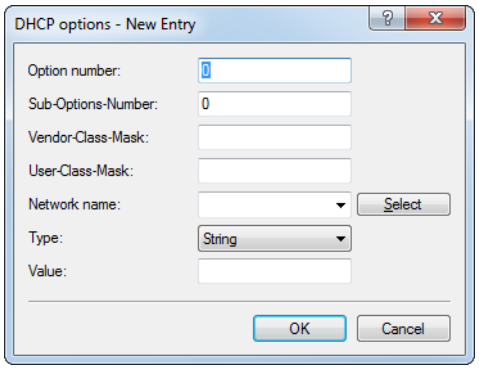
empty

DHCP options

From HiLCOS 10.32, Hirschmann devices support suboptions for the DHCP options.

The DHCP server uses the DHCP options to transmit additional configuration parameters to the DHCP clients. The vendor class ID (DHCP option 60) shows e.g. the type of device. DHCP option 43 is used by various device manufacturers to distribute additional information about network devices during the initial startup. The parameters themselves are manufacturer-specific.

In LANconfig, the DHCP options are configured under **IPv4** > **DHCPv4** > **DHCP options**. Click on **Add** to create a new entry.



Option number

Number of the option that should be sent to the DHCP client. The option number describes the transmitted information. For example "17" (root path) is the path to a boot image that a PC without its own hard disk uses to obtains its operating system via BOOTP.

You can find a list of all DHCP options in "RFC 2132 – DHCP Options and BOOTP Vendor Extensions" of the Internet Engineering Task Force (IETF).

Sub-option number

Number of the sub-option that should be sent to the DHCP client. A DHCP option is made up of sub-options. For example, network devices such as SIP phones are often notified about where their firmware and configuration can be downloaded by means of DHCP option 43. The sub-option settings are defined by the respective manufacturer.

Vendor-class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. These usually allow the client to be clearly assigned to a manufacturer or even a specific device class. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields "Vendor-class mask" and "User-class mask" can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be

entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards "*" (any number of characters) and "?" (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

User class mask

Filter criterion used by some manufacturers for requests to the DHCP server. See also Vendor-class mask. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards "*" (any number of characters) and "?" (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

Network name

Name of the IP network where this DHCP option is to be used.

Type

Entry type. This value depends on the respective option. For example, RFC 2132 defines the option "35" (ARP cache timeout) as follows:

```
ARP Cache Timeout Option
This option specifies the timeout in seconds for ARP cache entries.
The time is specified as a 32-bit unsigned integer.
The code for this option is 35, and its length is 4.
Code Len Time
+-----+-----+-----+-----+-----+-----+
| 35  | 4   | t1  | t2  | t3  | t4  |
+-----+-----+-----+-----+-----+-----+
```

This description tells you that the type "32-bit integer" is used for this option.

You can find out the type of the option either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

Value

With this field you define the contents of the DHCP option.

IP addresses are specified with the usual notation for IPv4 addresses, e.g. as "123.123.123.100", integer types are entered as normal decimal numbers, and strings as simple text.

Multiple values in a single field are separated with commas, e.g. "123.123.123.100, 123.123.123.200".

You can find out the possible length of the option value either from the corresponding RFC or from the manufacturer's documentation of their DHCP options.

Additions to the Setup menu

Sub-option number

Number of the sub-option that should be sent to the DHCP client. A DHCP option is made up of sub-options. For example, network devices such as SIP phones are often notified about where their firmware and configuration can be downloaded by means of DHCP option 43. The sub-option settings are defined by the respective manufacturer.

SNMP ID:

2.10.26.5

Telnet path:

Setup > **DHCP** > **Additional-Options**

Possible values:

Max. 3 characters from `[0-9]`

Default:

empty

Vendor-class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. These usually allow the client to be clearly assigned to a manufacturer or even a specific device class. For example, DHCP requests from Hirschmann devices always contain the string "Hirschmann" in the vendor-class ID, which is supplemented by the exact device type, if required. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields "Vendor-class mask" and "User-class mask" can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards "*" (any number of characters) and "?" (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

SNMP ID:

2.10.26.6

Telnet path:

Setup > **DHCP** > **Additional-Options**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

User class mask

When sending requests to DHCP servers, some DHCP clients submit a vendor-class ID and/or a user-class ID. This usually allows the manufacturer or even the specific device class of the client to be identified. The DHCP server can use this information to provide the best suited DHCP options for the given device type. This is especially relevant for DHCP option 43, as its content is not standardized, but vendor-specific—the DHCP server has to transmit different information depending on the manufacturer or device type. The two fields "Vendor-class mask" and "User-class mask" can be used as filters. Strings that the DHCP server requires to be present in incoming requests can be entered here. The DHCP option is only delivered when the configured filter matches the DHCP request. The wildcards "*" (any number of characters) and "?" (exactly one character) can be used. If the fields are empty, they are ignored and the option is always delivered.

SNMP ID:

2.10.26.7

Telnet path:

Setup > **DHCP** > **Additional-Options**

Possible values:

Max. 32 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

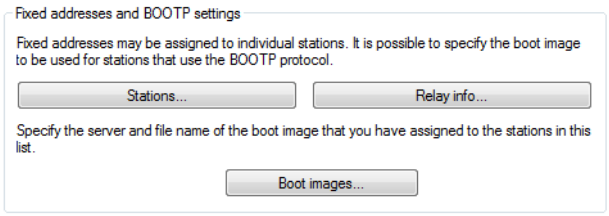
Default:

empty

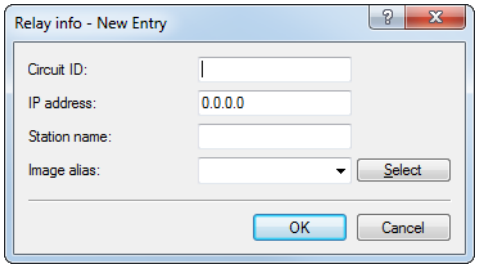
Assigning IP addresses based on DHCP option 82

DHCP option 82 assigns IP addresses depending on the switch port to which the device is connected. The switch in question uses DHCP option 82 to supplement the DHCP request with the Circuit ID, which identifies the port that this device is connected to. This information is then used by the DHCP server to assign a specific IP address. This establishes a relationship between an IP address and a location, which simplifies network monitoring.

In LANconfig under **IPv4** > **BOOTP**, you can set the switch-port based assignment of IP addresses for each port separately by clicking on **Relay info**.



After selecting the switch port that is automatically added by the DHCP option 82, you can set the following:



Circuit-ID

This is the storage location for the "Circuit ID" used for address assignment and inserted by the relay agent or switch using DHCP option 82. The string is evaluated case-sensitive. Depending on the particular switch, the "Circuit ID" is delivered by the relay agent in various formats and stored accordingly. This can be a complete hexadecimal string with leading 0x. An alternative syntax allows the entry of binary values, as with the user class identifier or vendor class identifier:

Binary values are specified in the form `{value/bit length}`. The value can be specified as decimal, hexadecimal (leading 0x) or octal (leading 0), and the available bit lengths are 8, 16, 24, 32, 48 and 64. The value is stored in big-endian representation. Little-endian representation requires "negative" bit lengths: -8, -16, -24, -32, -48 or -64

A circuit ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) can be stored in one of the following representations:

- 0x0002001e4d45532d33373238
- {0/8} {2/8} {30/16}
- {0x00/8} {0x02/8} {0x1e/16}
- {00/8} {02/8} {036/16}

IP address

Enter the IP address assigned to the host on this port. Do not leave this column unspecified (0.0.0.0). Otherwise only one host per circuit ID would be able to authenticate. As long as there is an entry in the DHCP table, any DHCP messages from other hosts using the same circuit ID would be ignored. In other words, if you want to operate another host on the port, the previous one must either log off correctly (e.g. under Microsoft Windows: `ipconfig/release`) or the entry must be deleted from the DHCP table.

Station name

Enter the name that is to be used to identify the station. If the station does not communicate its name, the device will use the name entered here.

