HIRSCHMANN
A BELDEN BRAND

User Manual

Configuration
Industrial Cellular Router
OWL 4G Family

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.

© 2019 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 the Hirschmann product site (http://www.hirschmann.com).

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

Open Source Information

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 in the graphical user interface of the software under `Status > General > System Information > Licenses`.
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 3 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 Str. 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.

Used Symbols

Danger – Information regarding user safety.

Note – Problems that can arise in specific situations.

Information – Useful tips or information of special interest.

Example – Example of function, command or script.

Safety Instructions

⚠ WARNING

UNCONTROLLED MACHINE ACTIONS

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all the data transmission devices.

Failure to follow these instructions can result in death, serious injury, or equipment damage.

Contents

About this Manual 13

1 Basic Information 14

1.1 Standard Equipment . . . 14
1.2 Optional Features . . . 14
1.3 Configuration . . . 14
1.4 Configuration Options . . . 14
1.4.1 Valid characters for web interface . . . 15
1.5 IPv6 Support . . . 15
1.6 This Configuration Manual Describes . . . 15

2 Access to the Web Configuration 16

2.1 Certificates and Preventing the Security Message . . . 17

3 Status 19

3.1 General Status . . . 19
3.1.1 Mobile Connection . . . 19
3.1.2 Primary LAN, Secondary LAN, WiFi . . . 20
3.1.3 Peripheral Ports . . . 20
3.1.4 System Information . . . 20
3.2 Mobile WAN Status . . . 21
3.3 WiFi . . . 24
3.4 WiFi Scan . . . 25
3.5 Network Status . . . 27
3.6 DHCP Status . . . 30
3.7 IPsec Status . . . 32
3.8 DynDNS Status . . . 33
3.9 System Log . . . 34

4 Configuration 36

4.1 LAN Configuration . . . 36
4.1.1 DHCP Server . . . 38
4.1.2 IPv6 Prefix Delegation . . . 38
4.1.3 802.1X Authentication to RADIUS Server . . . 40
4.1.4 LAN Configuration Examples . . . 41
4.2 VRRP Configuration . . . 46
4.2.1 Connection to Mobile Network . . . 49
4.2.2 DNS Address Configuration . . . 50
4.2.3 Check Connection to Mobile Network Configuration . . . 51
4.2.4 Example of Check Connection Configuration . . . 51
4.2.5 Data Limit Configuration . . . 52
4.2.6 Switch between SIM Cards Configuration . . . 52
4.2.7 Examples of SIM Card Switching Configuration . . . 56
4.2.8 PPPoE Bridge Mode Configuration . . . 56
4.3 PPPoE Configuration . . . 57

4.4 WiFi Configuration . . . 59
4.5 WLAN Configuration . . . 65
4.6 Backup Routes . . . 67
4.6.1 Default Priorities for Backup Routes . . . 69
4.7 Static Routes . . . 70
4.8 Firewall Configuration . . . 71
4.8.1 Example of the IPv4 Firewall Configuration . . . 74
4.9 NAT Configuration . . . 76
4.9.1 Examples of NAT Configuration . . . 79
4.10 OpenVPN Tunnel Configuration . . . 82
4.10.1 Example of the OpenVPN Tunnel Configuration in IPv4 Network . . . 86
4.11 IPsec Tunnel Configuration . . . 87
4.11.1 Example of the IPSec Tunnel Configuration in IPv4 Network . . . 93
4.12 GRE Tunnels Configuration . . . 94
4.12.1 Example of the GRE Tunnel Configuration . . . 95
4.13 L2TP Tunnel Configuration . . . 97
4.13.1 Example of the L2TP Tunnel Configuration . . . 98
4.14 PPTP Tunnel Configuration . . . 99
4.14.1 Example of the PPTP Tunnel Configuration . . . 100
4.15 Services . . . 101
4.15.1 DynDNS . . . 101
4.15.2 FTP . . . 102
4.15.3 HTTP . . . 103
4.15.4 NTP . . . 104
4.15.5 SNMP . . . 105
4.15.6 SMTP . . . 109
4.15.7 SMS . . . 111
4.15.8 SSH . . . 119
4.15.9 Syslog . . . 120
4.15.10 Telnet . . . 121
4.16 Expansion Port – SERIAL I/O Configuration . . . 122
4.16.1 Examples of the Expansion Port Configuration . . . 125
4.17 Scripts . . . 126
4.17.1 Startup Script . . . 126
4.17.2 Example of Startup Script . . . 126
4.17.3 Up/Down Scripts . . . 127
4.17.4 Example of IPv6 Up/Down Script . . . 127
4.18 Automatic Update Configuration . . . 129
4.18.1 Example of Automatic Update . . . 131
4.18.2 Example of Automatic Update Based on MAC . . . 132

5 Customization 133

5.1 User Modules . . . 133

6 Administration 134

6.1 Users . . . 134
6.2 Change Profile . . . 135
6.3 Change Password . . . 136
6.4 Set Real Time Clock . . . 136
6.5 Set SMS Service Center Address . . . 137

6.6 Unlock SIM Card . . . 137
6.7 Unblock SIM Card . . . 138
6.8 Send SMS . . . 138
6.9 Backup Configuration . . . 139
6.10 Restore Configuration . . . 140
6.11 Update Firmware . . . 141
6.12 Reboot . . . 142
6.13 Logout . . . 142

7 Typical Situations 143

7.1 Access to the Internet from LAN . . . 143
7.2 Backup Access to the Internet from LAN . . . 145
7.3 Secure Networks Interconnection or Using VPN . . . 149
7.4 Serial Gateway . . . 151

A Maintenance 153

B Glossary and Acronyms 154

C Index 158

D Recommended Literature 161

E Further support 162

List of Figures

1 Example of the Web Configuration . . . 16
2 Mobile WAN status . . . 23
3 WiFi Status . . . 24
4 WiFi Scan . . . 26
5 Network Status . . . 29
6 DHCP Status . . . 30
7 IPsec Status . . . 32
8 DynDNS Status . . . 33
9 System Log . . . 34
10 Example program syslogd start with the parameter -R . . . 35
11 LAN Configuration page . . . 36
12 IPv6 Address with Prefix Example . . . 39
13 Network Topology for Example 1 . . . 41
14 LAN Configuration for Example 1 . . . 42
15 Network Topology for Example 2 . . . 43
16 LAN Configuration for Example 2 . . . 44
17 Network Topology for Example 3 . . . 45
18 LAN Configuration for Example 3 . . . 45
19 Topology of VRRP configuration example . . . 47
20 Example of VRRP configuration – main router . . . 47
21 Example of VRRP configuration – backup router . . . 48
22 Example of Check Connection Configuration . . . 52
23 Mobile WAN Configuration . . . 55
24 Configuration for SIM card switching Example 1 . . . 56
25 Configuration for SIM card switching Example 2 . . . 56
26 PPPoE Configuration . . . 57
27 WiFi Configuration . . . 64
28 WLAN Configuration . . . 65
29 Backup Routes Configuration . . . 67
30 Static Routes Configuration . . . 70
31 Firewall Configuration – IPv6 Firewall . . . 71
32 Topology for the IPv4 Firewall Configuration Example . . . 75
33 IPv4 Firewall Configuration Example . . . 75
34 NAT – IPv6 NAT Configuration . . . 76
35 Topology for NAT Configuration Example 1 . . . 79
36 NAT Configuration for Example 1 . . . 79
37 Topology for NAT Configuration Example 2 . . . 80
38 NAT Configuration for Example 2 . . . 81
39 OpenVPN tunnel configuration . . . 85
40 Topology of OpenVPN Configuration Example . . . 86
41 IPsec Tunnels Configuration . . . 92
42 Topology of IPsec Configuration Example . . . 93
43 GRE Tunnel Configuration . . . 95
44 Topology of GRE Tunnel Configuration Example . . . 95
45 L2TP Tunnel Configuration . . . 97
46 Topology of L2TP Tunnel Configuration Example . . . 98
47 PPTP Tunnel Configuration . . . 99

48 Topology of PPTP Tunnel Configuration Example . . . 100
49 DynDNS Configuration Example . . . 101
50 Enabling of FTP server . . . 102
51 Configuration of HTTP and HTTPS services . . . 103
52 Example of NTP Configuration . . . 104
53 OID Basic Structure . . . 106
54 SNMP Configuration Example . . . 107
55 MIB Browser Example . . . 108
56 SMTP Client Configuration Example . . . 109
57 SMS Configuration for Example 1 . . . 116
58 SMS Configuration for Example 2 . . . 117
59 SMS Configuration for Example 3 . . . 117
60 SMS Configuration for Example 4 . . . 118
61 Configuration of HTTP service . . . 119
62 Syslog configuration . . . 120
63 Enabling of Telnet service . . . 121
64 SERIAL I/O configuration pages overview . . . 122
65 Expansion Port Configuration . . . 124
66 Example of Ethernet to serial communication configuration . . . 125
67 Example of serial interface configuration . . . 125
68 Example of a Startup Script . . . 126
69 Example of IPv6 Up/Down Script . . . 127
70 Example of Automatic Update 1 . . . 131
71 Example of Automatic Update 2 . . . 132
72 User modules . . . 133
73 Added user module . . . 133
74 Users . . . 135
75 Change Profile . . . 135
76 Change Password . . . 136
77 Set Real Time Clock . . . 136
78 Set SMS Service Center Address . . . 137
79 Unlock SIM Card . . . 137
80 Unblock SIM Card . . . 138
81 Send SMS . . . 138
82 Backup Configuration . . . 139
83 Restore Configuration . . . 140
84 Update Firmware . . . 141
85 Reboot . . . 142
86 Access to the Internet from LAN – sample topology . . . 143
87 Access to the Internet from LAN – *LAN* configuration . . . 144
88 Access to the Internet from LAN – *Mobile WAN* configuration . . . 144
89 Backup access to the Internet – sample topology . . . 145
90 Backup access to the Internet – LAN configuration . . . 145
91 Backup access to the Internet – WiFi configuration . . . 146
92 Backup access to the Internet – WLAN configuration . . . 147
93 Backup access to the Internet – Mobile WAN configuration . . . 147
94 Backup access to the Internet – Backup Routes configuration . . . 148
95 Secure networks interconnection – sample topology . . . 149
96 Secure networks interconnection – OpenVPN configuration . . . 150
97 Serial Gateway – sample topology . . . 151

98 Serial Gateway – konfigurace *Expansion Port 1* 152

List of Tables

1 Mobile Connection . . . 19
2 Peripheral Ports . . . 20
3 System Information . . . 20
4 Mobile Network Information . . . 21
5 Value ranges of signal strength for different technologies. . . . 22
6 Description of Periods . . . 22
7 Mobile Network Statistics . . . 22
8 Access Point State Information . . . 24
9 State Information about Connected Clients . . . 24
10 Information about Neighbouring WiFi Networks . . . 25
11 Description of Interfaces in Network Status . . . 27
12 Description of Information in Network Status . . . 28
13 DHCP Status Description for IPv4 and IPv6 leases . . . 31
14 Configuration of the Network Interface – IPv4 and IPv6 . . . 37
15 Configuration of the Network Interface – global items . . . 38
16 Configuration of Dynamic DHCP Server . . . 39
17 Configuration of Static DHCP Server . . . 39
18 IPv6 prefix delegation configuration . . . 40
19 Configuration of 802.1X Authentication . . . 40
20 VRRP configuration . . . 46
21 Check connection . . . 46
22 Mobile WAN Connection Configuration . . . 50
23 Check Connection to Mobile Network Configuration . . . 51
24 Data Limit Configuration . . . 52
25 Switch between SIM cards configuration . . . 53
26 Parameters for SIM card switching . . . 54
27 PPPoE configuration . . . 58
28 WiFi Configuration . . . 63
29 WLAN Configuration . . . 66
30 Configuration of DHCP Server . . . 66
31 Backup Routes Configuration . . . 68
32 Backup Routes . . . 68
33 Static Routes configuration . . . 70
34 Filtering of Incoming Packets . . . 72
35 Forwarding filtering . . . 73
36 NAT Configuration . . . 77
37 Remote Access Configuration . . . 78
38 Configuration of Send all incoming packets to server . . . 78
39 OpenVPN Configuration . . . 84
40 OpenVPN Configuration Example . . . 86
41 IPsec Tunnel Configuration . . . 90
42 Example IPsec configuration . . . 93
43 GRE Tunnel Configuration . . . 94
44 GRE Tunnel Configuration Example . . . 96
45 L2TP Tunnel Configuration . . . 97
46 L2TP Tunnel Configuration Example . . . 98
47 PPTP Tunnel Configuration . . . 99

48 PPTP Tunnel Configuration Example . . . 100
49 DynDNS Configuration . . . 101
50 Parameters for HTTP and HTTPS services configuration . . . 103
51 NTP Configuration . . . 104
52 SNMP Agent Configuration . . . 105
53 SNMPv3 Configuration . . . 105
54 SNMP Configuration (R-SeeNet) . . . 106
55 Object identifier for binary inputs and output . . . 107
56 SMTP client configuration . . . 109
57 SMS Configuration . . . 111
58 Control via SMS . . . 112
59 Control SMS . . . 113
60 Send SMS on the serial Port 1 . . . 113
61 Send SMS on the serial Port 2 . . . 114
62 Sending/receiving of SMS on TCP port specified . . . 114
63 List of AT Commands . . . 115
64 Parameters for SSH service configuration . . . 119
65 Syslog configuration . . . 120
66 Expansion Port Configuration – serial interface . . . 123
67 Expansion Port Configuration – *Check TCP connection* . . . 123
68 CD Signal Description . . . 123
69 DTR Signal Description . . . 124
70 Automatic Update Configuration . . . 129
71 Users Overview . . . 134
72 Add User . . . 134

About this Manual

This "Configuration" user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

1 Basic Information

OWL-4G routers are designed for communication across cellular networks using either LTE technology Category 4 (theoretically 150 Mbps downlink and 50 Mbps uplink), or LTE Category M1 (CAT-M1 for IoT and M2M communications). The router is an ideal solution for industrial wireless connection of traffic and security camera systems, individual computers, LANs, automatic teller machines (ATM), other self-service terminals, and many other devices.

1.1 Standard Equipment

Standard features include the LTE cellular module (with two antenna connectors – for main and diversity antenna), two Ethernet 10/100 ports, one binary input, one binary output, RS-232 serial interface, RS-485 serial interface (single 10-pin connector for serial and binary interfaces), and two SIM card readers for 3 V and 1.8 V SIM cards. The router is supplied in a metal casing.

1.2 Optional Features

If desired, the router can be ordered in extended version with WiFi module and GPS. On this version of router there are two WiFi antenna connectors on the right side of the router and GNSS antenna connector between them. Note that routers cannot be retrofitted with interfaces feature at some point in the future. See the router's technical manual for details on versions and possible combinations of interfaces.

1.3 Configuration

Configuring OWL-4G routers is made easy by name and password protected web interface. The interface provides detailed statistics about router activities, signal strength, system logs and more. The router supports both IPv4 and IPv6 protocols, the creation of secure VPN tunnels using technologies IPsec, OpenVPN and L2TP. The router also supports DHCP, NAT, NAT-T, DynDNS client, NTP, VRRP, control by SMS, backup of primary connection, multiple WANs, RADIUS authentication on Ethernet and WiFi, and many other functions.

Additional diagnostic features designed to ensure continuous communication include automatic inspection of Mobile WAN connections, an automatic restart feature in case a connection is lost, and a hardware watchdog that monitors the status of the router. Using a start up script window, users can insert Linux scripts for various actions. Users may insert multiple scripts and the router can switch between configurations as needed. Examples would include using SMS or checking the status of the binary input. OWL-4G routers can automatically update their configurations and firmware from a central server, allowing for mass reconfiguration of multiple routers at the same time.

1.4 Configuration Options

Routers can be configured via web browser or Secure Shell (SSH). Configuration via Web Browser is described in this Configuration Manual. Commands and scripts applicable in config-

uration using SSH are described in *Commands and Scripts for v2 and v3 Routers – Application Note* [1]. Technical parameters and a full description of the router can be found in the User Manual of your router. You can also use additional software – communication VPN server SmartCluster [2] and software for router monitoring R-SeeNet [3, 4].

1.4.1 Valid characters for web interface

If the router is configured through the web interface, avoid entering of forbidden characters into any of input form (not just for password). Forbidden characters can by written into a form, but they will be deleted during data storing.

Valid characters are: `0-9 a-z A-Z * , + - . / : = ? ! # % @ [ ] _ { } ~`

Forbidden characters are: `‘‘ $ & ’ ( ) ; < > \ ^ ‘ | "space"`

1.5 IPv6 Support

There is independent IPv4 and IPv6 dual stack configuration implemented in the router's firmware. This means that you can configure traffic through both IP protocols independently and both are supported. Additional EUI-64 IPv6 addresses of network interfaces are generated automatically by standard methods. There is a NAT64 internal gateway network interface for automatic translation between IPv6 and IPv4 (see Chapter 3.5 for more information). This gateway works together with DNS64 seamlessly (for domain names translation).

For cellular IPv6 connection see *Mobile WAN Configuration* in Chapter 4.2.1. For IPv6 LAN configuration see *LAN Configuration* in Chapter 4.1, DHCPv6 server/client is also supported. IPv4 is the default, but IPv6 can be enabled or used with all features and protocols in the router, except for non-secured tunnels GRE, L2TP and PPTP, and VRRP. Using the secured tunnels OpenVPN and IPsec it is possible to run IPv6 traffic through an IPv4 tunnel and vice versa. The configuration forms for *NAT*, *Firewall* and *Up/Down Scripts* are completely separate for the IPv4 and IPv6 stacks. ICMPv6 protocol is also supported. IPv6 configuration is covered in each following Chapter when possible.

1.6 This Configuration Manual Describes

- Configuration of the router item by item according to the web interface (chapters 3 to 6).
- Configuration in typical situations examples (chapter 7):
  - Access to the Internet from LAN (Local Area Network) via mobile network, Ch. 7.1.
  - Backed up access to the Internet (from LAN), Ch. 7.2.
  - Secure networks interconnection or using VPN (Virtal Private Network), Ch. 7.3.
  - Serial Gateway (connection of serial devices to the Internet), Ch. 7.4

2 Access to the Web Configuration

Wireless transmissions work only when you activate the SIM card for data traffic and insert it into the router. Remove the power source before inserting the SIM card.

You may use the web interface to monitor, configure and manage the router. To do so, enter the router's IP address in your browser. The default address is 192.168.1.1. Only access via secured HTTPS protocol is permitted. So the syntax for the IP address must be https://192.168.1.1. When accessing the router for the first time you will need to install a security certificate if you don't want the browser to show you a domain disagreement message. To avoid receiving domain disagreement messages, follow the procedure described in the follow-

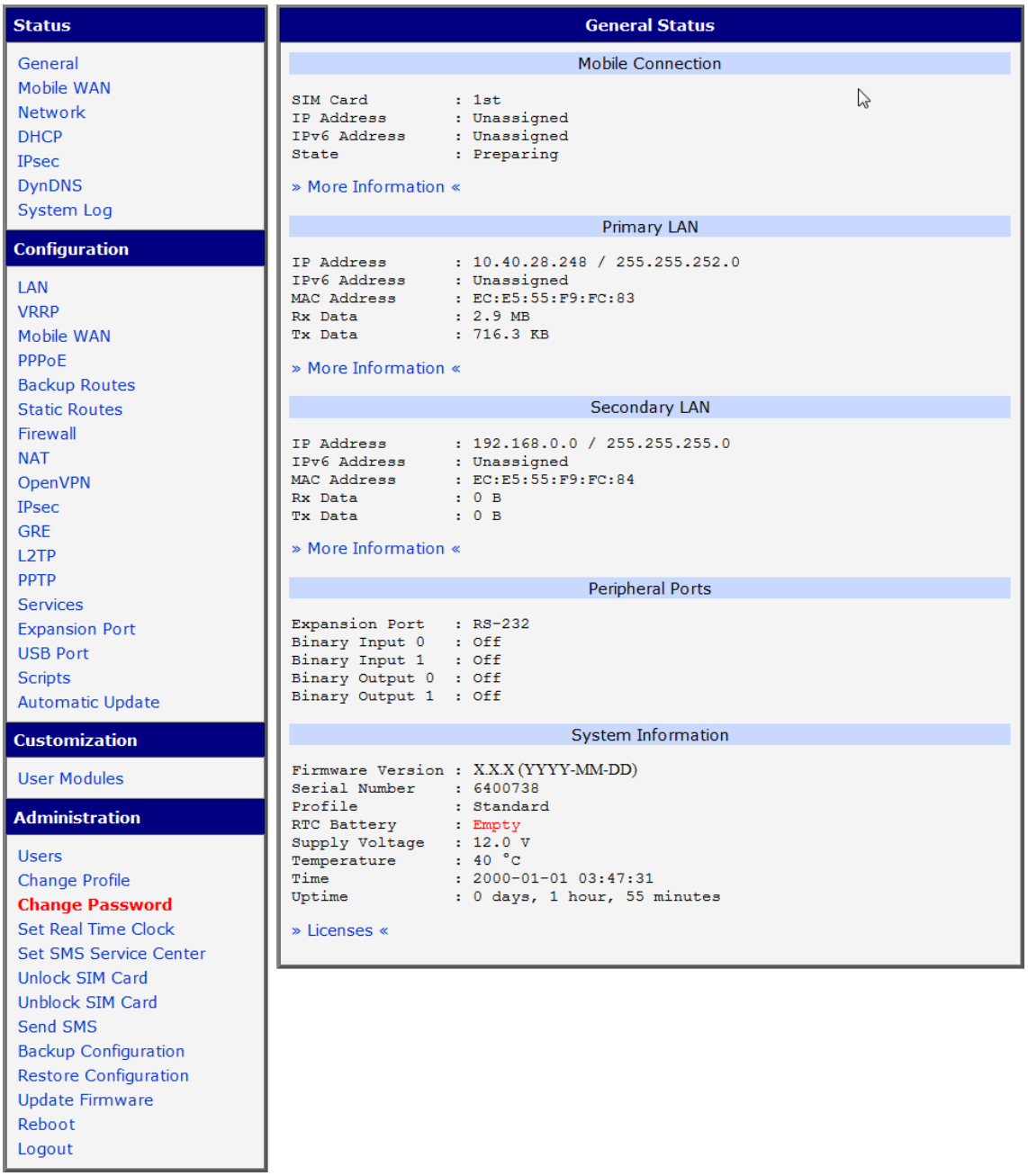


Figure 1: Example of the Web Configuration

ing subchapter.

The default username is "***admin***". The default password is "***private***". Change the default pass-word as soon as possible!

For increased security of the network connected to the router, change the default router password. When the default password of the router is still active, the ***Change password*** title is highlighted in red.

After three unsuccessful login attempts, any HTTP(S) access from an IP address is blocked for one minute.

When you successfully enter login information on the login page, web interface will be displayed. The left side of the web interface contains a menu tree with sections for monitoring (*Status*), configuration (*Configuration*), customization (*Customization*) and administration (Administration) of the router.

Name and *Location* items in the right upper corner display the name and location of the router in the SNMP configuration (see 4.15.5). These fields are user-defined for each router.

After the green LED starts to blink you may restore the initial router settings by pressing the reset (*RST*) button on the back panel. If the reset button is pressed, all configuration will revert to factory defaults and the router will reboot (the green LED will be on during the reboot).

2.1 Certificates and Preventing the Security Message

There is the self-signed HTTPS certificate in the router. Because the identity of this certificate cannot be validated, a message can appear in the web browser. To solve this, upload your own certificate, signed by Certification Authority, to the router. If you want to use your own certificate (e.g. in combination with the dynamic DNS service), you need to replace the */etc/certs/https_cert* and */etc/certs/https_key* files in the router. This can be done easily in the GUI on *HTTP* configuration page, see chapter 4.15.3.

HTTPS certificate creation in the router was updated since FW 5.3.5 to be more secure. Existing HTTPS certificates on already manufactured routers will not be automatically upgraded with the firmware upgrade! You can upgrade HTTPS certificate or upload your own certificate, for more information see chapter 4.15.3.

If you decide to use the self-signed certificate in the router to prevent the security message (domain disagreement) from pop up every time you log into the router, you can take the following steps:

Note: You will have to use the domain name based on the MAC address of the router and it is not guaranteed to work with every combination of an operating system and a browser.

- Add the DNS record to your DNS system: Edit /etc/hosts (Linux/Unix OS) or C:\WINDOWS\system32\drivers\etc\hosts (Windows OS) or configure your own DNS server. Add a new record with the IP address of your router and the domain name based of the MAC address of the router (MAC address of the first network interface seen in *Network Status* in the Web interface of the router.) Use dash separators instead of colons. Example: A router with the MAC address 00:11:22:33:44:55 will have a domain name 00-11-22-33-44-55.

- Access the router via the new domain name address (E.g. https://00-11-22-33-44-55). If you see the security message, add an exception so the next time the message will not pop up (E.g. in Firefox Web browser). If there is no possibility to add an exception, export the certificate to the file and import it to your browser or operating system.

3 Status

3.1 General Status

Selecting the *General* item will open a screen displaying a summary of basic information about the router and its activities. This page is also displayed when you login to the web interface. Information is divided into several sections, based upon the type of router activity or the properties area: *Mobile Connection*, *Primary LAN*, *Secondary LAN*, *Peripheral Ports* and *System Information*. If the router is WiFi equipped, there will be a *WiFi* section.

IPv6 Address item can show multiple different addresses for one network interface. This is standard behavior since an IPv6 interface uses more addresses. The second IPv6 Address showed after pressing *More Information* is automatically generated EUI-64 format link local IPv6 address derived from MAC address of the interface. It is generated and assigned the first time the interface is used (e.g. cable is connected, Mobile WAN connecting, etc.).

3.1.1 Mobile Connection

Item	Description
SIM Card	Identification of the SIM card (*Primary* or *Secondary*).
Interface	Defines the network interface.
Flags	Displays network interface flags.
IP Address	IPv4 address of the network interface.
IPv6 Address	IPv6 address or addresses of the network interface – there can be more IPv6 addresses assigned to one network interface.
MTU	Maximum packet size that the equipment is able to transmit.
Rx Data	Total number of received bytes
Rx Packets	Received packets
Rx Errors	Erroneous received packets
Rx Dropped	Dropped received packets
Rx Overruns	Lost received packets because of overload.
Tx Data	Total number of sent bytes
Tx Packets	Sent packets
Tx Errors	Erroneous sent packets
Tx Dropped	Dropped sent packets
Tx Overruns	Lost sent packets because of overload.
Uptime	Indicates how long the connection to the cellular network has been established.

Table 1: Mobile Connection

3.1.2 Primary LAN, Secondary LAN, WiFi

Items displayed in this part have the same meaning as items in the previous part. Moreover, the *MAC Address* item shows the MAC address of the corresponding router's interface (*Primary LAN – eth0, Secondary LAN – eth1, WiFi – wlan0*). Visible information depends on configuration (see 4.1 or 4.4).

3.1.3 Peripheral Ports

Item	Description
Expansion Port 1	RS-232 interface. Indicates where to configure RS-232 interface (pins 6 to 10 of 10-pin SERIAL I/O connector).
Expansion Port 2	RS-485 interface. Indicates where to configure RS-485 interface (pins 1 to 3 of 10-pin SERIAL I/O connector).
Binary Input	State of binary input (pin 4 of 10-pin SERIAL I/O connector).
Binary Output	State of binary output (pin 5 of 10-pin SERIAL I/O connector).

Table 2: Peripheral Ports

3.1.4 System Information

Item	Description
Firmware Version	Information about the firmware version
Serial Number	Serial number of the router (in case of *N/A* is not available)
Profile	Current profile – standard or alternative profiles (profiles are used for example to switch between different modes of operation)
Supply Voltage	Supply voltage of the router
Temperature	Temperature in the router
Time	Current date and time
Uptime	Indicates how long the router is used
Licenses	Link to the list of open source software components of the firmware together with their complete license texts (GPL versions 2 and 3, LGPL version 2, BSD-style licenses, MIT-style licenses).

Table 3: System Information

3.2 Mobile WAN Status

The *Mobile WAN* menu item contains current information about connections to the mobile network. The first part of this page (*Mobile Network Information*) displays basic information about mobile network the router operates in. There is also information about the module, which is mounted in the router.

Item	Description
Registration	State of the network registration
Operator	Specifies the operator's network the router operates in.
Technology	Transmission technology
PLMN	Code of operator
Cell	Cell the router is connected to.
LAC	Location Area Code – unique number assigned to each location area
Channel	Channel the router communicates on • ARFCN in case of GPRS/EDGE technology, • UARFCN in case of UMTS/HSPA technology, • EARFCN in case of LTE technology.
Signal Strength	Signal strength of the selected cell, for details see the Table 5.
Signal Quality	Signal quality of the selected cell: • EC/IO for UMTS (it's the ratio of the signal received from the pilot channel – EC – to the overall level of the spectral density, ie the sum of the signals of other cells – IO). • RSRQ for LTE technology (Defined as the ratio $\frac{N \times RSRP}{RSSI}$). • The value is not available for the EDGE technology.
CSQ	Cell Signal Quality, relative value is given by RSSI (dBm). 2–9 range means Marginal, 10–14 range means OK, 15–16 range means Good, 20–30 range means excellent.
Neighbours	Signal strength of neighboring hearing cells (GPRS only)[1].
Manufacturer	Module manufacturer
Model	Type of module
Revision	Revision of module
IMEI	IMEI (International Mobile Equipment Identity) number of module
MEID	MEID number of module
ICCID	Integrated Circuit Card Identifier is international and unique serial number of the SIM card.

Table 4: Mobile Network Information

[1] If a neighboring cell for GPRS is highlighted in red, router may repeatedly switch between the neighboring and the primary cell affecting the router's performance. To prevent this, re-orient the antenna or use a directional antenna.

The value of signal strength is displayed in different color: in black for good, in orange for fair and in red for poor signal strength.

Signal strength	GPRS/EDGE/CDMA (RSSI)	UMTS/HSPA (RSCP)	LTE (RSRP)
good	> -70 dBm	> -75 dBm	> -90 dBm
fair	-70 dBm to -89 dBm	-75 dBm to -94 dBm	-90 dBm to -109 dBm
poor	< -89 dBm	< -94 dBm	< -109 dBm

Table 5: Value ranges of signal strength for different technologies.

The middle part of this page displays information about mobile signal quality, transferred data and number of connections for all the SIM cards (for each period). The router has standard intervals, such as the previous 24 hours and last week, and also period starting with *Accounting Start* defined for the MWAN module.

Period	Description
Today	Today from 0:00 to 23:59
Yesterday	Yesterday from 0:00 to 23:59
This week	This week from Monday 0:00 to Sunday 23:59
Last week	Last week from Monday 0:00 to Sunday 23:59
This period	This accounting period
Last period	Last accounting period

Table 6: Description of Periods

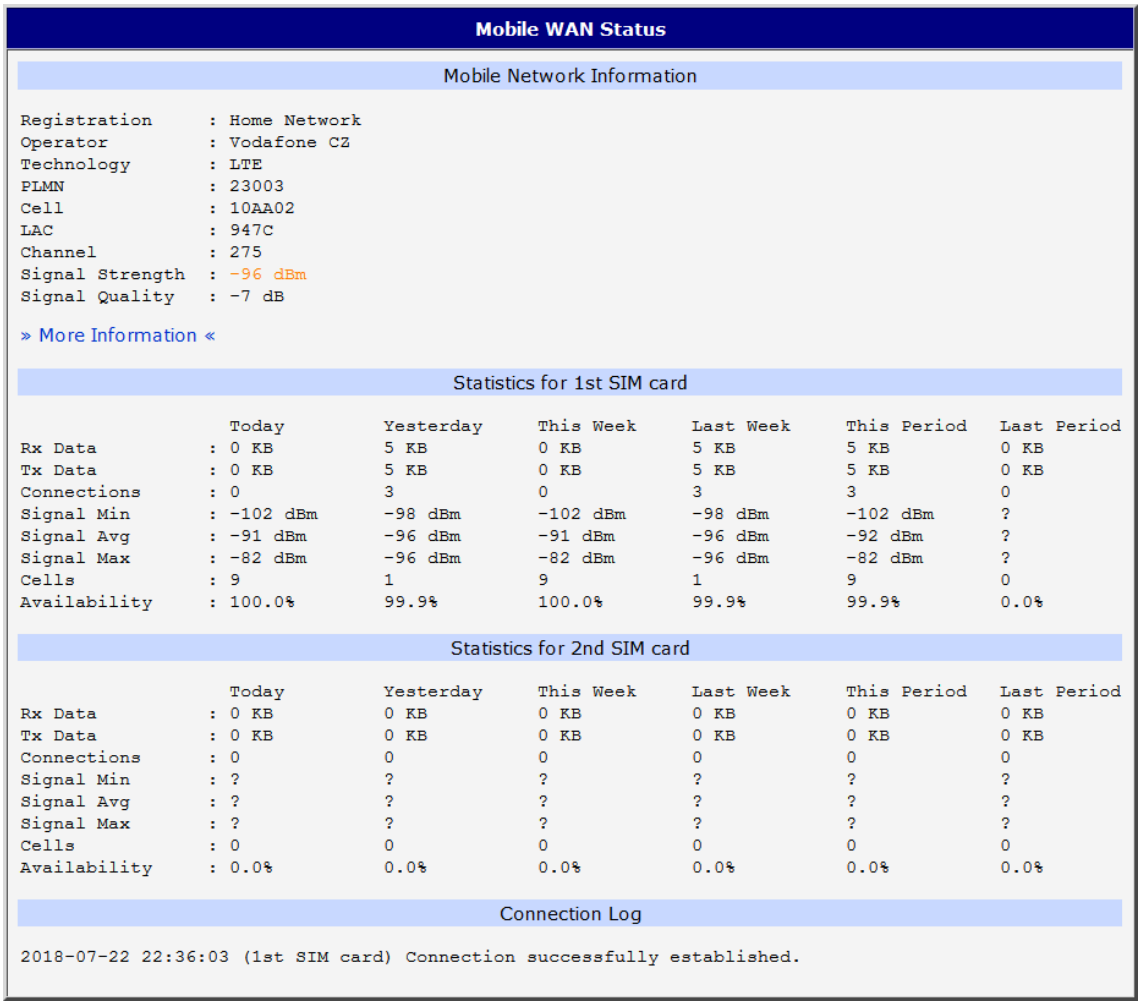
Item	Description
RX data	Total volume of received data
TX data	Total volume of sent data
Connections	Number of connection to mobile network establishment
Signal Min	Minimal signal strength
Signal Avg	Average signal strength
Signal Max	Maximal signal strength
Cells	Number of switch between cells
Availability	Availability of the router via the mobile network (expressed as a percentage)

Table 7: Mobile Network Statistics

Tips for *Mobile Network Statistics* table:

- *Availability* is expressed as a percentage. It is the ratio of time connection to the mobile network has been established to the time that router has been is turned on.
- Placing your cursor over the maximum or minimum signal strength will display the last time the router reached that signal strength.

The last part (*Connection Log*) displays information about the mobile network connections and any problems that occurred while establishing them.



Mobile WAN Status

Mobile Network Information

```
Registration     : Home Network
Operator         : Vodafone CZ
Technology       : LTE
PLMN             : 23003
Cell             : 10AA02
LAC              : 947C
Channel          : 275
Signal Strength  : -96 dBm
Signal Quality   : -7 dB
```

» More Information «

Statistics for 1st SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	0 KB	5 KB	0 KB	5 KB	5 KB	0 KB
Tx Data	0 KB	5 KB	0 KB	5 KB	5 KB	0 KB
Connections	0	3	0	3	3	0
Signal Min	-102 dBm	-98 dBm	-102 dBm	-98 dBm	-102 dBm	?
Signal Avg	-91 dBm	-96 dBm	-91 dBm	-96 dBm	-92 dBm	?
Signal Max	-82 dBm	-96 dBm	-82 dBm	-96 dBm	-82 dBm	?
Cells	9	1	9	1	9	0
Availability	100.0%	99.9%	100.0%	99.9%	99.9%	0.0%

Statistics for 2nd SIM card

	Today	Yesterday	This Week	Last Week	This Period	Last Period
Rx Data	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Tx Data	0 KB	0 KB	0 KB	0 KB	0 KB	0 KB
Connections	0	0	0	0	0	0
Signal Min	?	?	?	?	?	?
Signal Avg	?	?	?	?	?	?
Signal Max	?	?	?	?	?	?
Cells	0	0	0	0	0	0
Availability	0.0%	0.0%	0.0%	0.0%	0.0%	0.0%

Connection Log

```
2018-07-22 22:36:03 (1st SIM card) Connection successfully established.
```

Figure 2: Mobile WAN status

3.3 WiFi

This item is available only if the router is equipped with a WiFi module.

Selecting the *WiFi* item in the main menu of the web interface will display information about the WiFi access point (AP) and associated stations.

Item	Description
hostapd state dump	Time the statistical data relates to
num_sta	Number of connected stations
num_sta_non_erp	Number of connected stations using 802.11b in 802.11g BSS connection
num_sta_no_short_slot_time	Number of stations not supporting the Short Slot Time
num_sta_no_short_preamble	Number of stations not supporting the Short Preamble

Table 8: Access Point State Information

Detailed information is displayed for each connected client. Most of them have an internal character. Here are two examples:

Item	Description
STA	MAC address of connected device (station)
AID	Identifier of connected device (1 – 2007). If 0 is displayed, the station is not currently connected.

Table 9: State Information about Connected Clients

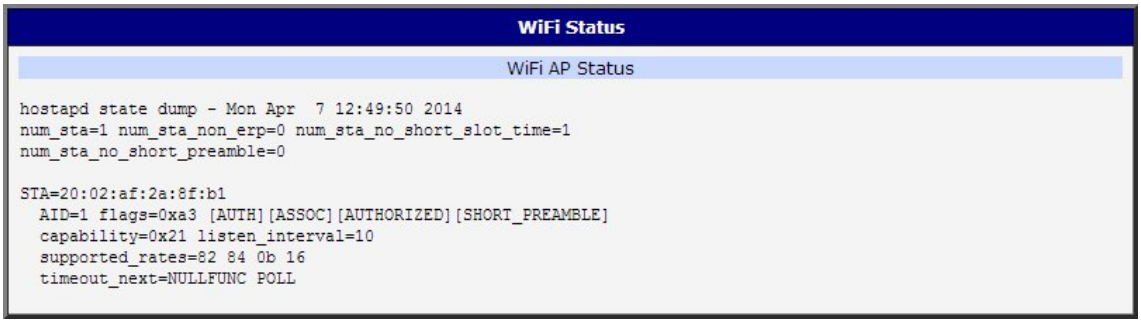


Figure 3: WiFi Status

3.4 WiFi Scan

This item is available only if the router is equipped with a WiFi module.

Selecting the *WiFi Scan* item scans for neighboring WiFi networks and displays the results. **Scanning can only be performed if the access point (WiFi AP) is off.**

Item	Description
BSS	MAC address of access point (AP)
TSF	A Timing Synchronization Function (TSF) keeps the timers for all stations in the same Basic Service Set (BSS) synchronized. All stations shall maintain a local TSF timer.
freq	Frequency band of WiFi network [kHz]
beacon interval	Period of time synchronization
capability	List of access point (AP) properties
signal	Signal level of access point (AP)
last seen	Last response time of access point (AP)
SSID	Identifier of access point (AP)
Supported rates	Supported rates of access point (AP)
DS Parameter set	The channel on which access point (AP) broadcasts
ERP	Extended Rate PHY – information element providing backward compatibility
Extended supported rates	Supported rates of access point (AP) that are beyond the scope of eight rates mentioned in *Supported rates* item
RSN	Robust Secure Network – The protocol for establishing a secure communication through wireless network 802.11

Table 10: Information about Neighbouring WiFi Networks

WiFi Scan output may look like this:

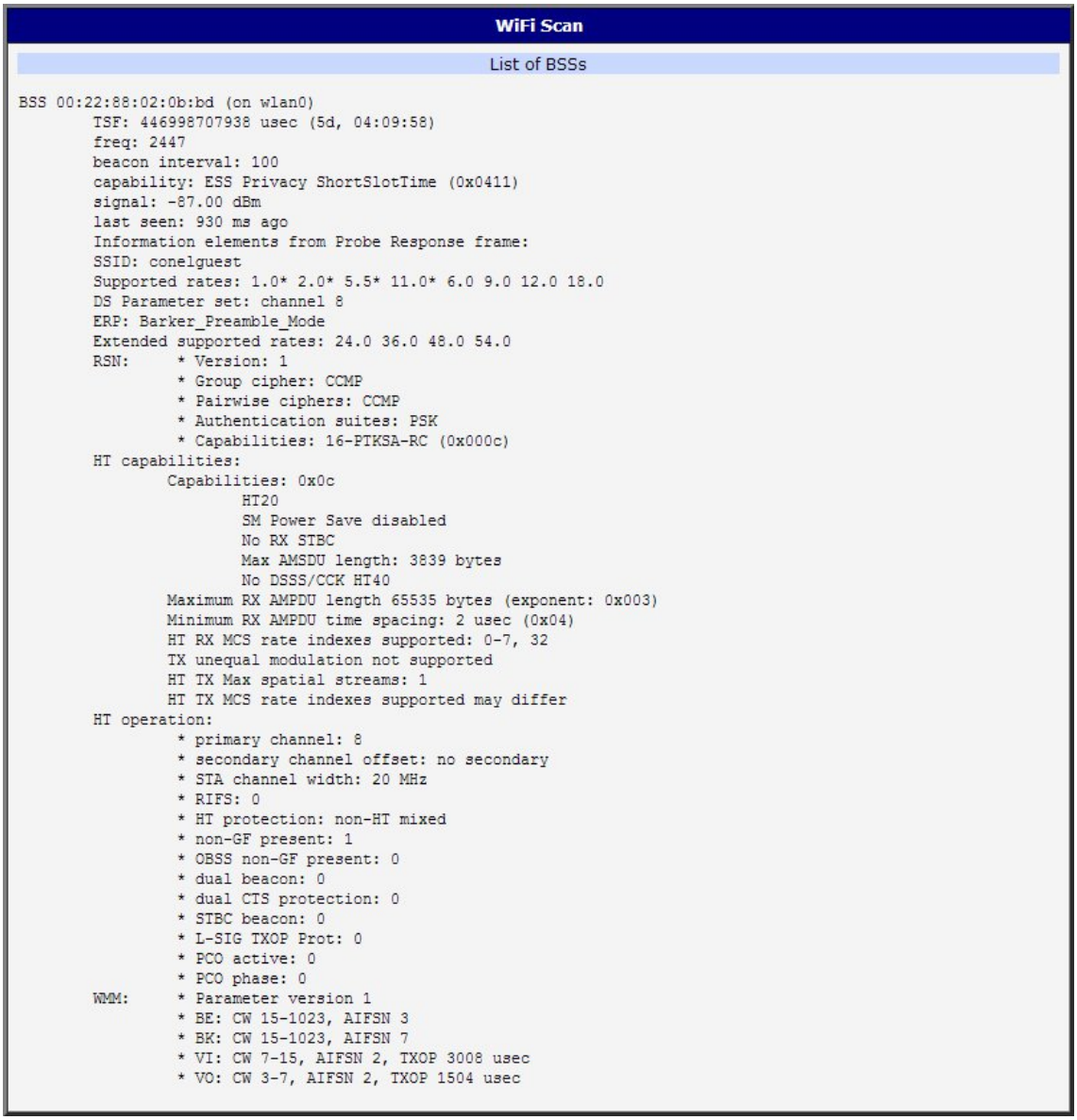


Figure 4: WiFi Scan

3.5 Network Status

To view information about the interfaces and the routing table, open the *Network* item in the *Status* menu. The upper part of the window displays detailed information about the active interfaces only:

Interface	Description
eth0, eth1, eth2	Network interfaces (Ethernet connection)
usb0	Active PPP connection to the mobile network – wireless module is connected via USB interface.
wlan0	WiFi interface
ppp0	PPP interface (e.g. PPPoE tunnel)
tun0	OpenVPN tunnel interface
ipsec0	IPSec tunnel interface
gre1	GRE tunnel interface
lo	Local loopback interface
nat64	Network interface of internal translator gateway between IPv6 and IPv4 addresses.

Table 11: Description of Interfaces in Network Status

The following information can be displayed at every network interface:

Item	Description
HWaddr	Hardware (unique, MAC) address of a network interface.
inet addr	IPv4 address of interface
inet6 addr	IPv6 address of interface. There can be more of them for single network interface.
P-t-P	IP address of the opposite end (in case of point-to-point connection).
Bcast	Broadcast address
Mask	Mask of network
MTU	Maximum packet size that the equipment is able to transmit.
Metric	Number of routers the packet must go through.
RX	• **packets** – received packets • **errors** – number of errors • **dropped** – dropped packets • **overruns** – incoming packets lost because of overload. • **frame** – wrong incoming packets because of incorrect packet size.

Continued on next page

Continued from previous page

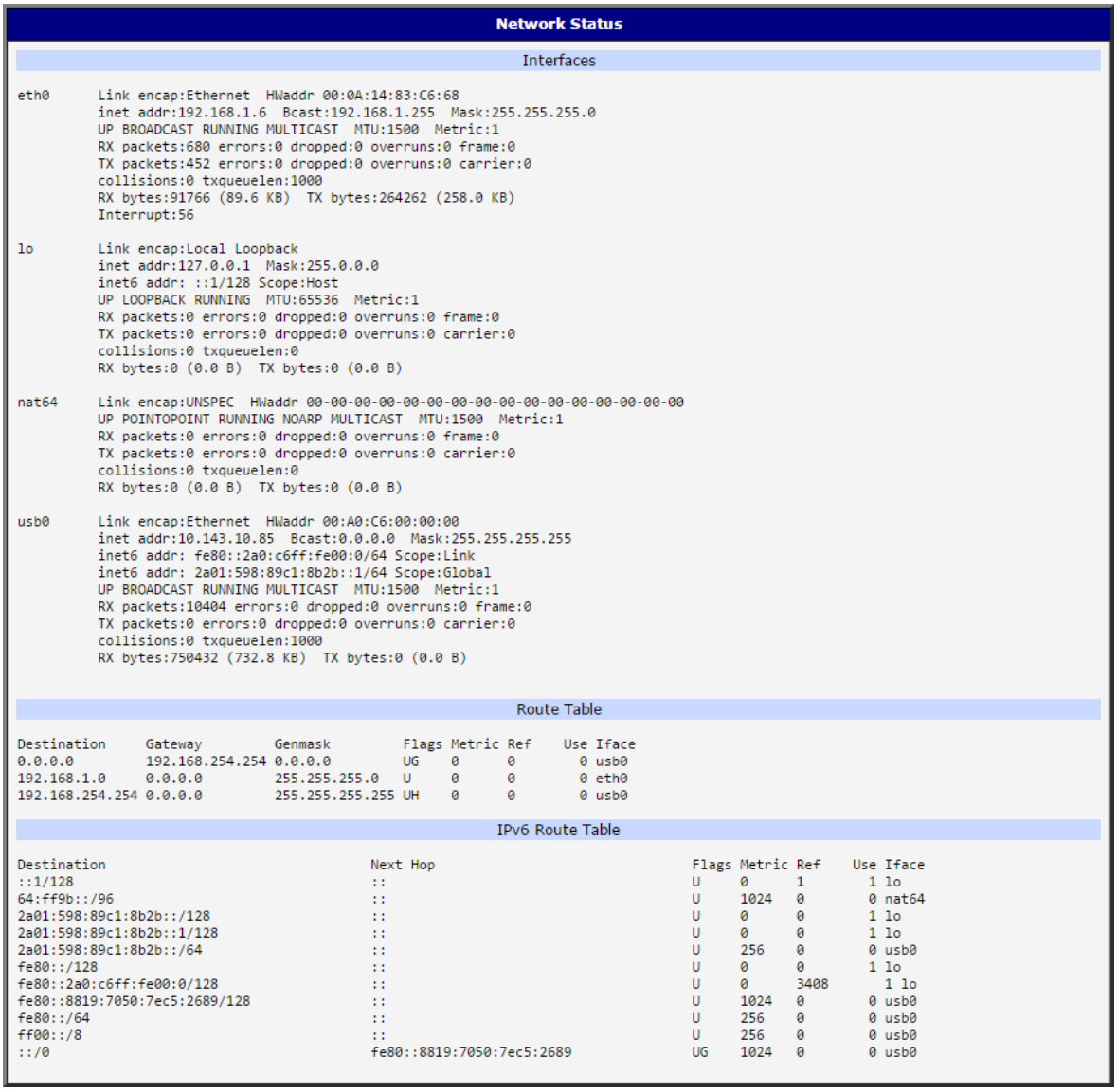
Item	Description
TX	• **packets** – transmit packets • **errors** – number of errors • **dropped** – dropped packets • **overruns** – outgoing packets lost because of overload. • **carrier** – wrong outgoing packets with errors resulting from the physical layer.
collisions	Number of collisions on physical layer.
txqueuelen	Length of buffer (queue) of the network interface.
RX bytes	Total number of received bytes.
TX bytes	Total number of transmitted bytes.

Table 12: Description of Information in Network Status

You may view the status of the mobile network connection on the network status screen. If the connection to the mobile network is active, it will appear in the system information as an usb0 interface.

The *Route Table* is displayed at the bottom of the *Network Status* page. There is IPv4 *Route Table* and *IPv6 Route Table* below.

If the router is connected to the Internet (a default route is defined), the *nat64* network interface is created automatically. This is the NAT64 internal gateway for translating the IPv6 and IPv4 communication. It is used automatically when connected via IPv6 and communicating with IPv4 device or network. It works together with DNS64 running in the router automatically (translation of domain names to IP addresses). The default NAT64 prefix 64:ff9b::/96 is used as you can see in Figure 5 below in the *IPv6 Route Table* section.



Network Status

Interfaces

```
eth0      Link encap:Ethernet  HWaddr 00:0A:14:83:C6:68
          inet addr:192.168.1.6  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:680 errors:0 dropped:0 overruns:0 frame:0
          TX packets:452 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:91766 (89.6 KB)  TX bytes:264262 (258.0 KB)
          Interrupt:56

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

nat64     Link encap:UNSPEC  HWaddr 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00
          UP POINTOPOINT RUNNING NOARP MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

usb0      Link encap:Ethernet  HWaddr 00:A0:C6:00:00:00
          inet addr:10.143.10.85  Bcast:0.0.0.0  Mask:255.255.255.255
          inet6 addr: fe80::2a0:c6ff:fe00:0/64 Scope:Link
          inet6 addr: 2a01:598:89c1:8b2b::1/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:10404 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:750432 (732.8 KB)  TX bytes:0 (0.0 B)
```

Route Table

Destination	Gateway	Genmask	Flags	Metric	Ref	Use	Iface
0.0.0.0	192.168.254.254	0.0.0.0	UG	0	0	0	usb0
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	eth0
192.168.254.254	0.0.0.0	255.255.255.255	UH	0	0	0	usb0

IPv6 Route Table

Destination	Next Hop	Flags	Metric	Ref	Use	Iface
::1/128	::	U	0	1	1	lo
64:ff9b::/96	::	U	1024	0	0	nat64
2a01:598:89c1:8b2b::/128	::	U	0	0	1	lo
2a01:598:89c1:8b2b::1/128	::	U	0	0	1	lo
2a01:598:89c1:8b2b::/64	::	U	256	0	0	usb0
fe80::/128	::	U	0	0	1	lo
fe80::2a0:c6ff:fe00:0/128	::	U	0	3408	1	lo
fe80::8819:7050:7ec5:2689/128	::	U	1024	0	0	usb0
fe80::/64	::	U	256	0	0	usb0
ff00::/8	::	U	256	0	0	usb0
::/0	fe80::8819:7050:7ec5:2689	UG	1024	0	0	usb0

Figure 5: Network Status

3.6 DHCP Status

Information about the DHCP server activity is accessible via *DHCP* item. The DHCP server provides automatic configuration of the client devices connected to the router. The DHCP server assigns each device an IP address, subnet mask, default gateway (IP address of router) and DNS server (IP address of router). DHCPv6 server is supported.

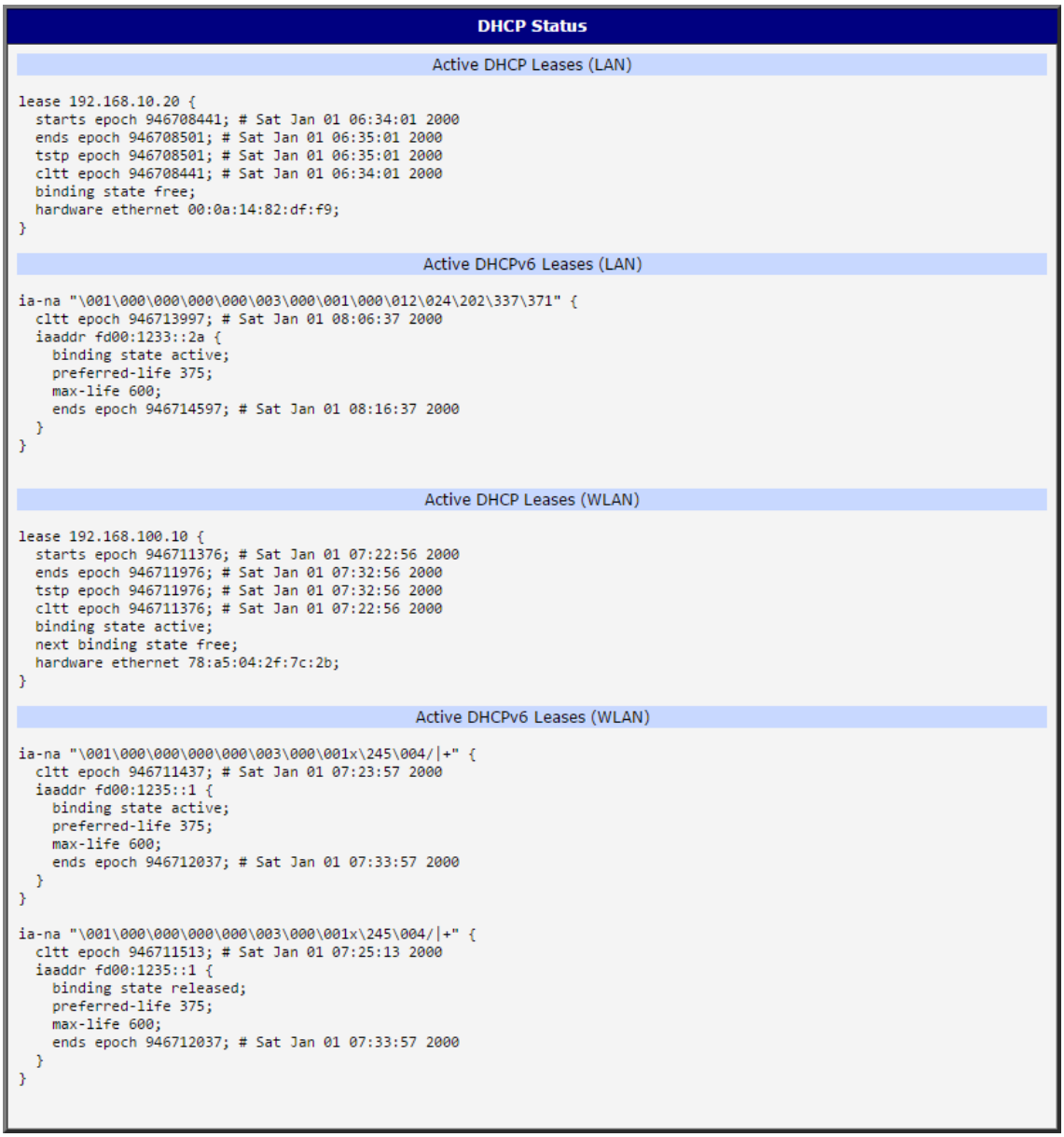


Figure 6: DHCP Status

The DHCP status may occasionally display two records for one IP address. This may be caused by resetting the client network interface.

Records in the *DHCP Status* window are divided into separate parts according to LAN and WLAN interface and IPv4 (DHCP) and IPv6 (DHCPv6) – there are parts *Active DHCP Leases (LAN)*, *Active DHCPv6 Leases (LAN)*, *Active DHCP Leases (WLAN)* and *Active DHCPv6 Leases (WLAN)* if the router has WiFi and WLAN network interface is enabled. In Figure 6 above there

are both DHCP (IPv4) and DHCPv6 (IPv6) servers enabled LAN interface and WLAN interface. The table below explains information from the client list:

Item	Description
lease	Assigned IPv4 address.
iaaddr	(IPv6) Assigned IPv6 address.
starts epoch	Time that the IP address was assigned.
ends epoch	Time that the IP address lease expires.
tstp epoch	What time the peer has been told the lease expires.
cltt epoch	Client last transaction time.
binding state	The lease's binding state.
next binding state	What state the lease will move to when the current state expires.
hardware ethernet	Unique hardware MAC address.
uid	Unique ID.
client-hostname	Host computer name.
preferred-life	(IPv6) Length of time the address can be used without any restrictions. When the preferred-life expires, the address should not be used for new communications, but might continue to be used for existing communications in certain cases.
max-life	(IPv6) Maximum time for which the DHCPv6 server can grant a lease.

Table 13: DHCP Status Description for IPv4 and IPv6 leases

3.7 IPsec Status

Selecting the *IPsec* option in the *Status* menu of the web page will bring up the information for any IPsec Tunnels that have been established. If the tunnel has been built correctly, the screen will display **ESTABLISHED** and the number of running IPsec connections **1 up** (orange highlighted in the figure below.) If there is no such text in log (e.g. "0 up"), the tunnel was not created!

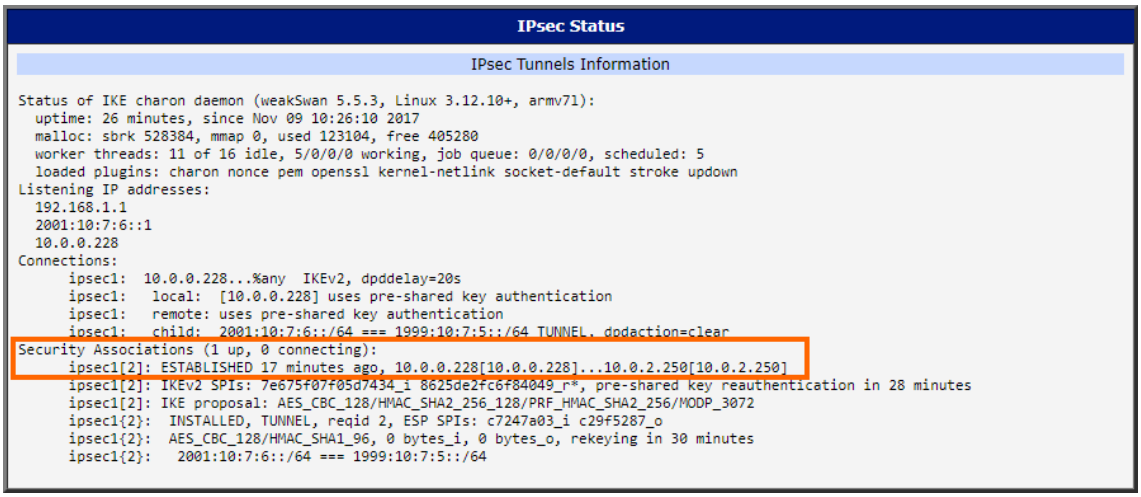


Figure 7: IPsec Status

3.8 DynDNS Status

The router supports DynamicDNS using a DNS server on www.dyndns.org. If Dynamic DNS is configured, the status can be displayed by selecting menu option DynDNS. Refer to www.dyndns.org for more information on how to configure a Dynamic DNS client.

You can use the following listed servers for the Dynamic DNS service. It is possible to use the DynDNSv6 service with *IP Mode* switched to IPv6 on *DynDNS Configuration* page.

- www.dyndns.org
- www.spdns.de
- www.dnsdynamic.org
- www.noip.com

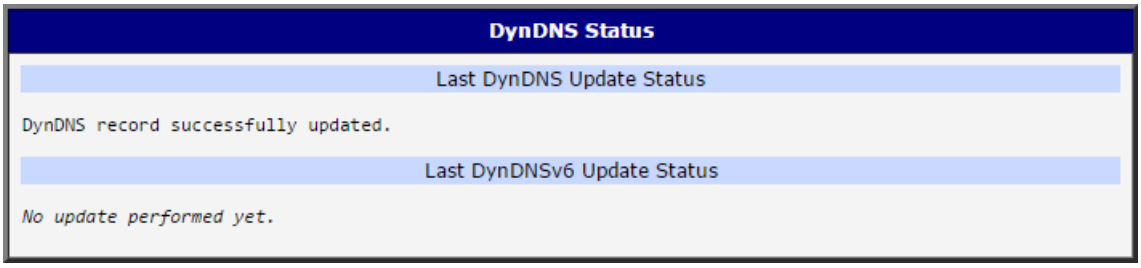


Figure 8: DynDNS Status

When the router detects a DynDNS record update, the dialog displays one or more of the following messages:

- DynDNS client is disabled.
- Invalid username or password.
- Specified hostname doesn't exist.
- Invalid hostname format.
- Hostname exists, but not under specified username.
- No update performed yet.
- DynDNS record is already up to date.
- DynDNS record successfully update.
- DNS error encountered.
- DynDNS server failure.

The router's SIM card must have public IP address assigned or DynDNS will not function correctly.

3.9 System Log

If there are any connection problems you may view the system log by selecting the *System Log* menu item. Detailed reports from individual applications running in the router will be displayed. Use the *Save Log* button to save the system log to a connected computer. (It will be saved as a text file with the .log extension.) The *Save Report* button is used for creating detailed reports. (It will be saved as a text file with the .txt extension. The file will include statistical data, routing and process tables, system log, and configuration.)

Sensitive data from the report are filtered out for security reasons.

The default length of the system log is 1000 lines. After reaching 1000 lines a new file is created for storing the system log. After completion of 1000 lines in the second file, the first file is overwritten with a new file.

The *Syslogd* program will output the system log. It can be started with two options to modify its behavior. Option "*-S*" followed by decimal number sets the maximal number of lines in one log file. Option "*-R*" followed by hostname or IP address enables logging to a remote syslog daemon. (If the remote syslog deamon is Linux OS, there has to be remote logging enabled (typically running "*syslogd -R*"). If it's the Windows OS, there has to be syslog server installed, e.g. *Syslog Watcher*). To start *syslogd* with these options, the "*/etc/init.d/syslog*" script can be modified via SSH or lines can be added into *Startup Script* (accessible in *Configuration* section) according to figure 10.

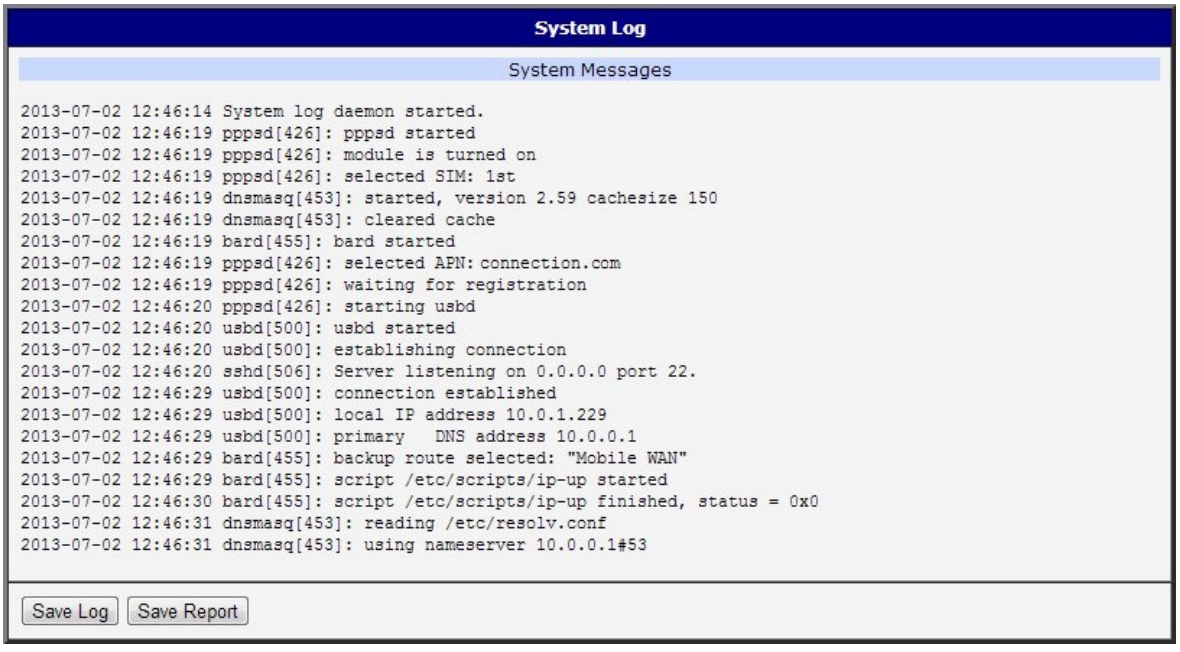


Figure 9: System Log

The following example (figure) shows how to send syslog information to a remote server at 192.168.2.115 on startup.

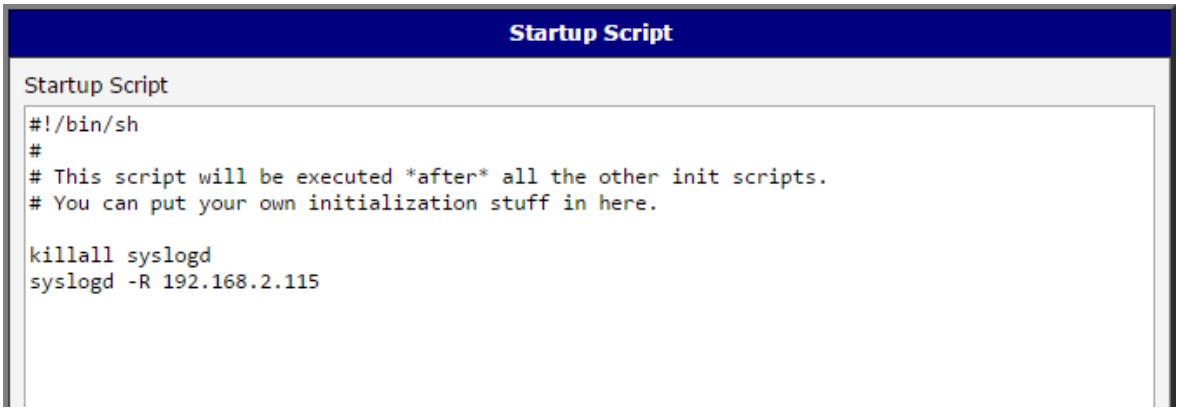


Figure 10: Example program syslogd start with the parameter -R

4 Configuration

4.1 LAN Configuration

To enter the Local Area Network configuration, select the *LAN* menu item in the *Configuration* section. The *LAN* item will expand in the menu on the left, so you can choose the proper Ethernet interface to configure: *Primary LAN* for the router's first Ethernet interface (ETH0), *Secondary LAN* for the router's second Ethernet interface (ETH1).

LAN Configuration page is divided into IPv4 and IPv6 columns, see Figure 11. There is dual stack support of IPv4 and IPv6 protocols – they can run alongside, you can configure either one of them or both. If you configure both IPv4 and IPv6, other network devices will choose the communication protocol. Configuration items and IPv6 to IPv4 differences are described in the tables below.

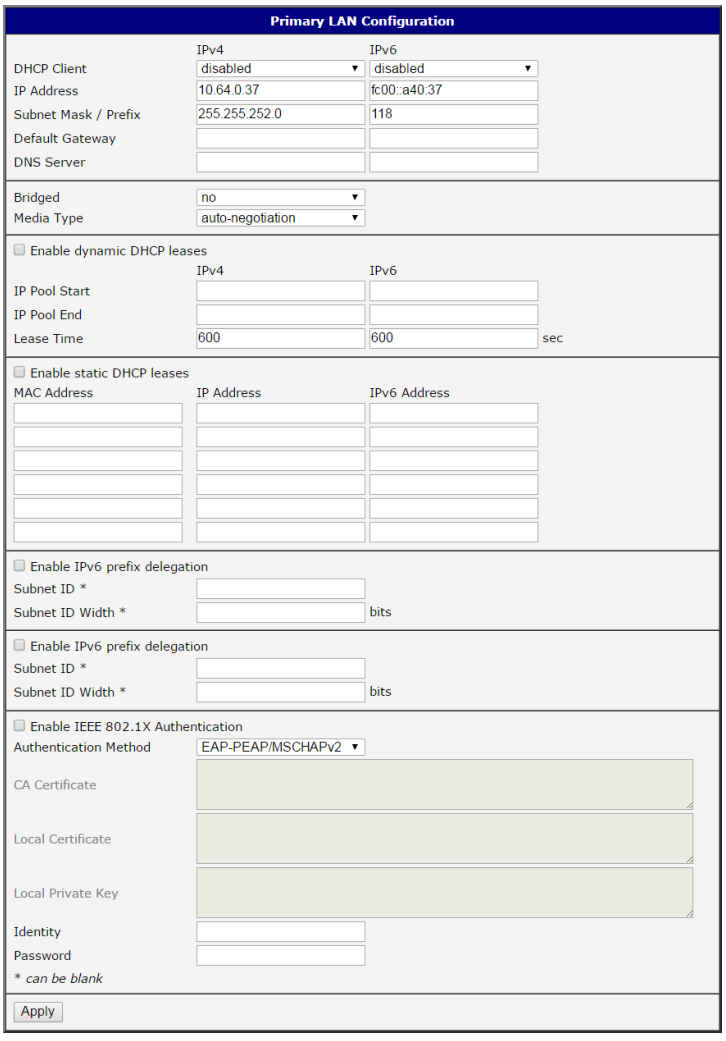


Figure 11: LAN Configuration page

Item	Description
DHCP Client	Enables/disables the DHCP client function. If in IPv6 column, the DHCPv6 client is enabled. DHCPv6 client supports all three methods of getting an IPv6 address – SLAAC, stateless DHCPv6 and statefull DHCPv6. • **disabled** – The router does not allow automatic allocation of an IP address from a DHCP server in LAN network. • **enabled** – The router allows automatic allocation of an IP address from a DHCP server in LAN network.
IP Address	A fixed IP address of the Ethernet interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent to this IP address. Use proper IP address notation in IPv4 and IPv6 column.
DNS Server	Specifies the IP address of the DNS server. When the IP address is not found in the Routing Table, the router forwards the request to DNS server specified here. Use proper IP address notation in IPv4 and IPv6 column.

Table 14: Configuration of the Network Interface – IPv4 and IPv6

The *Default Gateway* and *DNS Server* items are only used if the *DHCP Client* item is set to *disabled* and if the Primary or Secondary LAN is selected by the Backup Routes system as the default route. (The selection algorithm is described in section 4.6). Since FW 5.3.0, *Default Gateway* and *DNS Server* are also supported on bridged interfaces.

The following items (in the table below) are global for the configured Ethernet interface. Only one bridge can be active on the router at a time. The *DHCP Client*, *IP Address* and *Subnet Mask / Prefix* parameters of the only one of the interfaces are used to for the bridge. Primary LAN has higher priority when other interfaces (wlan0) are added to the bridge. Other interfaces (wlan0 – wifi) can be added to or deleted from an existing bridge at any time. The bridge can be created on demand for such interfaces, but not if it is configured by their respective parameters.

Item	Description
Bridged	Activates/deactivates the bridging function on the router. • **no** – The bridging function is inactive (default). • **yes** – The bridging function is active.
Media Type	Specifies the type of duplex and speed used in the network. • **Auto-negation** – The router automatically sets the best speed and duplex mode of communication according to the network's possibilities. • **100 Mbps Full Duplex** – The router communicates at 100 Mbps, in the full duplex mode. • **100 Mbps Half Duplex** – The router communicates at 100 Mbps, in the half duplex mode. • **10 Mbps Full Duplex** – The router communicates at 10 Mbps, in the full duplex mode. • **10 Mbps Half Duplex** – The router communicates at 10 Mbps, in the half duplex mode.

Table 15: Configuration of the Network Interface – global items

4.1.1 DHCP Server

The DHCP server assigns the IP address, gateway IP address (IP address of the router) and IP address of the DNS server (IP address of the router) to the connected clients. If these values are filled in by the user in the configuration form, they will be preferred.

The DHCP server supports static and dynamic assignment of IP addresses. *Dynamic DHCP* assigns clients IP addresses from a defined address space. *Static DHCP* assigns IP addresses that correspond to the MAC addresses of connected clients.

If IPv6 column is filled in, the DHCPv6 server is used. DHCPv6 server offers stateful address configuration to connected clients. Only when the *Subnet Prefix* above is set to 64, the DHCPv6 server offers both – the stateful address configuration and SLAAC (Stateless Address Autoconfiguration).

Do not to overlap ranges of static allocated IP addresses with addresses allocated by the dynamic DHCP server. IP address conflicts and incorrect network function can occur if you overlap the ranges.

4.1.2 IPv6 Prefix Delegation

This is an advanced configuration option. IPv6 prefix delegation works automatically with DHCPv6 – use only if different configuration is desired and if you know the consequences.

Item	Description
Enable dynamic DHCP leases	Select this option to enable a dynamic DHCP server.
IP Pool Start	Starting IP addresses allocated to the DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of IP addresses allocated to the DHCP clients. Use proper IP address notation in IPv4 and IPv6 column.
Lease time	Time in seconds that the IP address is reserved before it can be re-used.

Table 16: Configuration of Dynamic DHCP Server

Item	Description
Enable static DHCP leases	Select this option to enable a static DHCP server.
MAC Address	MAC address of a DHCP client.
IPv4 Address	Assigned IPv4 address. Use proper notation.
IPv6 Address	Assigned IPv6 address. Use proper notation.

Table 17: Configuration of Static DHCP Server

If you want to override the automatic IPv6 prefix delegation, you can configure it in this form. You have to know your Subnet ID Width (part of IPv6 address), see Figure below for the calculation help – it is an example: 48 bits is Site Prefix, 16 bits is Subnet ID (*Subnet ID Width*) and 64 bits is Interface ID.

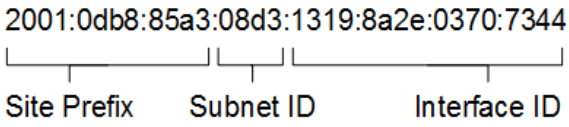


Figure 12: IPv6 Address with Prefix Example

Item	Description
Enable IPv6 prefix delegation	Enables prefix delegation configuration filled-in below.
Subnet ID	The decimal value of the Subnet ID of the Ethernet interface. Maximum value depends on the *Subnet ID Width*.
Subnet ID Width	The maximum *Subnet ID Width* depends on your Site Prefix – it is the remainder to 64 bits.

Table 18: IPv6 prefix delegation configuration

4.1.3 802.1X Authentication to RADIUS Server

Authentication (802.1X) to RADIUS server can be enabled in next configuration section. The router can be RADIUS client only (not the server). This functionality requires additional setting of identity and certificates as described in the following table.

Item	Description
Enable IEEE 802.1X Authentication	Select this option to enable 802.1X Authentication.
Authentication Method	Select authentication method (EAP-PEAPMSCHAPv2 or EAP-TLS).
CA Certificate	Definition of CA certificate for EAP-TLS authentication protocol.
Local Certificate	Definition of local certificate for EAP-TLS authentication protocol.
Local Private Key	Definition of local private key for EAP-TLS authentication protocol.
Identity	User name – identity.
Password	Access password. This item is available for EAP-PEAPMSCHAPv2 protocol only. Enter valid characters only, see chap. 1.4.1!
Local Private Key Password	Definition of password for private key of EAP-TLS protocol. This item is available for EAP-TLS protocol only. Enter valid characters only, see chap. 1.4.1!

Table 19: Configuration of 802.1X Authentication

4.1.4 LAN Configuration Examples

Example 1: IPv4 Dynamic DHCP Server, Default Gateway and DNS Server

- The range of dynamic allocated IPv4 addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 second (10 minutes).
- Default gateway IP address is 192.168.1.20
- DNS server IP address is 192.168.1.20

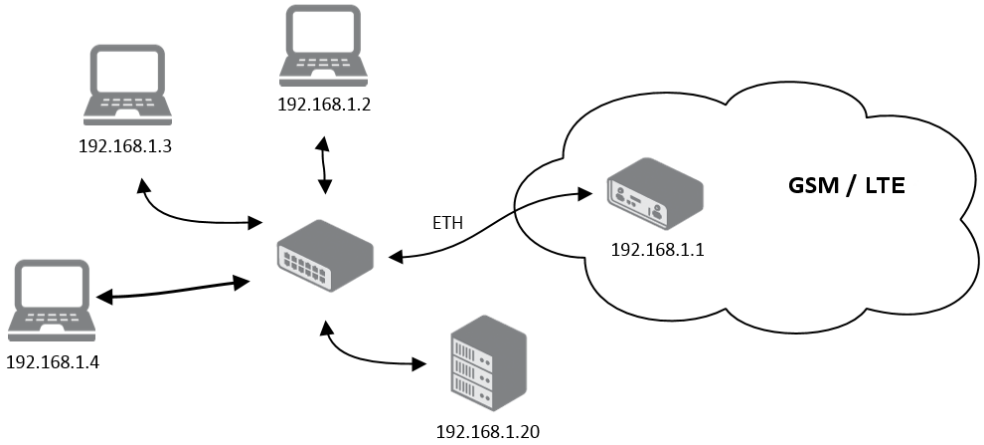


Figure 13: Network Topology for Example 1

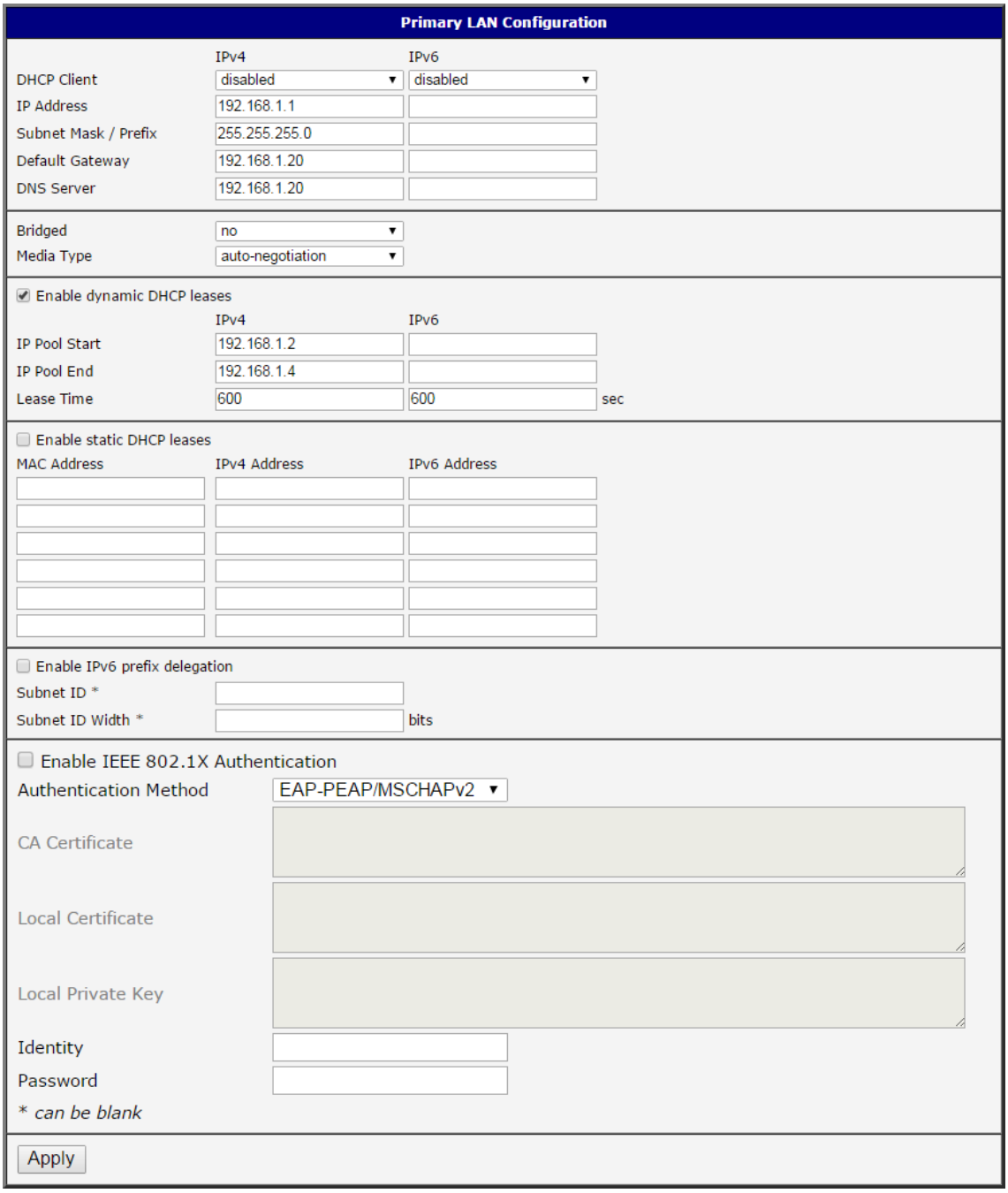


Figure 14: LAN Configuration for Example 1

Example 2: IPv4 Dynamic and Static DHCP server

- The range of allocated addresses is from 192.168.1.2 to 192.168.1.4.
- The address is allocated for 600 seconds (10 minutes).
- The client with the MAC address 01:23:45:67:89:ab has the IP address 192.168.1.10.
- The client with the MAC address 01:54:68:18:ba:7e has the IP address 192.168.1.11.

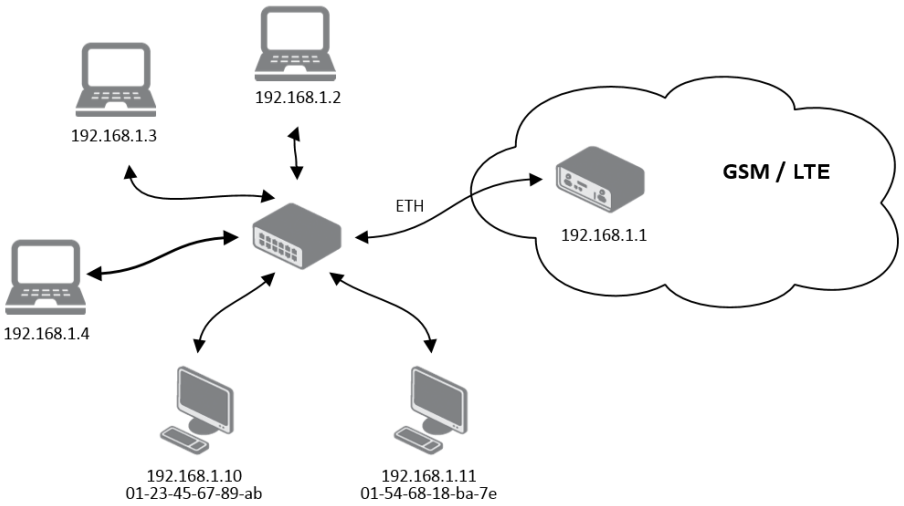


Figure 15: Network Topology for Example 2

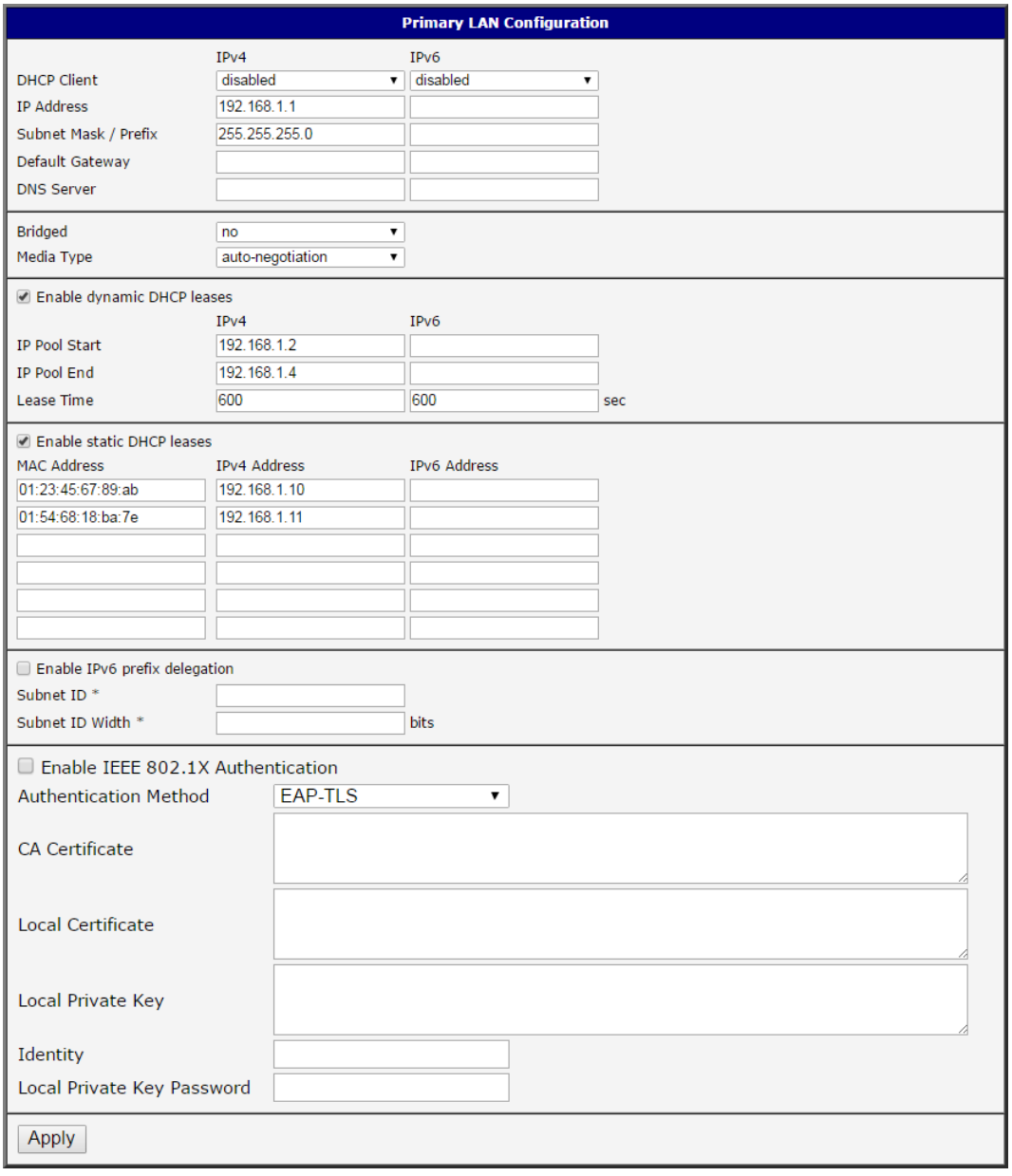


Figure 16: LAN Configuration for Example 2

Example 3: IPv6 Dynamic DHCP Server

- The range of dynamic allocated IPv6 addresses is from 2001:db8::1 to 2001:db8::ffff.
- The address is allocated for 600 second (10 minutes).
- The router is still accessible via IPv4 (192.168.1.1).

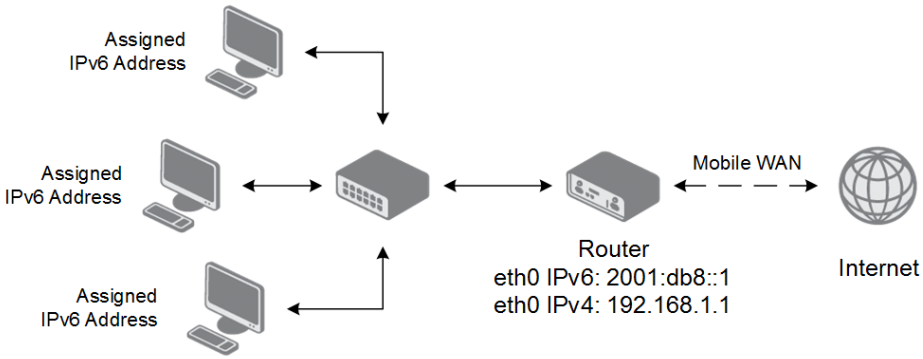


Figure 17: Network Topology for Example 3

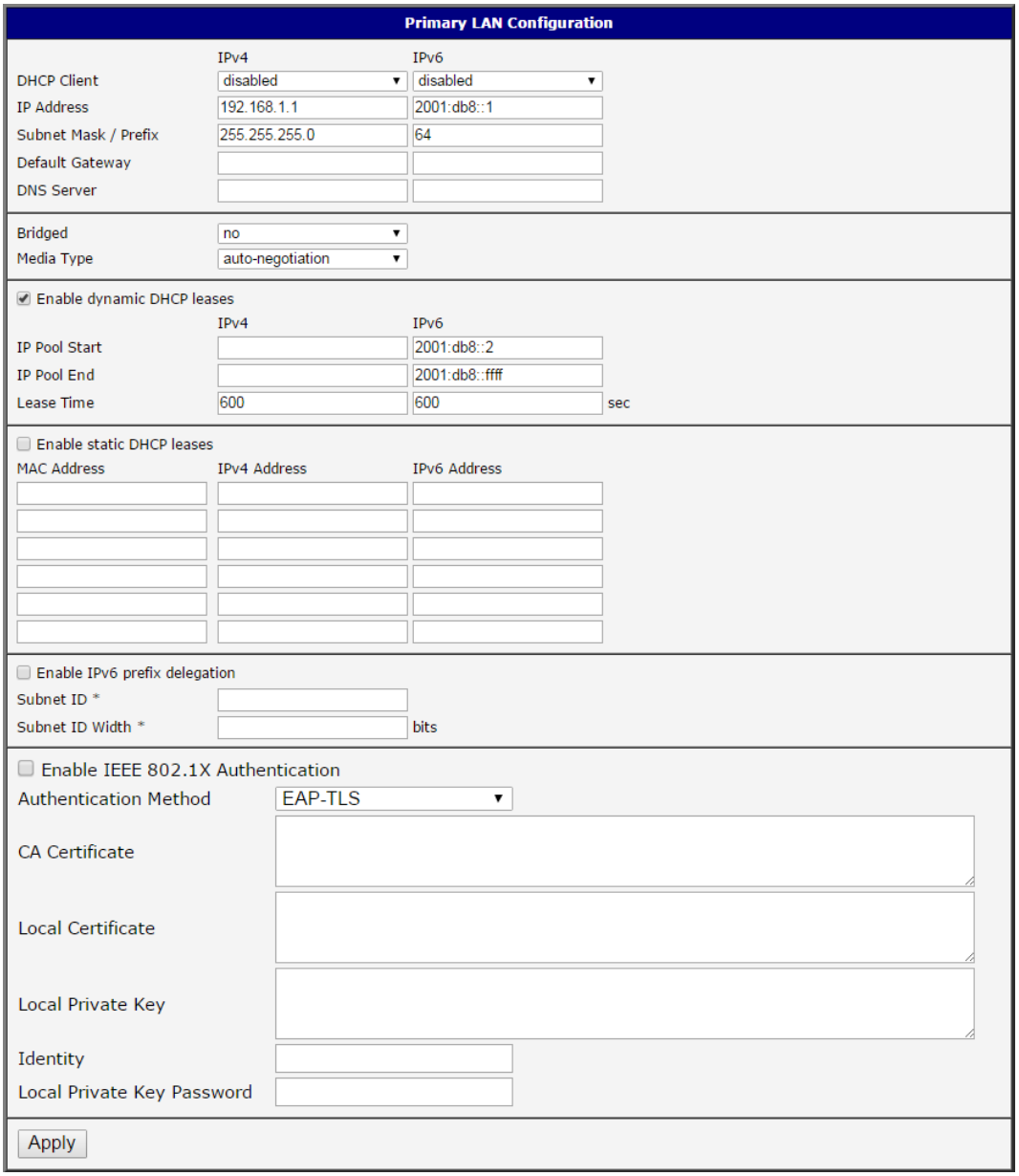


Figure 18: LAN Configuration for Example 3

4.2 VRRP Configuration

VRRP via IPv6 (VRRPv3) is not supported.