Image alias

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

Enter the server providing the boot image and the name of the file on the server in the boot image table.

Additions to the Setup menu

Relay-Info-List

DHCP option 82 assigns IP addresses depending on the switch port to which the device is connected. To this end, the switches provide the "Circuit ID" of the respective ports. Each port is then assigned exactly one IP address, host name and a boot image. The latter works analogous to the BOOTP table.

SNMP ID:

2.10.27

Telnet path:

Setup > **DHCP**

Circuit-ID

This is the storage location for the "Circuit ID" used for address assignment and inserted by the relay agent or switch using DHCP option 82. The string is evaluated case-sensitive. Depending on the particular switch, the "Circuit ID" is delivered by the relay agent in various formats and stored accordingly. This can be a complete hexadecimal string with leading 0x. An alternative syntax allows the entry of binary values, as with the user class identifier or vendor class identifier:

Binary values are specified in the form `{value/bit length}`. The value can be specified as decimal, hexadecimal (leading 0x) or octal (leading 0), and the available bit lengths are 8, 16, 24, 32, 48 and 64. The value is stored in big-endian representation. Little-endian representation requires "negative" bit lengths: -8, -16, -24, -32, -48 or -64

A circuit ID (00 02 00 1e 4d 45 53 2d 33 37 32 38) can be stored in one of the following representations:

- 0x0002001e4d45532d33373238
- {0/8} {2/8} {30/16}
- {0x00/8} {0x02/8} {0x1e/16}
- {00/8} {02/8} {036/16}

SNMP ID:

2.10.27.1

Telnet path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

Max. 64 characters from `[A-F][a-f]x[0-9]{}/`

IP address

Enter the IP address assigned to the host on this port. Do not leave this column unspecified (0.0.0.0). Otherwise only one host per circuit ID would be able to authenticate. As long as there is an entry in the DHCP table, any DHCP messages from other hosts using the same circuit ID would be ignored. In other words, if you want to operate another host on the port, the previous one must either log off correctly (e.g. under Microsoft Windows: `ipconfig/release`) or the entry must be deleted from the DHCP table.

SNMP ID:

2.10.27.2

Telnet path:

Setup > **DHCP** > **Relay-Info-List**

Host name

Enter the name that is to be used to identify the station. If the station does not communicate its name, the device will use the name entered here.

SNMP ID:

2.10.27.3

Telnet path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

Max. 64 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

Image-alias

If the client uses the BOOTP protocol, you can select a boot image that the client should use to load its operating system from.

Enter the server providing the boot image and the name of the file on the server in the boot image table.

SNMP ID:

2.10.27.4

Telnet path:

Setup > **DHCP** > **Relay-Info-List**

Possible values:

Max. 16 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

11.2 DHCP server – suppress ARP request

As of HiLCOS Rel. 10.32 your device supports the option to suppress the ARP request that usually precedes the assignment of an IP address.

11.2.1 Additions to the Setup menu

Suppress-ARP-check

Before the DHCP server assigns an IP address, an ARP request is usually used to check whether the address has been assigned already. If there is no response to the ARP request within 3 seconds, the assignment goes ahead. This query is especially useful when computers are booting in normal networks that use fixed IP addresses. In a Public Spot network where, for example, a smartphone has to recognize that there is no Internet connection in order to display the login popup, this ARP request leads to an unnecessary delay. For scenarios such as this, this check can be disabled here.

SNMP ID:

2.10.20.23

Telnet path:

Setup > **DHCP** > **Network-List**

Possible values:

Yes

Do not carry out check by ARP request.

No

Perform check by ARP request.

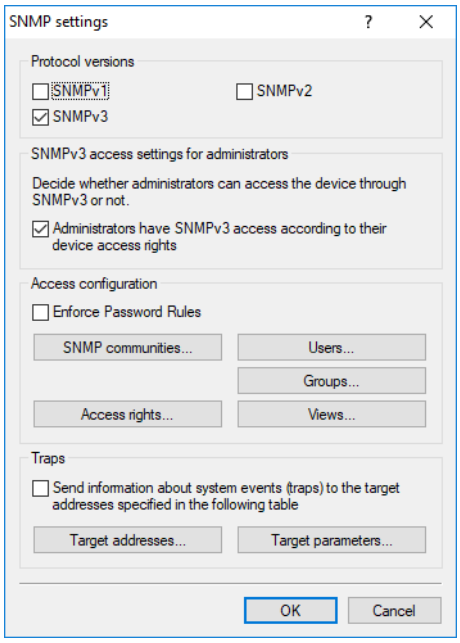
Default:

No

11.3 Simple Network Management Protocol (SNMP)

11.3.1 SNMPv3 Password Rules

HiLCOS 10.32 supports enforcing password rules for SNMPv3 authentication and the password for SNMPv3 encryption. The setting is made under **Management** > **Admin** > **SNMP settings** > **Access configuration** using the **Enforce Password Rules** option.



The following rules become active:

- The length of the password must be at least 16 characters.
- The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

Please note that the current passwords are not immediately checked when this function is switched on. Only future password changes will be checked for compliance with the policy.

11.3.2 Additions to the Setup menu

Enforce-Password-Rules

This entry gives you the option to disable or enable the enforcing of password rules. The following rules then apply for the SNMPv3 passwords:

- The length of the password must be at least 16 characters.
- The password must contain at least 3 of the 4 character classes lower case letters, upper case letters, numbers and special characters.

Please note that the current passwords are not immediately checked when this function is switched on. Only future password changes will be checked for compliance with the policy.

Please note that SNMPv3 only uses passwords, when in the table **Setup** > **SNMP** > **Users** neither **Authentication-Protocol** nor **Privacy-Protocol** is set to **None**.

SNMP ID:

2.11.93

Telnet path:

Setup > **Config**

Possible values:

No

Password rules enforcement is disabled.

Yes

Password rules enforcement is enabled.

Default:

No

11.4 TACACS+

11.4.1 Configuring the TACACS+ server

Two servers can be defined to work with TACACS+ functions. One server acts as a backup in case the other one fails. When logging in via telnet or WEBconfig, the user can select the server to be used.

As of HiLCOS 10.32, TACACS+ supports IPv6. Consequently, the server address can be configured as a DNS name, an IPv4 address, and also as an IPv6 address.

The parameters for configuring the TACACS+ server are to be found under:

Command line: **Setup** > **TACACS+** > **Server**

Server address

Address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

Possible values:

- Valid DNS resolvable name, or valid IPv4 or IPv6 address.

Default

- Blank

Additions to the Setup menu

Server-address

DNS name, or IPv4 or IPv6 address of the TACACS+ server to which requests for authentication, authorization and accounting are to be forwarded.

SNMP ID:

2.54.9.1

Telnet path:

Setup > **Tacacs+** > **Server**

Possible values:

Max. 31 characters from `[A-Z][a-z][0-9]#@{|}~!$%&'()*+-,/:;<=>?[\]^_. ``

Default:

empty

12 Quality of Service

12.1 Configurable DSCP tags for internal Hirschmann services

From HiLCOS 10.32, internal HiLCOS applications can be marked with configurable DiffServ CodePoints (DSCP). This allows downstream hardware to recognize and prioritize these packets. Further information about DiffServ CodePoints is available in the Reference Manual under the section Quality of Service.

12.1.1 Additions to the Setup menu

DSCP marking

Internal HiLCOS applications can be marked with configurable DiffServ CodePoints (DSCP). This allows downstream hardware to recognize and prioritize these packets. Further information about DiffServ CodePoints is available in the Reference Manual under the section Quality of Service.

This configuration marks only the control messages of the respective protocols.

SNMP ID:

2.11.94

Telnet path:

Setup > **Config**

Application

Column with the internal applications.

SNMP ID:

2.11.94.1

Telnet path:

Setup > **Config** > **DSCP-Marking**

DSCP

Column with the DiffServ codepoints. Default values are listed for the possible internal applications.

SNMP ID:

2.11.94.2

Telnet path:

Setup > **Config** > **DSCP-Marking**

Possible values:

BGP

CS6

OSPF

CS6

RIP

CS6

IKE

CS6

Incl. Dynamic VPN UDP packets, but not supported with SSL encapsulation.

TACACS

BE/CS0

SNMP

BE/CS0

L2TP

CS6

PPTP

CS6

LISP

CS6

TFTP

BE/CS0

ICMP

BE/CS0

HIRSCHMANN
A BELDEN BRAND

Addendum
HiLCOS Rel. 10.34

Contents

Addendum to HiLCOS Rel. 10.34.....3

1 Voice over IP – VoIP.....3

1.1 Dynamic SIP lines.....4

1.1.1 Additions to the Setup menu.....5

1.2 Flex mode.....7

1.2.1 Additions to the Setup menu.....8

2 WLAN-Diagnostics.....10

2.1 Feature introduction.....10

2.2 Description of the WLAN-Diagnostics table.....10

2.3 Configuration via WEBconfig (graphical user interface).....29

2.4 Additions to the Setup menu (CLI).....31

3 Chain-Noises 34

4 Force-Background-Scan 35

5 Factory-Default Network-Exposed Services 36

6 Post-Initial-Password Security Hardening 38

7 Antenna Chain Noise Observation Mechanism 39

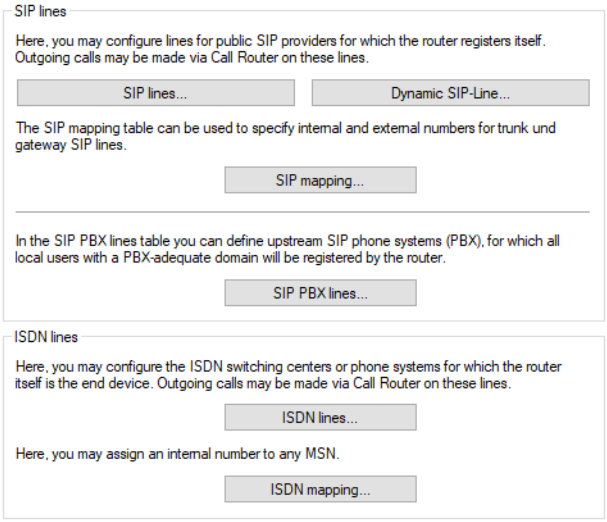
Addendum to HiLCOS Rel. 10.34

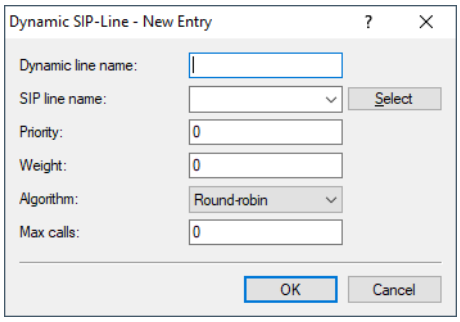
This document describes the changes and enhancements in HiLCOS Rel. 10.34 since the previous release.

1 Voice over IP – VoIP

1.1 Dynamic SIP lines

From HiLCOS 10.34 it is possible to set up dynamic SIP lines. The configuration is found under **Voice call manager** > **Lines** by clicking the button **Dynamic SIP line**.





Dynamic line name

Enter the name for the dynamic line here. If the dynamic line consists of several physical lines, you can also use this dynamic line name for other table entries. This dynamic line name can later be used in the call routing table as the destination line.

SIP line name

Here you select one of the already configured physical SIP connections.

Priority

Here you specify the priority of the physical line for consideration when outgoing calls are distributed.

Weight

Here you specify the weighting of the physical line for consideration when outgoing calls are distributed.

Algorithm

The algorithm must be configured identically for all entries that belong to a dynamic line. The following algorithms can be used:

Weight

This algorithm controls the percentage of calls being distributed between different physical lines.

Round-Robin

With this algorithm, outgoing calls are distributed sequentially to the physical lines.

Priority

The physical line with the highest priority is fully utilized first, before the physical line with the next-lowest priority is used.

Max. calls

Here you enter how many simultaneous voice channels can be used on the physical SIP line. For no restriction on the number of voice channels, enter 0 here.

1.1.1 Additions to the Setup menu

Dynamic line

Configure the dynamic SIP lines here.

SNMP ID:

2.33.4.1.3

Telnet path:

Setup > **Voice-Call-Manager** > **Line** > **SIP-Provider**

Dynamic line name

Enter the name for the dynamic line here. If the dynamic line consists of several physical lines, you can also use this dynamic line name for other table entries. This dynamic line name can later be used in the call routing table as the destination line.

SNMP ID:

2.33.4.1.3.1

Telnet path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[]^_.`

SIP line name

Here you specify one of the already configured physical SIP connections.

SNMP ID:

2.33.4.1.3.2

Telnet path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 32 characters from `[A-Z][0-9]@{|}~!$%&'()+-,/:;<=>?[]^_.`

Priority

Here you specify the priority of the physical line for consideration when outgoing calls are distributed.

SNMP ID:

2.33.4.1.3.3

Telnet path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 3 characters from `[0-9]`

Weight

Here you specify the weighting of the physical line for consideration when outgoing calls are distributed.

SNMP ID:

2.33.4.1.3.4

Telnet path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Max. 3 characters from `[0-9]`

Algorithm

The algorithm must be configured identically for all entries that belong to a dynamic line.

SNMP ID:

2.33.4.1.3.5

Telnet path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

Possible values:

Weight

This algorithm controls the percentage of calls being distributed between different physical lines.

Round-Robin

With this algorithm, outgoing calls are distributed sequentially to the physical lines.

Priority

The physical line with the highest priority is fully utilized first, before the physical line with the next-lowest priority is used.

Max. calls

Here you enter how many simultaneous voice channels can be used on the physical SIP line. For no restriction on the number of voice channels, enter 0 here.

SNMP ID:

2.33.4.1.3.6

Telnet path:

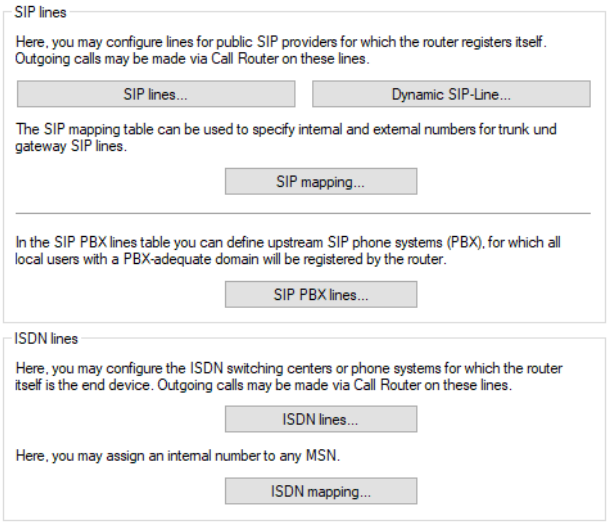
Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Dynamic-Line**

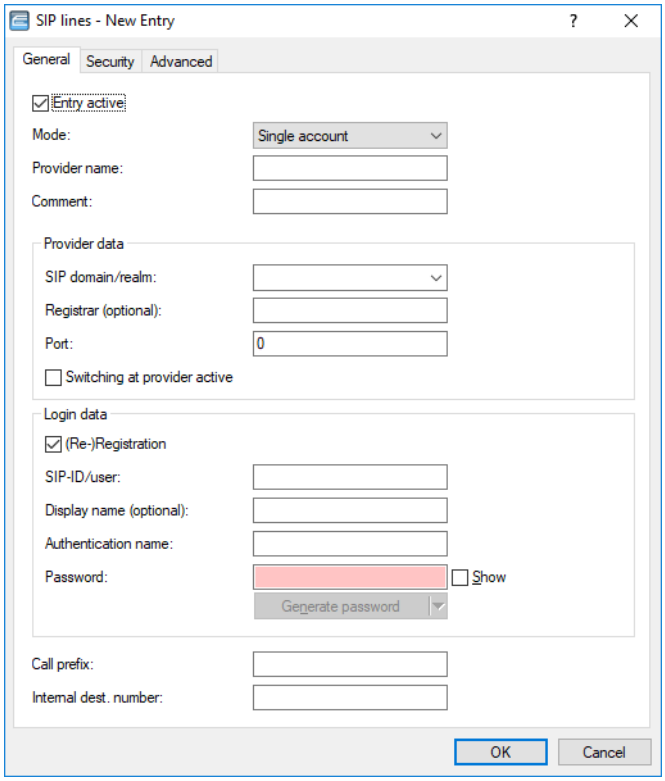
Possible values:

Max. 3 characters from `[0-9]`

1.2 Flex mode

From HiLCOS 10.34, the new Flex mode for SIP lines is supported. The configuration is found under **Voice call manager** > **Lines** by clicking the button **SIP lines**.