Select the *VRRP* menu item to enter the VRRP configuration. VRRP protocol (Virtual Router Redundancy Protocol) allows you to transfer packet routing from the main router to a backup router in case the main router fails. (This can be used to provide a wireless cellular backup to a primary wired router in critical applications.) If the *Enable VRRP* is checked, you may set the following parameters.

Item	Description
Virtual Server IP Address	This parameter sets the virtual server IP address. This address must be the same for both the primary and backup routers. Devices on the LAN will use this address as their default gateway IP address.
Virtual Server ID	This parameter distinguishes one virtual router on the network from another. The main and backup routers must use the same value for this parameter.
Host Priority	The active router with highest priority set by the parameter Host Priority, is the main router. According to RFC 2338, the main router should have the highest possible priority – 255. The backup router(s) have a priority in the range 1 – 254 (default value is 100). A priority value of 0 is not allowed.

Table 20: VRRP configuration

You may set the *Check connection* flag in the second part of the window to enable automatic test messages for the cellular network. In some cases, the mobile WAN connection could still be active but the router will not be able to send data over the cellular network. This feature is used to verify that data can be sent over the PPP connection and supplements the normal VRRP message handling. The currently active router (main/backup) will send test messages to the defined *Ping IP Address* at periodic time intervals (*Ping Interval*) and wait for a reply (*Ping Timeout*). If the router does not receive a response to the Ping command, it will retry up to the number of times specified by the *Ping Probes* parameter. After that time, it will switch itself to a backup router until the PPP connection is restored.

Item	Description
Ping IP Address	Destinations IP address for the Ping commands. IP Address can not be specified as a domain name.
Ping Interval	Interval in seconds between the outgoing Pings.
Ping Timeout	Time in seconds to wait for a response to the Ping.
Ping Probes	Maximum number of failed ping requests.

Table 21: Check connection

You may use the DNS server of the mobile carrier as the destination IP address for the test messages (Pings).

The *Enable traffic monitoring* option can be used to reduce the number of messages that are sent to test the PPP connection. When this parameter is set, the router will monitor the

interface for any packets different from a ping. If a response to the packet is received within the timeout specified by the *Ping Timeout* parameter, then the router knows that the connection is still active. If the router does not receive a response within the timeout period, it will attempt to test the mobile WAN connection using standard Ping commands.

Example of the VRRP protocol:

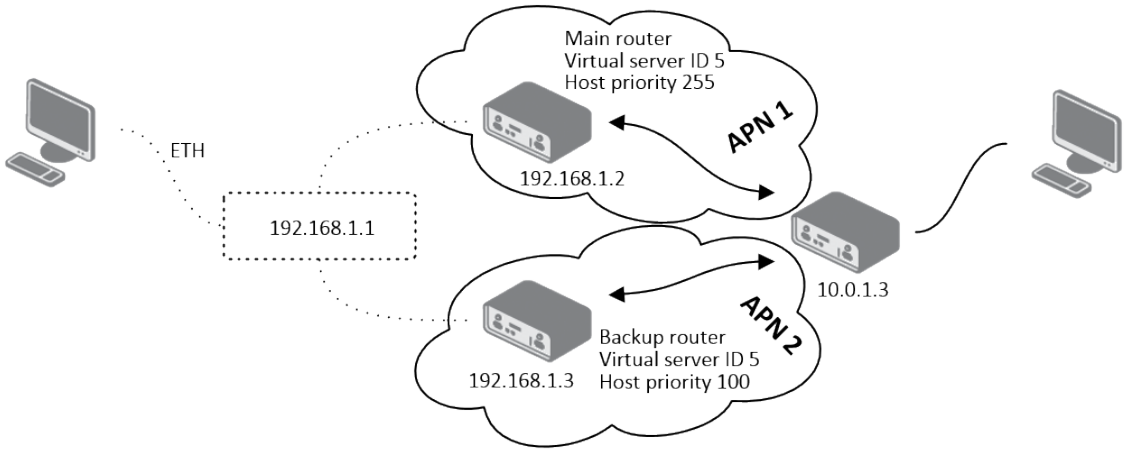


Figure 19: Topology of VRRP configuration example

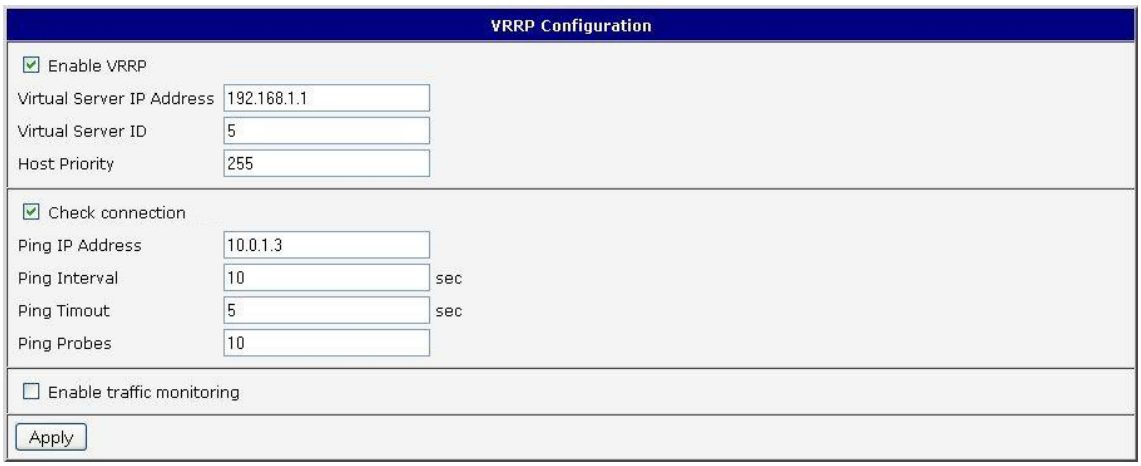


Figure 20: Example of VRRP configuration – main router

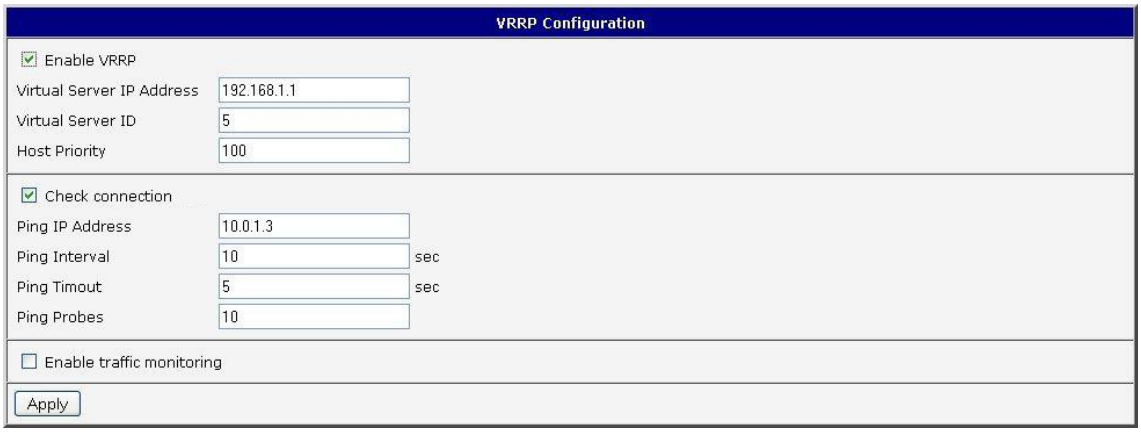


Figure 21: Example of VRRP configuration – backup router

Select the *Mobile WAN* item in the *Configuration* menu section to enter the cellular network configuration page. See *Mobile WAN Configuration* page in Figure 23.

4.2.1 Connection to Mobile Network

If the *Create connection to mobile network* checkbox is checked, then the router will automatically attempt to establish a connection after booting up. You can specify the following parameters for each SIM card separately.

Item	Description
Carrier	**Available For NAM routers only**. Network carrier selection. Provides either *automatic detection* option, or manual selection of *AT&T*, *Rogers* or *Verizon*.
APN	Network identifier (Access Point Name).
Username	The user name used for logging on to the GSM network.
Password	The password used for logging on to the GSM network. Enter valid characters only, see chap. 1.4.1!
Authentication	Authentication protocol used in the GSM network: • **PAP or CHAP** – The router selects the authentication method. • **PAP** – The router uses the PAP authentication method. • **CHAP** – The router uses the CHAP authentication method.
IP Mode	Specifies the version of IP protocol used: • **IPv4** – IPv4 protocol is used only (default). • **IPv6** – IPv6 protocol is used only. • **IPv4/IPv6** – IPv4 and IPv6 independent dual stack is enabled.
IP Address	For use in IPv4 and IPv4/IPv6 mode only. Specifies the IPv4 address of the SIM card. You manually enter the IP address only when mobile network carrier has assigned the IP address.
Dial Number	Specifies the telephone number which the router dials for a GPRS or CSD connection. The router uses the default telephone number *99***1 #.
Operator	Specifies the carrier code. You can specify this parameter as the PLNM preferred carrier code.
Network type	Specifies the type of protocol used in the mobile network. • **Automatic selection** – The router automatically selects a transmission method according to the availability of transmission technologies. • It is also possible to select one of the following specific methods of data transmission: **LTE**, **UMTS/HSPA**, **GPRS/EDGE**.
PIN	Specifies the PIN used to unlock the SIM card. Use only if this is required by a given SIM card. The SIM card will be blocked after several failed attempts to enter the PIN.

Continued on next page

Continued from previous page

Item	Description
MRU	Maximum Receive Unit – maximum size of packet that the router can receive via Mobile WAN. The default value is 1500 B. Other settings may cause the router to receive data incorrectly. Minimal value in IPv4 and IPv4/IPv6 mode: 128 B. Minimal value in IPv6 mode: 1280 B.
MTU	Maximum Transmission Unit – maximum size of packet that the router can transmit via Mobile WAN. The default value is 1500 B. Other settings may cause the router to transmit data incorrectly. Minimal value in IPv4 and IPv4/IPv6 mode: 128 B. Minimal value in IPv6 mode: 1280 B.

Table 22: Mobile WAN Connection Configuration

The following list contains tips for working with the *Mobile WAN* configuration form:

- If the MTU size is set incorrectly, then the router will not exceed the data transfer. If the MTU value is set too low, more frequent fragmentation of data will occur. More frequent fragmentation will mean a higher overhead and also the possibility of packet damage during defragmentation. In contrast, a higher MTU value can cause the network to drop the packet.
- If the *IP address* field is left blank, when the router establishes a connection, the mobile network carrier will automatically assign an IP address. If you assign an IP address manually, then the router will access the network quicker.
- If the ***APN*** field is left blank, then the router automatically selects the APN using the IMSI code of the SIM card. If the PLMN (operator number format) is not in the APN list, then the router uses the default APN "**internet**". If AT&T carrier network is detected, "**phone**" is used as default APN. The mobile network carrier defines the APN.
- If you enter the word `blank` in the *APN* field, then the router interprets the APN as blank.

The correct PIN must be filled in. An incorrect PIN may block the SIM card.

Parameters identified with an asterisk require you to enter the appropriate information only if this information is required by the mobile network carrier.

When the router is unsuccessful in establishing a connection to mobile network, you should verify accuracy of the entered data. Alternatively, you could try a different authentication method or network type.

4.2.2 DNS Address Configuration

The *DNS Settings* parameter is designed for easier configuration on the client's side. When this value is set to *get from operator* the router will attempt to automatically obtain an IP address from the primary and secondary DNS server of the mobile network carrier. To specify the IP addresses of the Primary DNS servers manually, on the *DNS Server* pull down list select the value *set manually*. You can also fill-in the IPv4 or IPv6 address of the DNS server (or both) based on the IP Mode option.

4.2.3 Check Connection to Mobile Network Configuration

Enabling the *Check Connection* function for mobile networks is necessary for uninterrupted and continuous operation of the router.

If the *Check Connection* item is set to *enabled* or *enabled + bind*, this activates checking of the connection to the mobile network. The router will automatically send ping requests to the specified domain or IP address (*Ping IP Address* or *Ping IPv6 Address* item) at regular time intervals (*Ping Interval*). In the case of an unsuccessful ping, a new one will be sent after ten seconds. If this ping a given IP address three times in a row, the router will terminate the connection and attempt to establish new ones. This checking can be set separate for two SIM cards. Send an ICMP (ICMPv6) ping to an IP address that you know is still functional. (The operator's DNS server, for example.)

If the *Check Connection* item is set to the *enabled* option, ping requests are sent on the basis of the routing table. Therefore, the requests may be sent through any available interface. If you require each ping request to be sent through the network interface, which was created when establishing a connection to the mobile operator, it is necessary to set the *Check Connection* item to *enabled + bind*. The *disabled* option deactivates checking of the connection to the mobile network.

For routers connected to **Verizon** carrier (autodetected by the router): The retry interval for connecting to the mobile network prolongs with more retries. First two retries are done after 1 minute. Then the interval prolongs to 2, 8 and 15 minutes. The ninth and every other retry is done in 90 minutes interval.

If *Enable Traffic Monitoring* item is checked, the router will stop sending ping requests to *Ping IP Address* (*Ping IPv6 Address*) and it will watch the Mobile WAN connection. When there is no traffic during period longer than *Ping Interval*, the router will send ping request to *Ping IP Address* (*Ping IPv6 Address*).

Item	Description
Ping IP Address	Specifies the ping queries destination IPv4 address or domain name. Available in IPv4 and IPv4/IPv6 *IP Mode*.
Ping IPv6 Address	Specifies the ping queries destination IPv6 address or domain name. Available in IPv6 and IPv4/IPv6 *IP Mode*.
Ping Interval	Specifies the time interval between outgoing pings.
Ping Timeout	Time in seconds to wait for a Ping response.

Table 23: Check Connection to Mobile Network Configuration

4.2.4 Example of Check Connection Configuration

The figure below displays the following scenario: the connection to the mobile network in IPv4 *IP Mode* is controlled on the address 8.8.8.8 with a time interval of 60 seconds for the first SIM card and on the address www.google.com with the time interval 80 seconds for the second SIM card. In the case of an active data stream on the router, the control pings are not sent, but the data stream is monitored.

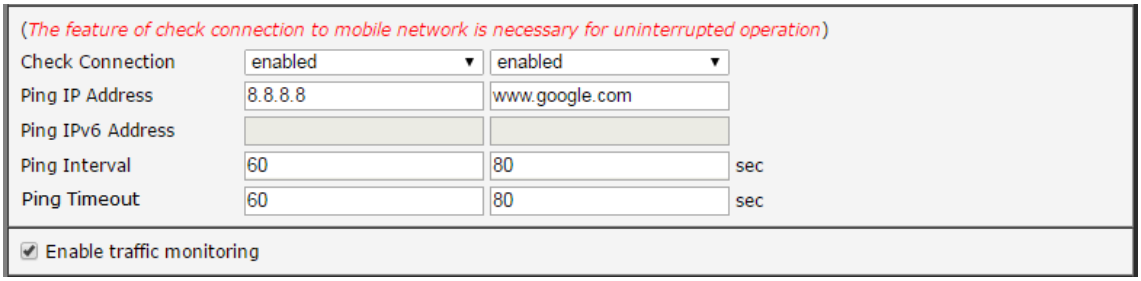


Figure 22: Example of Check Connection Configuration

Item	Description
Data Limit	Specifies the maximum expected amount of data transmitted (sent and received) over GPRS in one billing period (one month). Maximum value is 2 TB (2097152 MB).
Warning Threshold	Specifies a percentage of the "Data Limit" in the range of 50 % to 99 %. If the given percentage data limit is exceeded, the router will send an SMS in the following form; *Router has exceeded (value of Warning Threshold) of data limit.*
Accounting Start	Specifies the day of the month in which the billing cycle starts for a given SIM card. When the service provider that issued the SIM card specifies the start of the billing period, the router will begin to count the amount of data transferred starting on this day.

Table 24: Data Limit Configuration

4.2.5 Data Limit Configuration

If the parameter *Data Limit State* (see below) is set to *not applicable* or *Send SMS when data limit is exceeded* in *SMS Configuration* is not selected, the *Data Limit* set here will be ignored.

4.2.6 Switch between SIM Cards Configuration

In the lower part of the configuration form you can specify the rules for toggling between the two SIM cards.

The router will automatically toggle between the SIM cards and their individual setups depending on the configuration settings specified here (manual permission, roaming, data limit, binary input state). Note that the SIM card selected for connection establishment is the result of the logical product (AND) of the configuration here (table below).

Item	Description
SIM Card	Enable or disable the use of a SIM card. If you set all the SIM cards to *disabled*, this means that the entire cellular module is disabled. • **enabled** – It is possible to use the SIM card. • **disabled** – Never use the SIM card, the usage of this SIM is forbidden.

Continued on next page

Continued from previous page

Item	Description
Roaming State	Configure the use of SIM cards based on roaming. This roaming feature has to be activated for the SIM card on which it is enabled! • **not applicable** – It is possible to use the SIM card everywhere. • **home network only** – Only use the SIM card if roaming is not detected.
Data Limit State	Configure the use of SIM cards based on the Data Limit set above: • **not applicable** – It is possible to use the SIM regardless of the limit. • **not exceeded** – Use the SIM card only if the Data Limit (set above) has not been exceeded.
BIN0 State	Configure the use of SIM cards based on binary input 0 state: • **not applicable** – It is possible to use the SIM regardless of BIN0 state. • **on** – Only use the SIM card if the BIN0 state is logical 0 – voltage present. • **off** – Only use the SIM card if the BIN0 state is logical 1 – no voltage.

Table 25: Switch between SIM cards configuration

Use the following parameters to specify the decision making of SIM card switching in the cellular module.

Item	Description
Default SIM Card	Specifies the modules' default SIM card. The router will attempt to establish a connection to mobile network using this default. • **1st** – The 1st SIM card is the default one. • **2nd** – The 2nd SIM card is the default one.
Initial State	Specifies the action of the cellular module after the SIM card has been selected. • **online** – establish connection to the mobile network after the SIM card has been selected (default). • **offline** – go to the off-line mode after the SIM card has been selected. Note: If offline, you can change this initial state by SMS message only – see *SMS Configuration*. The cellular module will also go into off-line mode if none of the SIM cards are not selected.

Continued on next page

Continued from previous page

Item	Description
Switch to other SIM card when connection fails	Applicable only when connection is established on the default SIM card and then fails. If the connection failure is detected by *Check Connection* feature above, the router will switch to the backup SIM card.
Switch to default SIM card after timeout	If enabled, after timeout, the router will attempt to switch back to the default SIM card. This applies only when there is default SIM card defined and the backup SIM is selected beacuse of a **failure** of the default one or if **roaming** settings cause the switch. This feature is available only when *Switch to other SIM card when connection fails* is enabled.
Initial Timeout	Specifies the length of time that the router waits before the first attempt to revert to the default SIM card, the range of this parameter is from 1 to 10000 minutes.
Subsequent Timeout	Specifies the length of time that the router waits after an unsuccessful attempt to revert to the default SIM card, the range is from 1 to 10000 min.
Additive Constant	Specifies the length of time that the router waits for any further attempts to revert to the default SIM card. This length time is the sum of the time specified in the "Subsequent Timeout" parameter and the time specified in this parameter. The range in this parameter is from 1 to 10000 minutes.

Table 26: Parameters for SIM card switching

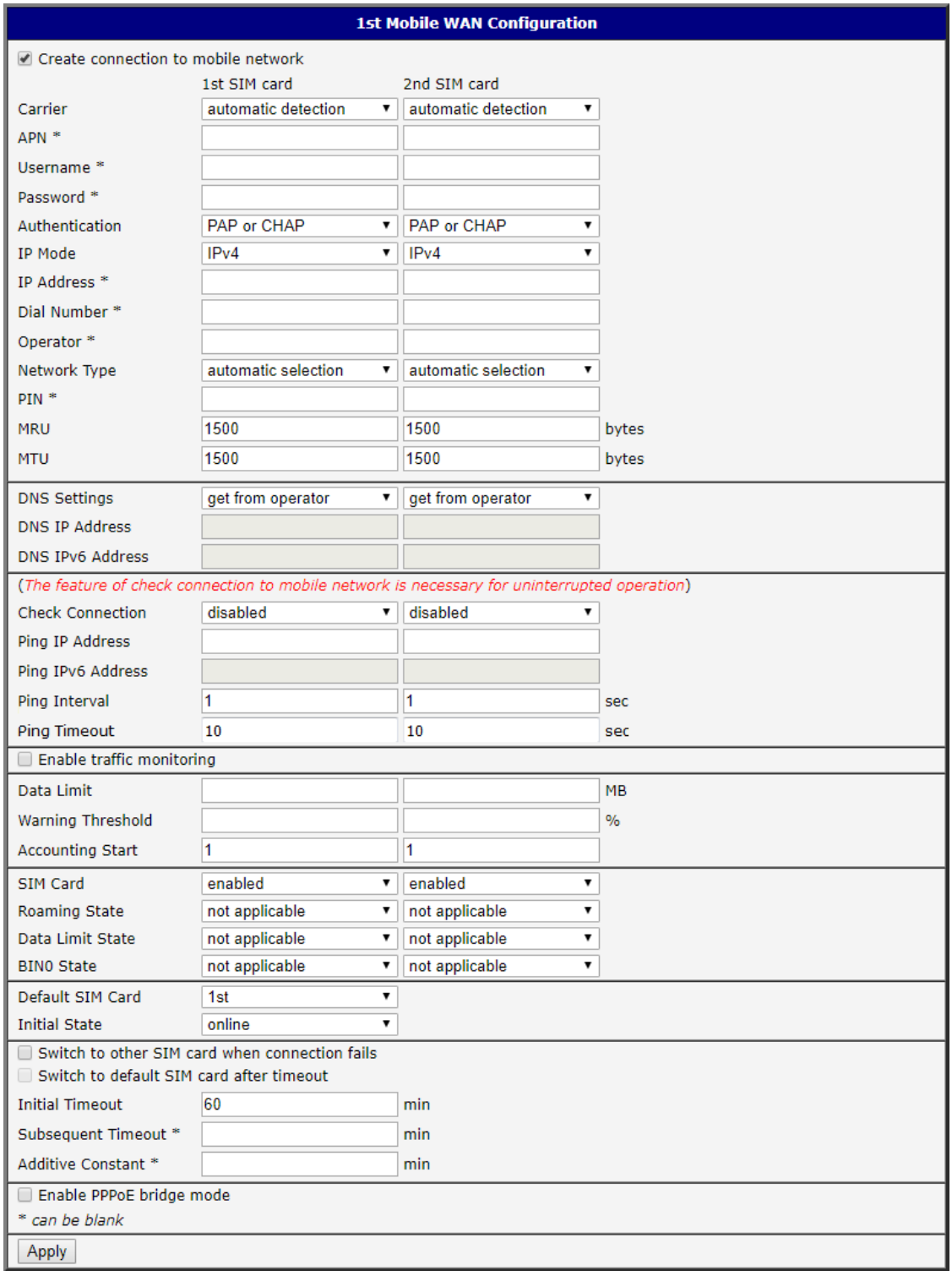


Figure 23: Mobile WAN Configuration

4.2.7 Examples of SIM Card Switching Configuration

Example 1: Timeout Configuration

Mark the *Switch to default SIM card after timeout* check box, and fill-in the following values:

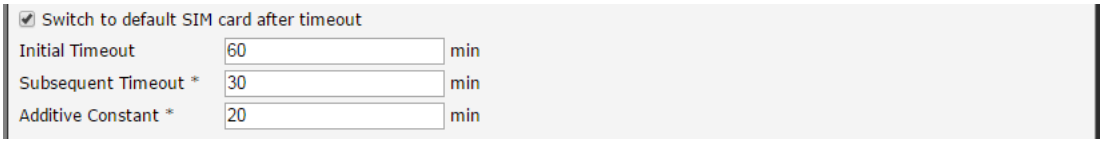


Figure 24: Configuration for SIM card switching Example 1

The first attempt to change to the default SIM card is carried out after 60 minutes. When the first attempt fails, a second attempt is made after 30 minutes. A third attempt is made after 50 minutes (30+20). A fourth attempt is made after 70 minutes (30+20+20).

Example 2: Data Limit Switching

The following configuration illustrates a scenario in which the router changes to the second SIM card after exceeding the data limit of 800 MB on the first (default) SIM card. The router sends a SMS upon reaching 400 MB (this settings has to be enabled on the *SMS Configuration* page). The accounting period starts on the 18th day of the month.

Figure 25: Configuration for SIM card switching Example 2

4.2.8 PPPoE Bridge Mode Configuration

If you mark the *Enable PPPoE bridge mode* check box, the router activates the PPPoE bridge protocol. PPPoE (point-to-point over ethernet) is a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames. The bridge mode allows you to create a PPPoE connection from a device behind the router. For example, a PC connected to the ETH port of the router. You assign the IP address of the SIM card to the PC. The changes in settings will apply after clicking the *Apply* button.

4.3 PPPoE Configuration

PPPoE (Point-to-Point over Ethernet) is a network protocol which encapsulates PPP frames into Ethernet frames. The router uses the PPPoE client to connect to devices supporting a PPPoE bridge or server. The bridge or server is typically an ADSL router.

To open the *PPPoE Configuration* page, select the *PPPoE* menu item. If you mark the *Create PPPoE connection* check box, then the router attempts to establish a PPPoE connection after boot up. After connecting, the router obtains the IP address of the device to which it is connected. The communications from a device behind the PPPoE server is forwarded to the router.

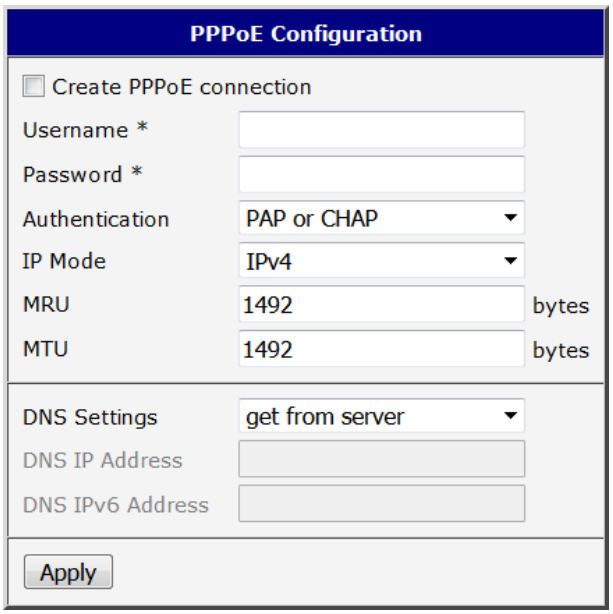


Figure 26: PPPoE Configuration

Item	Description
Username	Username for secure access to PPPoE.
Password	Password for secure access to PPPoE. Enter valid characters only, see chap. 1.4.1!
Authentication	Authentication protocol in GSM network. • **PAP or CHAP** – The router selects the authentication method. • **PAP** – The router uses the PAP authentication method. • **CHAP** – The router uses the CHAP authentication method.
IP Mode	Specifies the version of IP protocol: • **IPv4** – IPv4 protocol is used only (default). • **IPv6** – IPv6 protocol is used only. • **IPv4/IPv6** – IPv4 and IPv6 dual stack is enabled.

Continued on next page

Continued from previous page

Item	Description
MRU	Specifies the Maximum Receiving Unit. The MRU identifies the maximum packet size, that the router can receive via PPPoE. The default value is 1492 B (bytes). Other settings can cause incorrect data transmission. Minimal value in IPv4 and IPv4/IPv6 mode is 128 B. Minimal value in IPv6 mode is 1280 B.
MTU	Specifies the Maximum Transmission Unit. The MTU identifies the maximum packet size, that the router can transfer in a given environment. The default value is 1492 B (bytes). Other settings can cause incorrect data transmission. Minimal value in IPv4 and IPv4/IPv6 mode is 128 B. Minimal value in IPv6 mode is 1280 B.
DNS Settings	Can be set to obtain the DNS address from the server or to set it manually.
DNS IP Address	Manual setting of DNS address.
DNS IP Address	Manual setting of IPv6 DNS address.

Table 27: PPPoE configuration

Setting an incorrect packet size value (MRU, MTU) can cause unsuccessful transmission.

4.4 WiFi Configuration

Versions of OWL-4G routers with WiFi are in development. The configuration described bellow may change in the future.

This item is available only if the router is equipped with a WiFi module.

Configure the WiFi network by selecting the *WiFi* item in the main menu of the router web interface. Activate WiFi by selecting *Enable WiFi* at the top of the form. You may set the following properties listed in the table below.

RADIUS (Remote Authentication Dial-In User Service) networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users is supported on WiFi. The router can be RADIUS client only (not the server) – typically as a WiFi AP (Access Point) negotiating with the RADIUS server. In WiFi STA (Station) operating mode the authentication method EAP-PEAP/MSCHAPv2 (both PEAPv0 and PEAPv1) is supported only.

Item	Description
Operating mode	WiFi operating mode: • **access point (AP)** – The router becomes an access point to which other devices in *station (STA)* mode can connect. • **station (STA)** – The router becomes a client station. It receives data packets from the available access point (AP) and sends data from cable connection via the WiFi network.
SSID	The unique identifier of WiFi network.
Broadcast SSID	Method of broadcasting the unique identifier of SSID network in beacon frame and type of response to a request for sending the beacon frame. • **Enabled** – SSID is broadcasted in beacon frame • **Zero length** – Beacon frame does not include SSID. Requests for sending beacon frame are ignored. • **Clear** – All SSID characters in beacon frames are replaced by 0. Original length is kept. Requests for sending beacon frames are ignored.
Probe Hidden SSID	Probes hidden SSID (only for *station (STA)* mode)
Client Isolation	In *access point (AP)* mode only. If checked, the access point will isolate every connected client so they do not see each other (they are in different networks, they cannot PING between each other). If unchecked, the access point behavior is like a switch, but wireless – the clients are in the same LAN and can see each other.

Continued on next page

Continued from previous page

Item	Description
Country Code	**This option is not available for NAM routers** – the "US" country code is set by default on these versions of router. Code of the country where the router is installed. This code must be entered in ISO 3166-1 alpha-2 format. If a *country code* isn't specified and the router has not implemented a system to determine this code, it will use "US" as the default *country code*. If no *country code* is specified or if the wrong country code is entered, the router may violate country-specific regulations for the use of WiFi frequency bands.
HW Mode	HW mode of WiFi standard that will be supported by WiFi access point. • IEE 802.11b (2.4 GHz) • IEE 802.11b+g (2.4 GHz) • IEE 802.11b+g+n (2.4 GHz) • IEE 802.11a (5 GHz) • IEE 802.11a+n (5 GHz) • IEE 802.11a+c (5 GHz)
Channel	The channel, where the WiFi AP is transmitting. Supported 2.4 GHz channels: 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13. **On NAM routers only channels 1 to 11 are supported!** Supported 5 GHz channels: 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 149, 153, 157, 161, 165.
BW 40 MHz	**The option for HW mode 802.11n** which allows transmission on two standard 20 MHz channels simultaneously. The option is also available in the STA mode and it has to be enabled in both the AP and the STA mode if using the high throughput mode.
BW 80 MHz	**The option for HW mode 802.11c** which allows transmission on two 40 MHz channels simultaneously. The option is also available in the STA mode and it has to be enabled in both the AP and the STA mode if using the high throughput mode.
WMM	Basic QoS for WiFi networks is enabled by checking this item. This version doesn't guarantee network throughput. It is suitable for simple applications that require QoS.

Continued on next page

Continued from previous page

Item	Description
Authentication	Access control and authorization of users in the WiFi network. • **Open** – Authentication is not required (free access point). • **Shared** – Basic authentication using WEP key. • **WPA-PSK** – Authentication using higher authentication methods PSK-PSK. • **WPA2-PSK** – WPA-PSK using newer AES encryption. • **WPA-Enterprise** – RADIUS authentication done by external server via username and password. • **WPA2-Enterprise** – RADIUS authentication with better encryption. • **802.1X** – RADIUS authentication with port-based Network Access Control (PNAC) using encapsulation of the Extensible Authentication Protocol (EAP) over LAN – EAPOL.
Encryption	Type of data encryption in the WiFi network: • **None** – No data encryption. • **WEP** – Encryption using static WEP keys. This encryption can be used for *Shared* authentication. • **TKIP** – Dynamic encryption key management that can be used for *WPA-PSK* and *WPA2-PSK* authentication. • **AES** – Improved encryption used for *WPA2-PSK* authentication.
WEP Key Type	Type of WEP key for WEP encryption: • **ASCII** – WEP key in ASCII format. • **HEX** – WEP key in hexadecimal format.
WEP Default Key	This specifies the default WEP key.

Continued on next page

Continued from previous page

Item	Description
WEP Key 1–4	Allows entry of four different WEP keys: • WEP key in ASCII format must be entered in quotes. This key can be specified in the following lengths. – 5 ASCII characters (40b WEP key) – 13 ASCII characters (104b WEP key) – 16 ASCII characters (128b WEP key) • WEP key in hexadecimal format must be entered in hexadecimal digits. This key can be specified in the following lengths. – 10 hexadecimal digits (40b WEP key) – 26 hexadecimal digits (104b WEP key) – 32 hexadecimal digits (128b WEP key)
WPA PSK Type	The possible key options for WPA-PSK authentication. • 256-bit secret • ASCII passphrase • PSK File
WPA PSK	Key for WPA-PSK authentication. This key must be entered according to the selected WPA PSK type as follows: • **256-bit secret** – 64 hexadecimal digits • **ASCII passphrase** – 8 to 63 characters • **PSK File** – absolute path to the file containing the list of pairs (PSK key, MAC address)
RADIUS Auth Server IP	IPv4 or IPv6 address of the RADIUS server. In AP mode only and with one of RADIUS authentications selected.
RADIUS Auth Password	RADIUS server access password. In AP mode only and with one of RADIUS authentications selected. Enter valid characters only, see chap. 1.4.1!
RADIUS Auth Port	RADIUS server port. The default is 1812. In AP mode only and with one of RADIUS authentications selected.
RADIUS Acct Server IP	IPv4 or IPv6 address of the RADIUS accounting server. Define only if different from the authentication and authorization server. In AP mode only and with one of RADIUS authentications selected.
RADIUS Acct Password	Access password of RADIUS accounting server. Define only if different from the authentication and authorization server. In AP mode only and with one of RADIUS authentications selected. Enter valid characters only, see chap. 1.4.1!
RADIUS Acct Port	RADIUS accounting server port. The default is 1813. Define only if different from the authentication and authorization server. In AP mode only and with one of RADIUS authentications selected.

Continued on next page

Continued from previous page

Item	Description
RADIUS EAP Authentication	Type of authentication protocol (EAP-PEAP/MSCHAPv2 or EAP-TLS).
RADIUS CA Certificate	Definition of CA certificate for EAP-TLS authentication protocol.
RADIUS Local Certificate	Definition of local certificate for EAP-TLS authentication protocol.
RADIUS Local Private Key	Definition of local private key for EAP-TLS authentication protocol.
RADIUS Local Private Key Password	Definition of password for private key of EAP-TLS protocol. Available for EAP-TLS protocol only. Enter valid characters only, see chap. 1.4.1!
RADIUS Identity	RADIUS user name – identity. In STA mode only and with one of RADIUS authentications selected.
RADIUS Password	RADIUS access password. In STA mode only and with one of RADIUS authentications selected. Enter valid characters only, see chap. 1.4.1!
Access List	Mode of Access/Deny list. • **Disabled** – Access/Deny list is not used. • **Accept** – Clients in Accept/Deny list can access the network. • **Deny** – Clients in Access/Deny list cannot access the network.
Accept/Deny List	Accept or Denny list of client MAC addresses that set network access. Each MAC address is separated by new line.
Syslog Level	Logging level, when system writes to the system log. • **Verbose debugging** – The highest level of logging. • **Debugging** • **Informational** – Default level of logging. • **Notification** • **Warning** – The lowest level of system communication.
Extra options	Allows the user to define additional parameters.

Table 28: WiFi Configuration

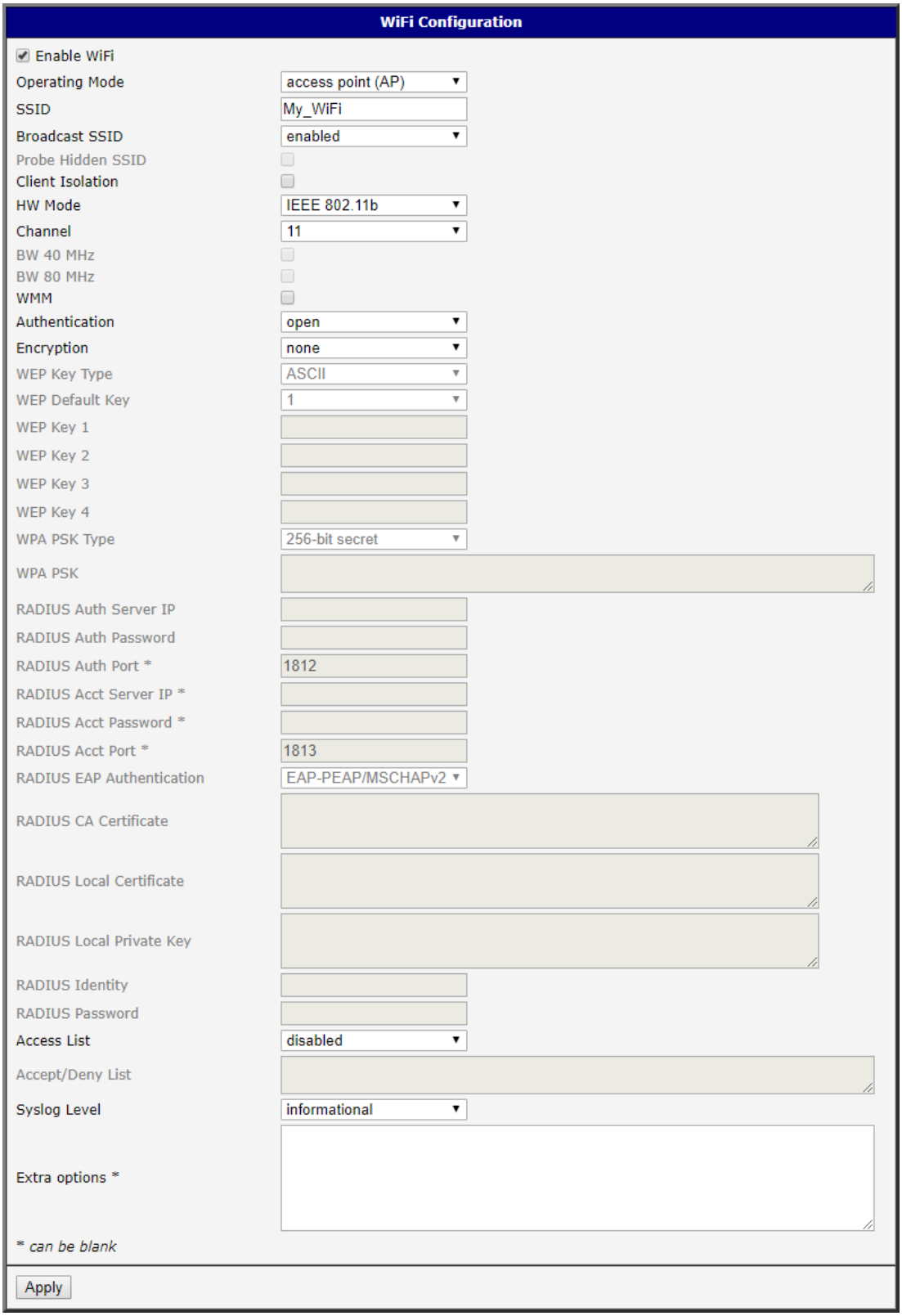


Figure 27: WiFi Configuration

4.5 WLAN Configuration

This item is available only if the router is equipped with a WiFi module.

The WiFi LAN and DHCP server page is displayed by selecting *WLAN* in the configuration section. You will then be able to set the following properties (see table below). Use the *Enable WLAN interface* check box at the top of this form to enable WiFi LAN interface.

WLAN Configuration page is divided into IPv4 and IPv6 columns. It is the independent dual stack configuration of IPv4 and IPv6 protocols – you can configure either one of them or both. Configuration items and IPv6 to IPv4 differences are described in the tables below.

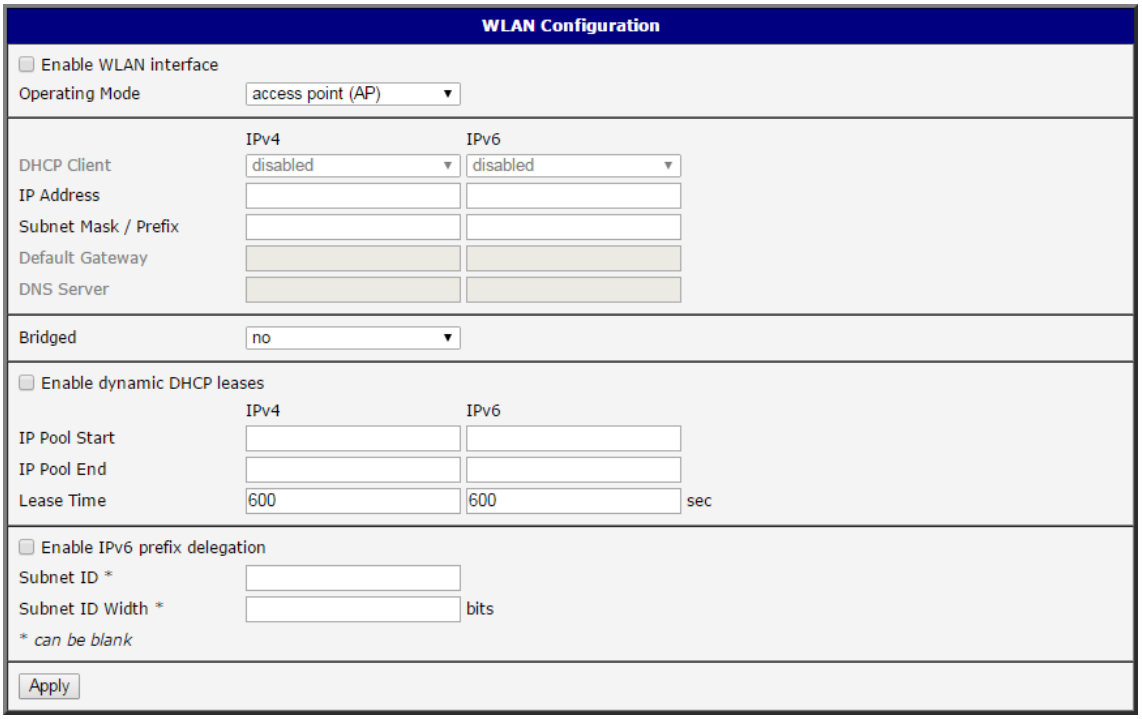


Figure 28: WLAN Configuration

Item	Description
Operating Mode	WiFi operating mode: • **access point (AP)** – The router becomes an access point to which other devices in *station (STA)* mode can be connected. • **station (STA)** – Router becomes a client station. It will receive data packets from the available access point (AP) and send data from cable connection via the WiFi network.
DHCP Client	Activates/deactivates DHCP client. If in IPv6 column, the DHCPv6 client is enabled.
IP Address	A fixed IP address of the WiFi interface. Use IPv4 notation in IPv4 column and IPv6 notation in IPv6 column. Shortened IPv6 notation is supported.
Subnet Mask / Prefix	Specifies a Subnet Mask for the IPv4 address. In the IPv6 column, fill in the Prefix for the IPv6 address – number in range 0 to 128.