Mode

Flex

› To the outside the line behaves like a commercially available SIP account with a single public number.

- The number is registered at the service provider and registration is refreshed on a regular basis.
- For outgoing calls, the calling-line number (sender) is not modified.
- For incoming calls the dialed number (destination) is not modified.
- The maximum number of connections at any one time is limited only by the available bandwidth.

1.2.1 Additions to the Setup menu

Mode

This selection specifies the operating mode of the SIP line.

The "Service provider" can be a server in the Internet, an IP PBX, or a voice gateway. Please observe the notices about "SIP mapping".

SNMP ID:

2.33.4.1.1.17

Telnet path:

Setup > **Voice-Call-Manager** > **Lines** > **SIP-Provider** > **Line**

Possible values:

Provider

Externally, the line behaves like a typical SIP account with a single public number. The number is registered with the service provider, the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number is replaced (masked) by the registered number. Incoming calls are sent to the configured internal destination number. Only one connection can exist at a time.

Trunk

Externally, the line acts like an extended SIP account with a main external telephone number and multiple extension numbers. The SIP ID is registered as the main switchboard number with the service provider and the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the switchboard number acts as a prefix placed in front of each calling number (sender; SIP: "From:"). For incoming calls, the prefix is removed from the destination number (SIP: "To:"). The remaining digits are used as the internal extension number. In case of error (prefix not found, destination equals prefix) the call is forwarded to the internal destination number as configured. The maximum number of connections at any one time is limited only by the available bandwidth.

Gateway

Externally the line behaves like a typical SIP account with a single public number, the SIP ID. The number (SIP ID) is registered with the service provider and the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender) is replaced (masked) by the registered number (SIP ID in SIP: "From:") and sent in a separate field (SIP: "Contact:"). For incoming calls the dialed number (destination) is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.

Link

Externally, the line behaves like a typical SIP account with a single public number (SIP ID). The number is registered with the service provider, the registration is refreshed at regular intervals (if (re-)registration has been activated for this SIP provider line). For outgoing calls, the calling-line number (sender; SIP:

"From:") is not modified. For incoming calls, the dialed number (destination; SIP: "To:") is not modified. The maximum number of connections at any one time is limited only by the available bandwidth.

Flex

- To the outside the line behaves like a commercially available SIP account with a single public number.
- The number is registered at the service provider and registration is refreshed on a regular basis.
- For outgoing calls, the calling-line number (sender) is not modified.
- For incoming calls the dialed number (destination) is not modified.
- The maximum number of connections at any one time is limited only by the available bandwidth.

Default:

Provider

2 WLAN-Diagnostics

2.1 Feature introduction

One challenge for setting up and operating a WLAN installation are events on the WLAN device that can impact the performance or quality of WLAN links. Thus, it is sometimes essential to have extended logging and information acquisition capabilities to understand the WLAN environment and the corresponding behavior of a WLAN installation.

The WLAN-Diagnostics feature gathers various WLAN information logged over time in a single table. The gathered information is made available for automated processing via SNMP or can be exported as .csv file. This way analysis tools, technicians and support staff can analyze the available information.

In summary, this feature will help to simplify and accelerate the diagnostic, fixing, and optimization of WLAN issues

Here you find the WLAN-Diagnostics table:
HiLCOS Menu Tree > Status > WLAN > WLAN-Diagnostics

2.2 Description of the WLAN-Diagnostics table

In the following, you find the description of each column from left to right in the WLAN-Diagnostics table:

2.2.1 Index

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the index of the row. The index is incremental and unique.

2.2.2 Time

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the current system time as per the RFC 3339 format.

Example: 2022-04-22T04:30:04.620+01:00

2.2.3 Interface

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows either the physical WLAN interface (for event based updates) or the logical WLAN interface (for periodic updates) for which the row is added.

Examples: WLAN-1, WLAN-1-4

2.2.4 Event Source

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the major event categories. If the row entry is generated because of a periodic update instead of an event, then it shows PERIODIC.

Examples: CLIENT CONNECT, ROAMING, PERIODIC etc.

2.2.5 Message

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows detailed text messages for the major event categories. For periodic updates, this column displays the static string PERIODIC ENTRY. The event based text messages are copied from the syslog, whereas the periodic entries are unique to this table.

Examples: Authenticated WLAN station 64:60:38:01:a5:c0, PERIODIC ENTRY

2.2.6 Device Name

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the device name of the device where the table is recorded.

Example: BAT-R_15D4C0

2.2.7 MAC-Address

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

For Access Point mode: This column shows the MAC address of the connected Client, or the BSSID of the device if no Client is connected.

For Client mode: This column shows the BSSID of the connected Access Point, or the WLAN MAC address of the device if no Access Point is connected.

Example: 64:60:38:01:a5:c0

2.2.8 Identification

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

For Access Point mode: This column shows the name of the connected Client, or no entry if no Client is connected.

For Client mode: This column shows the name of the connected Access Point, or no entry if no Access Point is connected.

Example: BAT-R_15D4F0

2.2.9 IP-Address

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

For Access Point mode: This column shows the IP address of the connected Client, or no entry if no Client is connected.

Example: 192.168.199.201

For Client mode: This column shows no entry.

2.2.10 Channel

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the base channel number on which the WLAN interface is operating.

Example: 6, 40

2.2.11 Channel-Bandwidth(MHz)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the channel bandwidth of the WLAN interface.

Example: 20

2.2.12 Ext.-Channel

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the extension channel mode used in 40 MHz bandwidth in HT+ and HT- notations.

Possible values:

HT+ for 40 MHz channel bandwidth and extension channel mode is above.

HT- for 40 MHz channel bandwidth and extension channel mode is below.

No entry if the bandwidth is NOT set as 40 MHz.

2.2.13 Signal Quality (%)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the physical signal strength in percent.

2.2.14 Noise (dBm)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the noise level combined from all chains in dBm.

For Access Point mode: The noise level measured by the device when the Client is connected. No entry if no Client is connected.

For Client mode: The noise level measured by the device when the Access Point is connected. No entry if no Access Point is connected.

Example: -90

2.2.15 Signal (dBm)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the signal level of the peer combined from all chains in dBm. Peer will be the connected device that can be identified with the MAC-Address column.

For Access Point mode: Signal level of the connected Client. No entry if no Client is connected.

For Client mode: Signal level of the connected Access Point. No entry if no Access Point is connected.

Example: -39

2.2.16 Chain Signal 1 (dBm)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the chain 1 signal level of the peer in dBm. Chain 1 is mapped to the antenna port 1 of the device. Peer will be the connected device that can be identified with the MAC-Address column.

For Access Point mode: Chain 1 signal level of the connected Client. No entry if no Client is connected.

For Client mode: Chain 1 signal level of the connected Access Point. No entry if no Access Point is connected.

Example: -45

2.2.17 Chain Signal 2 (dBm)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the chain 2 signal level of the peer in dBm. Chain 2 is mapped to the antenna port 2 of the device. Peer will be the connected device that can be identified with the MAC-Address column.

For Access Point mode: Chain 2 signal level of the connected Client. No entry if no Client is connected.

For Client mode: Chain 2 signal level of the connected Access Point. No entry if no Access Point is connected.

Example: -58

2.2.18 Chain Signal 3 (dBm)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the chain 3 signal level of the peer in dBm. Chain 3 is mapped to the antenna port 3 of the device. Peer will be the connected device that can be identified with the MAC-Address column.

For Access Point mode: Chain 3 signal level of the connected Client. No entry if no Client is connected.

For Client mode: Chain 3 signal level of the connected Access Point. No entry if no Access Point is connected.

Example: -51

2.2.19 Chain Noise 1 (dBm)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the chain 1 noise level in dBm. Chain 1 is mapped to the antenna port 1 of the device.

For Access Point mode: The chain 1 noise level measured by the device when the Client is connected. No entry if no Client is connected.

For Client mode: The chain 1 noise level measured by the device when the Access Point is connected. No entry if no Access Point is connected.

Example: -95

2.2.20 Chain Noise 2 (dBm)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the chain 2 noise level in dBm. Chain 2 is mapped to the antenna port 2 of the device.

For Access Point mode: The chain 2 noise level measured by the device when the Client is connected. No entry if no Client is connected.

For Client mode: The chain 2 noise level measured by the device when the Access Point is connected. No entry if no Access Point is connected.

Example: -95

2.2.21 Chain Noise 3 (dBm)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the chain 3 noise level in dBm. Chain 3 is mapped to the antenna port 3 of the device.

For Access Point mode: The chain 3 noise level measured by the device when the Client is connected. No entry if no Client is connected.

For Client mode: The chain 3 noise level measured by the device when the Access Point is connected. No entry if no Access Point is connected.

Example: -95

2.2.22 SNR (dB)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the Signal-to-Noise Ratio (SNR) value in dB.

For Access Point mode: SNR value of the connected Client. No entry if no Client is connected.

For Client mode: SNR value of the connected Access Point. No entry if no Access Point is connected.

Example: -95

2.2.23 Broadcast SNR (dB)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the Signal-to-Noise Ratio (SNR) value received from the broadcast frames.

For Access Point mode: SNR value from the last received broadcast frame from the connected Client. The SNR value is updated when the next broadcast frame is received from the Client. No entry if no Client is connected.

For Client mode: SNR value from the last received broadcast frame from the connected Access Point. The SNR value is updated when the next broadcast frame is received from the Access Point. No entry if no Access Point is connected.

Example: 51

2.2.24 Mgmt. SNR (dB)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the Signal-to-Noise Ratio (SNR) value received from the management frames which are NOT broadcast, multicast, or beacon frames.

For Access Point mode: SNR value from the last management frame received from the Client. The SNR value is updated when the next broadcast frame is received from the Client. No entry if no Client is connected.

For Client mode: SNR value from the last received management frame from the connected Access Point. The SNR value is updated when the next management frame is received from the Access Point. No entry if no Access Point is connected.

Example: 51

2.2.25 Beacon SNR (dB)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the Beacon Signal-to-Noise Ratio (SNR) value received from the management beacon frames.

For Access Point mode: SNR value from the last management beacon frame received from other Access Points. The SNR value is updated when the next management beacon frame is received.

For Client mode: SNR value from the last management beacon frame received from the connected Access Point. The SNR value is updated when the next management beacon frame is received. No entry if no Access Point is connected.

Example: 51

2.2.26 Multicast SNR (dB)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the Signal-to-Noise Ratio (SNR) value received from the multicast frames.

For Access Point mode: SNR value from the last multicast frame received from the connected Client. The SNR value is updated when the next multicast frame is received from the Client. No entry if no Client is connected.

For Client mode: SNR value from the last multicast frame received from the connected Access Point. The SNR value is updated when the next multicast frame is received from the Access Point. No entry if no Access Point is connected.

Example: 51

2.2.27 Total-Channel-Utilization (%)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the total radio channel utilization for the device in percent.

For Access Point and Client mode: WLAN radio channel utilization from the last entry recorded in the table in percent.

Example: 15

2.2.28 Own-Channel-Utilization(%)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the channel utilization including TX and RX for the device in percent.

For Access Point and Client mode: WLAN radio channel utilization from the last entry recorded in the table in percent.

Example: 18

2.2.29 TX-MCS

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

For Access Point and Client mode: This column shows the index of the modulation and coding scheme for the transmitting side based on the selected physical rates.

Possible value range for 11n devices: 0 to 7

Possible value range for 11ac devices: 0 to 9

No entry if no Client-Access Point connection is made.

Example: 3

2.2.30 RX-MCS

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

For Access Point and Client mode: This column shows the index of the modulation and coding scheme for the receiving side based on the selected physical rates.

Possible value range for 11n devices: 0 to 7

Possible value range for 11ac devices: 0 to 9

No entry if no Client-Access Point connection is made.

Example: 3

2.2.31 TX-Spatial-Stream

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

For Access Point mode: This column shows the TX spatial stream of a connected Client.

For Client mode: This column shows the TX spatial stream of a connected Access Point.

No entry if no connection is made.

Example: 3

2.2.32 RX-Spatial-Stream

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

For Access Point mode: This column shows the RX spatial stream of a connected Client.

For Client mode: This column shows the RX spatial stream of a connected Access Point.

No entry if no connection is made.

Example: 3

2.2.33 Retried(%)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the percentage value of retries performed by the Access Point or Client on packets sent within 1 second since the last logged entry.

Example: 3

2.2.34 BE-TX-Error(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of errors per second for transmitted Best-Effort (BE) QoS traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostic table will be “0”, and in the .csv file there will be no entry.

2.2.35 BG-TX-Error(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of errors per second for transmitted Background (BG) QoS traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostic table will be “0”, and in the .csv file there will be no entry.

2.2.36 Video-TX-Error(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of errors per second for transmitted Video QoS traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.37 Voice-TX-Error(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of errors per second for transmitted Voice QoS traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.38 Hi-Prio-RX-Error(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of errors per second for received High-Priority traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.39 Low-Prio-RX-Error(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of errors per second for received Low-Priority traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostic table will be “0”, and in the .csv file there will be no entry.

2.2.40 Hi-Prio-CRC-Error(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of errors per second for High Priority CRC traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.41 Low-Prio-CRC-Error(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of errors per second for Low Priority CRC traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.42 BE-TX-packets(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Best-Effort (BE) QoS traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.43 BG-TX-packets(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Background (BG) QoS traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.44 Video-TX-packets(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Video QoS traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.45 Voice-TX-packets(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Voice QoS TX traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.46 BE-TX-Broadcast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Best-Effort (BE) QoS broadcast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.47 BG-TX-Broadcast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Background (BG) QoS broadcast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.48 Video-TX-Broadcast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Video QoS broadcast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.49 Voice-TX-Broadcast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Voice QoS broadcast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.50 BE-TX-Multicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Best-Effort (BE) QoS multicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.51 BG-TX-Multicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Background (BG) QoS multicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.52 Video-TX-Multicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Video QoS multicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.53 Voice-TX-Multicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Voice QoS multicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.54 BE-TX-Unicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Best-Effort (BE) QoS unicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.55 BG-TX-Unicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Background (BG) QoS unicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.56 Video-TX-Unicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Video QoS unicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.57 Voice-TX-Unicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Voice QoS unicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.58 BE-TX-Aggregate(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of aggregate frames per second under Best-Effort (BE) QoS class for WLAN TX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.59 BG-TX-Aggregate(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of aggregate frames per second under Background (BG) QoS class for WLAN TX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.60 Video-TX-Aggregate(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of aggregate frames per second under Video QoS class for WLAN TX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.61 Voice-TX-Aggregate(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of aggregate frames per second under Voice QoS class for WLAN TX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.62 BE-TX-Aggregate-frames(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the total number of frames in aggregated frames for Best-Effort (BE) QoS class for WLAN TX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.63 BG-TX-Aggregate-frames(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the total number of frames in aggregated frames for Background (BG) QoS class for WLAN TX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.64 Video-TX-Aggregate-frames(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the total number of frames in aggregated frames for Video QoS class for WLAN TX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.65 Voice-TX-Aggregate-frames(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for transmitted Voice QoS aggregate traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.66 Hi-Prio-Rx-Packets(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the total number of frames in aggregated frames for Voice QoS class for WLAN TX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.67 Low-Prio-Rx-Packets(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for received Low-Priority traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.68 Hi-Prio-Rx-Broadcast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for received High-Priority broadcast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.69 Low-Prio-Rx-Broadcast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for received Low-Priority broadcast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.70 Hi-Prio-Rx-Multicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for received High-Priority multicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.71 Low-Prio-Rx-Multicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for received Low-Priority multicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.72 Hi-Prio-Rx-Unicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for received High Priority unicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.73 Low-Prio-Rx-Unicast(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of packets per second for received High Priority unicast traffic frames on the WLAN interface since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.74 Hi-Prio-Rx-Aggregate(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of aggregate frames per second for WLAN High-Priority RX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.75 Low-Prio-Rx-Aggregate(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the number of aggregate frames per second for WLAN Low-Priority RX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.76 Hi-Prio-Rx-Aggregate-Frame(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the total number of frames in aggregated frames for WLAN High-Priority RX queues since the last logged entry.