Continued on next page

Continued from previous page

Item	Description
Default Gateway	Specifies the IP address of a default gateway. If filled-in, every packet with the destination not found in the routing table is sent there. Use proper IP address notation in IPv4 and IPv6 column.
DNS Server	Specifies the IP address of the DNS server. When the IP address is not found in the Routing Table, the this DNS server is requested. Use proper IP address notation in IPv4 and IPv6 column.
Bridged	Activates bridge mode: • **no** – Bridged mode is not allowed (default value). WLAN network is not connected with LAN network of the router. • **yes** – Bridged mode is allowed. WLAN network is connected with one or more LAN networks of the router. In this case, the setting of most items in this table are ignored. Instead, the router uses the settings of the selected network interface (LAN).

Table 29: WLAN Configuration

Use *Enable dynamic DHCP leases* item at the bottom of this form to enable dynamic allocation of IP addresses using the DHCP (DHCPv6) server. Items explained:

Item	Description
IP Pool Start	Beginning of the range of IP addresses which will be assigned to DHCP clients. Use proper notation in IPv4 and IPv6 column.
IP Pool End	End of the range of IP addresses which will be assigned to DHCP clients. Use proper notation in IPv4 and IPv6 column.
Lease Time	Time in seconds for which the client may use the IP address.

Table 30: Configuration of DHCP Server

See Chapter 4.1.2 for information on *IPv6 Prefix Delegation* configuration. It works automatically – it is an advanced configuration item you probably do not need to change.

All changes in settings will apply after pressing the *Apply* button.

4.6 Backup Routes

Using the configuration form on the *Backup Routes* page, you can back up the primary connection with alternative connections to the Internet (mobile network) or enable *Multiple WANs* mode. It is also possible to prioritize each backup connection option. Switching between connections is carried out according to order of priority and the state of the connections.

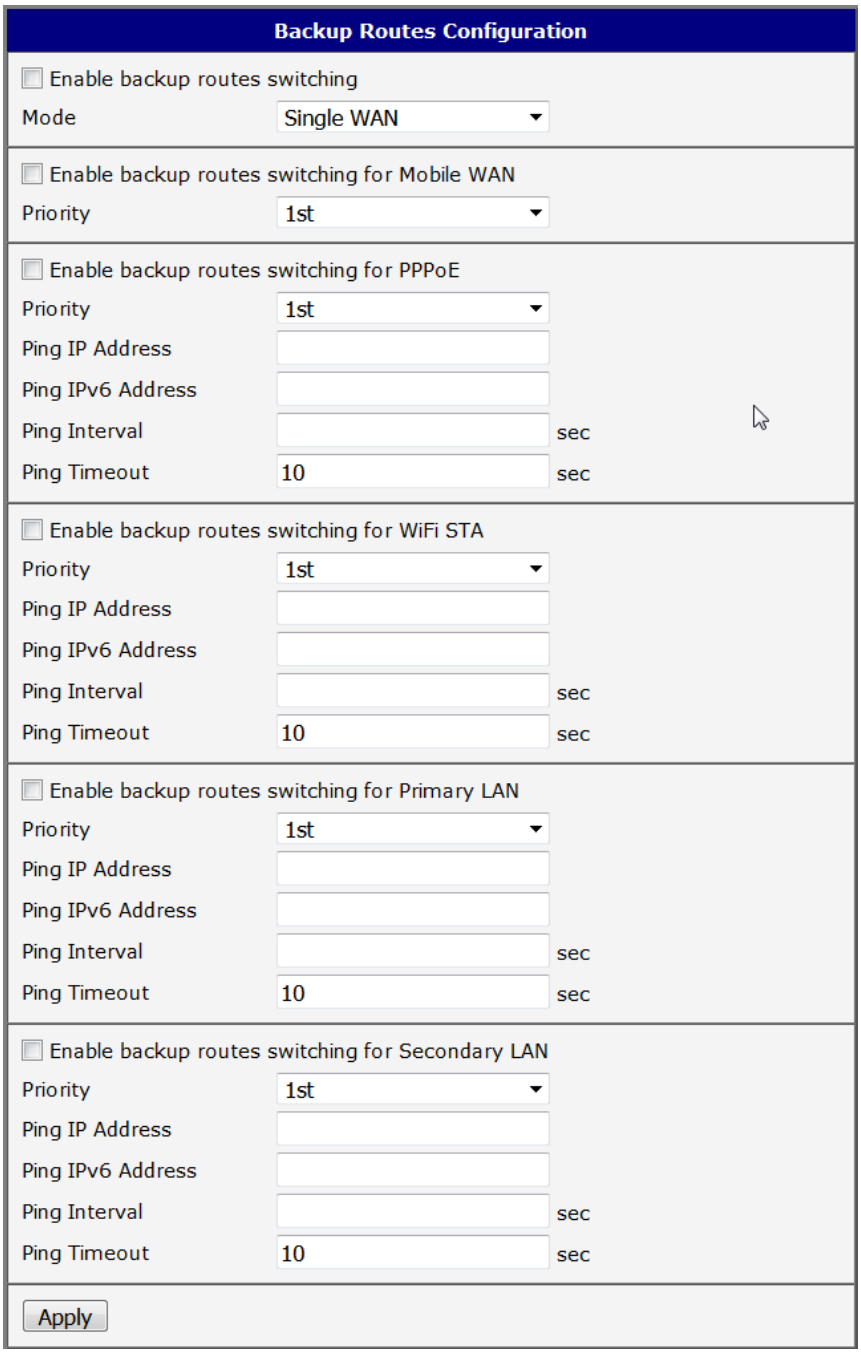


Figure 29: Backup Routes Configuration

Item	Description
Enable backup routes switching	The default route is selected according to the settings below. If disabled (unchecked), the backup routes system operates in the backward compatibility mode based on the default priorities of the network interfaces (listed below).
Mode	• **Single WAN** – The default mode. Only one interface is used for WAN communication at a time. Other interfaces are used for WAN when the preferred interface fails, based on the priorities set. • **Multiple WANs** – Multiple interfaces can be used for WAN connection. When WAN communication via multiple interfaces is received, the same interface is used in reply, therefor; the traffic will stay on the given interface. The set priorities are used when transmitting data from the router or from the network behind the router. The highest priority interface is used for these transmissions.

Table 31: Backup Routes Configuration

To add the network interfaces to the backup routes system, mark the checkbox(s) of the following interface options: *Enable backup routes switching for Mobile WAN*, *Enable backup routes switching for PPPoE*, *Enable backup routes switching for WiFi STA*, *Enable backup routes switching for Primary LAN* or *Enable backup routes switching for Secondary LAN*. Enabled interfaces are then used for WAN access either in *Single WAN* mode (only one interface at a time) or in *Multiple WANs* mode (multiple interfaces at a time), based on priorities set:

Item	Description
Priority	Priority for the type of connection (network interface).
Ping IP Address	Destination IPv4 address or domain name of ping queries to check the connection.
Ping IPv6 Address	Destination IPv6 address or domain name of ping queries to check the connection.
Ping Interval	The time interval between consecutive ping queries.
Ping Timeout	Time in seconds to wait for a response to the Ping.

Table 32: Backup Routes

If you want to use a mobile WAN connection as a backup route, you must choose the *enable + bind* option in the *Check Connection* item on the *Mobile WAN* page and fill in the ping address. See chapter 4.2.1.

Network interfaces belonging to individual backup routes are also checked before use for flags which indicate the state of the interface. (E.g. RUNNING on the *Network Status* page.) This prevents, for example, the disconnection of an Ethernet cable. You can fill-in one or both Ping IP Addresses (IPv4 and IPv6) – based on IP protocol used on particular network interface and WAN connection settings. IPv4 and IPv6 are dual stack implemented in the router. Any changes made to settings will be applied after pressing the *Apply* button.

4.6.1 Default Priorities for Backup Routes

If the *Enable backup routes switching* check box is unchecked, the backup routes system will operate in the backward compatibility mode. The router selects the route based on the default priorities of the enabled settings for each of the network interfaces, enabling appropriate services that comply with these network interfaces. The following list contains the names of backup routes and corresponding network interfaces in order of default priorities:

- Mobile WAN (usbX)
- PPPoE (ppp0)
- WiFi STA (wlan0)
- Secondary LAN (eth1)
- Primary LAN (eth0)

Example of default priorities: *Backup Routes* are disabled. The router selects the *Secondary LAN* as the default route only if you unmark the *Create connection to mobile network* check box on the *Mobile WAN* page, unmark the *Create PPPoE connection* check box on the *PPPoE* page and unmark the *Enable WiFi* on the *WiFi* page (or use WiFi in AP mode). To select the *Primary LAN*, delete the IP address from the *Secondary LAN* page and disable the *DHCP Client* for the *Secondary LAN*.

Note: Consider there is a concept of variable WAN and LAN interfaces even if the *Backup Routes* are not enabled. The situation may occur, that LAN intended interface becomes WAN interface (because of specified or default priorities). Communication from WAN interface to LAN interface can then be blocked depending on the *NAT* and *Firewall* Configuration.

4.7 Static Routes

Static routes can be specified on the *Static Routes* configuration page. A static route provide fixed routing path through the network. It is manually configured on the router and must be updated if the network topology was changed recently. Static routes are private routers unless they are redistributed by a routing protocol. Static routes configuration form is shown on Figure 30.

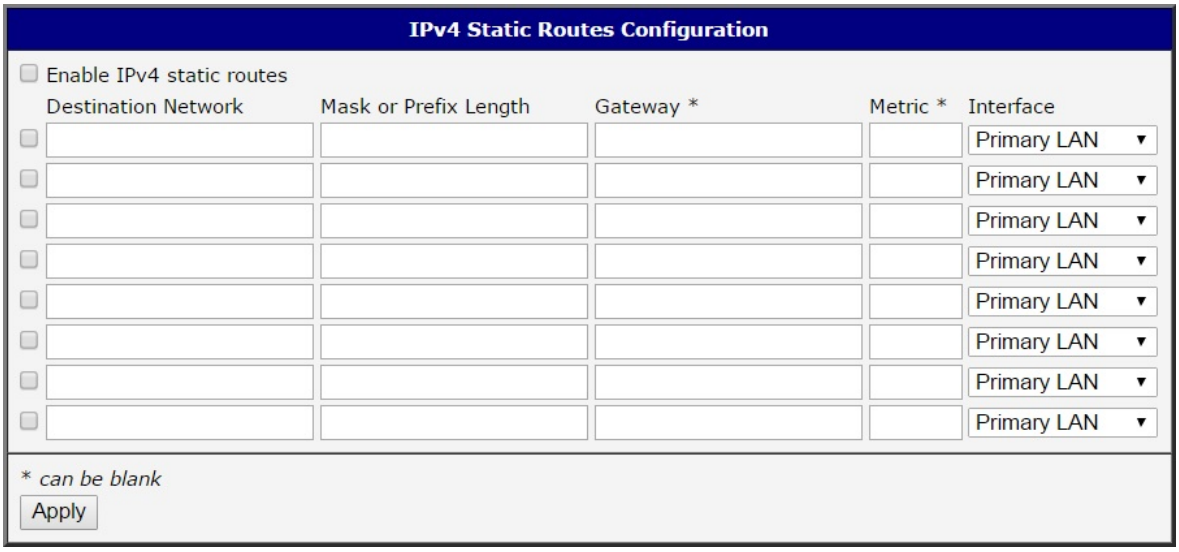


Figure 30: Static Routes Configuration

The description of all items is listed in Table 33.

Item	Description
Enable IPv4 (IPv6) static routes	If checked, static routing functionality is enabled. Active are only routes enabled by the checkbox in the first column of the table.
Destination Network	The destination IP address of the remote network or host to which you want to assign a static route.
Mask or Prefix Length	The subnet mask of the remote network or host IP address.
Gateway	IP address of the gateway device that allows for contact between the router and the remote network or host.
Metric	Metric definition, means number rating of the priority for the route in the routing table. Routes with lower metrics have higher priority.
Interface	Select an interface the remote network or host is on.

Table 33: Static Routes configuration

4.8 Firewall Configuration

The first security element for incoming packets is a check of the enabled source IP addresses and destination ports. There is independent IPv4 and IPv6 firewall since there is dual stack IPv4 and IPv6 implemented in the router. If you click the *Firewall* item in the *Configuration* menu on the left, it will expand to *IPv4* and *IPv6* options and you can click *IPv6* to enable and configure the IPv6 firewall – see Figure below. The configuration fields have the same meaning in the *IPv4 Firewall Configuration* and *IPv6 Firewall Configuration* forms.

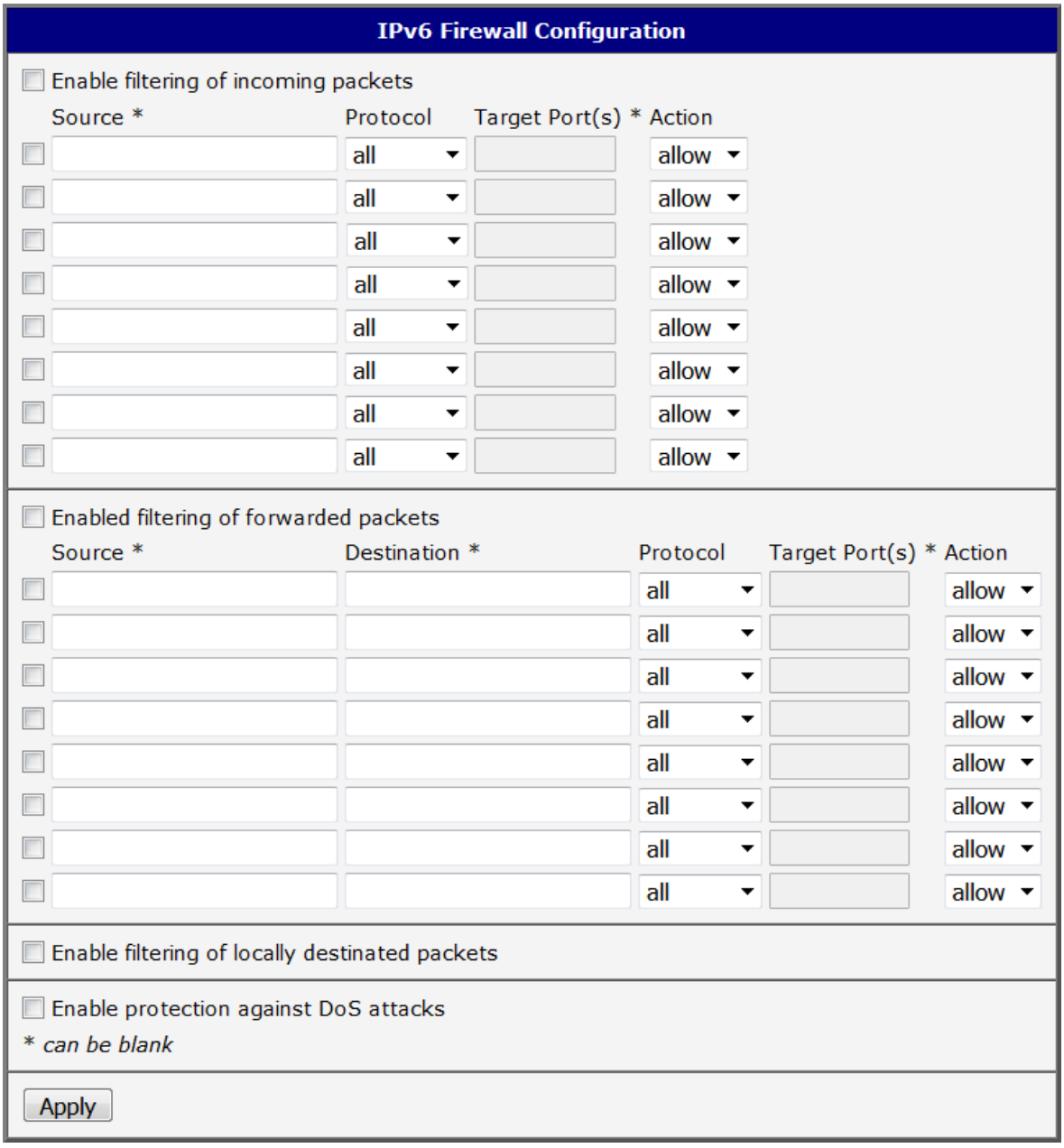


Figure 31: Firewall Configuration – IPv6 Firewall

You can specify the rules for IP addresses, protocols and ports to allow or deny the access to the router and internal network connected behind the router. To enable this function, tick the *Enable filtering of incoming packets* check box located at the top of the *IPv4 (IPv6) Firewall Configuration* page. Accessibility is checked against the IP address table. This means that

access is permitted only to addresses allowed in the table. It is possible to specify up to eight remote IP addresses for access/denial. You can specify the following parameters:

Item	Description
Source	IP address the rule applies to. Use IPv4 address in *IPv4 Firewall Configuration* and IPv6 address in *IPv6 Firewall Configuration*.
Protocol	Specifies the protocol the rule applies to: • **all** – The rule applies to all protocols. • **TCP** – The rule applies to TCP protocol. • **UDP** – The rule applies to UDP protocol. • **GRE** – The rule applies to GRE protocol. • **ESP** – The rule applies to ESP protocol. • **ICMP/ICMPv6** – The rule applies to ICMP protocol. In *IPv6 Firewall Configuration* there is the ICMPv6 option.
Target Port(s)	The port numbers range allowing access to the router. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the rule – the type of action the router performs: • **allow** – The router allows the packets to enter the network. • **deny** – The router denies the packets from entering the network.

Table 34: Filtering of Incoming Packets

The next section of the configuration form specifies the forwarding policy. If you unmark the *Enabled filtering of forwarded packets* check box, then packets are automatically accepted. If you activate this function, and a packet is addressed to another network interface, then the router sends the packet to the FORWARD chain. When the FORWARD chain accepts the packet and there is a rule for forwarding it, the router sends the packet. If a forwarding rule is unavailable, then the router drops the packet.

This configuration form also contains a table for specifying the filter rules. It is possible to create a rule to allow data with the selected protocol by specifying only the protocol, or to create stricter rules by specifying values for source IP addresses, destination IP addresses, and ports.

Item	Description
Source	IP address the rule applies to. Use IPv4 address in *IPv4 Firewall Configuration* and IPv6 address in *IPv6 Firewall Configuration*.
Destination	Destination IP address the rule applies to. Use IPv4 address in *IPv4 Firewall Configuration* and IPv6 address in *IPv6 Firewall Configuration*.

Continued on next page

Continued from previous page

Item	Description
Protocol	Specifies the protocol the rule applies to: • **all** – The rule applies to all protocols. • **TCP** – The rule applies to TCP protocol. • **UDP** – The rule applies to UDP protocol. • **GRE** – The rule applies to GRE protocol. • **ESP** – The rule applies to ESP protocol. • **ICMP/ICMPv6** – The rule applies to ICMP protocol. In *IPv6 Firewall Configuration* there is the ICMPv6 option.
Target Port(s)	The target port numbers. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Action	Specifies the rule – the type of action the router performs: • **allow** – The router allows the packets to enter the network. • **deny** – The router denies the packets from entering the network.

Table 35: Forwarding filtering

When you enable the *Enable filtering of locally destined packets* function, the router drops the packets requesting an unsupported service. The packet is dropped automatically without any information.

As a protection against DoS attacks, the *Enable protection against DoS attacks* limits the number of allowed connections per second to five. The DoS attack floods the target system with meaningless requirements.

4.8.1 Example of the IPv4 Firewall Configuration

The router allows the following access:

- From IP address 171.92.5.45 using any protocol.
- From IP address 10.0.2.123 using the TCP protocol on port 1000.
- From IP address 142.2.26.54 using the ICMP protocol.
- from IP address 142.2.26.54 using the TCMP protocol on target ports from 1020 to 1040

See the network topology and configuration form in the Figures below.

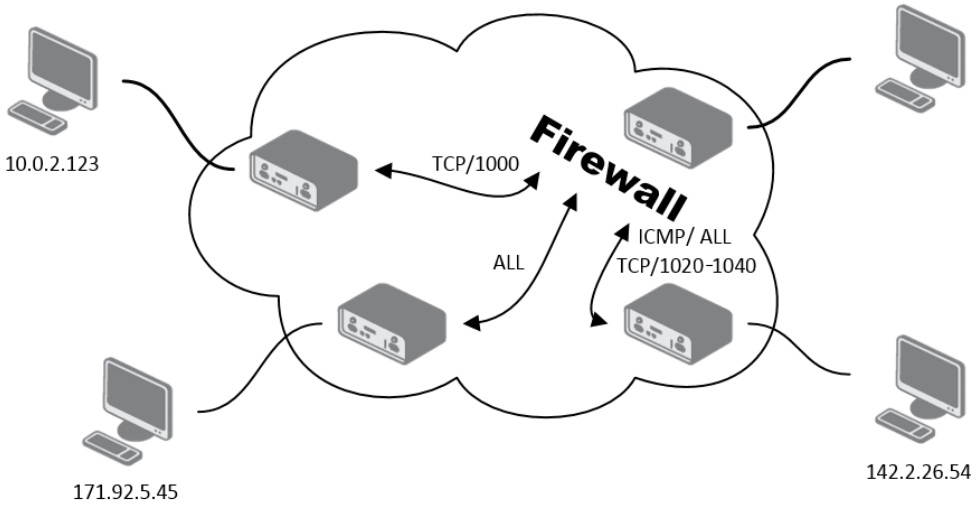


Figure 32: Topology for the IPv4 Firewall Configuration Example

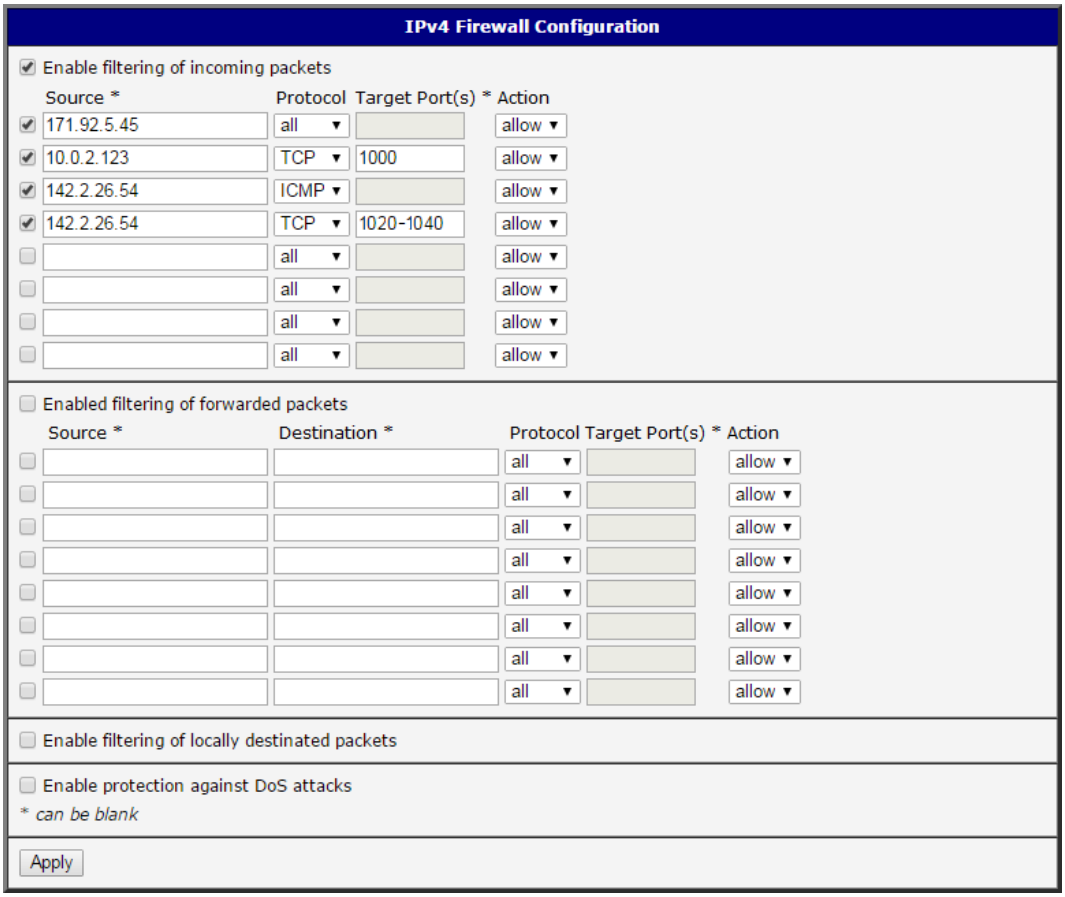


Figure 33: IPv4 Firewall Configuration Example

4.9 NAT Configuration

To configure the address translation function, click on *NAT* in the *Configuration* section of the main menu. There is independent IPv4 and IPv6 NAT configuration since there is dual stack IPv4 and IPv6 implemented in the router. The *NAT* item in the menu on the left will expand to *IPv4* and *IPv6* options and you can click *IPv6* to enable and configure the IPv6 NAT – see Figure below. The configuration fields have the same meaning in the *IPv4 NAT Configuration* and *IPv6 NAT Configuration* forms.

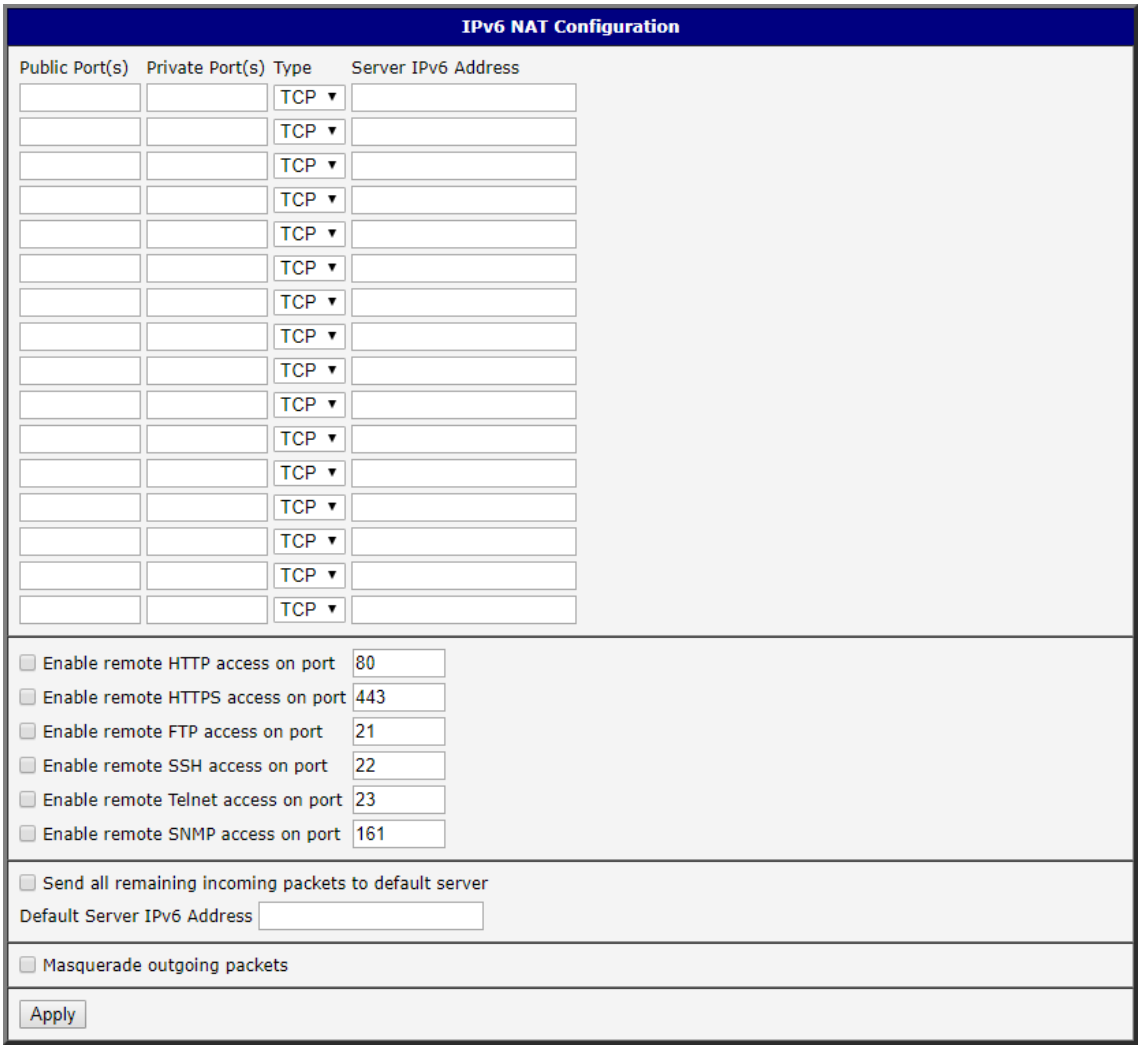


Figure 34: NAT – IPv6 NAT Configuration

The router actually uses Port Address Translation (PAT), which is a method of mapping a TCP/UDP port to another TCP/UDP port. The router modifies the information in the packet header as the packets traverse a router. This configuration form allows you to specify up to 16 PAT rules.

Item	Description
Public Port(s)	The public port numbers range for NAT. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Private Port(s)	The private port numbers range for NAT. Enter the initial and final port numbers separated by the hyphen mark. One static port is allowed as well.
Type	Protocol type – TCP or UDP.
Server IPv4 address	In *IPv4 NAT Configuration* only. IPv4 address where the router forwards incoming data.
Server IPv6 address	In *IPv6 NAT Configuration* only. IPv6 address where the router forwards incoming data.

Table 36: NAT Configuration

If you require more than sixteen NAT rules, insert the remaining rules into the Startup Script. The *Startup Script* dialog is located on *Scripts* page in the *Configuration* section of the menu. When creating your rules in the Startup Script, use this command for IPv4 NAT:

```
iptables -t nat -A pre_nat -p tcp --dport [PORT_PUBLIC] -j DNAT
--to-destination [IPADDR]:[PORT_PRIVATE]
```

Enter the IP address [IPADDR], the public ports numbers [PORT_PUBLIC], and private [PORT_PRIVATE] in place of square brackets. For IPv6 NAT use `ip6tables` command with same options.:

```
ip6tables -t nat -A napt -p tcp --dport [PORT_PUBLIC] -j DNAT
--to-destination [IP6ADDR]:[PORT_PRIVATE]
```

If you enable the following options and enter the port number, the router allows you to remotely access to the router from WAN (Mobile WAN) interface.

Item	Description
Enable remote HTTP access on port	This option **sets the redirect** from HTTP to HTTPS **only** (disabled in default configuration).
Enable remote HTTPS access on port	If field and port number are filled in, configuration of the router over web interface is allowed (disabled in default configuration).
Enable remote FTP access on port	Select this option to allow access to the router using FTP (disabled in default configuration).
Enable remote SSH access on port	Select this option to allow access to the router using SSH (disabled in default configuration).
Enable remote Telnet access on port	Select this option to allow access to the router using Telnet (disabled in default configuration).
Enable remote SNMP access on port	Select this option to allow access to the router using SNMP (disabled in default configuration).

Continued on next page

Continued from previous page

Item	Description
Masquerade outgoing packets	Activates/deactivates the network address translation function.

Table 37: Remote Access Configuration

Enable remote HTTP access on port activates **the redirect from HTTP to HTTPS protocol only**. The router doesn't allow unsecured HTTP protocol to access the web configuration. To access the web configuration, always check the *Enable remote HTTPS access on port* item. Never enable the HTTP item only to access the web configuration from the Internet (configuration would not be accessible from the Internet). Always check the HTTPS item or HTTPS and HTTP items together (to set the redirect from HTTP).

Use the following parameters to set the routing of incoming data from the WAN (Mobile WAN) to a connected computer.

Item	Description
Send all remaining incoming packets to default server	Activates/deactivates forwarding unmatched incoming packets to the default server. The prerequisite for the function is that you specify a default server in the *Default Server IPv4/IPv6 Address* field. The router can forward incoming data from a GPRS to a computer with the assigned IP address.
Default Server IP Address	In *IPv4 NAT Configuration* only. The IPv4 address.
Default Server IPv6 Address	In *IPv6 NAT Configuration* only. The IPv6 address.

Table 38: Configuration of Send all incoming packets to server

4.9.1 Examples of NAT Configuration

Example 1: IPv4 NAT Configuration with Single Device Connected

It is important to mark the *Send all remaining incoming packets to default server* check box for this configuration. The IP address in this example is the address of the device behind the router. The default gateway of the devices in the subnetwork connected to router is the same IP address as displayed in the *Default Server IPv4 Address* field. The connected device replies if a PING is sent to the IP address of the SIM card.

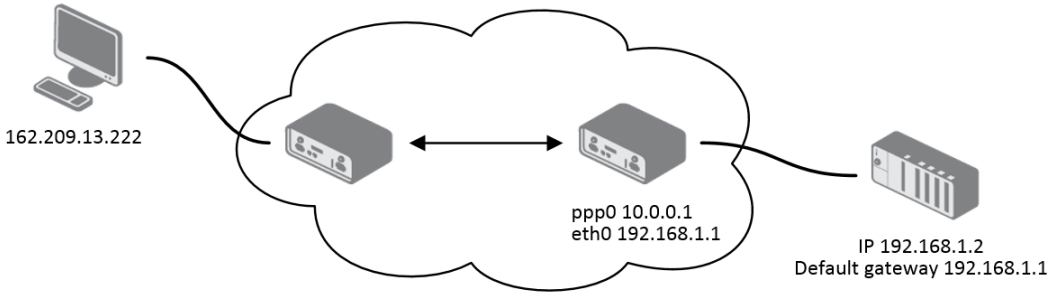


Figure 35: Topology for NAT Configuration Example 1

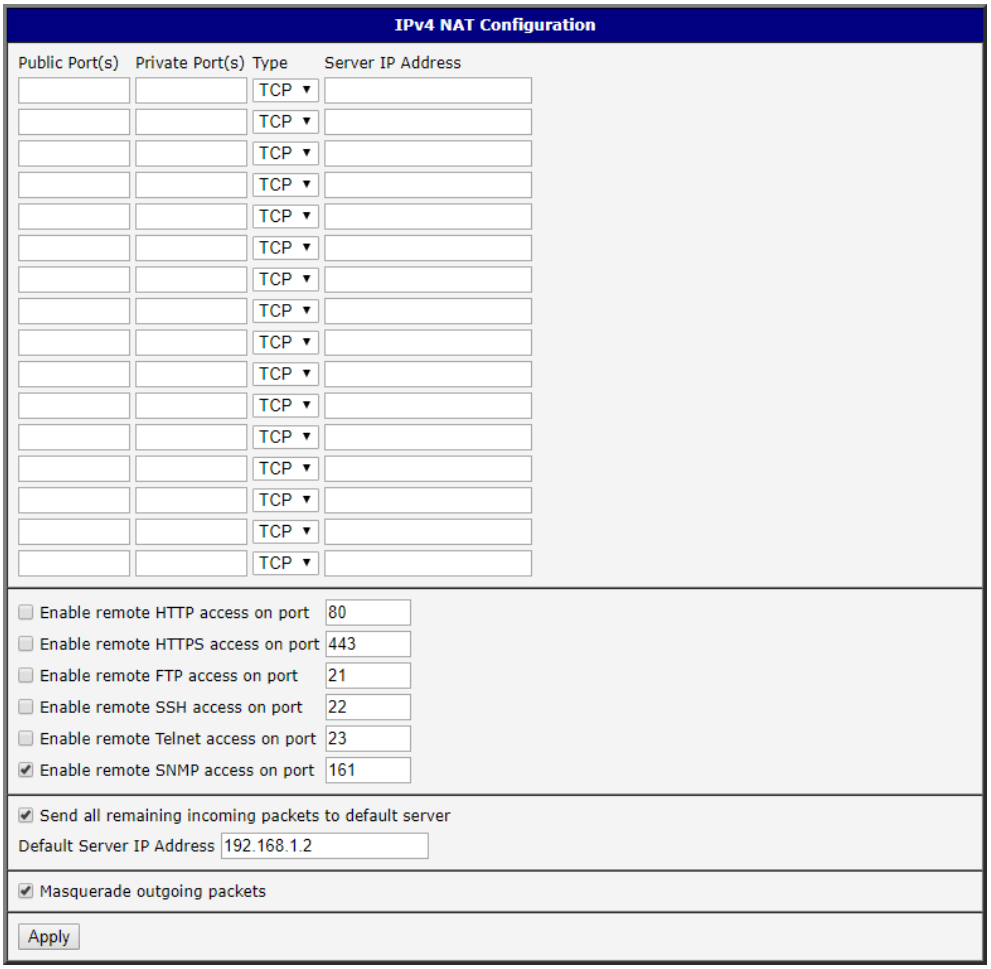


Figure 36: NAT Configuration for Example 1

Example 2: IPv4 NAT Configuration with More Equipment Connected

In this example, using the switch you can connect more devices behind the router. Every device connected behind the router has its own IP address. Enter the address in the *Server IPv Address* field in the *NAT* dialog. The devices are communicating on port 80, but you can set port forwarding using the *Public Port* and *Private Port* fields in the NAT dialog. You have now configured the router to access the 192.168.1.2:80 socket behind the router when accessing the IP address 10.0.0.1:81 from the Internet. If you send a ping request to the public IP address of the router (10.0.0.1), the router responds as usual (not forwarding). And since the *Send all remaining incoming packets to default server* is inactive, the router denies connection attempts.

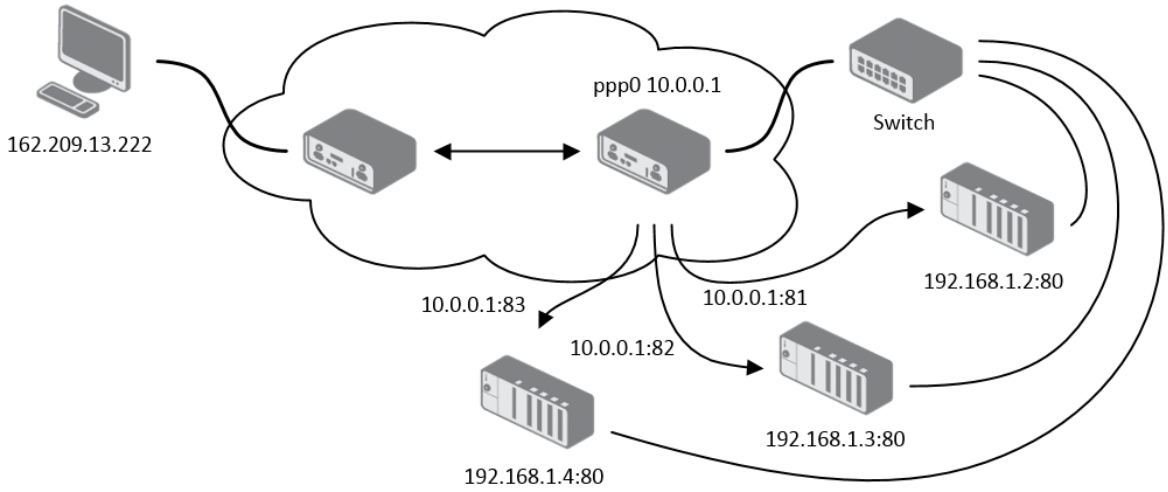


Figure 37: Topology for NAT Configuration Example 2

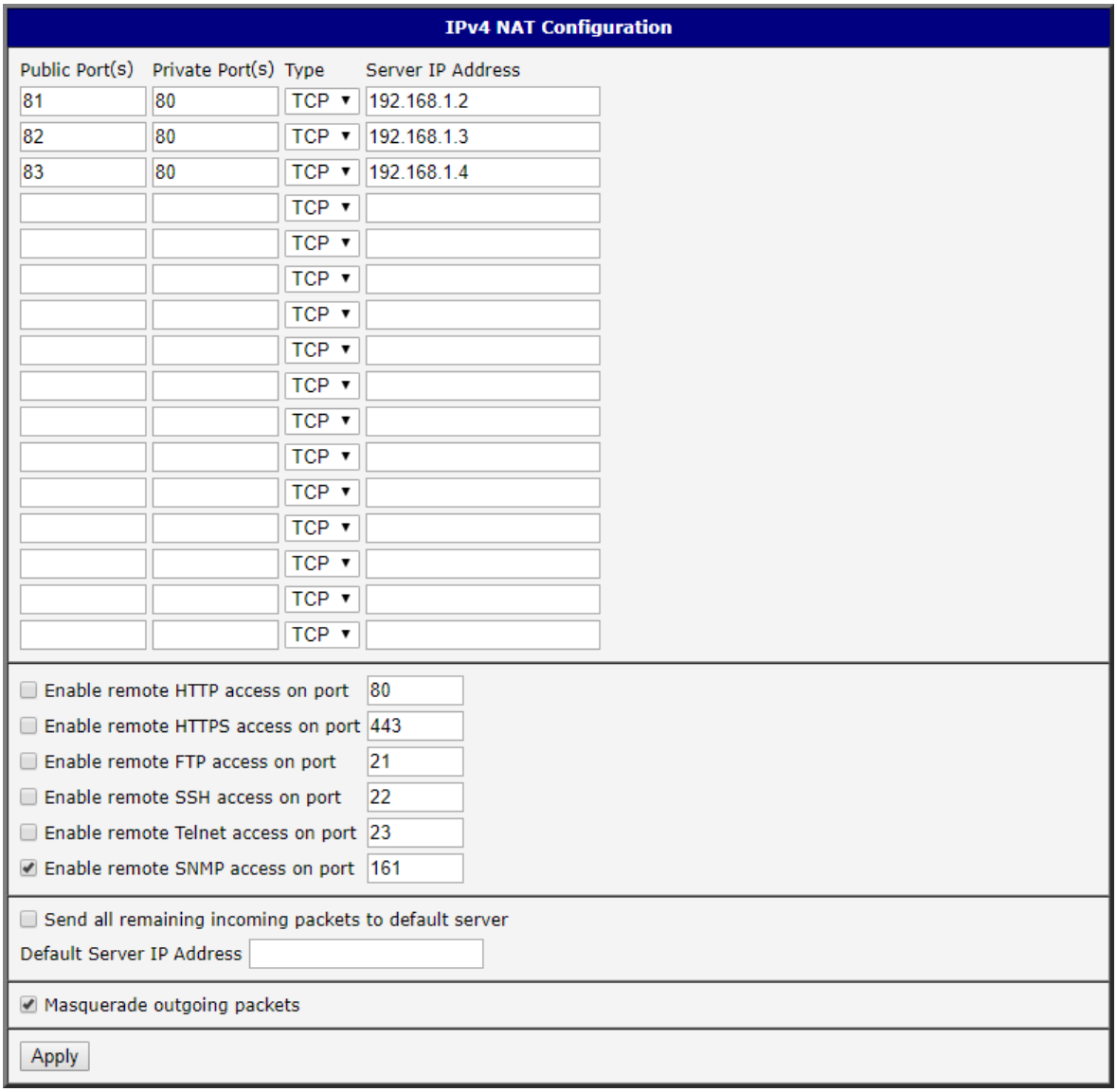


Figure 38: NAT Configuration for Example 2

4.10 OpenVPN Tunnel Configuration

Select the *OpenVPN* item to configure an OpenVPN tunnel. The menu item will expand and you will see four separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. The OpenVPN tunnel function allows you to create a secure connection between two separate LAN networks. The router allows you to create up to four OpenVPN tunnels. IPv4 and IPv6 dual stack is supported.

Item	Description
Description	Specifies the description or name of tunnel.
Protocol	Specifies the communication protocol. • **UDP** – The OpenVPN communicates using UDP. • **TCP server** – The OpenVPN communicates using TCP in server mode. • **TCP client** – The OpenVPN communicates using TCP in client mode. • **UDPv6** – The OpenVPN communicates using UDP over IPv6. • **TCPv6 server** – The OpenVPN communicates using TCP over IPv6 in server mode. • **TCPv6 client** – The OpenVPN communicates using TCP over IPv6 in client mode.
UDP/TCP port	Specifies the port of the relevant protocol (UDP or TCP).
Remote IP Address	Specifies the IPv4, IPv6 address or domain name of the opposite side of the tunnel.
Remote Subnet	IPv4 address of a network behind opposite side of the tunnel.
Remote Subnet Mask	IPv4 subnet mask of a network behind opposite tunnel's side.
Redirect Gateway	Adds (rewrites) the default gateway. All the packets are then sent to this gateway via tunnel, if there is no other specified default gateway inside them.
Local Interface IP Address	Specifies the IPv4 address of a local interface. **For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.**
Remote Interface IP Address	Specifies the IPv4 address of the interface of opposite side of the tunnel. **For proper routing it is recommended to fill-in any IPv4 address from local range even if you are using IPv6 tunnel only.**
Remote IPv6 Subnet	IPv6 address of the remote IPv6 network. Equivalent of the *Remote Subnet* in IPv4 section.
Remote IPv6 Prefix	IPv6 prefix of the remote IPv6 network. Equivalent of the *Remote Subnet Mask* in IPv4 section.
Local Interface IPv6 Address	Specifies the IPv6 address of a local interface.