Example: 100

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

2.2.77 Low-Prio-Rx-Aggregate-Frame(fps)

Column supported for devices according to: IEEE 802.11n

This column shows the total number of frames in aggregated frames for WLAN Low-Priority RX queues since the last logged entry

Note: For 11ac devices, the value in the WLAN-Diagnostics table will be “0”, and in the .csv file there will be no entry.

Example: 100

2.2.78 WLAN-TX(fps)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the number of packets per second for transmitted traffic frames on the WLAN interface since the last logged entry.

Example: 100

2.2.79 WLAN-RX(fps)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the number of packets per second for received traffic frames on the WLAN interface since the last logged entry.

Example: 100

2.2.80 WLAN-TX-Error(fps)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the number of errors per second for transmitted traffic frames on the WLAN interface since the last logged entry.

Example: 100

2.2.81 WLAN-RX-Error(fps)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the number of errors per second for received traffic frames on the WLAN interface since the last logged entry.

Example: 100

2.2.82 WLAN BE TX-Buffer (%)

Column supported for devices according to: IEEE 802.11n

This column shows the utilized space in percent for the Best-Effort (BE) QoS transmission buffer on the WLAN interface since the last logged entry.

Note: For 11ac devices, this column shows no entry.

Example: 25

2.2.83 WLAN BG TX-Buffer (%)

Column supported for devices according to: IEEE 802.11n

This column shows the utilized space in percent for the Background (BG) QoS transmission buffer on the WLAN interface since the last logged entry.

Note: For 11ac devices, this column shows no entry.

Example: 25

2.2.84 WLAN Video TX-Buffer (%)

Column supported for devices according to: IEEE 802.11n

This column shows the utilized space in percent for the Video QoS transmission buffer on the WLAN interface since the last logged entry.

Note: For 11ac devices, this column shows no entry.

Example: 25

2.2.85 WLAN Voice TX-Buffer (%)

Column supported for devices according to: IEEE 802.11n

This column shows the utilized space in percent for the Voice QoS transmission buffer on the WLAN interface since the last logged entry.

Note: For 11ac devices, this column shows no entry.

Example: 25

2.2.86 WLAN Low Prio RX-Buffer (%)

Column supported for devices according to: IEEE 802.11n

This column shows the utilized space in percent for the Low Priority receiving buffer on the WLAN interface at the time of log collection.

Note: For 11ac devices, this column shows no entry.

Example: 25

2.2.87 WLAN High Prio RX-Buffer (%)

Column supported for devices according to: IEEE 802.11n

This column shows the utilized space in percent for the High Priority receiving buffer on the WLAN interface at the time of log collection.

Note: For 11ac devices, this column shows no entry.

Example: 25

2.2.88 Missed Beacons

Column supported for devices according to: IEEE 802.11n

For Client mode: This column shows the number of missed beacons from the connected Access Point since the last logged entry.

For Access Point mode: This column shows no entry.

Example: 0,2,3 etc..

Note: For 11 ac devices, this column shows no entry.

2.2.89 Maximum Missed Beacons (Consec.)

Column supported for devices according to: IEEE 802.11n

For Client mode: This column shows the maximum number of consecutive missed beacons from the connected Access Point since the last logged entry.

Example: 0,2,3 etc.

For Access Point mode: This column shows no entry.

Note: For 11 ac devices, this column shows no entry.

2.2.90 Modem Temperature(C)

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the temperature of the WLAN interface in degrees Celsius at the time of log collection.

Note: This column shows no entry if no value is available.

2.2.91 CPU Load

Column supported for devices according to: IEEE 802.11n, IEEE 802.11ac

This column shows the average CPU load since the last logged entry.

2.3 Configuration via WEBconfig (graphical user interface)

HiLCOS Menu Tree > Setup > WLAN > WLAN-Diagnostics > Active

Here you activate the WLAN-Diagnostics table.

Possible values:

Yes
No

Default:

No

HiLCOS Menu Tree > Setup > WLAN > WLAN-Diagnostics > Config > Time-Interval (ms)

Here you specify the time interval for recording the entries in the WLAN-Diagnostics table.

Possible values: 200 ms to 60000 ms

Default: 1000 ms

HiLCOS Menu Tree > Setup > WLAN > WLAN-Diagnostics > Filter > SSID

Here you can specify a SSID that serves as a basis for filtering the entries in the WLAN-Diagnostics table. The Clients connected to that SSID will then be logged in the WLAN-Diagnostics table.
If you do NOT specify any SSID, then the connected Clients in every SSID will be logged.

Possible values: Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:

1) Test?0: All clients connected with SSID having any character in place of “?” will be logged (for example Test10, Test20)
2) Test*: All clients connected with SSID starting with “Test” will be logged (for example Test123, Testfirst)

Default: No entry

HiLCOS Menu Tree > Setup > WLAN > WLAN-Diagnostics > Filter > Lowest SNR Clients

Here you specify the number of connected Clients with the lowest SNR that shall be logged in the WLAN-Diagnostics table.
If you set the value to 0, all the connected Clients will be logged in the WLAN-Diagnostics table.

Possible values: 0 to 255

Default: 3

HiLCOS Menu Tree > Setup > WLAN > WLAN-Diagnostics > Filter > Client Name

Here you can specify the name of a Client that shall be logged in the WLAN-Diagnostics table.
If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

Possible values: max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:

1) BAT45?1: All Clients with a name having any character in place of “?” will be logged (for example BAT4501, BAT4521)
2) BAT45*: All Clients with a name starting with “BAT45” will be logged (for example BAT45012, BAT45655)

Default: No entry

HiLCOS Menu Tree > Setup > WLAN > WLAN-Diagnostics > Filter > Client MAC

Here you can specify the MAC address of a Client that shall be logged in the WLAN-Diagnostics table. If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

Possible values: Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:

1) 04:f0:21:33:2c:?d: All Clients with a MAC address having any character in place of “?” will be logged (for example 04:f0:21:33:2c:fd).
2) 04:f0:21:33:2c:*.: All Clients with a MAC address starting with “04:f0:21:33:2c:” will be logged (for example 04:f0:21:33:2c:6d).

Default: No entry

Examples for possible MAC address formats:

1) 04:f0:21:33:2c:9d
2) 04f021332c9d
3) 04-f0-21-33-2c-9d

HiLCOS Menu Tree > Setup > WLAN > WLAN-Diagnostics > Filter > Client IP

Here you can specify the IP address of a Client that shall be logged in the WLAN-Diagnostics table. If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

Possible values: Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported
Examples for using a wild card:

1) 192.168.10.2?: All Clients with an IP address having any character in place of “?” will be logged (for example 192.168.10.23).
2) 192.168.10.*: All Clients with an IP address starting with “192.168.10.” will be logged (for example 192.168.10.40).