Continued on next page

Continued from previous page

Item	Description
Remote Interface IPv6 Address	Specifies the IPv6 address of the interface of opposite side of the tunnel.
Ping Interval	Time interval after which the router sends a message to opposite side of tunnel to verify the existence of the tunnel.
Ping Timeout	Specifies the time interval the router waits for a message sent by the opposite side. For proper verification of the OpenVPN tunnel, set the *Ping Timeout* to greater than the *Ping Interval*.
Renegotiate Interval	Specifies the renegotiate period (reauthorization) of the OpenVPN tunnel. You can only set this parameter when the *Authenticate Mode* is set to *username/password* or *X.509 certificate*. After this time period, the router changes the tunnel encryption to keep the tunnel secure.
Max Fragment Size	Maximum size of a sent packet.
Compression	Compression of the data sent: • **none** – No compression is used. • **LZO** – A lossless compression is used, use the same setting on both sides of the tunnel.
NAT Rules	Activates/deactivates the NAT rules for the OpenVPN tunnel: • **not applied** – NAT rules are not applied to the tunnel. • **applied** – NAT rules are applied to the OpenVPN tunnel.
Authenticate Mode	Specifies the authentication mode: • **none** – No authentication is set. • **Pre-shared secret** – Specifies the shared key function for both sides of the tunnel. • **Username/password** – Specifies authentication using a CA Certificate, Username and Password. • **X.509 Certificate (multiclient)** – Activates the X.509 authentication in multi-client mode. • **X.509 Certificate (client)** – Activates the X.509 authentication in client mode. • **X.509 Certificate (server)** – Activates the X.509 authentication in server mode.
Pre-shared Secret	Specifies the pre-shared secret which you can use for every authentication mode.
CA Certificate	Specifies the CA Certificate which you can use for the username/password and X.509 Certificate authentication modes.

Continued on next page

Continued from previous page

Item	Description
DH Parameters	Specifies the protocol for the DH parameters key exchange which you can use for X.509 Certificate authentication in the server mode.
Local Certificate	Specifies the certificate used in the local device. You can use this authentication certificate for the X.509 Certificate authentication mode.
Local Private Key	Specifies the key used in the local device. You can use the key for the X.509 Certificate authentication mode.
Username	Specifies a login name which you can use for authentication in the username/password mode.
Password	Specifies a password which you can use for authentication in the username/password mode. Enter valid characters only, see chap. 1.4.1!
Extra Options	Specifies additional parameters for the OpenVPN tunnel, such as DHCP options. The parameters are proceeded by two dashes. For possible parameters see the help text in the router using SSH – run the `openvpnd --help` command.

Table 39: OpenVPN Configuration

There is a condition for tunnel to be established: WAN route has to be active (for example mobile connection established) even if the tunnel does not go through the WAN.

The changes in settings will apply after pressing the *Apply* button.

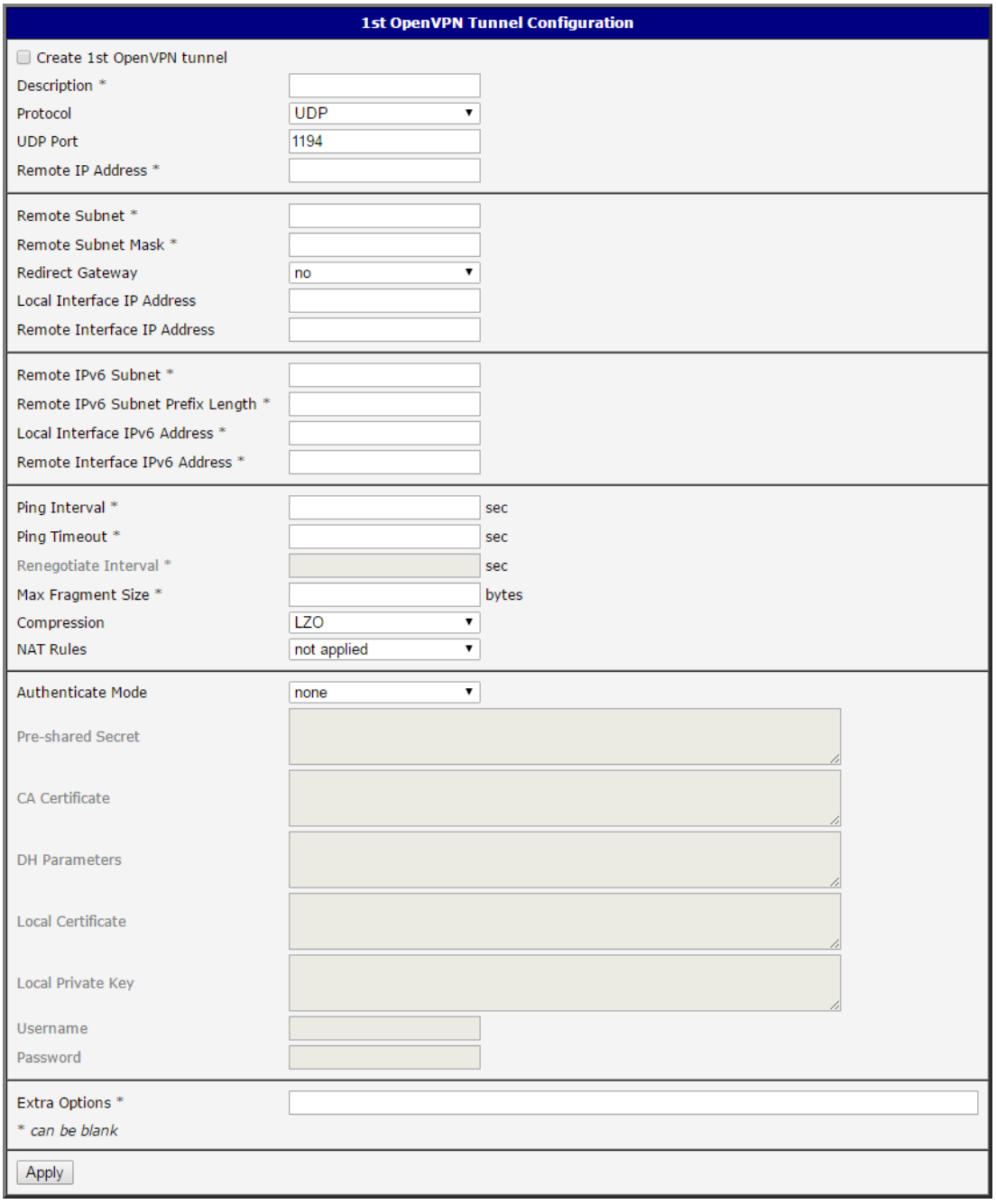


Figure 39: OpenVPN tunnel configuration

4.10.1 Example of the OpenVPN Tunnel Configuration in IPv4 Network

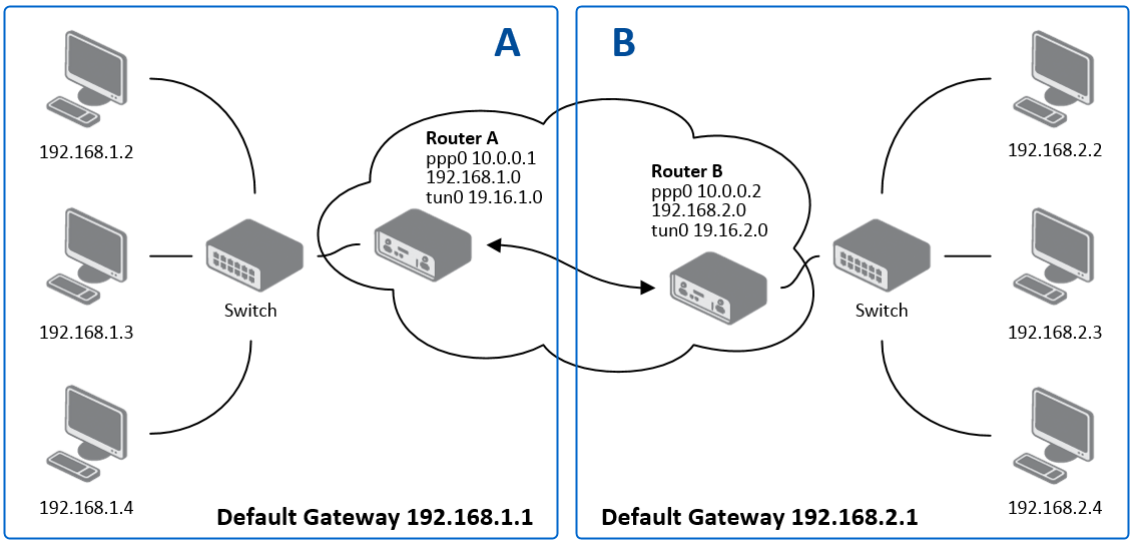


Figure 40: Topology of OpenVPN Configuration Example

OpenVPN tunnel configuration:

Configuration	A	B
Protocol	UDP	UDP
UDP Port	1194	1194
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Interface IP Address	19.16.1.0	19.16.2.0
Remote Interface IP Address	19.16.2.0	19.18.1.0
Compression	LZO	LZO
Authenticate mode	none	none

Table 40: OpenVPN Configuration Example

Examples of different options for configuration and authentication of OpenVPN tunnel can be found in the "OpenVPN Tunnel" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

4.11 IPsec Tunnel Configuration

To open the *IPsec Tunnel Configuration* page, click *IPsec* in the *Configuration* section of the main menu. The menu item will expand and you will see four separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. The IPsec tunnel function allows you to create a secured connection between two separate LAN networks. The router allows you to create up to four IPsec tunnels. IPv4 and IPv6 tunnels are supported (dual stack), you can transport IPv6 traffic through IPv4 tunnel and vice versa.

To encrypt data between the local and remote subnets, specify the appropriate values in the subnet fields on both routers. To encrypt the data stream between the routers only, leave the local and remote subnets fields blank.

If you specify the protocol and port information in the *Local Protocol/Port* field, then the router encapsulates only the packets matching the settings.

For optimal setup, we recommend to follow instructions on the web page: https://wiki.strongswan.org/projects/strongswan/wiki/SecurityRecommendations.

Item	Description
Description	Name or description of the tunnel.
Host IP Mode	• **IPv4** – The router communicates via IPv4 with the opposite side of the tunnel. • **IPv6** – The router communicates via IPv4 with the opposite side of the tunnel.
Remote IP Address	IPv4, IPv6 address or domain name of the remote side of the tunnel, based in the *Host IP Mode* above.
Remote ID	Identifier (ID) of remote side of the tunnel. It consists of two parts: a *hostname* and a *domain-name*.
Tunnel IP Mode	• **IPv4** – The IPv4 communication runs inside the tunnel. • **IPv6** – The IPv6 communication runs inside the tunnel.
First Remote Subnet	IPv4 or IPv6 address of a network behind remote side of the tunnel, based on *Tunnel IP Mode* above.
First Remote Subnet Mask/Prefix	IPv4 subnet mask of a network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128).
Second Remote Subnet	IPv4 or IPv6 address of the second network behind remote side of the tunnel, based on *Tunnel IP Mode* above. For *IKE Protocol* = IKEv2 only.
Second Remote Subnet Mask/Prefix	IPv4 subnet mask of the second network behind remote side of the tunnel, or IPv6 prefix (single number 0 to 128). For *IKE Protocol* = IKEv2 only.

Continued on next page

Continued from previous page

Item	Description
Remote Protocol/Port	Specifies Protocol/Port of remote side of the tunnel. The general form is *protocol*/*port*, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Local ID	Identifier (ID) of local side of the tunnel. It consists of two parts: a *hostname* and a *domain-name*.
First Local Subnet	IPv4 or IPv6 address of a local network, based on *Tunnel IP Mode* above.
First Local Subnet Mask/Prefix	IPv4 subnet mask of a local network, or IPv6 prefix (single number 0 to 128).
Second Local Subnet	IPv4 or IPv6 address of the second local network, based on *Tunnel IP Mode* above. For *IKE Protocol* = IKEv2 only.
Second Local Subnet Mask/Prefix	IPv4 subnet mask of the second local network, or IPv6 prefix (single number 0 to 128). For *IKE Protocol* = IKEv2 only.
Local Protocol/Port	Specifies Protocol/Port of a local network. The general form is *protocol*/*port*, for example 17/1701 for UDP (protocol 17) and port 1701. It is also possible to enter only the number of protocol, however, the above mentioned format is preferred.
Encapsulation Mode	Specifies the IPsec mode, according to the method of encapsulation. You can select the *tunnel* mode in which the entire IP datagram is encapsulated or the *transport* mode in which only IP header is encapsulated.
Force NAT Traversal	Enable NAT traversal enforcement (UDP encapsulation of ESP packets). (*Enabled*).
IKE Protocol	Specifies the version of IKE (IKEv1/IKEv2, IKEv1 or IKEv2).
IKE Mode	Specifies the mode for establishing a connection (*main* or *aggressive*). If you select the aggressive mode, then the router establishes the IPsec tunnel faster, but the encryption is permanently set to 3DES-MD5. **We recommend that you not use the *aggressive* mode due to lower security!**
IKE Algorithm	Specifies the means by which the router selects the algorithm: • **auto** – The encryption and hash algorithm are selected automatically. • **manual** – The encryption and hash algorithm are defined by the user.
IKE Encryption	Encryption algorithm – 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128.
IKE Hash	Hash algorithm – MD5, SHA1, SHA256 or SHA512.
IKE DH Group	Specifies the Diffie-Hellman groups which determine the strength of the key used in the key exchange process. Higher group numbers are more secure, but require more time to compute the key.

Continued on next page

Continued from previous page

Item	Description
IKE Reauthentication	Enable or disable IKE reauthentication (IKEv2 only).
XAUTH Enabled	Enable extended authentication (for IKEv1 only).
XAUTH Mode	Select XAUTH mode (client or server).
XAUTH Username	XAUTH username.
XAUTH Password	XAUTH password.
ESP Algorithm	Specifies the means by which the router selects the algorithm: • **auto** – The encryption and hash algorithm are selected automatically. • **manual** – The encryption and hash algorithm are defined by the user.
ESP Encryption	Encryption algorithm – DES, 3DES, AES128, AES192, AES256, AES128GCM128, AES192GCM128, AES256GCM128.
ESP Hash	Hash algorithm – MD5, SHA1, SHA256 or SHA512.
PFS	Enables/disables the Perfect Forward Secrecy function. The function ensures that derived session keys are not compromised if one of the private keys is compromised in the future.
PFS DH Group	Specifies the Diffie-Hellman group number (see *IKE DH Group*).
Key Lifetime	Lifetime key data part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
IKE Lifetime	Lifetime key service part of tunnel. The minimum value of this parameter is 60 s. The maximum value is 86400 s.
Rekey Margin	Specifies how long before a connection expires that the router attempts to negotiate a replacement. Specify a maximum value that is less than half of IKE and Key Lifetime parameters.
Rekey Fuzz	Percentage of time for the Rekey Margin extension.
DPD Delay	Time after which the IPsec tunnel functionality is tested.
DPD Timeout	The period during which device waits for a response.
Authenticate Mode	Specifies the means by which the router authenticates: • **Pre-shared key** – Sets the shared key for both sides of the tunnel. • **X.509 Certificate** – Allows X.509 authentication in multi-client mode.
Pre-shared Key	Specifies the shared key for both sides of the tunnel. The prerequisite for entering a key is that you select pre-shared key as the authentication mode.
CA Certificate	Certificate for X.509 authentication.
Remote Certificate \ PubKey	Certificate for X.509 authentication or PubKey for public key signature authentication.

Continued on next page

Continued from previous page

Item	Description
Local Certificate \ PubKey	Certificate for X.509 authentication or PubKey for public key signature authentication.
Local Private Key	Private key for X.509 authentication.
Local Passphrase	Passphrase used during private key generation.
Debug	Choose the level of verbosity to System Log. Silent (default), audit, control, control-more, raw, private (most verbose including the private keys). See strongSwan documentation for more details.

Table 41: IPsec Tunnel Configuration

Do not miss:

- If local and remote subnets are not configured then only packets between local and remote IP address are encapsulated, so only communication between two routers is encrypted.
- If protocol/port fields are configured then only packets matching these settings are encapsulated.

The following procedure describes how to generate certificates and keys without a password phrase:

```
******************** certification authority ************************
openssl rand -out private/.rand 1024
openssl genrsa -des3 -out private/ca.key 2048
openssl req -new -key private/ca.key -out tmp/myrootca.req
openssl x509 -req -days 7305 -sha1 -extensions v3_ca -signkey
private/ca.key -in tmp/myrootca.req -out ca.crt

******************** server cert ************************************
openssl genrsa -out private/server.key 2048
openssl req -new -key private/server.key -out tmp/server.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/server.req -CAserial ca.srl -CAcreateserial
-out server.crt

******************** client cert ************************************
openssl genrsa -out private/client.key 2048
openssl req -new -key private/client.key -out tmp/client.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/client.req -CAserial ca.srl -CAcreateserial
-out client.crt
```

Listed below are the certificates with password phrase "router" (certification authority remains unchanged):

```
******************** server cert ************************************
openssl genrsa -des3 -passout pass:router -out private/server.pem 2048
openssl req -new -key private/server.pem -out tmp/server.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/server.req -CAserial ca.srl -CAcreateserial
-out server.crt

******************** client cert ************************************
openssl genrsa -des3 -passout pass:router -out private/client.pem 2048
openssl req -new -key private/client.pem -out tmp/client.req
openssl x509 -req -days 7305 -sha1 -extensions v3_req -CA ca.crt -CAkey
private/ca.key -in tmp/client.req -CAserial ca.srl -CAcreateserial
-out client.crt
```

The IPsec function supports the following types of identifiers (ID) for both sides of the tunnel, *Remote ID* and *Local ID* parameters:

- IP address (for example, 192.168.1.1)
- DN (for example, C=CZ,O=CompanyName,OU=TP,CN=A)
- FQDN (for example, @director.companyname.cz) – **the @ symbol proceeds the FQDN. FQDN resolving is not supported.**
- User FQDN (for example, director@companyname.cz)

The certificates and private keys have to be in the PEM format. Use only certificates containing start and stop tags.

The random time, after which the router re-exchanges new keys is defined as follows:

*Lifetime - (Rekey margin + random value in range (from 0 to Rekey margin * Rekey Fuzz/100))*

The default exchange of keys is in the following time range:

- Minimal time: 1h - (9m + 9m) = 42m
- Maximal time: 1h - (9m + 0m) = 51m

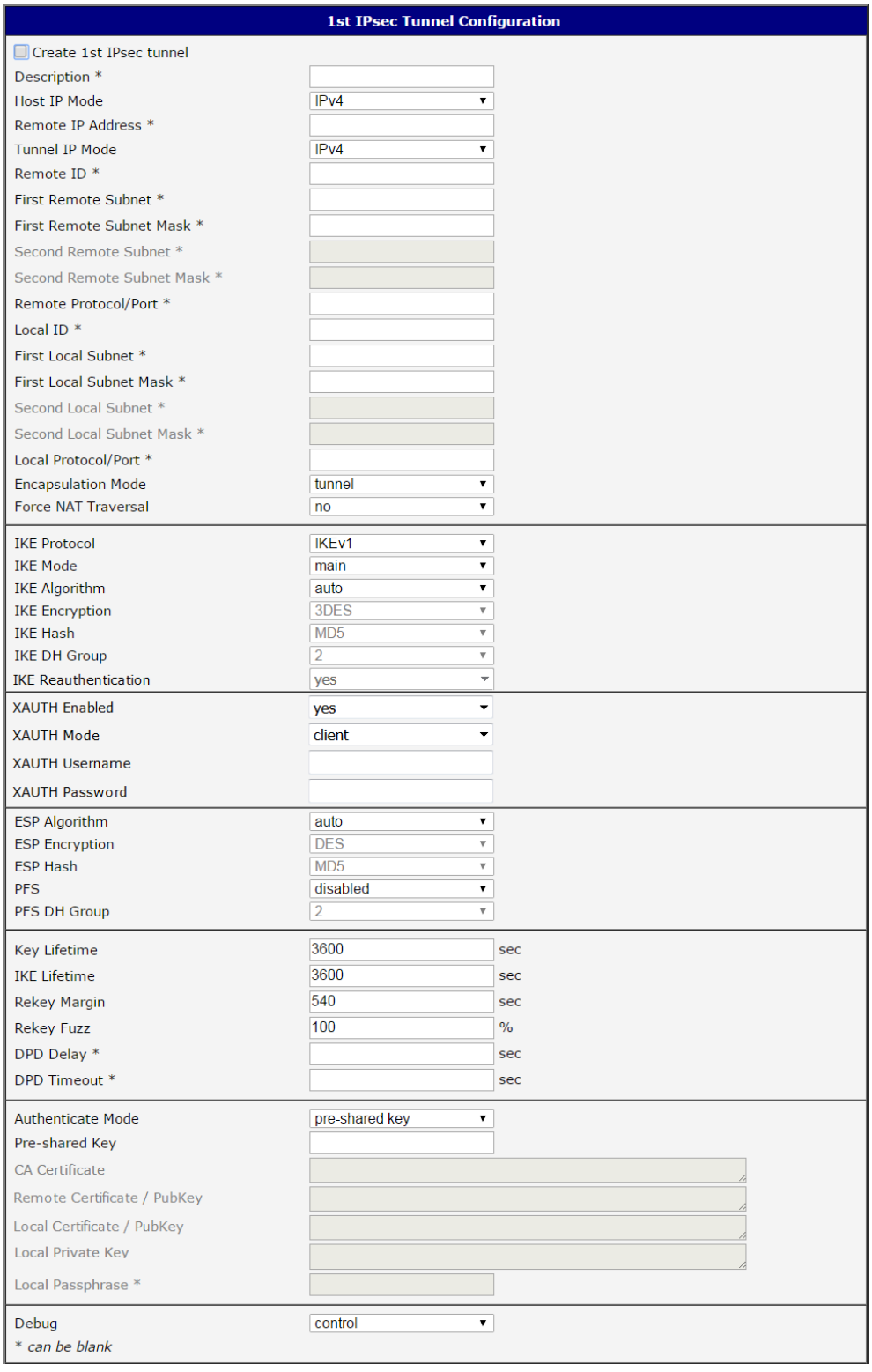


Figure 41: IPsec Tunnels Configuration

We recommend that you maintain the default settings. When you set key exchange times higher, the tunnel produces lower operating costs, but the setting also provides less security. Conversely, when you reducing the time, the tunnel produces higher operating costs, but provides for higher security.

The changes in settings will apply after clicking the *Apply* button.

4.11.1 Example of the IPSec Tunnel Configuration in IPv4 Network

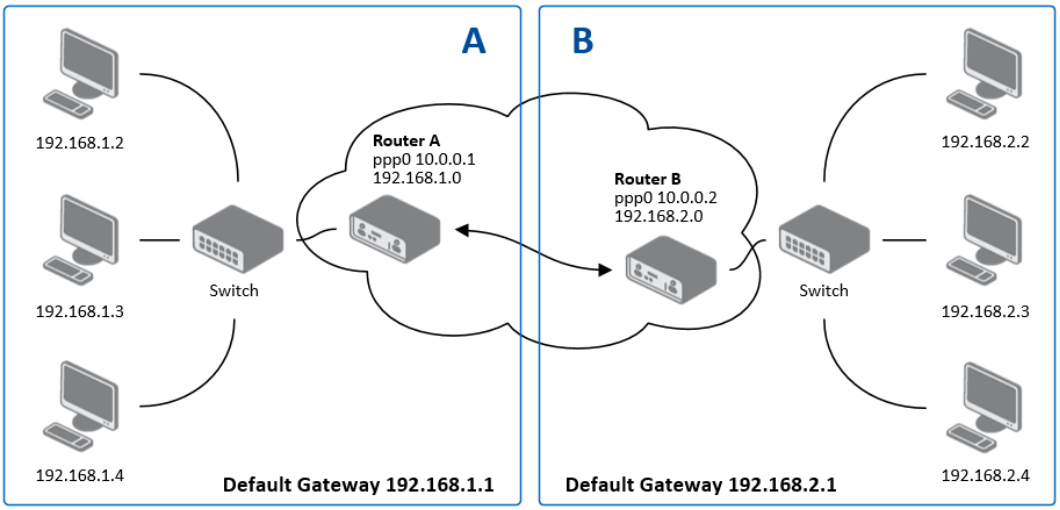


Figure 42: Topology of IPsec Configuration Example

IPsec tunnel configuration:

Configuration	A	B
Host IP Mode	IPv4	IPv4
Remote IP Address	10.0.0.2	10.0.0.1
Tunnel IP Mode	IPv4	IPv4
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Local Subnet	192.168.1.0	192.168.2.0
Local Subnet Mas:	255.255.255.0	255.255.255.0
Authenticate mode	pre-shared key	pre-shared key
Pre-shared key	test	test

Table 42: Example IPsec configuration

Examples of different options for configuration and authentication of IPsec tunnel can be found in the "IPsec Tunnel" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

4.12 GRE Tunnels Configuration

GRE is an unencrypted protocol. GRE via IPv6 is not supported.

To open the *GRE Tunnel Configuration* page, click *GRE* in the *Configuration* section of the main menu. The menu item will expand and you will see four separate configuration pages: *1st Tunnel*, *2nd Tunnel*, *3rd Tunnel* and *4th Tunnel*. The GRE tunnel function allows you to create an unencrypted connection between two separate LAN networks. The router allows you to create four GRE tunnels.

Item	Description
Description	Description of the GRE tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	IP address of the network behind the remote side of the tunnel.
Remote Subnet Mask	Specifies the mask of the network behind the remote side of the tunnel.
Local Interface IP Address	IP address of the local side of the tunnel.
Remote Interface IP Address	IP address of the remote side of the tunnel.
Multicasts	Activates/deactivates sending multicast into the GRE tunnel: • **disabled** – Sending multicast into the tunnel is inactive. • **enabled** – Sending multicast into the tunnel is active.
Pre-shared Key	Specifies an optional value for the 32 bit shared key in numeric format, with this key the router sends the filtered data through the tunnel. Specify the same key on both routers, otherwise the router drops received packets.

Table 43: GRE Tunnel Configuration

The GRE tunnel cannot pass through the NAT.

The changes in settings will apply after pressing the *Apply* button.

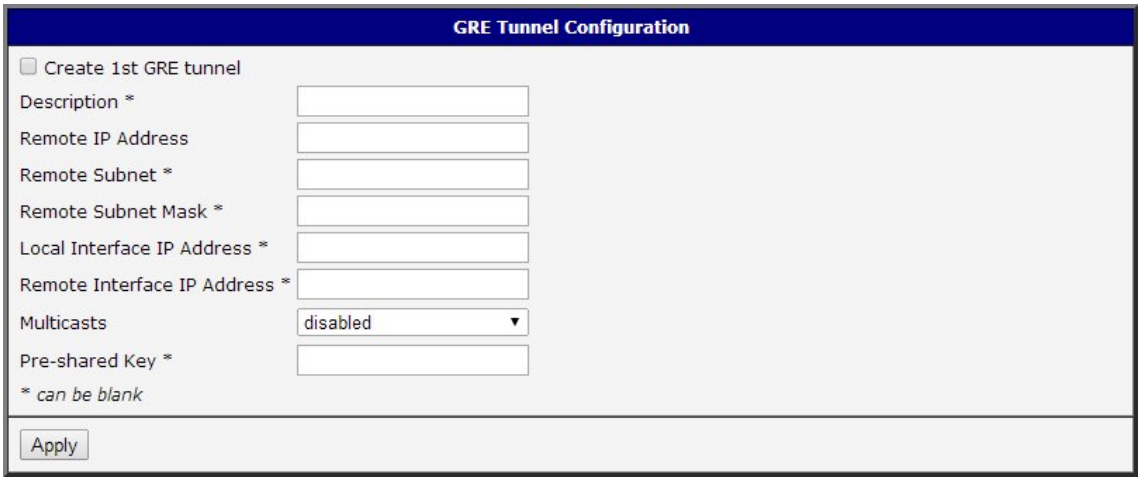


Figure 43: GRE Tunnel Configuration

4.12.1 Example of the GRE Tunnel Configuration

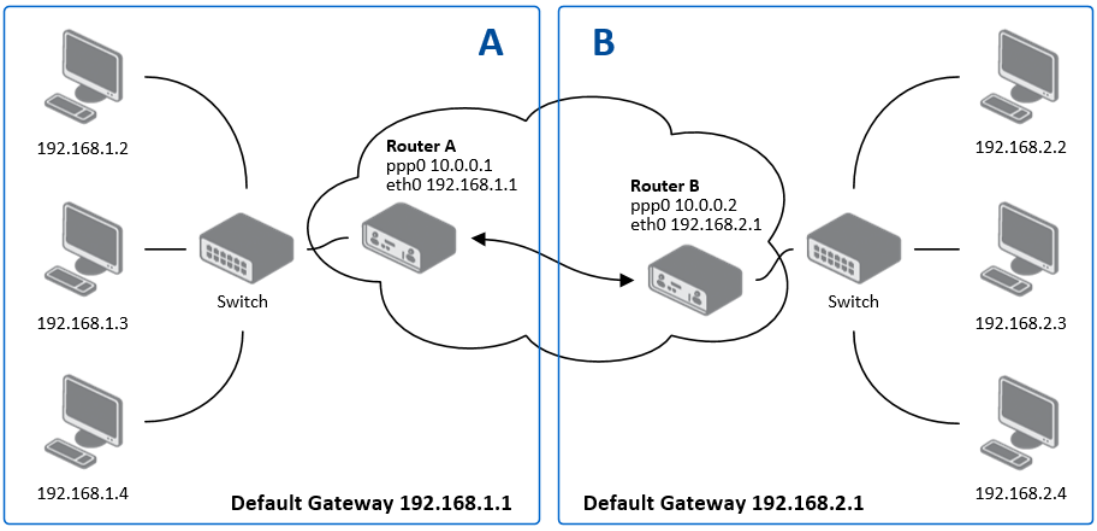


Figure 44: Topology of GRE Tunnel Configuration Example

GRE tunnel configuration:

Configuration	A	B
Remote IP Address	10.0.0.2	10.0.0.1
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0

Table 44: GRE Tunnel Configuration Example

Examples of different options for configuration of GRE tunnel can be found in the "GRE Tunnel" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

4.13 L2TP Tunnel Configuration

L2TP is an unencrypted protocol. L2TP via IPv6 is not supported.

To open the *L2TP Tunnel Configuration* page, click *L2TP* in the *Configuration* section of the main menu. The L2TP tunnel function allows you to create a password protected connection between 2 LAN networks. Enable the *Create L2TP tunnel* checkbox to activate the tunnel.

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: • **L2TP server** – Specify an IP address range offered by the server. • **L2TP client** – Specify the IP address of the server.
Server IP Address	IP address of the server.
Client Start IP Address	IP address to start with in the address range. The range is offered by the server to the clients.
Client End IP Address	The last IP address in the address range. The range is offered by the server to the clients.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel.
Username	Username for the L2TP tunnel login.
Password	Password for the L2TP tunnel login. Enter valid characters only, see chap. 1.4.1.

Table 45: L2TP Tunnel Configuration

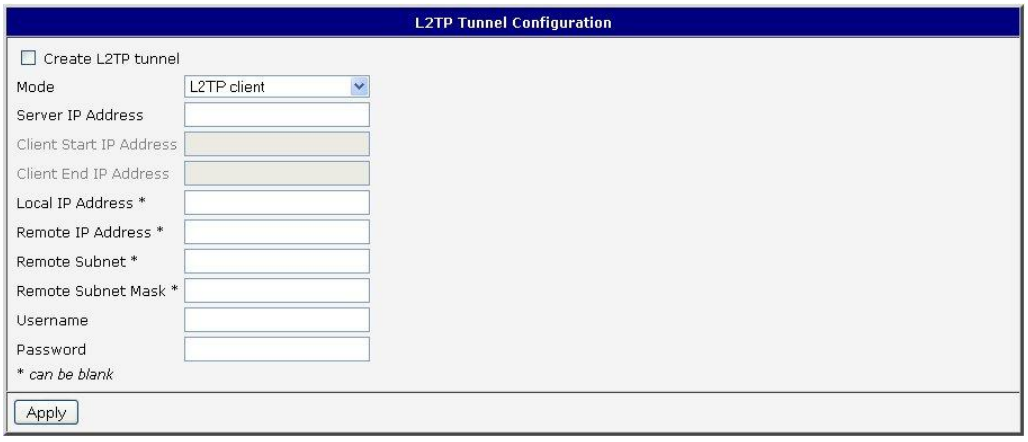


Figure 45: L2TP Tunnel Configuration

4.13.1 Example of the L2TP Tunnel Configuration

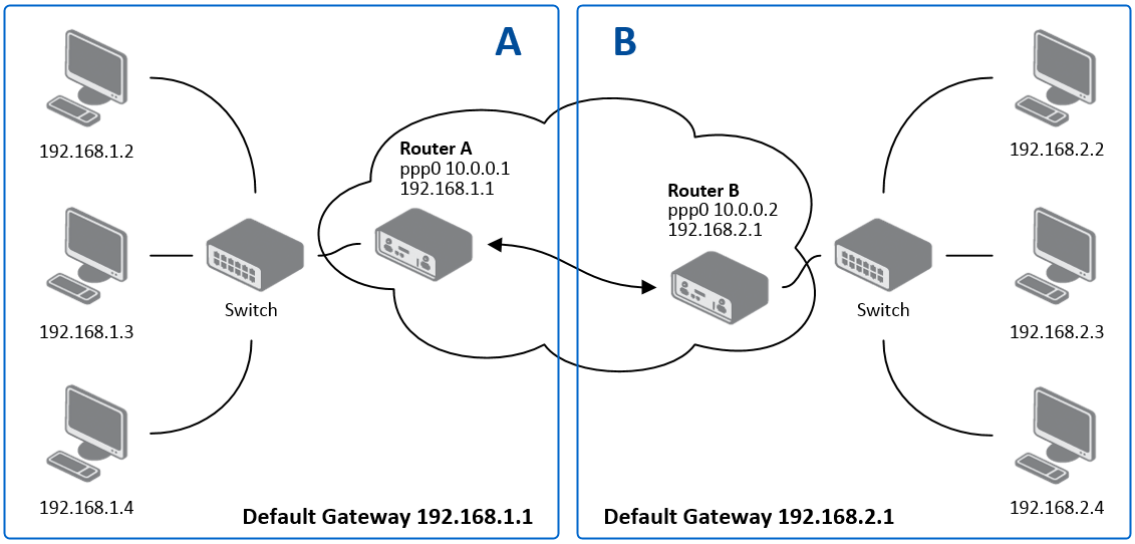


Figure 46: Topology of L2TP Tunnel Configuration Example

Configuration of the L2TP tunnel:

Configuration	A	B
Mode	L2TP Server	L2TP Client
Server IP Address	—	10.0.0.1
Client Start IP Address	192.168.2.5	—
Client End IP Address	192.168.2.254	—
Local IP Address	192.168.1.1	—
Remote IP Address	—	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 46: L2TP Tunnel Configuration Example

4.14 PPTP Tunnel Configuration

PPTP is an unencrypted protocol. PPTP via IPv6 is not supported.

Select the *PPTP* item in the menu to configure a PPTP tunnel. PPTP tunnel allows password protected connections between two LANs. It is similar to L2TP. The tunnels are active after selecting *Create PPTP tunnel*.

Item	Description
Mode	Specifies the L2TP tunnel mode on the router side: • **PPTP server** – Specify an IP address range offered by the server. • **PPTP client** – Specify the IP address of the server.
Server IP Address	IP address of the server.
Local IP Address	IP address of the local side of the tunnel.
Remote IP Address	IP address of the remote side of the tunnel.
Remote Subnet	Address of the network behind the remote side of the tunnel.
Remote Subnet Mask	The mask of the network behind the remote side of the tunnel
Username	Username for the PPTP tunnel login.
Password	Password for the PPTP tunnel login. Enter valid characters only, see chap. 1.4.1!

Table 47: PPTP Tunnel Configuration

The changes in settings will apply after pressing the *Apply* button.

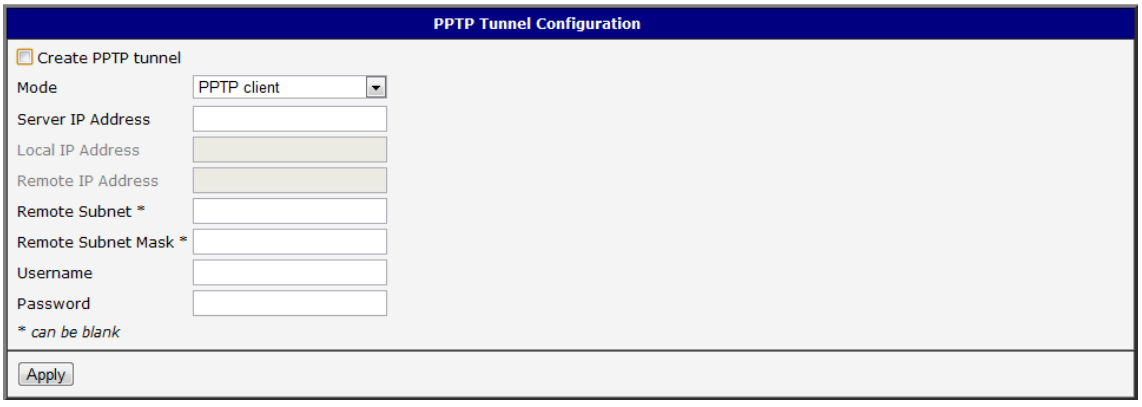


Figure 47: PPTP Tunnel Configuration

The firmware also supports PPTP passthrough, which means that it is possible to create a tunnel through the router.

4.14.1 Example of the PPTP Tunnel Configuration

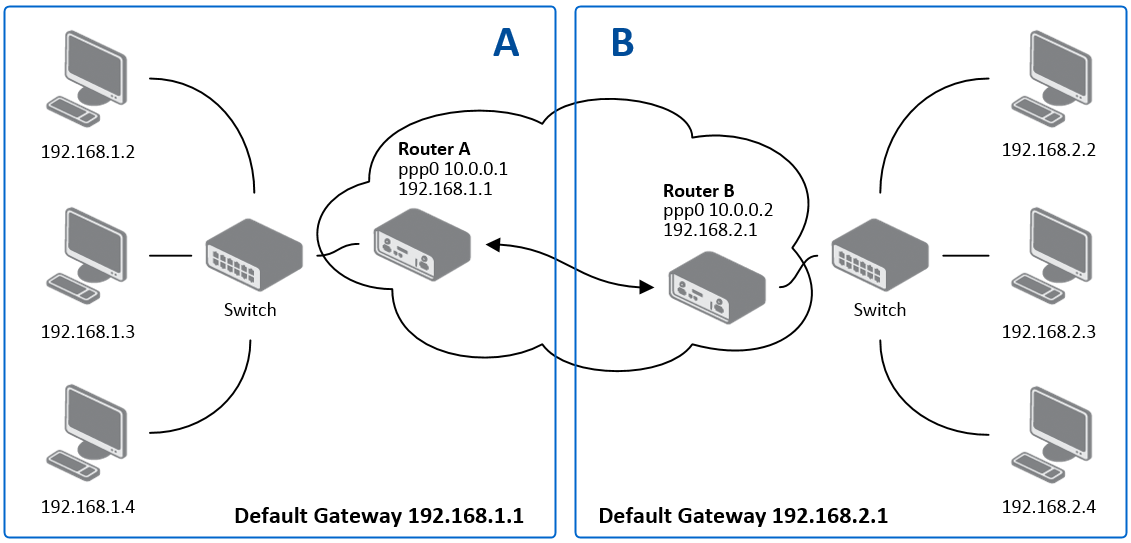


Figure 48: Topology of PPTP Tunnel Configuration Example

Configuration of the PPTP tunnel:

Configuration	A	B
Mode	PPTP Server	PPTP Client
Server IP Address	—	10.0.0.1
Local IP Address	192.168.1.1	—
Remote IP Address	192.168.2.1	—
Remote Subnet	192.168.2.0	192.168.1.0
Remote Subnet Mask	255.255.255.0	255.255.255.0
Username	username	username
Password	password	password

Table 48: PPTP Tunnel Configuration Example

4.15 Services

4.15.1 DynDNS

The DynDNS function allows you to access the router remotely using an easy to remember custom hostname. This DynDNS client monitors the IP address of the router and updates the address whenever it changes. In order for DynDNS to function, you require a public IP address, either static or dynamic, and an active Remote Access service account at www.dyndns.org. Register the custom domain (third-level) and account information specified in the configuration form. You can use other services, too – see the table below, Server item. To open the *DynDNS Configuration* page, click *DynDNS* in the main menu.

Item	Description
Hostname	The third order domain registered on the www.dyndns.org server.
Username	Username for logging into the DynDNS server.
Password	Password for logging into the DynDNS server. Enter valid characters only, see chap. 1.4.1!
IP Mode	Specifies the version of IP protocol: • **IPv4** – IPv4 protocol is used only (default). • **IPv6** – IPv6 protocol is used only. • **IPv4/IPv6** – IPv4 and IPv6 dual stack is enabled.
Server	Specifies a DynDNS service other than the www.dyndns.org. Possible other services: www.spdns.de, www.dnsdynamic.org, www.noip.com Enter the update server service information in this field. If you leave this field blank, the default server members.dyndns.org will be used.

Table 49: DynDNS Configuration

Example of the DynDNS client configuration with the domain company.dyndns.org:

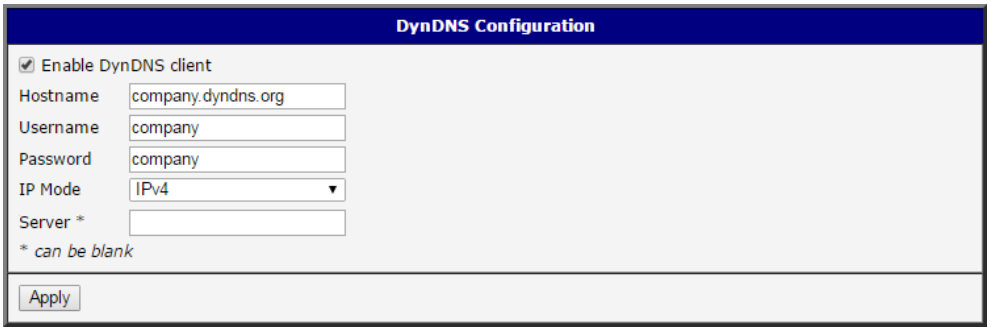


Figure 49: DynDNS Configuration Example

To access the router's configuration remotely, you will need to have enabled this option in the NAT configuration (bottom part of the form), see chapter 4.9.

4.15.2 FTP

FTP protocol (File Transfer Protocol) can be used to transfer files between the router and another device on the computer network. Configuration form of TP server can be done in *FTP* configuration page under *Services* menu item. By ticking *Enable FTP service* item the FTP server on the router is enabled.

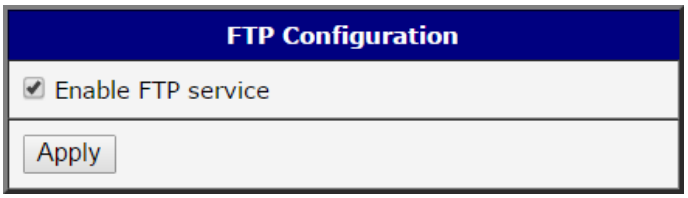


Figure 50: Enabling of FTP server

4.15.3 HTTP

HTTP protocol (Hypertext Transfer Protocol) is internet protocol used for exchange of hypertext documents in HTML format. This protocol is used for accessing the web server used for user's configuration of the router. Recommended usage however is of HTTPS protocol, which used encryption for secure exchange of transferred data. Configuration form of HTTP and HTTPS service can be done in *HTTP* configuration page under *Services* menu item. By default, HTTP service is disabled and preferred is using of HTTPS service. For this default setting, a request for communication with HTTP protocol is redirected to HTTPS protocol automatically.

Item	Description
Enable HTTP service	Enabling of HTTP service.
Enable HTTPS service	Enabling of HTTPS service.
Session Timeout	Inactivity timeout when the session is closed.
Keep the current certificate	Left the current one certificate in the router.
Generate a new certificate	Generate a new self-signed certificate to the router.
Upload a new certificate	Upload custom PEM certificate, which can be signed by Certificate Authority.
Certificate	Choose a file with the PEM certificate.
Private Key	Choose a file with the certificate private key.

Table 50: Parameters for HTTP and HTTPS services configuration

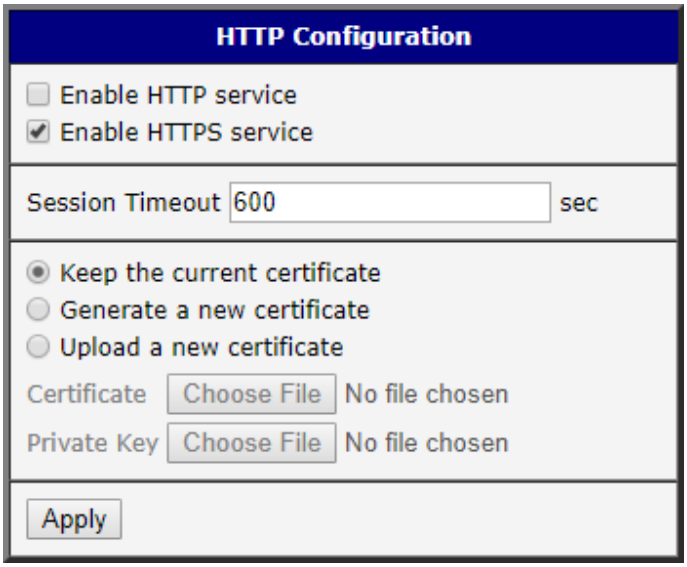


Figure 51: Configuration of HTTP and HTTPS services

4.15.4 NTP

The *NTP* configuration form allows you to configure the NTP client. To open the *NTP* page, click *NTP* in the *Configuration* section of the main menu. NTP (Network Time Protocol) allows you to periodically set the internal clock of the router. The time is set from servers that provide the exact time to network devices. IPv6 Time Servers are supported.

- If you mark the *Enable local NTP service* check box, then the router acts as a NTP server for other devices in the local network (LAN).
- If you mark the *Synchronize clock with NTP server* check box, then the router acts as a NTP client. This means that the router automatically adjusts the internal clock every 24 hours.

Item	Description
Primary NTP Server Address	IPv4 address, IPv6 address or domain name of primary NTP server.
Secondary NTP Server Address	IPv4 address, IPv6 address or domain name of secondary NTP server.
Timezone	Specifies the time zone where you installed the router.
Daylight Saving Time	Activates/deactivates the DST shift. • **No** – The time shift is inactive. • **Yes** – The time shift is active.

Table 51: NTP Configuration

The figure below displays an example of a NTP configuration with the primary server set to ntp.cesnet.cz and the secondary server set to tik.cesnet.cz and with the automatic change for daylight saving time enabled.

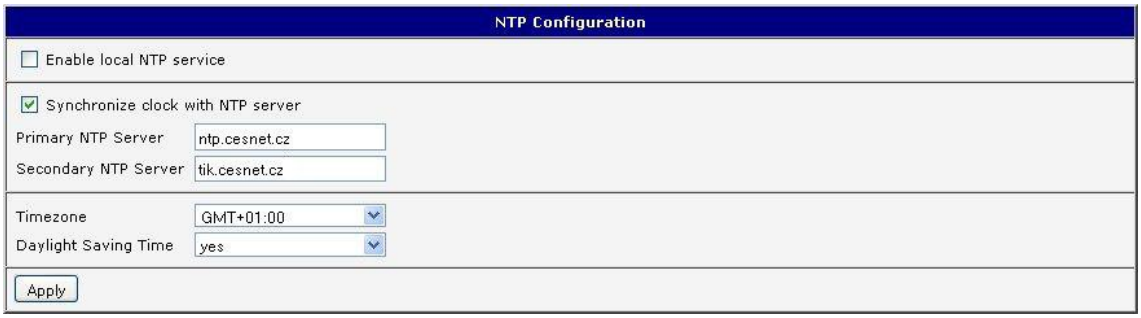


Figure 52: Example of NTP Configuration

4.15.5 SNMP

The *SNMP* page allows you to configure the SNMP v1/v2 or v3 agent which sends information about the router (and its expansion ports) to a management station. To open the *SNMP* page, click *SNMP* in the *Configuration* section of the main menu. SNMP (Simple Network Management Protocol) provides status information about the network elements such as routers or endpoint computers. In the version v3, the communication is secured (encrypted). To enable the SNMP service, mark the *Enable the SNMP agent* check box. Sending SNMP traps to IPv6 address is supported.

Item	Description
Name	Designation of the router.
Location	Location of where you installed the router.
Contact	Person who manages the router together with information how to contact this person.

Table 52: SNMP Agent Configuration

To enable the SNMPv1/v2 function, mark the *Enable SNMPv1/v2 access* check box. It is also necessary to specify a password for access to the *Community* SNMP agent. The default setting is *public*.

You can define a different password for the *Read* community (read only) and the *Write* community (read and write) for SNMPv1/v2. You can also define 2 SNMP users for SNMPv3. You can define a user as read only (*Read*), and another as read and write (*Write*). The router allows you to configure the parameters in the following table for every user separately. The router uses the parameters for SNMP access only.

To enable the SNMPv3 function, mark the *Enable SNMPv3 access* check box, then specify the following parameters:

Item	Description
Username	User name
Authentication	Encryption algorithm on the Authentication Protocol that is used to verify the identity of the users.
Authentication Password	Password used to generate the key used for authentication. Enter valid characters only, see chap. 1.4.1!
Privacy	Encryption algorithm on the Privacy Protocol that is used to ensure confidentiality of data.
Privacy Password	Password for encryption on the Privacy Protocol. Enter valid characters only, see chap. 1.4.1!

Table 53: SNMPv3 Configuration

Activating the *Enable I/O extension* function allows you monitor the binary I/O inputs on the router.

Selecting *Enable M-BUS extension* and entering the *Baudrate*, *Parity* and *Stop Bits* lets you monitor the meter status connected via MBUS interface. MBUS expansion port is not currently supported, but it is possible to use an external RS232/MBUS converter.

Selecting Enable reporting to supervisory system and entering the *IP Address* and *Period* lets you send statistical information to the monitoring system, R-SeeNet.

Item	Description
IP Address	IPv4 or IPv6 address.
Period	Period of sending statistical information (in minutes).

Table 54: SNMP Configuration (R-SeeNet)

Each monitored value is uniquely identified using a numerical identifier *OID – Object Identifier*. This identifier consists of a progression of numbers separated by a point. The shape of each OID is determined by the identifier value of the parent element and then this value is complemented by a point and current number. So it is obvious that there is a tree structure. The following figure displays the basic tree structure that is used for creating the OIDs.

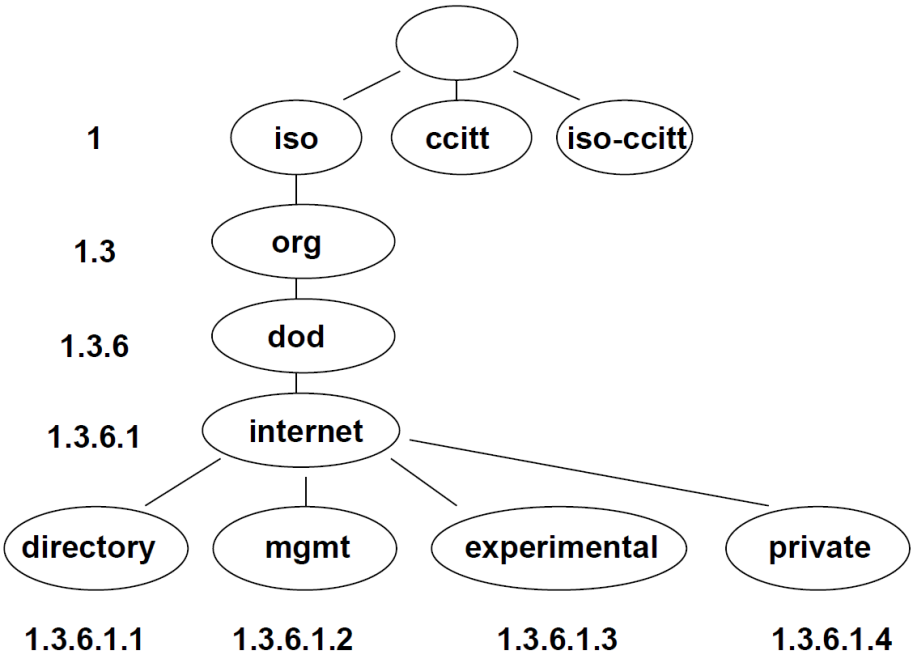


Figure 53: OID Basic Structure

The SNMP values that are specific for Hirschmann routers create the tree starting at OID = .1.3.6.1.4.1.30140. You interpret the OID in the following manner:

iso.org.dod.internet.private.enterprises.hirschmann

This means that the router provides for example, information about the internal temperature (OID 1.3.6.1.4.1.248.40.1.3.3) or about the power voltage (OID 1.3.6.1.4.1.248.40.1.3.4). For binary inputs and output, the following range of OID is used:

The list of available and supported OIDs and other details can be found in the application note *SNMP Object Identifier* [8].

OID	Description
.1.3.6.1.4.1.30140.2.3.1.0	Binary input BIN0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.2.0	Binary output OUT0 (values 0,1)
.1.3.6.1.4.1.30140.2.3.3.0	Binary input BIN1 (values 0,1)

Table 55: Object identifier for binary inputs and output

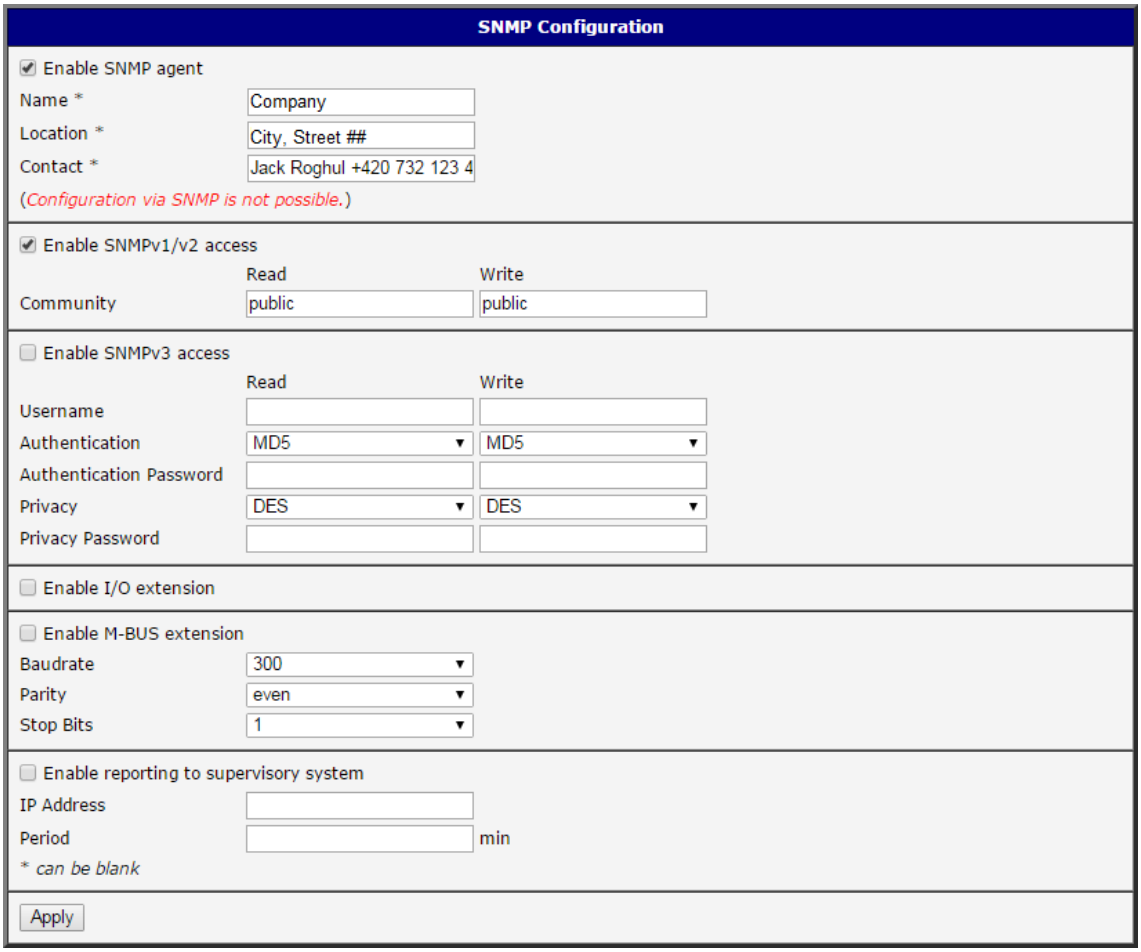


Figure 54: SNMP Configuration Example

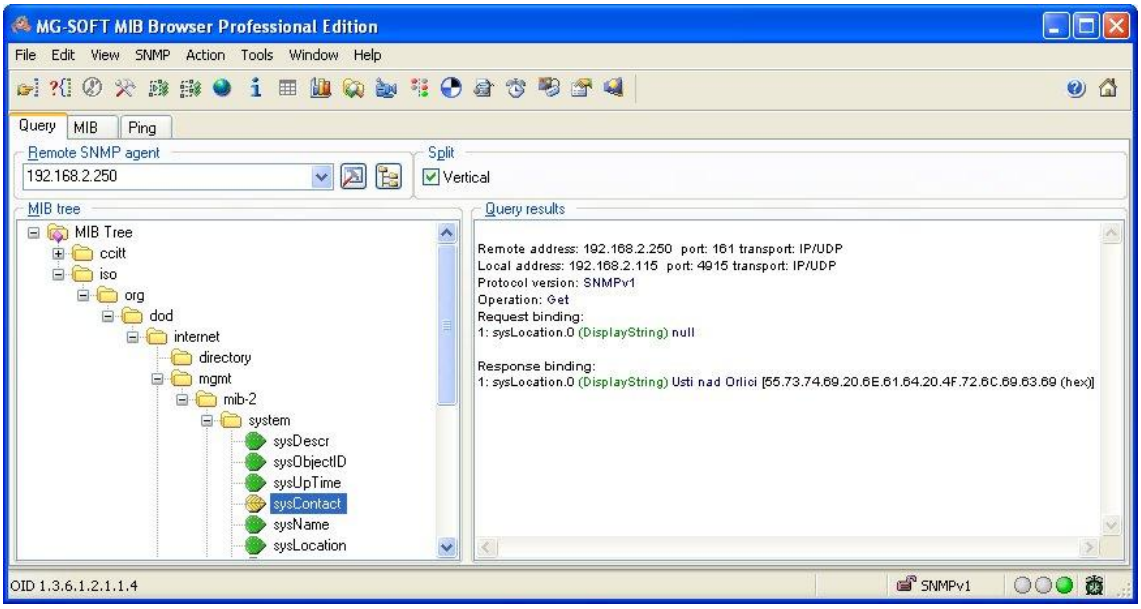


Figure 55: MIB Browser Example

In order to access a particular device enter the IP address of the SNMP agent which is the router, in the *Remote SNMP agent* field. The dialog displayed the internal variables in the MIB tree after entering the IP address. Furthermore, you can find the status of the internal variables by entering their OID.

The path to the objects is:

iso → org → dod → internet → private → enterprises → hirschmann → protocols

The path to information about the router is:

iso → org → dod → internet → mgmt → mib-2 → system

4.15.6 SMTP

Use the *SMTP* form to configure the Simple Mail Transfer Protocol client (SMTP) for sending e-mails. IPv6 e-mail servers are supported.

Item	Description
SMTP Server Address	IPv4 address, IPv6 address or domain name of the mail server.
SMTP Port	Port the SMTP server is listening on.
Secure Method	none, SSL/TLS, or STARTTLS. Secure method has to be supported by the SMTP server.
Username	Name for the e-mail account.
Password	Password for the e-mail account. Enter valid characters only, see chap. 1.4.1!
Own E-mail Address	Address of the sender.

Table 56: SMTP client configuration

The mobile service provider can block other SMTP servers, then you can only use the SMTP server of the service provider.

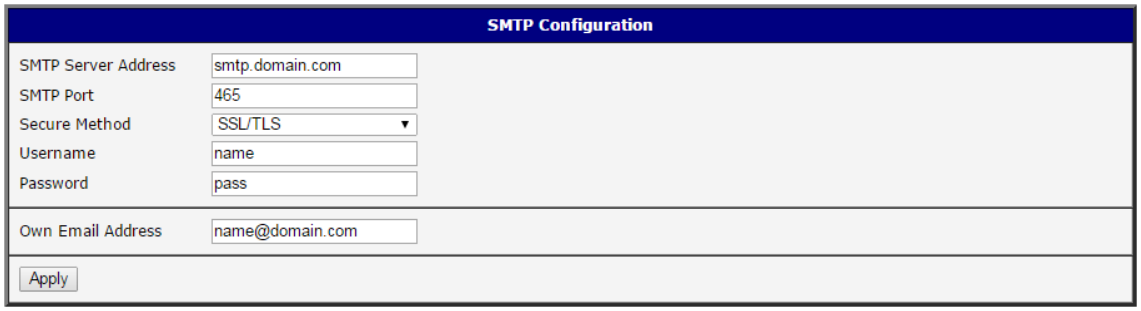


Figure 56: SMTP Client Configuration Example

You can send e-mails from the Startup script. The *Startup Script* dialog is located in *Scripts* in the *Configuration* section of the main menu. The router also allows you to send e-mails using an SSH connection. Use the email command with the following parameters:

-t e-mail address of the receiver
-s subject, enter the subject in quotation marks
-m message, enter the subject in quotation marks
-a attachment file
-r number of attempts to send e-mail (default setting: 2)

Commands and parameters can be entered only in lowercase.

Example of sending an e-mail:

```
email -t john@doe.com -s "System Log" -m "Attached" -a /var/log/messages
```

The command above sends an e-mail to address *john@doe.com* with the subject *"System Log"*, body message *"Attached"* and attachment *messages* file with *System Log* of the router directly from the directory /var/log/.

4.15.7 SMS

Open the *SMS* page in the *Services* submenu of the *Configuration* section of the main menu. The router can automatically send SMS messages to a cell phone or SMS message server when certain events occur. The form allows you to select which events generate an SMS message.

Item	Description
Send SMS on power up	Activates/deactivates the sending of an SMS message automatically on power up.
Send SMS on connect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is connected to a mobile network.
Send SMS on disconnect to mobile network	Activates/deactivates the sending of an SMS message automatically when the router is disconnection from a mobile network.
Send SMS when datalimit exceeded	Activates/deactivates the sending of an SMS message automatically when the data limit exceeded.
Send SMS when binary input on I/O port (BIN0) is active	Automatic sending SMS message after binary input on I/O port (BIN0) is active. Text of message is intended parameter BIN0.
Add timestamp to SMS	Activates/deactivates the adding a time stamp to the SMS messages. This time stamp has a fixed format YYYY-MM-DD hh:mm:ss.
Phone Number 1	Specifies the phone number to which the router sends the generated SMS.
Phone Number 2	Specifies the phone number to which the router sends the generated SMS.
Phone Number 3	Specifies the phone number to which the router sends the generated SMS.
Unit ID	The name of the router. The router sends the name in the SMS.
BIN0 – SMS	Text of the SMS message the binary input is activated.

Table 57: SMS Configuration

Remote Control via SMS

After you enter a phone number in the *Phone Number 1* field, the router allows you to configure the control of the device using an SMS message. You can configure up to three numbers for incoming SMS messages. To enable the function, mark the *Enable remote control via SMS* check box. The default setting of the remote control function is active.

Item	Description
Phone Number 1	Specifies the first phone number allowed to access the router using an SMS.
Phone Number 2	Specifies the second phone number allowed to access the router using an SMS.
Phone Number 3	Specifies the third phone number allowed to access the router using an SMS.

Table 58: Control via SMS

- If you leave the phone number field blank, then you can still restart the router using an SMS Reboot message from any phone number.
- If you enter one or more phone numbers, then you can control the router using SMS messages sent only from the specified phone numbers.
- If you enter the wild card character $*$, then you can control the router using SMS messages sent from any phone number.

Most of the control SMS messages do not change the router configuration. For example, if the router is changed to the off line mode using an SMS message, the router remains in this mode, but it will return back to the on-line mode after reboot. The only exception is *set profile* command that changes the configuration permanently, see the table below.

To control the router using an SMS, send only message text containing the control command. You can send control SMS messages in the following form:

SMS	Description
go online sim 1	The router changes to SIM1
go online sim 2	The router changes to SIM2
go online	Changes the router to the online mode
go offline	Changes the router to the off line mode
set out0=0	Sets the binary output to 0
set out0=1	Sets the binary output to 1
set profile std	Sets the standard profile. This change is permanent.
set profile alt1	Sets the alternative profile 1. This change is permanent.
set profile alt2	Sets the alternative profile 2. This change is permanent.
set profile alt3	Sets the alternative profile 3. This change is permanent.

Continued on next page

Continued from previous page

SMS	Description
reboot	The router reboots
get ip	The router responds with the IP address of the SIM card

Table 59: Control SMS

Note: Every received control SMS is processed and then **deleted** from the router! This may cause a confusion when you want to use AT-SMS protocol for reading received SMS (see section below).

Advanced SMS control: If there is unknown command in received SMS and remote control via SMS is enabled, the script located in "/var/scripts/sms" is run before the SMS is deleted. It is possible to define your own additional SMS commands using this script. Maximum of 7 words can be used in such SMS. Since the script file is located in RAM of the router, it is possible to add creation of such file to Startup Script. See example in the "Commands and Scripts" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

AT-SMS Protocol

AT-SMS protocol is a private set of AT commands supported by the routers. It can be used to access the cellular module in the router directly via commonly used AT commands, work with short messages (send SMS) and cellular module state information and settings.

Choosing *Enable AT-SMS protocol on expansion port 1* and *Baudrate* makes it possible to use AT-SMS protocol on the serial Port 1.

Item	Description
Baudrate	Communication speed on the expansion port 1

Table 60: Send SMS on the serial Port 1

Choosing *Enable AT-SMS protocol on expansion port 2* and *Baudrate* makes it possible to use AT-SMS protocol on the serial Port 2.

Item	Description
Baudrate	Communication speed on the expansion port 2

Table 61: Send SMS on the serial Port 2

Setting the parameters in the *Enable AT-SMS protocol over TCP* frame, you can enable the router to use AT-SMS protocol on a TCP port. This function requires you to specify a TCP port number.

Item	Description
TCP Port	TCP port on which will be allowed to send/receive SMS messages.

Table 62: Sending/receiving of SMS on TCP port specified

If you establish a connection to the router using a serial interface or Ethernet (TCP), then you can use AT commands to manage SMS messages.

Only the commands supported by the routers are listed in the following table. For other AT commands the OK response is always sent. There is no support for treatment of complex AT commands, so in such a case the router sends ERROR response.

AT Command	Description
AT+CGMI	Returns the manufacturer specific identity
AT+CGMM	Returns the manufacturer specific model identity
AT+CGMR	Returns the manufacturer specific model revision identity
AT+CGPADDR	Displays the IP address of the Mobile WAN interface
AT+CGSN	Returns the product serial number
AT+CIMI	Returns the International Mobile Subscriber Identity number (IMSI)
AT+CMGD	Deletes a message from the location
AT+CMGF	Sets the presentation format of short messages
AT+CMGL	Lists messages of a certain status from a message storage area
AT+CMGR	Reads a message from a message storage area
AT+CMGS	Sends a short message from the device to entered tel. number
AT+CMGW	Writes a short message to SIM storage
AT+CMSS	Sends a message from SIM storage location value
AT+CNUM	Returns the phone number, if available (stored on SIM card)
AT+COPS?	Identifies the available mobile networks
AT+CPIN	Is used to find out the SIM card state and enter a PIN code
AT+CPMS	Selects SMS memory storage types, to be used for short message operations
AT+CREG	Displays network registration status
AT+CSCA	Sets the short message service centre (SMSC) number

Continued on next page

Continued from previous page

AT Command	Description
AT+CSCS	Selects the character set
AT+CSQ	Returns the signal strength of the registered network
AT+GMI	Returns the manufacturer specific identity
AT+GMM	Returns the manufacturer specific model identity
AT+GMR	Returns the manufacturer specific model revision identity
AT+GSN	Returns the product serial number
ATE	Determines whether or not the device echoes characters
ATI	Transmits the manufacturer specific information about the device

Table 63: List of AT Commands

A detailed description and examples of these AT commands can be found in the "AT Commands" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

Sending SMS from Router

There are more ways how to send your own SMS from the router:

- Using AT-SMS protocol described above – if you establish a connection to the router using a serial interface or Ethernet (TCP), then you can use AT commands to send and manage SMS messages. See "AT Commands" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.
- Using HTTP POST method for a remote execution, calling CGI scripts in the router. For more details and examples, see the "Commands and Scripts" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.
- From Web interface of the router, in *Administration* section, *Send SMS* item, see Chapter 6.8.
- Using `gsmsms` command e.g. in terminal when connected to the router via SSH, see the "Commands and Scripts" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

Examples of SMS Configuration

Example 1 Sending SMS Configuration

After powering up the router, the phone with the number entered in the dialog receives an SMS in the following form:

Router (Unit ID) has been powered up. Signal strength –xx dBm.

After connecting to mobile network, the phone with the number entered in the dialog receives an SMS in the following form:

Router (Unit ID) has established connection to mobile network. IP address xxx.xxx.xxx.xxx

After disconnecting from the mobile network, the phone with the number entered in the dialog receives an SMS in the following form:

Router (Unit ID) has lost connection to mobile network. IP address xxx.xxx.xxx.xxx

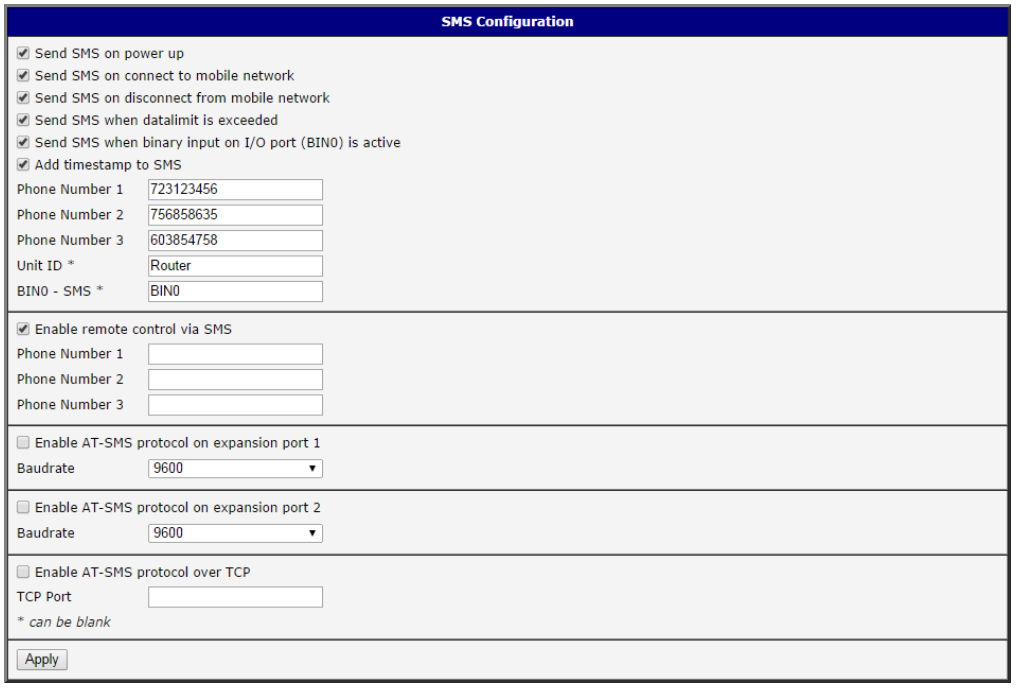


Figure 57: SMS Configuration for Example 1

Example 2 Sending SMS via Serial Interface on the Port 1

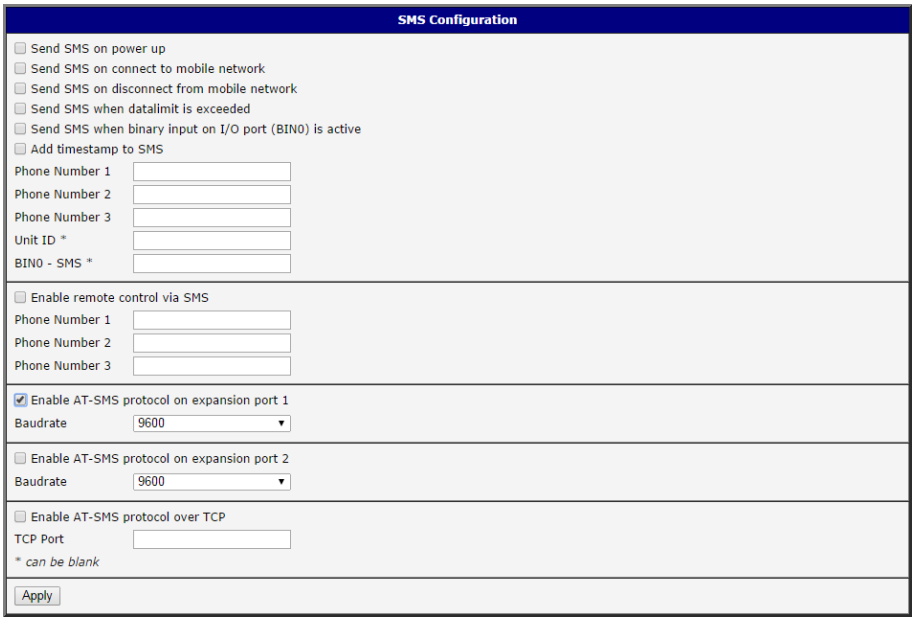


Figure 58: SMS Configuration for Example 2

Example 3 Control the Router Sending SMS from any Phone Number

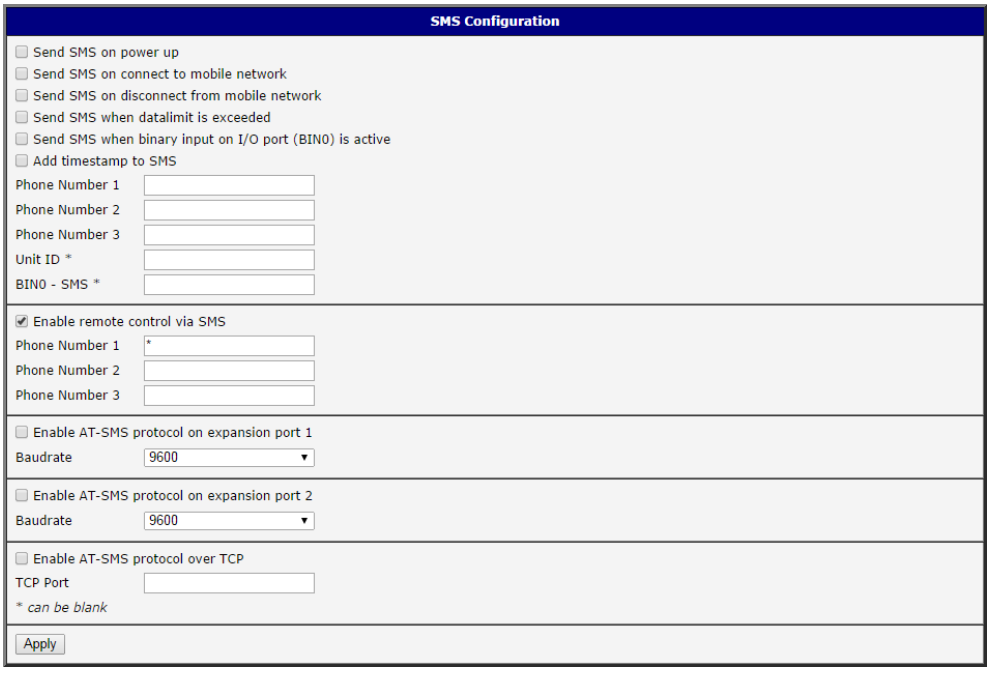


Figure 59: SMS Configuration for Example 3

Example 4 Control the Router Sending SMS from Two Phone Numbers

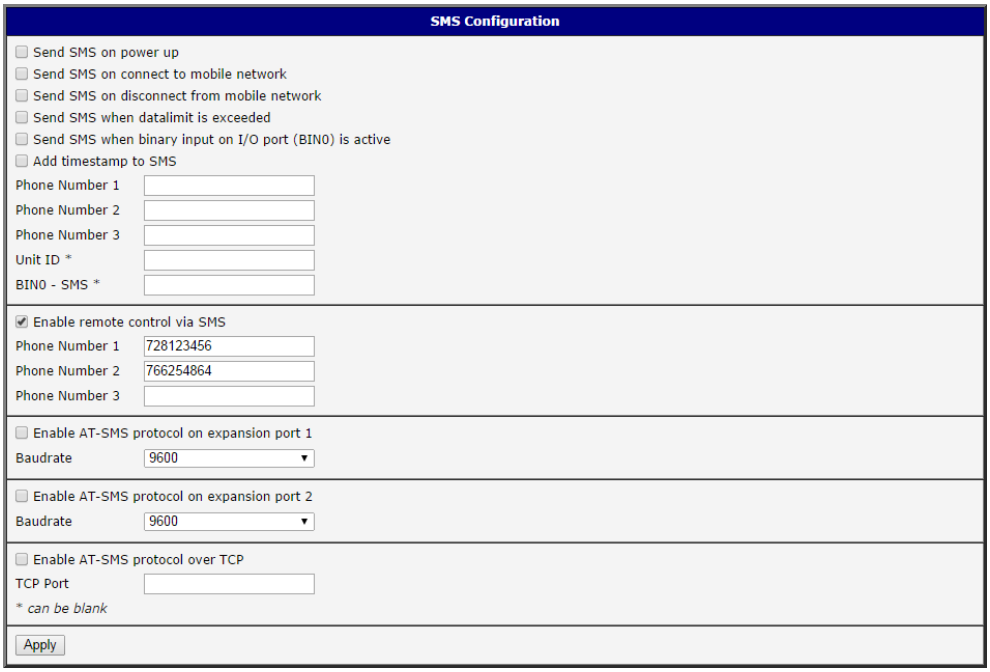


Figure 60: SMS Configuration for Example 4

4.15.8 SSH

SSH protocol (Secure Shell) allows to carry out a secure remote login to the router. Configuration form of SSH service can be done in *SSH* configuration page under *Services* menu item. By ticking *Enable SSH service* item the SSH server on the router is enabled.

Item	Description
Enable SSH service	Enabling of SSH service.
Session Timeout	Inactivity timeout when the session is closed.

Table 64: Parameters for SSH service configuration

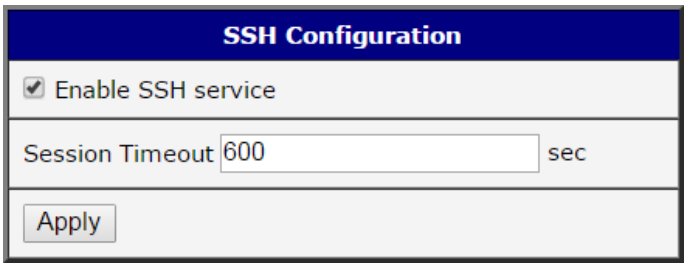


Figure 61: Configuration of HTTP service

4.15.9 Syslog

Configuration of system log, called syslog, can be done on this configuration page. Size of this log can be restricted by maximal number of its rows. Optionally, the IP address and UDP port can be configured for the real-time log distribution.

Položka	Popis
Log Size	Log size restriction by maximal number of its rows.
Remote IP Address	Optional settings of IP address for real-time log distribution.
Remote UDP Port	Optional settings of UDP port for real-time log distribution.

Table 65: Syslog configuration

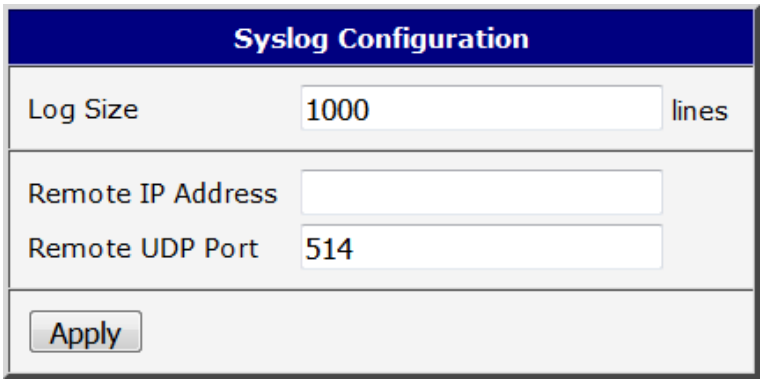


Figure 62: Syslog configuration

4.15.10 Telnet

Telnet is a protocol used to provide a bidirectional interactive text-oriented communication facility with the router. Configuration form of Telnet service can be done in *Telnet* configuration page under *Services* menu item. By ticking *Enable Telnet service* item the Telnet server on the router is enabled.

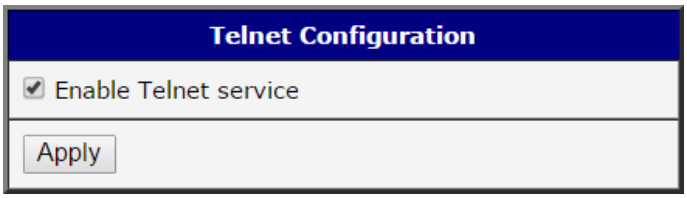


Figure 63: Enabling of Telnet service

4.16 Expansion Port – SERIAL I/O Configuration

Configuration of the **SERIAL I/O** connector can be done via *Expansion Port 1* and *Expansion Port 2* menu items. SERIAL I/O connector combines **RS232** and **RS485** serial interfaces with **Binary Input** and **Binary Output** on single 10-pin connector.

Configuration of RS232 interface is accessible on *Expansion Port 1* page, configuration of RS485 is accessible on *Expansion Port 2* page. See the self-explanation Figure below:

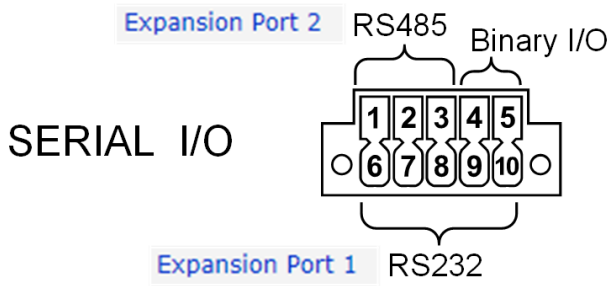


Figure 64: SERIAL I/O configuration pages overview

Binary input and output can be used multiple ways accross the router's configuration pages: SMS can be sent from router on binary input, binary output can be set by SMS (Chap. 4.15.7). State of binary I/O can be read by SNMP (Chap. 4.15.5). SIM cards can be switched on binary input (Chap. 4.2.1). Binary I/O can be read or set by commands in *Scripts* (see more in Chap. 4.17 and Application Note *Commands and Scripts* [1]).

Expansion Port 1 page configuration options are described below. Same configuration options are accessible at the *Expansion Port 2* page.

In the upper part of the configuration window, the port can be enabled and the type of the connected port is shown in the *Port Type* item. Other items are described in the table below. IPv6 TCP/UDP client/server are supported.

Item	Description
Baudrate	Applied communication speed.
Data Bits	Number of data bits.
Parity	Control parity bit: • **none** – data will be sent without parity. • **even** – data will be sent with even parity. • **odd** – data will be sent with odd parity.
Stop Bits	Number of stop bits.
Split Timeout	Time to rupture reports. If the gap between two characters exceeds the parameter in milliseconds, any buffered characters will be sent over the Ethernet port.

Continued on next page

Continued from previous page

Item	Description
Protocol	Protocol: • **TCP** – communication using a linked protocol TCP. • **UDP** – communication using a unlinked protocol UDP.
Mode	Mode of connection: • **TCP server** – The router will listen for incoming TCP connection requests. • **TCP client** – The router will connect to a TCP server on the specified IP address and TCP port.
Server Address	When set to *TCP client* above, it is necessary to enter the *Server address* and *TCP port*. IPv4 and IPv6 addresses are allowed.
TCP Port	TCP/UDP port used for communications. The router uses the value for both the server and client modes.
Inactivity Timeout	Time period after which the TCP/UDP connection is interrupted in case of inactivity.

Table 66: Expansion Port Configuration – serial interface

If you mark the *Reject new connections* check box, then the router rejects any other connection attempt. This means that the router no longer supports multiple connections.

If you mark the *Check TCP connection* check box, the router verifies the TCP connection.

Item	Description
Keepalive Time	Time after which the router verifies the connection.
Keepalive Interval	Length of time that the router waits on an answer.
Keepalive Probes	Number of tests that the router performs.

Table 67: Expansion Port Configuration – *Check TCP connection*

When you mark the *Use CD as indicator of the TCP connection* check box, the router uses the carrier detection (CD) signal to verify the status of the TCP connection. The CD signal verifies that another device is connected to the other side of the cable.

CD	Description
Active	TCP connection is enabled
Nonactive	TCP connection is disabled

Table 68: CD Signal Description

When you mark the *Use DTR as control of TCP connection* check box, the router uses the data terminal ready (DTR) single to control the TCP connection. The remote device sends a DTR single to the router indicating that the remote device is ready for communications.

DTR	Description server	Description client
Active	The router allows the establishment of TCP connections.	The router initiates a TCP connection.
Nonactive	The router denies the establishment of TCP connections.	The router terminates the TCP connection.

Table 69: DTR Signal Description

The changes in settings will apply after pressing the *Apply* button.

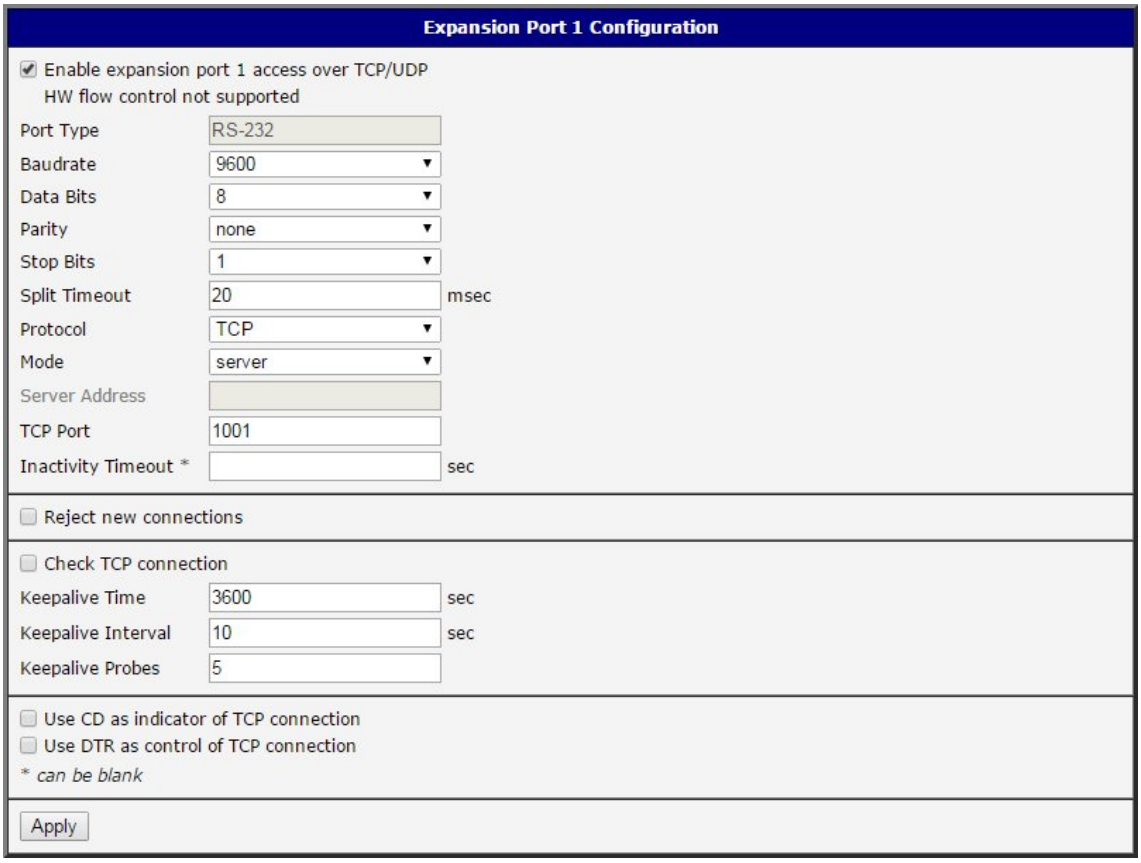


Figure 65: Expansion Port Configuration

4.16.1 Examples of the Expansion Port Configuration

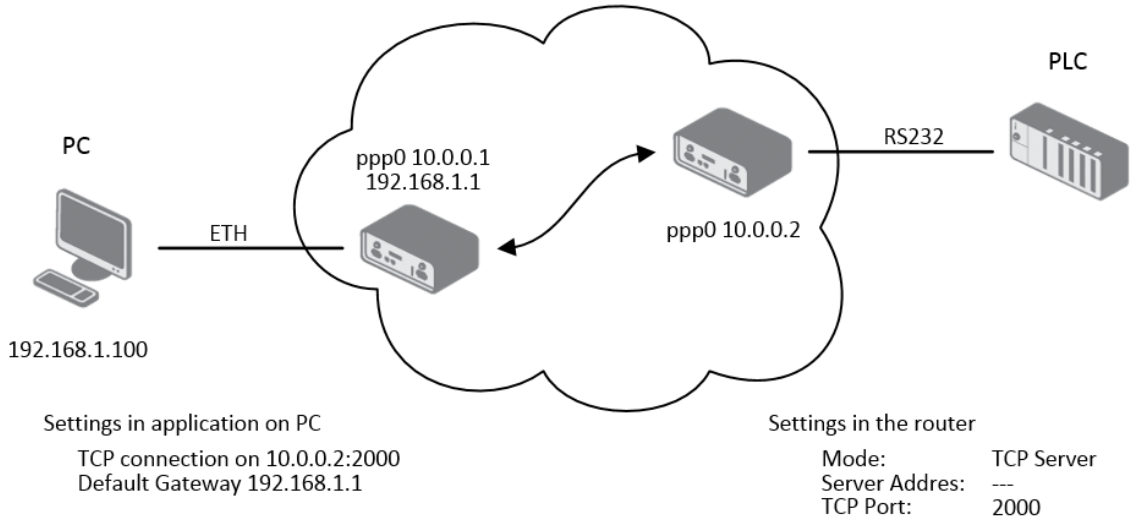


Figure 66: Example of Ethernet to serial communication configuration

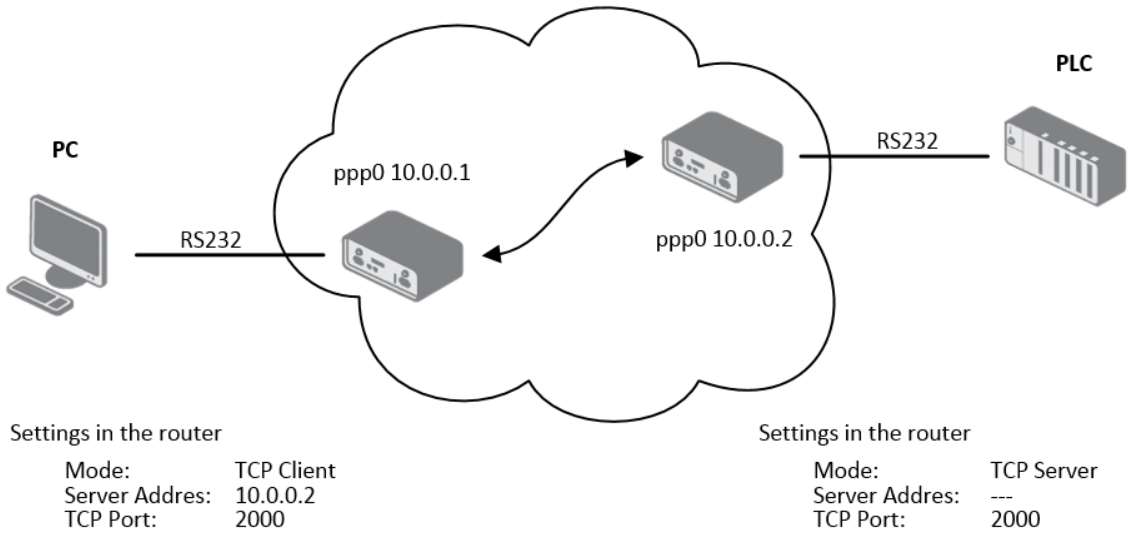


Figure 67: Example of serial interface configuration

4.17 Scripts

There is possibility to create your own shell scripts executed in the specific situations. Go to the *Scripts* page in the *Configuration* section in the menu. The menu item will expand and there are *Startup Script*, *Up/Down IPv4* and *Up/Down IPv6* scripts you can use – there is IPv4 and IPv6 independent dual stack. For more examples of Scripts and possible commands see the "Commands and Scripts" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

4.17.1 Startup Script

Use the *Startup Script* window to create your own scripts which will be executed after all of the initialization scripts are run – right after the router is turned on or rebooted. The changes in settings will apply after pressing the *Apply* button.