Default: No entry

HiLCOS Menu Tree > Setup > WLAN > WLAN-Diagnostics > Filter > Highest SNR Neighbor AP

Here you can specify values ranging from 0 to 3. These values represent the number of strongest neighboring Access Points with the event source labeled as 'Neighbor'. When a background scan is initiated, rows containing information about these neighboring Access Points are added to the WLAN Diagnostics table. The value selected determines how many of the strongest neighboring Access Points are included.

Possible values: 0-3

Default: 0

HiLCOS Menu Tree > File management > Download Certificate or File
Here you can download the WLAN-Diagnostics table.

1) Open the “File management > Download Certificate or File” dialog.
2) In the dropdown menu, choose “WLAN-Diagnostics Table(*.csv)”
3) Click “Start Download”
4) The downloaded file will be named as follows: “[Date]-[Time]-[Device Name].csv”

2.4 Additions to the Setup Menu (CLI)

Active
Here you activate the WLAN-Diagnostics table.

SNMP ID:
2.12.260.263

Telnet path:
Setup > WLAN > WLAN-Diagnostics

Possible values: Yes, No

Default: No

Time-Interval (ms)
Here you specify the time interval for recording the entries in the WLAN-Diagnostics table.

SNMP-ID:
2.12.260.261.2

Telnet path:
Setup > WLAN > WLAN-Diagnostics > Config

Possible values: 200 ms to 60000 ms

Default: 1000 ms

SSID
Here you can specify a SSID that serves as a basis for filtering the entries in the WLAN-Diagnostics table. The Clients connected to that SSID will then be logged in the WLAN-Diagnostics table.
If you do NOT specify any SSID, then the connected Clients in every SSID will be logged.

SNMP ID:
2.12.260.262.10

Telnet path:
Setup > WLAN > WLAN-Diagnostics > Filter

Possible values: Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:
1) Test?0: All clients connected with SSID having any character in place of “?” will be logged (for example Test10, Test20)
2) Test*: All clients connected with SSID starting with “Test” will be logged (for example Test123, Testfirst)

Default: No entry

Lowest-SNR-Clients

Here you specify the number of connected Clients with the lowest SNR that shall be logged in the WLAN-Diagnostics table.
If you set the value to 0, all the connected Clients will be logged in the WLAN-Diagnostics table.

SNMP ID:

2.12.260.262.11

Telnet path:

Setup > WLAN > WLAN-Diagnostics > Filter

Possible values: 0 to 255

Default: 3

Client-Name

Here you can specify the name of a Client that shall be logged in the WLAN-Diagnostics table.
If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

SNMP ID:

2.12.260.262.12

Telnet path:

Setup > WLAN > WLAN-Diagnostics > Filter

Possible values: Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:

1) BAT45?1: All Clients with a name having any character in place of “?” will be logged (for example BAT4501, BAT4521)
2) BAT45*: All Clients with a name starting with “BAT45” will be logged (for example BAT45012, BAT45655)

Default: No entry

Client-MAC

Here you can specify the MAC address of a Client that shall be logged in the WLAN-Diagnostics table.
If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

SNMP ID:

2.12.260.262.13

Telnet path:

Setup > WLAN > WLAN-Diagnostics > Filter

Possible values: Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported.
Examples for using a wild card:

1) 04:f0:21:33:2c:?d: All Clients with a MAC address having any character in place of “?” will be logged (for example 04:f0:21:33:2c:fd).
2) 04:f0:21:33:2c:*.: All Clients with a MAC address starting with “04:f0:21:33:2c:” will be logged (for example 04:f0:21:33:2c:6d).

Default: No entry

Examples for possible MAC address formats:

1) 04:f0:21:33:2c:9d
2) 04f021332c9d
3) 04-f0-21-33-2c-9d

Client-IP

Here you can specify the IP address of a Client that shall be logged in the WLAN-Diagnostics table. If you do NOT specify any Client, then all the connected Clients will be logged in the WLAN-Diagnostics table.

SNMP ID:

2.12.260.262.14

Telnet path:

Setup > WLAN > WLAN-Diagnostics > Filter

Possible values: Max. 256 characters from [A-Z] [a-z] [0-9] #@{|}~!$%&'()*+-,/:;<=>?[\]^_. `
Wild cards are also supported
Examples for using a wild card:

1) 192.168.10.2?: All Clients with an IP address having any character in place of “?” will be logged (for example 192.168.10.23).
2) 192.168.10.*: All Clients with an IP address starting with “192.168.10.” will be logged (for example 192.168.10.40).

Default: No entry

Highest-SNR-Neighbor-AP

Here you can specify values ranging from 0 to 3. These values represent the number of strongest neighboring Access Points with the event source labeled as 'Neighbor'. When a background scan is initiated, rows containing information about these neighboring Access Points are added to the WLAN Diagnostics table. The value selected determines how many of the strongest neighboring Access Points are included.

SNMP ID:

2.12.260.262.15

Telnet path:

Setup > WLAN > WLAN-Diagnostics > Filter

Possible values: 0-3

Default: 0

3 Chain-Noises

For 802.11N devices, SNMP values are available to assist in detecting potential Front End Module (FEM) damage. The Chain-Noises table displays noise values measured on each antenna/chain in dBm on the physical WLAN interface. If an antenna is configured, its respective noise level appears in the table; otherwise, the column remains empty.

Here you find the Chain-Noises table:
HiLCOS Menu Tree > Status > WLAN > Chain-Noises

4 Force-Background-Scan

This feature initiates background scanning without taking into account the "NoRoamingThreshold" for a specified WLAN interface. When the force background scan is successfully triggered, a syslog is generated indicating: "[WLAN-X] Roaming indication: Immediate roaming Triggered".

Here you find the syslog:
HiLCOS Menu Tree > Status > WLAN > Force-Background-Scan

5. Factory-Default Network-Exposed Services

Upon first power-up, HiLCOS ships with a predefined set of network services and built-in network functions in its factory-default state to support out-of-the-box connectivity, management, and diagnostics. For each service, the table below indicates:

- **Port:** TCP and/or UDP port number(s) used.
- **Proto.:** Transport protocol.
- **Local Access:** Whether the service listens on LAN-side interfaces by default.
- **External Access:** Whether it listens on the WAN (Internet) side by default.
- **Config Path:** Where in the CLI, WebConfig or menu to locate the setting
- **SNMP ID:** The numeric MIB Object Identifier (OID) used to monitor or configure this service via SNMP.
- **Auth. Req.:** Whether user authentication is required to use the service.
- **Encrypt. :** Whether the service encrypts traffic by default.

Disabled entries require explicit administrator action and, for any service that is access-controlled (for example WebConfig, CLI/SSH, SNMP v3), a valid administrator login to enable or connect to it.

Service	Port	Proto.	Local Access	External Access	Config Path	SNMP ID	Auth. Req.	Encrypt.
ComPort-Server	0	TCP	disabled	disabled	Setup > COM-Ports > COM-Port-Server	2.52.2	no	no
DNS-Server	53	TCP, UDP	enabled	disabled	Setup > DNS	2.17	no	no
HiLCOSCap/ CAPWAP	41047/ 1027	UDP	enabled	disabled	Setup > WLAN-Management > AP-Configuration	2.37.1	yes	yes
IAPP	2313	UDP	enabled	disabled	Setup > WLAN	2.12	no	no
iPerf	5001	TCP, UDP	enabled	disabled	Setup > Iperf	2.96	no	no
IPsec / IKE	500/ 4500	UDP	disabled	disabled	Setup > VPN	2.19	yes	yes
L2TP-Server	1701	UDP	disabled	disabled	Setup > WAN	2.2	yes	no
					Setup > WAN > RADIUS	2.2.22		
NetBIOS-Datagram-Distribution	138	TCP	disabled	disabled	Setup > NetBIOS	2.16	no	no
NetBIOS-Name-Service	137	TCP	disabled	disabled	Setup > NetBIOS	2.16	no	no
NTP / SNTP-Server	123	UDP	disabled	disabled	Setup > NTP > NetworkList	2.26.16	no	no
PPTP-Server	1723	TCP, GRE	disabled	disabled	Setup > WAN	2.2	yes	yes
Printerserver-LPD	515	UDP	disabled	disabled	Setup > Printer	2.34	no	no

Service	Port	Proto.	Local Access	External Access	Config Path	SNMP ID	Auth. Req.	Encrypt.
Printerserver-RawIP	9100	UDP	disabled	disabled	Setup > Printer > Printer	2.34.1	no	no
RPCap	2002	TCP	disabled	disabled	Setup > Packet-Capture	2.63	no	no
RADIUS Client	1812	UDP	disabled	disabled	Setup > WAN > RADIUS	2.2.22	yes	yes
RADIUS-Accounting	1813	UDP	disabled	disabled	Setup > WLAN > RADIUS-Accounting	2.12.45	yes	yes
RADIUS-Authentication	1812	UDP	disabled	disabled	Setup > WAN > RADIUS	2.2.22	yes	yes
RADSEC	2083	TCP	disabled	disabled	Setup > RADIUS > RADSEC	2.25.20	yes	yes
					Setup > RADIUS > Server	2.25.10		
RIP (Routing Info. Prot.)	520	UDP	disabled	disabled	Setup > IP-Router > RIP	2.8.8	no	no
SFTP	22	TCP	enabled	disabled	Setup > Config > SSH > SFTP-Server	2.11.28.10	yes	yes
SSH	22	TCP	enabled	disabled	Setup > Config > SSH	2.11.28	yes	yes
SNMP v1/v2c (RO)	161	UDP	enabled	disabled	Setup > SNMP	2.9	no[1]	no
SNMP v3	161	UDP	enabled	disabled	Setup > SNMP	2.9	yes[1]	yes[1]
Telnet	23	TCP	enabled	disabled	Setup > Config	2.11	yes[1]	no
Telnet/SSL	992	TCP	enabled	disabled	Setup > Config > Telnet-SSL	2.11.29	yes[1]	yes[1]
TFTP	69	UDP	enabled	disabled	Setup > Config > Access-Table	2.11.15	no[1]	no
WEBservices-HTTP	80	TCP	enabled	disabled	Setup > HTTP	2.21	yes[2]	no
WEBservices-HTTPS	443	TCP	enabled	disabled	Setup > HTTP > SSL	2.21.40	yes	yes

[1] The administrator may enable (yes) or disable (no) this service at will via the indicated Config Path, according to their operational requirements.

[2] Every SOAP- or REST-based management API endpoint exposed over HTTP or HTTPS requires a valid session token or API key. There are no publicly writable or readable methods available without authentication.

6. Post-Initial-Password Security Hardening

Immediately after the administrator sets a device password, HiLCOS automatically enforces a stricter security posture to mitigate clear-text and unauthenticated attack vectors:

1. **HTTPS First:**
   - HiLCOS generates a self-signed X.509 certificate.
   - HTTPS (port 443) is forced as the primary management channel.
   - HTTP (port 80) is redirected to HTTPS or disabled, per policy.
2. **Service Lock-Down:**
   - All remaining clear-text access services (HTTP, Telnet, SNMP v1/v2c, TFTP) are disabled or restricted to local-only access until explicitly re-enabled by the administrator.
   - Any optional SNMP v3 privacy/auth settings default to “on” when enabled.
3. **Administrative Reminder:**
   The following services carry no built-in confidentiality or strong authentication and should remain disabled unless your network design explicitly requires them—ideally placed behind dedicated firewalls or inside a VPN tunnel:
   - HTTP (TCP 80)
   - Telnet (TCP 23)
   - SNMP v1/v2c (UDP 161)
   - TFTP (UDP 69)

   Where possible, avoid clear-text or unauthenticated services, use these secure replacements instead:

   - HTTP (TCP 80) → HTTPS (TCP 443)
     TLS-encrypted WebConfig; HiLCOS auto-generates a self-signed cert once the admin password is set.
   - Telnet (TCP 23) → SSH (TCP 22)
     Encrypted CLI tunnel with public-key or password auth.
   - SNMP v1/v2c (UDP 161) → SNMP v3 (UDP 161)
     Provides authentication (SHA) and optional privacy (AES) for management.
   - TFTP (UDP 69) → SFTP (over SSH, TCP 22) or SCP
     Secure, authenticated file transfers instead of unencrypted TFTP.

   Adopting these changes ensures all management traffic is both authenticated and encrypted.

7. Antenna Chain Noise Observation Mechanism (applies exclusively to 11n devices)

The Antenna Chain Noise Observation Mechanism continuously monitors the RF chain-noise on each antenna of 802.11n radios and detects short-term fluctuations that may indicate front-end module (FEM) degradation, antenna damage, or environmental interference. The feature samples per-antenna noise values at runtime and counts how many times the noise level of each antenna crosses a user-configurable negative dBm threshold within a configurable time window. If any crossings occur during that time window, it emits an aggregate syslog containing the per-antenna crossing counts and the lowest noise value observed.This mechanism is intended as a diagnostic aid for field technicians and network operators: It provides early, antenna-specific indicators of hardware health. The feature is exclusively for 11n devices and is disabled by default. The feature should be enabled by an administrator for targeted troubleshooting. Hirschmann recommends choosing conservative thresholds and reasonable intervals to avoid excessive logging.

To use the feature, perform the following work steps:

1. Enable chain noise threshold monitoring.
2. Set the maximum acceptable chain-noise level in negative dBm.
3. Specify the aggregation interval.

If, during the interval, the chain noise level of any antenna crosses the threshold, the device generates a syslog message for the WLAN interface with following information:

• The number of threshold crossings per antenna.

Example for a syslog message:
2025-01-01 10:00:00 KERN Info [WLAN-1] Chain noise threshold of -80 dBm

• The lowest noise value measured.

Example for a syslog message:
2025-01-01 10:00:00 KERN Info [WLAN-1] Lowest noise captured: -98 dBm exceeded on antenna chain 1/2/3: 1/2/1 occurrences in the last 30 seconds.

Note: Current chain-noise values are shown in the Chain-Noises status table.

The Chain-Noises status table displays noise values measured on each antenna/chain in dBm on the physical WLAN interface. If an antenna is configured, its respective noise level appears in the table; otherwise, the column remains empty.

Here you find the Chain-Noises status table:
HiLCOS Menu Tree > Status > WLAN > Chain-Noises

Additions to the Setup menu

Active

Here you can enable or disable Antenna Chain Noise Observation Mechanism syslogs. When enabled, the device will sample per-antenna chain noise and produce aggregated syslog entries when configured thresholds/intervals are breached. When disabled, no syslogs are produced.

SNMP ID:

2.12.90.1

Telnet path:

Setup > WLAN > Chain-Noise-Threshold > Active

Possible values:

Yes
No

Default:

No

Max-Chain-Noise (dBm)

Specify the threshold (in dBm) for counting chain-noise fluctuations. Each time the per-antenna chain-noise value exceeds this threshold during a syslog interval, the fluctuation counter for that antenna is incremented. Values are negative dBm integers.

SNMP ID:

2.12.90.2

Telnet path:

Setup > WLAN > Chain-Noise-Threshold > Max-Chain-Noise(dBm)

Possible values:

Any integer in the range from -128 to -1 (dBM)

Default:

- 101 (dBm)

Syslog-Time-Interval (s)

Time window (in seconds) used to aggregate fluctuation counts and the lowest chain-noise value. At the end of each configured interval, if at least 1 fluctuation occurred on that WLAN interface, the device generates a syslog entry containing per-antenna counts and the lowest noise observed in that interval. If no fluctuations occurred during the interval, no syslog is generated.

SNMP ID:

2.12.90.3

Telnet path:

Setup > WLAN > Chain-Noise-Threshold > Syslog-Time-Interval(s)

Possible values:

Any integer in the range from 0 to 65535 (seconds)

Default:

30 (seconds)

HIRSCHMANN

A BELDEN BRAND