Any changes to the *Startup Script* will take effect the next time the router is power cycled or rebooted. This can be done with the *Reboot* button in the *Administration* section, or by SMS message.

4.17.2 Example of Startup Script

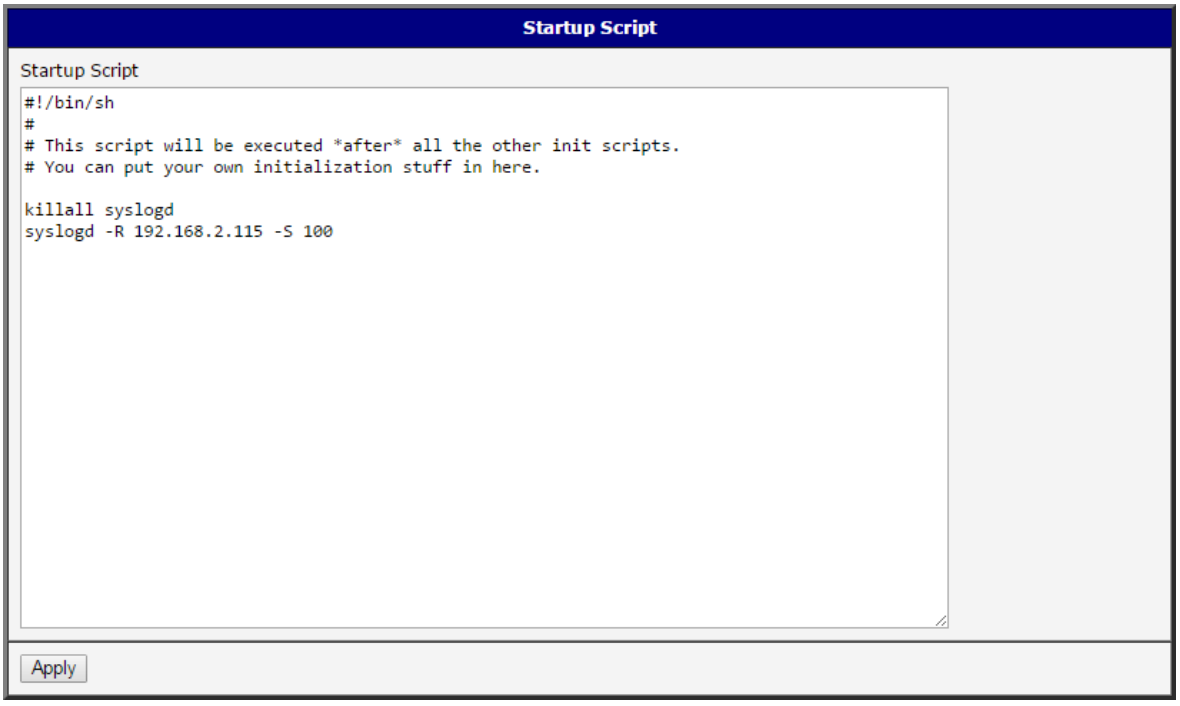


Figure 68: Example of a Startup Script

When the router starts up, stop syslogd program and start syslogd with remote logging on address 192.168.2.115 and limited to 100 entries. Add these lines to the *Startup Script*:

```
killall syslogd
syslogd -R 192.168.2.115 -S 100
```

4.17.3 Up/Down Scripts

Use the *Up/Down IPv4* and *Up/Down IPv6* page to create scripts executed when the Mobile WAN connection is established (up) or lost (down). There is independent IPv4 and IPv6 dual stack implemented in the router, so there is independent IPv4 and IPv6 Up/Down script. *IPv4 Up/Down Script* runs only on the IPv4 WAN connection established/lost, *IPv6 Up/Down Script* runs only on the IPv6 WAN connection established/lost. Any scripts entered into the *Up Script* window will run after a WAN connection is established. Script commands entered into the *Down Script* window will run when the WAN connection is lost.

The changes in settings will apply after pressing the *Apply* button. Also you need to reboot the router to make Up/Down Script work.

4.17.4 Example of IPv6 Up/Down Script

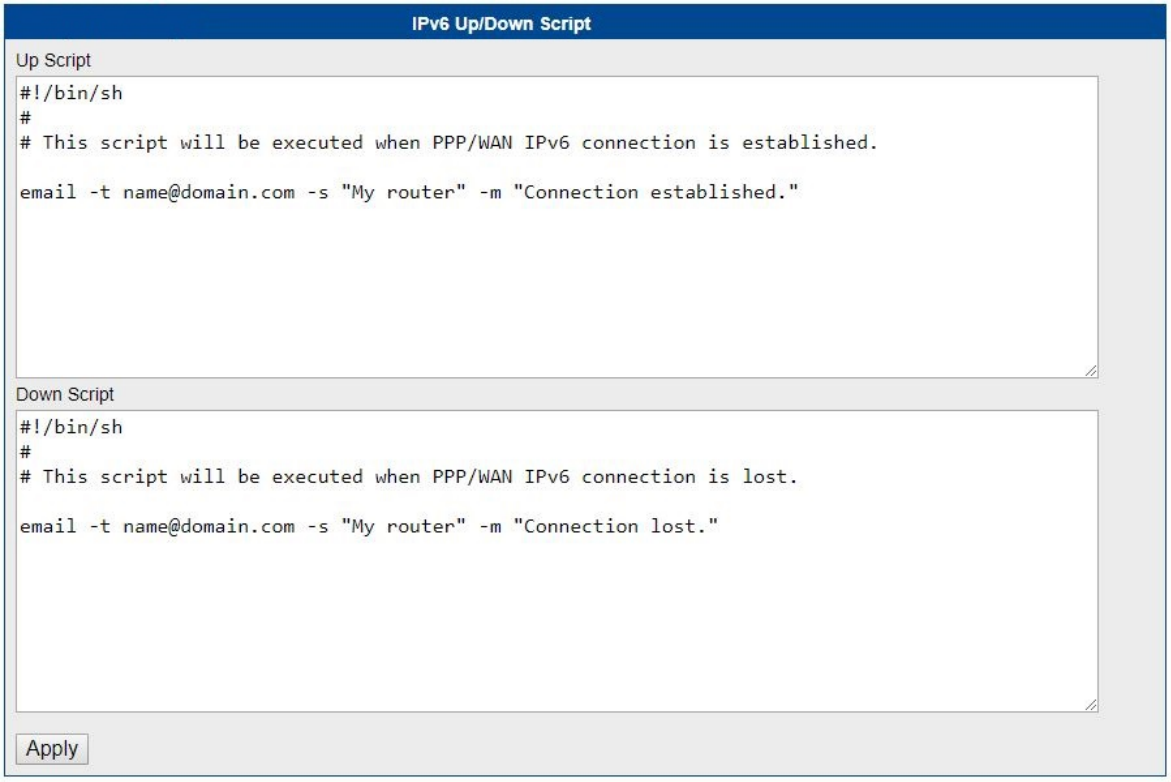


Figure 69: Example of IPv6 Up/Down Script

After establishing or losing an IPv6 WAN connection (connection to mobile network), the router sends an email with information about the connection state. It is necessary to configure *SMTP* before.

Add this line to the *Up Script* field:

```
email -t name@domain.com -s "Router" -m "Connection up."
```

Add this line to the *Down Script* field:

```
email -t name@domain.com -s "Router" -m "Connection down."
```

4.18 Automatic Update Configuration

Use the *Automatic Update* menu to configure the automatic update settings. The router can be configured to automatically check for firmware and configuration updates from a HTTP(S) or FTP(S) server. IPv6 sites/servers are supported. Used protocol is specified by an address in *Base URL* field: HTTP, HTTPS, FTP or FTPS. To prevent possible unwanted manipulation of the files, the router verifies that the downloaded file is in the tar.gz format. At first, the format of the downloaded file is checked. Then the type of architecture and each file in the archive (tar.gz file) is checked.

If the *Enable automatic update of configuration* option is selected, the router will check if there is a configuration file on the remote server, and if the configuration in the file is different than its current configuration, it will update its configuration to the new settings and reboot.

If the *Enable automatic update of firmware* option is checked, the router will look for a new firmware file and update its firmware if necessary.

Item	Description
Base URL	Base URL, IPv4 or IPv6 address from which the configuration file will be downloaded. This option also specifies the communication protocol (HTTP, HTTPS, FTP or FTPS (only implicit mode is supported)), see examples below.
Unit ID	Name of configuration (name of the file without extension). If the *Unit ID* is not filled, the MAC address of the router is used as the filename (the delimiter colon is used instead of a dot.)
Update Hour	Use this item to set the hour (range 1-24) when the automatic update will be performed every day. If the time is not specified, automatic update is performed five minutes after turning on the router and then every 24 hours. If the detected configuration file is different from the running one, it is downloaded and the router is restarted automatically.
Decryption Password	Password for decryption of crypted configuration file. This is required only in case the configuration is encrypted.
Update Window Start	Choose an hour (range from 1 to 24) when the automatic update will be performed on a daily basis. If the time is not specified (set to *dynamic*), the automatic update is performed five minutes after router boots up and then regularly every 24 hours.
Update Window Length	This value defines the period within the update will be done. This period starts at the time set in the *Update Window Start* field. The exact time, when the update will be done, is generated randomly.

Table 70: Automatic Update Configuration

The **configuration file** name consists of *Base URL*, hardware MAC address of ETH0 interface and cfg extension. Hardware MAC address and cfg extension are added to the file name automatically and it isn't necessary to enter them. When the parameter *Unit ID* is enabled, it defines the concrete configuration name which will be downloaded to the router, and the hardware MAC address in the configuration name will not be used.

The **firmware file** name consists of *Base URL*, type of router and bin extension. For the proper firmware filename, see the *Update Firmware* page in *Administration* section – it us written out there. See Chapter 6.11.

It is necessary to load two files (.bin and .ver) to the HTTP/FTP server. If only the .bin file is uploaded and the HTTP server sends the incorrect answer of *200 OK* (instead of the expected *404 Not Found*) when the device tries to download the nonexistent .ver file, then it can happen that the router will download the .bin file over and over again.

Firmware update can cause incompatibility with the user modules. It is recommended that you update user modules to the most recent version. Information about the user modules and the firmware compatibility is at the beginning of the user module's Application Note.

The automatic update feature is also executed five minutes after the firmware upgrade, regardless of the scheduled time.

4.18.1 Example of Automatic Update

The following example the router checks for new firmware or configuration file each day at 1:00 a.m. This example is given for the Hirschmann router.

- Firmware file: https://example.com/OWL-4G-EUANZ.bin
- Configuration file: https://example.com/test.cfg

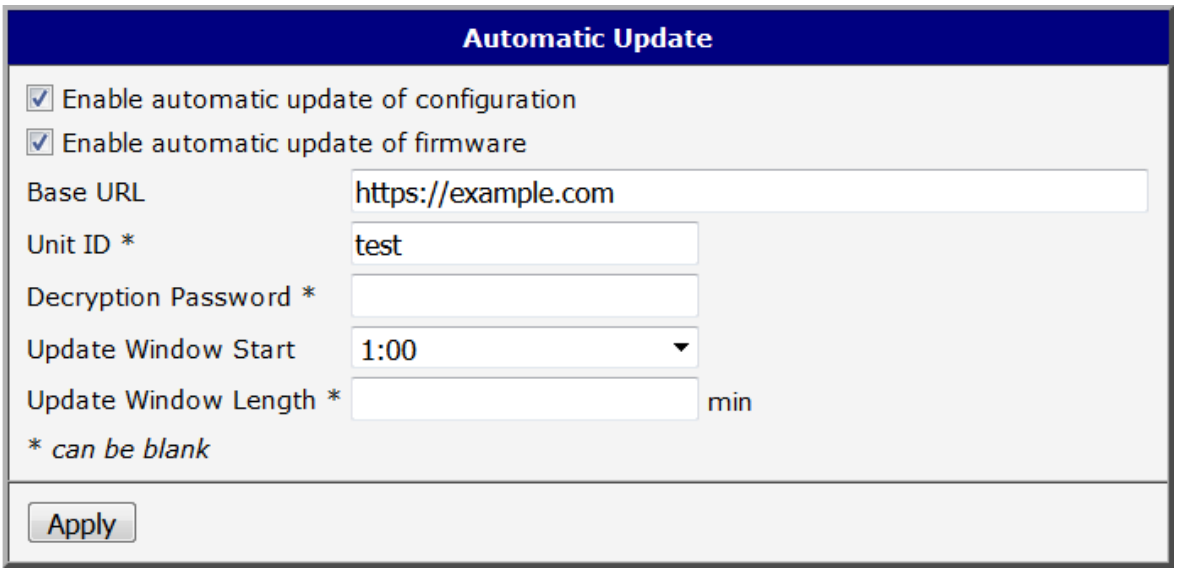


Figure 70: Example of Automatic Update 1

4.18.2 Example of Automatic Update Based on MAC

The following example checks for new firmware or configurations each day between 1:00 a.m. and 3:00 a.m. The configuratin file is encrypted, therefore the decryption password was configured. This example is given for the Hirschmann router with MAC address 00:11:22:33:44:55.

- Firmware file: https://example.com/OWL-4G-EUANZ.bin
- Configuration file: https://example.com/00.11.22.33.44.55.cfg

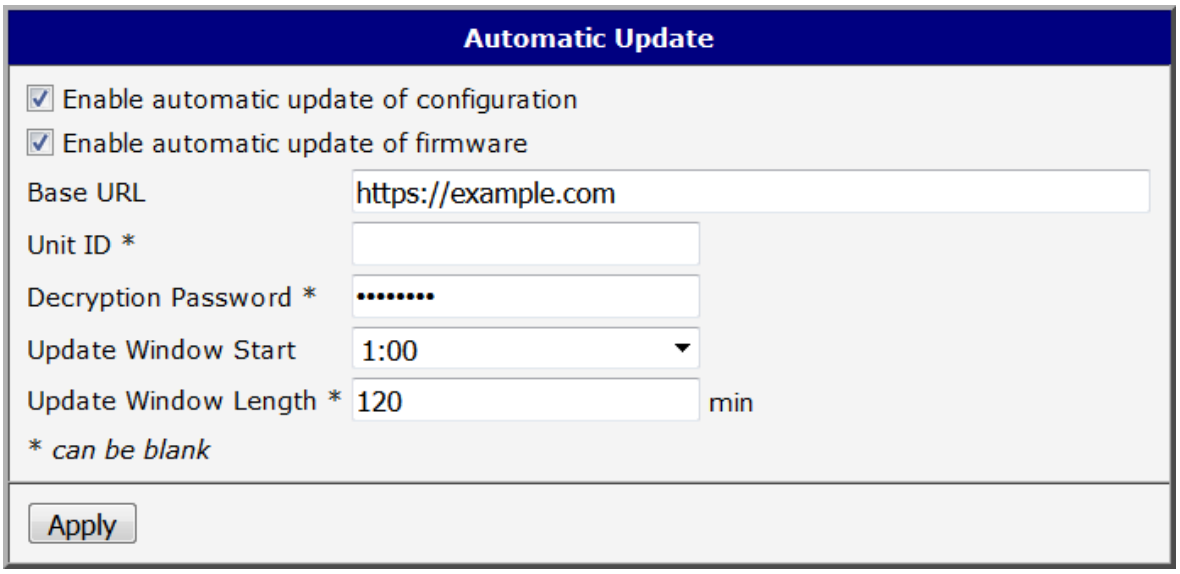


Figure 71: Example of Automatic Update 2

5 Customization

5.1 User Modules

You may run custom software programs in the router to enhance the features of the router. Use the *User Modules* menu item to add new software modules to the router, to remove them, or to change their configuration. Use the *Browse* button to select the user module (compiled module has tgz extension). Use the *Add* button to add a user module.

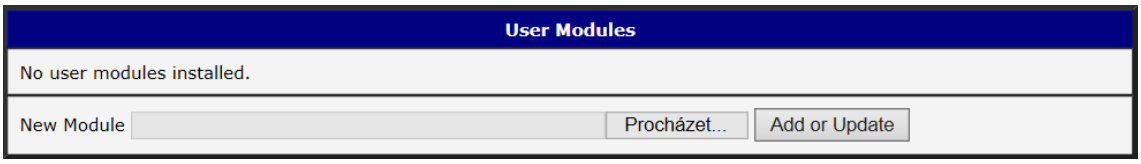


Figure 72: User modules

The new module appears in the list of modules on the same page. If the module contains an index.html or index.cgi page, the module name serves as a link to this page. The module can be deleted using the *Delete* button.

Updating a module is done the same way. Click the *Add* button and the module with the higher (newer) version will replace the existing module. The current module configuration is left in the same state.

Programming and compiling of modules is described in the "Programming of User Modules" application note. You can get the PDF at: https://hirschmann-support.belden.com.

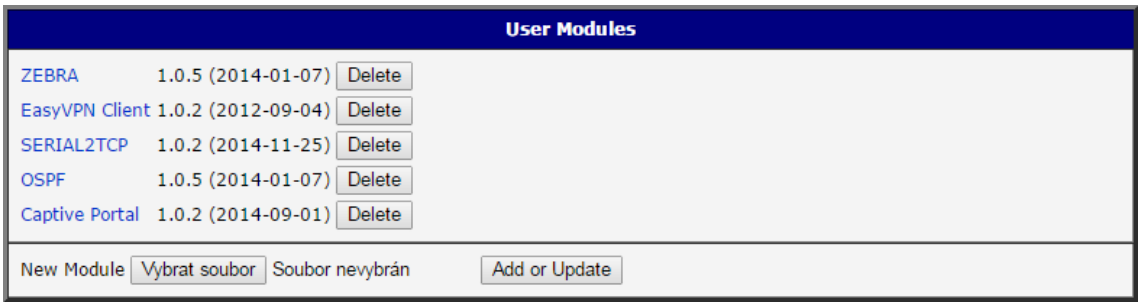


Figure 73: Added user module

User modules can be custom-programmed. Some typical user modules are prepared by Hirchmann and are available on the web site for the download.

In some cases the firmware update can cause incompatibility with installed user modules. Please refer to the release notes of the OWL firmware and of the user modules to check for compatibility.

Information about the user module and the firmware compatibility is at the beginning of the user module's Application Note.

6 Administration

6.1 Users

This configuration function is only available for users assigned the admin role!

To assign roles and manage user accounts open the *Users* form in the *Administration* section of the main menu. The first frame of this configuration form contains an overview of available users. The table below describes the meaning of the buttons in this frame.

Button	Description
Lock	Locks the user account. This user is not allowed to log in to the router, neither web interface nor SSH.
Change Password	Allows you to change the password for the corresponding user. Characters are not restricted.
Delete	Deletes the corresponding user account.

Table 71: Users Overview

If you lock every account with the permission role *Admin*, you can not unlock these accounts. This also means that the *Users* dialog is unavailable for every user, because every *admin* account is locked and the *users* do not have sufficient permissions.

The second block contains configuration form which allows you to add new user. All items are described in the table below.

Item	Description
Role	Specifies the type of user account: • **User** – User with basic permissions. • **Admin** – User with full permissions.
Username	Specifies the name of the user allowed to log in the device.
Password	Specifies the password for the corresponding user. Characters are not restricted.
Confirm Password	Confirms the password you specified above.

Table 72: Add User

Ordinary users are not able to access router via Telnet, SSH or SFTP. Read only FTP access is allowed for these users.

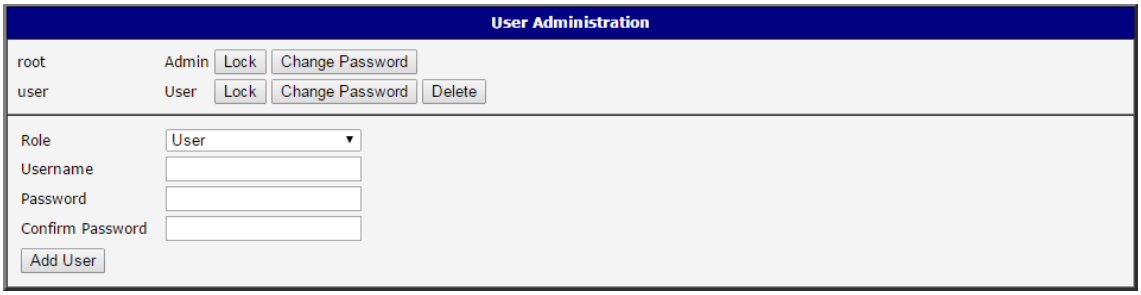


Figure 74: Users

6.2 Change Profile

In addition to the standard profile, up to three alternate router configurations or profiles can be stored in router's non-volatile memory. You can save the current configuration to a router profile through the *Change Profile* menu item. Select the alternate profile to store the settings to and ensure that the *Copy settings from current profile to selected profile* box is checked. The current settings will be stored in the alternate profile after the *Apply* button is pressed. Any changes will take effect after restarting router through the *Reboot* menu in the web administrator or using an SMS message.

Example of using profiles: Profiles can be used to switch between different modes of operation of the router such as PPP connection, VPN tunnels, etc. It is then possible to switch between these settings using the front panel binary input, an SMS message, or Web interface of the router.

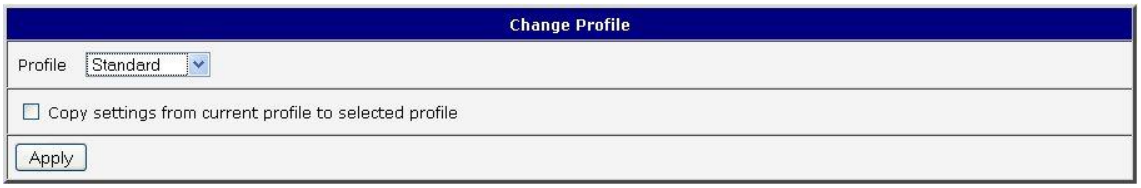


Figure 75: Change Profile

6.3 Change Password

Use the *Change Password* configuration form in the *Administration* section of the main menu for changing your password used to log on the device. Enter the new password in the *New Password* field, confirm the password using the *Confirm Password* field, and press the *Apply* button. Characters for the password are not restricted.

The default password of the router is **root** for the **root** user. To maintain the security of your network change the default password. You can not enable remote access to the router for example, in NAT, until you change the password.

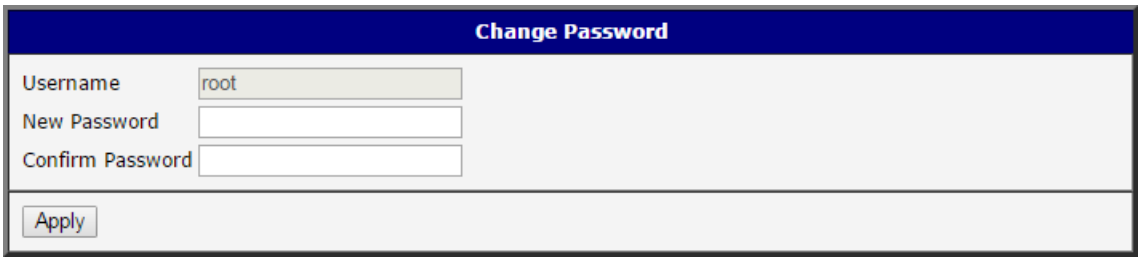


Figure 76: Change Password

6.4 Set Real Time Clock

You can set the internal clock directly using the *Set Real Time Clock* dialog in the *Administration* section of in the main menu. You can set the *Date* and *Time* manually. When entering the values manually use the format yyyy-mm-dd as seen in the figure below. You can also adjust the clock using the specified NTP server. IPv4, IPv6 address or domain name is supported. After you enter the appropriate values, click the *Apply* button.

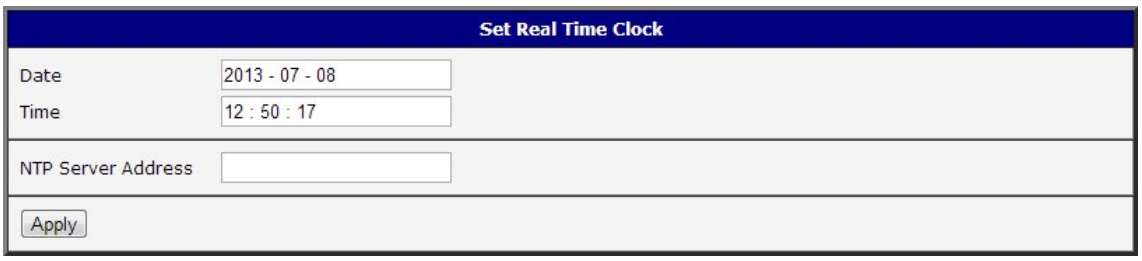


Figure 77: Set Real Time Clock

6.5 Set SMS Service Center Address

The function requires you to enter the phone number of the SMS service center to send SMS messages. To specify the SMS service center phone number use the *Set SMS Service Center* configuration form in the *Administration* section of the main menu. You can leave the field blank if your SIM card contains the phone number of the SMS service center by default. This phone number can have a value without an international prefix (xxx-xxx-xxx) or with an international prefix (+420-xxx-xxx-xxx). If you are unable to send or receive SMS messages, contact your carrier to find out if this parameter is required.

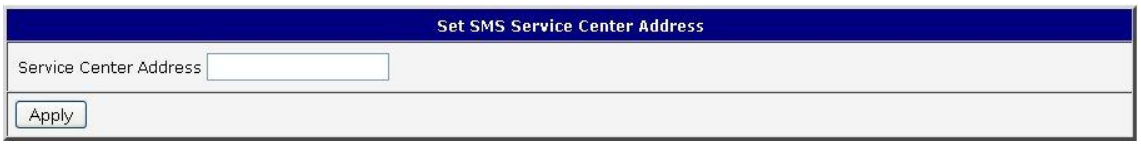


Figure 78: Set SMS Service Center Address

6.6 Unlock SIM Card

It is possible to use the SIM card protected by PIN number in the router – just fill in the PIN on the *Mobile WAN Configuration* page. Here you can remove the PIN protection (4–8 digit Personal Identification Number) from the SIM card, if your SIM card is protected by one. Open the *Unlock SIM Card* form in the *Administration* section of the main menu and enter the PIN number in the *SIM PIN* field, then click the *Apply* button. It is applied on the currently enabled SIM card, or on the first SIM card if there is no SIM card enabled at the moment.

The SIM card is blocked after three failed attempts to enter the PIN code. Unblocking of SIM card by PUK number is described in next chapter.

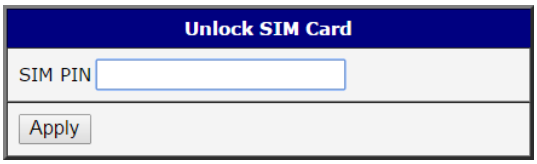


Figure 79: Unlock SIM Card

6.7 Unblock SIM Card

On this page you can unblock the SIM card after 3 wrong PIN attempts or change the PIN code of the SIM card. To unblock the SIM card, go to *Unblock SIM Card* administration page. In both cases enter the PUK code into *SIM PUK* field and new SIM PIN code into *New SIM PIN* field. To proceed click on *Apply* button. It is applied on the currently enabled SIM card, or on the first SIM card if there is no SIM card enabled at the moment.

The SIM card will be permanently blocked after the three unsuccessful attempts of the PUK code entering.

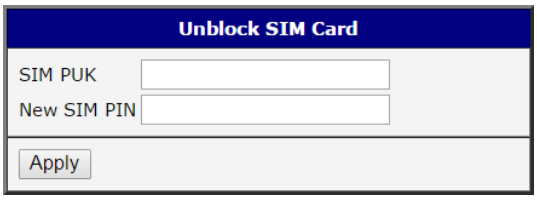


Figure 80: Unblock SIM Card

6.8 Send SMS

You can send an SMS message from the router to test the cellular network. Use the *Send SMS* dialog in the *Administration* section of the main menu to send SMS messages. Enter the *Phone number* and text of your message in the *Message* field, then click the *Send* button. The router limits the maximum length of an SMS to 160 characters. (To send longer messages, install the pduSMS user module).

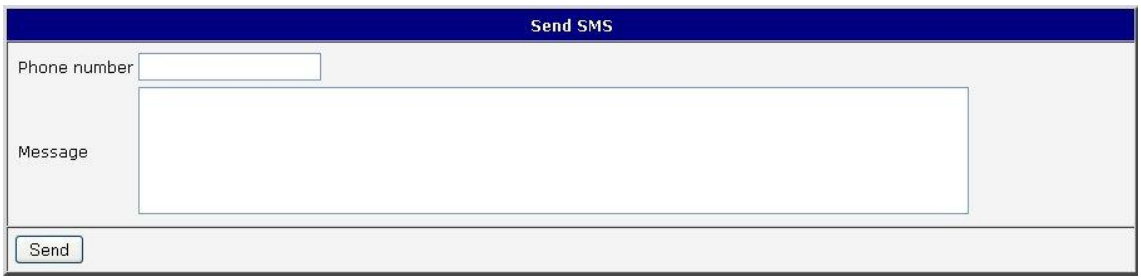


Figure 81: Send SMS

It is also possible to send an SMS message using CGI script. For details of this method, see the "Commands and Scripts" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

6.9 Backup Configuration

Keep in mind potential security issues when creating backup, especially for user accounts. Encrypted configuration or secured connection to the router should be used.

You can save actual configuration of the router using the *Backup Configuration* item in the *Administration* menu section. If you click on this item a configuration pane will open, see Figure 82. Here you can choose what will be backed up. You can back up configuration of the router (item *Configuration*) or configuration of all user accounts (item *Users*). Both types of the configuration can be backed up separately or at once into one configuration file.

It is recommended to save the configuration into an encrypted file. If the encryption password is not configured, the configuration is stored into an unencrypted file.

Click on *Apply* button and the configuration will be stored into configuration file (file with *cfg* extension) into a directory according the settings of the web browser. Stored configuration can be later used for its restoration, see chapter 6.10 for more information.

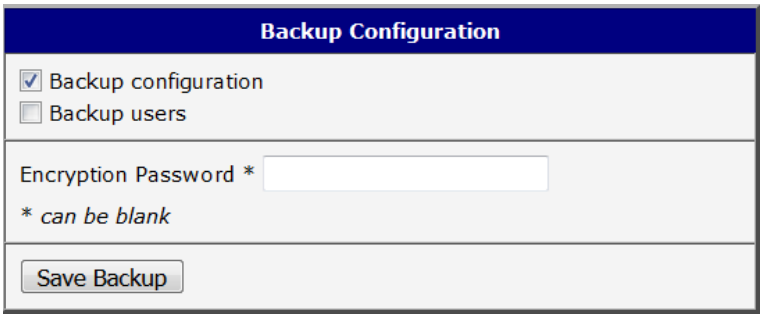


Figure 82: Backup Configuration

6.10 Restore Configuration

Due to the different format it is not possible to import user accounts backed up on a router of v1 product line (and older) to a router of v2 product line (and newer). The same limmitation is for opposite direction.

You can restore a configuration of the router stored into a file using the *Restore Configuration* form. Click on *Browse* button to navigate to the directory containing the configuration file you wish to load to the router. If the configuration was stored into an encrypted file, the decryption password must be set to decrypt the file successfully. To start the restoration process click on *Apply* button.

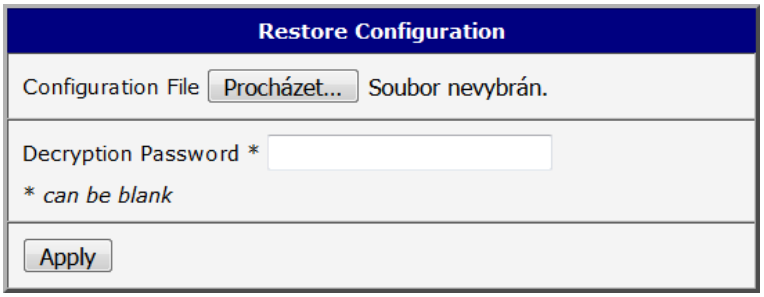


Figure 83: Restore Configuration

6.11 Update Firmware

Select the *Update Firmware* menu item to view the current router firmware version and load new firmware into the router. There is current firmware version and firmware filename written out. When loading the new firmware, it has to have this name. To load new firmware, browse to the new firmware file and press the *Update* button to begin the update.

Do not turn off the router during the firmware update. The firmware update can take up to five minutes to complete. Always use the filename written out as *Firmware Name* when updating the firmware.

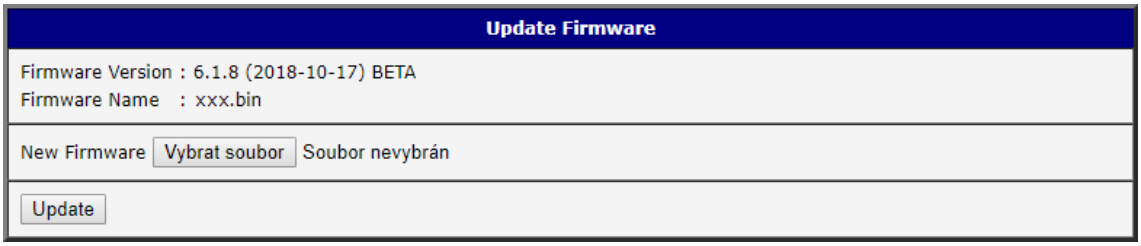


Figure 84: Update Firmware

Uploading firmware intended for a different device can cause damage to the router.

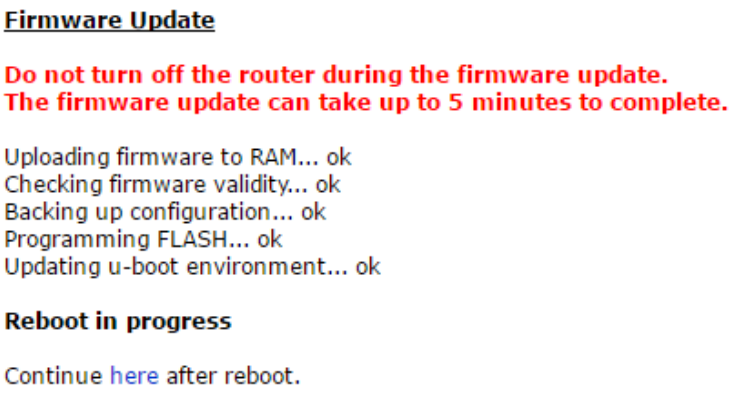
During the firmware update, the router will show the following messages. The progress of programming flash memory is shown in the form of increasing percentage number:

Firmware Update

Do not turn off the router during the firmware update.
The firmware update can take up to 5 minutes to complete.

Uploading firmware to RAM... ok
Checking firmware validity... ok
Backing up configuration... ok
Programming FLASH... 3 %

After the firmware update, the router will automatically reboot:



A mechanism to prevent multiple startups of the firmware update is included. Firmware update can cause incompatibility with the user modules. It is recommended to update user modules to the most recent version. Information about user module and firmware compatibility is at the beginning of the user module's Application Note.

It is highly recommended to always **update to latest firmware** for security reasons. Downgrading the firmware to a lower version than version uploaded during production may cause malfunction of the device.

6.12 Reboot

To reboot the router select the *Reboot* menu item and then press the *Reboot* button.

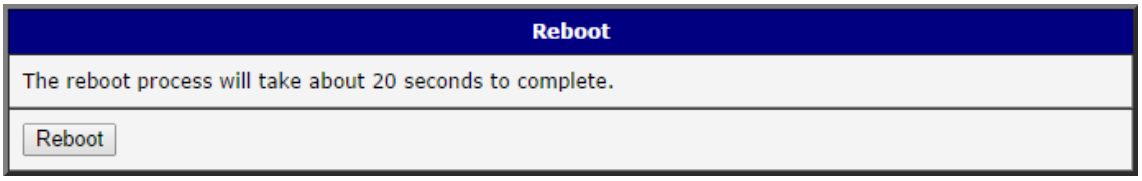


Figure 85: Reboot

6.13 Logout

By clicking the *Logout* menu item, the user is logged out from the web interface.

7 Configuration in Typical Situations

Although Hirschmann routers have wide variety of uses, they are commonly used in the following ways. All the examples below are for IPv4 networks.

7.1 Access to the Internet from LAN

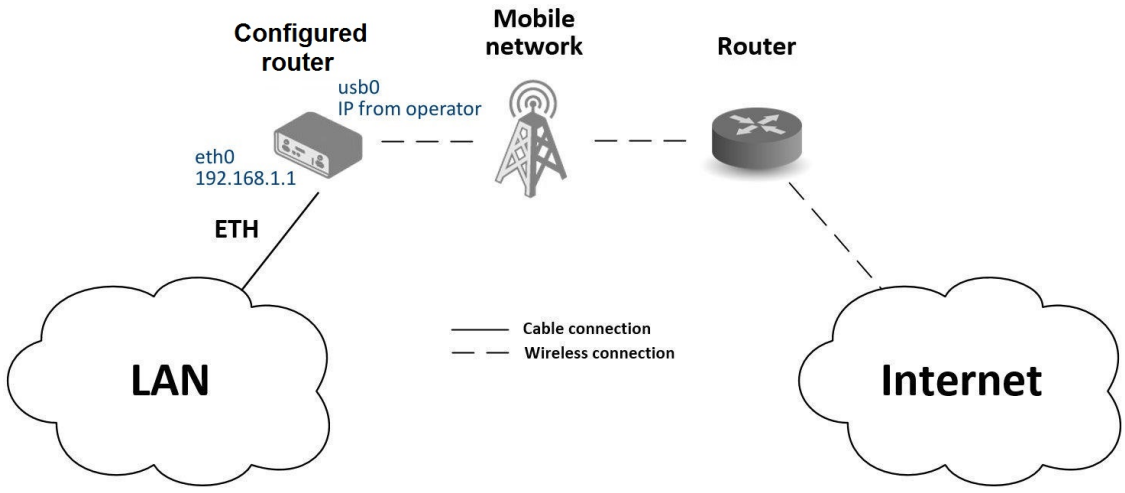


Figure 86: Access to the Internet from LAN – sample topology

In this example, a LAN connecting to the Internet via a mobile network, the SIM card with a data tariff has to be provided by the mobile network operator. This requires no initial configuration. You only need to place the SIM card in the *SIM1* slot (Primary SIM card), attach the antenna to the *ANT* connector and connect the computer (or switch and computers) to the router's eth0 interface (LAN). Wait a moment after turning on the router. The router will connect to the mobile network and the Internet. This will be indicated by the LEDs on the front panel of the router (*WAN* and *DAT*).

Additional configuration can be done in the *LAN* and *Mobile WAN* items in the *Configuration* section of the web interface.

LAN configuration The factory default IP address of the router's eth0 interface is in the form of 192.168.1.1. This can be changed (after login to the router) in the *LAN* item in the *Configuration* section. (See Figure 87.) In this case there is no need of any additional configuration. The DHCP server is also enabled by factory default (so the first connected computer will get the 192.168.1.2 IP address etc.). Other configuration options are described in the Chapter 4.1.

Mobile WAN Configuration Use the *Mobile WAN* item in the *Configuration* section to configure the connection to the mobile network. (Fig. 88.) In this case (depending on the SIM card) the configuration form can be blank. But make sure that *Create connection to mobile network* is checked (this is the factory default). For more details, see Chapter 4.2.1.

To check whether the connection is working properly, go to the *Mobile WAN* item in the *Status* section. You will see information about operator, signal strength etc. At the bottom, you should see the message: *Connection successfully established*. The *Network* item should

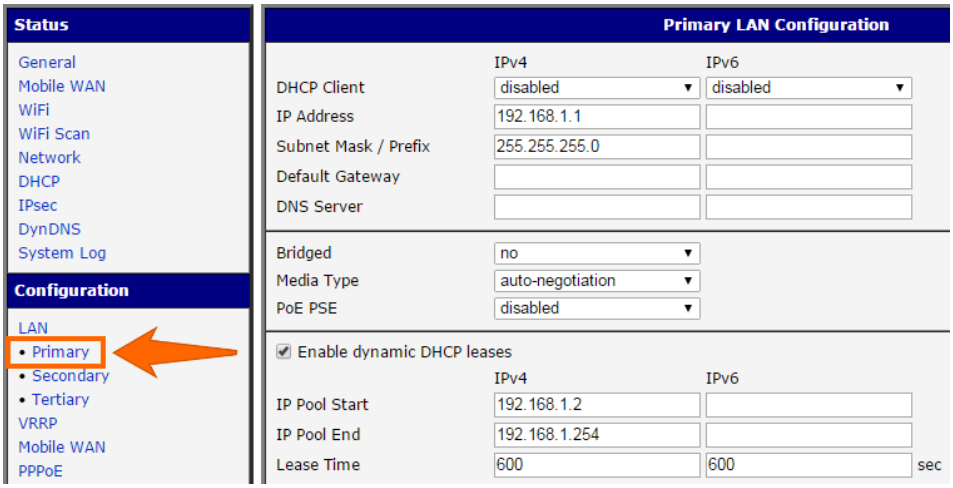


Figure 87: Access to the Internet from LAN – *LAN* configuration

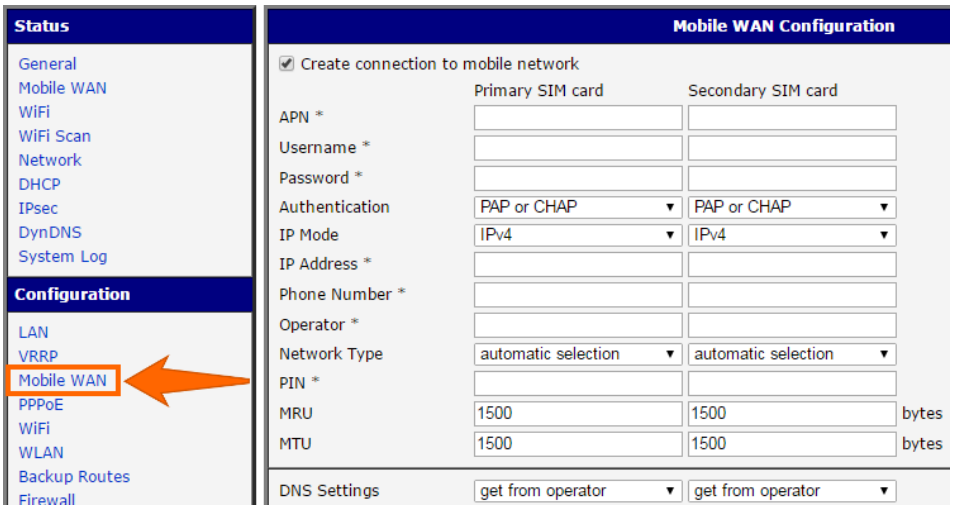


Figure 88: Access to the Internet from LAN – *Mobile WAN* configuration

display information about the newly created network interface, usb0 (mobile connection). You should also see the IP address provided by the network operator, as well as the route table etc. The LAN now has Internet access.

7.2 Backup Access to the Internet from LAN

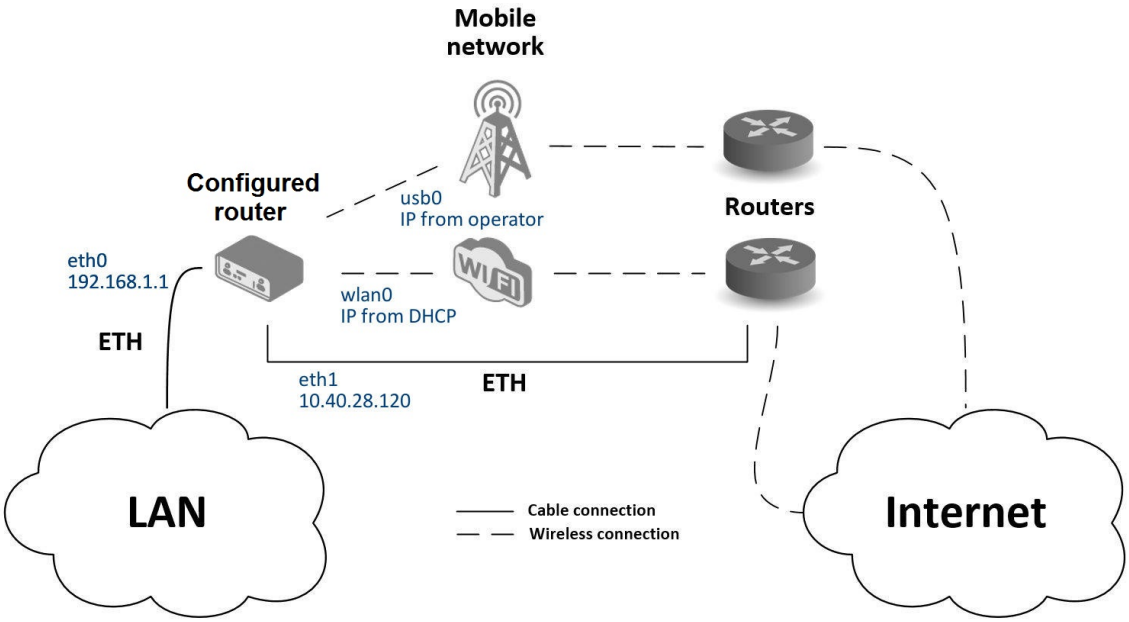


Figure 89: Backup access to the Internet – sample topology

The configuration form on the *Backup Routes* page lets you back up the primary connection with alternative connections to the Internet/mobile network. Each backup connection can be assigned a priority.

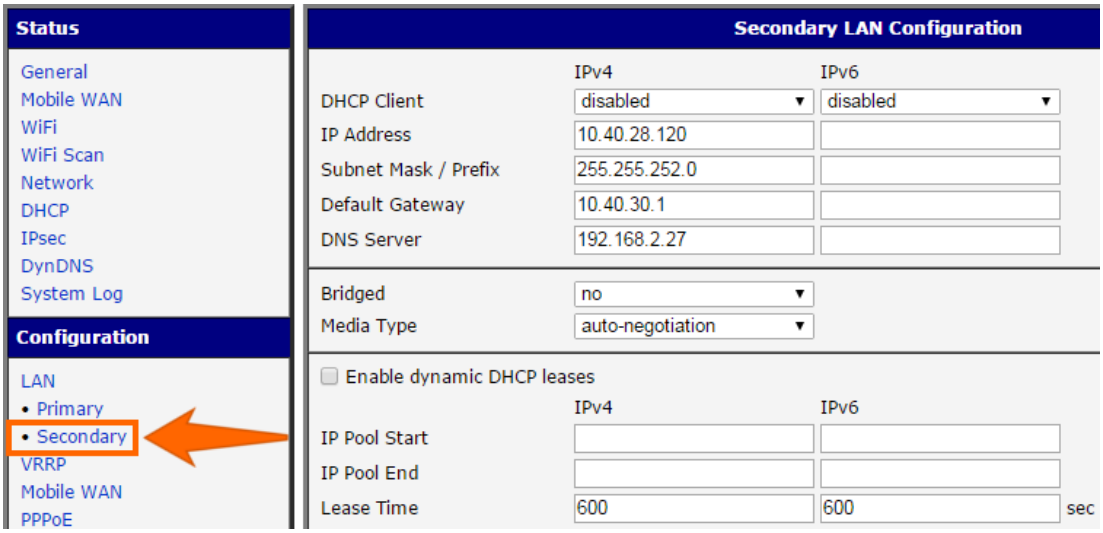


Figure 90: Backup access to the Internet – LAN configuration

LAN configuration In the *LAN* item, *Primary LAN*, you can use the factory default configuration as in the previous situation. The *ETH1* interface on the front panel of the router is used for connection to the Internet. It can be configured in *Secondary LAN*. Connect the cable to the router and set the appropriate values as in Fig. 90. You may configure the static IP address, default gateway and DNS server. Changes will take effect after you click on the *Apply* button. Detailed LAN configuration is described in Chapter 4.1.

WLAN and WiFi configuration To use the WLAN and WiFi options you will need to enable the wlan0 network interface in the *WLAN* item, as shown in Fig. 92. Check the *Enable WLAN interface*, set the *Operating Mode* to *station (STA)*, enable the DHCP client and fill in the default gateway and DNS server. Click the *Apply* button to confirm the changes. For details see Chapter 4.5.

Use the *WiFi* item to configure a connection to a WiFi network. (See Fig. 91.) Check the *Enable WiFi* box and fill in the data for the connection (SSID, security, password). Click the *Apply* button to confirm the changes. For detailed configuration see Chapter 4.4.

To verify that the WiFi connection is successful, check the *WiFi* item in the *Status* section. If the connection is successful you should see the following message: `wpa_state=COMPLETED`.

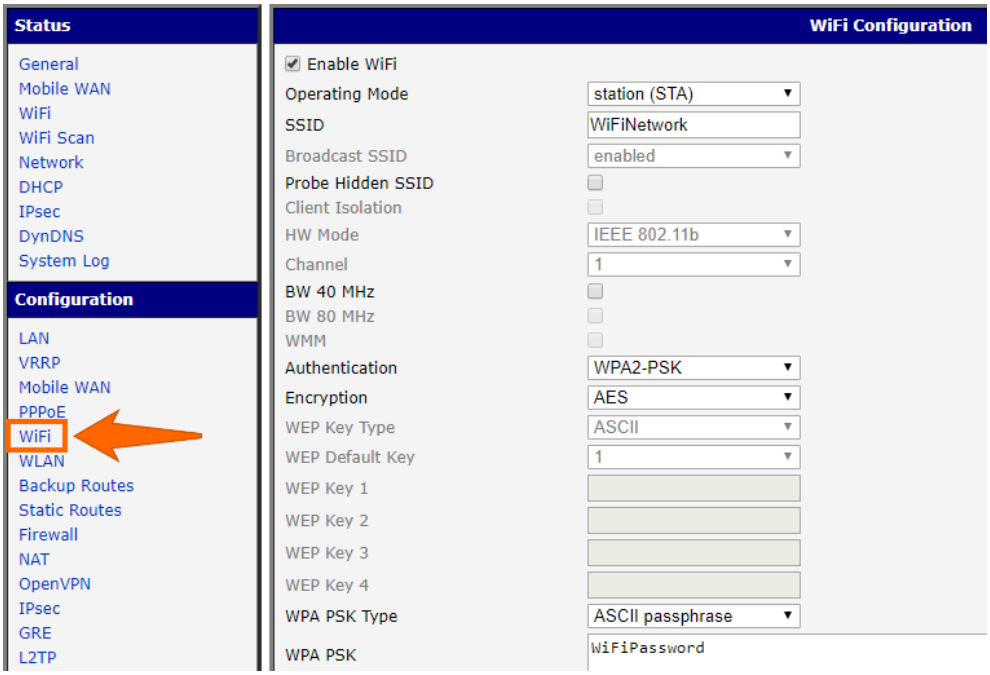


Figure 91: Backup access to the Internet – WiFi configuration

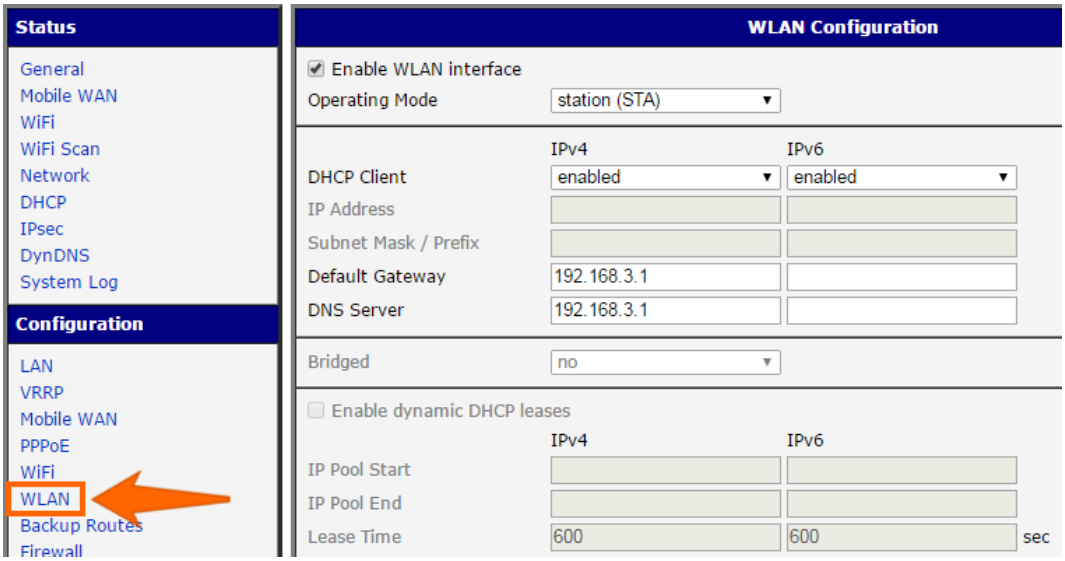


Figure 92: Backup access to the Internet – WLAN configuration

Mobile WAN configuration To configure the mobile connection it should be sufficient to insert the SIM card into the *SIM1* slot and attach the antenna to the *ANT* connector. (Depending on the SIM card you are using).

To set up backup routes you will need to enable Check Connection in the *Mobile WAN* item. (See Fig. 93.) Set the *Check connection* option to *enabled + bind* and fill in an IP address of the mobile operator's DNS server or any other reliably available server and enter the time interval of the check. For detailed configuration, see Chapter 4.2.1.

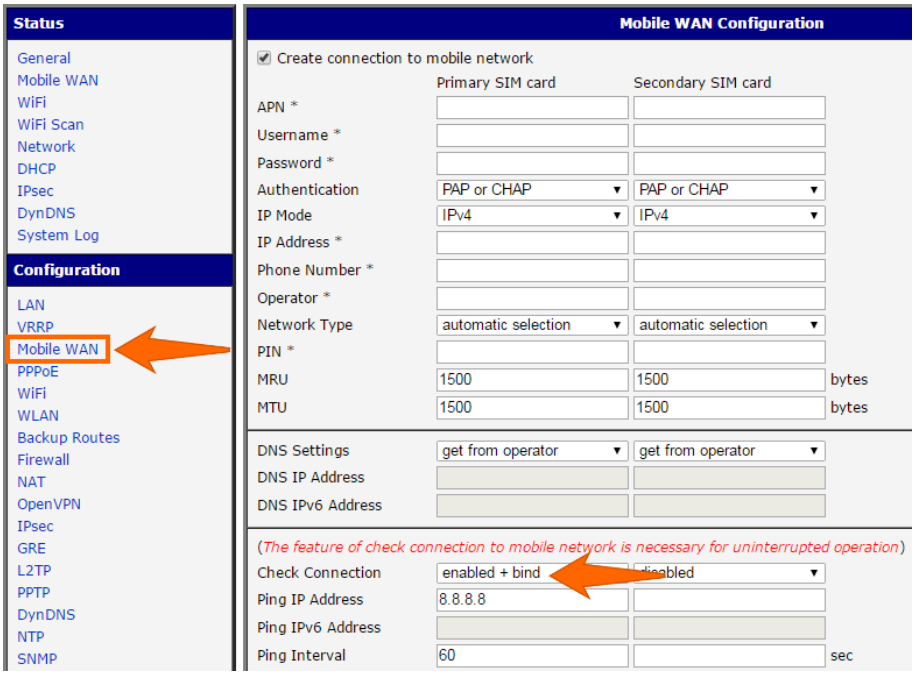


Figure 93: Backup access to the Internet – Mobile WAN configuration

Backup Routes configuration After setting up the backup routes you will need to set their priorities. In Figure 94 the eth1 wired connection has the highest priority. If that connection fails,

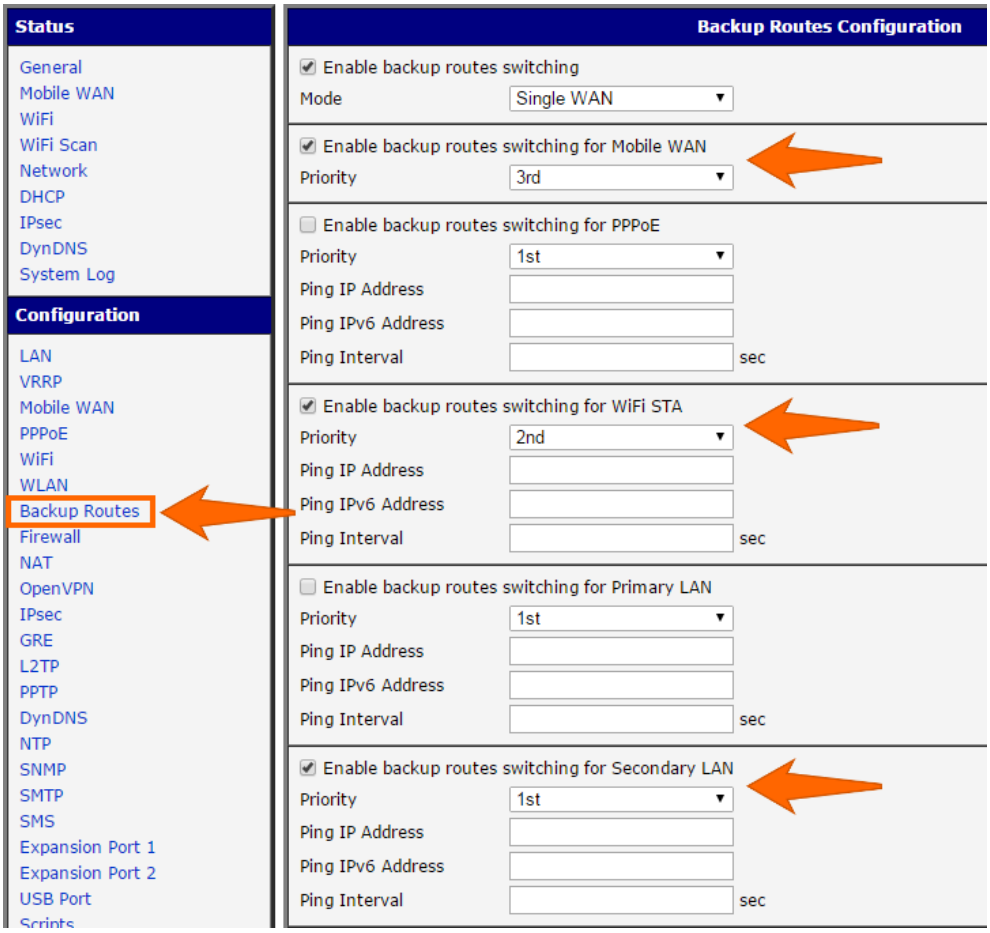


Figure 94: Backup access to the Internet – Backup Routes configuration

the second choice will be the WiFi wlan0 network interface. The third choice will be the mobile connection – usb0 network interface.

The backup routes system must be activated by checking the *Enable backup routes switching* item for each of the routes. Click the *Apply* button to confirm the changes. For detailed configuration see Chapter 4.6.

You can verify the configured network interfaces in the *Status* section in the *Network* item. You will see the active network interfaces: eth0 (connection to LAN), eth1 (wired connection to the Internet), wlan0 (WiFi connection to the Internet) and usb0 (mobile connection to the Internet). IP addresses and other data are included.

At the bottom of the page you will see the *Route Table* and corresponding changes if a wired connection fails or a cable is disconnected (the default route changes to wlan0). Similarly, if a WiFi connection is not available, the mobile connection will be used.

Backup routes work even if they are not activated in the *Backup Routes* item, but the router will use the factory defaults.

7.3 Secure Networks Interconnection or Using VPN

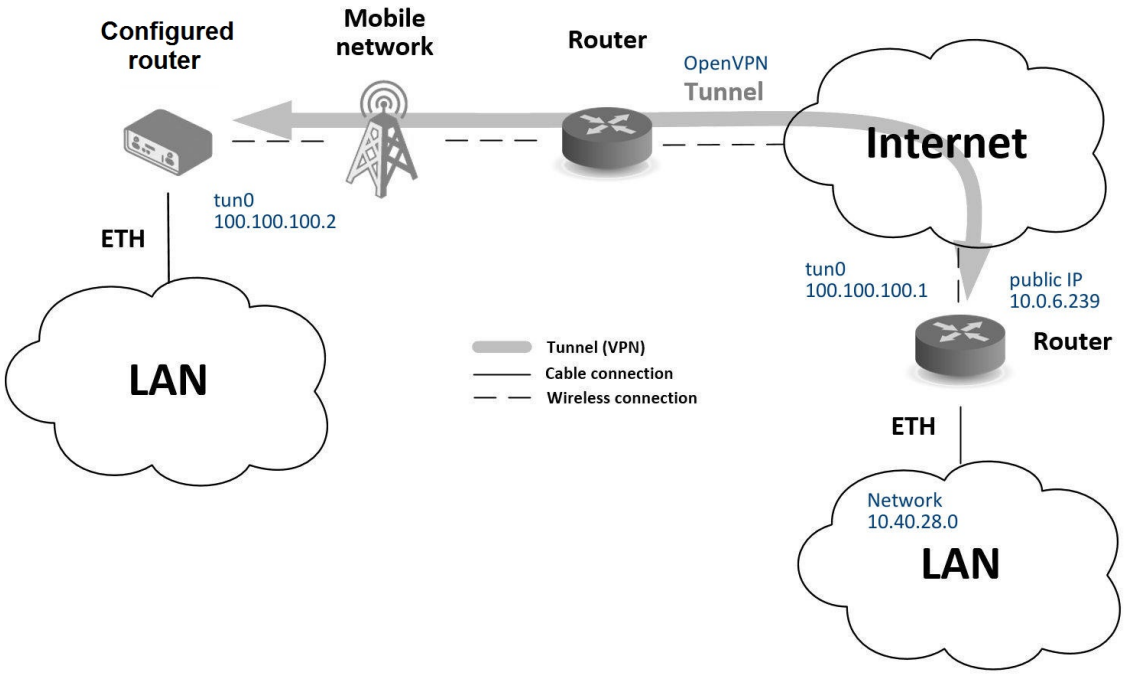


Figure 95: Secure networks interconnection – sample topology

VPN (Virtual Private Network) is a protocol used to create a secure connection between two LANs, allowing them to function as a single network. The connection is secured (encrypted) and authenticated (verified). It is used over public, untrusted networks. (See fig. 95.) You may use several different secure protocols.

- *OpenVPN* (it is a configuration item in the web interface of the router), see chapter 4.10 or the "OpenVPN Tunnel" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com,
- *IPsec* (it is also configuration item in the web interface of the router), see chapter 4.11 or the "IPsec Tunnel" application note. You can download the PDF on the Internet at: https://www.doc.hirschmann.com.

You can also create non-encrypted tunnels: *GRE*, *PPTP* and *L2TP*. You can use GRE or L2TP tunnel in combination with IPsec to create VPNs.

There is an example of an OpenVPN tunnel in Fig. 95. To establish this tunnel you will need the opposite router's IP address, the opposite router's network IP address (not necessary) and the pre-shared secret (key). Create the OpenVPN tunnel by configuring the *Mobile WAN* and *OpenVPN* items in the *Configuration* section.

Mobile WAN configuration The mobile connection can be configured as described in the previous situations. (The router connects itself after a SIM card is inserted into *SIM1* slot and an antenna is attached to the *ANT* connector.)

Configuration is accessible via the *Mobile WAN* item the *Configuration* section. (See Chapter 4.2.1). The mobile connection has to be enabled.

OpenVPN configuration OpenVPN configuration is done with the *OpenVPN* item in the *Configuration* section. Choose one of the two possible tunnels and enable it by checking the *Create 1st OpenVPN tunnel*. You will need to fill in the protocol and the port (according to the settings on the opposite side of the tunnel or Open VPN server). You may fill in the public IP address of the opposite side of the tunnel including the remote subnet and mask (not necessary). The important items are *Local* and *Remote Interface IP Address* where the information regarding the interfaces of the tunnel's end must be filled in. In the example shown, the *pre-shared secret* is known, so you would choose this option in the *Authentication Mode* item and insert the secret (key) into the field. Confirm the configuration clicking the *Apply* button. For detailed configuration see Chapter 4.10 or the "OpenVPN Tunnel" application note. You can download the PDF on the Internet at: `https://www.doc.hirschmann.com`.

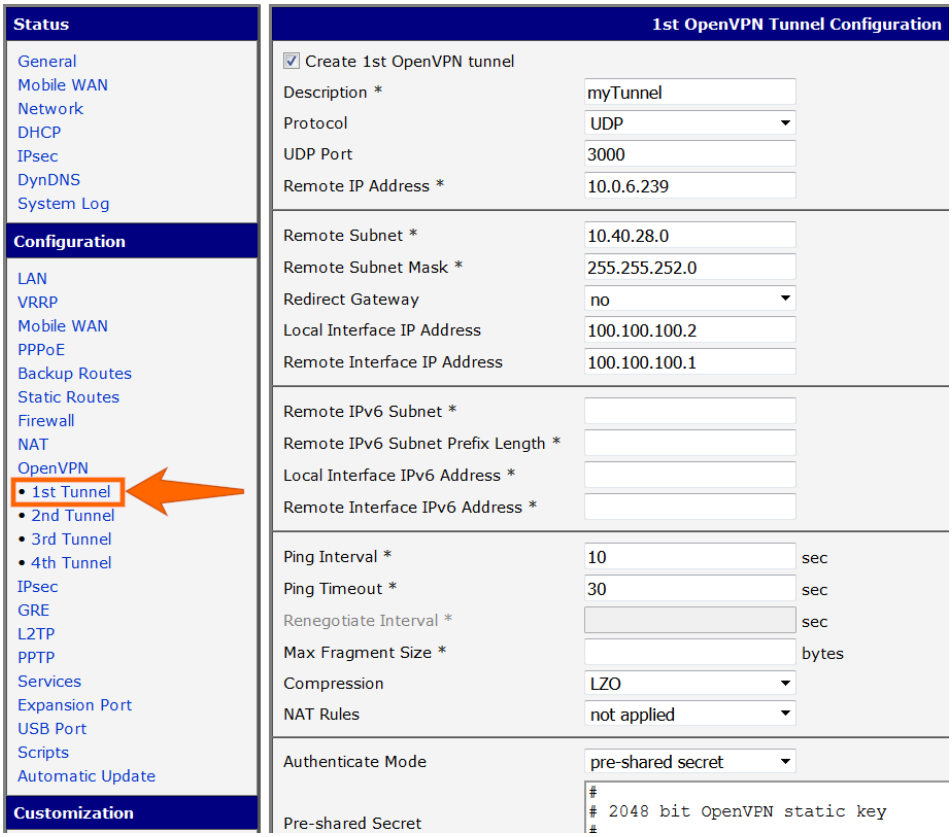


Figure 96: Secure networks interconnection – OpenVPN configuration

The *Network* item in the *Status* section will let you verify the activated network interface tun0 for the tunnel with the IP addresses of the tunnel's ends set. Successful connection can be verified in the *System Log* where you should see the message: `Initialization Sequence Completed`. The networks are now interconnected. This can also be verified by using the `ping` program. (Ping between tunnel's endpoint IP addresses from one of the routers. The console is accessible via SSH).

7.4 Serial Gateway

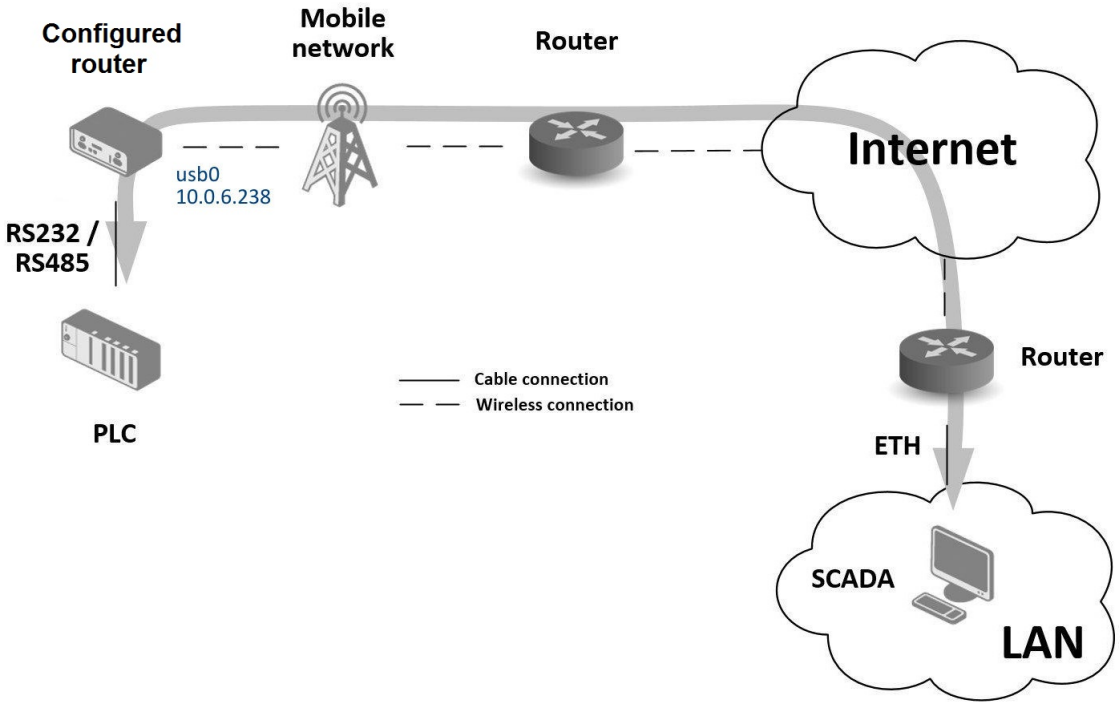


Figure 97: Serial Gateway – sample topology

The router's serial gateway function lets you establish serial connectivity across the Internet or with another network. Serial devices (meters, PLC, etc.) can then upload and download data. (See Fig. 97.)

Configuration is done in the *Configuration* section, *Mobile WAN*, with the *Expansion Port 1* item for RS232, or *Expansion Port 2* for RS485. In this example, the RS232 interface of the router is used.

Mobile WAN configuration Mobile WAN configuration is the same as in the previous examples. Just insert the SIM card into the *SIM1* slot at the back of the router and attach the antenna to the *ANT* connector at the front. No extra configuration is needed (depending on the SIM card used). For more details see Chapter 4.2.1.

Expansion Port 1 configuration The RS232 interface (port) can be configured in the *Configuration* section, via the *Expansion Port 1* item. (See fig. 98.) You will need to enable the RS232 port by checking *Enable expansion port 1 access over TCP/UDP*. You may edit the serial communication parameters (not needed in this example). The important items are *Protocol*, *Mode* and *Port*. These set the parameters of communication out to the network and the Internet. In this example the TCP protocol is chosen, and the router will work as a server listening on the 2345 TCP port. Confirm the configuration clicking the *Apply* button.

To communicate with the serial device (PLC), connect from the PC (Labeled as SCADA in Fig. 97) as a TCP client to the IP address 10.0.6.238, port 2345 (the public IP address of the SIM card used in the router, corresponding to the usb0 network interface). The devices can now communicate. To check the connection, go to *System Log* (*Status* section) and look for the *TCP connection established* message.

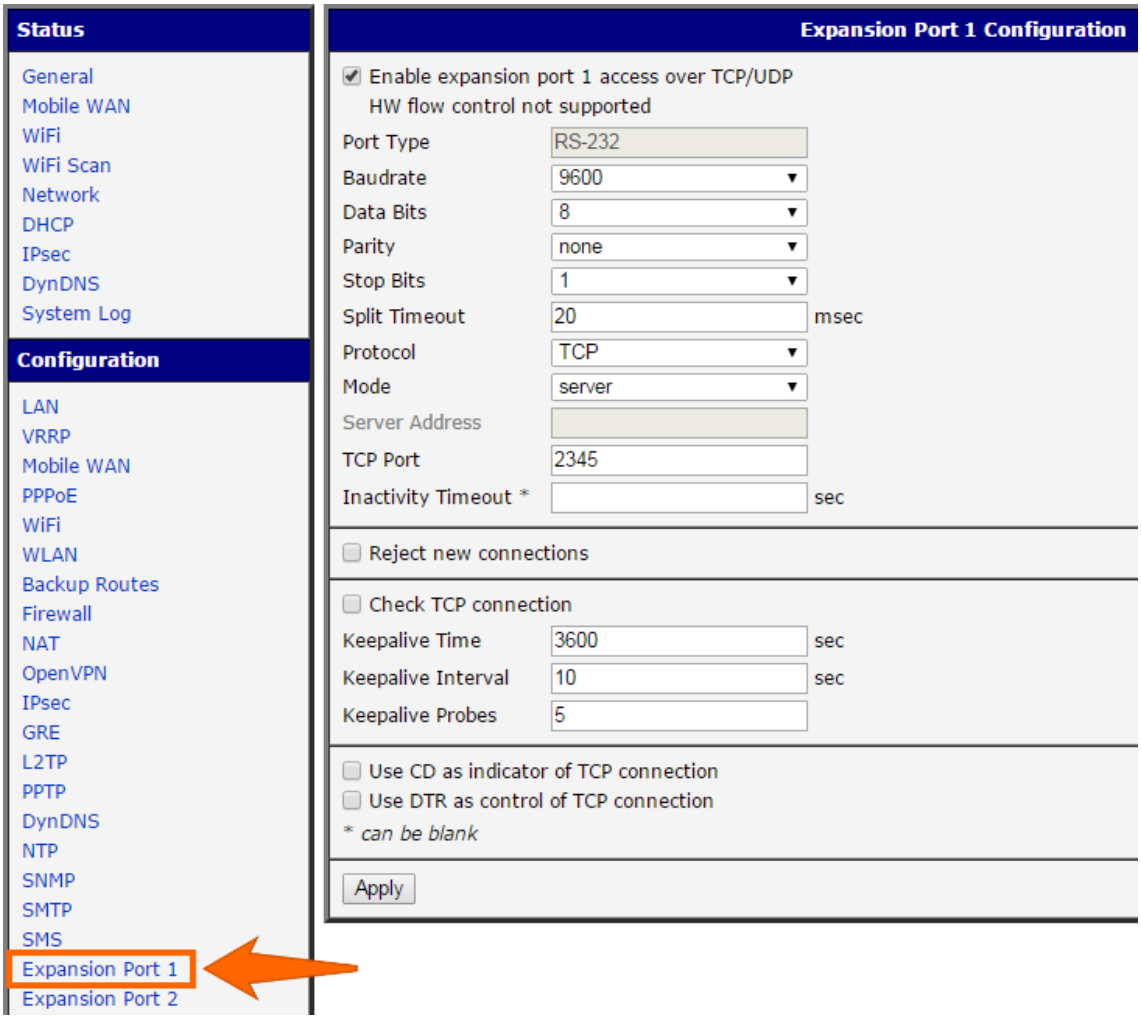


Figure 98: Serial Gateway – konfigurace *Expansion Port 1*

A Maintenance

Hirschmann is continually working on improving and developing their software. Check regularly whether there is an updated version of the software that provides you with additional benefits. You find information and software downloads on the Hirschmann product pages on the Internet (http://www.hirschmann.com).

B Glossary and Acronyms

Backup Routes Allows user to back up the primary connection with alternative connections to the Internet/mobile network. Each backup connection can have assigned a priority. Switching between connections is done based upon set priorities and the state of the connections.

DHCP The Dynamic Host Configuration Protocol (DHCP) is a network protocol used to configure devices that are connected to a network so they can communicate on that network using the Internet Protocol (IP). The protocol is implemented in a client-server model, in which DHCP clients request configuration data, such as an IP address, a default route, and one or more DNS server addresses from a DHCP server.

DHCP client Requests network configuration from DHCP server.

DHCP server Answers configuration request by DHCP clients and sends network configuration details.

DNS The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates various information with domain names assigned to each of the participating entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for the purpose of locating computer services and devices worldwide. By providing a worldwide, distributed keyword-based redirection service, the Domain Name System is an essential component of the functionality of the Internet.

DynDNS client DynDNS service lets you access the router remotely using an easy to remember custom hostname. This client monitors the router's IP address and updates it whenever it changes.

GRE Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network. It is possible to create four different tunnels.

HTTP The Hypertext Transfer Protocol (HTTP) is an application protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web.
Hypertext is structured text that uses logical links (hyperlinks) between nodes containing text. HTTP is the protocol to exchange or transfer hypertext.

HTTPS The Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. Technically, it is not a protocol in and of itself; rather, it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol, thus adding the security capabilities of SSL/TLS to standard HTTP communications.

IP address An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: *A name indicates what we seek. An address indicates where it is. A route indicates how to get there*
The designers of the Internet Protocol defined an IP address as a 32-bit number and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995.

IP masquerade Kind of NAT.

IP masquerading see NAT.

IPsec Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. The router allows user to select encapsulation mode (tunnel or transport), IKE mode (main or aggressive), IKE Algorithm, IKE Encryp-

tion, ESP Algorithm, ESP Encryption and much more. It is possible to create four different tunnels.

IPv4 The Internet Protocol version 4 (IPv4) is the fourth version in the development of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. It is one of the core protocols of standards-based internetworking methods of the Internet, and routes most traffic in the Internet. However, a successor protocol, IPv6, has been defined and is in various stages of production deployment. IPv4 is described in IETF publication RFC 791 (September 1981), replacing an earlier definition (RFC 760, January 1980).

IPv6 The Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP), the communications protocol that provides an identification and location system for computers on networks and routes traffic across the Internet. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is intended to replace IPv4, which still carries the vast majority of Internet traffic as of 2013. As of late November 2012, IPv6 traffic share was reported to be approaching 1%.
IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons (2001:0db8:85a3:0042:1000:8a2e:0370:7334), but methods of abbreviation of this full notation exist.

L2TP Layer 2 Tunnelling Protocol (L2TP) is a tunnelling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

LAN A local area network (LAN) is a computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building using network media. The defining characteristics of LANs, in contrast to wide area networks (WANs), include their usually higher data-transfer rates, smaller geographic area, and lack of a need for leased telecommunication lines.

NAT In computer networking, Network Address Translation (NAT) is the process of modifying IP address information in IPv4 headers while in transit across a traffic routing device.
The simplest type of NAT provides a one-to-one translation of IP addresses. RFC 2663 refers to this type of NAT as basic NAT, which is often also called a one-to-one NAT. In this type of NAT only the IP addresses, IP header checksum and any higher level checksums that include the IP address are changed. The rest of the packet is left untouched (at least for basic TCP/UDP functionality; some higher level protocols may need further translation). Basic NATs can be used to interconnect two IP networks that have incompatible addressing.

NAT-T NAT traversal (NAT-T) is a computer networking methodology with the goal to establish and maintain Internet protocol connections across gateways that implement network address translation (NAT).

NTP Network Time Protocol (NTP) is a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks.

OpenVPN OpenVPN implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections. It is possible to create four different tunnels.

PAT Port and Address Translation (PAT) or Network Address Port Translation (NAPT) see NAT.

Port In computer networking, a Port is an application-specific or process-specific software construct serving as a communications endpoint in a computer's host operating system. A port is associated with an IP address of the host, as well as the type of protocol used for communication. The purpose of ports is to uniquely identify different applications or processes running on a single computer and thereby enable them to share a single physical connection to a packet-switched network like the Internet.

PPTP The Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol that operates at the Data Link Layer (Layer 2) of the OSI Reference Model. PPTP is a proprietary technique that encapsulates Point-to-Point Protocol (PPP) frames in Internet Protocol (IP) packets using the Generic Routing Encapsulation (GRE) protocol. Packet filters provide access control, end-to-

end and server-to-server.

RADIUS Remote Authentication Dial-In User Service (RADIUS) is a networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA or Triple A) management for users who connect and use a network service. Because of the broad support and the ubiquitous nature of the RADIUS protocol, it is often used by ISPs and enterprises to manage access to the Internet or internal networks, wireless networks, and integrated e-mail services.

Root certificate In cryptography and computer security, a root certificate is either an unsigned public key certificate or a self-signed certificate that identifies the Root Certificate Authority (CA). A root certificate is part of a public key infrastructure scheme. The most common commercial variety is based on the ITU-T X.509 standard, which normally includes a digital signature from a certificate authority (CA).
Digital certificates are verified using a chain of trust. The trust anchor for the digital certificate is the Root Certificate Authority (CA). See X.509.

Router A router is a device that forwards data packets between computer networks, creating an overlay internetwork. A router is connected to two or more data lines from different networks. When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the *traffic directing* functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

SFTP Secure File Transfer Protocol (SFTP) is a secure version of File Transfer Protocol (FTP), which facilitates data access and data transfer over a Secure Shell (SSH) data stream. It is part of the SSH Protocol. This term is also known as SSH File Transfer Protocol.

SMTP The SMTP (Simple Mail Transfer Protocol) is a standard e-mail protocol on the Internet and part of the TCP/IP protocol suite, as defined by IETF RFC 2821. SMTP defines the message format and the message transfer agent (MTA), which stores and forwards the mail. SMTP by default uses TCP port 25. The protocol for mail submission is the same, but uses port 587. SMTP connections secured by SSL, known as SMTPS, default to port 465.

SMTPS SMTPS (Simple Mail Transfer Protocol Secure) refers to a method for securing SMTP with transport layer security. For more information about SMTP, see description of the SMTP.

SNMP The Simple Network Management Protocol (SNMP) is an *Internet-standard protocol for managing devices on IP networks*. Devices that typically support SNMP include routers, switches, servers, workstations, printers, modem racks, and more. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention. SNMP is a component of the Internet Protocol Suite as defined by the Internet Engineering Task Force (IETF). It consists of a set of standards for network management, including an application layer protocol, a database schema, and a set of data objects.

SSH Secure Shell (SSH), sometimes known as Secure Socket Shell, is a UNIX-based command interface and protocol for securely getting access to a remote computer. It is widely used by network administrators to control Web and other kinds of servers remotely. SSH is actually a suite of three utilities – slogin, ssh, and scp – that are secure versions of the earlier UNIX utilities, rlogin, rsh, and rcp. SSH commands are encrypted and secure in several ways. Both ends of the client/server connection are authenticated using a digital certificate, and passwords are protected by being encrypted.

TCP The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered, error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer.
Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another.

UDP The User Datagram Protocol (UDP) is one

of the core members of the Internet protocol suite (the set of network protocols used for the Internet). With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768.

URL A uniform resource locator, abbreviated URL, also known as web address, is a specific character string that constitutes a reference to a resource. In most web browsers, the URL of a web page is displayed on top inside an address bar. An example of a typical URL would be `http://www.example.com/index.html`, which indicates a protocol (http), a hostname (www.example.com), and a file name (index.html). A URL is technically a type of uniform resource identifier (URI), but in many technical documents and verbal discussions, URL is often used as a synonym for URI, and this is not considered a problem.

VPN A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefiting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.
A VPN connection across the Internet is similar to a wide area network (WAN) link between the sites. From a user perspective, the extended network resources are accessed in the same way as resources available from the private network.

VPN server see VPN.

VPN tunnel see VPN.

VRRP VRRP protocol (Virtual Router Redundancy Protocol) allows you to transfer packet routing from the main router to a backup router in case the main router fails. (This can be used to provide a wireless cellular backup to a primary wired router in critical applications).

WAN A wide area network (WAN) is a network that covers a broad area (i.e., any telecommunications network that links across metropolitan, regional, or national boundaries) using private or public network transports. Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations. In essence, this mode of telecommunication allows a business to effectively carry out its daily function regardless of location. The Internet can be considered a WAN as well, and is used by businesses, governments, organizations, and individuals for almost any purpose imaginable.

X.509 In cryptography, X.509 is an ITU-T standard for a public key infrastructure (PKI) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.

C Index

A

Access Point
- Configuration . . . 59
- Information . . . 24

Accessing the router . . . 17
Add User . . . 134
APN . . . 49
AT commands . . . 114

B

Backup Configuration . . . 139
Backup Routes . . . 67
Binary I/O . . . 122
Bridge . . . 38

C

Change Password . . . 136
Change Profile . . . 135
Clock synchronization . . . 104
Configuration update . . . 129
Control SMS messages . . . 112

D

Data limit . . . 52
Default Gateway . . . 37, 66
Default IP address . . . 17
Default password . . . 17
Default SIM card . . . 53
Default username . . . 17
DHCP . . . 30, 37, 65, 154
- DHCPv6 . . . 38
- Dynamic . . . 38
- Static . . . 38

DHCPv6 . . . 30, 37, 65
DNS . . . 154
DNS server . . . 37, 50, 66
DNS64 . . . 28
Domain Name System . . . *see* DNS
DoS attacks . . . 73
Dynamic Host Configuration Protocol . . . *see* DHCP
DynDNS . . . 33, 101
DynDNSv6 . . . 33, 101

E

Expansion Port
- RS232 . . . 122
- RS485 . . . 122

F

Firewall . . . 71
- Filtering of Forwarded Packets . . . 72
- Filtering of Incoming Packets . . . 72
- Protection against DoS attacks . . . 73

Firmware update . . . 129, 141
Firmware version . . . 20
FTP . . . 102

G

GRE . . . 94, 154

H

HTTP . . . 103

I

ICMPv6 . . . 51
IPsec . . . 87, 154
- Authenticate Mode . . . 89
- Encapsulation Mode . . . 88
- IKE Mode . . . 88

IPv4 . . . 155
IPv6 19, 28, 36, 38, 49, 51, 71, 76, 82, 87, 101, 127

L

L2TP . . . 97, 155
LAN

IPv6 36
Primary LAN 36
Secondary LAN 36
Location Area Code 21
Logout 142

M

Mobile network 49
Multiple WANs 67, 68, 70

N

NAT 76, 155
NAT64 28
Neighbouring WiFi Networks 25
Network Address Translation . . . . . *see* NAT
NTP 104, 155
NTP server 136

O

Object Identifier 106
OpenVPN 82, 155
Authenticate Mode 83

P

Password 136
PAT 76
PIN number 137
PLMN 21
Port 155
PPPoE 57
PPPoE Bridge Mode 56
PPTP 99, 155
Prefix delegation 38
PUK number 138

R

RADIUS 40, 59, 62
Reboot 142
Remote access 77
Restore Configuration 140
Router 14
Accessing 17
Equipment 14
Optional Features 14

S

Save Log 34
Save Report 34
Security certificate 17
Send SMS 138
SERIAL I/O 122
Serial line
RS232 122
RS485 122
Serial number 20
Set internal clock 136
Signal Quality 21
Simple Network Management Protocol . . . . *see* SNMP
SMS 111
SMS Service Center 137
SMTP 109, 156
SNMP 105, 156
SSH 119
Startup Script 126
Static Routes 70
Switch between SIM Cards 52
Syslog 120
System Log 34

T

TCP 156
Telnet 121
Transfer speed 14
Transmission Control Protocol . . . . . *see* TCP

U

UDP 156
Unblock SIM card 138
Uniform resource locator . . . . . *see* URL
Unlock SIM card 137
Up/Down script 127
URL 157
Usage Profiles 135
User Datagram Protocol . . . . . *see* UDP
User Module 133
Users 134

V

Virtual private network . . . . . *see* VPN

VPN 157

VRRP 46, 157

W

Web interface 17
WiFi 59
Authentication 61
HW Mode 60
Operating mode 59
WLAN 65
Operating mode 65

D Recommended Literature

Application Notes, the “Installation” user manual, and documentation of several OWL user modules can be found as PDF files for downloading on the Internet at: https://www.doc.hirschmann.com/.

E 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.

Hirschmann Competence Center

The Hirschmann Competence 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 http://www.hicomcenter.com.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you decided against making any compromises. Our client-customized package leaves you free to choose the service components you want to use.

Internet:

http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND