HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

Classic L3P Rel. 09000

Referenz-Handbücher

- Grafische Benutzeroberfläche
- Command Line Interface

Anwender-Handbücher

- Grundkonfiguration
- Industrie-Protokolle
- Redundanz-Konfiguration
- Routing-Konfiguration

HIRSCHMANN
A BELDEN BRAND

Referenz-Handbuch

Grafische Benutzeroberfläche (GUI)
Industrial ETHERNET (Gigabit-)Switch
PowerMICE, MACH 104, MACH 1040, MACH 4000

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

© 2015 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken. Bei Geräten mit eingebetteter Software gilt die Endnutzer-Lizenzvereinbarung auf der mitgelieferten CD/DVD.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die jeweils neueste Version dieses Handbuches finden Sie im Internet auf den Hirschmann-Produktseiten (www.hirschmann.com).

Gedruckt in Deutschland
Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Rel. 9.0 - 02/2015 – 03.03.2015

Inhalt

Sicherheitshinweise 9

Über dieses Handbuch 11

Legende 13

Grafische Benutzeroberfläche 15

1 Grundeinstellungen 21

1.1 System 22

1.2 Module (MS, PowerMICE, MACH102 und MACH4000) 26

1.3 Netz 29

1.4 Software 32
1.4.1 Anzeige der im Gerät vorhandenen Software-Versionen 33
1.4.2 Wiederherstellen der Backup-Version 33
1.4.3 tftp-Software-Update 34
1.4.4 tftp-Bootcode-Update 34
1.4.5 http-Software-Update 35
1.4.6 Automatischer Software-Update vom ACA 35

1.5 Portkonfiguration 37

1.6 Power over ETHERNET 40

1.7 Power over Ethernet Plus 44
1.7.1 Power over Ethernet Plus - Global 45
1.7.2 Power over Ethernet Plus - Port 49

1.8 Laden/Speichern 52
1.8.1 Konfiguration laden 53
1.8.2 Konfiguration speichern 60
1.8.3 URL 63
1.8.4 Konfiguration löschen 63
1.8.5 AutoConfiguration Adapter (ACA) verwenden 64
1.8.6 Konfigurationsänderung widerrufen 66

1.9 Neustart 68

2 Sicherheit 71

2.1 Passwort / SNMPv3-Zugriff 72

2.2 SNMPv1/v2-Zugriffs-Einstellungen 76

2.3 Telnet-/Web-/SSH-Zugriff 80
2.3.1 Beschreibung Telnet-Zugriff 81
2.3.2 Beschreibung Web-Zugriff (http) 82
2.3.3 Beschreibung Web-Zugriff (https) 82
2.3.4 Beschreibung SSH-Zugriff 83

2.4 Restricted Management Access 85

2.5 Portsicherheit 89

2.6 802.1X Port-Authentifizierung 98
2.6.1 802.1X Globale Konfiguration 98
2.6.2 802.1X-Portkonfiguration 103
2.6.3 802.1X-Port-Clients 111
2.6.4 802.1X-Port-Statistiken 114

2.7 RADIUS 116
2.7.1 Global 116
2.7.2 RADIUS-Server 119

2.8 Login-/CLI-Banner 124
2.8.1 Login-Banner 125
2.8.2 CLI-Banner 127

2.9 Access Control Lists (ACLs) 129

3 Zeit 131

3.1 Grundeinstellungen 132

3.2 SNTP-Konfiguration 135

3.3 PTP (IEEE 1588) 139
3.3.1 PTP Global (MS20/MS30, PowerMICE, MACH 104, MACH 1040) 142
3.3.2 PTP Version 1 (MS20/MS30, PowerMICE, MACH 104, MACH 1040) 147
3.3.3 PTP-Version 2 (BC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040) 150
3.3.4 PTP Version 2 (TC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040) 157

4 Switching 163

4.1 Switching Global 164

4.2 Filter für MAC-Adressen 169

4.3 Lastbegrenzer 173
4.3.1 Lastbegrenzer-Einstellungen (PowerMICE und MACH 4000) 174

4.4 Multicasts 176
4.4.1 IGMP (Internet Group Management Protocol) 176
4.4.2 GMRP (GARP Multicast Registration Protocol) 183

4.5 VLAN 187
4.5.1 VLAN Global 187
4.5.2 VLAN Aktuell 193
4.5.3 VLAN Statisch 195
4.5.4 VLAN Port 198
4.5.5 Voice-VLAN 202

5 QoS/Priorität 207

5.1 Global 208

5.2 Portkonfiguration 210
5.2.1 Port-Priorität eingeben 212
5.2.2 Trust-Modus wählen 213
5.2.3 Untrusted Traffic Class anzeigen 214
5.2.4 Shaping Rate 214

5.3 802.1D/p-Mapping 216

5.4 IP-DSCP-Mapping 218

5.5 Queue-Management 221
5.5.1 Strict Priority 222
5.5.2 Weighted Fair Queuing 223
5.5.3 Maximale Bandbreite 224

6 Routing 225

6.1 Routing Global 226

6.2 Router-Interfaces konfigurieren 227
6.2.1 Konfiguration 227
6.2.2 Weitere Adressen konfigurieren 231

6.3 ARP 232
6.3.1 ARP-Parameter einstellen 232
6.3.2 Anzeige ARP-Statistik 234

6.3.3 Anzeige ARP-Tabelle 234
6.3.4 ARP-Tabelle bearbeiten 235
6.4 Konfiguration Router-Discovery 237
6.5 RIP 238
6.5.1 Konfiguration 238
6.5.2 Route Distribution 241
6.5.3 Statistik 243
6.6 Routingtabelle 244
6.6.1 Aktuell 244
6.6.2 Statisch 246
6.6.3 Präferenzen 247
6.7 Tracking 249
6.7.1 Konfiguration 249
6.7.2 Applikationen 252

7 Redundanz 253

7.1 Link-Aggregation 254
7.2 Ring-Redundanz 258
7.2.1 HIPER-Ring konfigurieren 261
7.2.2 MRP-Ring konfigurieren 265
7.2.3 Fast HIPER-Ring konfigurieren (MACH 1040) 272
7.3 Sub-Ring 275
7.3.1 Sub-Ring-Konfiguration 276
7.3.2 Sub-Ring – Neuer Eintrag 279
7.4 Ring-/Netzkopplung 282
7.4.1 Ring-/Netzkopplung vorbereiten 282
7.5 Spanning Tree 288
7.5.1 Global 291
7.5.2 MSTP (Multiple Spanning Tree) 297
7.5.3 Port 305
7.6 VRRP/HiVRRP 318
7.6.1 VRRP/HiVRRP Konfiguration 318
7.6.2 HiVRRP-Domänen 323
7.6.3 Statistik 326
7.6.4 Tracking 327

8 Diagnose 331

8.1 Syslog 332
8.2 Trap-Log 336

8.3 Ports 338
8.3.1 Portstatistiken 338
8.3.2 Auslastung (Netzlast) 340
8.3.3 SFP-Transceiver 342
8.3.4 TP-Kabeldiagnose 343
8.3.5 Port Monitor 346
8.3.6 Auto-Disable 358

8.4 Konfigurations-Check 362

8.5 Topologie-Erkennung 365
8.5.1 LLDP-Informationen von Nachbargeräten 365
8.5.2 LLDP-MED (Media Endpoint Discovery) 367

8.6 Port-Mirroring 371

8.7 Gerätestatus 374

8.8 Meldekontakt 377
8.8.1 Manuelle Einstellung 377
8.8.2 Funktionsüberwachung 378
8.8.3 Gerätestatus 380
8.8.4 Trapeinstellung 381

8.9 Alarme (Traps) 383

8.10 Bericht 386
8.10.1 Systeminformationen 389
8.10.2 Event-Log 389

8.11 IP-Adressen-Konflikterkennung 391

8.12 MAC-Benachrichtigung 394
8.12.1 Funktion 394
8.12.2 Konfiguration 395
8.12.3 Tabelle 395

8.13 Selbsttest 397

9 Erweitert 399

9.1 DHCP-Relay-Agent 400
9.1.1 Global 400
9.1.2 Server 403

9.2 DHCP-Server 405
9.2.1 Global 405
9.2.2 Pool 408
9.2.3 Lease-Tabelle 413

9.3 Industrieprotokolle 416
9.3.1 PROFINET IO 416
9.3.2 EtherNet/IP 419
9.3.3 IEC61850 MMS Protokoll (RSR, MACH 1000) 420
9.3.4 Digital IO-Module 422
9.4 DIP-Switch via Software überschreiben (Mice, PowerMICE und RS) 431
9.5 Command Line 433

A Anhang 435

A.1 Technische Daten 436
A.2 Liste der RFCs 438
A.3 Zugrundeliegende IEEE-Normen 440
A.4 Zugrundeliegende IEC-Normen 441
A.5 Zugrundeliegende ANSI-Normen 442
A.6 Literaturhinweise 443
A.7 Copyright integrierter Software 444
A.7.1 Bouncy Castle Crypto APIs (Java) 444
A.7.2 Broadcom Corporation 445

B Leserkritik 446

C Stichwortverzeichnis 449

D Weitere Unterstützung 453

Sicherheitshinweise

⚠ WARNUNG
UNKONTROLLIERTE MASCHINENBEWEGUNGEN Um unkontrollierte Maschinenbewegungen aufgrund von Datenverlust zu vermeiden, konfigurieren Sie alle Geräte zur Datenübertragung individuell. Nehmen Sie eine Maschine, die mittels Datenübertragung gesteuert wird, erst in Betrieb, wenn Sie alle Geräte zur Datenübertragung vollständig konfiguriert haben. **Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.**

Über dieses Handbuch

Das Dokument „Referenz-Handbuch GUI“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über die grafische Oberfläche.
Das GUI (Graphical User Interface) wird im Folgenden mit Web-based Interface bezeichnet.

Das Dokument „Referenz-Handbuch Command Line Interface“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über das Command Line Interface.

Das Dokument „Anwender-Handbuch Installation“ enthält eine Gerätebeschreibung, Sicherheitshinweise, Anzeigebeschreibung und weitere Informationen, die Sie zur Installation des Gerätes benötigen, bevor Sie mit der Konfiguration des Gerätes beginnen.

Das Dokument „Anwender-Handbuch Grundkonfiguration“ enthält die Informationen, die Sie zur Inbetriebnahme des Gerätes benötigen. Es leitet Sie Schritt für Schritt von der ersten Inbetriebnahme bis zu den grundlegenden Einstellungen für einen Ihrer Umgebung angepassten Betrieb.

Das Dokument „Anwender-Handbuch Redundanzkonfiguration“ enthält die Informationen, die Sie zur Auswahl des geeigneten Redundanzverfahrens und dessen Konfiguration benötigen.

Das Dokument „Anwender-Handbuch Industrie-Protokolle“ beschreibt die Anbindung des Gerätes über ein in der Industrie übliches Kommunikationsprotokoll wie z.B. EtherNet/IP und PROFINET.

Das Dokument „Anwender-Handbuch Routing-Konfiguration“ enthält Informationen, die Sie zur Inbetriebnahme der Routing-Funktion benötigen. Das Handbuch versetzt Sie in die Lage, durch Ableitung aus den Beispielen Ihre Router zu konfigurieren.

Die Netzmanagement-Software Industrial HiVision bietet Ihnen weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:

- ActiveX-Control für SCADA-Integration
- Autotopologie-Erkennung
- Browser-Interface
- Client/Server-Struktur
- Ereignisbehandlung
- Ereignislogbuch
- Gleichzeitige Konfiguration mehrerer Geräte
- Grafische Benutzeroberfläche mit Netz-Layout
- SNMP/OPC-Gateway

Wartung

Hirschmann arbeitet ständig an der Verbesserung und Weiterentwicklung der Software. Prüfen Sie regelmäßig, ob ein neuerer Stand der Software Ihnen weitere Vorteile bietet. Informationen und Software-Downloads finden Sie auf den Hirschmann-Produktseiten im Internet (www.hirschmann.com).

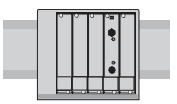
Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
☐	Arbeitsschritt
■	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	ASCII-Darstellung in der grafischen Benutzeroberfläche

Verwendete Symbole:

	WLAN-Access-Point
	Router mit Firewall
	Switch mit Firewall
	Router
	Switch
	Bridge

	Hub
	Beliebiger Computer
	Konfigurations-Computer
	Server
	SPS - Speicherprogrammier-bare Steuerung
	I/O - Roboter

Grafische Benutzeroberfläche

Systemvoraussetzungen

Verwenden Sie zum Öffnen der grafischen Benutzeroberfläche HiView. Diese Applikation bietet Ihnen die Möglichkeit, frei von weiteren Anwendungen wie einem Web-Browser oder einer installierten Java-Laufzeitumgebung (JRE), die grafische Benutzeroberfläche zu bedienen.

Alternativ haben Sie die Möglichkeit, die grafische Benutzeroberfläche im Web-Browser zu öffnen, z. B. im Mozilla Firefox ab Version 3.5 oder im Microsoft Internet Explorer ab Version 6. Installieren Sie hierzu auch die Java-Laufzeitumgebung (JRE-7) in der zuletzt freigegebenen Version. Installationspakete für Ihr Betriebssystem finden Sie unter http://java.com.

Grafische Benutzeroberfläche starten

Voraussetzung für das Starten der grafischen Benutzeroberfläche ist, dass die IP-Parameter im Gerät konfiguriert sind. Das Anwender-Handbuch „Grundkonfiguration“ enthält ausführliche Informationen, die Sie zum Festlegen der IP-Parameter im Gerät benötigen.

Grafische Benutzeroberfläche in HiView starten:

☐ Starten Sie HiView.

☐ Geben Sie in das URL-Feld des Startfensters die IP-Adresse Ihres Gerätes ein.

☐ Klicken Sie „Öffnen“.

HiView stellt die Verbindung zum Gerät her und zeigt das Login-Fenster.

Grafische Benutzeroberfläche im Web-Browser starten:

– Voraussetzung ist, dass Java in den Sicherheitseinstellungen Ihres Web-Browsers aktiviert ist.

☐ Starten Sie Ihren Web-Browser.

☐ Schreiben Sie die IP-Adresse des Gerätes in das Adressfeld des Web-Browsers. Verwenden Sie die folgende Form:
`https://xxx.xxx.xxx.xxx`

Der Web-Browser stellt die Verbindung zum Gerät her und zeigt das Login-Fenster.

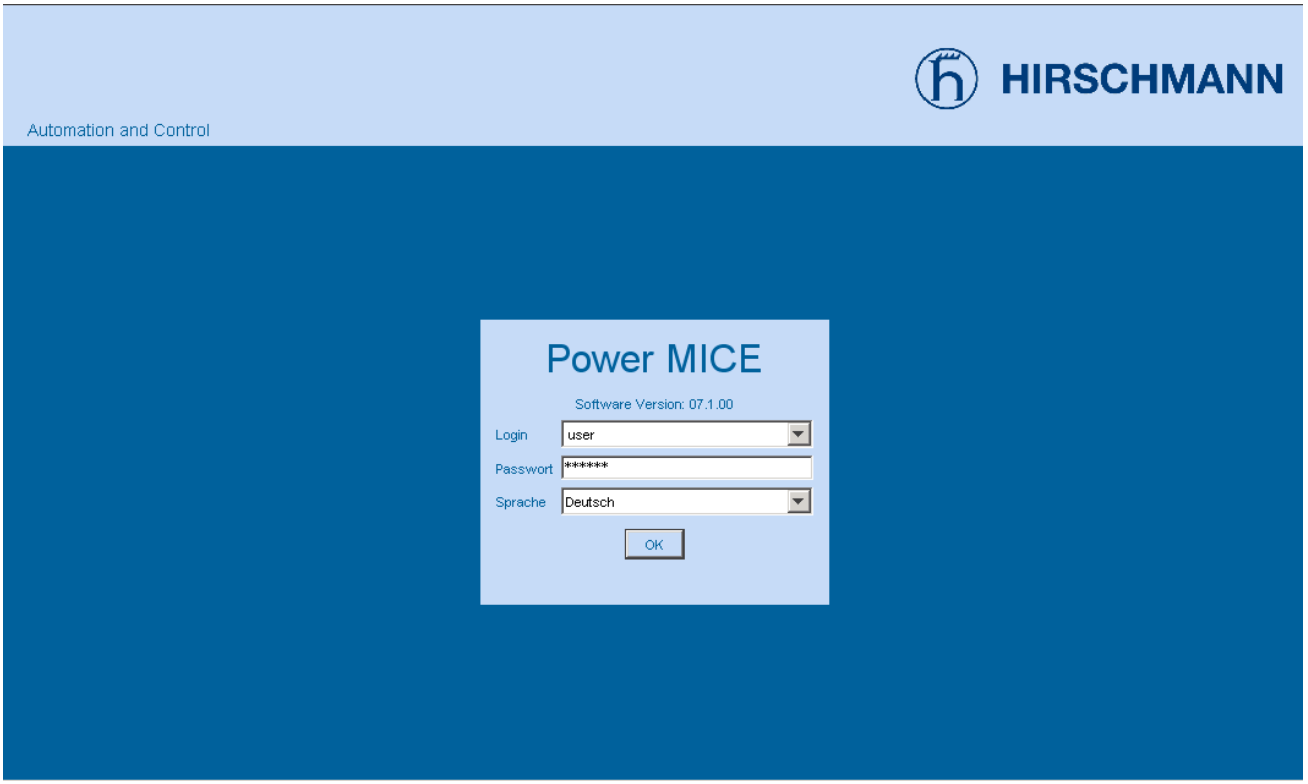


Abb. 1: Login-Fenster

- ☐ Wählen Sie den Benutzernamen und geben Sie das Passwort ein.
- ☐ Wählen Sie die Sprache, in der Sie die grafische Benutzeroberfläche verwenden möchten.
- ☐ Klicken Sie „Ok“.

Der Web-Browser zeigt die grafische Benutzeroberfläche.

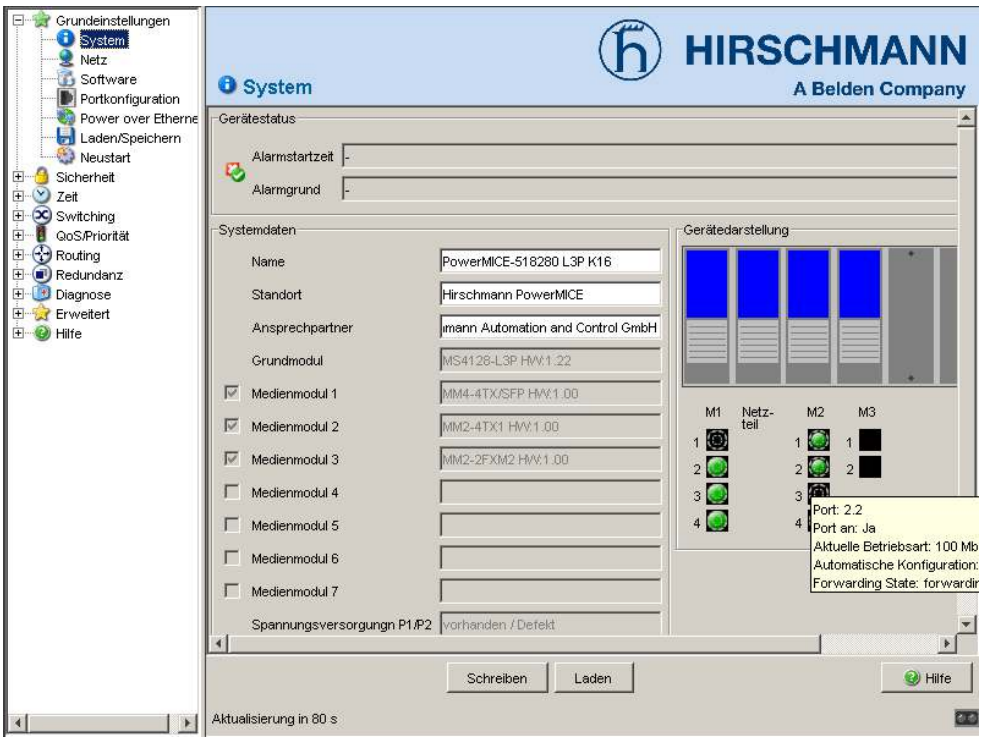
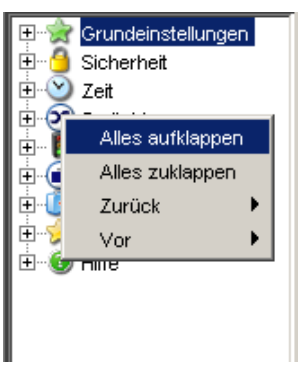


Abb. 2: Benutzeroberfläche (Web-based Interface) des Gerätes mit Tooltip

Hinweise zur Bedienung

Das Menü zeigt die Menüpunkte. Nach einem Klick auf einen Menüpunkt zeigt die Benutzeroberfläche den zugehörigen Dialog im Dialogteil an.



Ein Rechtsklick im Menüteil öffnet das Kontextmenü.

Bezeichnung	Bedeutung
Alles aufklappen	Klappt die Knoten im Menübaum auf. Der Menüteil zeigt die Menüpunkte sämtlicher Ebenen.
Alles zuklappen	Klappt die Knoten im Menübaum ein. Der Menüteil zeigt die Menüpunkte der obersten Ebene.
Knoten aufklappen	Klappt den ausgewählten Knoten auf und klappt die anderen Knoten im Menübaum ein. Diese Funktion bietet Ihnen die Möglichkeit, einen Hauptknoten aufzuklappen, ohne zu scrollen und ohne andere Knoten von Hand einzuklappen.
Zurück	Bietet Ihnen die Möglichkeit, per Schnellzugriff auf einen zuvor ausgewählten Menüpunkt zurückzuspringen.
Vor	Bietet Ihnen die Möglichkeit, per Schnellzugriff auf einen bereits ausgewählten Menüpunkt vorzuspringen, wenn Sie zuvor die „Zurück“-Funktion angewendet haben.

Tab. 1: Menüteil: Funktionen im Kontextmenü

Hinweise zum Speichern des Konfigurationsprofils

- ☐ Um geänderte Einstellungen in den flüchtigen Speicher zu kopieren, klicken Sie die Schaltfläche „Schreiben“.
- ☐ Um in den Dialogen die Anzeige zu aktualisieren, klicken Sie die Schaltfläche „Laden“.
- ☐ Damit geänderte Einstellungen auch nach dem Neustart des Gerätes erhalten bleiben, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken im Rahmen „Speichern“ die Schaltfläche „Sichern“.

Anmerkung: Unbeabsichtigte Änderungen an den Einstellungen führen möglicherweise zum Verbindungsabbruch zwischen Ihrem PC und dem Gerät. Bevor Sie die Einstellungen ändern, schalten Sie die Funktion „Konfigurationsänderung widerrufen“ im Dialog `Grundeinstellungen:Laden/Speichern` ein. Mit dieser Funktion stellt das Gerät die vorherige Konfiguration wieder her, wenn die Verbindung nach dem Ändern der Einstellungen abbricht. Das Gerät bleibt erreichbar.

1 Grundeinstellungen

Das Grundeinstellungen-Menü enthält die Dialoge, Anzeigen und Tabellen zur Grundkonfiguration:

- System
- Module
- Netz
- Software
- Portkonfiguration
- Power over Ethernet Plus
- Laden/Speichern
- Neustart

Anmerkung: Die grafische Oberfläche verwendet Java 7.

Installieren Sie die Software von www.java.com.

1.1 System

Das Untermenü „System“ im Grundeinstellungsmenü ist untergliedert in:

- Gerätestatus
- Systemdaten
- Gerätedarstellung
- Aktualisierung

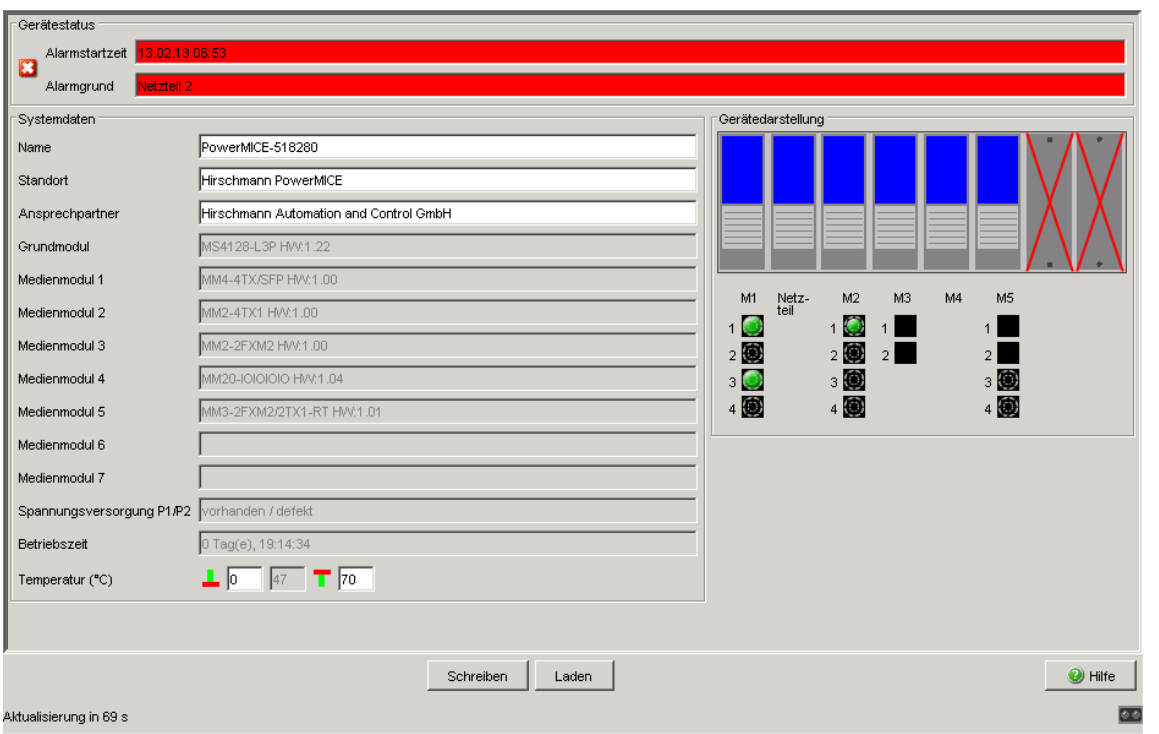


Abb. 3: Untermenü „System“

Gerätestatus

Dieser Bereich der grafischen Benutzeroberfläche gibt Auskunft über den Gerätestatus und Alarmzustand, den das Gerät erkannt hat.

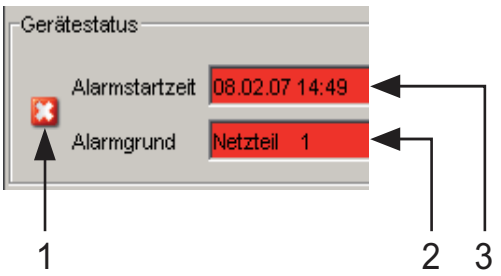


Abb. 4: Gerätestatus- und Alarm-Anzeige
1 - Das Symbol zeigt den Gerätestatus an
2 - Ursache des ältesten, bestehenden Alarms
3 - Beginn des ältesten, bestehenden Alarms

Systemdaten

Die Felder in diesem Rahmen zeigen Betriebsdaten sowie Informationen zum Standort des Gerätes.

– den Systemnamen,
– die Standortbezeichnung,
– den Namen des Ansprechpartners für dieses Gerät
– die Temperaturschwellen.

Bezeichnung	Bedeutung
Name	Systemname dieses Gerätes Wenn Sie die PROFINET-Funktion des Gerätes verwenden, darf der Systemname ausschließlich alphanumerische Zeichen, Bindestriche und Punkte enthalten.
Standort	Standort dieses Gerätes
Ansprechpartner	Ansprechpartner für dieses Gerät
Grundmodul	Hardware-Version des Geräts
Medienmodul 1	Hardware-Version des Medienmoduls 1
Medienmodul 2	Hardware-Version des Medienmoduls 2
Medienmodul 3	Hardware-Version des Medienmoduls 3
Medienmodul 4	Hardware-Version des Medienmoduls 4
Medienmodul 5	Hardware-Version des Medienmoduls 5
Medienmodul 6	Hardware-Version des Medienmoduls 6
Medienmodul 7	Hardware-Version des Medienmoduls 7
Spannungsversorgung (P1/P2)	Status der Netzteile (P1/P2)
Spannungsversorgung 3-1/3-2	Status der Netzteile 3-1/3-2
Spannungsversorgung 4-1/4-2	Status der Netzteile 4-1/4-2

Tab. 2: Systemdaten

Bezeichnung	Bedeutung
Lüfter	Status der Lüfter
Betriebszeit	Zeigt die Zeit, die seit dem letzten Neustart dieses Gerätes vergangen ist.
Temperatur (°C)	Temperatur im Gerät. Untere/obere Temperaturschwelle, bei deren Unter-/Überschreiten das Gerät einen Alarm generiert.

Tab. 2: Systemdaten

Gerätedarstellung

Die Gerätedarstellung zeigt das Gerät mit der aktuellen Bestückung. Der Zustand der einzelnen Ports wird durch eines der nachfolgenden Symbole dargestellt. Sie erhalten eine vollständige Beschreibung des Portzustandes, indem Sie den Mauszeiger über das Portsymbol stellen.

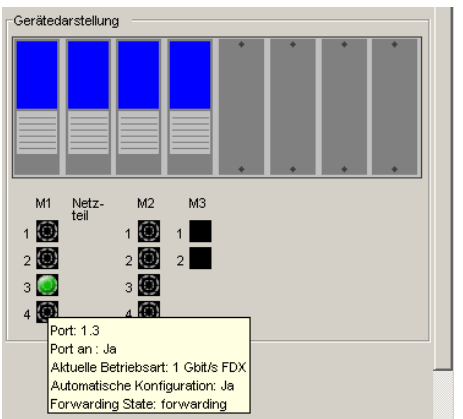


Abb. 5: Gerätedarstellung

Bedeutung der Symbole:

Der Port (10, 100 MBit/s, 1, 10 GBit/s) ist freigegeben und die Verbindung ist in Ordnung.

Der Port ist vom Management gesperrt und hat eine Verbindung.

Der Port ist vom Management gesperrt und hat keine Verbindung.

Der Port ist im Autonegotiation-Modus.

Der Port ist im HDX-Modus.

Der Port (100 MBit/s) ist im Discarding-Modus eines Redundanzprotokolls wie z.B. Spanning Tree oder HIPER-Ring.

Der Port ist im Routing-Modus (100 MBit/s).

Aktualisierung

Die grafische Benutzeroberfläche aktualisiert automatisch die Anzeige des Dialogs nach jeweils 100 Sekunden. Dabei aktualisiert sie die Felder und Symbole mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind. Im Dialog sehen Sie unten links, wann die nächste Aktualisierung stattfindet.

Abb. 6: Zeit bis zur Aktualisierung

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 3: Schaltflächen

1.2 Module (MS, PowerMICE, MACH102 und MACH4000)

Wenn Sie ein Modul in einen leeren Steckplatz des modularen Gerätes stecken, weist das Gerät dem Modul automatisch die Voreinstellungen für die Ports zu. Sobald das Modul alle Port-Voreinstellungen übernommen hat, ist ein Zugriff auf das Netzwerk möglich. Um einem Modul den Netzzugang zu verweigern, deaktivieren Sie den betreffenden Modul-Steckplatz. Das Gerät erkennt zwar das Modul und erlaubt eine Konfiguration der Ports, die Ports selber aber bleiben deaktiviert.

Um den Netzzugang über einen leeren Steckplatz zu verhindern nachdem Sie ein Modul entfernt haben, folgen Sie den untenstehenden Handlungsschritten.

- ☐ Entfernen Sie das Modul und aktualisieren Sie die grafische Benutzeroberfläche mit einem Klick auf „Laden“.
- ☐ Die Spalte „Modul-Status“ für das entfernte Modul enthält den Wert `configurable`. Das Gerät graut das entfernte Modul außerdem in der „Gerätedarstellung“ im Dialog `Grundeinstellungen:System` aus.
- ☐ Markieren Sie den Eintrag und klicken Sie „Modul entfernen“. Der Wert in der Spalte „Modul-Status“ ändert sich zu `remove`. Der betreffende Steckplatz ist in der „Gerätedarstellung“ im Dialog `Grundeinstellungen:System` als leer ausgewiesen. Zusätzlich enthält die Spalte „Typ“ für diesen Eintrag den Wert `none`. Die anderen Modulparameter löscht das Gerät selbstständig.
- ☐ Das angewählte Kontrollkästchen „Aktiv“ zeigt, dass der Steckplatz aktiv ist. Um über den leeren Steckplatz einen weiteren Netzzugang zu verbieten, deaktivieren Sie den Eintrag. Ein Abwählen des Kontrollkästchens deaktiviert den Eintrag. Sobald ein Eintrag in der Tabelle deaktiviert ist, zeigt das Gerät ein rotes „X“ über dem Steckplatz in der „Gerätedarstellung“ im Dialog `Grundeinstellungen:System`.

Um ein Modul in einen Steckplatz zu installieren, folgen Sie den untenstehenden Handlungsanweisungen.

☐ Stecken Sie das Modul in den Steckplatz und aktualisieren Sie die grafische Benutzeroberfläche mit einem Klick auf „Laden“. Das Gerät konfiguriert das Modul automatisch mit den Voreinstellungen, erkennt die Modul-Parameter und fügt die dazugehörigen Werte in die Tabelle ein.
☐ Der „Modul-Status“-Wert ändert sich zu `physical`.
☐ Um für das Modul den Netzzugang zu erlauben, wählen Sie das Kontrollkästchen „Aktiv“ an.

Anmerkung: Folgende modulare Geräte unterstützen diese Funktion: MS (soho), PowerMICE (ms4128), MACH102 (soho) und MACH4000 (ex und dx) Geräte-Familie.

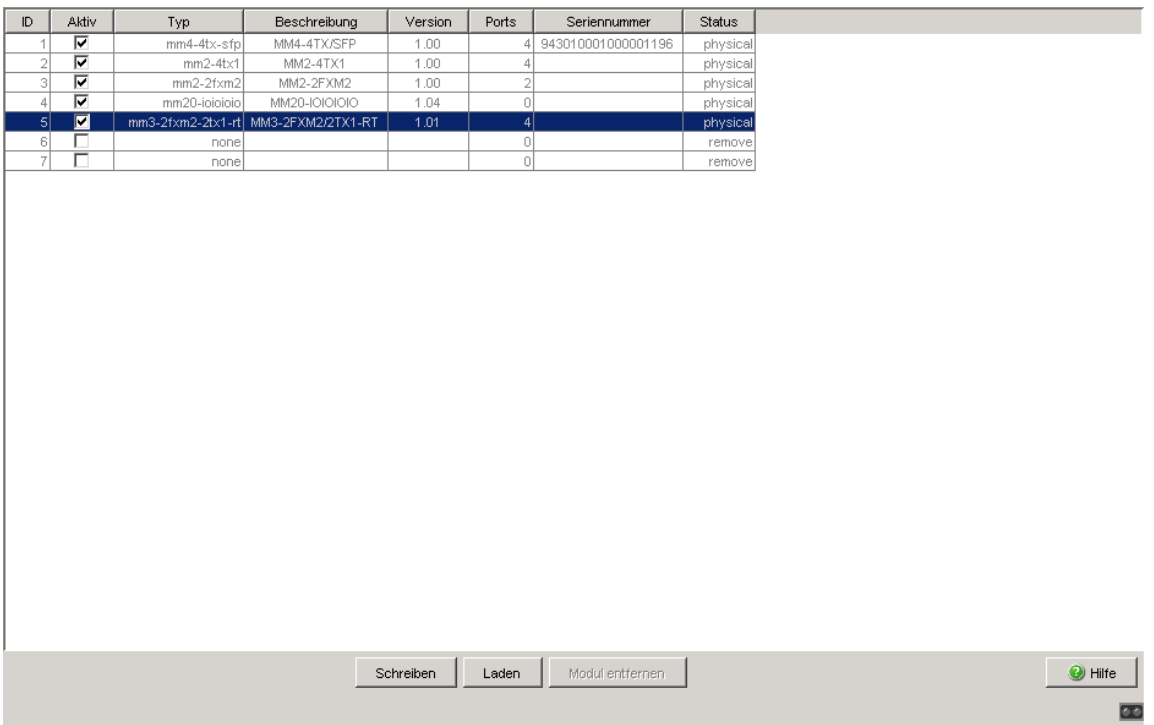


Abb. 7: Dialog „Module“

Diese Konfigurationstabelle bietet Ihnen die Möglichkeit, die Steckplätze zu aktivieren, zu deaktivieren oder die Modulparameter anzuzeigen.

- Die Spalte „ID“ bezeichet den Steckplatz, auf den sich der Eintrag bezieht.
- Die Spalte „Aktiv“ aktiviert den Netzzugang für das Modul, das in diesem Steckplatz installiert ist. Ist der Eintrag deaktiviert, zeigt das Gerät ein rotes „X“ über dem Steckplatz in der „Gerätedarstellung“ im Dialog `Grundeinstellungen:System`. Ist der Eintrag deaktiviert, erkennt das Gerät das in diesem Steckplatz installierte Modul. Das Modul selbst bleibt konfigurierbar.
- Die Spalte „Typ“ zeigt den Modul-Typ, der im Steckplatz installiert ist. Der Wert `none` zeigt an, dass der Steckplatz leer ist.
- Die Spalte „Beschreibung“ zeigt eine kurze Beschreibung des installierten Moduls.
- Die Spalte „Version“ zeigt die Modul-Version.
- Die Spalte „Ports“ zeigt, wie viele Ports am Modul verfügbar sind.
- Die Spalte „Seriennummer“ zeigt die Seriennummer des Moduls.
- Die Spalte „Modul-Status“ zeigt den Status des Steckplatzes an.
  - `physical` - zeigt an, dass ein Modul in einem Steckplatz vorhanden ist.
  - `configurable` - zeigt an, dass der Steckplatz leer und konfigurierbar ist.
  - `remove` - zeigt an, dass der Steckplatz leer.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Modul entfernen	Entfernt die Modulkonfiguration aus dem Gerät, wenn der Steckplatz leer ist.
Hilfe	Öffnet die Online-Hilfe.

Tab. 4: Schaltflächen

1.3 Netz

Mit dem Dialog `Grundeinstellungen:Netz` legen Sie fest, aus welcher Quelle das Gerät seine IP-Parameter nach dem Start erhält, weisen IP-Parameter und VLAN-ID zu und konfigurieren den HiDiscovery-Zugriff.

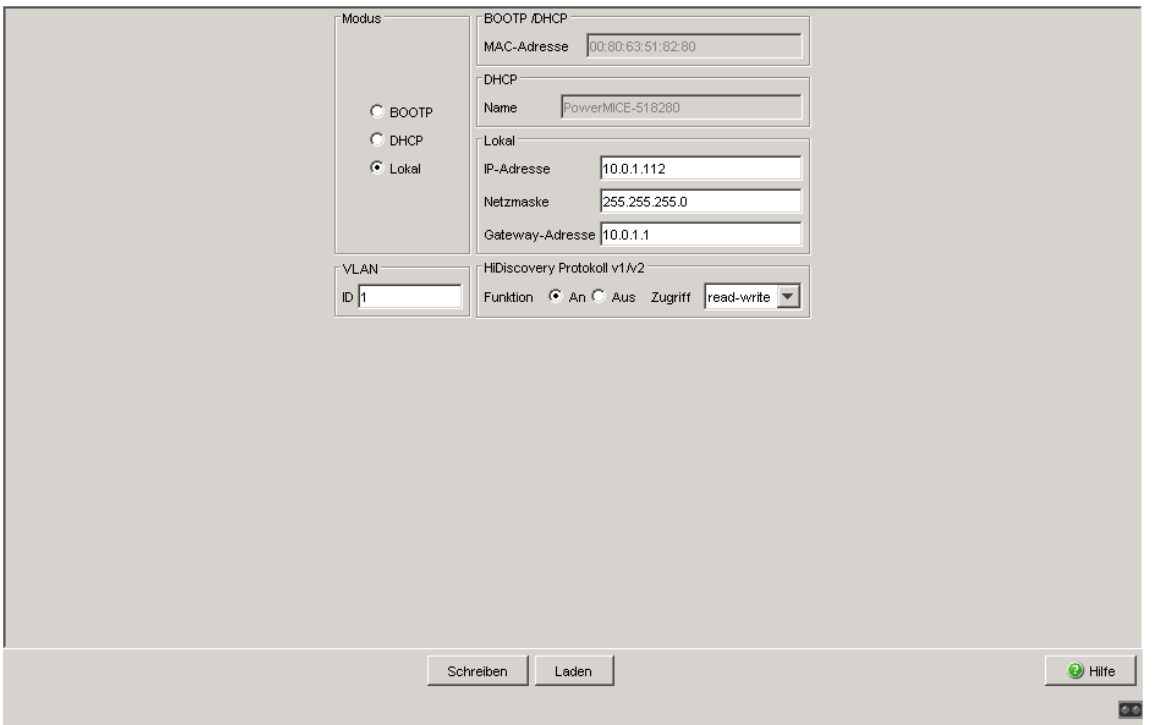


Abb. 8: Dialog Netzparameter

☐ Geben Sie unter „Modus“ ein, woher das Gerät seine IP-Parameter bezieht:
- Im Modus BOOTP erfolgt die Konfiguration durch einen BOOTP- oder DHCP-Server auf der Basis der MAC-Adresse des Gerätes (siehe auf Seite 52 „Laden/Speichern“).
- Im Modus DHCP erfolgt die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes (siehe auf Seite 52 „Laden/Speichern“).
- Im Modus lokal werden die Netzparameter aus dem Speicher des Gerätes verwendet.

☐ Geben Sie entsprechend des gewählten Modus rechts die Parameter ein.

☐ Den für das DHCP-Protokoll relevanten Namen geben Sie in der grafischen Benutzeroberfläche in der Zeile „Name“ des Dialogs `Grundeinstellungen:System` ein.

☐ Der Rahmen „VLAN“ bietet Ihnen die Möglichkeit, der Management-CPU des Geräts ein VLAN zuzuweisen. Wenn Sie hier als VLAN-ID 0 eingeben (im VLAN-Standard nicht enthalten), dann ist die Management-CPU von allen VLANs erreichbar.

☐ Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät eine IP-Adresse zuzuweisen. Aktivieren Sie das HiDiscovery-Protokoll, wenn Sie von Ihrem PC aus mit der mitgelieferten HiDiscovery-Software dem Gerät eine IP-Adresse zuweisen wollen (Voreinstellung: Funktion „an“, Zugriff „read-write“).

Anmerkung: Wenn Sie den Netz-Modus von „Lokal“ auf „BOOTP“ oder „DHCP“ setzen, weist der Server dem Gerät eine neue IP-Adresse zu. Wenn der Server nicht antwortet, wird die IP-Adresse auf 0.0.0.0 gesetzt und der BOOTP/DHCP-Prozess versucht erneut, eine IP-Adresse zu bekommen.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 5: Schaltflächen

1.4 Software

Dieser Dialog bietet Ihnen folgende Funktionen:

- die im Gerät vorhandenen Software-Versionen anzeigen.
- ein Software-Update des Gerätes mittels http (über ein Datei-Auswahl-Fenster), tftp oder ACA durchführen.
- die im Flash gespeicherte Backup-Version der Software wiederherstellen.

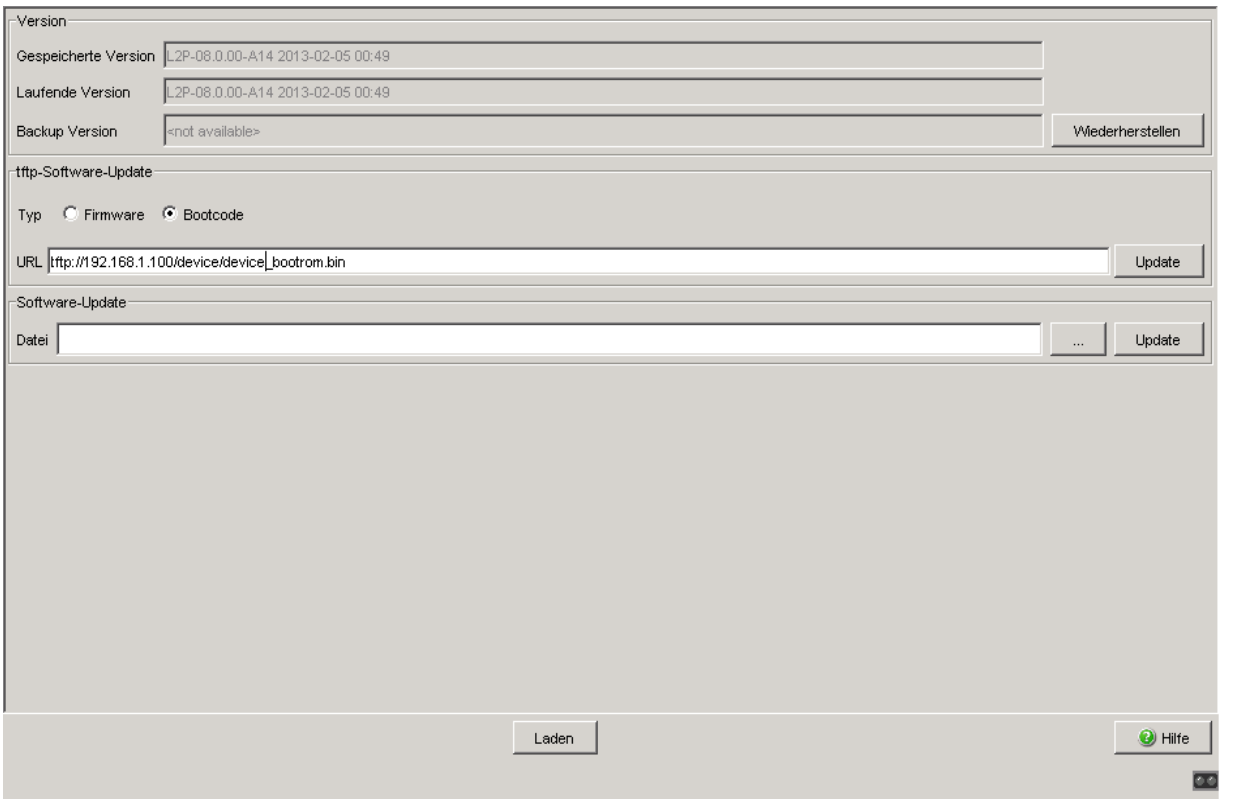


Abb. 9: Dialog Software

1.4.1 Anzeige der im Gerät vorhandenen Software-Versionen

Der Dialog zeigt die vorhandenen Software-Versionen:

- Gespeicherte Version:
  Die Version der im Flash gespeicherten Software.
- Laufende Version:
  Die Version der aktuell ausgeführten Software.
- Backup-Version:
  Die Version der im Flash gespeicherten vorigen Software.

1.4.2 Wiederherstellen der Backup-Version

„Wiederherstellen“ tauscht die gespeicherte Version der Software mit der Backup-Version der Software. Zeitgleich findet ein Austausch der zugehörigen Konfigurations-Dateien statt. Der Austausch der Software-Versionen wird erst nach einem Kaltstart wirksam. Ein Warmstart hat keinerlei Auswirkung.

☐ Klicken Sie auf die Schaltfläche „Wiederherstellen“, um die gespeicherte Version der Software mit der Backup-Version zu tauschen.

☐ Nach erfolgreichem Tausch aktivieren Sie die wieder hergestellte Software:
Wählen Sie den Dialog `Grundeinstellungen: Neustart` und führen Sie einen Kaltstart durch.
Bei einem Kaltstart lädt das Gerät die Software neu aus dem nichtflüchtigen Speicher, startet neu und führt einen Selbsttest durch.

☐ Laden Sie die grafische Benutzeroberfläche in Ihrem Browser neu, um nach dem Neustart wieder auf das Gerät zuzugreifen.

1.4.3 tftp-Software-Update

Für ein tftp-Update benötigen Sie einen tftp-Server, auf dem die zu ladende Software abgelegt ist.
Der URL kennzeichnet den Pfad zu der auf dem tftp-Server gespeicherten Software. Der URL hat die Form
tftp://IP-Adresse des tftp-Servers/Pfadname/Dateiname
(z.B. `tftp://192.168.1.1/device/device.bin`).

☐ Wählen Sie das Optionsfeld „Firmware“.
☐ Geben Sie den URL zum Speicherort der Software ein.
☐ Klicken Sie auf „Update“, um die Software vom TFTP-Server auf das Gerät zu laden.
☐ Um die neue Software nach dem Laden zu starten, führen Sie einen Kaltstart des Gerätes durch.

Siehe „Neustart” auf Seite 68.

1.4.4 tftp-Bootcode-Update

Für ein TFTP-Update benötigen Sie einen TFTP-Server, auf dem der notwendige Bootcode abgelegt ist.
Der URL kennzeichnet den Pfad zum auf dem TFTP-Server gespeicherten Bootcode. Der URL hat die Form
tftp://IP-Adresse des TFTP-Servers/Pfadname/Dateiname
(z. B. `tftp://192.168.1.1/device/device_bootrom.bin`).

Anmerkung: Im Falle einer Unterbrechung des Bootcode-Updates ist das Gerät irreparabel beschädigt. Führen Sie dieses Update unter der Aufsicht des Hirschmann-Support-Desks durch.

☐ Wählen Sie das Optionsfeld „Bootcode“.
☐ Geben Sie den URL zum Speicherort des Bootcodes ein.

☐ Klicken Sie auf „Update“, um den Bootcode vom TFTP-Server auf das Gerät zu laden.
☐ Um den neuen Bootcode nach dem Laden zu starten, führen Sie einen Kaltstart des Gerätes durch.
Siehe „Neustart” auf Seite 68.

1.4.5 http-Software-Update

Für ein Software-Update über das Datei-Auswahl-Fenster kopieren Sie die Geräte-Software auf einem Datenträger, den Sie von Ihrem PC aus erreichen.

☐ Klicken Sie auf „…" im Rahmen „Software-Update“.

☐ Wählen Sie im Dialog „Öffnen“ die Image-Datei der Geräte-Software mit der Endung `*.bin`.

☐ Klicken Sie „Öffnen“.

☐ Klicken Sie „Update“, um die Software auf das Gerät zu übertragen. Sobald die Datei vollständig übertragen ist, beginnt das Gerät mit dem Update der Geräte-Software. Wenn das Update erfolgreich war, zeigt das Gerät die Meldung „Firmware-Update erfolgreich …“.

1.4.6 Automatischer Software-Update vom ACA

Das Gerät bietet Ihnen außerdem die Möglichkeit, ein automatisches Software-Update von einem externen Speicher aus durchzuführen. Details dazu finden Sie im Dokument „Anwender-Handbuch Grundkonfiguration“ im Kapitel „Automatisches Software-Update von externem Speicher“.

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 6: Schaltflächen

1.5 Portkonfiguration

Diese Konfigurationstabelle bietet Ihnen die Möglichkeit, jeden Port des Gerätes zu konfigurieren und die aktuelle Betriebsart jedes Ports anzuzeigen (Verbindungszustand (Link), Bitrate (Geschwindigkeit) und Duplex-Modus).

- Die Spalte „Port“ zeigt die Nummer des Geräte-Ports, auf den sich der Tabelleneintrag bezieht.
- In der Spalte „Name“ haben Sie die Möglichkeit, für jeden Port einen beliebigen Namen einzutragen.
- In der Spalte „Port an“ haben Sie die Möglichkeit, den Port durch Ankreuzen einzuschalten.
- In der Spalte „Verbindungsfehler weitermelden“ legen Sie durch Ankreuzen fest, dass beim Auftreten eines Link-Alarms dies an den Gerätezustand und/oder direkt an den Meldekontakt weitergeleitet wird.
- In der Spalte „Automatische Konfiguration“ aktivieren Sie die automatische Auswahl der Betriebsart (Autonegotiation) und die automatische Belegung der Anschlüsse (Auto Cable-Crossing) eines TP-Ports, indem Sie das zugehörige Feld ankreuzen. Nach dem Einschalten der automatischen Konfiguration vergehen einige Sekunden, bis die Betriebsart eingestellt ist.
- In der Spalte „Manuelle Konfiguration“ stellen Sie die Betriebsart an diesem Port ein. Die möglichen Betriebsarten sind vom Medienmodul abhängig. Mögliche Betriebsarten sind:
  - 10 Mbit/s Halbduplex (HDX)
  - 10 Mbit/s Vollduplex (FDX)
  - 100 Mbit/s Halbduplex (HDX)
  - 100 Mbit/s Vollduplex (FDX)
  - 1000 Mbit/s Halbduplex (HDX)
  - 1000 Mbit/s Vollduplex (FDX)
  - 10 Gbit/s Vollduplex (FDX)
- Die Spalte „Link/Aktuelle Betriebsart“ zeigt die aktuelle Betriebsart und damit gleichzeitig eine bestehende Verbindung an.

- In der Spalte „Manuelles Cable-Crossing (Auto. Konfig. aus)“ stellen Sie die Belegung der Anschlüsse eines TP-Ports ein, wenn „Automatische Konfiguration“ für diesen Port deaktiviert ist. Mögliche Einstellungen sind:
  - enable: Das Gerät behält das Sende- und Empfangs-Leitungspaar des TP-Kabels für diesen Port unvertauscht bei (MDI).
  - disable: Das Gerät vertauscht das Sende- und Empfangs-Leitungspaar des TP-Kabels für diesen Port (MDIX).
  - nicht unterstützt: Der Port unterstützt diese Funktion nicht (optischer Port, TP-SFP-Port).
- In der Spalte „Flusskontrolle“ legen Sie durch Ankreuzen fest, dass an diesem Port Flusskontrolle aktiv ist. Aktivieren Sie hierzu auch den globalen Schalter "Flusskontrolle" (siehe auf Seite 164 „Switching Global“).

Anmerkung: Das Gerät unterstützt Copper-Gigabit-Ports mit eingeschaltetem Auto-Negotiation.

Anmerkung: Die aktive automatische Konfiguration hat Vorrang vor der manuellen Konfiguration.

Anmerkung: Falls Sie Link-Aggregation einsetzen, beachten Sie deren Konfiguration (siehe auf Seite 254 „Link-Aggregation“).

Anmerkung: Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Geräte-Ports. Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt.

Anmerkung: Für die Ringports beim HIPER-Ring sind folgende Einstellungen erforderlich:

Port-Typ	Bitrate	Autonegotiation (Automatische Konfiguration)	Port-Einstellung	Duplex
TX	100 Mbit/s	aus	an	voll
TX	1 Gbit/s	an	an	-
Optisch	100 Mbit/s	aus	an	voll
Optisch	1 Gbit/s	an	an	-
Optisch	10 Gbit/s	aus	an	voll

Tab. 7: Port-Einstellungen für Ring-Ports

Mit dem Umschalten des DIP-Schalters für die Ringports setzt das Gerät diese erforderlichen Einstellungen für die Ringports in der Konfigurationstabelle. Der durch das Umschalten vom Ringport zum normalen Port gewandelte Port erhält die Einstellung Autonegotiation (Automatische Konfiguration) an und Port an. Die Einstellungen bleiben für alle Ports weiterhin veränderbar.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 8: Schaltflächen

1.6 Power over ETHERNET

Anmerkung: Die folgenden Geräte sind mit Power over Ethernet- (PoE-) Ports ausgestattet:

- RS20/30
- MS20/30
- PowerMICE
- OCTOPUS
- MACH 4002
- MACH 1020/1030/1040

Die Bedienung dieser Geräte finden Sie in diesem Kapitel.

Anmerkung: Die beiden folgenden Geräte sind dagegen mit Power over Ethernet **Plus**- (**PoE+**-) Ports ausgestattet

- MACH104-16TX-PoEP und
- MACH 102 mit Medienmodul M1-8TP-RJ45 PoEP

Die Bedienung dieser Geräte finden Sie im Kapitel „Power over Ethernet Plus“.

Ist das Gerät mit PoE-Medienmodulen ausgestattet, dann bietet es Ihnen die Möglichkeit, Endgeräte wie z.B. IP-Telefone über das Twisted-Pair-Kabel mit Strom zu versorgen. PoE-Medienmodule unterstützen Power over ETHERNET nach IEEE 802.3af.
Im Lieferzustand ist die Funktion Power over ETHERNET global und an allen PoE-fähigen Ports eingeschaltet.

Nominale Leistung für MS20/30, MACH 1000 und PowerMICE:
Das Gerät bietet die nominale Leistung für die Summe aller PoE-Ports zuzüglich einer Reserve. Da das PoE-Medienmodul seine PoE-Spannung von extern bezieht, kennt das Gerät die mögliche nominale Leistung nicht. Deshalb nimmt das Gerät an dieser Stelle als „Nominale Leistung“ den Wert 60 Watt pro PoE-Medienmodul an.

Nominale Leistung für MACH 4000:
Das Gerät bietet die nominale Leistung für die Summe aller PoE-Ports zuzüglich einer Reserve. Benötigen die angeschlossenen Geräte mehr PoE-Leistung, als die angebotene PoE-Leistung, dann schaltet das Gerät PoE an Ports aus. Zunächst schaltet das Gerät PoE an den Ports mit der niedrigsten PoE-Priorität ab. Haben mehrere Ports die gleiche Priorität, dann schaltet das Gerät zuerst PoE an den Ports mit der höheren Portnummer ab.

Rahmen „Funktion“:
☐ Mit „An/Aus" schalten Sie PoE ein oder aus.

Rahmen „Konfiguration“:
☐ „Verschicke Trap“ bietet Ihnen die Möglichkeit, das Gerät zu veranlassen, in folgenden Fällen einen Trap zu senden:
  – Beim Überschreiten/Unterschreiten der Leistungsschwelle.
  – Beim Ein-/Ausschalten der PoE-Versorgungsspannung an mindestens einem Port.
☐ Geben Sie eine Leistungsschwelle unter „Threshold“ an. Ist die Funktion „Verschicke Trap“ aktiviert, sendet das Gerät einen Trap, sobald das Gerät diesen Wert über- oder unterschreitet. Die Leistungsschwelle geben Sie in Prozent der abgegebenen Leistung zur nominalen Leistung ein.
☐ „Budget [W]“ zeigt die Leistung an, die das Gerät den PoE-Ports nominal zur Verfügung stellt.
☐ „Reserviert [W]“ zeigt an, wieviel Leistung das Gerät den angeschlossenen PoE-Geräten aufgrund ihrer Klassifizierung maximal zur Verfügung stellt.
☐ „Abgegeben [W]" zeigt an, wie groß der momentane Leistungsbedarf der PoE-Ports ist.

Die Differenz von „Nominale“ und „Reservierte“ Leistung gibt an, wieviel Leistung an den freien PoE+-Ports noch zur Verfügung steht.

Port-Tabelle:

Die Tabelle zeigt ausschließlich Ports an, die PoE unterstützen.

☐ In der Spalte „POE an“ haben Sie die Möglichkeit, PoE an diesem Port ein-/auszuschalten.
☐ Die Spalte „Status" zeigt den PoE-Status des Ports an.
☐ In der Spalte „Priorität" (MACH 4000) legen Sie die PoE-Priorität „niedrig“, „hoch“ oder „kritisch" des Ports fest.

- ☐ Die Spalte "Class" zeigt die Klasse des angeschlossenen Gerätes an:
  Class: Maximal abgegebene Leistung
  0: 15,4 W = Lieferzustand
  1: 4,0 W
  2: 7,0 W
  3: 15,4 W
  4: reserviert, wie Klasse 0 behandeln
- ☐ Die Spalte „Verbrauch [W]“ zeigt die aktuelle Leistungsabgabe an dem jeweiligen Port an.
- ☐ Die Spalte „Name“ zeigt den Namen des Ports an, siehe `Grundeinstellungen:Portkonfiguration`.

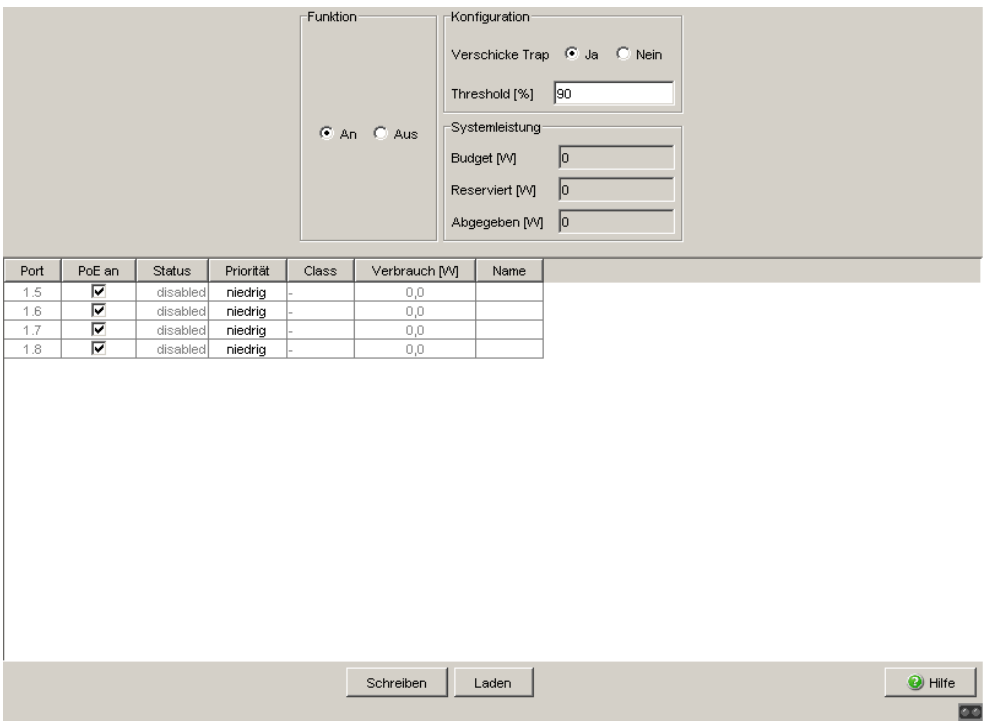


Abb. 10: Dialog Power over Ethernet

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 9: Schaltflächen

1.7 Power over Ethernet Plus

Anmerkung: Die folgenden Geräte sind mit Power over Ethernet **Plus**-(**PoE+**-) Ports ausgestattet

- MACH104-16TX-PoEP und
- MACH 102 mit Medienmodul M1-8TP-RJ45 PoEP

Die Bedienung dieser beiden Geräte finden Sie in diesem Kapitel.

Die folgenden Geräte sind dagegen mit Power over Ethernet- (PoE-) Ports ausgestattet:

- RS20/30
- MS20/30
- PowerMICE
- OCTOPUS
- MACH 4002
- MACH 1020/1030/1040

Die Bedienung dieser Geräte finden Sie im Kapitel „Power over ETHERNET“.

Geräte mit Power over Ethernet Plus- (PoE+-) Ports bieten Ihnen die Möglichkeit, Endgeräte wie z.B. IP-Telefone über das Twisted-Pair-Kabel mit Strom zu versorgen. PoE+-Ports unterstützen Power over Ethernet Plus nach IEEE 802.3at.
Im Lieferzustand ist die Funktion Power over Ethernet Plus sowohl global als auch an allen PoE+-fähigen Ports eingeschaltet.

Das Anschließen einer zu hohen Anzahl von PoE+ Powered Devices (PD) kann Ihre externe PoE+ Spannungsversorgung überlasten. Diese kann dadurch möglicherweise ausfallen. Der Dialog Power over Ethernet Plus unterstützt Sie beim Verwalten Ihrer Spannungsversorgung und hilft Ihnen, Ihre externen PoE+ Spannungsversorgungsgeräte vor Überlastung zu schützen.

Für die Geräte

- MACH104-16TX-PoEP und
- MACH 102 mit Medienmodul M1-8TP-RJ45 PoEP:

- Maximale Leistung für MACH104-16TX-PoEP:
  Das Gerät bietet eine maximale Leistung von 248 W für die Summe aller PoE-Ports.

- Maximale Leistung für MACH 102 mit Medienmodul M1-8TP-RJ45 PoE:
  Das Gerät bietet die maximale Leistung für die Summe aller PoE-Ports. Da das PoE+-Medienmodul seine PoE+-Spannung von extern bezieht, kennt das Gerät die mögliche maximale Leistung nicht.
  Deshalb verwendet das Gerät an dieser Stelle als „maximale Leistung“ den Wert 124 Watt pro PoE+-Medienmodul M1-8TP-RJ45 PoE.

Benötigen die angeschlossenen PDs mehr PoE-Leistung als die angebotene PoE-Leistung, dann schaltet das Gerät PoE an bestimmten Ports aus. Zunächst schaltet das Gerät PoE an den Ports mit der niedrigsten PoE-Priorität ab. Haben mehrere Ports die gleiche Priorität, dann schaltet das Gerät zuerst PoE an den Ports mit der höheren Portnummer ab.

1.7.1 Power over Ethernet Plus - Global

Rahmen „Funktion“:

Parameter	Bedeutung	Wertebereich	Voreinstellung
Funktion	Power over Ethernet Plus Funktion ein-/ausschalten.	`An, Aus`	An

Tab. 10: PoE+ Global - Funktion

Rahmen „Konfiguration“:

Parameter	Bedeutung	Wertebereich	Voreinstellung
Verschicke Trap	Veranlasst das Gerät, in folgenden Fällen einen Trap zu senden: ▶ beim Überschreiten/Unterschreiten der Leistungsschwelle. ▶ beim Ein-/Ausschalten der PoE+-Versorgungsspannung an mindestens einem Port.	`Ja, Nein`	Ja
Threshold [%] (Leistungsschwelle)	Leistungsschwelle in Prozent der nominalen Leistung, bei deren Überschreiten/Unterschreiten das Gerät ein Trap sendet, sofern „Verschicke Trap" eingeschaltet ist.	`0 - 99%`	90%

Tab. 11: PoE+ Global - Konfiguration

Rahmen „Systemleistung“:

Parameter	Bedeutung	Wertebereich	Voreinstellung
Budget [W]	Zeigt die Leistung an, die das Gerät nominal für die PoE+-Ports zur Verfügung stellt.	`0 - 248 W`	`248 W`
Reserviert [W]	Zeigt an, wie viel Leistung das Gerät den angeschlossenen PoE+-Geräten aufgrund ihrer Klassifizierung maximal zur Verfügung stellt.	`0 - 248 W`	`0 W`
Abgegeben [W]	Zeigt an, wie groß der momentane Leistungsbedarf an den PoE+-Ports ist.	`0 - 248 W`	-

Tab. 12: PoE+ Global - Systemleistung

Die Differenz von „Konfigurierte Leistung“ und „Reservierte Leistung“ gibt an, wieviel Leistung an den freien PoE+-Ports noch zur Verfügung steht.

Tabelle „Global“:

Parameter	Bedeutung	Wertebereich	Voreinstellung
Modul	▶ Für MACH102-Medienmodule M1-8TP-RJ45 PoE: Modul = Steckplatznummer des PoE+Moduls ▶ Für MACH104-16TX-PoEP Geräte: Modul = 1	1 - 2	-
Konfiguriertes Leistungsbudget [W]	Konfigurieren Sie, welches Leistungsbudget das Gerät nominal für die PoE+-Ports des Moduls zur Verfügung stellt.	0 - 248 W	248 W
Maximales Leistungsbudget [W]	Zeigt die Leistung an, die das Gerät nominal für die PoE+-Ports des Moduls zur Verfügung stellt.	0 - 248 W	248 W
Reservierte Leistung [W]	Zeigt an, wie viel Leistung das Gerät allen am Modul angeschlossenen PoE+-Geräten zusammen auf Grund ihrer Klassifizierung maximal zur Verfügung stellt.	0 - 248 W	0 W
Abgegebene Leistung [W]	Zeigt an, wie groß der momentane Leistungsbedarf an allen PoE+-Ports des Moduls ist.	0 - 248 W	-
Threshold (Grenzwert) [%]	Geben Sie die Leistungsschwelle in Prozent der nominalen Leistung an, bei deren Überschreiten/Unterschreiten am Modul das Gerät ein Trap sendet, sofern „Verschicke Trap“ eingeschaltet ist.	0 - 99%	90%
Trap Benachrichtigung	Veranlasst das Gerät, in folgenden Fällen einen Trap zu senden: ▶ Beim Überschreiten/Unterschreiten der Leistungsschwelle. ▶ Beim Ein-/Ausschalten der PoE+-Versorgungsspannung an mindestens einem Port.	An, Aus	An

Tab. 13: Power over Ethernet Plus - Global

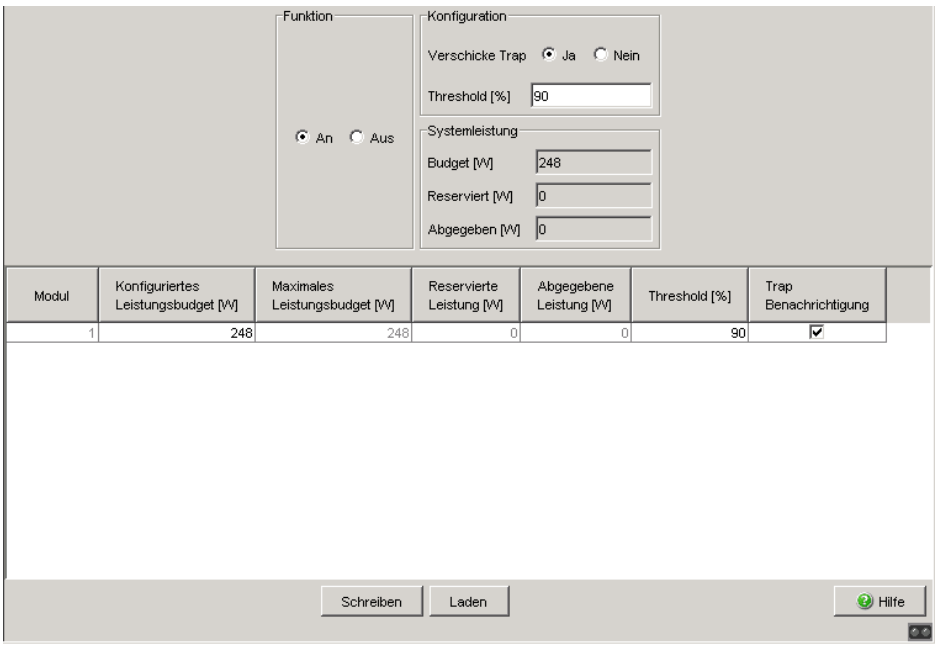


Abb. 11: Dialog Power over Ethernet Plus:Global

Anmerkung: Für die Geräte MACH 102 mit Medienmodul M1-8TP-RJ45 PoE: Wir empfehlen, die PoE+-Leistung auf die beiden Portgruppen (Ports 5 bis 12 und Ports 13 bis 20) gleichmäßig zu verteilen.

1.7.2 Power over Ethernet Plus - Port

Die Tabelle zeigt ausschließlich Ports an, die PoE+ unterstützen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Port	Modul- und Port-Nummer des PoE+–Ports, für den dieser Eintrag gilt. Beim MACH104-16TX-PoEP Gerät unterstützen die Ports 1.5 bis 1.20 PoE+.	`1,5 - 1,20 dB`	-
PoE an	Power over Ethernet Plus Funktion für diesen Port ein-/ausschalten.	`An, Aus`	`An`
Status	Zeigt den PoE+-Status des Ports an.	`suche, …`	`suche, …`
Priorität	Legen Sie die PoE+-Priorität des Ports fest.	`niedrig, hoch, kritisch`	`niedrig`
Klasse	Zeigt die Klasse des angeschlossenen Gerätes an:Class: Maximal abgegebene Leistung ▶ 0: 15,4 W ▶ 1: 4,0 W ▶ 2: 7,0 W ▶ 3: 15,4 W ▶ 4: 30,0 W	`0 - 4`	-
Verbrauch [W]	Zeigt die aktuelle Leistungsabgabe an dem jeweiligen Port an.	`0,0 - 248,0 W`	-

Tab. 14: Power over Ethernet Plus - Port

Parameter	Bedeutung	Wertebereich	Voreinstellung
Leistungslimit [mW]	Legt die Leistung in Watt fest, die der Port maximal abgibt. Diese Funktion bietet Ihnen die Möglichkeit, das zur Verfügung stehende Leistungs-Budget bedarfsgerecht auf die PoE-Ports zu verteilen. Beispielsweise reserviert der Port für ein angeschlossenes Gerät ohne "Power Class"-Funktion pauschal 15,4 W (Klasse 0), selbst wenn das Gerät weniger Leistung benötigt. Die überschüssige Leistung steht keinem anderen Port zur Verfügung. Durch das Festlegen des Leistungslimits reduzieren Sie die reservierte Leistung auf den tatsächlichen Bedarf des angeschlossenen Gerätes. Die ungenutzte Leistung steht für andere Ports zur Verfügung. Wenn Ihnen die genaue Leistungsaufnahme des angeschlossenen Gerätes unbekannt ist, beobachten Sie den Wert im Feld „Maximal überwacht [W]“. Das Leistungslimit muss größer sein als der Wert im Feld „Maximal überwacht [W]“. Wenn die maximal überwachte Leistung größer ist als das eingestellte Leistungslimit, betrachtet das Gerät das Leistungslimit als ungültig. Das Gerät zieht in diesem Fall wieder die PoE-Klasse zur Berechnung heran.	`0 - 30,0`	`0`
Maximal überwacht [mW]	Zeigt, welche maximale Leistung in Watt das Gerät bisher aufgenommen hat. Den Wert setzen Sie zurück, wenn Sie PoE auf dem Port deaktivieren oder wenn die Verbindung zum angeschlossenen Gerät trennen.	`0 - 30,0`	–
Name	Zeigt den Namen des Ports an, siehe `Grundeinstellungen:Portkonfiguration`	-	-

Tab. 14: Power over Ethernet Plus - Port

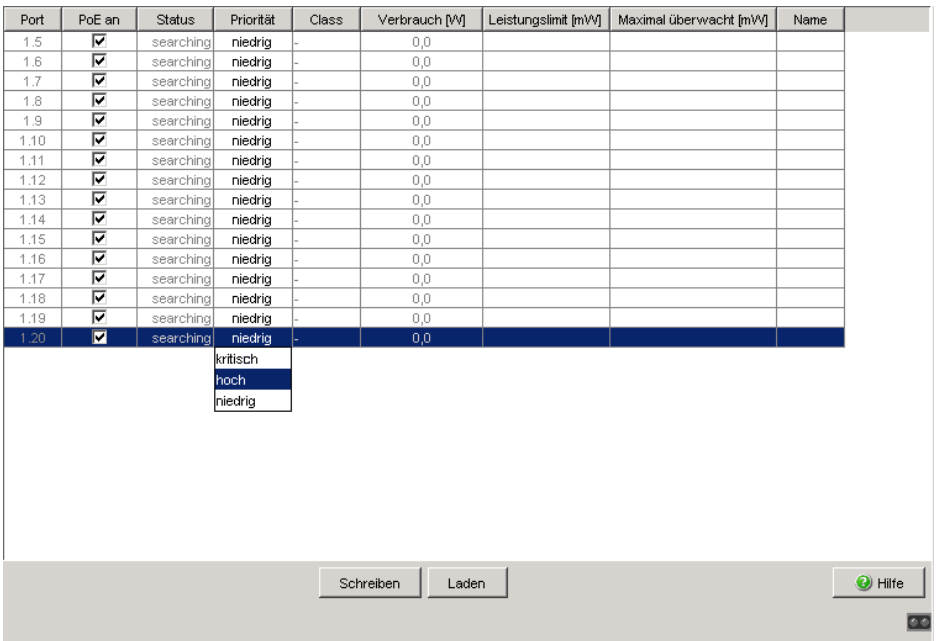


Abb. 12: Dialog Power over Ethernet Plus:Port

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 15: Schaltflächen

1.8 Laden/Speichern

Dieser Dialog bietet Ihnen die Möglichkeit,

- eine Konfiguration zu laden,
- eine Konfiguration zu speichern,
- einen URL einzugeben,
- den Lieferzustand herzustellen,
- den ACA zur Konfiguration zu verwenden,
- eine Konfigurationsänderung zu widerrufen.

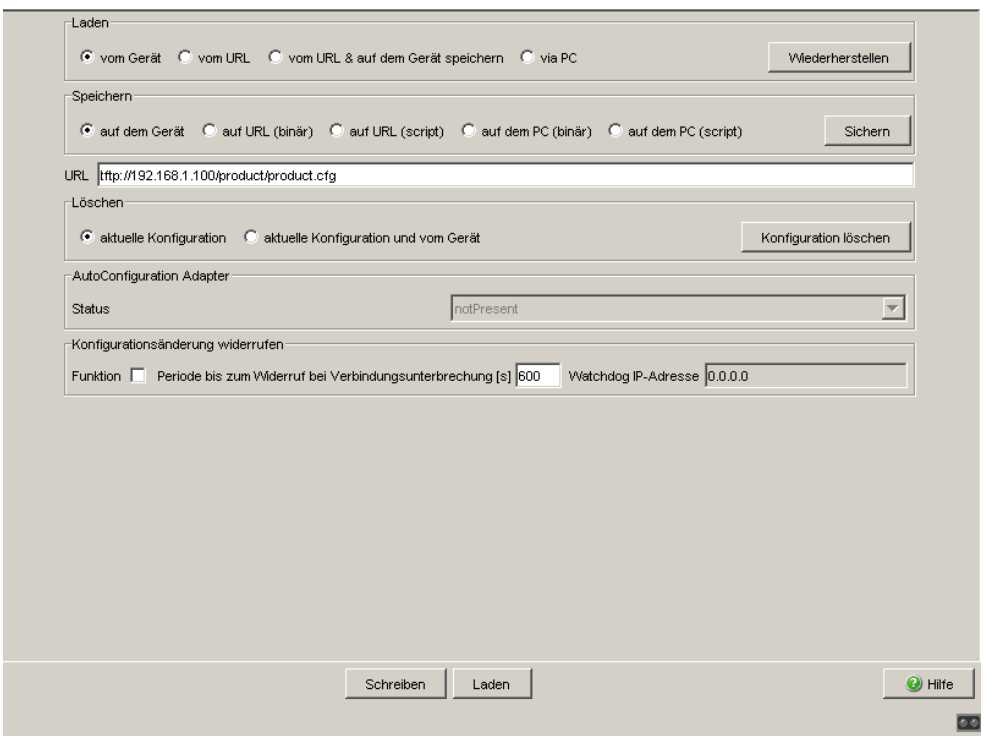


Abb. 13: Dialog Laden/Speichern

1.8.1 Konfiguration laden

Im Rahmen „Laden“ haben Sie die Möglichkeit,

- eine auf dem Gerät gespeicherte Konfiguration zu laden,
- eine unter dem angegebenen URL gespeicherte Konfiguration zu laden,
- eine unter dem angegebenen URL gespeicherte Konfiguration zu laden und auf dem Gerät zu speichern,
- eine auf dem PC als editier- und lesbares Script oder im Binärformat gespeicherte Konfiguration zu laden.
- eine auf dem PC für den Offline-Konfigurator im XML-Format gespeicherte Konfiguration zu laden.

Wenn Sie die laufende Konfiguration verändern (z. B. einen Port ausschalten), ändert die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol im Navigationsbaum von einem Diskettensymbol in ein gelbes Dreieck. Nach dem Speichern der Konfiguration zeigt die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol wieder als Diskette an.

Konfiguration von Offline-Konfigurator laden

Offline-Konfigurator installieren und starten
Um eine Konfigurationsdatei im Offline-Konfigurator zu erstellen, gehen Sie wie folgt vor:

☐ Falls Sie den Offline-Konfigurator noch nicht auf Ihrem PC installiert haben: Installieren Sie den Offline-Konfigurator, indem Sie die auf der CD-ROM enthaltene Installationsdatei „Setup.exe“ aus dem Ordner „ocf_setup“ ausführen.

☐ Starten Sie den Offline-Konfigurator durch Doppelklick auf das Desktop-Symbol „Offline Management“.

Eine XML-Konfigurationsdatei mit dem Offline-Konfigurator erstellen

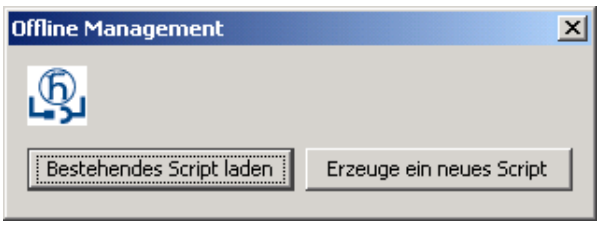


Abb. 14: Auswahl Offline Management

▶ Ein bestehendes Script überarbeiten

☐ Klicken Sie auf „Bestehendes Script laden“, um ein bereits erstelltes Script zur Überarbeitung in den Offline-Konfigurator zu laden.

▶ Ein neues Script erzeugen

☐ Klicken Sie auf „Erzeuge ein neues Script“, um mit Hilfe des Offline-Konfigurators ein neues Script zu erstellen.

☐ Wählen Sie anschließend in der Liste „Produktauswahl“ das Produkt aus, für welches Sie das Script erstellen möchten.

Abb. 15: Dialog Neues Script erzeugen - Produktauswahl

☐ Stellen Sie in der Oberfläche des Offline-Konfigurators die gewünschten Parameter entsprechend Ihrer Erfordernisse ein.

Anmerkung: Die Oberfläche des Offline-Konfigurators enthält ausschließlich Dialoge, Tabellen und Eingabefelder für auf das Gerät schreibbare Parameter. Im Offline-Modus können Sie keine Parameter aus dem Gerät auslesen. Die Oberfläche des Offline-Konfigurators enthält gegenüber der grafischen Benutzeroberfläche einen reduzierten Umfang.

Eine Beschreibung zu den Einstellungen, die Sie in der Oberfläche des Offline-Konfigurators durchführen können, entnehmen Sie dem jeweils entsprechenden Kapitel in diesem Handbuch.

▶ Beispiel: Dialog Grundeinstellungen - System

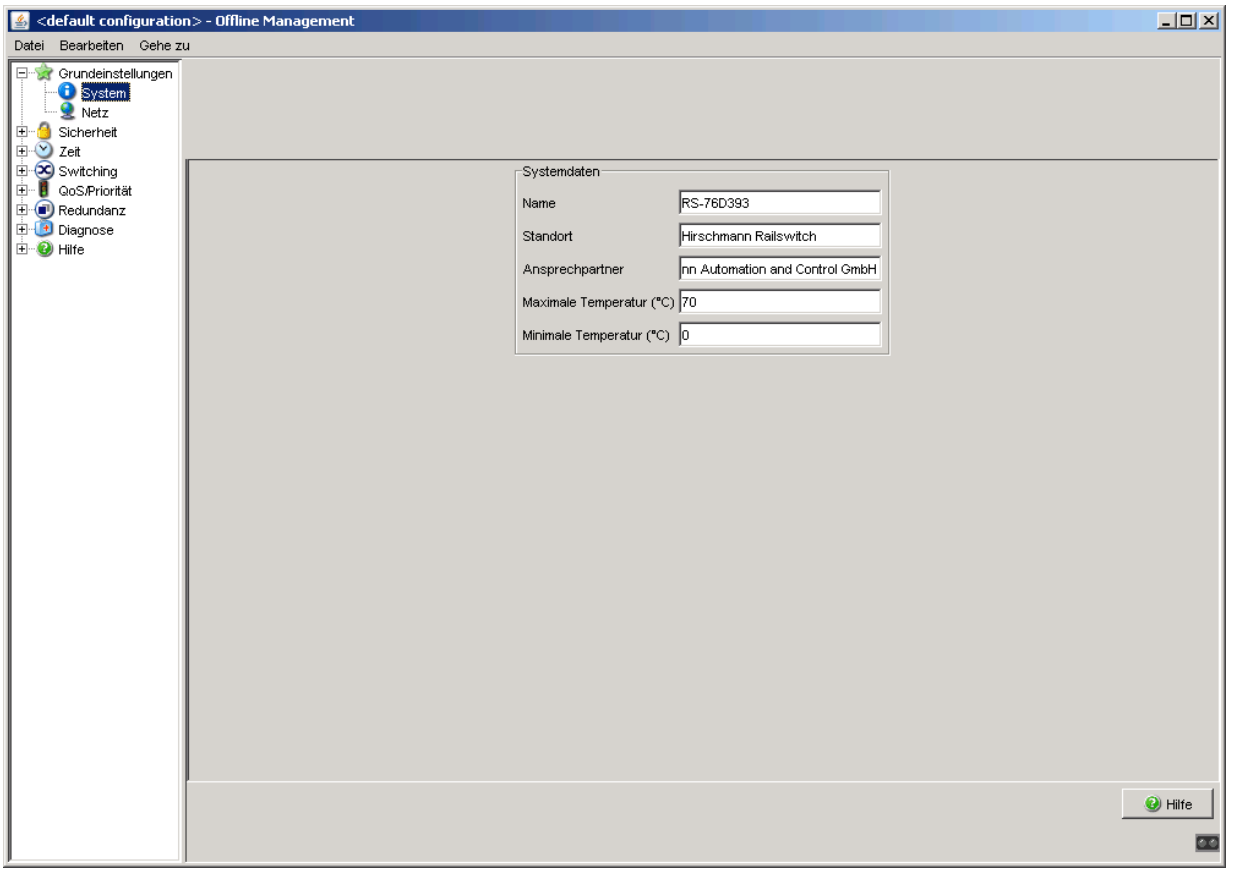


Abb. 16: Dialog Grundeinstellungen:System im Offline-Konfigurator

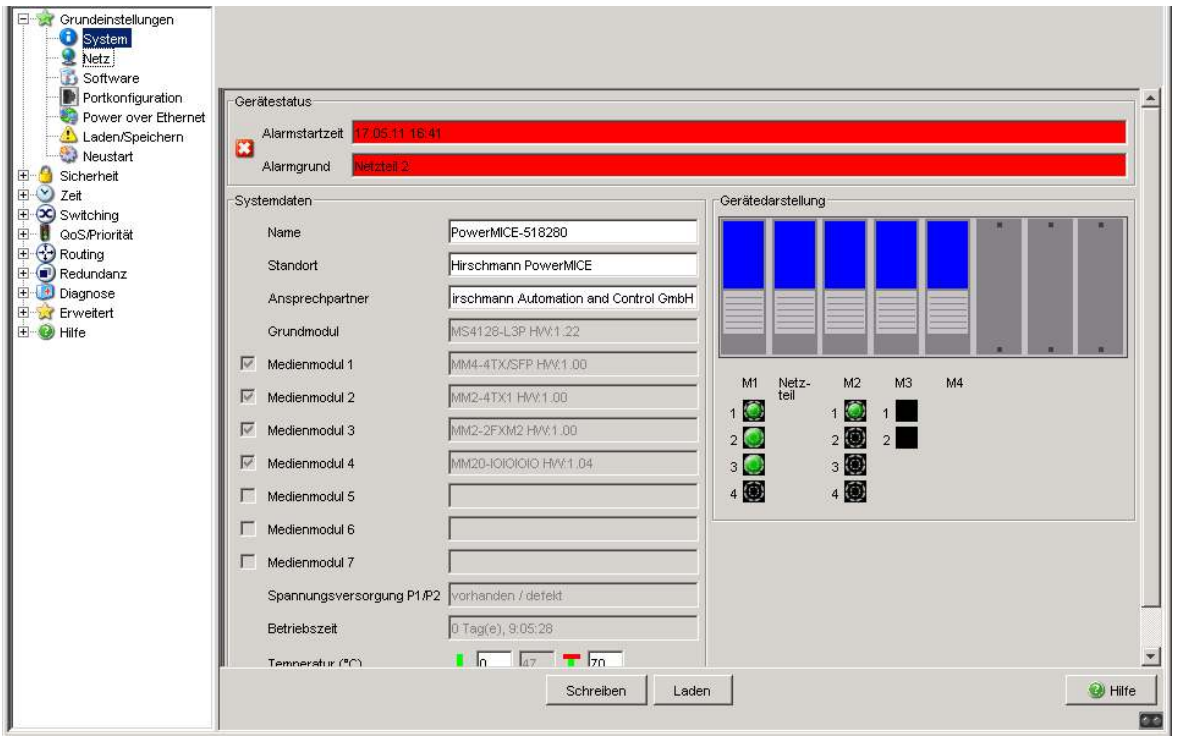


Abb. 17: Dialog Grundeinstellungen:System in der grafischen Benutzeroberfläche

Für das obige Beispiel gilt: Eine Beschreibung zu den einstellbaren Parametern des Offline-Konfigurators entnehmen Dialog `Grundeinstellungen:System`.
Siehe „System” auf Seite 22.

☐ Nachdem Sie die gewünschten Parameter entsprechend Ihrer Erfordernisse in der Oberfläche des Offline-Konfigurators eingestellt haben, speichern Sie die Konfiguration:
- `Datei - Speichern unter` oder
- `Datei - Speichern`

☐ Beenden Sie den Offline-Konfigurator mit Datei - Beenden.

Eine XML-Konfigurationsdatei ins Gerät laden

☐ Wählen Sie in der grafischen Benutzeroberfläche den Menüpunkt `Grundeinstellungen:Laden/Speichern`.

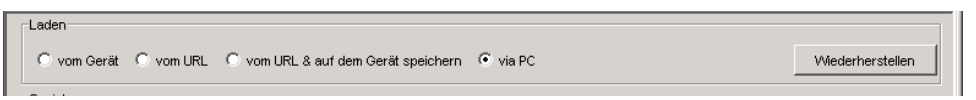


Abb. 18: Dialog Konfiguration laden - Via PC

☐ Um eine auf dem PC mit dem Offline-Konfigurator im XML-Format gespeicherte Konfiguration zu laden, markieren Sie im Rahmen „Laden“ per Mausklick das Feld „via PC“ und klicken Sie auf „Wiederherstellen“.

☐ Wählen Sie im „Öffnen“-Fenster den gewünschten Pfad aus, von dem das Gerät Ihre Konfigurationsdatei laden soll. Geben Sie im Feld „Dateinamen“ den Namen der gewünschten Datei mit der Endung .ocf (Offline Configurator) an.

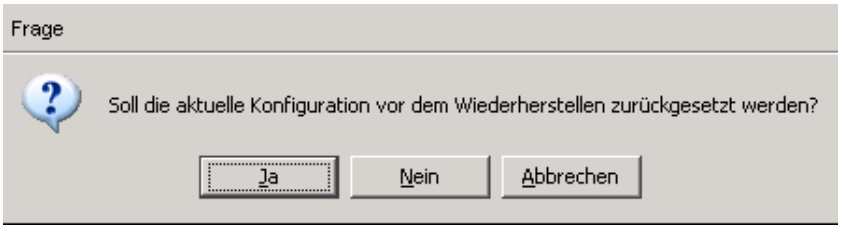


Abb. 19: Abfrage - Konfiguration zurücksetzen

- ☐ Um die aktuelle Konfiguration auf Ihrem Gerät vor dem Laden der Offline-Konfigurationsdatei zurückzusetzen, klicken Sie auf „Ja“.
- ☐ Um die aktuelle Konfiguration auf Ihrem Gerät vor dem Laden der Offline-Konfigurationsdatei beizubehalten und diese dann mit den Inhalten der Offline-Konfigurationsdatei zu überschreiben, klicken Sie auf „Nein“.

Im folgenden Fenster „Konfiguration“ gibt das Gerät nach erfolgreichem Laden der Offline-Konfigurationsdatei eine Übersicht über die geladenen Konfigurationsparameter aus. Sie können in diesem Fenster durch Anklicken zwischen den folgenden zwei Ansichten wählen:

- Tabellen-Ansicht
- Text-Ansicht

Tabellen-Ansicht

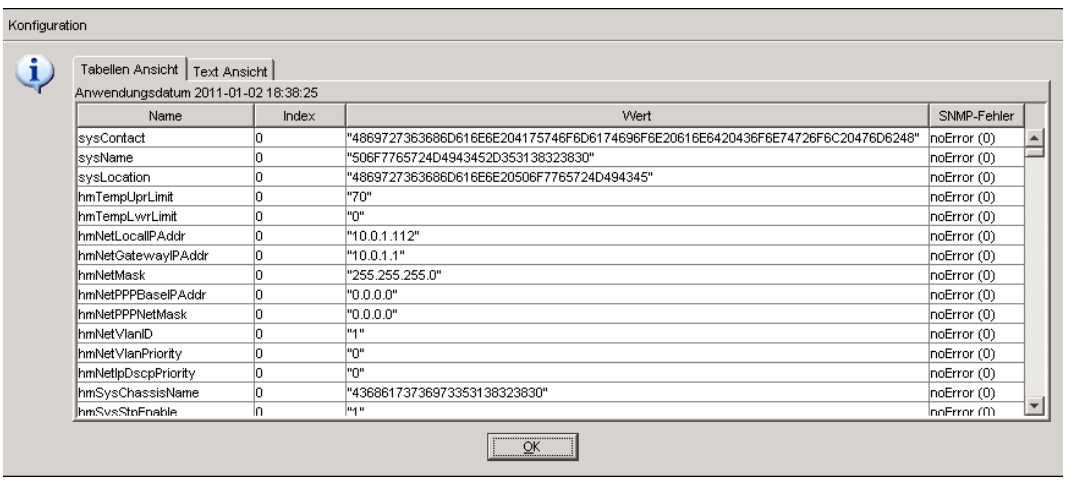


Abb. 20: Information - Konfiguration - Tabellen Ansicht

In der Tabellen-Ansicht erhalten Sie einen Überblick über die geladenen Konfigurationsparameter in tabellarischer Darstellung:

Parameter	Bedeutung	Mögliche Werte
Anwendungsdatum	Zeitpunkt (Datum und Uhrzeit), zu dem Sie die Offline-Konfigurationsdatei ins Gerät geladen haben. Notation: `yyyy-mm-dd hh-mm-ss`	`yyyy` = gültige Jahreszahl `mm` = 1 bis 12 `dd` = 1 bis 31 `hh` = 0 bis 23 `mm` = 0 bis 59 `ss` = 0 bis 59
Name	Name des Konfigurationsparameters (MIB-Variable)	siehe MIB
Index	Index des Konfigurationsparameters (MIB-Variable)	siehe MIB
Wert	Wert des Konfigurationsparameters (MIB-Variable), der durch das Laden der Offline-Konfigurationsdatei gesetzt wurde.	siehe MIB
SNMP-Fehler	Erfolg des Gerätes beim Laden des entsprechenden Konfigurationsparameters	▶ (0) = Success ▶ (1) = Response PDU Too Big ▶ (2) = Variable does not exist ▶ (3) = Cannot modify variable: Bad Value ▶ (4) = Cannot modify object, Read Only ▶ (5) = Cannot perform operation, General Error

Tab. 16: Information - Konfiguration - Tabellen Ansicht

Text-Ansicht

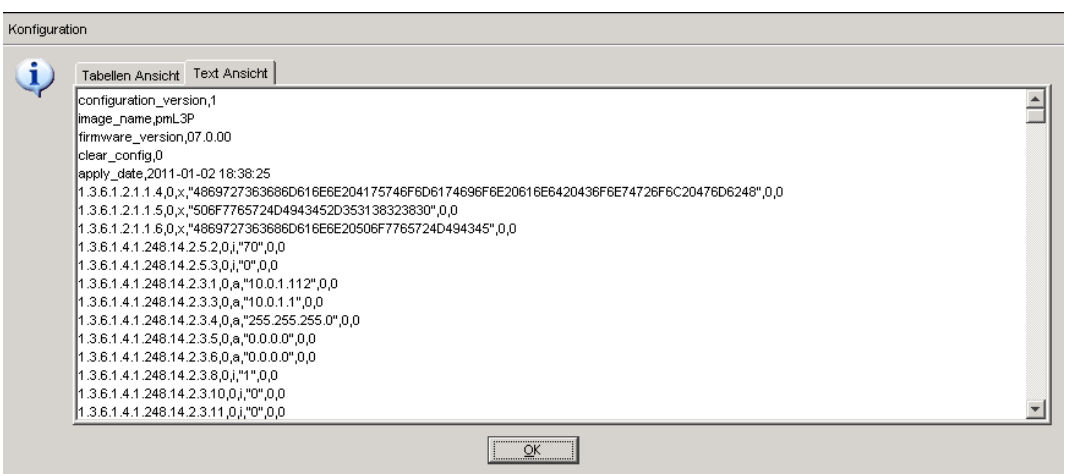


Abb. 21: Information - Konfiguration - Text Ansicht

In der Text-Ansicht erhalten Sie einen Überblick über die geladenen Konfigurationsparameter (MIB-Variablen) in Textdarstellung.

Das Gerät listet die einzelnen Konfigurationsparameter in der folgenden Form auf. Die Angaben sind durch Kommata getrennt:

- Position in der MIB, z.B. 1.3.6.1.2.1.1.4
- Index
- Wert
- SNMP-Fehler (siehe Tabelle 16, Parameter „SNMP-Fehler“)
- Der letzte Parameter hat den Wert 0. Er ist für zukünftige Erweiterungen vorgesehen.

1.8.2 Konfiguration speichern

Im Rahmen „Speichern“ haben Sie die Möglichkeit,

- die aktuelle Konfiguration auf dem Gerät speichern,
- die aktuelle Konfiguration in einer Datei unter dem angegebenen URL im Binärformat oder als editier- und lesbares Script zu speichern,
- die aktuelle Konfiguration im Binärformat oder als editier- und lesbares Script auf dem PC zu speichern.
- die aktuelle Konfiguration für den Offline-Konfigurator im XML-Format auf dem PC zu speichern.

Anmerkung: Für Skript-Konfigurationsdateien beachten Sie die folgenden Besonderheiten:

- Wenn Sie die Konfiguration in eine Binärdatei speichern, speichert das Gerät alle Konfigurationseinstellungen in der Binärdatei.
  Im Gegensatz dazu speichert das Gerät beim Speichern in eine Skriptdatei nur diejenigen Konfigurationseinstellungen, die von der Voreinstellung abweichen.
- Wenn Sie eine Konfiguration aus einer Skriptdatei laden, löschen Sie zuerst die Konfiguration auf dem Gerät, so dass der geladene Skript richtig die Konfigurations-Voreinstellungen überschreibt.
  Ist bereits eine Konfiguration auf der Gerät vorhanden, resultiert das Laden einer Skriptdatei in einer Konfiguration mit der Vereinigungsmenge

der Einstellungen, die in der vorhandenen Konfiguration oder in der Skriptdatei von der Voreinstellung abweichen. Wenn Sie diese Eigenschaft benutzen, denken Sie daran, dass das Laden eines Skripts Konfigurationseinstellungen ausschließlich auf Werte setzt, die von der Voreinstellung abweichen.

- Um die Konfiguration auf einem Gerät zu löschen, wählen Sie „aktuelle Konfiguration“ im Rahmen „Löschen“ und klicken Sie auf „Konfiguration löschen“. Das Gerät löscht seine aktuelle Konfiguration im flüchtigen Speicher sofort (siehe auf Seite 63 „Konfiguration löschen“). Die Konfiguration im nicht-flüchtigen Speicher bleibt erhalten, ebenso die IP-Adresse. Somit bleibt das Gerät erreichbar.

Anmerkung: Den von DHCP/BOOTP (siehe auf Seite 29 „Netz“) gestarteten Ladevorgang zeigt die Selektion von "vom URL & lokal speichern" im Rahmen "Laden" an. Sollten Sie beim Speichern einer Konfiguration eine Fehlermeldung erhalten, dann kann eine Ursache ein aktiver Ladevorgang sein. DHCP/BOOTP beendet einen Ladevorgang erst, wenn eine gültige Konfiguration geladen ist. Findet DHCP/BOOTP keine gültige Konfiguration, dann beenden Sie den Ladevorgang durch Laden der lokalen Konfiguration vom Gerät im Rahmen "Laden".

Wenn Sie die laufende Konfiguration verändern (z. B. einen Port ausschalten), ändert die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol im Navigationsbaum von einem Diskettensymbol in ein gelbes Dreieck. Nach dem Speichern der Konfiguration zeigt die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol wieder als Diskette an.

Nachdem Sie die Konfiguration erfolgreich auf dem Gerät gespeichert haben, sendet das Gerät einen Trap `hmConfigurationSavedTrap`, zusammen mit der Information über einen ggf. angeschlossenen AutoConfiguration Adapter (ACA). Wenn Sie die Konfiguration nach dem Speichern zum ersten Mal verändern, sendet das Gerät einen Trap `hmConfigurationChangedTrap`.

Konfiguration für Offline-Konfigurator speichern

☐ Wählen Sie in der grafischen Benutzeroberfläche den Menüpunkt `Grundeinstellungen:Laden/Speichern`.

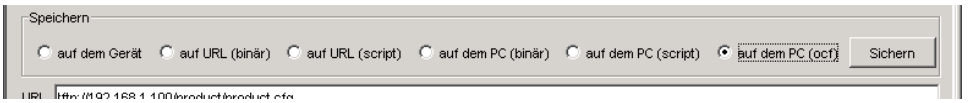


Abb. 22: Dialog Konfiguration speichern - Auf dem PC (ocf)

☐ Um die aktuelle Konfiguration für den Offline-Konfigurator als XML-Konfigurationsdatei auf dem PC zu speichern, markieren Sie im Rahmen „Speichern“ per Mausklick das Feld „auf dem PC (ocf)“ und klicken Sie auf „Sichern“.

☐ Wählen Sie im „Speichern“-Fenster den gewünschten Pfad aus, auf dem das Gerät Ihre Konfigurationsdatei abspeichern soll. Geben Sie im Feld „Dateinamen“ den gewünschten Namen an. Das Gerät speichert Ihre Konfiguration in einer Datei mit der Endung .ocf (Offline Configurator).

Konfigurations-Signatur

Eine Konfigurations-Signatur identifiziert über eine einzigartige Kennung eine bestimmte Konfiguration. Die Konfigurations-Signatur ist über den Dialog `Grundeinstellungen:Laden/Speichern` im Rahmen „Konfigurations-Signatur“ einsehbar. Das Gerät generiert jedes Mal, wenn Sie eine Konfiguration auf dem Gerät speichern, eine zufällige Zeichenfolge aus Nummern und/oder Buchstaben als Signatur für die Konfiguration. Die Signatur ändert sich jedes Mal, wenn Sie eine Konfiguration auf dem Gerät speichern. Das Gerät speichert die zufällig generierte Signatur zusammen mit der Konfiguration, um sicherzustellen, dass das Gerät bei einem Neustart die korrekte Konfiguration lädt.

1.8.3 URL

Der URL kennzeichnet den Pfad zum tftp-Server auf dem die Konfigurationsdatei zu speichern ist. Der URL hat die Form tftp://IP-Adresse des tftp-Servers/Pfadname/Dateiname (z.B. `tftp://192.168.1.100/device/config.dat`).

Anmerkung: Die Konfigurationsdatei enthält alle Konfigurationsdaten, auch die Passwörter für den Zugriff auf das Gerät. Achten Sie deshalb auf die Zugriffsrechte auf dem tftp-Server.

1.8.4 Konfiguration löschen

Im Rahmen „Löschen“ haben Sie die Möglichkeit,

- die aktuelle Konfiguration in den Lieferzustand zurückzusetzen. Die auf dem Gerät gespeicherte Konfiguration bleibt erhalten.
- das Gerät in den Lieferzustand zurückzusetzen. In diesem Fall löscht das Gerät seine Konfigurationen sowohl aus dem flüchtigen Speicher als auch dem nicht-flüchtigen Speicher. Dies umfasst auch die IP-Adresse. Sobald das Gerät eine neue IP-Adresse erhalten hat, z. B. über DHCP oder die V.24-Schnittstelle, ist es wieder über das Netzwerk erreichbar.

Anmerkung: Mit Ausnahme der Watchdog-Konfiguration speichert das Gerät die benutzerdefinierten Konfigurationen im nicht-flüchtigen Speicher. Die Watchdog-Konfiguration speichert das Gerät getrennt. Daher bleibt die Watchdog-Konfiguration im Gerät erhalten, wenn Sie die Konfigurationen über die Funktionen „aktuelle Konfiguration“ oder „aktuelle Konfiguration und vom Gerät“ in den Lieferzustand zurücksetzen.

1.8.5 AutoConfiguration Adapter (ACA) verwenden

Die ACAs sind Geräte zum Speichern der Konfigurationsdaten eines Geräts. Ein ACA ermöglicht eine denkbar einfache Konfigurationsdatenübernahme durch ein Ersatzgerät des gleichen Typs.

Anmerkung: Wenn Sie ein Gerät mit DIP-Schaltern ersetzen, prüfen Sie die DIP-Schalterstellungen, um sicherzustellen, dass sie dieselben sind.

- **Aktuelle Konfigurationsdaten in den ACA speichern:**
  Sie haben die Möglichkeit, die aktuelle Geräte-Konfiguration inklusive SNMP-Passwort im Rahmen „Speichern“ mit der Auswahl "auf dem Gerät" auf den ACA und in den Flash-Speicher zu übertragen.

  Anmerkung: Das Gerät speichert die Konfiguration mit Ausnahme seines SSH-Schlüssels (siehe auf Seite 80 „Telnet-/Web-/SSH-Zugriff“). Eine Anleitung, um den SSH-Schlüssel des alten Geräts auf das neue zu bringen, finden Sie im Dokument „Anwender-Handbuch Grundkonfiguration“ im Kapitel „Defekte Geräte ersetzen“.

- **Download der Konfigurationsdatei des ACA:**
  Bei einem Neustart des Gerätes mit angeschlossenem ACA übernimmt das Gerät die Konfigurationsdaten des ACA und speichert sie nichtflüchtig im Flash-Speicher. Enthält der angeschlossene ACA ungültige Daten, z. B. wenn sich der ACA im Lieferzustand befindet, dann lädt das Gerät die Daten aus dem Flash-Speicher.

  Anmerkung: Vor dem Laden der Konfigurationsdaten vom ACA vergleicht das Gerät das Passwort im Gerät mit dem Passwort in den Konfigurationsdaten des ACA.

  Das Gerät übernimmt die Konfigurationsdaten, wenn
  - das Admin-Passwort übereinstimmt oder
  - lokal kein Passwort gespeichert ist oder

- lokal das Passwort im Lieferzustand ist oder
- lokal keine Konfiguration gespeichert ist.

Status	Bedeutung
notPresent	Kein ACA vorhanden
ok	Konfigurationsdaten von ACA und Gerät stimmen überein.
removed	Der ACA wurde nach dem Booten entfernt.
notInSync	- Die Konfigurationsdaten von ACA und Gerät stimmen nicht überein oder nur eine Datei existiert[a], oder - weder auf dem ACA noch auf dem Gerät ist eine Konfigurationsdatei vorhanden[b].
outOfMemory	Die lokalen Konfigurationsdaten sind zu umfangreich, um sie auf dem ACA zu speichern.
wrongMachine	Die Konfigurationsdaten im externen Speicher stammen von einem anderen Gerätetyp und lassen sich nicht einlesen oder konvertieren.
checksumErr	Die Konfigurationsdaten sind beschädigt.

Tab. 17: ACA-Status

a. In diesen Fällen ist der ACA-Status identisch mit dem Status „ACA nicht synchron“, der „Nicht OK“ an die Meldekontakte und den Gerätestatus weitermeldet.
b. In diesem Fall weicht der ACA-Status („notInSync“) vom Status „ACA nicht synchron“ ab, der „OK“ an die Meldekontakte und den Gerätestatus weitermeldet.

1.8.6 Konfigurationsänderung widerrufen

Funktion

Ist die Funktion an und die Verbindung zum Gerät länger als die im Feld „Periode bis zum Widerruf bei Verbindungsunterbrechung [s]“ angegebene Zeit unterbrochen, dann lädt das Gerät die zuletzt gespeicherte Konfiguration.

☐ Schalten Sie die Funktion ein, bevor Sie das Gerät konfigurieren, damit Sie nach einer Fehlkonfiguration, die Ihre Verbindung zum Gerät unterbrochen hat, wieder Verbindung zum Gerät erhalten.

☐ Geben Sie die „Periode bis zum Widerruf bei Verbindungsunterbrechung [s]“ in Sekunden ein.
Mögliche Werte: 10-600 Sekunden.
Voreinstellung: 600 Sekunden.

Anmerkung: Schalten Sie die Funktion nach erfolgreicher Abspeicherung der Konfiguration aus. Das hilft Ihnen zu vermeiden, dass das Gerät die Konfiguration erneut lädt, nachdem Sie das Web-Interface schließen.

Anmerkung: Beachten Sie beim Zugriff auf das Gerät über ssh zusätzlich die TCP-Verbindungstimeouts für den Konfigurationswiderruf.

Watchdog IP-Adresse

„Watchdog IP-Adresse“ zeigt Ihnen die IP-Adresse des PCs an, von dem Sie die Funktion (Watchdog) aktiviert haben. Das Gerät überwacht die Verbindung zu dem PC mit dieser IP-Adresse auf Verbindungsunterbrechung.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 18: Schaltflächen

1.9 Neustart

Dieser Dialog bietet Ihnen folgende Funktionen:

- einen Kaltstart oder verzögerten Kaltstart des Gerätes auslösen. Nach Ablauf der eingestellten Zeit lädt das Gerät die Software neu aus dem nichtflüchtigen Speicher, startet neu und führt einen Selbsttest durch.
  - ☐ Laden Sie die grafische Benutzeroberfläche in Ihrem Browser neu, um nach dem Neustart wieder auf das Gerät zuzugreifen.
- einen Warmstart oder verzögerten Warmstart des Gerätes auslösen. Nach Ablauf der eingestellten Zeit prüft das Gerät die Software im flüchtigen Speicher und startet neu. Ist ein Warmstart nicht möglich, wird automatisch ein Kaltstart ausgeführt.
- einen verzögerten Neustart abbrechen.
- die Einträge mit dem Status „learned“ aus der Filtertabelle zurücksetzen (MAC-Adresstabelle),
- die ARP-Tabelle zurücksetzen.
  Das Gerät führt intern eine ARP-Tabelle.
  Sollten Sie z.B. einem Rechner eine neue IP-Adresse zuweisen und danach keine Verbindung zum Gerät herstellen können, dann setzen Sie die ARP-Tabelle zurück.
- die Portzähler zurücksetzen.
- die Logdatei löschen.

Anmerkung: Während des Neustarts überträgt das Gerät kurzfristig keine Daten und ist nicht durch die grafische Benutzeroberfläche oder andere Management-Systeme wie z. B. Industrial HiVision erreichbar.

Abb. 23: Dialog Neustart

Anmerkung: Nach Auswahl von „Kaltstart“ oder „Warmstart“ erscheint das Fenster „Neustart“. Hier geben Sie die Verzögerungszeit ein, nach der das Gerät seinen Neustart durchführt. Der maximale Wert beträgt 24 d, 20 h, 31 min, 23 s.
Um den Neustart-Vorgang abzubrechen, klicken Sie „Abbrechen“.

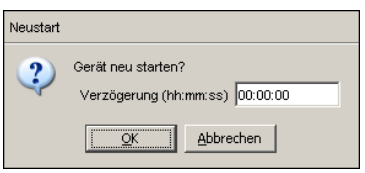


Abb. 24: Dialog verzögerter Neustart

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 19: Schaltflächen

2 Sicherheit

Das Menü „Sicherheit“ enthält die Dialoge, Anzeigen und Tabellen zur Konfiguration der Sicherheitseinstellungen:

- Passwort/SNMPv3-Zugriff
- SNMPv1/v2-Zugriff
- Telnet/Web/SSH-Zugriff
- Restricted Management Access (Eingeschränkter Management-Zugriff)
- Portsicherheit
- 802.1X Port-Authentifzierung
- RADIUS
- Login-Banner
- Access Control Lists (ACLs, Bedienung ausschließlich per CLI)

2.1 Passwort / SNMPv3-Zugriff

Dieser Dialog bietet Ihnen die Möglichkeit, das Lese- und das Schreib/Lese-Passwort für den Zugriff über die grafische Benutzeroberfläche, über das CLI und per SNMPv3 (SNMP-Version 3) auf dem Gerät zu ändern.
Stellen Sie für das Lesepasswort und das Schreib-/Lesepasswort unterschiedliche Passwörter ein, damit ein Benutzer, der nur Lesezugriff hat (Benutzername „user“), das Passwort für den Schreib-/Lesezugriff (Benutzername „admin“) nicht kennen oder erraten kann.
Wenn Sie identische Passwörter setzen, meldet das Gerät beim Versuch, diese Daten zu schreiben, einen allgemeinen Fehler.

Die grafische Benutzeroberfläche und das Command-Line-Interface (CLI) verwenden für die Benutzer „admin“ und „user“ die selben Passwörter wie SNMPv3.

Anmerkung: Passwörter unterscheiden Groß- und Kleinschreibung.

☐ Wählen Sie „Lesepasswort ändern (user)“, um das Lesepasswort einzugeben.
☐ Geben Sie das neue Lesepasswort in der Zeile „Neues Passwort“ ein und wiederholen Sie die Eingabe in der Zeile „Bitte nochmals eingeben“.

☐ Wählen Sie „Schreib-/Lesepasswort ändern (admin)“, um das Schreib-/Lesepasswort einzugeben.
☐ Geben Sie das Schreib-/Lesepasswort ein und wiederholen Sie die Eingabe.

☐ Die Funktion „Nur verschlüsselte Anfragen akzeptieren“ steuert die Verschlüsselung der Management-Daten bei der Übertragung mit SNMPv3 zwischen Ihrem PC und dem Gerät.
  – Bei abgeschalteter Datenverschlüsselung ist die Übertragung der Konfigurationsdaten unverschlüsselt und vor Verfälschung geschützt.
  – Die grafische Benutzeroberfläche überträgt das Passworts stets sicher.
  – Die grafische Benutzeroberfläche überträgt die Benutzernamen stets im Klartext.

- Das Gerät bietet Ihnen die Möglichkeit, die Funktion „Nur verschlüsselte Anfragen akzeptieren“ für den Zugriff mit dem Lesepasswort und mit dem Schreib-/Lesepasswort unterschiedlich einzustellen.
- Die grafische Benutzeroberfläche fragt beim Login die aktuelle Einstellung des Gerätes ab und sendet verschlüsselte Anfragen, wenn das Gerät das verlangt.

☐ Wenn Sie die Funktion „Passwort als v1/v2-Community übernehmen“ aktivieren, synchronisiert das Gerät beim Ändern des Passworts den korrespondierenden Community-Namen.
- Wenn Sie das Passwort für den Schreib-/Lesezugriff ändern, aktualisiert das Gerät die readWrite-Community für den SNMPv1/v2-Zugriff auf denselben Wert.
- Wenn Sie das Passwort für den Lesezugriff ändern, aktualisiert das Gerät die readOnly-Community für den SNMPv1/v2-Zugriff auf denselben Wert.

Anmerkung: Da die grafische Benutzeroberfläche im Dialog für SNMPv1/v2 die Communitys lesbar anzeigt, kann auf diesen Dialog nur ein Benutzer zugreifen, der sich mit dem Benutzernamen „admin“ und dem richtigen Schreib-/Lesepasswort angemeldet hat.

Anmerkung: Wenn Sie das SNMPv3-Passwort für den Benutzernamen ändern, mit dem Sie sich über die grafische Benutzeroberfläche angemeldet haben, melden Sie sich neu an, damit Sie wieder auf die grafische Benutzeroberfläche des Geräts zugreifen können. Andernfalls erhalten Sie bei einem Zugriffsversuch eine allgemein gehaltene Fehlermeldung.

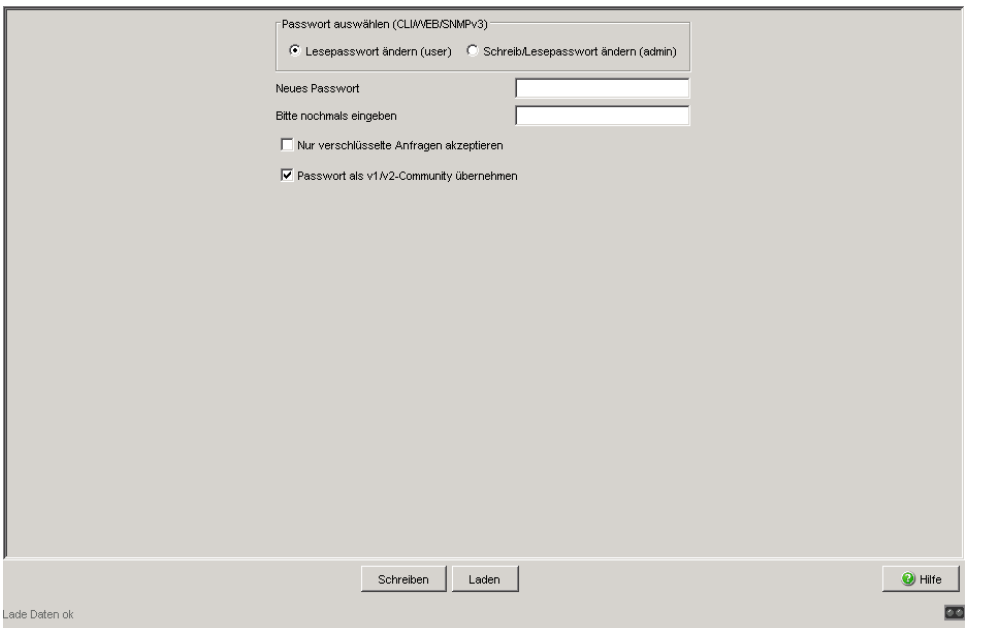


Abb. 25: Dialog Passwort/SNMP-Zugriff

Anmerkung: Wenn Sie kein Passwort mit der Berechtigung „schreiben/lesen“ kennen, haben Sie keine Möglichkeit, auf das Gerät schreibend zuzugreifen.

Anmerkung: Aus Sicherheitsgründen zeigt das Gerät die Passwörter nicht an. Notieren Sie sich jede Änderung. Ohne gültiges Passwort können Sie nicht auf das Gerät zugreifen.

Anmerkung: Aus Sicherheitsgründen verschlüsselt SNMPv3 das Passwort. Mit der Einstellung „SNMPv1“ oder „SNMPv2“ im Dialog `Sicherheit: SNMPv1/v2-Zugriff` überträgt das Gerät das Passwort unverschlüsselt, dieses kann dann mitgelesen werden.

Anmerkung: Verwenden Sie bei SNMPv3 für das Passwort 5-32 Zeichen, da viele Anwendungen keine kürzeren Passwörter akzeptieren.

Die Sperre des Zugriffs über einen Web-Browser, SSH- oder Telnet-Client nehmen Sie in einem eigenen Dialog vor .
Siehe „Telnet-/Web-/SSH-Zugriff” auf Seite 80.

Die Beschränkung des Zugriffs auf IP-Adressebene erfolgt in einem separaten Dialog.
Siehe „SNMPv1/v2-Zugriffs-Einstellungen” auf Seite 76.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 20: Schaltflächen

2.2 SNMPv1/v2-Zugriffs-Einstellungen

Dieser Dialog bietet Ihnen die Möglichkeit, den Zugriff über SNMPv1 oder SNMPv2 auszuwählen. Im Lieferzustand sind beide Protokolle aktiviert. Damit können Sie das Gerät mit Industrial HiVision verwalten und mit früheren Versionen von SNMP kommunizieren.

Anmerkung: Damit Sie die Daten dieses Dialogs lesen und/oder ändern können, melden Sie sich über die grafische Benutzeroberfläche mit dem Benutzernamen `admin` und dem dazu passenden Passwort an.

- In der Spalte „Index“ zeigt das Gerät die laufende Nummer an.
- In der Spalte „Community-Name“ tragen Sie das Passwort ein, mit dem eine Management-Station aus dem angegebenen Adressbereich per SNMPv1/v2 auf das Gerät zugreifen darf.

  Anmerkung: Passwörter unterscheiden Groß- und Kleinschreibung.

Wenn Sie die Funktion „Community als v3-Passwort übernehmen“ im Rahmen „Konfiguration“ aktivieren, synchronisiert das Gerät beim Ändern des Community-Namens das korrespondierende SNMPv3-Passwort.

– Wenn Sie die readWrite-Community ändern, aktualisiert das Gerät das SNMPv3-Passwort für den Schreib-/Lesezugriff auf denselben Wert.
– Wenn Sie die readOnly-Community ändern, aktualisiert das Gerät das SNMPv3-Passwort für den Lesezugriff auf denselben Wert.

- In der Spalte "IP-Adresse" tragen Sie die IP-Adresse ein, die auf das Gerät zugreifen darf. Kein Eintrag oder der Eintrag "0.0.0.0" in diesem Feld erlaubt den Zugriff von Rechnern mit beliebigen IP-Adressen auf dieses Gerät. In diesem Fall ist das Passwort der einzige Zugriffsschutz.
- In der Spalte "IP-Maske" haben Sie die Möglichkeit ähnlich wie bei Netzmasken, eine Gruppe von IP-Adressen auszuwählen.
  Beispiel:
  255.255.255.255: eine einzige IP-Adresse
  255.255.255.240 mit IP-Adresse = 172.168.23.20:
  die IP-Adressen 172.168.23.16 bis 172.168.23.31.

binäre Darstellung der Maske 255.255.255.240:
1111 1111 1111 1111 1111 1111 1111 0000
└──┴──┴──Maskenbits
binäre Darstellung der IP-Adresse 172.168.23.20:
1010 1100 1010 1000 0001 0111 0001 0100

Die binäre Darstellung der Maske mit der IP-Adresse ergibt einen Adressbereich von:
1010 1100 1010 1000 0001 0111 0001 0000 bis
1010 1100 1010 1000 0001 0111 0001 1111
also: 172.168.23.16 bis 172.168.23.31

- In der Spalte „Zugriffsrecht“ legen Sie fest, ob dieser Rechner mit dem Lesepasswort (Zugriffsrecht `readOnly`) oder mit dem Schreib/Lese-Passwort (Zugriffsrecht `readWrite`) zugreifen darf.
  Siehe „Passwort / SNMPv3-Zugriff” auf Seite 72.

  Anmerkung: Das Passwort für das Zugriffsrecht `readOnly` ist das selbe wie das SNMPv3-Passwort für den Lesezugriff.
  Das Passwort für das Zugriffsrecht `readWrite` ist das selbe wie das SNMPv3-Passwort für den Schreib-/Lesezugriff.
  Ändern Sie eines der Passwörter, setzen Sie das entsprechende Passwort für SNMPv3 manuell auf den selben Wert. Oder markieren Sie das Kontrollkästchen „Community als v3-Passwort übernehmen“ im Rahmen „Konfiguration“. So erreichen Sie, dass Sie auch per SNMPv3 mit dem selben Passwort zugreifen können.

- In der Spalte „Aktiv“ aktivieren/deaktivieren Sie diesen Tabelleneintrag.

  Anmerkung: Haben Sie keine Zeile aktiviert, dann kennt das Gerät keine Zugriffsbeschränkung bezüglich der IP-Adressen.

- Mit „Erzeugen“ erzeugen Sie eine neue Zeile in der Tabelle.
- Mit „Löschen“ löschen Sie ausgewählte Zeilen aus der Tabelle.

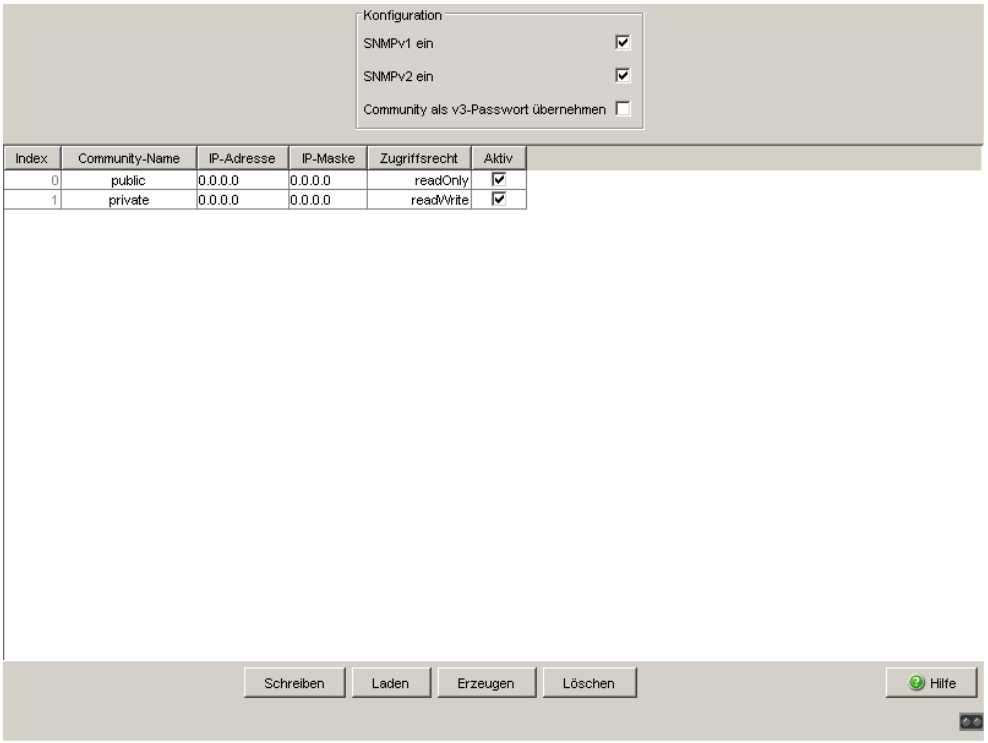


Abb. 26: Dialog SNMPv1/v2-Zugriff

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 21: Schaltflächen

2.3 Telnet-/Web-/SSH-Zugriff

Dieser Dialog bietet Ihnen die Möglichkeit, den Telnet-Server und den SSH-Server auf dem Gerät ein-/auszuschalten und den Web-Server auszuschalten.

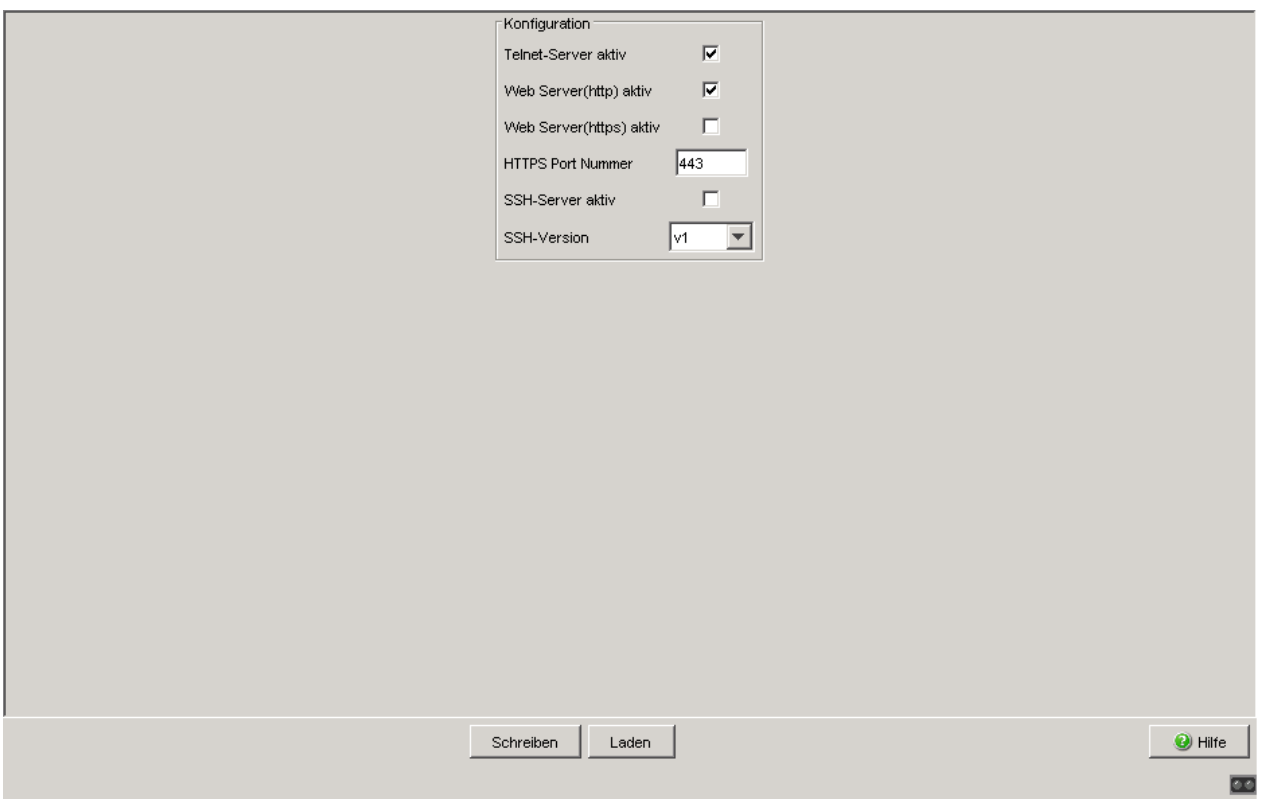


Abb. 27: Dialog Telnet-/Web-/SSH-Zugriff

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Telnet-Server aktiv	Aktiviert oder deaktiviert den Telnet-Dienst (Telnet-Zugang) für das Gerät.	`An` `Aus`	`An`
Web-Server (HTTP) aktiv	Aktiviert oder deaktiviert den http-Dienst (Web-Server) für das Gerät.	`An` `Aus`	`An`
Web-Server (HTTPS) aktiv	Aktiviert oder deaktiviert den https-Dienst (Web-Server) für das Gerät.	`An` `Aus`	`Aus`

Tab. 22: Telnet-/Web-/SSH-Zugriff

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
HTTPS Port Nummer	Eingabe der Port-Nummer des https-Web-Servers für den https-Zugriff auf das Gerät.	`1..65535`	`443`
SSH-Server aktiv	Aktiviert oder deaktiviert den ssh-Dienst (ssh-Zugang) für das Gerät.	`An` `Aus`	`Aus`

SSH-Version	Bestimmt die für das Gerät geltende SSH-Protokoll-Version.	`v1`
		`v2`
		`v1 & v2`
			`v1 & v2`

Tab. 22: Telnet-/Web-/SSH-Zugriff

2.3.1 Beschreibung Telnet-Zugriff

Der Telnet-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe des Command Line Interfaces (in-band) zu konfigurieren. Sie können den Telnet-Server deaktivieren, um einen Telnet-Zugriff auf das Gerät abzuschalten.
Im Lieferzustand ist der Server eingeschaltet.
Nach dem Abschalten des Telnet-Servers ist ein erneuter Zugriff auf das Gerät über eine neue Telnet-Verbindung nicht mehr möglich. Eine bestehende Telnet-Verbindung bleibt erhalten.

Anmerkung: Das Command-Line-Interface (out-of-band) und der Dialog `Sicherheit:Telnet/Web-/SSH-Zugriff` in der grafischen Benutzeroberfläche bieten Ihnen die Möglichkeit, den Telnet-Server wieder zu aktivieren.

2.3.2 Beschreibung Web-Zugriff (http)

Der Web-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe der grafische Benutzeroberfläche zu konfigurieren. Sie können den Web-Server ausschalten, um einen Web-Zugriff auf das Gerät zu verhindern.
Im Lieferzustand ist der Server eingeschaltet.

Nach dem Abschalten des HTTP-Web-Servers ist ein erneutes Anmelden über einen HTTP-Web-Browser nicht mehr möglich. Die HTTP-Session im offenen Browserfenster bleibt aktiv.

Anmerkung: Das Command Line Interface bietet Ihnen die Möglichkeit, den Web-Server wieder zu aktivieren.

2.3.3 Beschreibung Web-Zugriff (https)

Der Web-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe der grafischen Benutzeroberfläche über HTTPS (Hypertext Transfer Protocol Secure) zu konfigurieren. Um den RADIUS-Server für die Authentifizierung zu nutzen, aktivieren Sie die HTTPS-Funktion.
Wenn Sie HTTPS und HTTP aktivieren, leitet das Gerät Anfragen an die HTTPS-Verbindung weiter. Sofern Sie während einer aktiven HTTPS-Sitzung den HTTPS-Port ändern, deaktvieren und reaktivieren Sie HTTPS, damit das Gerät den neuen Port verwendet.
Sie können bis zu 16 http-/https-Verbindungen gleichzeitig öffnen.

- ☐ Um den https-Zugriff auf das Gerät zu ermöglichen,
  - ☐ setzen Sie im Feld `Web Server (https) aktiv` den Haken.
  - ☐ tragen Sie im Feld HTTPS Port Nummer die Port-Nummer des https-Web-Servers ein.
- ☐ Um den https-Zugriff auf das Gerät zu verhindern, entfernen Sie im Feld `Web Server (https) aktiv` den Haken.

Im Lieferzustand ist der HTTPS-Zugriff auf den Web-Server des Gerätes deaktiviert und die Port-Nummer des HTTPS-Web-Servers lautet 443.

Durch das Deaktivieren des Web-Servers verhindern Sie eine erneute Anmeldung über einen Web-Browser per https. Die Anmeldung im offenen Browserfenster bleibt aktiv.

Anmerkung: Das Command Line Interface bietet Ihnen die Möglichkeit, den Zugriff auf den Web-Server über https wieder zu aktivieren.

2.3.4 Beschreibung SSH-Zugriff

Der SSH-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe des Command Line Interfaces (in-band) zu konfigurieren. Sie können den SSH-Server ausschalten, um einen SSH-Zugriff auf das Gerät zu verhindern. Im Lieferzustand ist der Server ausgeschaltet.
Nach dem Abschalten des SSH-Servers ist ein erneuter Zugriff auf das Gerät über eine neue SSH-Verbindung nicht mehr möglich. Eine bestehende SSH-Verbindung bleibt erhalten.

Anmerkung: Das Command-Line-Interface (out-of-band) und der Dialog `Sicherheit:Telnet/Web-/SSH-Zugriff` in der grafischen Benutzeroberfläche bieten Ihnen die Möglichkeit, den SSH-Server wieder zu aktivieren.

Anmerkung: Um über SSH auf das Gerät zugreifen zu können, benötigen Sie einen Schlüssel. Ist kein Schlüssel vorhanden, erzeugt das Gerät einen zufälligen Schlüssel (siehe das „Anwender-Handbuch Grundkonfiguration“).

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 23: Schaltflächen

2.4 Restricted Management Access

Dieser Dialog bietet Ihnen die Möglichkeit, den Management-Zugang zu dem Gerät nach IP-Adressbereichen und einzelnen Management-Diensten zu differenzieren (einzuschränken).

Wenn Sie diese Funktion aktivieren, haben Sie ausschließlich von den angegebenen IP-Adressbereichen Zugriff auf die für diese Adressbereiche aktivierten Management-Dienste. Andere Anfragen verwirft das Gerät. Sie können bis zu 16 Einträge in die Liste aufnehmen, jedem Adressbereich gesondert Management-Zugriffe erlauben oder verbieten und die einzelnen Einträge getrennt aktivieren oder deaktivieren.

Die folgenden Management-Dienste unterstützen den eingeschränkten Management-Zugriff:

- http
- https
- snmp
- telnet
- ssh

Anmerkung: Der CLI-Zugang über die V.24-Schnittstelle ist von der Funktion ausgenommen und lässt sich nicht einschränken.

Anmerkung: Sie benötigen den http- oder https-Dienst zum Starten der grafischen Benutzeroberfläche in einem Browser.
Sie benötigen anschließend den snmp-Dienst zum Zugriff auf das Gerät über die grafische Benutzeroberfläche. Wenn Sie die grafische Benutzeroberfläche außerhalb des Browsers starten, benötigen Sie ausschließlich snmp.

In der Voreinstellung ist der eingeschränkte Management-Zugriff abgeschaltet. In diesem Fall hat jeder mit den richtigen Administrator-Zugangsdaten Zugriff auf alle Management-Dienste.

Haben Sie die Funktion aktiviert und existiert mindestens ein aktiver Eintrag, dessen IP-Adressbereich zur Anfrage passt und bei dem der angefragte Management-Dienst erlaubt ist, bearbeitet das Gerät die Anfrage. Andernfalls verwirft es sie.

Im Lieferzustand bietet Ihnen das Gerät einen voreingestellten Eintrag mit der IP-Adresse 0.0.0.0, der Netzmaske 0.0.0.0 und allen Management-Diensten. Dies erlaubt den Zugriff auf die Dienste von einer beliebigen IP-Adresse aus. Das ermöglicht Ihnen den Zugriff auf das Gerät auch bei eingeschalteter Beschränkung, z. B., um die Funktion erstmals zu konfigurieren. Sie haben die Möglichkeit diesen Eintrag zu ändern oder zu löschen. Wenn Sie einen Eintrag neu erzeugen, hat dieser ebenfalls diese voreingestellten Eigenschaften.

Anmerkung: Wenn Sie die Funktion einschalten und kein Eintrag in der Tabelle Ihren momentanen Zugriff erlaubt, ist es Ihnen nicht mehr möglich, auf das Management des Geräts zuzugreifen, sobald Sie diese Einstellungen auf das Gerät schreiben.
Wenn kein Eintrag einen Zugriff erlaubt, hat niemand Zugriff auf das Geräte-Management.
Verwenden Sie in diesem Fall den CLI-Zugang per V.24, um auf das Management des Geräts zuzugreifen.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Funktion	Ein- oder Ausschalten der Funktion für das Gerät.	`An` `Aus`	`Aus`
Index	Laufende Nummer des Eintrags.Wenn Sie einen Eintrag löschen, bleibt eine Nummerierungslücke. Wenn Sie mit dem Web-based Interface einen neuen Eintrag erzeugen, schließt das Gerät die 1. Lücke.	1 - 16	1 (der voreingestellte Eintrag).
IP-Adresse	Legt zusammen mit der Netzmaske den Netzbereich fest, für den dieser Eintrag gilt.	Gültige IPv4-Adresse oder 0.0.0.0	0.0.0.0 (für alle neu erzeugten Einträge)

Tab. 24: Restricted Management Access

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Netzmaske	Legt zusammen mit der IP-Adresse den Netzbereich fest, für den dieser Eintrag gilt.	Gültige IPv4-Netzmaske oder 0.0.0.0	0.0.0.0 (für alle neu erzeugten Einträge)
HTTP	Aktiviert oder deaktiviert den http-Dienst (Web-Server) für diesen Eintrag.	An Aus	An (für alle neu erzeugten Einträge)
HTTPS	Aktiviert oder deaktiviert den https-Dienst (Web-Server) für diesen Eintrag.	An Aus	An (für alle neu erzeugten Einträge)
SNMP	Aktiviert oder deaktiviert den SNMP-Dienst (SNMP-Zugang) für diesen Eintrag.	An Aus	An (für alle neu erzeugten Einträge)
Telnet	Aktiviert oder deaktiviert den Telnet-Dienst (Telnet-Zugang) für diesen Eintrag.	An Aus	An (für alle neu erzeugten Einträge)
SSH	Aktiviert oder deaktiviert den ssh-Dienst (ssh-Zugang) für diesen Eintrag.	An Aus	An (für alle neu erzeugten Einträge)
Aktiv	Aktiviert oder deaktiviert den gesamten Eintrag.	An Aus	An (für alle neu erzeugten Einträge)

Tab. 24: Restricted Management Access

Anmerkung: Ein Eintrag mit einer IP-Adresse von 0.0.0.0 zusammen mit einer Netzmaske von 0.0.0.0 gilt für alle IP-Adressen.

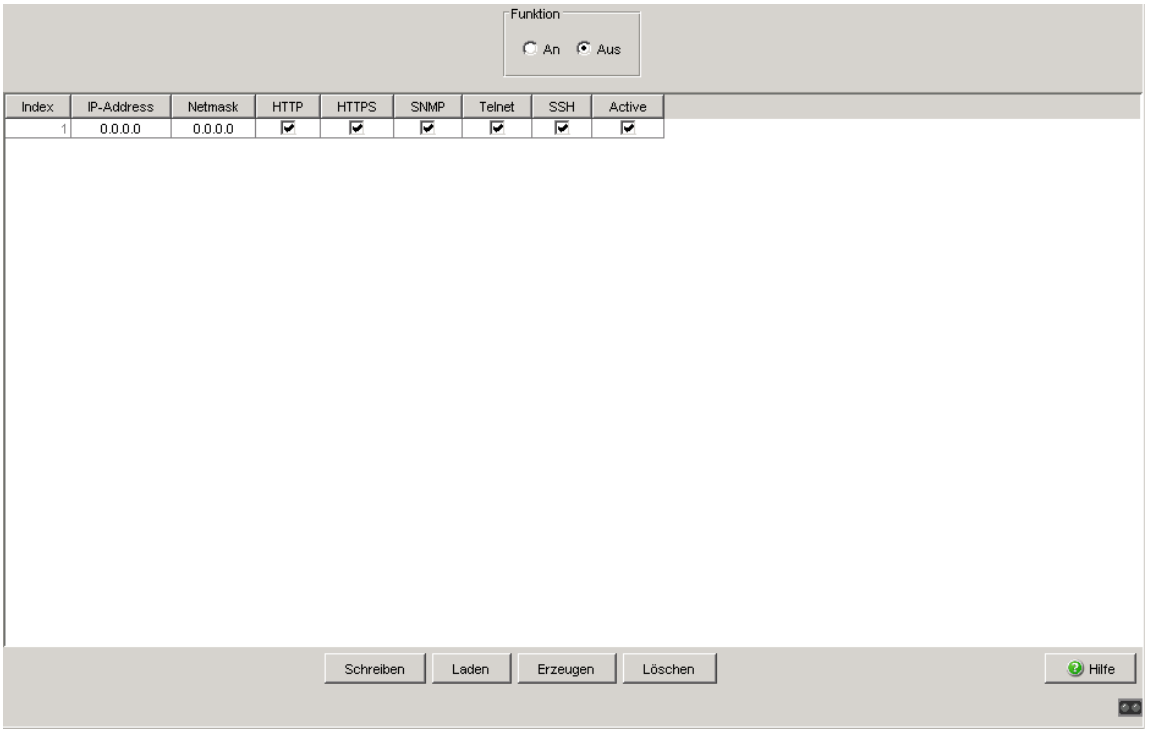


Abb. 28: Dialog Restricted Management Access (Eingeschränkter Management-Zugriff)

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 25: Schaltflächen

2.5 Portsicherheit

Das Gerät bietet Ihnen die Möglichkeit, jeden Port so zu konfigurieren, dass er unberechtigten Zugriff zu verhindern hilft. Abhängig von Ihrer Auswahl prüft das Gerät die MAC-Adresse oder die IP-Adresse des angeschlossenen Geräts.

Wenn das Gerät auf einem Port von einem unerwünschten Absender Datenpakete empfängt, führt es die für den Port festgelegte Aktion aus, z.B. Trap senden, Port ausschalten oder Auto-Disable.

Im Rahmen „Konfiguration“ stellen Sie ein, ob die Portsicherheit mit MAC- oder mit IP-Adressen arbeitet.

Name	Bedeutung
MAC-basierte Portsicherheit	Quell-MAC-Adresse der empfangenen Datenpakete prüfen.
IP-basierte Portsicherheit	Die IP-basierte Portsicherheit verwendet intern die MAC-basierte Portsicherheit. Funktionsprinzip: Wenn sie die Funktions konfigurieren, übersetzt das Gerät die eingegebene IP-Adresse in die entsprechende MAC-Adresse. Im Betrieb prüft es die Quell-MAC-Adresse der empfangenen Datenpakete gegen die intern gespeicherte MAC-Adresse.

Tab. 26: Konfiguration der Portsicherheit global für alle Ports

In der Port-Tabelle stellen Sie für jeden Port die individuellen Parameter ein.

Bei der MAC-basierten Portsicherheit bietet das Gerät Ihnen die Möglichkeit, entweder die erlaubten MAC-Adressen konkret festzulegen oder die MAC-Adressen automatisch zu erfassen.

Beim automatischen Erfassen „lernt“ das Gerät die MAC-Adressen der Absender durch Auswertung der empfangenen Datenpakete. Sobald die benutzerdefinierte Obergrenze erreicht ist, führt das Gerät die festgelegte Aktion aus.

Das automatische Erfassen bietet Ihnen gegenüber dem konkreten Festlegen von MAC-Adressen den Vorteil, dass Sie angeschlossene Endgeräte jederzeit ersetzen können, ohne die MAC-Adressliste im Gerät anzupassen.

Name	Bedeutung
Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.
Port-Status	`enabled`: Port ist eingeschaltet und vermittelt. `disabled`: Port ist ausgeschaltet und vermittelt nicht. Der Port ist eingeschaltet, wenn - mit einer erlaubten Adresse auf diesen Port zugegriffen wird oder - versucht wird, mit einer nicht erlaubten Adresse auf den Port zuzugreifen und unter "Aktion" `trapOnly` oder `none` angewählt ist. Der Port ist ausgeschaltet, wenn versucht wird, mit einer nicht erlaubten Adresse auf den Port zuzugreifen und unter "Aktion" `portDisable` angewählt ist.
Erlaubte MAC-Adressen	MAC-Adressen der Geräte, mit denen Sie einen Datenaustausch an diesem Port erlauben. Die grafische Benutzeroberfläche bietet Ihnen die Möglichkeit, bis zu 50 MAC-Adressen, durch Leerzeichen getrennt, einzugeben. Nach jeder MAC-Adresse können Sie, durch einen Schrägstrich getrennt, eine Zahl zur Kennzeichnung eines Adressbereichs eingeben. Diese Zahl zwischen 2 und 47 kennzeichnet die Anzahl der relevanten Bits. Beispiel: 00:80:63:01:02:00/40 steht für 00:80:63:01:02:00 to 00:80:63:01:02:FF oder 00:80:63:00:00:00/24 steht für 00:80:63:00:00:00 to 00:80:63:FF:FF:FF Ohne Eintrag können beliebige Geräte über diesen Port kommunizieren.
Aktuelle MAC-Adresse	Anzeige der MAC-Adresse des Gerätes, von dem der Port zuletzt Daten empfangen hat. Die grafische Benutzeroberfläche bietet Ihnen die Möglichkeit, einen Eintrag aus der Spalte „Aktuelle MAC-Adresse“ durch Ziehen bei gedrückter Maustaste in die Spalte „Erlaubte MAC-Adresse“ zu kopieren.
Erlaubte IP-Adressen	IP-Adressen der Geräte, mit denen Sie einen Datenaustausch an diesem Port erlauben. Die grafische Benutzeroberfläche bietet Ihnen die Möglichkeit, bis zu 10 IP-Adressen, durch Leerzeichen getrennt, einzugeben. Ohne Eintrag können beliebige Geräte über diesen Port kommunizieren.

Tab. 27: Konfiguration der Portsicherheit pro Port

Name	Bedeutung
Dynamisches Limit	Legt die Obergrenze fest für die Anzahl automatisch erfasster Absender. Sobald die Obergrenze erreicht ist, führt das Gerät die in der Spalte „Aktion“ festgelegte Aktion aus. Mögliche Werte: ▶ `0` oder – (Voreinstellung: –) Deaktiviert das automatische Erfassen der Absender auf diesem Port. ▶ `1..50` Obergrenze für das automatische Erfassen von Absendern. Passen Sie den Wert an die Anzahl der zu erwartenden Absender an. Damit erschweren Sie MAC-Flooding-Attacken.

Tab. 27: Konfiguration der Portsicherheit pro Port

Name	Bedeutung
Dynamische Anzahl	Zeigt, wie viele Absender das Gerät automatisch erfasst hat.
Aktion	Aktion, die das Gerät nach einem unberechtigten Zugriff ausführt. Mögliche Werte: ▶ `none` (Voreinstellung) Keine Aktion. ▶ `trapOnly` Alarm verschicken. ▶ `portDisable` Deaktiviert den Port. Danach blinkt die Port-LED auf dem Gerät 3 mal grün je Periode. Das Gerät re-aktiviert den Port, wenn Sie im Dialog `Diagnose:Ports:Auto-Disable` folgende Einstellungen festgelegt haben: – Im Rahmen „Konfiguration“ ist das Kontrollkästchen für das auslösende Ereignis „Port-Sicherheit“ markiert. – Der Reset-Timer ist für den Port >0 festgelegt. ▶ `autoDisable` Deaktiviert den Port abhängig von den Einstellungen im Dialog `Diagnose:Ports:Auto-Disable`, Rahmen „Konfiguration“. – Das Gerät deaktiviert den Port, wenn das Kontrollkästchen für das auslösende Ereignis „Port-Sicherheit“ markiert ist. Danach blinkt die Port-LED auf dem Gerät 3 mal grün je Periode. Das Gerät re-aktiviert den Port, wenn im Dialog `Diagnose:Ports:Auto-Disable` für den Port der Reset-Timer für den Port >0 festgelegt ist. – Der Port bleibt aktiviert, wenn das Kontrollkästchen für das auslösende Ereignis „Port-Sicherheit“ unmarkiert ist. **Anmerkung:** Voraussetzungen, damit das Gerät einen Alarm (Trap) senden kann: – Sie haben mindestens einen Empfänger eingetragen, – Sie haben mindestens einen Empfänger in der Spalte „Aktiv“ angekreuzt, – Sie haben im Rahmen „Auswahl“ die „Portsicherheit“ angekreuzt.

Tab. 27: Konfiguration der Portsicherheit pro Port

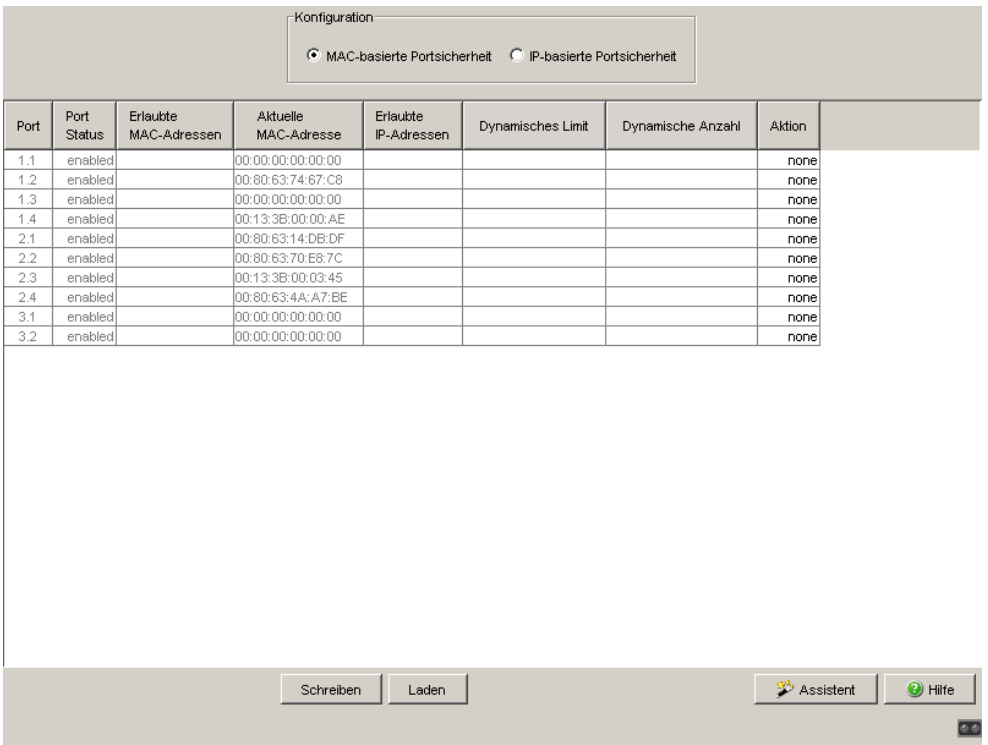


Abb. 29: Dialog Portsicherheit

Anmerkung: Die IP-Portsicherheit arbeitet intern auf Layer 2. Das Gerät übersetzt eine erlaubte IP-Adresse intern in eine erlaubte MAC-Adresse, wenn Sie die IP-Adresse eintragen. Dazu verwendet es eine ARP-Anfrage.

Voraussetzungen für die IP-basierte Portsicherheit:
– das Gerät mit der erlaubten IP-Adresse unterstützt ARP,
– das Gerät ist während der Konfiguration der IP-Portsicherheit erreichbar,
– die MAC-Adresse, die der erlaubten IP-Adresse zugeordnet ist, ist eindeutig und bleibt nach dem Eintragen der IP-Adresse unverändert.

Haben Sie als erlaubte IP-Adresse die eines Router-Interface eingetragen, gelten alle von diesem Interface versandten Pakete als erlaubt, da sie die selbe MAC-Quelladresse enthalten.

Sendet ein angeschlossenes Gerät Pakete mit der erlaubten IP-Adresse, aber einer anderen MAC-Adresse, verweigert der Switch diesen Datenverkehr. Wenn Sie das Gerät mit der erlaubten IP-Adresse gegen ein anderes mit der selben IP-Adresse austauschen, tragen Sie auf dem Switch die IP-Adresse erneut ein, damit der Switch die neue MAC-Adresse lernt.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Assistent	Öffnet den „Assistenten“. Mit dem „Assistenten“ weisen Sie einem Port die zulässigen MAC-Adressen zu.
Hilfe	Öffnet die Online-Hilfe.

Tab. 28: Schaltflächen

Assistent – Port auswählen

Der „Assistent“ unterstützt Sie dabei, die Geräte-Ports mit einem oder mehreren erwünschten Absendern zu verknüpfen.

Parameter	Bedeutung
Port auswählen	Legt den Geräte-Port fest, dem Sie im nächsten Schritt die Absender zuweisen.

Tab. 29: Assistent im Dialog Sicherheit:Portsicherheit, Seite „Port auswählen“

Assistent – Adressen

Der „Assistent“ unterstützt Sie dabei, die Geräte-Ports mit einem oder mehreren erwünschten Absendern zu verknüpfen. Wenn Sie die Einstellungen festgelegt haben, klicken Sie auf „Fertig“. Um die Änderungen anschließend zu speichern, klicken Sie im Dialog `Sicherheit:Portsicherheit` auf „Schreiben“.

Parameter	Bedeutung
Erlaubte MAC-Adressen	Listet die MAC-Adressen auf, die auf den Port zugreifen dürfen. Mögliche Werte: ▶ `Gültige Unicast-MAC-Adresse` Klicken Sie „Hinzufügen“, um die MAC-Adressen in das Feld „Erlaubte MAC-Adressen“ zu übertragen.
MAC-Adresse	Definiert die MAC-Adressen, die auf den Port zugreifen dürfen. Mögliche Werte: ▶ Gültige Unicast-MAC-Adresse Geben Sie den Wert in einem der folgenden Formate ein: – ohne Trennzeichen, z. B. `001122334455` – durch Leerzeichen getrennt, z. B. `00 11 22 33 44 55` – durch Doppelpunkte getrennt, z. B. `00:11:22:33:44:55` – durch Bindestriche getrennt, z. B. `00-11-22-33-44-55` – durch Punkte getrennt, z. B. `00.11.22.33.44.55` – durch Punkte nach jedem 4. Zeichen getrennt, z. B.`0011.2233.4455` Klicken Sie „Hinzufügen“, um die MAC-Adressen in das Feld „Erlaubte MAC-Adressen“ zu übertragen.
Mask	Definiert die Anzahl der wesentlichen Stellen im MAC-Adressbereich. Mögliche Werte: ▶ 1..48 Dieses Feld bietet Ihnen die Möglichkeit, die Anzahl der wesentlichen Stellen in CIDR-Schreibweise anzugeben. Beispiel: 00:11:22:33:44:00/40 bedeutet, dass der Port jenen Geräten den Netzzugang erlaubt, deren MAC-Adresse mit den ersten 5 Hexadezimal-Zahlengruppen übereinstimmt.
Hinzufügen	Überträgt die im Feld „MAC-Addresse“ eingetragenen Werte in das Feld „Erlaubte MAC-Adressen“.
Entfernen	Löscht die im Feld „Erlaubte MAC-Adressen“ ausgewählten Einträge.

Tab. 30: Assistent im Dialog `Sicherheit:Portsicherheit`, Seite „Adressen“

Assistent – Aktion

Dieser Dialog legt die Aktionen fest, die das Gerät ausführt, wenn ein unauthorisierter Zugriff auf den Port erfolgt.

Name	Bedeutung
Aktion	Aktion, die das Gerät nach einem unberechtigten Zugriff ausführt. Mögliche Werte: ▶ `none` (Voreinstellung) Keine Aktion. ▶ `trapOnly` Alarm verschicken. ▶ `portDisable` Deaktiviert den Port. Danach blinkt die Port-LED auf dem Gerät 3 mal grün je Periode. Das Gerät re-aktiviert den Port, wenn Sie im Dialog `Diagnose:Ports:Auto-Disable` folgende Einstellungen festgelegt haben: – Im Rahmen „Konfiguration“ ist das Kontrollkästchen für das auslösende Ereignis „Port-Sicherheit“ markiert. – Der Reset-Timer ist für den Port >0 festgelegt. ▶ `autoDisable` Deaktiviert den Port abhängig von den Einstellungen im Dialog `Diagnose:Ports:Auto-Disable`, Rahmen „Konfiguration“. – Das Gerät deaktiviert den Port, wenn das Kontrollkästchen für das auslösende Ereignis „Port-Sicherheit“ markiert ist. Danach blinkt die Port-LED auf dem Gerät 3 mal grün je Periode. Das Gerät re-aktiviert den Port, wenn im Dialog `Diagnose:Ports:Auto-Disable` für den Port der Reset-Timer für den Port >0 festgelegt ist. – Der Port bleibt aktiviert, wenn das Kontrollkästchen für das auslösende Ereignis „Port-Sicherheit“ unmarkiert ist. **Anmerkung:** Voraussetzungen, damit das Gerät einen Alarm (Trap) senden kann: – Sie haben mindestens einen Empfänger eingetragen, – Sie haben mindestens einen Empfänger in der Spalte „Aktiv“ angekreuzt, – Sie haben im Rahmen „Auswahl“ die „Portsicherheit“ angekreuzt.

Tab. 31: Assistent im Dialog `Sicherheit:Portsicherheit`, Seite „Aktion“

Nach Schließen des Assistenten klicken Sie auf „Schreiben“, um Ihre Einstellungen zu speichern.

Schaltflächen

Schaltfläche	Bedeutung
Zurück	Zeigt die vorherige Seite wieder an. Änderungen gehen dabei verloren.
Weiter	Übernimmt die Änderungen und öffnet die nächste Seite.
Fertig	Übernimmt die Änderungen und schließt die Konfiguration ab.
Abbrechen	Beendet den Assistenten. Änderungen gehen dabei verloren.

Tab. 32: Schaltflächen

2.6 802.1X Port-Authentifizierung

Die 802.1X-Port-Authentifizierung bietet Ihnen die Dialoge
- „802.1X Globale Konfiguration“
- „802.1X-Portkonfiguration“
- „802.1X-Port-Clients“
- „802.1X-Port-Statistiken“

Die portbasierte Netzzugriffskontrolle ist eine im Standard IEEE 802.1X beschriebene Methode zum Schutz von IEEE 802-Netzen vor unberechtigtem Zugriff. Durch die Authentifizierung und Autorisierung eines Endgerätes, das an einem Port des Gerätes angeschlossen ist, kontrolliert das Protokoll den Zugang an diesem Port.
Die 802.1X-Funktion zur Port-Authentifzierung benötigt einen RADIUS-Server, der zur Authentifizierung und Authorisierung eingerichtet ist. Die Authentifizierung und Autorisierung erfolgt durch den Authentikator, in diesem Fall das Gerät. Das Gerät authentifiziert den Supplikanten; d. h. es lässt den Zugriff auf die von ihm angebotenen Dienste zu oder weist ihn ab. Supplikanten sind anfragende Geräte wie z. B. PCs; ein möglicher Dienst ist z. B. der Zugang zum Netzwerk, an das das Gerät angeschlossen ist. Das Gerät greift dafür auf einen externen Authentifizierungsserver (RADIUS-Server) zu, der die Authentifizierungsdaten des Supplikanten überprüft. Die Authentifizierungsdaten tauscht das Gerät mit dem Supplikanten über das Extensible Authentication Protocol over LANs (EAPOL) aus; mit dem RADIUS-Server über das RADIUS-Protokoll.

2.6.1 802.1X Globale Konfiguration

Der Dialog Global bietet Ihnen die Möglichkeit:
- die Port-Authentifizierung ein- oder auszuschalten,
- die VLAN-Zuweisung durch RADIUS zu steuern.

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Funktion	Schaltet die Funktion an oder aus	`An`, `Aus`	`Aus`
VLAN-Zuweisung aktivieren	Aktiviert oder deaktiviert das Zuweisen einer VLAN-ID durch den RADIUS-Server an einen Port. Wenn ein Gerät an einem Port per 802.1X eine Anfrage stellt, sendet der RADIUS-Server bei einer positiven Antwort optional eine VLAN-ID mit. Haben Sie die Funktion aktiviert, nimmt der Switch den Port daraufhin als ungetaggtes Mitglied in das angegebene VLAN auf und setzt die Port-VLAN-ID auf diesen Wert. Beachten Sie die folgenden Hinweise zur VLAN-Zuweisung.	`An`, `Aus`	`Aus`

Tab. 33: Dialog 802.1X-Port-Sicherheit, Teil 1

Anmerkung:

- **Für das Gerät MACH 1040:**
- **Für andere Geräte:**

  Der Switch kann ungetaggte Frames pro Port einem VLAN zuweisen.
  Wenn Sie:
  – für einen Port die Multi-Client-Einstellung verwenden und
  – der Switch bereits ein Port-VLAN für den bestehenden Client eingerichtet hat,

  dann akzeptiert der Switch einen zusätzlichen Client ausschließlich dann:
  – wenn der RADIUS-Server diesem dieselbe VLAN-ID zuweist.

  Weicht die VLAN-ID für den neuen Client ab, entscheidet der Switch anhand der Authentifizierungs-Priorität der Clients, welchem Client er Zugriff gewährt:
  Ein Client, der sich per 802.1X authentifiziert, hat eine höhere Priorität als ein Client mit Zugang in das Gast- oder unauthentifizierte VLAN.
  – Meldet sich ein Client mit niedriger Priorität an, verweigert der Switch dem Client mit niedriger Priorität den Zugang und gewährt weiterhin dem Client mit der höheren Priorität Zugang.
  – Meldet sich ein Client mit hoher Priorität an, sperrt der Switch dem Client mit niedriger Priorität den bisherigen Zugang und gewährt statt dessen dem Client mit der höheren Priorität Zugang.

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Dynamische VLAN-Erzeugung aktivieren	Weist den Switch an, das vom RADIUS-Server genannte VLAN anzulegen, falls es noch nicht existiert.	`An` `Aus`	`Aus`
Safe-VLAN-Modus aktivieren	**Für die Gerätefamilien außer MACH 104 und MACH 1040:** Stellt ein, ob der Switch einem Client, der ungetaggte Frames sendet, ausschließlich Zugang in ein sicheres VLAN gewährt oder ob er dem Client ein anderes als das vom RADIUS-Server vorgegebene VLAN zuweisen darf. ▶ `An`: Der Switch gewährt dem Client ausschließlich Zugang zu dem VLAN, dessen ID der RADIUS-Server vorgibt. Stellt der Switch einen Konflikt zwischen der bestehenden Port-VLAN-ID und der vom RADIUS-Server vorgegebenen fest, dann stellt der Switch die Port-VLAN-ID ein, die der Client mit der höheren Authentifizierungs-Priorität anfordert (s. o.). Der Switch verweigert dem Client mit der niedrigeren Priorität den Zugang. ▶ `Aus`: Stellt der Switch einen Konflikt zwischen der bestehenden Port-VLAN-ID und der vom RADIUS-Server vorgegebenen fest, ignoriert der Switch die vom RADIUS-Server vorgegebenen VLAN-ID und gibt dem Client Zugang in das VLAN der Port-VLAN-ID (Native VLAN-ID).	`An` `Aus`	`Aus`

Tab. 34: Dialog 802.1X-Portsicherheit, Teil 2

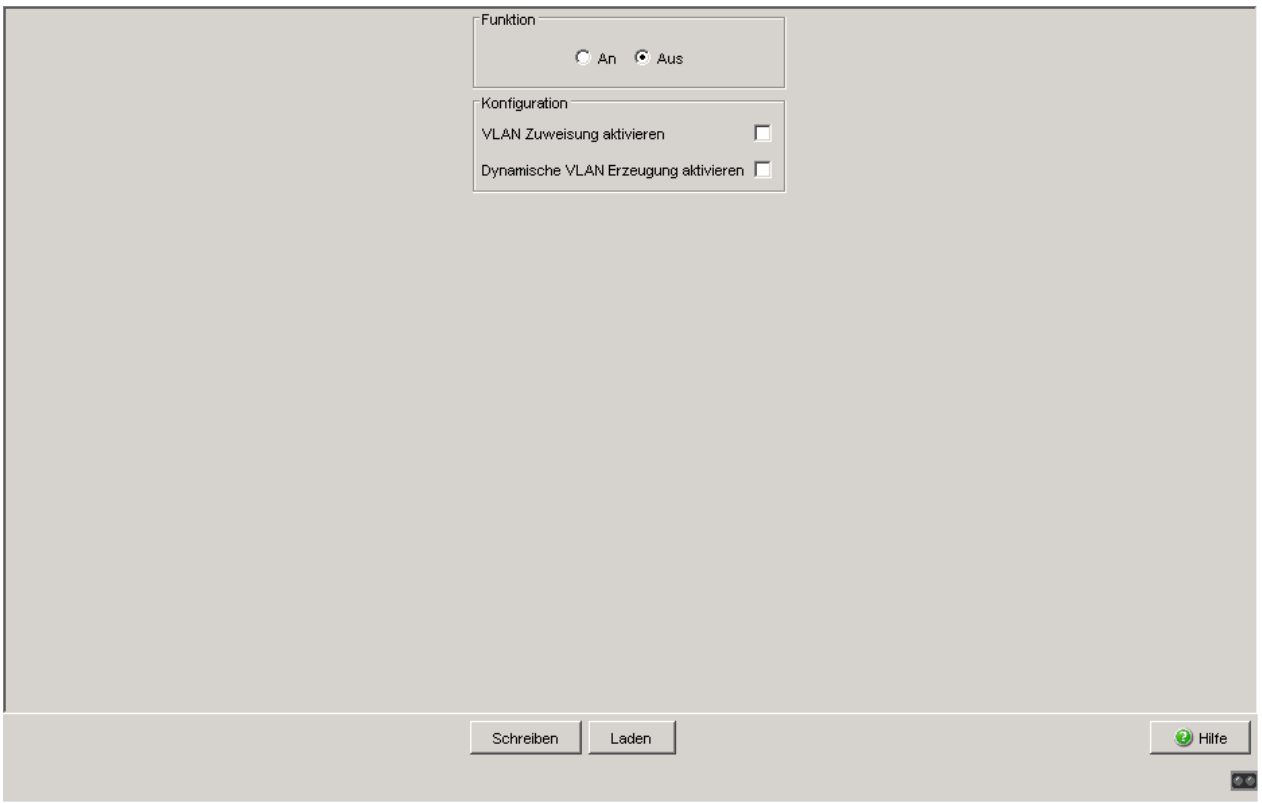


Abb. 30: Dialog 802.1X Global für die Gerätefamilien MACH 104 und MACH 1040

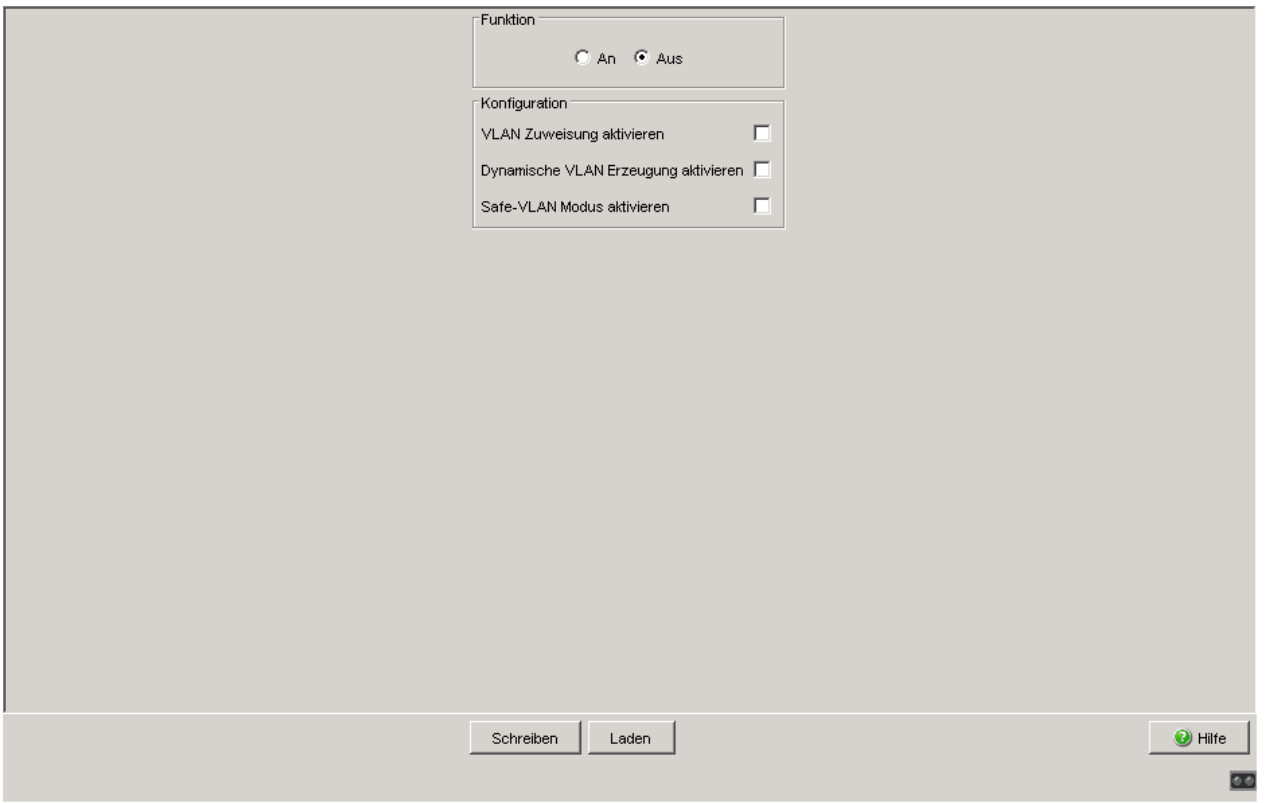


Abb. 31: Dialog 802.1X Global

Vorbereitung des Gerätes auf die 802.1X-Port-Authentifizierung:

☐ Konfigurieren Sie die IP-Parameter des Gerätes.
☐ Schalten Sie die Funktion der 802.1X-Port-Authentifizierung global ein.
☐ Setzen Sie die 802.1X- „Port-Kontrolle“ auf `auto`. Voreingestellt ist `forceAuthorized`.
☐ Konfigurieren Sie einen Radius-Server zur Authorisierung und Authentifizierung.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 35: Schaltflächen

2.6.2 802.1X-Portkonfiguration

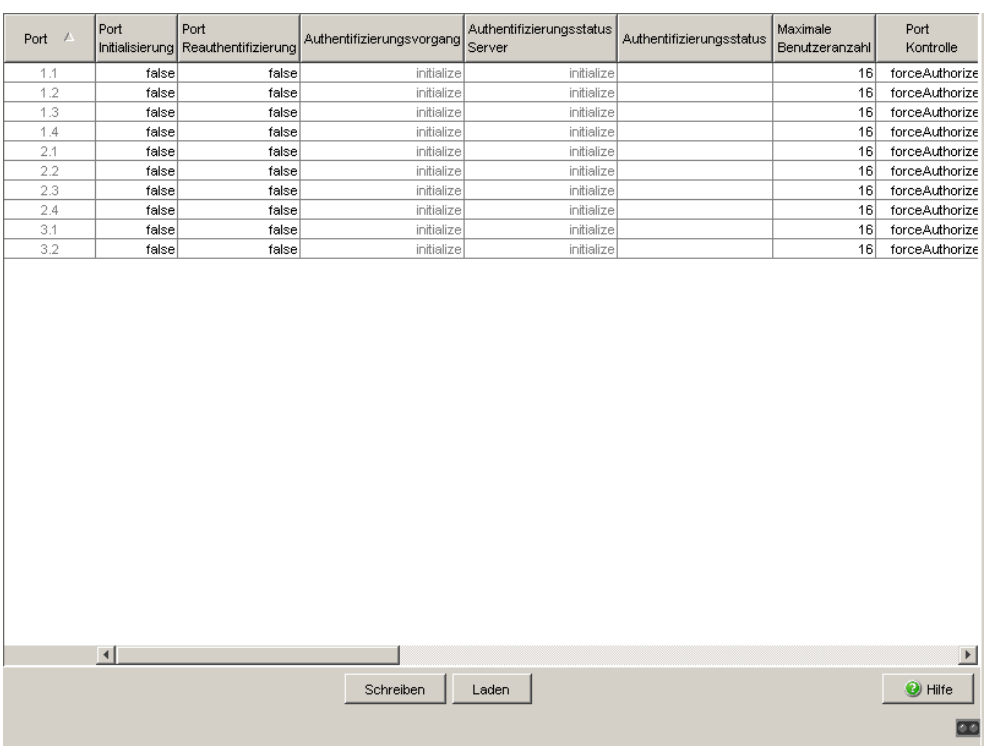


Abb. 32: 802.1X-Port-Konfigurationstabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port-Initialisierung	Rücksetzen der Initialisierungsfunktion. "true" veranlasst das Gerät für diesen Port die Funktion zurückzusetzen. Nach Abschluss des Rücksetzvorganges fällt der Wert wieder auf "false" zurück	`true, false`	`false`
Port-Reauthentifizierung	Ein- und Ausschalten der erneuten Authentifizierung des Ports. "true" veranlasst das Gerät, den Supplikant aufzufordern, sich an diesem Port erneut zu authentifizieren. Nach Anstoß der erneuten Authentifizierung setzt das Gerät den Wert wieder auf "false".	`true, false`	`false`
Authentifizierungsvorgang	Zeigt den aktuellen Zustand des Authentifizierungvorgangs an.	1 = aktiviert (initialize) 2 = getrennt (disconnected) 3 = Verbindung aufbauen (connecting) 4 = Authentifizierung durchführen (authenticating) 5 = authentifiziert (authenticated) 6 = Authentifizierung abbrechen (aborting authenticating) 7 = temporär nicht authentifiziert (held) 8 = Zugang ohne Authentifizierung (force Autherized) 9 = Kein Zugang (force Unauthorized)	
Authentifizierungsstatus Server	Zeigt den aktuellen Status des Authentifizierungsservers.	1 = Anforderung (request) 2 = Antwort (response) 3 = Erfolg (success) 4 = Fehler (fail) 5 = Zeitüberschreitung (timeout) 6 = Ruhephase (idle) 7 = Einrichten (initialize)	

Tab. 36: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Konfigurationstabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Authentifizierungsstatus	Zeigt den aktuellen Wert des Authentifizierungsstatus´ für den Port an.	`authorized` = der angeschlossene Teilnehmer ist authentifiziert `unauthorized` = der angeschlossene Teilnehmer ist nicht authentifiziert.	
Maximale Benutzeranzahl	Maximale Anzahl an Clients, die das Gerät an einem Port gleichzeitig authentifiziert. Dieser Parameter wirkt sich aus, wenn Sie die Portkontrolle (s.u.) auf `macBased` eingestellt haben.	`1 - 16`	`16`
Port-Kontrolle	Einstellen der Portzugangskontrolle. **Anmerkung:** ▶ In den Modi `ForceAuthorized`, `ForceUnauthorized` und `auto` öffnet oder sperrt der Switch den Port für alle Clients. Verwenden Sie diese Modi, wenn Sie einen einzelnen Client an den Switch anschließen. ▶ Im Modus `macBased` authentifiziert der Switch die Clients auf der Basis der einzelnen MAC-Adressen und erlaubt oder sperrt deren Datenverkehr individuell. Verwenden Sie diesen Modus, wenn Sie die Multi-Client-Authentifizierung oder die Funktion „MAC Authentication Bypass“ nutzen möchten.	▶ ForceAuthorized: Zugang auch ohne Authentifizierung für alle Clients offen. ▶ `ForceUnauthorized`: Zugang für alle Clients gesperrt, auch für Clients mit Authentifizierung. ▶ `auto`: der Zugang zum Port ist vom Authentifizierungsergebnis abhängig. ▶ `macBased`: Verhalten wie bei auto. Zusätzlich Zugang für Clients mit einer MAC-Adresse, die der Client bei der Authentifizierung verwendet.	`ForceAuthorized`
Ruheperiode	Periode in Sekunden, in der der Authentifizierungsablauf keine Authentifizierung vom Supplikanten erwartet.	0-65.535	60
Sendeperiode	Wartezeit, bevor das Gerät ein EAP-Paket erneut sendet.	1-65.535	30
Supplikant-Zeitüberschreitung	Zeitüberschreitung bei der Kommunikation zwischen Gerät und Supplikant in Sekunden.	1-65.535	30

Tab. 36: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Konfigurationstabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Server-Zeitüberschreitung	Zeitüberschreitung bei der Kommunikation zwischen Gerät und Server in Sekunden.	1-65.535	30
Maximale Requestanzahl	Maximale Anzahl von Anforderungsversuchen an den Supplikanten, bevor der Authentifizierungsvorgang endet.	1-10	2
Zugewiesene VLAN-ID	VLAN, das der Switch dem Port zugewiesen hat. Der Port ist ungetaggtes Mitglied in diesem VLAN und die Port-VLAN-ID hat den selben Wert. Voraussetzung: Die Portkontrolle ist auf `auto` gesetzt. **Anmerkung:** Wenn Sie die Multi-Client-Einstellung verwenden, indem Sie die „Port-Kontrolle“ auf `macBased` setzen, beachten Sie: ▶ die geräteabhängige Auflösung von etwaigen VLAN-Zuweisungs-Konflikten für ungetaggt empfangene Frames; (siehe auf Seite 98 „802.1X Globale Konfiguration“) ▶ die zugewiesenen VLANs finden Sie die aktuellen Werte in der Tabelle „Port-Clients“ . (siehe auf Seite 111 „802.1X-Port-Clients“)	`0 - 4094`	0

Tab. 36: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Konfigurationstabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand

Zuweisungsgrund	Grund der Zuweisung des VLANs an den Port.
	Voraussetzung: Die Portkontrolle ist auf `auto` gesetzt.
	
	Anmerkung: Wenn Sie die Multi-Client-Einstellung verwenden, indem Sie die „Port-Kontrolle“ auf `macBased` setzen, beachten Sie:
	▶ die geräteabhängige Auflösung von etwaigen VLAN-Zuweisungs-Konflikten für ungetaggt empfangene Frames;
	(siehe auf Seite 98 „802.1X Globale Konfiguration“)
	▶ die zugewiesenen VLANs finden Sie die aktuellen Werte in der Tabelle „Port-Clients“ .
	(siehe auf Seite 111 „802.1X-Port-Clients“)
		`notAssigned`
		`radius`
		`unauthenticated-VLAN`
			`notAssigned`

Reauthentifizierungsperiode	Zeit in Sekunden, nach der das Gerät eine erneute Authentifizierung vom Supplikanten anfordert.	1-65.535	3.600
Reauthentifikation ein	Ein- oder Ausschalten der Reauthentifikation	Markiert (ein), Nicht markiert (aus)	Nicht markiert (aus)

Tab. 36: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Konfigurationstabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Gast-VLAN-ID	ID eines VLANs, das der Switch dem Port zuweist, wenn: ▶ das Protokoll 802.1X an dem Port aktiv ist und die Port-Kontrolle auf `auto` oder `macBased` gesetzt ist, ▶ ein Client Datenverkehr aufnehmen will ▶ und EAPOL-Frames vom Client ausbleiben, der Client also das 802.1X-Protokoll nicht unterstützt. Der Switch: ▶ schaltet den Port in den authentifizierten Zustand, ▶ lässt den Datenverkehr zu, ▶ jedoch ausschließlich in das Gast-VLAN. Geben Sie eine Gast-VLAN-ID an, wenn Sie Geräten ohne 802.1X-Unterstützung einen Zugang in ein Gast-VLAN erlauben möchten. **Anmerkung:** ▶ Verwenden Sie als Gast-VLAN ausschließlich ein VLAN, das Sie im Switch statisch eingerichtet haben. ▶ Meldet sich ein Client dagegen per 802.1X und schlägt dessen Authentifizierung fehl, dann gibt der Switch ihm ausschließlich Zugang zum unauthentifizierten VLAN. ▶ Wenn Sie Funktion MAC-Authorized-Bypass (MAB) aktivieren, setzt Gerät die Gast-VLAN-ID automatisch auf 0.	0 - 4094 Mit einer VLAN-ID von 0 blockiert der Switch den Datenverkehr, da er die Einrichtung eines VLANs mit dieser ID ablehnt.	0
Gast-VLAN-Intervall	Zeit, die der Switch nach dem Anschließen eines Gerätes an diesem Port auf EAPOL-Frames wartet, um festzustellen, ob dieses das 802.1X-Protokoll unterstützt. Läuft diese Zeit ab, stellt der Switch dem angeschlossenen Gerät einen Zugang ausschließlich ins Gast-VLAN zur Verfügung.	1 - 300 s	90 s

Tab. 36: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Konfigurationstabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Unauthenticated VLAN ID	ID eines VLANs, das der Switch dem Port zuweist, wenn: ▶ das Protokoll 802.1X an dem Port aktiv ist, ▶ der Switch EAPOL-Frames vom Client empfängt, dieser also das 802.1X-Protokoll unterstützt, ▶ und die Authentifizierung des Clients fehlschlägt. Der Switch: ▶ schaltet den Port in den authentifizierten Zustand, ▶ lässt den Datenverkehr zu, ▶ jedoch ausschließlich in das unauthentifizierte VLAN. Geben Sie eine VLAN-ID für unauthentifizierte Geräte an, wenn: ▶ Sie Geräten einen Zugang in ein bestimmtes VLAN erlauben möchten, ▶ diese Geräte 802.1X zwar unterstützen, ▶ Ihrem Netz jedoch deren Identität und Authentizität unbekannt ist. **Anmerkung:** ▶ Verwenden Sie als unauthentifiziertes VLAN ausschließlich ein VLAN, das Sie im Switch statisch eingerichtet haben.	0 - 4094 Mit einer VLAN-ID von 0 blockiert der Switch den Datenverkehr, da er die Einrichtung eines VLANs mit dieser ID ablehnt.	0

Tab. 36: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Konfigurationstabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
MAC-Authorized-Bypass ein	Durch MAB stellt der Switch einen authentifizierten Zugang zur Verfügung, wenn: ▶ Sie die „Port-Kontrolle“ auf `macBased` gesetzt haben, ▶ ein Gerät mit einer bestimmten bekannten MAC-Adresse Datenverkehr aufnehmen will, ▶ sich dieses Gerät nicht per 802.1X authentifiziert und ▶ der RADIUS-Server die zugriffsberechtigten MAC-Adressen kennt. Der Switch: ▶ wartet dazu den Ablauf des Gast-VLAN-Intervalls ab, ▶ sendet dann eine Anfrage an den RADIUS-Server und verwendet dabei die MAC-Adresse als Benutzername und Passwort. Aktivieren Sie diese Funktion, wenn: ▶ Sie bestimmten Geräten einen normalen Zugang erlauben möchten, ▶ obwohl diese Geräte 802.1X nicht unterstützen. **Anmerkung:** ▶ Lehnt der RADIUS-Server die MAB-Authentifizierung ab, sperrt der Switch den Zugang für das Gerät. ▶ Wenn Sie Funktion aktivieren, schaltet das Gerät den Gast-VLAN-Zugang automatisch ab.	`An` `Aus`	`Aus`

Tab. 36: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Konfigurationstabelle

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 37: Schaltflächen

2.6.3 802.1X-Port-Clients

Das Gerät bietet Ihnen die Möglichkeit, an einem Port mehrere Geräte zu betreiben (z. B. über einen Hub) und diese Geräte einzeln zu authentifizieren (Multi-Client-Authentifizierung).
Das bedeutet, dass der Switch einem authentifizierten Gerät Datenverkehr erlaubt, aber gleichzeitig den noch nicht authentifizierten Geräten den Datenverkehr in Sende- und Empfangsrichtung verweigert.
Dies gilt ebenso für Geräte, deren Authentifizierung abgelaufen ist und die diese nicht erneuert haben.
Ebenso kann sich ein Gerät aus dem authentifizierten Status abmelden und wird danach vom Switch für seinen Datenverkehr blockiert, ohne dass dies Auswirkungen auf den Datenverkehr anderer authentifizierter Geräte hat.
Dabei unterscheidet der Switch die Geräte anhand ihrer MAC-Absenderadresse.
Sie haben die Möglichkeit, an einem Port bis zu 16 Geräte einzeln zu authentifizieren.

Der Dialog zeigt Ihnen die Daten der authentifizierten Geräte pro Port an.

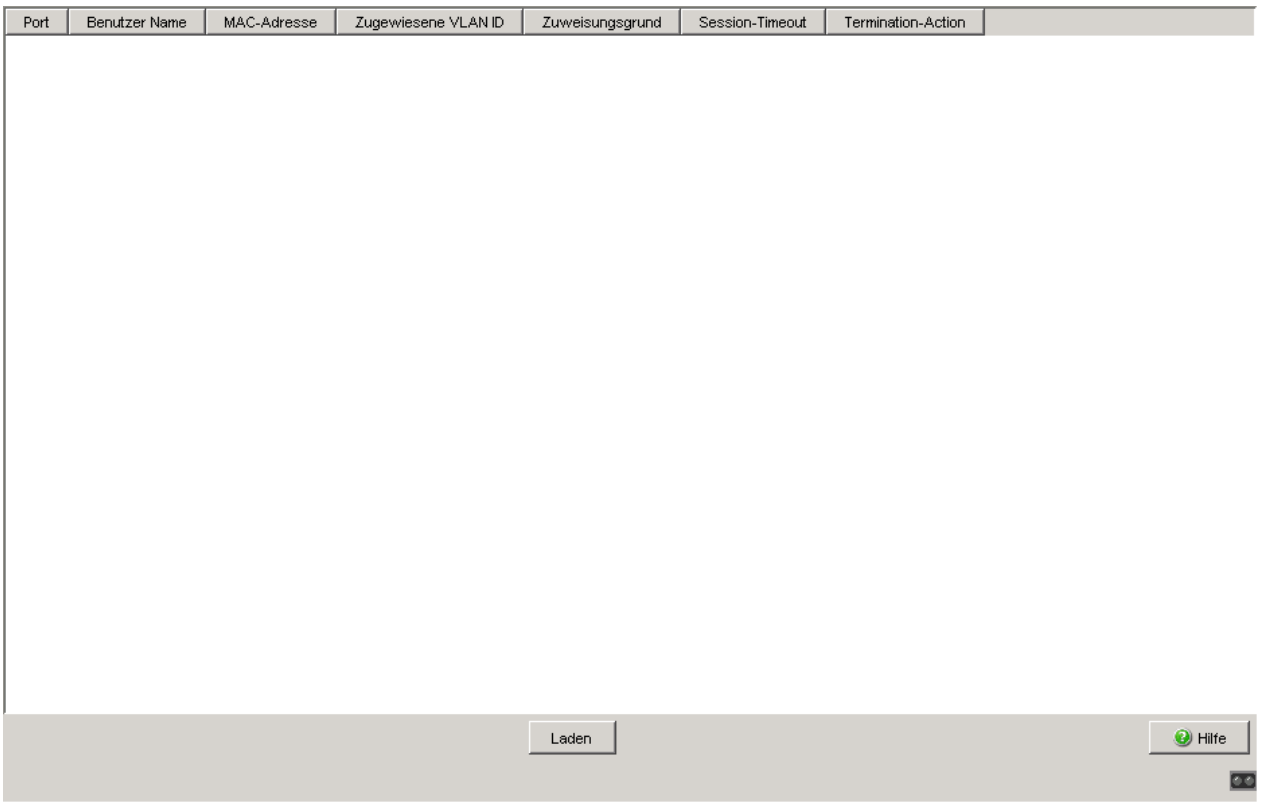


Abb. 33: 802.1X-Port-Client-Tabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port	Modul- und Port-Nummer, für die dieser Eintrag gilt	-	-
Benutzer Name	Der Name, mit dem sich der Client (in der Rolle des IEEE 802.1X-Supplikanten) gegenüber dem Switch identifiziert hat	Der Benutzername des IEEE 802.1X-Supplikanten	-
MAC-Adresse	Die MAC-Adresse des Clients	Unicast-MAC-Adresse	-

Tab. 38: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Port-Client-Tabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Zugewiesene VLAN-ID	Die VLAN-ID, die das Protokoll 802.1X dem Port nach erfolgreicher Authentifizierung des 1. Clients zugewiesen hat. **Anmerkung:** Wenn Sie die Multi-Client-Einstellung verwenden, indem Sie die „Port-Kontrolle“ auf `macBased` setzen, beachten Sie: ▶ die geräteabhängige Auflösung von etwaigen VLAN-Zuweisungs-Konflikten für ungetaggt empfangene Frames; (siehe auf Seite 98 „802.1X Globale Konfiguration“) ▶ die zugewiesenen VLANs finden Sie die aktuellen Werte in der Tabelle „Port-Clients“ . (siehe auf Seite 111 „802.1X-Port-Clients“)	`0 – 4094`	-
Zuweisungsgrund	Grund der Zuweisung des VLANs an den Client.	`default`, `radius`, `unauthenticatedVlan`, `invalid`	-
Session-Timeout	Dauer der authentifizierten Sitzung des Clients nach der Authentifizierung oder Reauthentifizierung, in Sekunden	0 - 65.535 s (0: kein Timeout)	-
Termination-Action	Aktion, die der Switch beim Ablauf der Sitzungszeit des Clients durchführt	`default`, `reauthenticate`	?

Tab. 38: 802.1X-Einstellmöglichkeiten pro Port, Einträge in der Port-Client-Tabelle

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 39: Schaltflächen

2.6.4 802.1X-Port-Statistiken

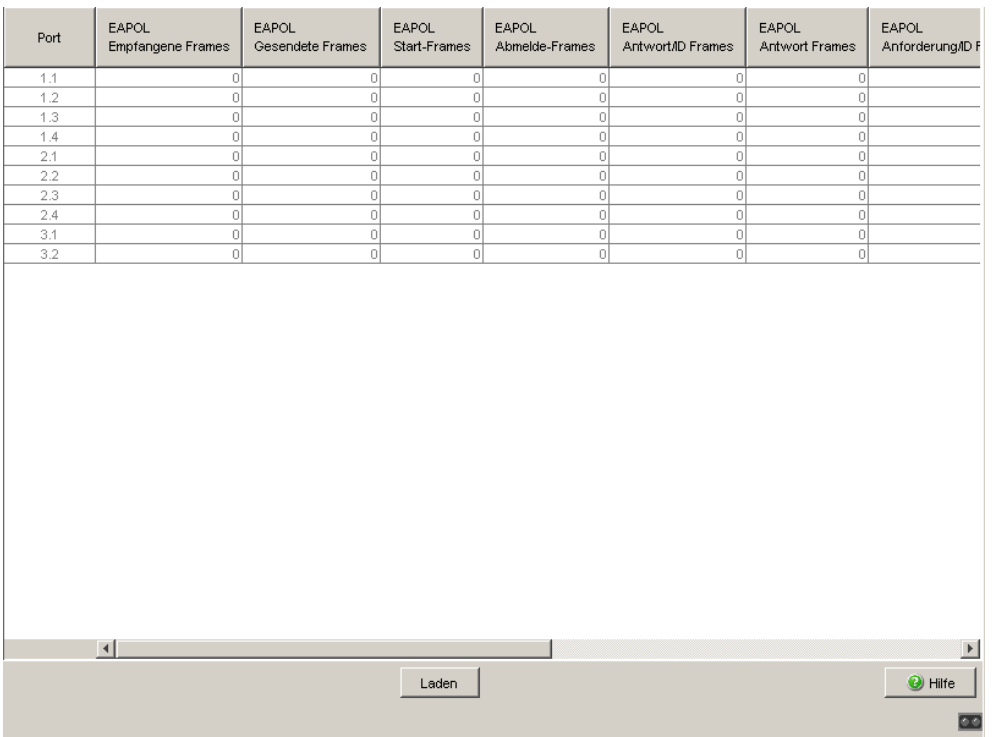


Abb. 34: 802.1X-Statistiktabelle

Parameter	Bedeutung
EAPOL Empfangene Frames	Anzahl der EAPOL-Frames (gültige sowie ungültige) beliebigen Typs, die an diesem Port empfangen worden sind.
EAPOL Gesendete Frames	Anzahl der EAPOL-Frames beliebigen Typs, die an diesem Port empfangen worden sind.
EAPOL Start-Frames	Anzahl der EAPOL-Start-Frames, die an diesem Port empfangen worden sind.
EAPOL Abmelde-Frames	Anzahl der EAPOL-Abmelde-Frames, die an diesem Port empfangen worden sind.
EAPOL Antwort/ID Frames	Anzahl der EAP-Antwort/ID-Frames, die an diesem Port empfangen worden sind.
EAPOL Antwort Frames	Anzahl der gültigen EAP-Antwort-Frames (außer Antwort/ID-Frames), die an diesem Port empfangen worden sind.
EAPOL Anforderung/ID Frames	Anzahl der EAP-Anforderung/ID-Frames, die an diesem Port gesendet worden sind.

Tab. 40: 802.1X-Statistiktabelle

Parameter	Bedeutung
EAPOL Anforderung Frames	Anzahl der EAPOL Anforderung Frames (außer Anforderung/ID-Frames), die an diesem Port gesendet worden sind.
EAPOL Ungültige Frames	Anzahl der EAPOL-Frames, mit nicht erkanntem Frametyp, die an diesem Port gesendet worden sind.
Empfangene EAPOL Fehler Frames mit ungültiger Längenangabe	Anzahl der EAPOL-Frames mit ungültigem Packet Body Length-Feld, die an diesem Port gesendet worden sind.
EAPOL Frame Version	Die Protokoll-Versionsnummer, die im zuletzt an diesem Port empfangenen EAPOL-Frame enthalten ist.
Quelladresse des zuletzt empfangenen EAPOL-Frames	Die MAC-Quelladresse des zuletzt empfangenen EAPOL-Frames. 00:00:00:00:00:0000:00:00:00:00:00 bedeutet: Noch keine Frames erhalten.

Tab. 40: 802.1X-Statistiktabelle

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 41: Schaltflächen

2.7 RADIUS

Das Gerät ist ab Werk so eingestellt, dass es Benutzer anhand der lokalen Benutzerverwaltung authentifiziert. Mit zunehmender Größe eines Netzes jedoch steigt der Aufwand, die Zugangsdaten der Benutzer über Geräte hinweg konsistent zu halten.

RADIUS (Remote Authentication Dial-In User Service) bietet Ihnen die Möglichkeit, die Benutzer an einer zentralen Stelle im Netz zu verwalten. Ein RADIUS-Server erledigt dabei folgende Aufgaben:

- Authentifizierung
  Der Authentication-Server authentifiziert die Benutzer, wenn der RADIUS-Client im Zugangspunkt die Zugangsdaten der Benutzer an ihn weiterleitet.
- Autorisierung
  Der Authentication-Server autorisiert angemeldete Benutzer für ausgewählte Dienste, indem er dem RADIUS-Client im Zugangspunkt diverse Parameter für das betreffende Endgerät zuweist.

Das Gerät leitet die Anmeldedaten des Benutzers an den Authentifizierungsserver weiter. Der Authentifizierungsserver prüft, ob die Anmeldedaten gültig sind und übermittelt die Authorisierungen für den Benutzers an das Gerät.

Das Menü enthält die folgenden Dialoge:

- Global
- RADIUS-Server

2.7.1 Global

In diesem Dialog konfigurieren Sie das Gerät dahingehend, dass es Requests des Benutzers zur Bearbeitung an den Radius-Server sendet. Sofern Sie mehrere Server eingerichtet haben und ein Request an den primären Server unbeantwortet bleibt, sendet das Gerät seine Requests an den nächsten aktiven RADIUS-Server.

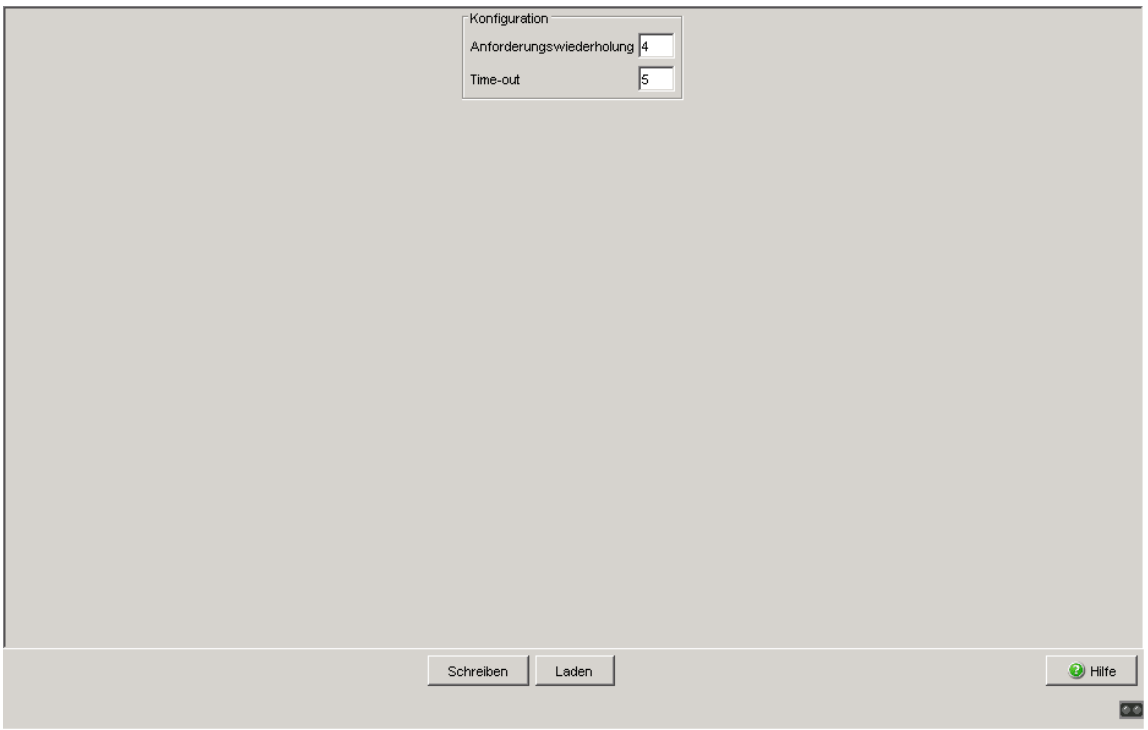


Abb. 35: Dialog `Sicherheit:RADIUS:Global`

Konfiguration

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Anforderungs-wiederholung	Gibt an, wie oft der Switch eine unbeantwortete Anforderung an den RADIUS-Server wiederholt, bevor er die Anforderung an einen anderen RADIUS-Server schickt.	1 - 15	4
Time-out	Stellt ein, wie lange (in Sekunden) der Switch auf eine Antwort des RADIUS-Servers wartet, bevor er die Anforderung erneut schickt.	1 - 30 s	5 s

Tab. 42: Dialog `Sicherheit:RADIUS:Global`

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 43: Schaltflächen

2.7.2 RADIUS-Server

Dieser Dialog bietet Ihnen die Möglichkeit, bis zu 3 RADIUS-Server zu konfigurieren. Der RADIUS-Server authentifiziert und authorisiert den Benutzer, nachdem das Gerät die Anmeldedaten an den Server weitergeleitet hat.

Das Gerät sendet die Anmeldedaten an den angegeben Primär-Server. Bleibt dessen Antwort aus, kontaktiert das Gerät den jeweils nächsten Server aus der Tabelle.

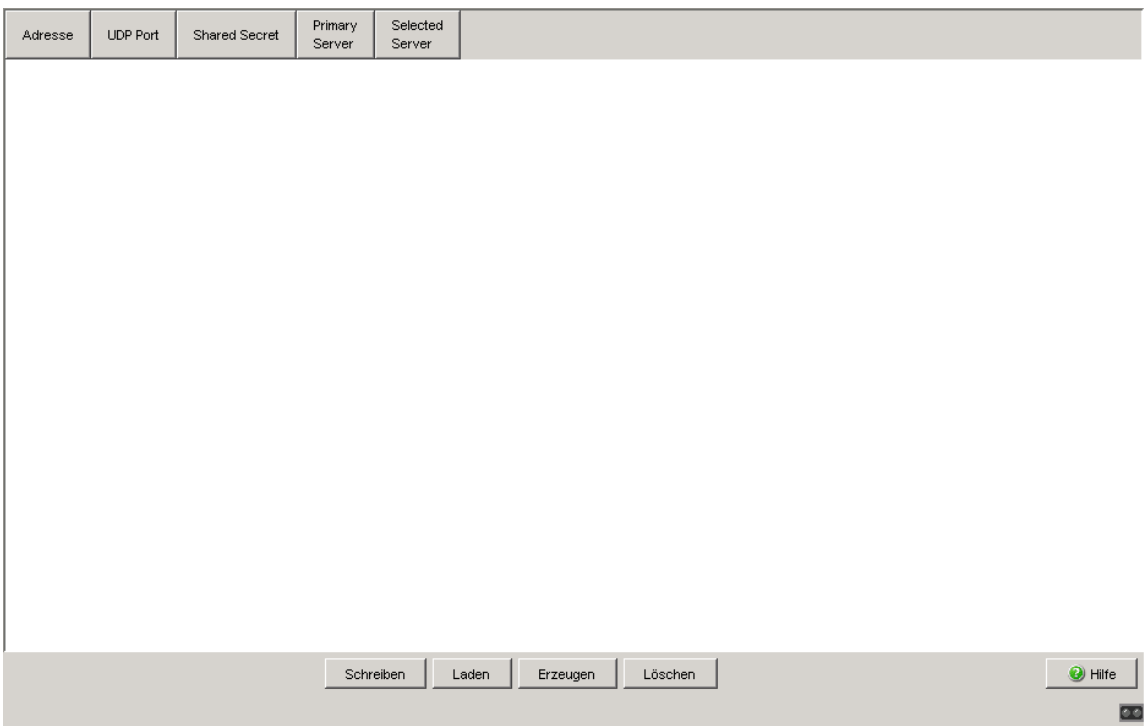


Abb. 36: Dialog `Sicherheit:RADIUS:RADIUS-Server` für das Gerät Power MICE

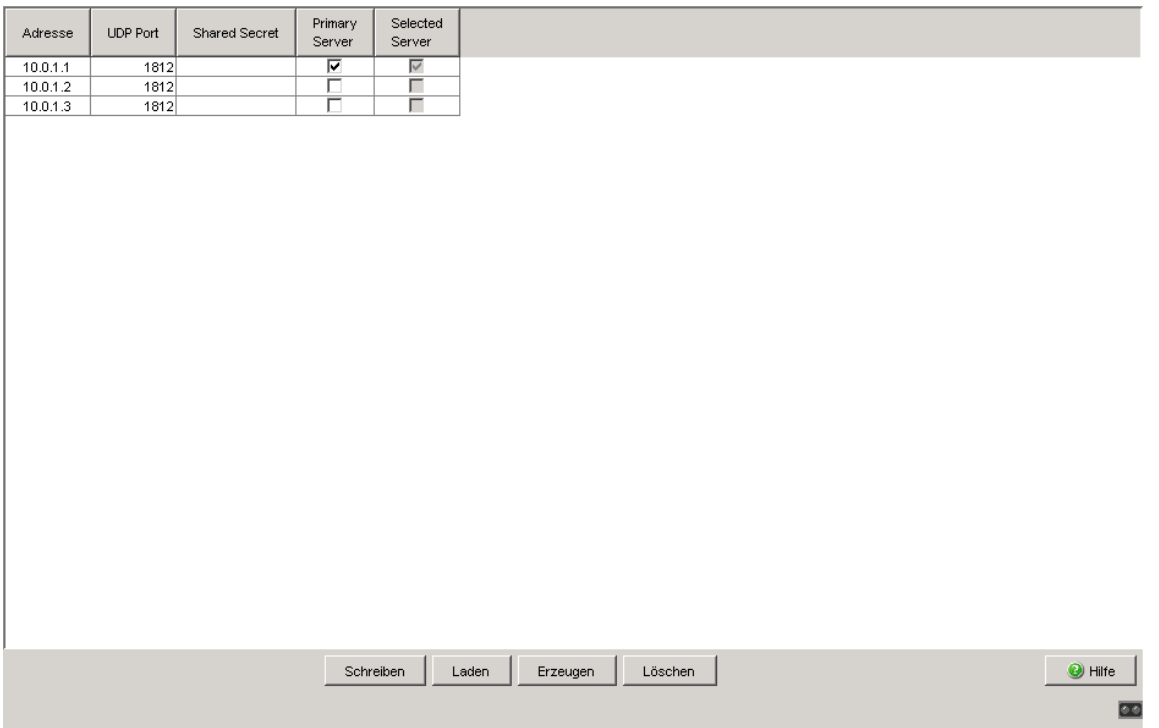


Abb. 37: Dialog `Sicherheit:RADIUS:RADIUS-Server` für die Gerätefamilie MACH 1040:

Tabelle

Parameter	Bedeutung
Adresse	Legt die IP-Adresse des Servers fest. Mögliche Werte: ▶ Gültige IPv4-Adresse
UDP-Port	Legt die Nummer des UDP-Ports fest, auf dem der Server Anfragen entgegennimmt. Mögliche Werte: ▶ `0..65535` (Lieferzustand: `1812`) Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Tab. 44: Tabelle im Dialog `Sicherheit:RADIUS:RADIUS-Server`

Parameter	Bedeutung
Shared Secret	Beinhaltet das Passwort, mit dem sich das Gerät beim Accounting-Server anmeldet. Um das Passwort für den Server zu ändern, klicken Sie in das betreffende Passwortfeld. Ein gespeichertes Passwort zeigt das Gerät als ****** (Asterisks) an. Mögliche Werte: ▶ 1..20 alphanumerische Zeichen Das Passwort erfahren Sie vom Administrator des RADIUS-Servers.
Primary Server	Kennzeichnet den Authentication-Server als primär oder sekundär. Mögliche Werte: ▶ `markiert` Der Server ist als primärer Authentication-Server gekennzeichnet. Das Gerät sendet die Zugangsdaten zum Authentifizieren der Benutzer an diesen Authentication-Server. Wenn Sie mehrere Server markieren, kennzeichnet das Gerät den zuletzt markierten Server als primären Authentication-Server. ▶ `unmarkiert` (Lieferzustand) Der Server ist als sekundärer Authentication-Server gekennzeichnet. Das Gerät sendet die Zugangsdaten an den sekundären Authentication-Server, wenn es vom primären Authentication-Server keine Antwort erhält.
Selected Server	Zeigt die Verbindung zu einem aktiven Server an. Mögliche Werte: ▶ `markiert` Die Verbindung ist aktiv. Sofern die oben beschriebenen Bedingungen erfüllt sind, sendet das Gerät die Anmeldedaten zur Authentisierung der Benutzer an diesen Server. ▶ `unmarkiert` Die Verbindung ist inaktiv. Das Gerät sendet keine Anmeldedaten an diesen Server.

Tab. 44: Tabelle im Dialog `Sicherheit:RADIUS:RADIUS-Server` (Forts.)

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.

Tab. 45: Schaltflächen

Schaltfläche	Bedeutung
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 45: Schaltflächen (Forts.)

RADIUS-Server Einstellungen

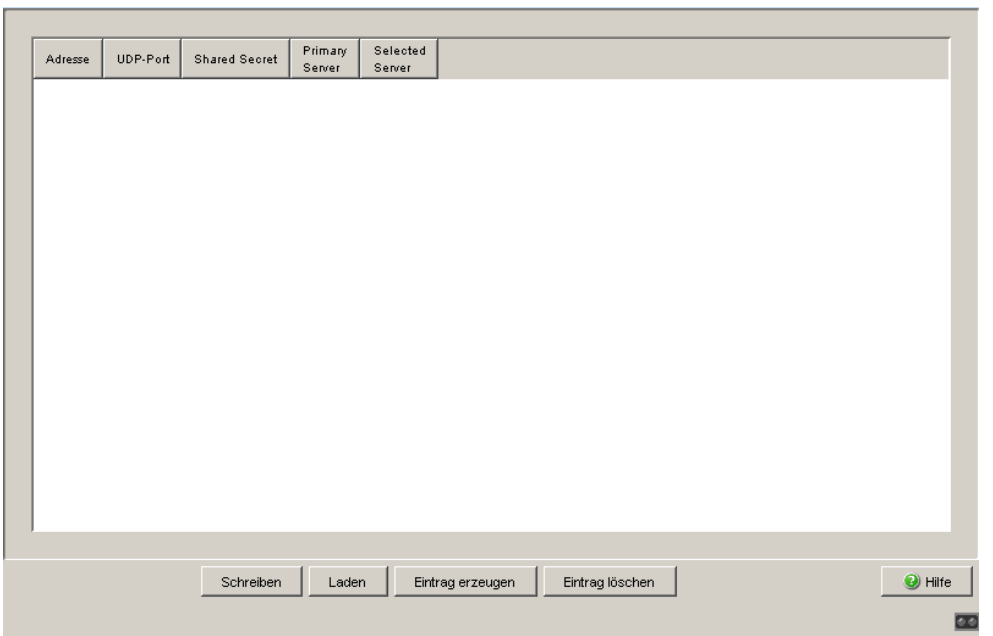


Abb. 38: Dialog RADIUS-Server

Dieser Dialog bietet Ihnen die Möglichkeit, die Daten für bis zu 3 RADIUS-Server einzugeben.

☐ Klicken Sie auf „Erzeugen“, um das Dialogfenster zur Eingabe der IP-Adresse eines RADIUS-Servers anzuzeigen und diese einzugeben.

☐ Bestätigen Sie die Eingabe der IP-Adresse mit „OK“. Damit erzeugen Sie eine neue Zeile in der Tabelle für diesen RADIUS-Server.

☐ Geben Sie in der Spalte „UDP Port“ den UDP-Port für den RADIUS-Server ein (die Voreinstellung ist 1812).

☐ Tragen Sie in der Spalte „Shared Secret“ die Zeichenfolge ein, die Sie vom Administrator Ihres RADIUS-Servers als Schlüssel erhalten.

☐ Mit „Primary Server“ ernennen Sie diesen Server zum ersten Server, den das Gerät bei Portauthentifizierungsanfragen kontaktieren soll. Ist dieser Server nicht erreichbar, dann richtet sich das Gerät an den nächsten Server in der Tabelle.

☐ „Ausgewählter Server“ zeigt Ihnen an, an welchen Server das Gerät seine Anfragen tatsächlich richtet.

☐ Mit „Löschen“ löschen Sie die ausgewählte Zeile in der Tabelle.

Anmerkung: Der Switch schützt das Passwort bei der Übertragung zum RADIUS-Server, indem er statt des Passworts eine MD5-Prüfsumme sendet.

2.8 Login-/CLI-Banner

Dieser Dialog bietet Ihnen die Möglichkeit, Benutzern einen Begrüßungs- oder Hinweistext anzuzeigen, bevor diese sich auf dem Gerät anmelden.

Der Dialog enthält die folgenden Registerkarten:

- Login-Banner
- CLI-Banner

2.8.1 Login-Banner

Diese Registerkarte bietet Ihnen die Möglichkeit, den Benutzern vor der Anmeldung einen Begrüßungs- oder Hinweistext im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface anzuzeigen.

Benutzer, die sich im Command Line Interface mit SSH anmelden, sehen den Text – abhängig vom verwendeten Client – vor oder während der Anmeldung.

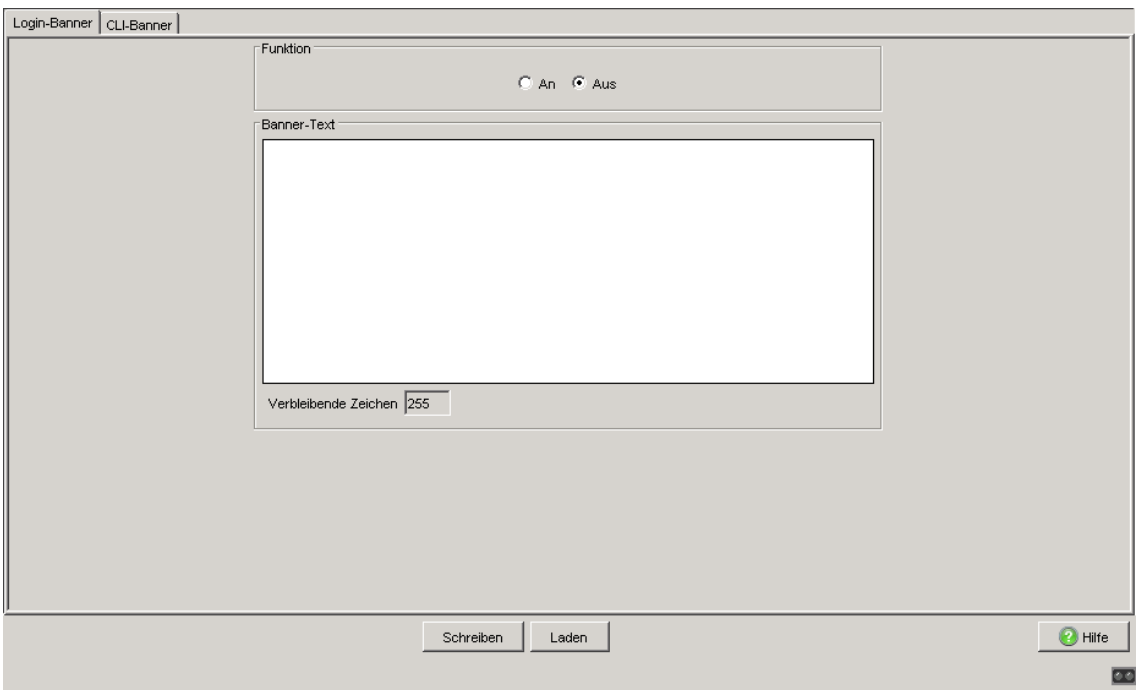


Abb. 39: Dialog „Login-/CLI-Banner“, Registerkarte „Login-Banner“

Funktion

Parameter	Bedeutung
Funktion	Bei eingeschalteter Funktion zeigt das Gerät den Benutzern, die sich im Login-Dialog der grafischen Benutzeroberfläche oder im Command Line Interface anmelden, den im Feld „Banner-Text“ festgelegten Text. Mögliche Werte: ▶ Aus (Voreinstellung) ▶ An

Banner-Text

Parameter	Bedeutung
Banner-Text	Legt den Text fest, den das Gerät im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface anzeigt. Mögliche Werte: ▶ alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen (`0x20..0x7E`) inklusive Leerzeichen ▶ Tabulator `\t` ▶ Zeilenumbruch `\n`
Verbleibende Zeichen	Zeigt, wie viele Zeichen im Feld „Banner-Text“ noch zur Verfügung stehen. Mögliche Werte: ▶ `255..0`

2.8.2 CLI-Banner

Diese Registerkarte bietet Ihnen die Möglichkeit, einen individuellen Text ausschließlich im Command Line Interface anzuzeigen.

In der Voreinstellung zeigt der CLI-Startbildschirm Informationen über das Gerät, z. B. die Software-Version und Geräte-Einstellungen. Mit der Funktion in dieser Registerkarte deaktivieren Sie diese Informationen und ersetzen sie durch den individuell festlegbaren Text.

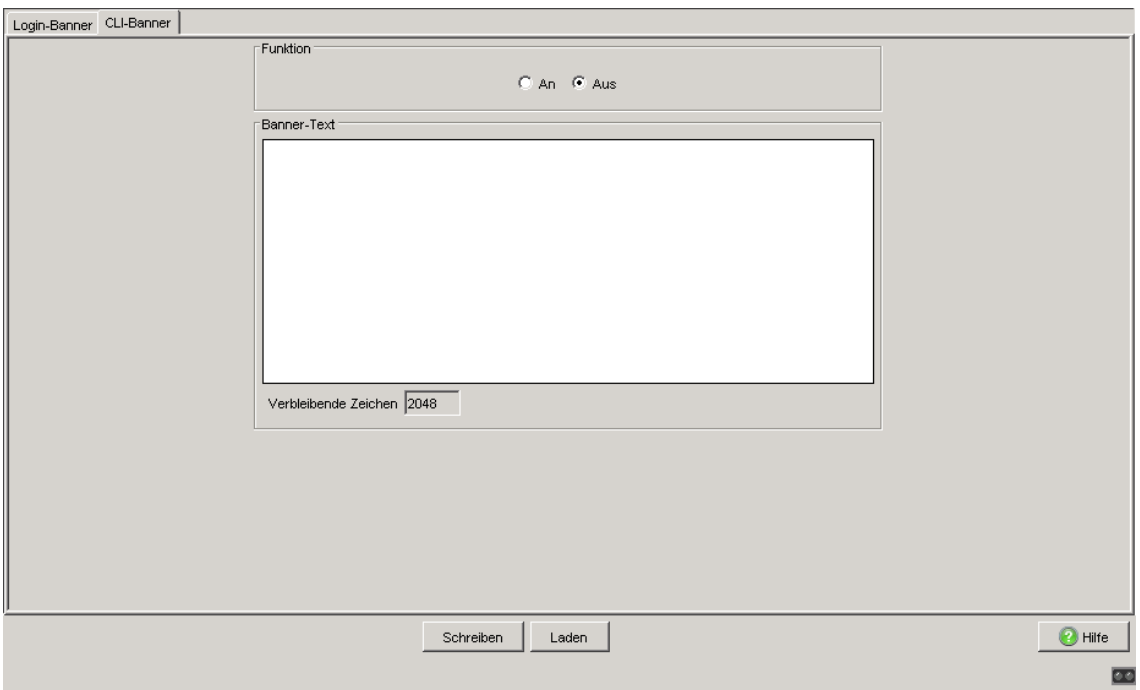


Abb. 40: Dialog „Login-/CLI-Banner“, Registerkarte „CLI-Banner“

Funktion

Parameter	Bedeutung
Funktion	Bei eingeschalteter Funktion zeigt das Gerät den Benutzern, die sich im Command Line Interface auf dem Gerät anmelden, den im Feld „Banner-Text“ festgelegten Text. Bei ausgeschalteter Funktion zeigt der CLI-Startbildschirm Informationen über das Gerät. Die Textinformation im Feld „Banner-Text“ bleibt erhalten. Mögliche Werte: ▶ Aus (Voreinstellung) ▶ An

Banner-Text

Parameter	Bedeutung
Banner-Text	Legt die Textinformation fest, die das Gerät den Benutzern anstatt der voreingestellten Informationen anzeigt. Mögliche Werte: ▶ alphanumerische ASCII-Zeichenfolge mit 0..2048 Zeichen (`0x20..0x7E`) inklusive Leerzeichen ▶ Tabulator `\t` ▶ Zeilenumbruch `\n`
Verbleibende Zeichen	Zeigt, wie viele Zeichen im Feld „Banner-Text“ noch für die Textinformation zur Verfügung stehen. Mögliche Werte: ▶ `2048..0`

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 46: Schaltflächen

2.9 Access Control Lists (ACLs)

Access Control Lists bieten Ihnen die Möglichkeit, eingehende Datenpakete basierend auf L2- und L3-Kriterien zu selektieren und sie entsprechend zu behandeln, z.B. sie zu verwerfen oder zu priorisieren.
Mit Hilfe von ACLs können Sie auf einfache Weise Sicherheits- sowie Quality-of-Service- (QoS-) Funktionen realisieren.
Die Bedingungen, anhand der das Gerät einen bestimmten Paket-Typ selektiert, können Sie feingranular mit einer ACL festlegen. Dies gilt auch für die Aktion, die das Gerät ausführt, wenn die Bedingung zutrifft.

Access Control Lists konfigurieren Sie über das Command Line Interface. Details hierzu finden Sie im Dokument „Referenz-Handbuch Command Line Interface“.

3 Zeit

3.1 Grundeinstellungen

Dieser Dialog bietet Ihnen die Möglichkeit, unabhängig vom gewählten Zeitsynchronisationsprotokoll zeitbezogene Einstellungen vorzunehmen.

- Die „Systemzeit (UTC)“ zeigt die Uhrzeit bezogen auf die koordinierte Weltzeitmessung UTC an.
  Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.

- Die „Systemzeit“ übernimmt die „Systemzeit (UTC)“ unter Berücksichtigung der lokalen Zeitdifferenz zur „Systemzeit (UTC)“.
  „Systemzeit“ = „Systemzeit (UTC)“ + „Lokaler Offset“.

- „Quelle der Zeit“ zeigt den Ursprung der folgenden Zeitangabe an. Das Gerät wählt automatisch die Quelle mit der höchsten Genauigkeit. Mögliche Quellen sind: `local`, `ptp` und `sntp`. Die Quelle ist zunächst `local`.
  Ist PTP aktiviert und empfängt das Gerät einen gültigen PTP-Frame, setzt es seine Zeit-Quelle auf `ptp`. Ist SNTP aktiviert und empfängt das Gerät ein gültiges SNTP-Paket, setzt es seine Zeit-Quelle auf `sntp`. Das Gerät gibt der Zeitquelle PTP den Vorrang vor SNTP.

☐ Mit „Setze Zeit vom PC“ übernimmt das Gerät die Zeit des PCs als Systemzeit und berechnet mit der lokalen Zeitdifferenz die „Systemzeit (UTC)“.
„Systemzeit (UTC)“ = „Systemzeit“ - „Lokaler Offset“

- „Lokaler Offset“ dient zur Anzeige/Eingabe der Zeitdifferenz zwischen der lokalen Zeit und der „Systemzeit (UTC)“.

☐ Mit „Setze Offset vom PC“ ermittelt das Gerät die Zeitzone auf Ihrem PC und berechnet daraus die lokale Zeitdifferenz.

Das Gerät ist mit einer gepufferten Hardware-Uhr ausgestattet. Diese führt die aktuelle Uhrzeit weiter,
- wenn die Stromversorgung ausfällt oder
- wenn Sie das Gerät von der Stromversorgung trennen.

Damit steht Ihnen nach dem Start des Gerätes wieder die aktuelle Uhrzeit zur Verfügung, z. B. für Log-Einträge.
Die Hardware-Uhr überbrückt eine Ausfallzeit der Stromversorgung von 1 Stunde. Voraussetzung dafür ist, dass die Stromversorgung das Gerät vorher mindestens 5 Minuten kontinuierlich gespeist hat.

Anmerkung: Passen Sie in Zeitzonen mit Sommer-/Winterzeit den lokalen Offset bei der Zeitumstellung an, falls erforderlich.
Der SNTP-Client kann die SNTP-Server-IP-Adressen und den lokalen Offset auch von einem DHCP-Server beziehen.

Interaktion von PTP und SNTP
Laut PTP (IEEE 1588) und SNTP können beide Protokolle parallel in einem Netz existieren. Da aber beide Protokolle die Systemzeit des Gerätes beeinflussen, können Situationen auftreten, in denen beide Protokolle konkurrieren.
Die PTP-Referenzuhr bezieht ihre Zeit entweder über SNTP oder von der eigenen Uhr. Alle anderen Uhren bevorzugen als Quelle die PTP-Zeit.

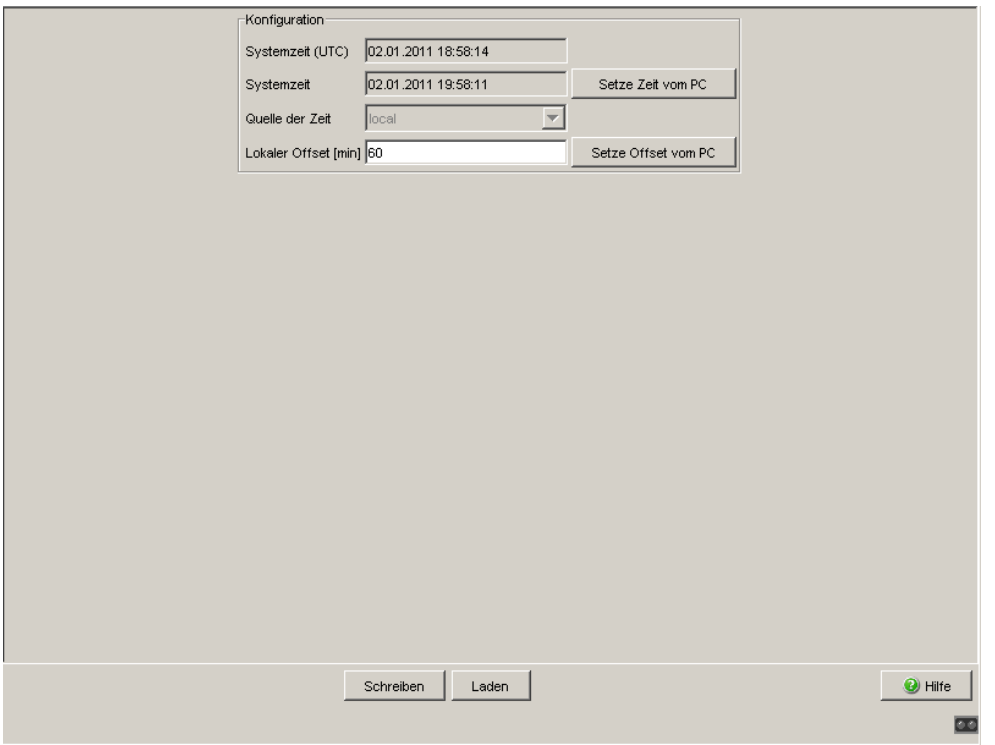


Abb. 41: Dialog Zeit, Grundeinstellungen

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 47: Schaltflächen

3.2 SNTP-Konfiguration

Das Simple Network Time Protocol (SNTP) bietet Ihnen die Möglichkeit, die Systemzeit in Ihrem Netz zu synchronisieren.
Das Gerät unterstützt die SNTP-Client- und die SNTP-Server-Funktion.

Der SNTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.

SNTP verwendet dasselbe Paketformat wie NTP, daher kann ein SNTP-Client seine Zeit sowohl von einem SNTP-Server als auch von einem NTP-Server beziehen.

Anmerkung: Für eine genaue Systemzeitverteilung mit kaskadierten SNTP-Servern und -Clients verwenden Sie im Signalpfad zwischen SNTP-Servern und SNTP-Clients ausschließlich Netzkomponenten (Router, Switches, Hubs), die SNTP-Pakete mit möglichst kleiner Verzögerung weiterleiten.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Funktion	Globales Ein-/Ausschalten der SNTP-Funktion.	`An, Aus`	`Aus`

Tab. 48: Globales Ein-/Ausschalten von SNTP

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
SNTP-Status	Anzeige von Zuständen, wie z.B. „Server nicht erreichbar“.	-	-

Tab. 49: SNTP-Status

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Client-Status	Ein-/Ausschalten des SNTP-Clients.	`An, Aus`	`An`
Externe Server-Adresse	IP-Adresse des SNTP-Servers, von dem das Gerät zyklisch die Systemzeit anfordert.	Gültige IPv4-Adresse	0.0.0.0
Redundante Server-Adresse	IP-Adresse des SNTP-Servers, von dem das Gerät zyklisch die Systemzeit anfordert, wenn es 0,5 Sekunden nach einer Anforderung keine Antwort vom „Externen Server Adresse“ erhält.	Gültige IPv4-Adresse	0.0.0.0
Server-Anforderungsintervall	Zeitabstand, in dem das Gerät SNTP-Pakete anfordert.	1 s - 3.600 s	30 s
SNTP-Broadcasts akzeptieren	Legt fest, ob das Gerät die Systemzeit aus SNTP-Broadcast-/Multicast-Paketen, die es empfängt, übernimmt.	`An, Aus`	`An`
Schwellwert für den Bezug der UTC [ms]	Das Gerät ändert die Zeit, sobald der Betrag der Abweichung zur Serverzeit größer ist als dieser Schwellwert in Millisekunden. Dies reduziert die Häufigkeit der Änderungen der Uhrzeit.	0 - 2.147.483.647 (2^{31}-1)	0
Client deaktivieren nach erfolgter Synchronisation	Ein-/Ausschalten von weiteren Synchronisationen der Uhrzeit, nachdem der Client nach seiner Aktivierung einmal seine Uhrzeit mit dem Server abgeglichen hat.	`An, Aus`	`Aus`

Tab. 50: Konfiguration SNTP-Client

Anmerkung: Haben Sie gleichzeitig PTP eingeschaltet, sammelt der SNTP-Client zuerst 60 Zeitstempel, bevor er sich deaktiviert. Dabei ermittelt das Gerät die Driftkompensation für seine PTP-Uhr. Dies dauert beim voreingestellten Server-Anforderungsintervall etwa eine halbe Stunde.

Anmerkung: Wenn Sie von einer externen/redundanten Server-Adresse die Systemzeit beziehen, schalten Sie den Empfang von SNTP-Broadcasts ab (siehe „SNTP-Broadcasts akzeptieren“). So erreichen Sie, dass das Gerät die Zeit ausschließlich von einem definierten SNTP-Server übernimmt.

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Server-Status	Ein-/Ausschalten des SNTP-Servers.	`An, Aus`	`An`
Anycast-Zieladresse	IP-Adresse, an die der SNTP-Server des Geräts die SNTP-Pakete schickt (siehe Tabelle 52).	Gültige IPv4-Adresse	0.0.0.0
VLAN-ID	VLANs, in das das Gerät zyklisch SNTP-Pakete verschickt.	1-4.042	1
Anycast-Sende-intervall	Zeitabstand, in dem das Gerät SNTP-Pakete verschickt.	1 - 3.600	120
Server deaktivieren bei lokaler Zeitquelle	Ein-/Ausschalten der SNTP-Server-Funk-tion, wenn der Status der Quelle der Zeit `local` ist (siehe Zeit-Dialog).	`An, Aus`	`Aus`

Tab. 51: Konfiguration des SNTP-Servers

IP-Zieladresse	SNTP-Paket versenden an
0.0.0.0	Niemand
Unicast-Adresse (0.0.0.1 - 223.255.255.254)	Unicast-Adresse
Multicast-Adresse (224.0.0.0 - 239.255.255.254), insbesondere 224.0.1.1 (NTP-Adresse)	Multicast-Adresse
255.255.255.255	Broadcast-Adresse

Tab. 52: Zieladressklassen für SNTP- und NTP-Pakete

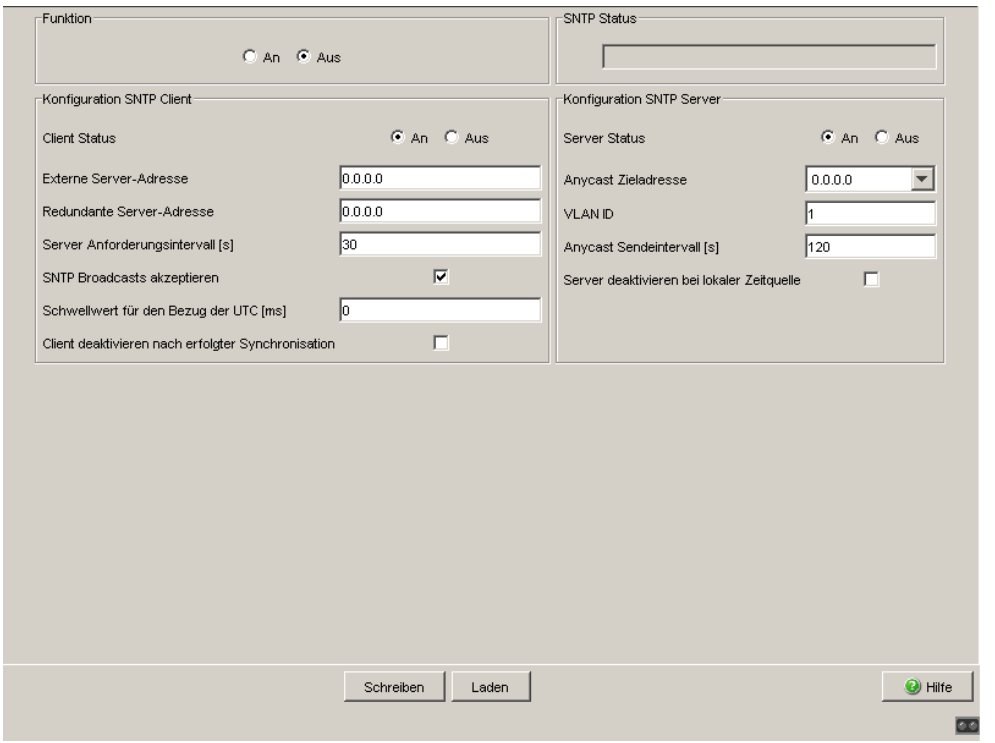


Abb. 42: Dialog SNTP

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 53: Schaltflächen

3.3 PTP (IEEE 1588)

Voraussetzung für zeitkritische, über ein LAN gesteuerte Anwendungen ist ein präzises Zeitmanagement.
Der Standard IEEE 1588 beschreibt mit dem Precision Time Protocol (PTP) ein Verfahren, das die beste Hauptuhr (Best Master Clock) in einem LAN bestimmt und somit die präzise Synchronisation der Uhren in diesem LAN ermöglicht.

Geräte ohne PTP-Hardware-Unterstützung

Geräte ohne PTP-Hardware-Unterstützung, die ausschließlich Ports ohne Zeitstempeleinheit aufweisen, unterstützen den Simple-Modus von PTP. Dieser Modus bietet eine geringere Genauigkeit der Zeitverteilung.

Bei diesen Geräten

- schalten Sie im Dialog `PTP` die PTP-Funktion ein/aus,
- wählen Sie im Dialog `PTP` den PTP-Modus.
  - Wählen Sie `v1-simple-mode`, wenn die Referenzuhr die PTP-Version 1 verwendet.
  - Wählen Sie `v2-simple-mode`, wenn die Referenzuhr die PTP-Version 2 verwendet.

Anmerkung: Im Simple-Modus synchronisiert sich ein Gerät auf empfangene PTP-Nachrichten. Dieser Modus bietet eine mit SNTP vergleichbare Präzision ohne weitere Funktionen wie z.B. PTP-Management oder Laufzeitmessung.Möchten Sie die PTP-Zeit präzise durch Ihr Netz transportieren, verwenden Sie in den Transportpfaden ausschließlich Geräte mit PTP-Hardware-Unterstützung.

Geräte mit PTP-Hardware-Unterstützung

Geräte mit PTP-Hardware-Unterstützung, die Ports mit Zeitstempeleinheit aufweisen, unterstützen abhängig von der Ausführung der Zeitstempeleinheit weitere Modi.

- Die Geräte MS20, MS30 und PowerMICE mit den Modulen
  - MM3-4TX1-RT
  - MM3-2FXM2/2TX1-RT
  - MM3-2FXS2/2TX1-RT
  - MM3-2FLM4/2TX1-RT

  unterstützen die Modi
  - `v1-boundary-clock`
  - `v1-simple-mode`
  - `v2-boundary-clock-twostep`, ausschließlich mit dem Netz-Protokoll `UDP/IPv4` und der Laufzeitmessung `E2E`

- Die Geräte MS20, MS30 und PowerMICE mit den Modulen
  - MM23
  - MM33

  unterstützen die Modi:
  - v1-boundary-clock
  - v1-simple-mode
  - v2-boundary-clock-onestep
  - v2-boundary-clock-twostep
  - v2-transparent-clock
  - v2-simple-mode

- Die Geräte MACH 104 und MACH 1040 unterstützen die Modi
  - v1-boundary-clock
  - v1-simple-mode
  - v2-boundary-clock-twostep
  - v2-transparent-clock
  - v2-simple-mode

Die folgenden Unterkapitel beziehen sich ausschließlich auf Geräte **mit** PTP-Hardware-Unterstützung.

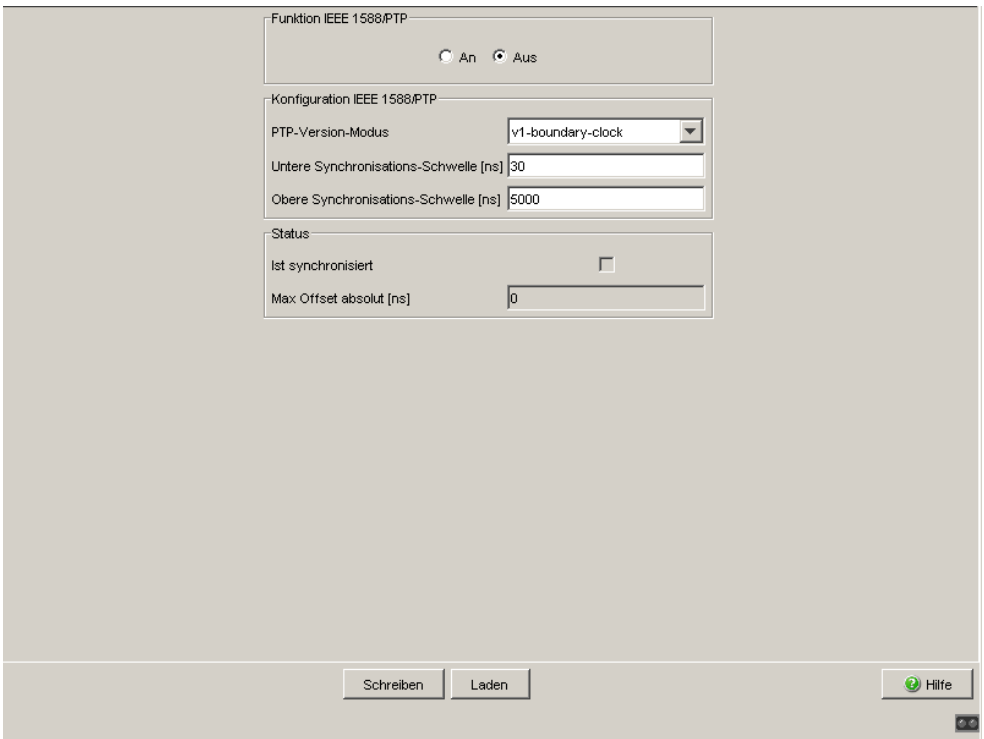


Abb. 43: Dialog PTP Global

Anmerkung: Das Gerät MACH 104 unterstützt PTP ausschließlich an Ports für die Datenraten 10 Mbit/s, 100 Mbit/s und 1 Gbit/s.

Anmerkung: Die Geräte MACH 104 und MACH 1040 unterstützen eine maximale Sync-Empfangs-Rate von 8 Frames/s.

Anmerkung: Die Geräte MACH 1140 und MACH 1142 unterstützen PTP ausschließlich an den Front-Ports 1 - 16.

3.3.1 PTP Global (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

Bei der Auswahl der PTP-Version und des PTP-Modus hilft Ihnen die untenstehende Tabelle.

Version	Modus	Referenzuhr verwendet	Gerät mit Zeitstempeleinheit	PTP-Nachrichten
Version 1	`v1-simple-mode`	Version 1	Nein	—
	`v1-boundary-clock`	Version 1	Ja	bearbeiten
Version 2	`v2-simple-mode`	Version 2	Nein	—
	`v2-boundary-clock-onestep`	Version 2	Ja	bearbeiten
	Anmerkung: Für die Geräte MS20, MS30 und PowerMICE mit den Modulen MM23 oder MM33, siehe die Abschnitte „Geräte ohne PTP-Hardware-Unterstützung” auf Seite 139 und „Geräte mit PTP-Hardware-Unterstützung” auf Seite 140.			
	`v2-boundary-clock-twostep`	Version 2	Ja	bearbeiten
	`v2-transparent-clock`	Version 2	Ja	weiterleiten

Tab. 54: Auswahl der PTP-Version und des PTP-Modus´

Die PTP-Modi
- `v1-boundary-clock`
- `v2-boundary-clock-onestep`[1]
- `v2-boundary-clock-twostep`
- `v2-transparent-clock`

bieten Ihnen die Möglichkeit, die Genauigkeit der Zeitverteilung zu optimieren.

Hierzu dienen die Dialoge
- Version 1
- Version 2 (Boundary Clock, BC)
- Version 2 (Transparent Clock, TC)

Die PTP-Modi
- v1-simple-mode
- `v2-simple-mode`

bieten Ihnen die Plug-and-Play-Inbetriebnahme.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Funktion An/Aus	Die PTP-Funktion ein-/ausschalten	`An, Aus`	`Aus`

Tab. 55: Funktion IEEE 1588/PTP

Parameter	Bedeutung	Mögliche Werte	Lieferzustand

PTP-Version/Modus	Version und Modus der lokalen Uhr.	`v1-boundary-clock`
		`v1-simple-mode`
		`v2-boundary-clock-onestep`
		`v2-boundary-clock-twostep`
		`v2-transparent-clock`
		`v2-simple-mode`
			`v1-boundary-clock`

Tab. 56: Konfiguration IEEE 1588/PTP, PTP-Version und -Modus, Übersicht

1. Für die Geräte MS20, MS30 und PowerMICE mit den Modulen MM23 oder MM33, siehe die Abschnitte „Geräte ohne PTP-Hardware-Unterstützung” auf Seite 139 und „Geräte mit PTP-Hardware-Unterstützung” auf Seite 140.

Wert für PTP-Version und PTP-Modus	Bedeutung
`v1-boundary-clock`	Boundary-Clock-Funktion nach IEEE1588-2002 (PTPv1) Für die Geräte MS20, MS30 und PowerMICE mit Echtzeit-Modulen sowie für MACH 104 und MACH 1040, siehe die Abschnitte „Geräte ohne PTP-Hardware-Unterstützung” auf Seite 139 und „Geräte mit PTP-Hardware-Unterstützung” auf Seite 140.
`v1-simple-mode`	Unterstützung für PTPv1 ohne spezielle Hardware. Das Gerät synchronisiert sich auf empfangene PTPv1-Nachrichten. Dieser Modus bietet keine weiteren Funktionen wie z.B. PTP-Management oder Laufzeitmessung. Wählen Sie diesen Modus, wenn das Gerät ausschließlich Ports ohne Zeitstempeleinheit besitzt.
`v2-boundary-clock-onestep`	Boundary-Clock-Funktion nach IEEE 1588-2008 (PTPv2). Der One-Step-Modus übermittelt die präzise PTP-Zeit mit 1 Nachricht. Für die Geräte MS20, MS30 und PowerMICE mit den Modulen MM23 oder MM33, siehe die Abschnitte „Geräte ohne PTP-Hardware-Unterstützung” auf Seite 139 und „Geräte mit PTP-Hardware-Unterstützung” auf Seite 140.
`v2-boundary-clock-twostep`	Boundary-Clock-Funktion nach IEEE 1588-2008 (PTPv2). Der Two-Step-Modus übermittelt die präzise PTP-Zeit mit 2 Nachrichten.
`v2-transparent-clock`	Transparent-Clock-Funktion nach IEEE 1588-2008 (PTPv2). Die Geräte MS20, MS30 und PowerMICE mit den Modulen MM23 oder MM33 verwenden dabei ausschließlich den One-Step-Modus. Die Geräte MACH 104 und MACH 1040 verwenden dabei ausschließlich den Two-Step-Modus. Sie unterstützen eine Empfangsrate von max. 8 Frames/s.
`v2-simple-mode`	Unterstützung für PTPv2 ohne spezielle Hardware. Das Gerät synchronisiert sich auf empfangene PTPv2-Nachrichten. Dieser Modus bietet keine weiteren Funktionen wie z.B. PTP-Management oder Laufzeitmessung. Wählen Sie diesen Modus, wenn das Gerät ausschließlich Ports ohne Zeitstempeleinheit besitzt.

Tab. 57: Konfiguration IEEE 1588/PTP, PTP-Version und -Modus, Details

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Untere Synchronisationsschwelle [ns]	Untere PTP-Synchronisationsschwelle, Eingabe in Nanosekunden. Unterschreitet der Betrag von (Referenzzeit - Lokale Zeit) den Wert der unteren PTP-Synchronisationsschwelle, dann gilt die lokale Uhr als synchron mit der Referenzuhr.	0-999.999.999	30
Obere Synchronisationsschwelle [ns]	Obere PTP-Synchronisationsschwelle, Eingabe in Nanosekunden. Überschreitet der Betrag von (Referenzzeit - Lokale Zeit), den Wert der oberen PTP-Synchronisationsschwelle, dann gilt die lokale Uhr als nicht synchron mit der Referenzuhr.	31-1.000.000.000	5.000

Tab. 58: Konfiguration IEEE 1588/PTP, Synchronisationsschwellen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Ist synchronisiert	Lokale Uhr läuft synchron mit der Referenzuhr, vergleiche `Untere Synchronisationsschwelle` und `Obere Synchronisationsschwelle`.	`true, false`	-
Max Offset absolut [ns]	Betrag der maximalen Abweichung der lokalen Uhr zur Referenzuhr in Nanosekunden seit dem letzten Zurücksetzen der lokalen Uhr. Die lokale Uhr setzen Sie zurück durch „Reinitialisieren“ in diesem Dialog oder durch ein Zurücksetzen des Gerätes.		-

Tab. 59: IEEE 1588/PTP-Status

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 60: Schaltflächen

3.3.2 PTP Version 1 (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

Die Wahl, welche PTP-Version Sie einsetzen, treffen Sie im Dialog `Zeit:PTP:Global`.

PTP Version 1, Globale Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Sync-Intervall	Periode zum Versenden von Synchronisationsnachrichten. Eingabe in Sekunden. Um die Änderungen durchzuführen, klicken Sie „Reinitialisieren“.	- sec-1 - sec-2 - sec-8 - sec-16 - sec-64	sec-2
Subdomänen-Name	Name der PTP-Subdomäne, der die lokale Uhr angehört. Um die Änderungen durchzuführen, klicken Sie „Reinitialisieren“.	1 bis 16 ASCII Zeichen, Hex-Wert 0x21 (!) bis einschließlich 0x7e (~)	_DFLT
Bevorzugter Master	Lokale Uhr als bevorzugten Master definieren. Findet PTP keinen anderen bevorzugten Master, dann wird die lokale Uhr zur Grandmaster-Uhr. Findet PTP weitere bevorzugte Master, dann verhandelt PTP, welcher der bevorzugten Master zur Grandmaster-Uhr wird.	`true, false`	`false`

Tab. 61: Funktion IEEE 1588/PTPv1

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Offset zum Master [ns]	Betrag der Abweichung der lokalen Uhr zur Referenzuhr in Nanosekunden.		
Laufzeit zum Master [ns]	Einfache Signallaufzeit zwischen lokalem Gerät und Referenzuhr in Nanosekunden.		
Grandmaster UUID	MAC-Adresse der Grandmaster-Uhr (Unique Universal Identifier).		
Parent UUID	MAC-Adresse der Master-Uhr, mit der die lokale Zeit direkt synchronisiert wird.		

Tab. 62: Status IEEE 1588/PTPv1

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Clock Stratum	Qualifikation der lokalen Uhr.		
Uhren-Kennung	Eigenschaften der Uhr (z.B. Genauigkeit, Epoche, usw.).		

Tab. 62: Status IEEE 1588/PTPv1

Anmerkung: PTPv1 verwendet als Geräte-UUID 48 Bits, die identisch mit der MAC-Adresse des jeweiligen Geräts sind.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Reinitialisieren	Startet nach einer Änderung des Zeitintervalls die Synchronisation neu und übernimmt den Namen für die Sub-Domäne.
Hilfe	Öffnet die Online-Hilfe.

Tab. 63: Schaltflächen

PTP Version 1, Port-Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port	Port, für den dieser Eintrag gilt. Die Tabelle bleibt leer, wenn das Gerät den gewählten PTP-Modus nicht unterstützt		
PTP an	Port sendet/empfängt PTP-Synchronisationsnachrichten	`an`	`an`
	Port blockiert PTP-Synchronisationsnachrichten.	`aus`	

Tab. 64: Port-Dialog Version 1

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
PTP Burst an	an: Während eines Synchronisationsintervalls finden 2 bis 8 Synchronisationsabläufe statt. Dies ermöglicht eine schnellere Synchronisation bei entsprechend erhöhter Netzlast. aus: Während eines Synchronisationsintervalls findet ein Synchronisationsablauf statt.	an aus	aus
PTP Status	Port befindet sich in der Initialisierungsphase.	initializing	
	Port befindet sich im Faulty Modus. Fehler im PTP Protokoll.	faulty	
	PTP-Funktion an diesem Port ist ausgeschaltet.	disabled	
	Port hat bisher keine Informationen und wartet auf Synchronisationsnachrichten.	listening	
	Port ist im PTP-Pre-Master Modus.	pre-master	
	Port ist im PTP-Master-Modus.	master	
	Port ist im PTP-Passiv-Modus.	passiv	
	Port ist im PTP-Unkalibriert-Modus.	uncalibrated	
	Port ist im PTP-Slave-Modus.	slave	

Tab. 64: Port-Dialog Version 1

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 65: Schaltflächen

3.3.3 PTP-Version 2 (BC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

PTP-Version 2 bietet wesentlich mehr Einstellmöglichkeiten. Dies ermöglicht
- eine schnellere Rekonfiguration des PTP Netzes als bei PTP-Version 1
- in manchen Umgebungen auch eine höhere Präzision.

Die Wahl, welche PTP-Version Sie einsetzen, treffen Sie im Dialog `Zeit:PTP:Global`.

PTP-Version 2 (BC), Globale Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Priorität 1	Die Uhr mit der niedrigsten Priorität 1 wird zur Referenzuhr (Grandmaster).	0-255	128
Priorität 2	Sind alle relevanten Werte zur Auswahl der Referenzuhr bei mehreren Geräten gleich, wird die Uhr mit der niedrigsten Priorität 2 als Referenzuhr (Grandmaster) ausgewählt.	0-255	128
Domänen-nummer	Zuordnung der Uhr zu einer PTPv2 Domäne. Auschließlich Uhren der gleichen Domäne werden synchro-nisiert.	0-255	0

Tab. 66: Funktion IEEE 1588/PTPv2-BC

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Two-Step	Zeigt den Protokoll-Modus des Gerätes an.	`Aus` (Auswahl `v2-boundary-clock-onestep` im Dialog `PTP Global`) `An` (Auswahl `v2-boundary-clock-twostep` im Dialog `PTP Global`)	
Steps Removed	Anzahl der Boundary Clocks zwischen diesem Gerät und der PTP-Referenzuhr.		
Offset zum Master [ns]	Betrag der Abweichung der lokalen Uhr zur Referenzuhr in Nanosekunden.		
Laufzeit zum Master [ns]	Einfache Signallaufzeit (Ende-zu-Ende) zwischen dem lokalen Gerät und der Referenzuhr in Nanosekunden. Voraussetzung: Der Laufzeit-Mechanismus des Slave-Ports ist auf `E2E` eingestellt.		

Tab. 67: Status IEEE 1588/PTPv2-BC

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Uhren-Kennung	Eigene Geräte-UUID (eindeutige Identifikationsnummer)		
Parent-Portkennung	Port-UUID des direkten Masters		
Grandmaster-Kennung	Geräte-UUID der Referenzuhr		

Tab. 68: PTP-Uhren-Kennungen

Anmerkung: PTPv2 verwendet als Geräte-UUID 64 Bits, bestehend aus der MAC-Adresse des Gerätes, zwischen deren Bytes Nr. 3 und Nr. 4 die Werte ff und fe eingefügt sind.
Eine Port-UUID besteht aus der Geräte-UUID, gefolgt von einer 16 Bit-Port-ID.
Das Gerät zeigt UUIDs als Byte-Folge in Hexadezimalnotation an.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Priorität 1	Anzeige der Priorität 1 der aktuellen Referenzuhr.		
Priorität 2	Anzeige der Priorität 2 der aktuellen Referenzuhr.		
Klasse	Klasse der Referenzuhr		
Präzision	Geschätzte Genauigkeit bezüglich der UTC, die die Referenzuhr (der Grandmaster) angibt.		
Varianz	Varianz wie im IEEE 1588-2008 Standard beschrieben		

Tab. 69: Grandmaster (Referenzuhr)

Parameter	Bedeutung	Mögliche Werte	Lieferzustand

Zeitquelle	Wahl der Bezugsquelle der eigenen Uhr.	`atomicClock`
		`gps`
		`terrestrialRadio`
		`ptp`
		`ntp`
		`handset`
		`other`
		`internalOscil-lator`
			`internal-Oscillator`

UTC-Offset [s]	Aktuelle Differenz der PTP-Zeitskala (siehe unten) zur UTC.	`-32768 bis 32767`	`35` (seit 01.07.2012)
UTC-Offset gültig	Gibt an, ob der Wert von UTC Offset gültig ist oder nicht.	`ja` `nein`	`nein`
Time Traceable	Das Gerät bezieht die Zeit von einer Primären UTC-Referenz, z.B. von einem NTP-Server.	`ja` `nein`	
Frequency Traceable	Das Gerät bezieht die Frequenz von einer primären UTC-Referenz, z.B. NTP-Server, GPS.	`ja` `nein`	
PTP-Zeitskala	Das Gerät verwendet die PTP-Zeitskala. Die PTP-Zeitskala ist laut IEEE 1588 die Atomzeit TAI mit dem Startzeitpunkt 01.01.1970. Im Gegensatz zu UTC kennt TAI keine Schaltsekunden. Die Differenz zwischen TAI und UTC betrug am 01.01.2011 +34 Sekunden.	`ja` `nein`	

Tab. 70: Eigenschaften der lokalen Zeit

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 71: Schaltflächen

PTP Version 2 (BC), Port-Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port	Port, für den dieser Eintrag gilt. Wenn das Gerät den gewählten PTP-Modus nicht unterstützt, ist die Tabelle leer.		
PTP an	Port sendet/empfängt PTP-Synchronisationsnachrichten	an	an
	Port blockiert PTP-Synchronisationsnachrichten.	aus	
PTP Status	Port befindet sich in der Initialisierungsphase.	initializing	
	Port befindet sich im Faulty Modus. Fehler im PTP Protokoll.	faulty	
	PTP-Funktion an diesem Port ist ausgeschaltet.	disabled	
	Port hat bisher keine Informationen und wartet auf Synchronisationsnachrichten.	listening	
	Port ist im PTP-Pre-Master Modus.	pre-master	
	Port ist im PTP-Master-Modus.	master	
	Port ist im PTP-Unkalibriert-Modus.	uncalibrated	
	Port ist im PTP-Passiv-Modus.	passiv	
	Port ist im PTP-Slave-Modus.	slave	
Sync-Intervall [s]	Intervall der Synchronisationsnachrichten in Sekunden	0,5; 1; 2	1

Tab. 72: Port-Dialog Version 2(BC)

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Laufzeitmess-Mechanismus	Mechanismus zur Messung der Nachrichtenlaufzeit. Stellen Sie auf dem an diesem Port angeschlossenen PTP-Gerät den gleichen Mechanismus ein.		
	Ein PTP-Slave-Port misst die Laufzeit des gesamten Vermittlungspfades zum Master. Das Gerät zeigt den Messwert im Dialog `PTP:Version 2(BC):Global` an (siehe auf Seite 150 „PTP-Version 2 (BC), Globale Einstellungen“).	`E2E` (end-to-end):	
	Das Gerät misst die Laufzeit zu allen angeschlossenen PTP-Geräten. Wenn alle diese Geräte P2P unterstützen, erspart dieser Mechanismus im Fall einer Rekonfiguration das erneute Ermitteln der Laufzeit. Die Geräte MS20, MS30 und PowerMICE mit den Modulen MM23 oder MM33 sowie die Geräte MACH 104 und MACH 1040 unterstützen diesen Mechanismus.	`P2P` (peer-to-peer)	
	Keine Laufzeitermittlung.	`Disabled`	`Disabled`
P2P-Laufzeit	Gemessene P2P- (Peer-to-Peer-) Laufzeit. Voraussetzung: Sie haben den Laufzeitmess-Mechanismus P2P gewählt.		
P2P-Laufzeit-mess-Intervall	Intervall für Peer-to-Peer-Laufzeitmessungen an diesem Port. Voraussetzung: Sie haben den Laufzeitmess-Mechanismus P2P am Gerät selbst und am verbundenen PTP-Gerät gewählt.		
Netz-Protokoll	Transport-Protokoll für PTP-Nachrichten.	`802.3 Ethernet`, `UDP/IPv4`	`UDP/IPv4`
Announce-Intervall	Intervall der Nachrichten zur PTP Topologieerkennung (Auswahl der Referenzuhr). Wählen Sie innerhalb einer PTP-Domäne auf allen Geräten den gleichen Wert.	`1`, `2`, `4`, `8`, `16`	`2`

Tab. 72: Port-Dialog Version 2(BC)

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Announce-Timeout	Announce Intervall Timeout zur PTP Topologieerkennung in Anzahl von Announce Intervallen. Die Standardeinstellung von Announce Intervall = 2 (2 pro s) und Announce Timeout = 3 führen zu einem Timeout von 3 x 2 Sekunden = 6 Sekunden. Wählen Sie innerhalb einer PTP-Domäne auf allen Geräten den gleichen Wert.	2-10	3
E2E-Laufzeit-mess-Intervall	Zeigt das Intervall für die E2E- (End-to-End-) Laufzeitmessungen an diesem Port in Sekunden an. Dies ist eine Größe des Gerätes und wird an Ports mit PTP Status Slave vom verbundenen Master vorgegeben. Ist der Port selbst Master, dann weißt das Gerät dem Port den Wert 8 (Lieferzustand) zu.		8
V1-Hardware-Kompatibilität	Manche Geräte anderer Hersteller benötigen PTP Nachrichten bestimmter Länge. Bei gewähltem Netzprotokoll `UDP/IPv4` und aktiver Funktion verlängert das Gerät die PTP-Nachrichten.	`auto, on, off`	`auto`
Asymmetrie	Korrektur der Laufzeitasymmetrie in ns. Ein durch asymmetrische Übertragungswege verfälschter Laufzeitmesswert von x ns entspricht einer Asymmetrie von x·2 ns		

Tab. 72: Port-Dialog Version 2(BC)

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
VLAN	Die VLAN-ID, mit der das Gerät PTP-Frames an diesem Port sendet. **Anmerkung:** ▶ Beachten Sie dabei auch die VLAN-Einstellungen des Ports (siehe auf Seite 195 „VLAN Statisch“), besonders, ob das VLAN existiert und ob der Port getaggtes oder ungetaggtes Mitglied in dem VLAN ist. ▶ `none`: das Gerät sendet PTP-Frames stets ohne VLAN-Tag, auch wenn der Port getaggtes Mitglied des VLANs ist. ▶ VLANs, die Sie im Gerät bereits eingerichtet haben, können Sie mit Hilfe der Drop-down-Liste der Tabellenzelle auswählen.	`none`, `0 - 4042`	`none`
VLAN-Priorität	Die VLAN-Priorität (Layer 2, IEEE 802.1p), mit der das Gerät getaggte PTP-Frames an diesem Port sendet. Haben Sie die VLAN-ID auf `none` gestellt, ignoriert das Gerät die VLAN-Priorität.	`0 - 7`	`4`

Tab. 72: Port-Dialog Version 2(BC)

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 73: Schaltflächen

3.3.4 PTP Version 2 (TC) (MS20/MS30, PowerMICE, MACH 104, MACH 1040)

Besonders in stark kaskadierten Netzen erreicht die in PTP Version 2 eingeführte Transparent Clock (TC) eine merklich höhere Präzision.
Die Kombination mit dem P2P-Laufzeitmess-Mechanismus (gleichzeitige Laufzeitmessung an allen Ports) ermöglicht eine "nahtlose" Rekonfiguration.

Für die Geräte MS20, MS30 und PowerMICE mit den Modulen MM23 oder MM33:
Folgende Einstellungen ermöglichen Ihnen, die TC auch für Unicast-PTP-Nachrichten zu verwenden:
– Wahl des E2E-Mechanismus
– Syntonize ausgeschaltet
– PTP-Management ausgeschaltet.

Die Wahl, welche PTP-Version Sie einsetzen, treffen Sie im Dialog `Zeit:PTP:Global`.

PTP Version 2 (TC), Globale Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand

Profil	Definiert relevante PTP-Parameter für ein bestimmtes Profil.	`E2E-Vorgaben`
		`P2P-Vorgaben`
		`Power-Vorgaben`	

Tab. 74: PTP Version 2(TC) Profil-Voreinstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Laufzeitmess-Mechanismus	Mechanismus zur Messung der Nachrichtenlaufzeit. Stellen Sie auf dem an diesem Port angeschlossenen PTP-Gerät den gleichen Mechanismus ein.		
	Ein PTP-Slave-Port misst die Laufzeit des gesamten Vermittlungspfades zum Master. Das Gerät zeigt den Messwert im Dialog `PTP:Version 2(BC):Global` an (siehe auf Seite 150 „PTP-Version 2 (BC), Globale Einstellungen“).	`E2E` (end-to-end):	
	Das Gerät misst selbst die Laufzeit zu allen angeschlossenen PTP Geräten. Im Falle einer Rekonfiguration erspart dies das erneute Ermitteln der Laufzeit.	`P2P` (peer-to-peer)	
	Für die Geräte MACH 104 und MACH 1040: Wie E2E, mit folgenden Besonderheiten: ▶ Das Gerät vermittelt Delay-Anfragen der PTP-Slaves nur an den PTP-Master, obwohl diese Anfragen Multicast-Frames sind. So entlastet das Gerät die anderen Clients von unnötigen Multicast-Anfragen. ▶ bei Änderungen der PTP-Master-Slave-Topologie lernt das Gerät den Port zum PTP-Master um, sobald es einen Frame von einem anderen PTP-Master empfangen hat. ▶ Kennt das Gerät keinen PTP-Master, flutet es empfangene Delay-Anfragen auch im `E2E-Optimized`-Modus.	`E2E-Optimized` (end-to-end, optimiert)	
	Für die Geräte MACH 104 und MACH 1040: Das Gerät lässt keine Laufzeitmessung zu, d.h., es verwirft empfangene Frames, die zur Laufzeitmessung dienen.	`Disabled`	
Primäre Domäne	Zuordnung der Uhr zu einer PTPv2 Domäne.	0-225	0

Tab. 75: Funktion IEEE 1588 / PTPv2 TC

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Netz-Protokoll	Netzprotokoll für P2P- und Management-Nachrichten.	`UDP/IPv4`, `IEEE 802.3`	`UDP/IPv4`
Syntonize	Frequenz synchronisieren.	`An` `Aus`	Für die Geräte MS20, MS30 und PowerMICE: `Aus` Für die Geräte MACH 104 und MACH 1040: `An`
Lokale Zeit synchronisieren	Das Gerät synchronisiert seine lokale Systemzeit mit der per PTP empfangenen Uhrzeit. Voraussetzung: die Einstellung Syntonize ist eingeschaltet.	`An` `Aus`	`Aus`
PTP-Management	Aktivieren/Deaktivieren des PTP-Managements. Zur Entlastung des Gerätes schalten Sie das PTP-Management und Syntonize aus - bei hohen Synchronisationsraten und - im Unicast-Betrieb.	`An` `Aus`	`Aus`
Multi Domain Mode	`An`: TC korrigiert Nachrichten aller Domänen. `Aus`: TC korrigiert ausschließlich Nachrichten der primären Domäne.	`An` `Aus`	`Aus`
Power-TLV-Check	Aktiviere/Deaktiviere Power-TLV-Check `An`: Das Gerät ignoriert Hinweisnachrichten ohne das Power-Profile-TLV.	`An` `Aus`	`Aus`

Tab. 75: Funktion IEEE 1588 / PTPv2 TC

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
VLAN	Die VLAN-ID, mit der das Gerät eigene Frames (wie PTP-Management-Frames oder P2P-Frames) an diesem Port sendet. **Anmerkung:** ▶ Beachten Sie dabei auch die VLAN-Einstellungen des Ports (siehe auf Seite 195 „VLAN Statisch“), besonders, ob das VLAN existiert und ob der Port getaggtes oder ungetaggtes Mitglied in dem VLAN ist. ▶ `none`: das Gerät sendet PTP-Frames stets ohne VLAN-Tag, auch wenn der Port getaggtes Mitglied des VLANs ist. ▶ VLANs, die Sie im Gerät bereits eingerichtet haben, können Sie mit Hilfe der Drop-down-Liste der Tabellenzelle auswählen.	`none`, `0 - 4042`	`none`
VLAN-Priorität	Die VLAN-Priorität (Layer 2, IEEE 802.1p), mit der das Gerät getaggte PTP-Frames sendet. Haben Sie die VLAN-ID auf `none` gestellt, ignoriert das Gerät die VLAN-Priorität.	`0 - 7`	`4`

Tab. 75: Funktion IEEE 1588 / PTPv2 TC

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Uhren-Kennung	Geräte-UUID der TC (Transparent Clock)		
Aktueller Master	Zeigt bei eingeschalteter Syntonize-Funktion die Port-UUID des Masters an, auf den das Gerät seine Frequenz synchronisiert. Ein Wert aus Nullen bedeutet, dass: ▶ die Funktion Syntonize abgeschaltet ist oder ▶ das Gerät keinen Master gefunden hat		

Tab. 76: Status IEEE 1588 / PTPv2 TC

Anmerkung: PTPv2 verwendet als Geräte-UUID 64 Bits, bestehend aus der MAC-Adresse des Gerätes, zwischen deren Bytes Nr. 3 und Nr. 4 die Werte ff und fe eingefügt sind.
Eine Port-UUID besteht aus der Geräte-UUID, gefolgt von einer 16 Bit-Port-ID.
Das Gerät zeigt UUIDs als Byte-Folge in Hexadezimalnotation an.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 77: Schaltflächen

PTP Version 2 (TC), Port-Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Modul	Modulnummer bei modularen Geräten, sonst 1.		
Port	Port, für den dieser Eintrag gilt. Wenn das Gerät den gewählten PTP-Modus nicht unterstützt, ist die Tabelle leer.		
PTP an	Port sendet/empfängt PTP-Synchronisationsnachrichten	`an`	`an`
	Port blockiert PTP-Synchronisationsnachrichten. Das Gerät bearbeitet keine PTP-Nachrichten, die es an diesem Port empfängt.	`aus`	

Tab. 78: Port-Dialog Version 2(TC)

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
P2P-Laufzeit-mess-Intervall	Intervall für Peer-to-Peer-Laufzeit-messungen an diesem Port. Voraussetzung: Sie haben den Laufzeitmess-Mechanismus P2P am Gerät selbst und am verbundenen PTP-Gerät gewählt.		
P2P-Laufzeit	Gemessene P2P- (Peer-to-Peer-) Laufzeit. Voraussetzung: Sie haben den Laufzeitmess-Mechanismus P2P gewählt.		
Asymmetrie	Korrektur der Laufzeitasymmetrie in ns. Ein durch asymmetrische Übertragungswege verfälschter Laufzeitmesswert von x ns entspricht einer Asymmetrie von x·2 ns		

Tab. 78: Port-Dialog Version 2(TC)

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 79: Schaltflächen

4 Switching

Das Switching-Menü enthält die Dialoge, Anzeigen und Tabellen zur Konfiguration der Switching-Einstellungen:

- Switching Global
- Filter für MAC-Adressen
- Lastbegrenzer
- Multicasts
- VLAN

4.1 Switching Global

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
MAC-Adresse (read-only)	Anzeige der MAC-Adresse des Gerätes		
Aging-Time (s)	Eingabe der Aging Time für dynamische MAC-Adress-Einträge in Sekunden. Im Zusammenhang mit der Router-Redundanz wählen Sie eine Zeit ≥ 30 s.	10-630	30
Flusskontrolle aktivieren	Ein-/Ausschalten der Flusskontrolle	`An`, `Aus`	`Aus`

Tab. 80: Switching:Global-Dialog

Anmerkung: Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Geräte-Ports. Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Adressen lernen	Ein-/Ausschalten des Lernens von MAC-Quell-Adressen. **Anmerkung:** Ist Routing aktiv, verhindert das Gerät das Abschalten des Adressen-Lernens. Wenn Sie Routing einschalten, aktiviert das Gerät automatisch das Adressen-Lernen.	`An`, `Aus`	`An`
Paketgröße	Einstellen der maximalen Paketgröße (Frame Size) in Bytes. Wählen Sie den größeren Wert, wenn das Gerät Pakete mit Double VLAN Tagging vermitteln soll. Damit können Sie z.B. das Gerät in Netzen mit MPLS-Switches/Routern betreiben.	MACH 104, MACH 1040: 1522, 1552, 9022 PowerMICE, MACH 4000: 1.522, 1.552	1.522
Address-Relearn-Detection aktivieren	Ein-/Ausschalten, ob das Gerät erkennt, wenn es wiederholt die selben MAC-Quell-Adressen an unterschiedlichen Ports gelernt hat. Dieser Vorgang weist mit großer Wahrscheinlichkeit auf eine Loop- (Schleifen-) Situation im Netz hin. Erkennt das Gerät diesen Vorgang, erzeugt es einen Eintrag in der Log-Datei und sendet einen Alarm (Trap).	`An`, `Aus`	`Aus`

Tab. 81: Switching:Global-Dialog

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Address-Relearn-Threshold	Anzahl der gelernten MAC-Adressen an unterschiedlichen Ports innerhalb eines Prüfintervalls. Erreicht die Anzahl der gelernten Adressen diesen Schwellenwert, betrachtet das Gerät dies als ein relevantes Ereignis. Das Intervall für diese Prüfung beträgt wenige Sekunden.	1 - 1.024	1
Duplex-Mismatch-Detection aktivieren	Ein-/Ausschalten, ob das Gerät bei spezifischen Fehlerereignissen an einem Port ein Duplex-Problem meldet. Dies bedeutet, dass der Duplex-Modus des Port möglicherweise nicht mit dem des entfernten Ports übereinstimmt. Entdeckt das Gerät eine mögliche Nichtübereinstimmung, erzeugt es einen Eintrag im Ereignis-Log und sendet einen Alarm (Trap). Um mögliche Nichtübereinstimmungen zu erkennen, wertet das Gerät die Fehlerzähler des Ports nach Verbindungsaufbau in Abhängigkeit von den Port-Einstellungen aus (siehe Tabelle 82).	`An`, `Aus`	`An`

Tab. 81: Switching:Global-Dialog

Die folgende Tabelle nennt die Duplex-Betriebsarten für TX-Ports zusammen mit den möglichen Fehlerereignissen. Die Begriffe in der Tabelle bedeuten:

- Kollisionen: Diese bedeuten im Halbduplexmodus Normalbetrieb.
- Duplex-Problem: Nicht übereinstimmende Duplex-Modi.
- EMI: Elektromagnetische Interferenz.
- Netzausdehnung: Die Netzausdehnung ist zu groß bzw. sind zu viele Kaskadenhubs vorhanden.

- Kollisionen, Spätkollisionen: Im Vollduplex-Modus keine Erhöhung der Port-Zähler für Kollisionen oder Spätkollisionen.
- CRC-Fehler: Das Gerät bewertet diese Fehler als nicht übereinstimmende Duplex-Modi im manuellen Vollduplex-Modus.

Nr.	Automatische Konfiguration	Aktueller Duplex-Modus	Erkannte Fehlerereignisse (≥ 10 nach Link-Up)	Duplex-Modi	Mögliche Ursachen
1	An	Halbduplex	Keine	OK	
2	An	Halbduplex	Kollisionen	OK	
3	An	Halbduplex	Späte Kollisionen (Late Collisions)	Duplex-Problem erkannt	Duplex-Problem, EMI, Netzausdehnung
4	An	Halbduplex	CRC-Fehler	OK	EMI
5	An	Vollduplex	Keine	OK	
6	An	Vollduplex	Kollisionen	OK	EMI
7	An	Vollduplex	Late Collisions	OK	EMI
8	An	Vollduplex	CRC-Fehler	OK	EMI
9	Aus	Halbduplex	Keine	OK	
10	Aus	Halbduplex	Kollisionen	OK	
11	Aus	Halbduplex	Late Collisions	Duplex-Problem erkannt	Duplex-Problem, EMI, Netzausdehnung
12	Aus	Halbduplex	CRC-Fehler	OK	EMI
13	Aus	Vollduplex	Keine	OK	
14	Aus	Vollduplex	Kollisionen	OK	EMI
15	Aus	Vollduplex	Late Collisions	OK	EMI
16	Aus	Vollduplex	CRC-Fehler	Duplex-Problem erkannt	Duplex-Problem, EMI

Tab. 82: Bewertung des nicht übereinstimmenden Duplex-Modus

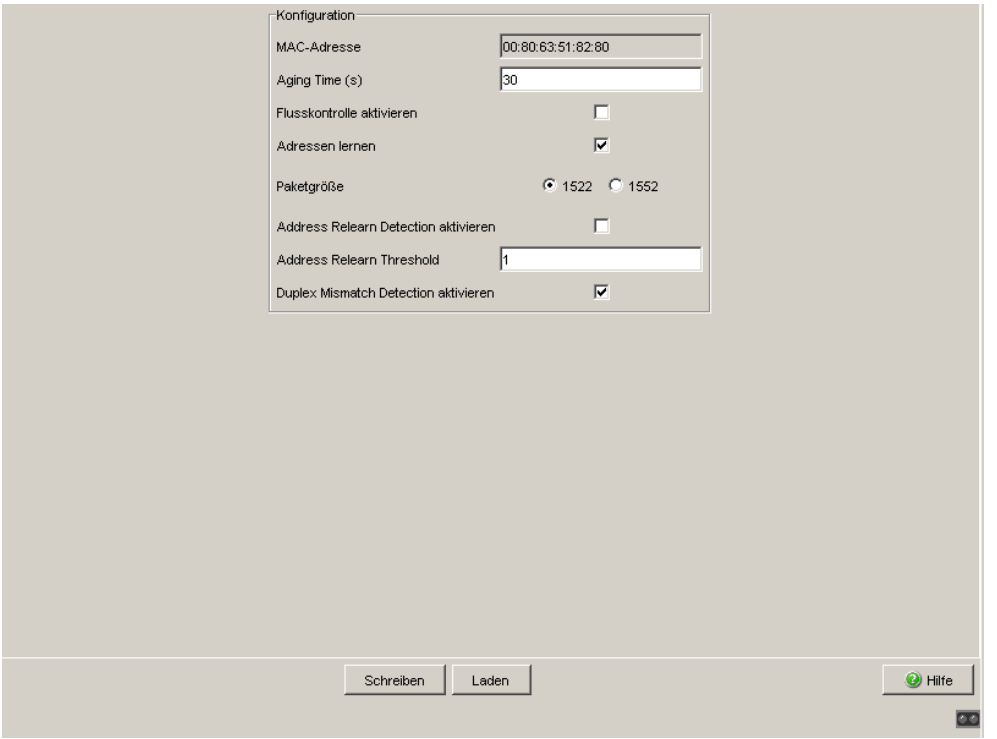


Abb. 44: Dialog Switching Global

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 83: Schaltflächen

4.2 Filter für MAC-Adressen

Die Filtertabelle für MAC-Adressen dient zur Anzeige und Bearbeitung von Filtern. Jede Zeile stellt einen Filter dar. Filter legen die Vermittlungsweise von Datenpaketen fest. Sie werden entweder automatisch vom Gerät (Status learned) oder manuell angelegt. Datenpakete deren Zieladresse in der Tabelle eingetragen ist, werden vom Empfangsport an die in der Tabelle markierten Ports vermittelt. Datenpakete, deren Zieladresse nicht in der Tabelle enthalten ist, werden vom Empfangsport an alle anderen Ports vermittelt. Folgende Zustände sind möglich:

- `learned`: Das Filter wurde vom Gerät automatisch angelegt.
- `invalid`: Mit diesem Status löschen Sie ein manuell angelegtes Filter.
- `permanent`: Das Filter wird im Gerät oder auf dem URL dauerhaft gespeichert (siehe auf Seite 52 „Laden/Speichern“).
- `gmrp`: Das Filter wurde durch GMRP angelegt.
- `gmrp/permanent`: GMRP hat dem Filter, nachdem es durch den Administrator angelegt worden ist, weitere Portmarken hinzugefügt. Die durch das GMRP hinzugefügten Portmarken werden bei einem Neustart gelöscht.
- `igmp`: Das Filter wurde durch IGMP-Snooping angelegt.

Der Dialog „Anlegen“ (siehe Bedientaste unten) bietet Ihnen die Möglichkeit, neue Filter zu erzeugen.

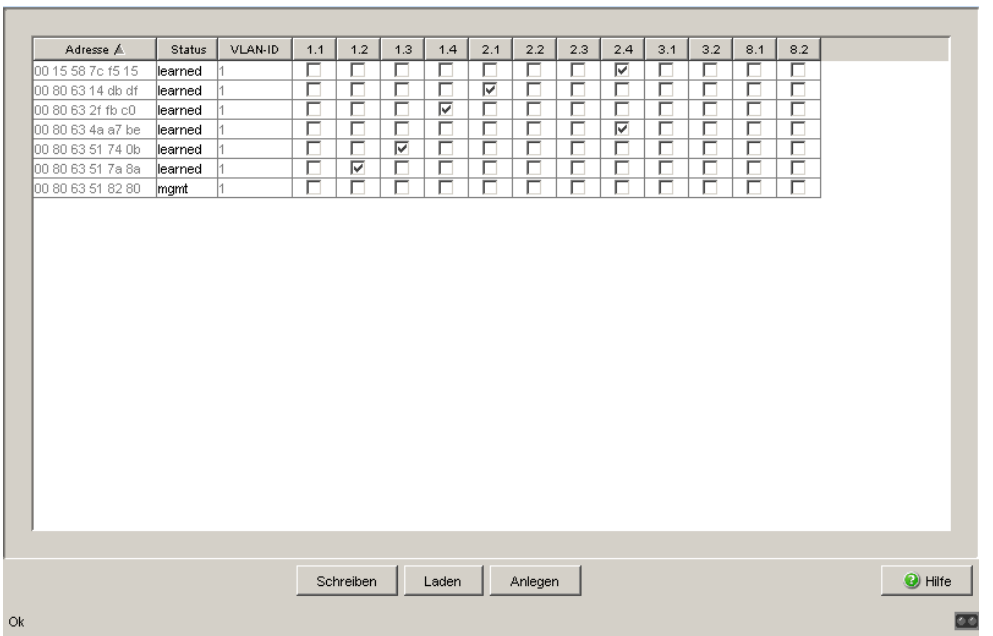


Abb. 45: Dialog Filtertabelle

Anmerkung: Das Gerät bietet Ihnen für Unicast-Adressen die Möglichkeit, mehrere Ports in einen Filter-Eintrag aufzunehmen. Nehmen Sie keinen Port auf, wenn Sie einen Discard-Filter-Eintrag erstellen möchten.

Anmerkung: Die Geräte PowerMICE, MACH 1040 und MACH 4000 bieten Ihnen für Unicast-Adressen die Möglichkeit, mehrere Ports in einen Filter-Eintrag aufzunehmen. Nehmen Sie keinen Port auf, wenn Sie einen Discard-Filter-Eintrag erstellen möchten.

Anmerkung: Die Filtertabelle bietet Ihnen für Multicast-Adressen die Möglichkeit, bis zu 100 Filter-Einträge zu erzeugen.

Erzeugen

Um einen Filter manuell einzurichten, klicken Sie auf die Schaltfläche „Erzeugen“.

Parameter	Bedeutung
VLAN-ID	Legt die ID des VLANs fest, für das der Tabelleneintrag gilt. Mögliche Werte: ▶ alle eingerichteten VLAN-IDs
Adresse	Legt die Ziel-MAC-Adresse fest, für die der Tabelleneintrag gilt. Mögliche Werte: ▶ gültige MAC-Adresse Geben Sie den Wert in einem der folgenden Formate ein: – ohne Trennzeichen, z. B. `001122334455` – Trennung mit Leerzeichen, z. B. `00 11 22 33 44 55` – Trennung mit Doppelpunkt, z. B. `00:11:22:33:44:55` – Trennung mit Bindestrich, z. B. `00-11-22-33-44-55` – Trennung mit Punkt, z. B. `00.11.22.33.44.55` – Trennung mit Punkt nach jeder 4.Stelle , z. B. `0011.2233.4455`
Mögliche Ports	Legt die Geräte-Ports fest, an die das Gerät Datenpakete mit der Ziel-MAC-Adresse vermittelt: ☐ Wählen Sie einen Port aus, wenn die Ziel-MAC-Adresse eine Unicast-Adresse ist. ☐ Wählen Sie einen oder mehrere Ports aus, wenn die Ziel-MAC-Adresse eine Multicast-Adresse ist. ☐ Wählen Sie keinen Port aus, um einen Discard-Filter einzurichten. Das Gerät verwirft Datenpakete mit der im Tabelleneintrag angegebenen Ziel-MAC-Adresse.

Tab. 84: Fenster „Erzeugen“

Eintrag bearbeiten

Um die Einstellungen eines Tabelleneintrags manuell anzupassen, klicken Sie auf die Schaltfläche „Eintrag bearbeiten“.

Parameter	Bedeutung
Mögliche Ports	Diese Spalte enthält die verfügbaren Geräte-Ports.
Zugewiesene Ports	Diese Spalte enthält die Geräte-Ports, die dem Tabelleneintrag zugewiesen sind. ☐ Wählen Sie einen Port aus, wenn die Ziel-MAC-Adresse eine Unicast-Adresse ist. ☐ Wählen Sie einen oder mehrere Ports aus, wenn die Ziel-MAC-Adresse eine Multicast-Adresse ist. ☐ Wählen Sie keinen Port aus, um einen Discard-Filter einzurichten. Das Gerät verwirft Datenpakete mit der im Tabelleneintrag angegebenen Ziel-MAC-Adresse.

Tab. 85: Fenster „Eintrag bearbeiten“ im Dialog `Switching:Filter für MAC-Adressen`

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Eintrag bearbeiten	Öffnet das Fenster „Eintrag bearbeiten“.
Hilfe	Öffnet die Online-Hilfe.
>	Verschiebt den markierten Eintrag in die rechte Spalte.
>>	Verschiebt alle Einträge in die rechte Spalte.
<	Verschiebt den markierten Eintrag in die linke Spalte.
<<	Verschiebt alle Einträge in die linke Spalte.

Tab. 86: Schaltflächen

4.3 Lastbegrenzer

Um bei hohem Verkehrsaufkommen einen zuverlässigen Betrieb zu gewährleisten, bieten Ihnen das Gerät die Möglichkeit, die Rate des Verkehrs an den Ports zu begrenzen.

Die Eingabe einer Begrenzungsrate je Port legt fest, welchen maximalen Verkehr das Gerät ausgangs- und eingangsseitig vermittelt.

Überschreitet der Verkehr an diesem Port die eingegebene maximale Rate, dann verwirft das Gerät die Überlast an diesem Port.

Eine globale Einstellung aktiviert/deaktiviert die Lastbegrenzer-Funktion an allen Ports.

Anmerkung: Die Begrenzerfunktionen arbeiten ausschließlich auf Layer 2 und dienen dem Zweck, Stürme von Frame-Typen, die der Switch flutet (typischerweise Broadcasts), in ihrer Auswirkung zu begrenzen. Die Begrenzerfunktion übergeht dabei Protokollinformationen höherer Schichten wie IP oder TCP. Dies kann sich z.B. auf TCP-Verkehr auswirken.

Um diese Auswirkungen zu minimieren, nutzen Sie die folgenden Möglichkeiten:

- die Begrenzungsfunktion auf bestimmte Frame-Typen einschränken (z.B. auf Broadcasts, Multicasts und Unicasts mit nicht gelernter Zieladresse) und Unicasts mit bekannter Zieladresse von der Begrenzung ausnehmen,
- die Ausgangsbegrenzerfunktion statt der Eingangsbegrenzerfunktion verwenden, da die erstere durch die Switch-interne Pufferung der Frames etwas besser mit der TCP-Flusssteuerung zusammenarbeitet.
- die Aging-Zeit für gelernte Unicast-Adressen erhöhen.

Anmerkung: Ports, die in eine Link-Aggregation (siehe auf Seite 254 „Link-Aggregation“) eingebunden sind, sind von der Lastbegrenzung ausgenommen, unabhängig von den Einträgen im Dialog „Lastbegrenzer“.

4.3.1 Lastbegrenzer-Einstellungen (PowerMICE und MACH 4000)

- „Eingangsbegrenzer (kbit/s)“ bietet Ihnen die Möglichkeit, die Eingangsbegrenzerfunktion für alle Ports ein-/auszuschalten und die Eingangsbegrenzung für Broadcast-Pakete oder für Broadcast- und Multicast-Pakete an allen Ports zu wählen.
- „Ausgangsbegrenzer (Pkt/s)“ bietet Ihnen die Möglichkeit, die Ausgangs-Broadcastbegrenzung an allen Ports ein/auszuschalten.

Einstellmöglichkeiten pro Port:

- Eingangsbegrenzerrate für den im Eingangsbegrenzerrahmen gewählten Pakettyp:
  - = 0, keine Begrenzung eingangsseitig an diesem Port.
  - > 0, maximale Übertragungsrate in kbit/s, die eingangsseitig an diesem Port empfangen werden darf.
- Ausgangsbegrenzerrate für Broadcast-Pakete:
  - = 0, keine Begrenzung der Broadcasts ausgangsseitig an diesem Port.
  - > 0, maximale Anzahl der Broadcasts, die pro Sekunde ausgangsseitig an diesem Port gesendet werden.

Anmerkung: Gegebenenfalls rundet das Gerät die eingegebenen Werte auf den nächstliegenden Wert, den die Hardware verarbeiten kann. Um nach Eingabe der Werte zu sehen, welche Werte das Gerät tatsächlich verwendet, klicken Sie „Schreiben“ und anschließend „Laden“.

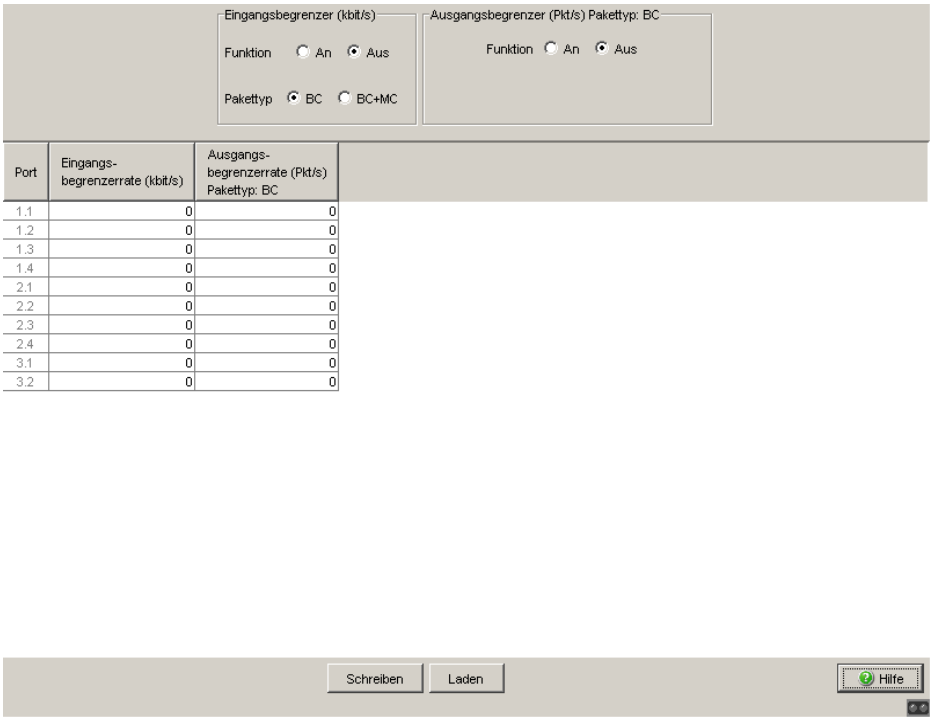


Abb. 46: Dialog Lastbegrenzer

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 87: Schaltflächen

4.4 Multicasts

4.4.1 IGMP (Internet Group Management Protocol)

Dieser Dialog bietet Ihnen die Möglichkeit,
- die IGMP-Funktion global ein- oder auszuschalten,
- das IGMP global und pro Port zu konfigurieren.

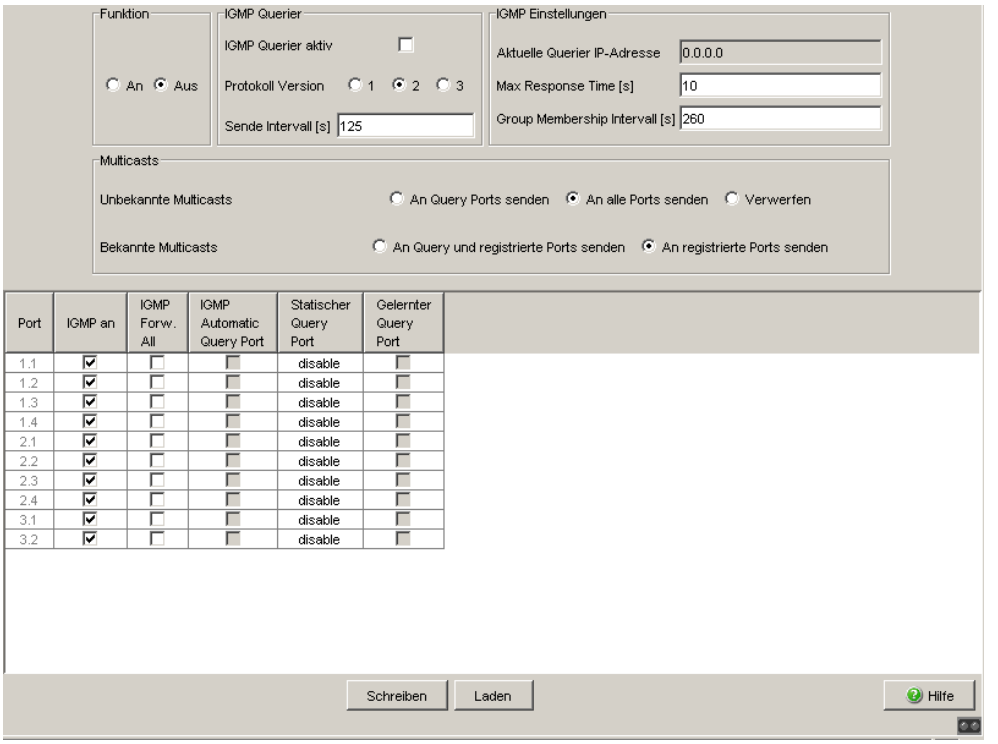


Abb. 47: Dialog IGMP-Snooping

Funktion

Dieser Rahmen bietet Ihnen die Möglichkeit,

- das IGMP-Snooping-Protokoll ein- oder auszuschalten.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Funktion	IGMP-Snooping für das Gerät global ein-/ausschalten. Ist IGMP-Snooping ausgeschaltet, dann: ▶ wertet das Gerät empfangene Query- und Report-Pakete nicht aus und ▶ sendet (flutet) empfangene Datenpakete mit einer Multicast-Adresse als Zieladresse an allen Ports.	`An` `Aus`	`Aus`

Tab. 88: IGMP-Snooping, globale Funktion

IGMP-Querier- und IGMP-Einstellungen

Diese Rahmen bieten Ihnen die Möglichkeit, globale Einstellungen für die IGMP- und die IGMP-Querier-Funktion vorzunehmen.
Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
IGMP-Querier			
IGMP-Querier aktiv	Query-Funktion ein-/ausschalten	ein aus	aus
Protokoll-Version	Die IGMP-Version 1, 2 oder 3 auswählen.	1, 2, 3	2
Sende-Intervall	Zeitabstand eingeben, in welchem der Switch Query-Pakete verschickt. Alle IGMP-fähigen Endgeräte antworten auf eine Query mit einer Report-Nachricht.	2-3.599 s[a]	125 s
IGMP- Einstellungen			
Aktuelle Querier-IP-Adresse	Anzeige der IP-Adresse des Routers /Switches, der die Query-Funktion innehat.		

Tab. 89: IGMP-Querier- und IGMP-Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Max. Response Time	Zeit eingeben, innerhalb derer die Multicast-Gruppen-Mitglieder auf ein Query antworten sollen. Die Multicast-Gruppen-Mitglieder wählen einen zufälligen Wert innerhalb der Response Time für ihre Antwort aus, um zu verhindern, dass alle Multicast-Gruppen-Mitglieder gleichzeitig auf den Query antworten.	Protokoll Version - 1, 2: 1-25 s - 3: 1-3.598 s[a]	10 s
Group Membership Intervall	Zeit eingeben, für die eine dynamische Multicastgruppe im Gerät eingetragen bleibt, wenn es keine Report-Nachrichten empfängt.	3-3.600 s[a]	260 s

Tab. 89: IGMP-Querier- und IGMP-Einstellungen

a. Beachten Sie den Parameter-Zusammenhang zwischen Max.-Response-Time, Sende-Intervall und Group-Membership-Intervall (siehe Tabelle 90.)

Die Parameter
– Max. Response-Time,
– Sende-Intervall und
– Group-Membership-Intervall
stehen in Beziehung zueinander:

Max. Response-Time < Sende-Intervall < Group-Membership-Intervall.

Wenn Sie Werte eingeben, die dieser Beziehung widersprechen, dann ersetzt das Gerät diese Werte durch eine Voreinstellung oder die zuletzt gültigen Werte.

Parameter	Protokoll-Version	Mögliche Werte	Lieferzustand
Max. Response-Time	1, 2 3	1-25 Sekunden 1-3.598 Sekunden	10 Sekunden
Sende-Intervall	1, 2, 3	2-3.599 Sekunden	125 Sekunden
Group-Membership-Intervall	1, 2, 3	3-3.600 Sekunden	260 Sekunden

Tab. 90: Wertebereich für Max. Response-Time, Sende-Intervall und Group-Membership-Intervall

Wählen Sie für "Sende-Intervall" und "Max. Response-Time"
– einen großen Wert, wenn Sie Ihr Netz entlasten wollen und die sich daraus ergebenden längeren Umschaltzeiten akzeptieren können,
– einen kleinen Wert, wenn Sie kurze Umschaltzeiten benötigen und die sich daraus ergebende Netzlast akzeptieren können.

Multicasts

In diesem Rahmen bestimmen Sie, wie das Gerät Pakete mit

- unbekannten -nicht mit IGMP-Snooping gelernten- MAC-/IP-Multicast-Adressen
- bekannten -mit IGMP-Snooping gelernten- MAC-/IP-Multicast-Adressen

vermittelt.

Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Unbekannte Multicasts	▶ An Query-Ports senden: Das Gerät sendet die Pakete mit unbekannter MAC/IP-Multicast-Adresse an alle Query-Ports. ▶ An alle Ports senden: Das Gerät sendet die Pakete mit unbekannter MAC/IP-Multicast-Adresse an alle Ports. ▶ Verwerfen: Das Gerät verwirft alle Pakete mit unbekannter MAC/IP-Multicast-Adresse.	An Query-Ports senden, An alle Ports senden, Verwerfen	An alle Ports senden
Bekannte Multicasts	▶ An Query- und registrierte Ports senden: Das Gerät sendet die Pakete mit bekannter MAC/IP-Multicast-Adresse an alle Query-Ports und an registrierte Ports. Diese Einstellung hat den Vorteil, dass sie in vielen Anwendungen ohne weitere Konfiguration funktioniert. Anwendung: „Flood and Prune”-Routing bei PIM-DM. ▶ An registrierte Ports senden: Das Gerät sendet die Pakete mit bekannter MAC/IP-Multicast-Adresse an registrierte Ports. Diese Einstellung hat den Vorteil, die verfügbare Bandbreite durch gezielte Vermittlung optimal zu nutzen. Sie erfordert zusätzliche Porteinstellungen. Anwendung: Routing-Protokoll PIM-SM.	An Query- und registrierte Ports senden, An registrierte Ports senden	An registrierte Ports senden

Tab. 91: Bekannte und unbekannte Multicasts

Anmerkung: Die Behandlung von ungelernten Multicast-Adressen gilt auch
für die reservierten Adressen aus dem „Local Network Control Block" (224.0.0.0 - 224.0.0.255). Dies kann z.B. Auswirkungen auf übergeordnete Routing-Protokolle haben.

Einstellungen pro Port (Tabelle)

Diese Konfigurationstabelle bietet Ihnen die Möglichkeit, portbezogene IGMP-Einstellungen vorzunehmen.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port	Modul- und Port-Nummer, für die dieser Eintrag gilt.	-	-
IGMP an	IGMP je Port ein-/ausschalten. Das Ausschalten von IGMP an einem Port verhindert Registrierungen für diesen Port. Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.	`An` `Aus`	`An`
IGMP Forward all	Die IGMP-Snooping-Funktion `Forward All` ein-/ausschalten. Mit der Einstellung `IGMP Forward All` vermittelt das Gerät an diesem Port alle Datenpakete mit einer Multicast-Adresse im Zieladressfeld. Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet. **Anmerkung:** Sind mehrere Router an ein Subnetz angeschlossen, dann verwenden Sie IGMP-Version 1, damit alle Router alle IGMP-Reports erhalten. **Anmerkung:** Wenn Sie IGMP-Version 1 in einem Subnetz verwenden, dann verwenden Sie IGMP-Version 1 auch im gesamten Netz.	`An` `Aus`	`Aus`
IGMP Automatic Query Port	Anzeige, welche Ports das Gerät als Query-Ports gelernt hat, wenn in „Statischer Query Port“ `automatic` gewählt ist. Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.	`ja`, `nein`	-

Tab. 92: IGMP-Einstellungen pro Port

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Statischer Query-Port	IGMP-Report-Nachrichten vermittelt das Gerät an die Ports, an denen es IGMP-Anfragen empfängt (Lieferzustand). Diese Tabellenspalte bietet Ihnen die Möglichkeit, IGMP-Report-Nachrichten auch an: anderen ausgewählten Ports (enable) oder angeschlossene Hirschmann-Geräte (automatic) zu vermitteln . Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.	`enable`, `disable`, `automatic`	`disable`
Gelernter Query-Port	Anzeige, an welchen Ports das Gerät IGMP-Anfragen empfangen hat, wenn in „Statischer Query Port“ „disable“ gewählt ist. Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.	`ja` `nein`	-

Tab. 92: IGMP-Einstellungen pro Port

Anmerkung: Ist das Gerät in einen HIPER-Ring eingebunden, dann erreichen Sie für Datenpakete mit registrierten Multicast-Zieladressen eine schnelle Rekonfiguration des Netzes nach einer Ringumschaltung durch die folgenden Einstellungen:

- Schalten Sie IGMP-Snooping an den Ringports und global ein; und
- schalten Sie „IGMP Forward All“ pro Port an den Ringports ein.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 93: Schaltflächen

4.4.2 GMRP (GARP Multicast Registration Protocol)

Dieser Dialog bietet Ihnen die Möglichkeit,

- die GMRP-Funktion global ein- oder auszuschalten,
- das GMRP pro Port zu konfigurieren.

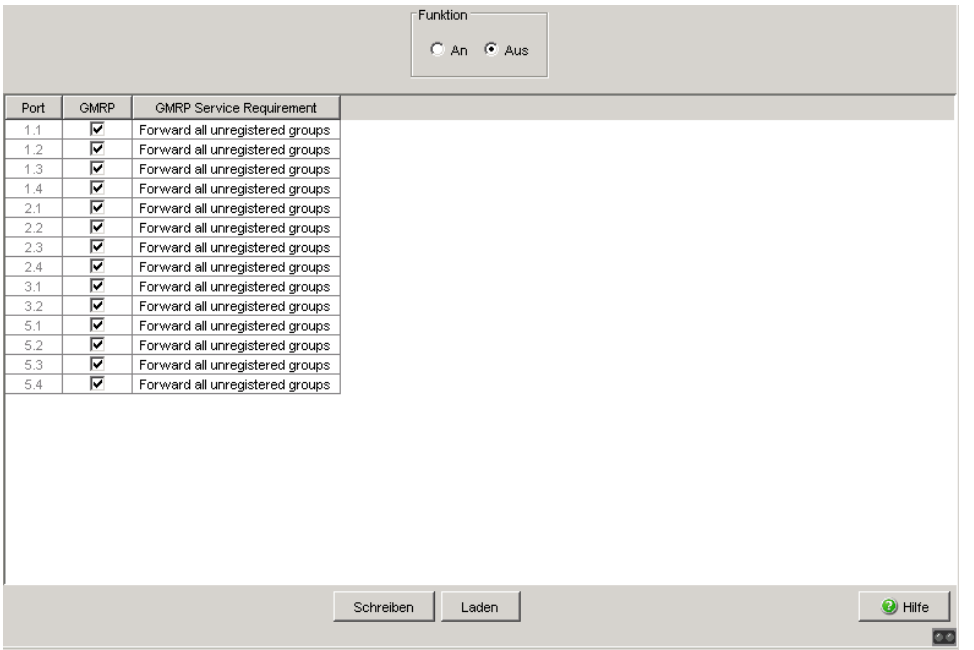


Abb. 48: Dialog GMRP

Funktion

Dieser Rahmen bietet Ihnen die Möglichkeit,

- die GMRP-Funktion global ein- oder auszuschalten.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
GMRP	GMRP für das gesamte Gerät global einschalten. Ist GMRP ausgeschaltet, dann: ▶ generiert das Gerät keine GMRP-Pakete, ▶ wertet empfangene GMRP-Pakete nicht aus und ▶ sendet (flutet) empfangene Datenpakete an allen Ports. Für empfangene GMRP-Pakete ist das Gerät unabhängig von der GMRP-Einstellung transparent.	`An, Aus`	`Aus`

Tab. 94: Globale Einstellung

Multicasts

Anmerkung: Die folgenden Gerätefamilien unterstützen diese Funktion: RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH100, MACH1000, OCTOPUS.

In diesem Rahmen bestimmen Sie, wie das Gerät Pakete mit

- unbekannten -nicht mit GMRP gelernten- MAC-Multicast-Adressen

vermittelt.

Voraussetzung: Die GMRP-Funktion ist global eingeschaltet.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Unbekannte Multicasts	▶ An alle Ports senden: Das Gerät sendet die Pakete mit unbekannter MAC-Multicast-Adresse an alle Ports. ▶ Verwerfen: Das Gerät verwirft die Pakete mit unbekannter MAC-Multicast-Adresse.	An alle Ports senden, Verwerfen	An alle Ports senden

Tab. 95: Unbekannte Multicasts

Einstellungen pro Port (Tabelle)

Diese Konfigurationstabelle bietet Ihnen die Möglichkeit, portbezogene Einstellungen vorzunehmen für:

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port	Modul- und Port-Nummer, für die dieser Eintrag gilt.	-	-
GMRP	GMRP je Port ein-/ausschalten. Das Ausschalten des GMRP an einem Port verhindert Registrierungen für diesen Port und das Weiterleiten von GMRP-Paketen an diesem Port. Voraussetzung: Die GMRP-Funktion ist global eingeschaltet.	`An`, `Aus`	`An`
GMRP Service Requirement	Geräte, die das GMRP nicht unterstützen, können in die Multicast-Adressierung mit eingebunden werden durch – einen statischen Filteradress-Eintrag am Anschluss-Port. – Auswählen von `Forward all groups`. Ports mit der Auswahl Forward all groups trägt das Gerät in alle Multicast-Filtereinträge ein, die über GMRP gelernt wurden. Voraussetzung: Die GMRP-Funktion ist global eingeschaltet.	`Forward all groups`, `Forward all unregistered groups`	`Forward all unregistered groups`

Tab. 96: GMRP-Einstellungen pro Port

Anmerkung: Ist das Gerät in einen HIPER-Ring eingebunden, dann erreichen Sie für Datenpakete mit registrierten Multicast-Zieladressen eine schnelle Rekonfiguration des Netzes nach einer Ringumschaltung durch die folgenden Einstellungen:

- Schalten Sie GMRP an den Ringports und global ein; und
- schalten Sie `Forward all groups` an den Ringports ein.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 97: Schaltflächen

4.5 VLAN

Unter VLAN finden Sie alle Dialoge und Ansichten, um:

- die VLAN-Funktionen nach dem Standard IEEE 802.1Q zu konfigurieren und zu überwachen.,
- für Voice-Geräte (z.B. VoIP-Telefone) pro Port:
  - eine Voice-VLAN-Netz-Richtlinie zu definieren, die der Switch den angeschlossenen Geräten per LLDP-MED übermittelt,
  - eine aktive 802.1X-Authentifizierung für Voice-Geräte zu umgehen

4.5.1 VLAN Global

Dieser Dialog bietet Ihnen die Möglichkeit:

- VLAN-Parameter anzuzeigen
- den VLAN 0 Transparent-Modus ein-/auszuschalten
- GVRP ein-/auszuschalten
- den Learning-Modus zu konfigurieren und anzuzeigen
- Die VLAN-Einstellungen des Gerätes in den Lieferzustand zurückzusetzen.

Parameter	Bedeutung
Größte VLAN-ID	Anzeige der größten möglichen VLAN-ID (siehe auf Seite 195 „VLAN Statisch“).
Max. Anzahl VLANs	Anzeige der maximal möglichen Anzahl von VLANs (siehe auf Seite 195 „VLAN Statisch“).
Eingerichtete VLANs	Zeigt die Anzahl der eingerichteten VLANs an (siehe auf Seite 195 „VLAN Statisch“).

Tab. 98: VLAN-Anzeigen

Anmerkung: Das Gerät gibt das VLAN mit der ID 1 vor. Das VLAN mit der ID 1 ist stets vorhanden.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
VLAN 0-Transparent-Modus	Ist der VLAN 0-Transparent-Modus eingeschaltet, akzeptiert das Gerät beim Empfang eine VLAN-ID von 0 im Paket, unabhängig von der Einstellung der Port-VLAN-ID im Dialog (siehe auf Seite 198 „VLAN Port“). Schalten Sie den „VLAN 0-Transparent-Modus“ ein, um Pakete mit Prioritäts-TAG ohne eine VLAN-Zugehörigkeit, also mit VLAN-ID 0, zu vermitteln.	`An`, `Aus`	`Aus`
GVRP aktiv	Schalten Sie „GVRP“ ein, um die Verteilung der VLAN-Information über GVRP-Datenpakete zu den Nachbargeräten sicherzustellen.	`An`, `Aus`	`Aus`
Double-VLAN-Tag Ethertype	Legt den Wert des äußeren VLAN-Tags fest, den ein Core-Port beim Senden eines Frames verwendet. Die auswählbaren Werte haben folgende Bedeutung: – 0x8100 (802.1Q): VLAN-Tag – 0x88A8 (vman): Provider Bridging **Anmerkung:** Diese Einstellung wirkt sich ausschließlich bei Core-Port aus. Access-Ports und normale Ports ignorieren diese Einstellung und verwenden immer 8100_H	0 - 65.535	33.024 (8100_H)

Tab. 99: VLAN-Einstellungen

Anmerkung: Wenn Sie das GOOSE-Protokoll gemäß IEC 61850-8-1 verwenden, dann aktivieren Sie den „VLAN 0-Transparent-Modus“. Auf diese Weise bleibt die Priorisierungsinformation nach IEEE 802.1D/p im Datenpaket auch dann erhalten, wenn das Gerät das Datenpaket weiter vermittelt.
Das gilt auch für andere Protokolle, die diese Priorisierung nach IEEE 802.1D/p verwenden, aber keine VLANs gemäß IEEE 802.1Q benötigen.

Anmerkung: Beachten Sie für die Handhabung des „Transparent-Modus“:

- Für PowerMICE, MACH 104, MACH 1040 und MACH 4000:
  Im „Transparent-Modus“ ignorieren die Geräte beim Empfang die VLAN-Tags und das Prioritäts-Tag. Stellen Sie die VLAN-Zugehörigkeit der Ports aller VLANs auf „U“ (Member Untagged).
- Für MACH 4002-24/48G:
  Im „Transparent-Modus“ ignorieren die Geräte beim Empfang die VLAN-Tags, das Prioritäts-Tag wird hingegen ausgewertet. Stellen Sie die VLAN-Zugehörigkeit der Ports aller VLANs auf „U“ (Untagged).

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Modus	Wahl des VLAN-Modus. **„Independent VLAN“** (unabhängiges VLAN), unterteilt die Forwarding Database (siehe auf Seite 169 „Filter für MAC-Adressen“) virtuell in je eine unabhängige Forwarding Database je VLAN. Datenpakete mit einer Zieladresse in einem anderen VLAN kann das Gerät nicht zuordnen und flutet sie an allen Ports des VLANs. **Anwendungsgebiet:** Aufbau identischer Netze, die auch gleiche MAC-Adressen benutzen. **„Shared VLAN“** (gemeinsames VLAN), benutzt für alle VLANs die gemeinsame Forwarding Database (siehe auf Seite 169 „Filter für MAC-Adressen“). Datenpakete mit einer Zieladresse in einem anderen VLAN kann das Gerät zuordnen und leitet sie ausschließlich an den Zielport weiter, falls der Empfangsport auch Mitglied der VLAN-Gruppe des Zielports ist. **Anwendungsgebiet:** Bei sich überlappenden Gruppen kann das Gerät VLAN-übergreifend direkt vermitteln, sofern die betroffenen Ports einem erreichbaren VLANs angehören. Änderungen des Modus werden erst nach einem Warmstart (siehe auf Seite 68 „Neustart“) des Gerätes übernommen und danach in der darunterliegenden Zeile unter „Status“ angezeigt.	Independent VLAN, Shared VLAN	Independent VLAN
Status	Anzeige des aktuellen Status. Nach einem Warmstart (siehe auf Seite 68 „Neustart“) des Gerätes übernimmt das Gerät die Einstellung von „Modus“ in die Statuszeile.	Independent VLAN, Shared VLAN	

Tab. 100: Einstellungen und Anzeigen im Rahmen „Learning“

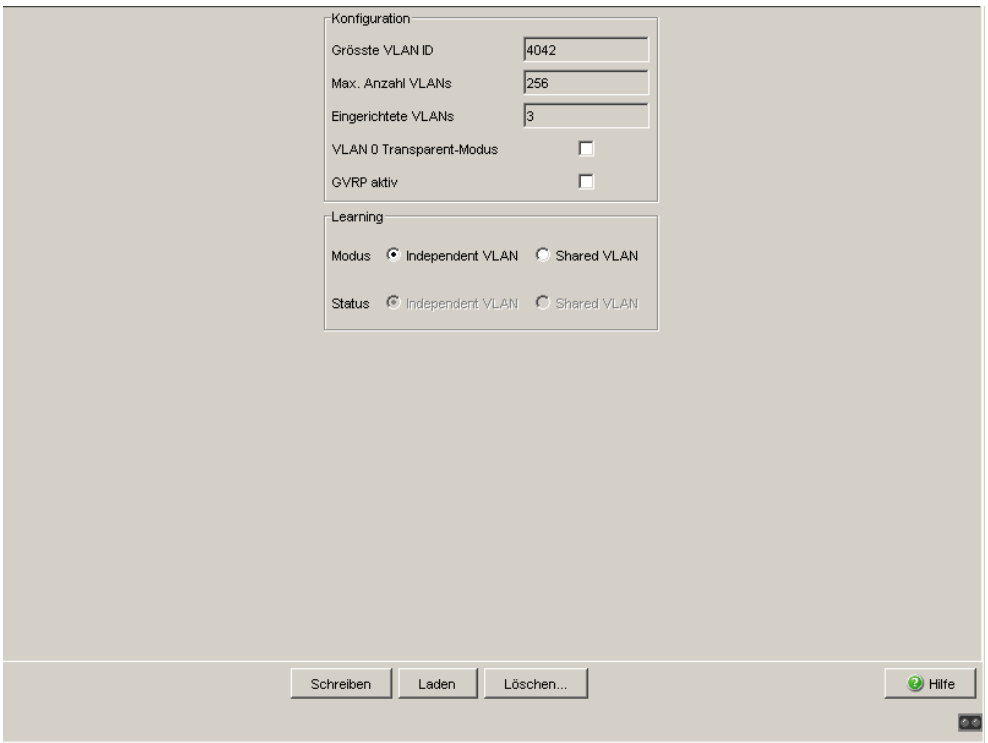


Abb. 49: Dialog VLAN Global

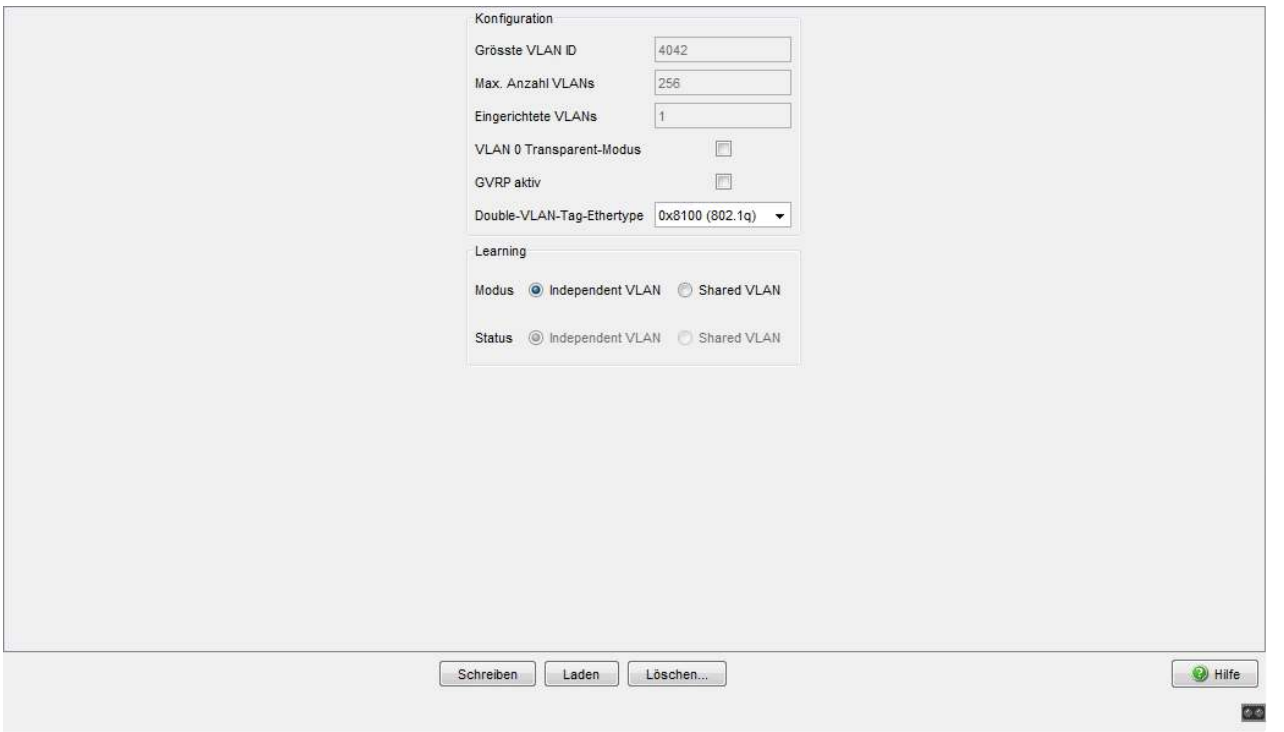


Abb. 50: Dialog `Switching:VLAN:Global` (MACH4000 und MACH 1040)

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Löschen…	Versetzt die VLAN-Einstellungen des Gerätes in den Lieferzustand. Vorsicht: Sie versperren sich den Zugang zum Gerät, wenn Sie im Dialog `Grundeinstellungen:Netz` die VLAN-ID für die Management-Funktionen des Gerätes geändert haben.
Hilfe	Öffnet die Online-Hilfe.

Tab. 101: Schaltflächen

4.5.2 VLAN Aktuell

Dieser Dialog bietet Ihnen die Möglichkeit, die aktuellen VLAN-Parameter anzuzeigen

Die VLAN Aktuell-Tabelle zeigt alle
- manuell konfigurierten VLANs
- durch Redundanz-Mechanismen konfigurierten VLANs
- durch GVRP konfigurierten VLANs

Die VLAN Aktuell-Tabelle dient ausschließlich der Anzeige. Änderungen der Einträge nehmen Sie im Dialog `VLAN:Statisch` vor (siehe auf Seite 195 „VLAN Statisch“).

Anmerkung: Nicht angezeigte Ports nehmen an einer Link-Aggregation teil. Diese Ports können Sie über den der Link-Aggregation zugeordneten Port im Modul 8 (Anzeige 8.X) einem VLAN zuordnen.

Parameter	Bedeutung	Mögliche Werte
VLAN-ID	Anzeige der ID des VLANs.	
Status	Anzeige des VLAN-Status	`other`: Dieser Eintrag tritt ausschließlich bei VLAN 1 auf. Das System gibt das VLAN 1 vor. VLAN 1 ist stets vorhanden. `permanent`: Ein von Ihnen eingegebener statischer Eintrag. Dieser Eintrag bleibt nach einem Neustart des Gerätes erhalten. `dynamic`: Dieses VLAN wurde dynamisch über GVRP erzeugt.
Zeit der Erstellung	Betriebszeit, zu der das VLAN erstellt wurde (siehe „Systemdaten“).	
Ports x.x	Zugehörigkeit des betreffenden Ports zu einem VLAN und Handhabung des VLAN-Tag.	- momentan kein Mitglied (Eintrag per GVRP möglich) `T` Mitglied im VLAN, Datenpakete mit Tag (Tagged) versenden. `U` Mitglied im VLAN, Datenpakete ohne Tag (Untagged) versenden. `F` Mitgliedschaft verboten (Forbidden), also auch kein Eintrag per GVRP möglich.

Tab. 102: VLAN Aktuell

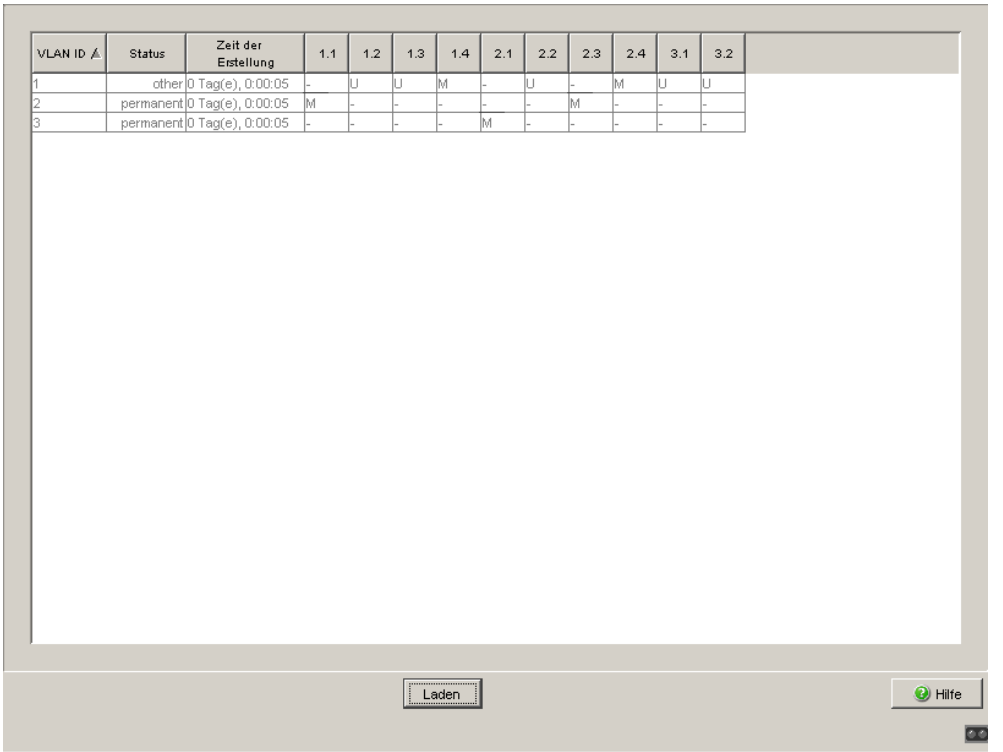


Abb. 51: Dialog VLAN Aktuell

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 103: Schaltflächen

4.5.3 VLAN Statisch

Dieser Dialog bietet Ihnen die Möglichkeit:

- VLANs zu erzeugen
- VLANs mit Namen zu versehen
- Ports VLANs zuzuordnen und zu konfigurieren
- VLANs zu löschen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
VLAN-ID	Anzeige der ID der bis zu 255 gleichzeitig möglichen VLANs. (Bis 256 gleichzeitig möglichen VLANs für Power MICE, MACH 104, MACH 1040, MACH 4000.)	1-4.042	
Name	Eingeben eines beliebigen Namens für dieses VLAN.	Maximal 32 Zeichen	VLAN 1: default
Ports x.x	Auswahl der Zugehörigkeit der Ports zu den VLANs.	`-`: momentan kein Mitglied (GVRP erlaubt). `T`: Mitglied im VLAN, Datenpakete mit Tag (Tagged) versenden. `U`: Mitglied im VLAN, Datenpakete ohne Tag (Untagged) versenden. `F`: Mitgliedschaft verboten (Forbidden), also auch kein Eintrag per GVRP möglich.	VLAN 1: `U`, neue VLANs: `-`

Tab. 104: Dialog VLAN Statisch

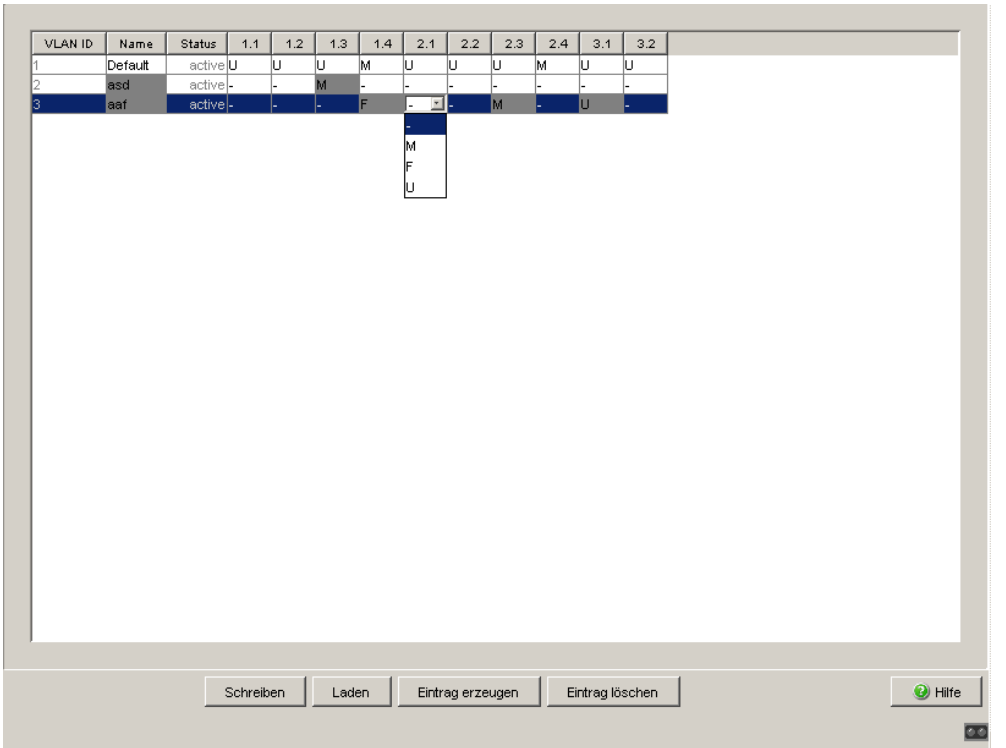


Abb. 52: Dialog VLAN Statisch

Anmerkung: Achten Sie bei der VLAN-Konfiguration darauf, dass die Managementstation auch nach dem Speichern der VLAN-Konfiguration noch Zugriff auf das Gerät hat.
Schließen Sie die Managementstation an einen Port an, der Mitglied im VLAN ist, das als Management-VLAN ausgewählt ist. Im Lieferzustand vermittelt das Gerät die Management-Daten in VLAN 1.

Anmerkung: Das Gerät legt automatisch VLANs für MRP-Ringe an. Die MRP-Ringfunktion verhindert das Löschen dieser VLANs.

Anmerkung: Beachten Sie die Tagging-Einstellungen von Ports, die Teil eines Redundanz-Rings oder der Ring-/Netzkopplung sind.

Redundanz	VLAN-Zugehörigkeit
HIPER-Ring	VLAN 1 U
MRP-Ring	beliebig
Ring-/Netzkopplung	VLAN 1 U

Tab. 105: Erforderliche VLAN-Einstellungen für Ports, die Teil von redundanten Ringen oder Ring-/ Netz-Kopplung sind.

Anmerkung: Betreiben Sie in einem Redundanz-Ring mit VLANs ausschließlich Geräte, deren Software-Version VLANs unterstützt:

- RS2 xx/xx (ab Rel. 7.00)
- RS2-16M
- RS20, RS30, RS40 (mit Software-Varianten L2E, L2P)
- MICE (ab Rel. 3.0)
- PowerMICE
- MS20, MS30
- RSR20, RSR30
- MACH 100
- MACH 1000
- MACH 4000
- MACH 3000 (ab Rel. 3.3),
- OCTOPUS

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 106: Schaltflächen

4.5.4 VLAN Port

Dieser Dialog bietet Ihnen die Möglichkeit:

- Ports VLANs zuzuordnen
- den Acceptable Frame Type zu bestimmen
- Ingress-Filtering ein-/auszuschalten
- GVRP ein-/auszuschalten

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port	Port, für den dieser Eintrag gilt.		
Port-VLAN-ID	Legt fest, welchem VLAN der Port ein empfangenes, ungetaggtes Datenpaket zuordnet.	Alle erlaubten VLAN-IDs	1

Acceptable-Frame-Types	Legt fest, ob der Port auch Datenpakete ohne VLAN-Tag empfangen darf.
	`admitAll`: Das Gerät akzeptiert auf diesem Port ankommende Frames, und weist nicht oder mit einer Priorität getaggte Frames die Port-PVID zu.
	`admitOnlyVlanTagged`: Das Gerät verwirft auf diesem Port ankommende ungetaggte Frames.
	`admitOnlyUntagged`: Das Gerät verwirft Frames mit VLAN-Tag. Dieser Wert ist auf den Geräten MS, RS, Octopus, MACH102, MACH1020/30 verfügbar.
		`admitAll`
		`admitOnlyVlanTagged`
		`admitOnlyUntagged`
			`admitAll`

Ingress-Filtering	Legt fest, ob der Port die empfangenen Tags auswertet.	`ein`, `aus`	`aus`

Tab. 107: Dialog VLAN Port

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
GVRP	- ein: Das Gerät sendet und empfängt GVRP-Datenpaketet. Das Gerät tauscht VLAN-Konfigurationsdaten mit anderen Geräten aus. - aus: Das Gerät sendet und empfängt keine GVRP-Datenpakete. Das Gerät tauscht keine VLAN-Konfigurations-daten mit anderen Geräten aus.	`An` (markiert), `Aus` (nicht markiert)	`Aus`
DVLAN-Tag-Modus	- `normal`: Der Port beteiligt sich nicht am DVLAN-Tagging. - `core`: Der Port sendet einen doppelt getaggten Frame mit dem Ethertype aus, der in "Double-VLAN-Ethertype" eingestellt ist. Nehmen Sie dazu den Port als Tagged Member in allen Tunnel-VLANs auf. - `access`: Der Port ordnet einem empfangenen Frame seine Port-VLAN-ID zu, auch bei einem bereits getaggten Frame. Der Port sendet den ursprünglich empfangenen Frame wieder aus (getaggt oder ungetaggt). Geben Sie dem Port die Tunnel-VLAN-ID als Port-VLAN-ID und nehmen Sie ihn als Untagged Member in dieses VLAN auf.	`normal`, `core`, `access`	`normal`

Tab. 107: Dialog VLAN Port

Anmerkung: Wenn Sie unter „Acceptable Frame Types“ `admitOnlyVlanTagged` gewählt haben und GVRP eingeschaltet ist, weisen Sie in `Grundeinstellungen:Netz` der VLAN-ID den Wert 0 zu.

Anmerkung: Beachten Sie in Zusammenhang mit:

- HIPER-Ring
  Wählen Sie für die Ringports die Port-VLAN-ID 1 und schalten Sie „`Ingress Filtering`“ aus.
- MRP-Ring
  - Wenn die MRP-Ring-Konfiguration (siehe auf Seite 265 „MRP-Ring konfigurieren“) keinem VLAN zugeordnet ist, wählen Sie die Port-VLAN-ID 1.
  - Wenn die MRP-Ring-Konfiguration (siehe auf Seite 265 „MRP-Ring konfigurieren“) einem VLAN zugeordnet ist, führt das Gerät die VLAN-Konfiguration für diesen Port automatisch durch.
- Netz-/Ring-Kopplung
  Wählen Sie für die Kopplungs- und Partner-Kopplungsports die VLAN-ID 1 und schalten Sie „`Ingress Filtering`“ aus.

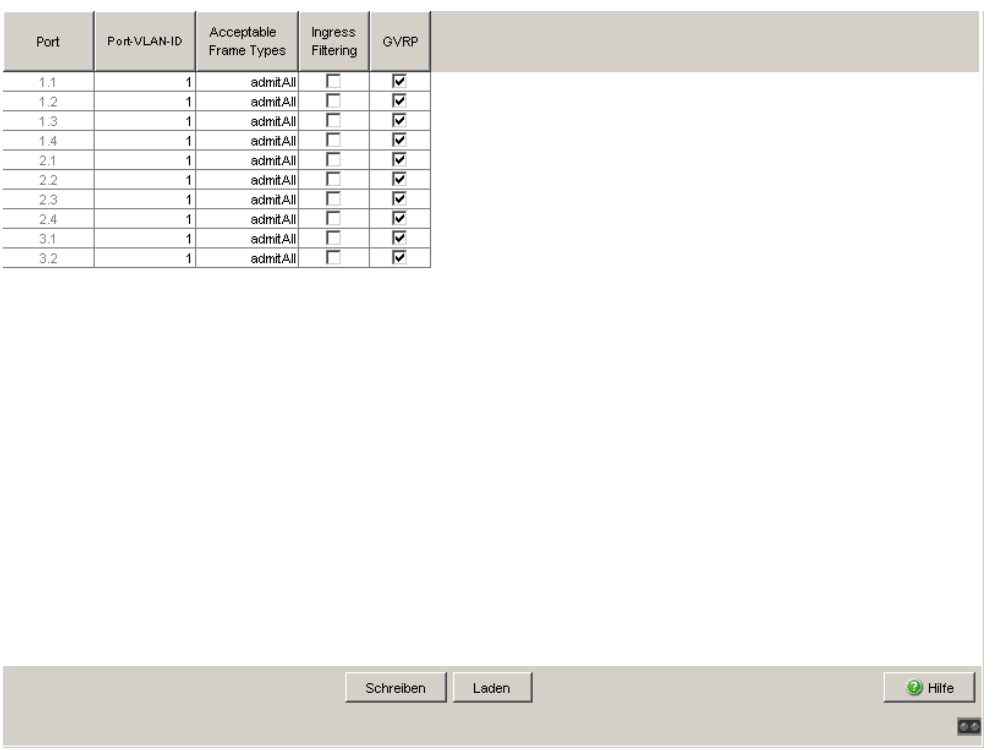


Abb. 53: Dialog VLAN Port

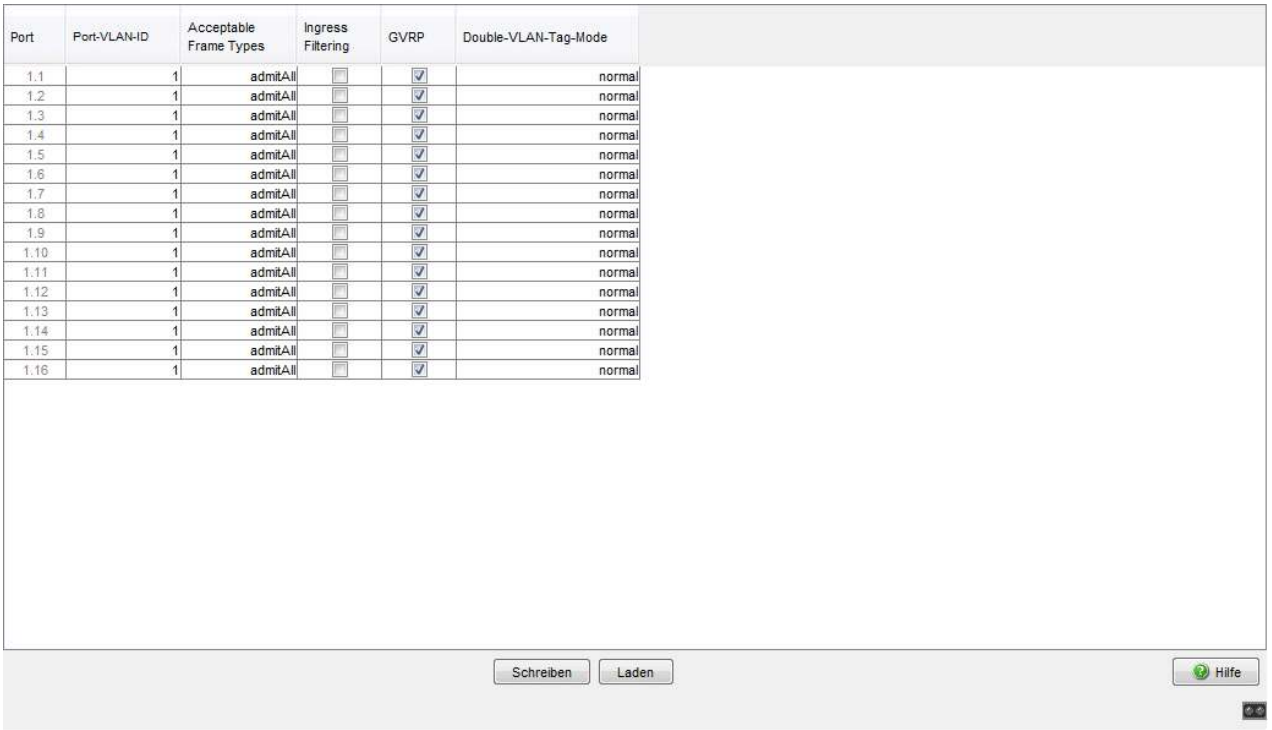


Abb. 54: Dialog `Switching:VLAN:Port` (MACH4000 und MACH1040)

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 108: Schaltflächen

4.5.5 Voice-VLAN

Die Funktion Voice-VLAN bietet Ihnen die Möglichkeit, Voice-Geräte wie z.B. VoIP-Telefone per Plug-and-Play in Betrieb zu nehmen.

Sie können dazu ein oder mehrere im Switch konfigurierte VLANs als Voice-VLANs verwenden und können pro Port eine Voice-VLAN-Netz-Richtlinie definieren (engl.: Voice VLAN Network Policy). Diese besteht aus dem Voice-VLAN-Modus, der Voice-VLAN-ID und der Voice-VLAN-Priorität. Diese sendet der Switch per LLDP-MED an die angeschlossenen Endgeräte.

Ein LLDP-MED-fähiges Endgerät kann dann automatisch die richtigen Einstellungen ermitteln, um seinen Datenverkehr aufzunehmen.

Die Voraussetzung dafür ist, dass Sie auf dem Switch sowohl LLDP (siehe auf Seite 365 „LLDP-Informationen von Nachbargeräten“) als auch LLDP-MED (siehe auf Seite 367 „LLDP-MED (Media Endpoint Discovery)“) aktivieren.

Dieser Dialog bietet Ihnen die folgenden Möglichkeiten:

- Das Senden einer Voice-VLAN-Netz-Richtlinie (Voice VLAN Network Policy) des Switch über LLDP-MED global ein- oder ausschalten.
- Einem Switch-Port eine Voice-VLAN-Netz-Richtlinie zuordnen.
  Der Switch informiert Geräte, die an diesem Port angeschlossen sind, per LLDP-MED über seine Voice-VLAN-Netz-Richtlinie.
- Einem Switch-Port eine Voice-VLAN-ID für die Voice-VLAN-Netz-Richtlinie zuordnen.
  Der Switch informiert Geräte an diesem Port per LLDP-MED über die Voice-VLAN-ID seiner Voice-VLAN-Netz-Richtlinie.
- Einem Switch-Port eine VLAN-Priorität für die Voice-VLAN-Netz-Richtlinie zuordnen.

Der Switch informiert Geräte an diesem Port per LLDP-MED über die VLAN-Priorität seiner Voice-VLAN-Netz-Richtlinie.

- An einem Switch-Port eine bereits aktive 802.1X-Authentifizierung für ein LLDP-MED-fähiges Gerät (z.B. ein VoIP-Telefon) explizit deaktivieren.
  - Bei aktiver Voice-Authentifizierung muss sich das angeschlossene Gerät zunächst per 802.1X beim Switch authentifizieren . Erst dann lässt der Switch den Datenverkehr des Gerätes an seinem Port zu.
  - Bei inaktiver Voice-Authentifizierung lässt der Switch trotz einer aktiven 802.1X-Authentifizierung den Datenverkehr für ein angeschlossenes Gerät bereits dann zu, wenn sich das Gerät per LLDP-MED als Voice-Gerät identifiziert hat und das Gerät getaggte Frames mit der Voice-VLAN-ID sendet.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Rahmen Funktion	Schaltet das Senden einer Port-spezifischen Voice-VLAN-Netz-Richtlinie (Voice VLAN Network Policy) per LLDP-MED global ein oder aus. **Anmerkung:** Voraussetzung für das Senden der Voice-VLAN-Netz-Richtlinien ist, dass Sie auf dem Switch sowohl LLDP (siehe auf Seite 365 „LLDP-Informationen von Nachbargeräten“) als auch LLDP-MED (siehe auf Seite 367 „LLDP-MED (Media Endpoint Discovery)“) aktiviert haben.	`An`, `Aus`	`Aus`

Tab. 109: Globale Einstellungen des Voice-VLAN-Dialogs

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port	Modul- und Port-Nummer, für die dieser Eintrag gilt	-	-
Voice VLAN Modus	Modus der Voice-VLAN-Netz-Richtlinie, die der Switch per LLDP-MED angeschlossenen Geräten mitteilt. ▶ `disabled`: Der Switch sendet keine Voice-VLAN-Netz-Richtlinie. ▶ `none`: Der Switch sendet die Voice-VLAN-Netz-Richtlinie „keine“; das bedeutet, dass das angeschlossene Gerät seine eigene Konfiguration verwenden soll. ▶ `untagged`: Das angeschlossene Gerät soll ungetaggte Frames senden. ▶ `vlan`: Das angeschlossene Gerät soll VLAN-getaggte Frames senden. ▶ `dot1p-priority`: Das angeschlossene Gerät soll Prioritäts-getaggte Frames (mit VLAN-ID 0) senden. ▶ `vlan & dot1p-priority`: Das angeschlossene Gerät soll VLAN- und Prioritäts-getaggte Frames senden.	`disabled`, `none`, `untagged`, `vlan`, `dot1p-priority`, `vlan & dot1p-priority`	`disabled`
VLAN-ID	VLAN-ID der Voice-VLAN-Netz-Richtlinie, die der Switch per LLDP-MED angeschlossenen Geräten mitteilt. **Anmerkung:** Verwenden Sie eine VLAN-ID, die im Switch bereits konfiguriert ist. So ermöglichen Sie die Plug-and-Play-Inbetriebnahme eines Voice-Gerätes.	`0 - 4094`	`0`

Tab. 110: Einstellungen des Voice-VLAN-Dialogs

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Priorität	Layer 2- (802.1p-) Priorität der Voice-VLAN-Netz-Richtlinie, die der Switch per LLDP-MED angeschlossenen Geräten mitteilt.	`none`, `0 - 7`	`none`
Bypass-Authentifizierung	▶ `An`: Das angeschlossene Gerät muss sich bei aktiver 802.1X-Authentifizierung zunächst beim Switch authentifizieren. Erst dann lässt der Switch den Datenverkehr des Gerätes an seinem Port zu. ▶ `Aus`: Der Switch lässt trotz einer aktiven 802.1X-Authentifizierung den Datenverkehr für ein angeschlossenes Gerät bereits dann zu, wenn - sich das Gerät per LLDP-MED als Voice-Gerät identifiziert hat, und - das Gerät getaggte Frames mit der Voice-VLAN-ID sendet. **Anmerkung:** ▶ Wenn Sie für einen Port die Authentifizierung verwenden, aktivieren Sie an diesen Port die 802.1X-basierte Portsicherheit (siehe auf Seite 103 „802.1X-Portkonfiguration“). ▶ Wenn Sie die 802.1X-basierte Portsicherheit verwenden, mehr als ein Gerät an einen Port anschließen[a] und zudem die Voice-Authentifizierung verwenden, dann aktivieren Sie die MAC-basierte Authentifizierung. ▶ Haben Sie für diesen Port eine MAC- oder IP-basierte Portsicherheit eingestellt, bleibt diese in jedem Fall aktiv. ▶ Verwenden Sie eine IP-basierte Portsicherheit ausschließlich dann, wenn das Voice-Gerät eine feste IP-Adresse besitzt.	`An` `Aus`	`An`

Tab. 110: Einstellungen des Voice-VLAN-Dialogs

[a] Z.B. ein VoIP-Telefon mit integriertem Switch, an dem Sie einen PC angeschlossen haben.

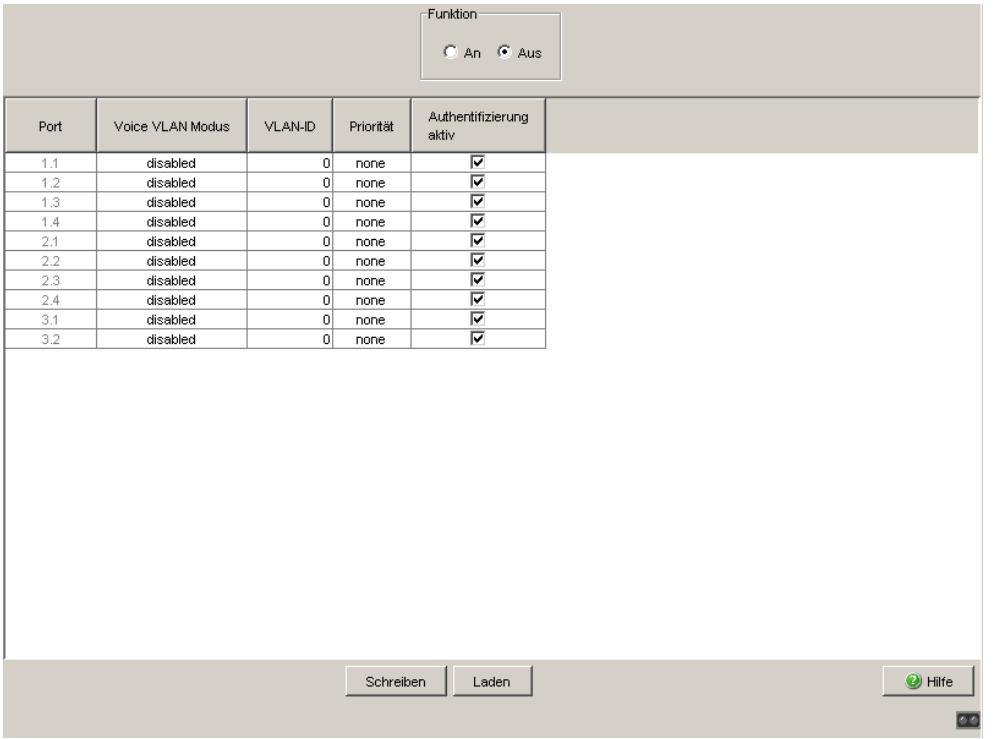


Abb. 55: Voice-VLAN-Dialog

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 111: Schaltflächen

5 QoS/Priorität

Das Gerät bietet Ihnen die Möglichkeit, einzustellen

- wie es die QoS-/Priorisierungs-Informationen eingehender Datenpakete auswertet:
  - VLAN-Priorität nach IEEE 802.1Q/ 802.1D (Layer 2)
  - Type-of-Service (ToS) bzw. DiffServ (DSCP) bei IP-Paketen (Layer 3)
- welche QoS-/Priorisierungs-Informationen es in ausgehende Datenpakete schreibt (z.B. Priorität für Management-Pakete, Portpriorität).

Das QoS/Priorität-Menü enthält hierzu die Dialoge, Anzeigen und Tabellen zur Konfiguration der QoS-/Prioritäts-Einstellungen:

- Global
- Portkonfiguration
- IEEE 802.1D/p-Mapping
- IP-DSCP-Mapping
- Queue-Management

5.1 Global

Dieser Dialog bietet Ihnen die Möglichkeit:

- die VLAN-Priorität für Management-Pakete im Bereich 0 bis 7 einzugeben (Voreinstellung 0).
  Damit Sie in Situationen großer Netzlast immer vollen Zugriff auf die Verwaltung des Gerätes haben, bietet Ihnen das Gerät die Möglichkeit, Management-Pakete zu priorisieren.
  Bei der Priorisierung von Management-Paketen (SNMP, Telnet, usw.) sendet das Gerät die Management-Pakete mit einer Prioritäts-Information.
  Beachten Sie die Zuordnung der VLAN-Priorität zu der Traffic Class (siehe Tabelle 116).
- den IP-DSCP-Wert für Management-Pakete im Bereich von 0 bis 63 einzugeben (Voreinstellung: 0 (be/cs0)).
  Damit Sie in Situationen großer Netzlast immer vollen Zugriff auf die Verwaltung des Gerätes haben, bietet Ihnen das Gerät die Möglichkeit, Management-Pakete zu priorisieren.
  Bei der Priorisierung von Management-Paketen (SNMP, Telnet, usw.) sendet das Gerät die Management-Pakete mit einer Prioritäts-Information.
  Beachten Sie die Zuordnung des IP-DSCP Wertes zu der Traffic Class (siehe Tabelle 114).

  Anmerkung: Bestimmte DSCP-Werte haben DSCP-Namen, wie z.B. be/cs0 bis cs7 (Class Selector) oder af11 bis af43 (Assured Forwarding) und ef (Expedited Forwarding).

- die maximal mögliche Anzahl Queues per Port anzuzeigen.
  Das Gerät unterstützt 4 (8 bei MACH 4000, MACH 104, MACH 1040 und PowerMICE) Prioritäts-Queues (Traffic Classes nach IEEE 802.1D).

Anmerkung: Das Ändern der globalen Einstellung für „Trust Mode“ und Klicken auf „Schreiben“ setzt jeden Port auf diese Einstellung. Sie können danach die Einstellung jedes Ports individuell verändern.
Das erneute Ändern der globalen Einstellung überschreibt die individuellen Port-Einstellungen.

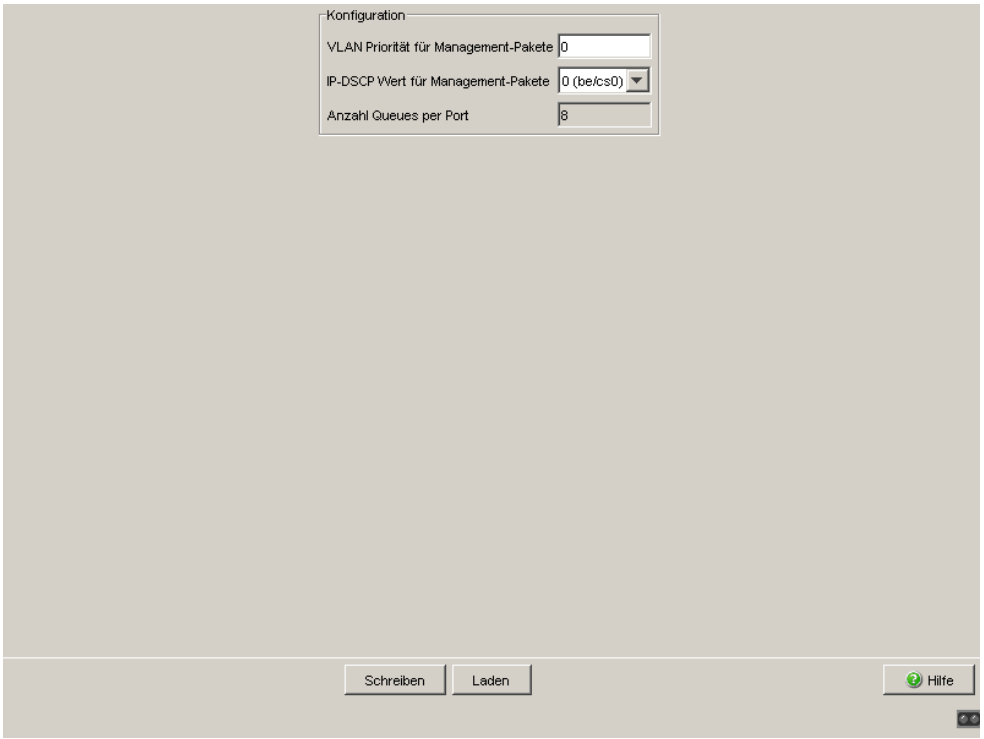


Abb. 56: Dialog Global

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 112: Schaltflächen

5.2 Portkonfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, die Ports zu konfigurieren. Sie können:

- einem Port eine Port-Priorität zuweisen.
- den Trust Modus für einen Port wählen,
- die Untrusted Traffic Class anzeigen,
- einem Port eine Shaping Rate zuweisen.

Parameter	Bedeutung
Modul.Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.
Port Priorität	Eingeben der Portpriorität
Trust Modus	Auswählen des Trust Modus.
Untrusted Traffic Class	Anzeige der Traffic Class, die im Trust Modus „untrusted“ verwendet wird.
Shaping Rate	Auswahl der maximal zur Verfügung gestellten Bandbreite in %. Zulässiger Bereich: 0% (off) bis 95% in Schritten von 5%.

Tab. 113: Portkonfiguration-Tabelle

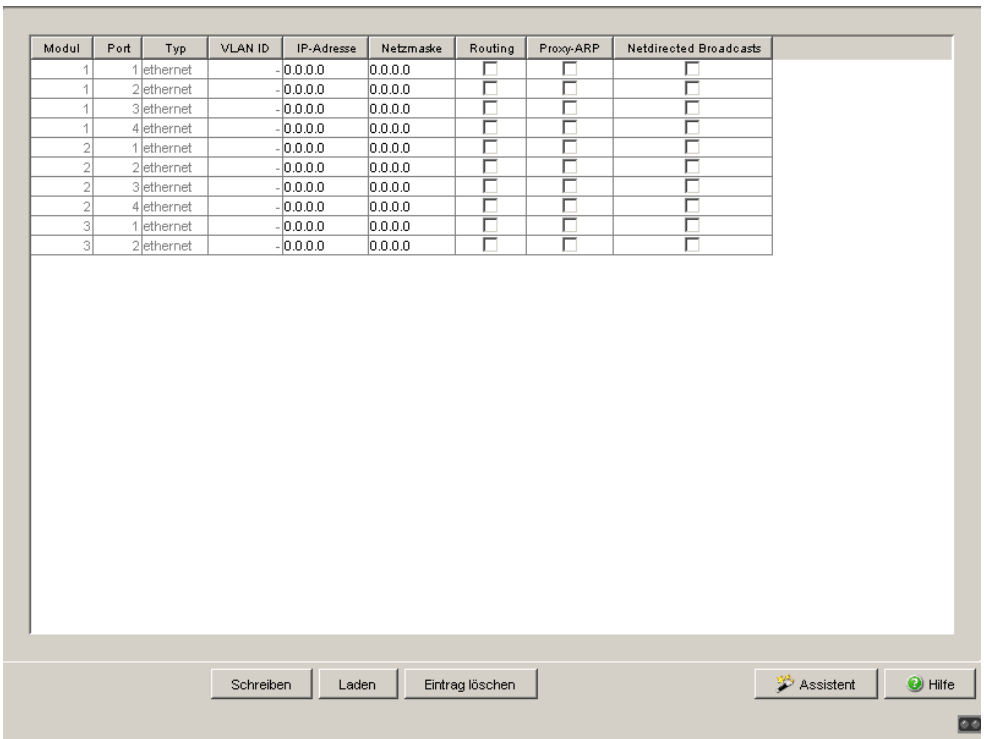


Abb. 57: Dialog Portkonfiguration

5.2.1 Port-Priorität eingeben

☐ Doppelklicken Sie in der Spalte „Port Priorität“ in eine Zelle und tragen Sie die Priorität (0-7) ein.
Das Gerät ordnet Datenpakete, die er an diesem Port empfängt, entsprechend der eingetragenen Priorität einer Prioritätsklasse zu. (siehe Tabelle 114).
Voraussetzung:
Einstellung in der Spalte `Trust Modus: untrusted` oder
Einstellung in der Spalte `Trust Modus: trustDot1p` und die Datenpakete enthalten kein VLAN-Tag oder
Einstellung in der Spalte `Trust Modus: trustIpDscp` und die Datenpakete sind keine IP-Pakete.

Port-Priorität	Traffic Class (Voreinstellung)	IEEE 802.1D Verkehrstyp
0	2	Best Effort (default)
1	0	Background
2	1	Standard
3	3	Excellent Effort (business critical)
4	4	Controlled Load (streaming multimedia)
5	5	Video, < 100 ms of latency and jitter
6	6	Voice; < 10 ms of latency and jitter
7	7	Network Control reserved traffic

Tab. 114: Zuordnung der Port-Priorität zu den Traffic Classes

5.2.2 Trust-Modus wählen

Das Gerät bietet Ihnen 3 Möglichkeiten, zu wählen, wie es empfangene Datenpakete behandelt, die eine Prioritätsinformation enthalten. Mit einem Klick in eine Zelle der Spalte „Trust Modus“ wählen Sie eine der 3 Möglichkeiten:

- „untrusted“:
  Das Gerät ignoriert die Prioritäts-Informationen im Paket und weist den Paketen immer die Port-Priorität des Empfangsports zu.
- „trustDot1p“:
  Empfangene Pakete, die VLAN-Tag-Information enthalten, priorisiert (einer Traffic Class zuordnen, siehe „802.1D/p-Mapping“) das Gerät entsprechend dieser Information.
  Empfangene Pakete, die keine Tag-Information enthalten, priorisiert (einer Traffic Class zuordnen, siehe „Port-Priorität eingeben“) das Gerät entsprechend der Port-Priorität des Empfangsports.
- „trustIpDscp“: Empfangene Pakete, die keine IP-Pakete sind, priorisiert (einer Traffic Class zuordnen, siehe „IP-DSCP-Mapping“) das Gerät entsprechend der Port-Priorität des Empfangsports. Empfangene Pakete, die keine IP-Pakete sind, priorisiert (einer Traffic Class zuordnen, siehe „Port-Priorität eingeben“) das Gerät entsprechend der Port-Priorität des Empfangsports.
  - Für empfangene IP-Pakete:
    Zusätzlich führt das Gerät ein VLAN-Prio-Remarking durch.
    Beim VLAN-Prio-Remarking modifiziert das Gerät die VLAN-Priorität der IP-Pakete, falls die Pakete mit VLAN-Tag gesendet werden sollen (siehe auf Seite 195 „VLAN Statisch“).
  - Für empfangene IP-Pakete:
    Entsprechend der Traffic Class, der das IP-Paket zugeordnet wurde (siehe oben), ordnet das Gerät anhand der Tabelle 118 dem IP-Paket die neue VLAN-Priorität zu.
    Beispiel: Einem empfangenen IP-Paket mit einem DSCP-Wert von 16 (cs2) wird der Traffic Class 1 zugeordnet (Voreinstellung). Das Paket erhält nun entsprechend der Tabelle 118 die VLAN-Priorität 2.

5.2.3 Untrusted Traffic Class anzeigen

„Untrusted Traffic Class“ zeigt Ihnen die Traffic Class an, die im Trust Modus „untrusted“ verwendet wird. Wenn Sie die Port-Priorität ändern (siehe auf Seite 212 „Port-Priorität eingeben“), dann ändert sich auch die Untrusted Traffic Class (siehe Tabelle 118).

5.2.4 Shaping Rate

Das Gerät bietet Ihnen die Möglichkeit, die maximale Bandbreite eines Ports zu begrenzen (Traffic Shaping).

Mit einem Klick in eine Zelle der Spalte „Shaping Rate“ wählen Sie einen der möglichen Werte für die Bandbreitenbegrenzung im Bereich von 5% bis 95% in Schritten von 5%.

- ☐ Der Wert „off“ bedeutet: keine Bandbreitenbegrenzung (0%).
- ☐ Der Wert „95“ bedeutet: 95% der Bandbreite stehen zur Verfügung.

Bei kurzzeitigem Überschreiten der eingestellten Bandbreite speichert das Gerät die Daten, um sie nach der Spitzenbelastung zu senden. Auf diese Weise glättet das Traffic Shaping Überlastsituationen.

Ist Traffic Shaping an einem Interface aktiv, dann ignoriert das Gerät die für Weighted Fair Queuing reservierten Bandbreiten.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 115: Schaltflächen

5.3 802.1D/p-Mapping

Der Dialog 802.1D/p-Mapping bietet Ihnen die Möglichkeit, jeder VLAN-Priorität eine Traffic Class zuzuordnen.

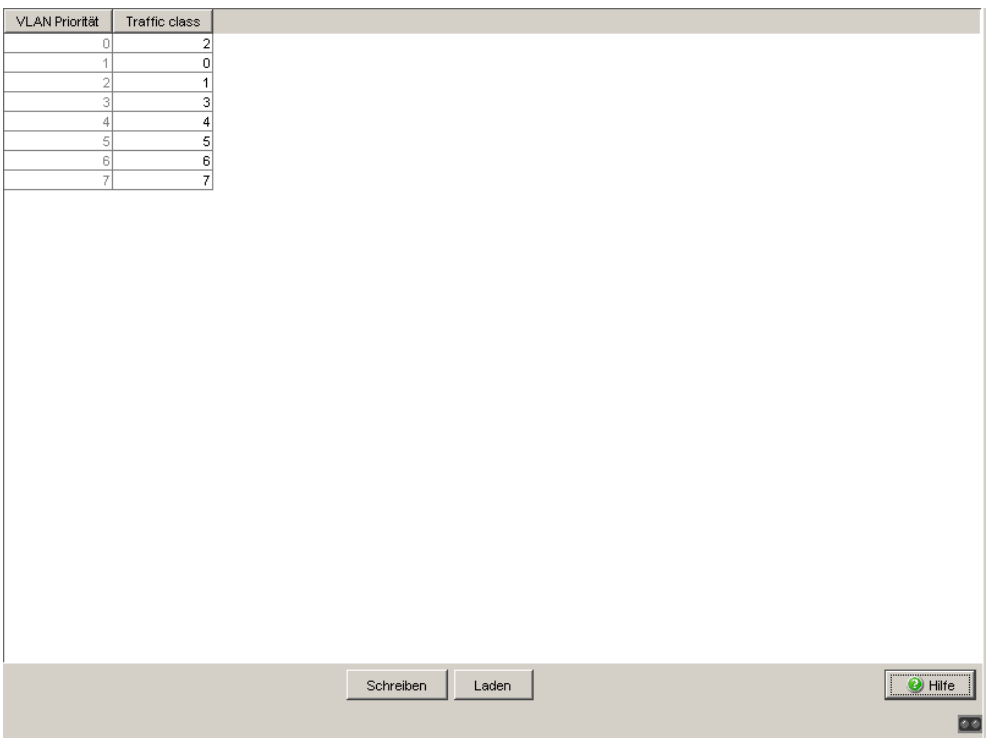


Abb. 58: Dialog 802.1D/p-Mapping

☐ Tragen Sie für jede VLAN-Priorität im Feld Traffic Class den gewünschten Wert zwischen 0 und 7 ein.

VLAN-Priorität	Traffic Class(Voreinstellung)	IEEE 802.1D Verkehrstyp
0	2	Best Effort (default)
1	0	Background

Tab. 116: Zuordnung der VLAN-Priorität zu den 8 Traffic Classes

VLAN-Priorität	Traffic Class(Voreinstellung)	IEEE 802.1D Verkehrstyp
2	1	Standard
3	3	Excellent Effort (business critical)
4	4	Controlled Load (streaming multimedia)
5	5	Video, < 100 ms of latency and jitter
6	6	Voice; < 10 ms of latency and jitter
7	7	Network Control reserved traffic

Tab. 116: Zuordnung der VLAN-Priorität zu den 8 Traffic Classes

Anmerkung: Netzprotokolle und Redundanzmechanismen nutzen die höchste Traffic Class 7. Wählen Sie deshalb andere Traffic Classes für Anwendungsdaten.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 117: Schaltflächen

5.4 IP-DSCP-Mapping

Die IP DSCP-Mapping-Tabelle bietet Ihnen die Möglichkeit, jedem DSCP-Wert eine Traffic Class zuzuordnen.

☐ Tragen Sie für jeden DSCP-Wert (0-63) im Feld Traffic Class den gewünschten Wert zwischen 0 und 7 ein.

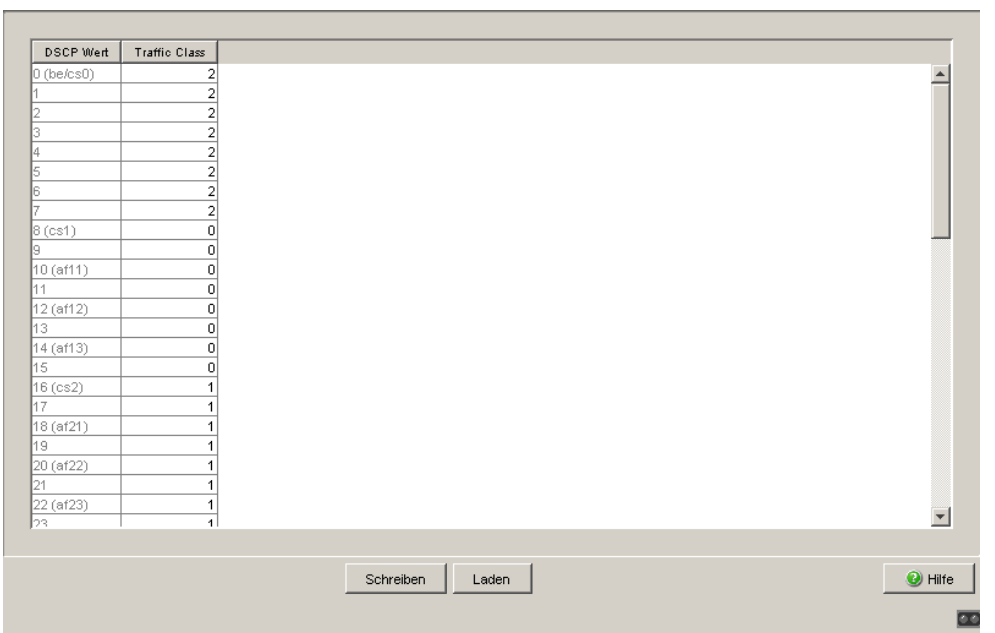


Abb. 59: Tabelle IP DSCP Mapping

Die unterschiedlichen DSCP-Werte bewirken bei dem Gerät ein unterschiedliches Weiterleitungs-Verhalten, das Per-Hop-Behavior (PHB).
PHB-Klassen:

- Class Selector (CS0-CS7): Aus Kompatibilitätsgründen zu TOS/IP-Precedence
- Expedited Forwarding (EF): Premium-Service.
  Geringe Verzögerung, Jitter + Paketverluste (RFC 2598)

- Assured Forwarding (AF): Bietet ein differenziertes Schema zur Behandlung unterschiedlichen Verkehrs (RFC 2597).
- Default Forwarding/Best Effort: Keine besondere Priorisierung.

DSCP-Wert	DSCP-Name	Traffic Class (Voreinstellung)
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

Tab. 118: Abbildung der DSCP-Werte auf die Traffic Classes

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

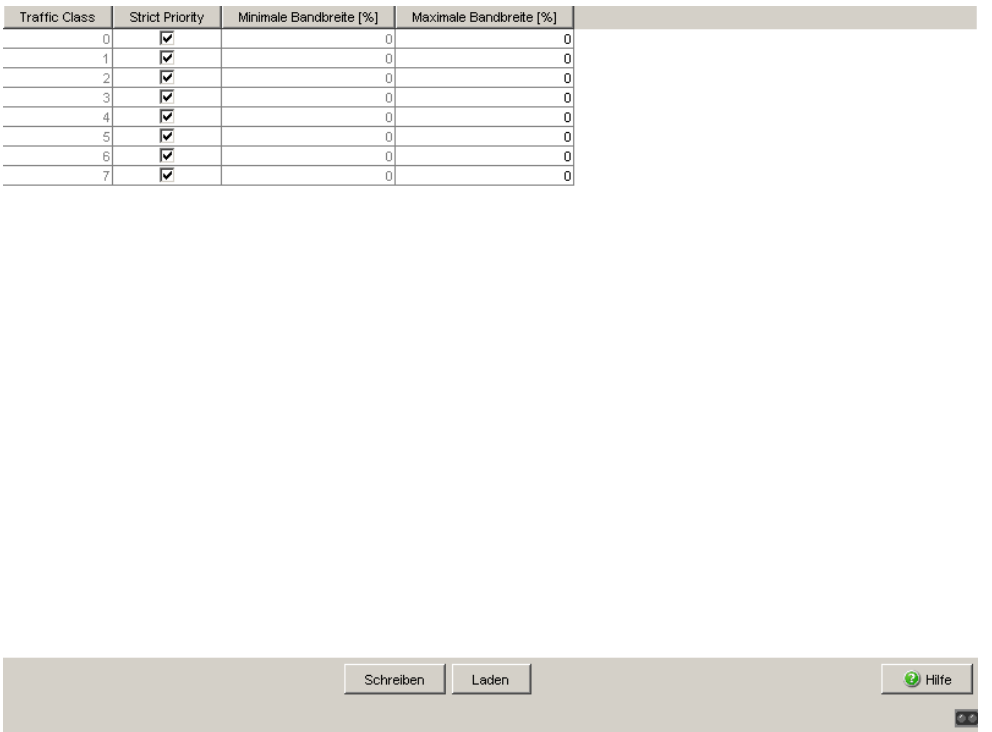
Tab. 119: Schaltflächen

5.5 Queue-Management

Die Queue-Management-Tabelle bietet Ihnen die Möglichkeit, für jede Traffic Class:

- Strict Priority einzuschalten (= Weighted Fair Queuing auszuschalten),
- Strict Priority auszuschalten (= Weighted Fair Queuing einzuschalten),
- für eingeschaltetes Weighted Fair Queuing einen Wert für Minimale Bandbreite einzugeben,
- einen Wert für Maximale Bandbreite einzugeben.

Anmerkung: Ausschalten von Strict Priority für eine Traffic Class bewirkt das Ausschalten von Strict Priority für alle Traffic Classes mit niedrigerer Prioritätsstufe. Einschalten von Strict Priority für eine Traffic Class bewirkt das Einschalten von Strict Priority für alle Traffic Classes mit höherer Prioritätsstufe.



Traffic Class	Strict Priority	Minimale Bandbreite [%]	Maximale Bandbreite [%]
0	☑	0	0
1	☑	0	0
2	☑	0	0
3	☑	0	0
4	☑	0	0
5	☑	0	0
6	☑	0	0
7	☑	0	0

Abb. 60: Tabelle Queue Management

5.5.1 Strict Priority

Bei Strict-Priority vermittelt das Gerät zuerst die Datenpakete mit höherer Verkehrsklasse (höherer Priorität), bevor es ein Datenpaket mit der nächst niedrigeren Verkehrsklasse vermittelt. Ein Datenpaket mit der niedrigsten Verkehrsklasse (niedrigsten Priorität) vermittelt das Gerät demnach erst, wenn keine anderen Datenpakete mehr in der Warteschlange stehen. In ungünstigen Fällen sendet das Gerät Pakete mit niedriger Priorität nie, wenn an diesem Port ein hohes Aufkommen von höherpriorem Verkehr zum Senden ansteht.

Bei zeit- und latenzkritischen Anwendungen, wie z.B. VoIP oder Video, ermöglicht Strict Priority das unmittelbare Senden hochpriorer Daten (siehe auf Seite 224 „Maximale Bandbreite“).

☐ Schalten Sie in der Spalte „Strict Priority“ für die gewünschte Traffic Class die Funktion ein.

5.5.2 Weighted Fair Queuing

Mit Weighted-Fair-Queuing, auch WeightedRoundRobin (WRR) genannt, weist der Anwender jeder Verkehrsklasse eine minimale oder reservierte Bandbreite zu. Dies hat zur Folge, dass das Gerät bei hoher Netzlast auch Datenpakete mit einer niedrigen Priorität vermittelt.

Wenn Sie allen Verkehrsklassen das Weighted-Fair-Queuing zuweisen, dann steht diesen die gesamte Bandbreite des entsprechenden Ports zur Verfügung.

Die Werte für die Gewichtung liegen im Bereich von 0% bis 100% der verfügbaren Bandbreite in Schritten von 5%.

- Die Gewichtung „0“ entspricht der Einstellung „keine Bandbreiten-reservierung“.
- Die Summe der Einzelbandbreiten darf bis zu 100% betragen.

☐ Schalten Sie in der Spalte „Strict Priority“ für die gewünschte Prioritäts-klasse die Funktion ein. Schalten Sie hierzu „Strict Priority“ aus.

☐ Tragen Sie in der Spalte „Minimale Bandbreite“ für die gewünschte Prioritätsklasse einen Wert ein.

5.5.3 Maximale Bandbreite

Die Eingabe einer maximalen Bandbreite bietet Ihnen die Möglichkeit, die Bandbreite jeder Traffic Class auf einen Maximalwert zu begrenzen, unabhängig davon, ob Sie „Weighted Fair Queuing“ oder „Strict Priority“ gewählt haben.

- Weighted Fair Queuing (siehe auf Seite 223 „Weighted Fair Queuing“) setzt voraus, dass die maximale Bandbreite mindestens so groß ist wie die minimale Bandbreite.
- Bei „Strict Priority“ werden einzelne hochpriore Pakete mit geringer Latenz bearbeitet (siehe auf Seite 222 „Strict Priority“). Die Konfiguration der maximalen Bandbreite auf einen Wert kleiner 100% ermöglicht auch bei einer hochprioren Überlast das Vermitteln von Datenpaketen mit niedrigeren Traffic Classes.
  Die Werte für die Gewichtung liegen im Bereich von 0% bis 100% der verfügbaren Bandbreite in Schritten von 5%.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 120: Schaltflächen

6 Routing

Ein Router ist ein Netzknoten zur Vermittlung von Daten auf Schicht 3 des ISO/OSI-Schichtenmodells (Vermittlungsschicht).

Unter Routing finden Sie die Dialoge zur Konfiguration der Routing-Funktion.

6.1 Routing Global

Dieser Dialog bietet Ihnen die Möglichkeit,

- die Routing-Funktion global einzuschalten.
  Voreinstellung: Routing ist abgeschaltet.
- die voreingestellte TTL (Time To Live) anzuzeigen.
  TTL ist ein Wert in einem IP-Datenpaket. Jeder Router, der ein Datenpaket weitervermittelt reduziert diesen Wert um 1. Der Router, der ein Datenpaket mit dem TTL-Wert 1 empfängt, verwirft das Datenpaket und meldet es dem Absender, dessen IP-Quell-Adresse im IP-Paket steht. Sendet der Switch ein eigenes Datenpaket, dann setzt er den TTL-Wert auf diesen angezeigten voreingestellten Wert. Voreinstellung: 64.

Anmerkung: Wenn Sie Routing einschalten, aktiviert das Gerät automatisch das Lernen von MAC-Quelladressen. Ist Routing aktiv, verhindert das Gerät das Abschalten des Adressen-Lernens.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 121: Schaltflächen

6.2 Router-Interfaces konfigurieren

Diese Dialoge bieten Ihnen die Möglichkeit:

- portbasierte und VLAN-basierte Router-Interfaces zu konfigurieren.
- mehrere IP-Adressen pro Router-Interface zu vergeben (Multinetting).

6.2.1 Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, die Router-Interfaces zu konfigurieren. Sie haben die Möglichkeit:

- einem Router-Interface eine IP-Adresse/Netzmaske zuweisen. Weitere Adressen für ein Router-Interface geben Sie im Dialog „Weitere Adressen“ ein (Multinetting).
- ein VLAN-basiertes Router-Interface einrichten.
- die Routing-Funktion pro Routing-Interface ein-/ausschalten.
- die Proxy-ARP-Funktion pro Routing-Interface ein-/ausschalten.
- die Netdirected-Broadcasts-Funktion pro Routing-Interface ein-/ausschalten.
- **Für die Geräte MACH 104 und MACH 1040:**
  Geben Sie für ein ausgewähltes Routing-Interface einen MTU-Wert zu den IP-Paketen an.

Parameter	Bedeutung
Modul	Modul des Switch, auf dem sich der Port befindet. Der Switch verwendet für ein VLAN-basiertes Router-Interface das virtuelle Modul 9.
Port	Port, für den dieser Eintrag gilt.

Tab. 122: Tabelle Router-Interface

Parameter	Bedeutung
Typ	Typ des Router-Interfaces: – Ethernet: Physischer Port – VLAN: VLAN-basiertes Router-Interface
VLAN ID	VLAN-ID des VLAN-basierten Router-Interfaces.
IP-Adresse	IP-Adresse für dieses Router-Interface.
Netzmaske	Netzmaske für dieses Router-Interface
Routing	Ein-/Ausschalten der Routing-Funktion für dieses Router-Interface.
Proxy-ARP	Ein-/Ausschalten der Proxy-ARP-Funktion für dieses Router-Interface.
Netdirected Broadcasts	Ein-/Ausschalten der Netdirected-Broadcasts-Funktion für dieses Router-Interface.
MTU	**Für die Geräte MACH 104 und MACH 1040:** Legt die für das Netzwerk größtmögliche Paketgröße fest. Mögliche Werte: 128..9000. Das Gerät bietet Ihnen die Möglichkeit, bis zu 8 verschiedene MTU-Werte zu konfigurieren.

Tab. 122: Tabelle Router-Interface

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Löschen	Entfernt den markierten Tabelleneintrag.
Assistent	Öffnet den „Assistenten“. Mit dem „Assistenten“ weisen Sie einem Port die zulässigen MAC-Adressen zu.
Hilfe	Öffnet die Online-Hilfe.

Tab. 123: Schaltflächen

Portbasiertes Router-Interface konfigurieren

- ☐ Doppelklicken Sie in der Spalte „IP-Adresse“ in eine Zelle und tragen Sie die IP-Adresse für dieses Router-Interface ein.
- ☐ Doppelklicken Sie in der Spalte „Netzmaske“ in eine Zelle und tragen Sie die Netzmaske für dieses Router-Interface ein.
- ☐ Mit einem Klick in eine Zelle der Spalte „Routing“ schalten Sie die Routing-Funktion für dieses Router-Interface ein.
- ☐ Mit einem Klick in eine Zelle der Spalte „Proxy-ARP“ schalten Sie die Proxy-ARP-Funktion für dieses Router-Interface ein.
- ☐ Mit einem Klick in eine Zelle der Spalte „Netdirected Broadcasts“ schalten Sie die Netdirected-Broadcasts-Funktion für dieses Router-Interface ein.

VLAN-basiertes Router-Interface einrichten

- ☐ Klicken Sie auf „Assistent“ rechts unten.
- ☐ Wählen Sie im Assistenten-Fenster
  – eine Zeile der Tabelle aus, um ein bestehendes VLAN zu konfigurieren oder
  – geben Sie eine VLAN-ID ein für ein neu zu konfigurierendes VLAN.
- ☐ Klicken Sie auf „Weiter“.
- ☐ Im nächsten Assistenten-Fenster geben Sie in "VLAN Name" dem VLAN einen beliebigen Namen.
- ☐ Wählen Sie in der Spalte „Mitglied“ die Ports, die Sie dem VLAN zuordnen möchten.
- ☐ „Untagged“: In dieser Spalte wählen Sie die Ports aus, die Mitglied im VLAN sein sollen und Datenpakete ohne Tag versenden sollen.
- ☐ „Port-VLAN-ID“: Diese Spalte gibt Ihnen nach einem Doppelklick in eine Zelle die Möglichkeit, die Port-VLAN-ID zu ändern. Datenpakete, die dieser Port ohne Tag empfängt, werden durch ein Tag mit dieser Port-VLAN-ID ergänzt.
- ☐ Klicken Sie auf „Weiter“.
- ☐ Geben Sie im Rahmen „Primäre IP-Adresse“ die IP-Adresse dieses Router-Interfaces und die zugehörige Netzmaske ein.
  Der Rahmen „Weitere Adressen/Multinetting“ bietet Ihnen die Möglichkeit, diesem Router-Interface weitere IP-Adressen zuzuweisen. Tragen Sie die IP-Adresse und Netzmaske ein.
  Klicken Sie auf „Hinzufügen“, um die Eingabe in die Tabelle zu übertragen.
  Wählen Sie eine Zeile in der Tabelle aus, um Sie mit „Entfernen“ aus der Tabelle zu löschen.

☐ Klicken Sie auf „Fertig“, um das konfigurierte VLAN-basierte Router-Interface in die Router-Interface-Tabelle zu übernehmen.

Anschließend haben Sie die Möglichkeit, in der Tabelle weitere Parameter für das VLAN-basierte Router-Interface zu konfigurieren, wie bei der Konfiguration von Port-basierten Router-Interfaces.

☐ Mit einem Klick in eine Zelle der Spalte „Routing“ schalten Sie die Routing-Funktion für dieses Router-Interface aus oder ein.

☐ Mit einem Klick in eine Zelle der Spalte „Proxy-ARP“ schalten Sie die Proxy-ARP-Funktion für dieses Router-Interface ein.

☐ Mit einem Klick in eine Zelle der Spalte „Netdirected Broadcasts“ schalten Sie die Netdirected-Broadcasts-Funktion für dieses Router-Interface ein.

Router-Interface löschen

☐ Wählen Sie eine Zeile aus und klicken Sie auf „Löschen“. Damit
– löschen Sie die Zeile, falls es sich um einen VLAN-basierten Eintrag handelt oder
– setzen Sie die Werte in der Zeile zurück, falls es sich um einen port-basierten Eintrag handelt.

Anmerkung: Voraussetzung für das Zurücksetzen der Werte ist das vorhergehende Löschen weiterer Einträge (falls vorhanden) im Dialog „Weitere Adressen“.

6.2.2 Weitere Adressen konfigurieren

Wenn Sie die Multinetting-Funktion benutzen wollen, dann bietet Ihnen dieser Dialog die Möglichkeit, einem Router-Interface weitere (sekundäre) IP-Adressen zuzuweisen.

☐ Wählen Sie mit der linken Maustaste eine Zeile aus, die in der ersten Spalte die Portbezeichnung trägt. Klicken Sie mit der rechten Maustaste in die ausgewählte Zeile und wählen Sie „IP-Adresse hinzufügen“, um dem Router-Interface eine sekundäre IP-Adresse/Netzmaske hinzuzufügen.

Anmerkung: Sie haben die Möglichkeit, bis zu 31 sekundäre IP-Adressen pro Router-Interface und insgesamt bis zu 1.024 sekundäre IP-Adressen pro Router zu konfigurieren.

☐ Um eine bestehende weitere Adresse zu löschen oder zu bearbeiten, wählen Sie die entsprechende Zeile aus, klicken mit der rechten Maustaste in diese Zeile und wählen „Bearbeiten“ oder „Löschen“.

Anmerkung: Voraussetzung für das Löschen ist, dass im Dialog „Router Interfaces“ Routing an diesem Router-Interface eingeschaltet ist.

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
IP-Adresse hinzufügen	Öffnet den Dialog „Erzeugen“. Mit diesem Dialog haben Sie die Möglichkeit,einem Router-Interface eine weitere IP-Adresse hinzuzufügen. Geben Sie dazu in die Felder „IP-Adresse“ und „Netzmaske“ die gewünschten Werte ein. Bestätigen Sie die Eingabe mit einem Klick auf die Schaltfläche „OK“.
IP-Adresse löschen	Mit dieser Schaltfläche haben Sie die Möglichkeit, eine IP-Adresse für ein Router-Interface zu löschen. Markieren Sie dazu eine IP-Adresse in der Liste und klicken Sie auf „IP-Adresse löschen“.
Hilfe	Öffnet die Online-Hilfe.

Tab. 124: Schaltflächen

6.3 ARP

Das Address Resolution Protocol (ARP) ermittelt zu einer IP-Adresse die zugehörige MAC-Adresse.

Dieser Dialog bietet Ihnen die Möglichkeit,
- Parameter für das ARP einzustellen,
- statistische Größen zu betrachten und
- die Tabelle der ARP-Einträge einzusehen, die dynamischen Einträge der ARP-Tabelle zu löschen und statische Einträge zu konfigurieren.

6.3.1 ARP-Parameter einstellen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Aging Time	Mit „Aging Time“ geben Sie die Zeit vor, wie lange ein Eintrag bestehen bleibt, bevor er aus der Tabelle gelöscht wird. Findet innerhalb dieser Zeit ein Datenverkehr mit dem Gerät statt, dann beginnt die Zeitmessung von vorne.	15-21.600 s	1.200 s
Antwortzeit	Mit „Antwortzeit“ geben Sie die Zeit vor, wie lange ARP auf eine Antwort wartet, bevor es die Anfrage als gescheitert betrachtet	1-10	1
Wiederholungsversuche	Mit „Wiederholungsversuche“ geben Sie die Anzahl vor, wie oft ARP eine gescheiterte Anfrage wiederholt, bevor ARP die Anfrage an diese Adresse einstellt.	0-10	4

Tab. 125: ARP-Parameter

Parameter	Bedeutung	Wertebereich	Voreinstellung
Speichergröße	Mit „Speichergröße“ haben Sie die Möglichkeit, die maximale Anzahl an Einträgen in die Tabelle zu begrenzen. Ist die maximale Anzahl erreicht, dann löscht ARP den jeweils ältesten Eintrag.	PowerMICE: 288-2.208 MACH 1040: 284-3.328 MACH 4000: 308-2.228 MACH 4000 24/48G: 308-2.228, erweiterbar via CLI auf 3.868	Maximum
Dynamische Erneuerung	Ist „Dynamische Erneuerung“ eingeschaltet, dann startet ARP eine erneute Anfrage an ein Gerät, dessen Eintrag die Aging Time überschritten hat. Wird diese Anfrage nicht beantwortet, dann entfernt der Switch den Eintrag aus der Tabelle.	ein/aus	ein
Gezieltes Lernen	In der Voreinstellung lernt der Router ARP-Einträge passiv. Das bedeutet, dass der Router alle ARP-Requests empfängt und automatisch die IP/MAC-Adresszuordnung des sendenden Gerätes lernt. Durch dieses automatische Lernen aller angeschlossenen Geräte entfallen zeitintensive ARP-Anfragen, falls der Router ein Datenpaket an ein unbekanntes Gerät senden muss. Hierbei werden die ARP-Tabellen eventuell auch mit unnötigen ARP-Einträgen gefüllt, z.B. von Geräten die nur lokal kommunizieren möchten. Wird „Gezieltes Lernen“ aktiviert, lernt der Router nur dann die IP/MAC-Adresszuordnung der Quelle, wenn der ARP-Request an den Router selbst gerichtet war, d.h. wenn explizit nach der Adresse des Routers gefragt wurde.	ein/aus	aus

Tab. 125: ARP-Parameter

6.3.2 Anzeige ARP-Statistik

Parameter	Bedeutung
Anzahl aktueller Einträge	Momentane Anzahl der ARP-Einträge in der ARP-Tabelle
Spitzenwert	Spitzenwert der ARP-Einträge in der ARP-Tabelle
Anzahl aktueller statischer Einträge	Momentane Anzahl der statischen ARP-Einträge in der ARP-Tabelle
Max. Anzahl statischer Einträge	Maximal mögliche Anzahl statischer ARP-Einträge in der ARP-Tabelle

Tab. 126: ARP-Statistik

6.3.3 Anzeige ARP-Tabelle

Parameter	Bedeutung
Modul	Modul des Routers
Port	Port, für den dieser Eintrag gilt.
IP-Adresse	IP-Adresse eines Gerätes, das auf eine ARP-Anfrage an diesem Port geantwortet hat.
MAC-Adresse	MAC-Adresse eines Gerätes, das auf eine ARP-Anfrage an diesem Port geantwortet hat.
Typ	Art des Eintrags: – static: statischer ARP-Eintrag, der auch nach dem Löschen der ARP-Tabelle erhalten bleibt. – dynamic: dynamischer Eintrag, der nach „Aging Time“ aus der Tabelle gelöscht wird, falls während dieser Zeit von diesem Gerät keine Daten empfangen werden. – local: IP- und MAC-Adresse des eigenen Ports

Tab. 127: ARP-Tabelle

6.3.4 ARP-Tabelle bearbeiten

Dynamische Einträge löschen

Mit einem Klick auf „Zurücksetzen“ löschen Sie die dynamischen Einträge aus der ARP-Tabelle.

Statische Einträge bearbeiten

Mit Hilfe eines Assistenten können Sie statische Einträge hinzufügen, bearbeiten und löschen.

Voraussetzungen für das Hinzufügen statischer Einträge sind:

- Ein Router-Interface ist konfiguriert, liegt in dem Netz des statischen Eintrags und die Routing-Funktion ist eingeschaltet (siehe auf Seite 227 „Konfiguration“).
- Das Router-Interface hat an mindestens einem Port eine Verbindung.
- Die Routing-Funktion ist global eingeschaltet (siehe auf Seite 226 „Routing Global“).

☐ Klicken Sie auf Assistent, um das Assistentenfenster zu öffnen.
☐ Geben Sie die IP-Adresse in der Form 0.0.0.0 und die MAC-Adresse in der Form 00:00:00:00:00:00 für einen neuen Eintrag ein und klicken Sie auf „Übernehmen“, um einen neuen Eintrag zu erzeugen.
☐ Wählen Sie einen Eintrag aus und klicken Sie auf „Löschen“, um diesen Eintrag zu löschen.
☐ Klicken Sie auf „Fertig“ um das Bearbeiten zu beenden und die Änderungen in die ARP-Tabelle zu übernehmen.
☐ Klicken Sie auf „Abbrechen“, um das Bearbeiten zu beenden und die Änderungen zu verwerfen.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Löschen	Entfernt den markierten Tabelleneintrag.
Zurücksetzen	Löscht die dynamischen Einträge aus der ARP-Tabelle.
Assistent	Öffnet den „Assistenten“. Mit dem „Assistenten“ weisen Sie einem Port die zulässigen MAC-Adressen zu.
Hilfe	Öffnet die Online-Hilfe.

Tab. 128: Schaltflächen

6.4 Konfiguration Router-Discovery

ICMP-Router-Discovery beschreibt ein Verfahren, mögliche Router im Netz zur Vermittlung ausfindig zu machen. Der Switch unterstützt dieses Verfahren, indem er bei aktivierter Funktion Anwesenheitsnachrichten übermittelt.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Modul	Modul des Routers	geräteabhängig	–
Port	Port des Moduls	geräteabhängig	–
VLAN ID	VLAN-Zugehörigkeit des Ports	geräteabhängig	
Advertise Mode	Aktivieren/Deaktivieren der Router Discovery-Funktion an diesem Port	ein/aus	aus
Advertise Address	Ziel zum Versenden der Anwesenheits-nachrichten.	Multicast/ Broadcast	Multicast

Tab. 129: Konfiguration Router-Discovery

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 130: Schaltflächen

6.5 RIP

Das Routing Information Protocol (RIP) ist ein Routing-Protokoll auf Basis des Distanzvektor-Algorithmus. Es dient der dynamischen Erstellung der Routingtabelle von Routern.

6.5.1 Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, generelle Einstellungen sowie Einstellungen pro Port für das Routing Information Protocol vorzunehmen.

Generelle Einstellungen

- Funktion: Ein-/Ausschalten der RIP-Funktion. Standardwert: Aus
- Auto-Summary-Mode: Ein-/Ausschalten des Auto-Summary-Mode. Im eingeschalteten Zustand fasst RIP, falls möglich, mehrere Subnetze zusammen, um den Umfang der Routing-Informationen in den Routingtabellen zu reduzieren. Standardwert: markiert
- Host-Routes-Accept-Mode: Ein-/Ausschalten des Host-Routes-Accept-Mode. Im eingeschalteten Zustand erlaubt RIP den Eintrag von Routen mit einer 32-Bit Netzmaske. Standardwert: markiert

- Propagiere Default-Route: Ein-/Ausschalten des Propagierens der Default-Route. Standardwert: unmarkiert
- Update-Intervall: der Zeitabstand mit dem der Router den gesamten Inhalt der Routingtabelle an die RIP-Nachbarn übermittelt. Sie können Werte im Bereich zwischen 1 und 1.000 Sekunden einstellen. Werte kleiner als 10 Sekunden führen bei größeren Netzen zu einer erhöhten Netzlast. Standardwert: 30 s
  Der Router setzt die anderen RIP-Timer entsprechend:
  – Timeout: 6 x Update-Intervall
  – Garbage collection: 10 x Update-Intervall

Update-Intervall	Maximale Anzahl der Routen
1 s	250
5 s	600
60 s	1.000

Tab. 131: Empfohlene Einstellung für das Update-Intervall

- Split-Horizon: Wählen Sie denSplit-Horizon-Modus. Der Split-Horizon-Modus dient dazu, das Count-to-Infinity-Problem zu umgehen. Standardwert: Split-Horizon ausschalten (Lieferzustand).
  – simple: Simple-Split-Horizon läßt beim Versenden der Routingtabelle an den Nachbarn die von diesem Nachbarn gelernten Einträge weg.
  – poisonReverse: PoisonReverse-Split-Horizon versendet die Routingtabelle an den Nachbarn mit den von diesem Nachbarn gelernten Einträgen, teilt diesen aber die Metrik Infinity zu.
- Default Metric: Voreingestellte Metrik für eine Route, die RIP von einem anderen Protokoll übernimmt. Diese Metrik kommt zum Zuge, wenn im Dialog (siehe auf Seite 241 „Route Distribution“) auf für das entsprechende Protokoll keine Metrik konfiguriert wurde. Standardwert: 0
  Wert 0 bedeutet keine Vorgabe für die Default Metric. In diesem Fall verwendet RIP die Metrik 1.

Einstellungen pro Port

Parameter	Bedeutung
Port	Port des Moduls des Switch
VLAN-ID	VLAN-Zugehörigkeit des Ports Standardwert: -
Funktion	Ein-/Ausschalten der RIP-Funktion an diesem Port. Standardwert: unmarkiert
Sendeversion	RIP-Version, die der Router an diesem Port benutzt, um RIP-Informationen zu senden. Standardwert: ripVersion2 – doNotSend: RIP versendet keine Routing-Informationen. – ripVersion1: RIP versendet Informationen mit Version 1 als Broadcast. – rip1Compatible: RIP versendet Informationen mit Version 2 als Broadcast. – ripVersion2: RIP versendet Informationen mit Version 2 als Multicast.
Empfangsversion	RIP-Version, die der Switch empfangsseitig akzeptiert. Standardwert: rip1OrRip2 – rip1: RIP akzeptiert RIP-V1-Pakete. – rip2: RIP akzeptiert RIP-V1-Pakete. – rip1OrRip2: RIP akzeptiert RIP-V1 und V2-Pakete. – doNotReceive: RIP lässt keinen Empfang von RIP-Informationen zu.
Authentifizierung	Die Art der angewendeten Authentifizierung: – “noAuthentication”: Austausch von RIP-Informationen ohne Authentifizierung. – “simplePassword”: Austausch von RIP-Informationen mit Klartext-Passwort-Authentifizierung. – “md5”: Austausch von RIP-Informationen mit Klartext-Passwort-Authentifizierung. Standardwert: noAuthentication
Schlüssel	Passwort für Authentifizierung. Zur Kommunikation benötigt der gegenüberliegende Port die gleichen Authentifizierungseinstellungen.
Schlüssel-ID	Passwortidentifikationsnummer für Authentifizierung. Zur Kommunikation benötigt der gegenüberliegende Port die gleiche Schlüssel-ID.

Tab. 132: RIP-Konfigurationstabelle

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 133: Schaltflächen

6.5.2 Route Distribution

Routenverteilung beschreibt, wie RIP Routen, die RIP von anderen Protokollen übernommen hat, an andere RIP-Router propagiert.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Quelle	Quelle, von der RIP Routinginformationen übernimmt: – connected: Die Route weist auf ein Subnetz, das direkt am Interface angeschlossen ist. – static: Die Route steht in der statischen Routingtabelle. – ospf: Die Route kommt von OSPF.	`connected`, `static`, `ospf`	
Modus	Mit Modus wählen Sie aus, ob RIP Routen von diesen Quellen übernehmen soll.		
Metric	In dieser Spalte geben Sie die Metrik ein, die RIP den Routen aus der Quelle zuweist. Ist der Wert 0 eingetragen, dann verwendet RIP den Wert, der unter „Default Metric“ (siehe auf Seite 238 „Generelle Einstellungen“) eingetragen ist.		
Match internal	Aktiv: Interne OSPF Routen (OSPF Intra, OSPF Inter) werden in RIP übernommen	`Aktiv`, `Inaktiv`	`Aktiv`

Tab. 134: Route Distribution-Tabelle

Parameter	Bedeutung	Wertebereich	Voreinstellung
Match external 1	Aktiv: Externe OSPF Routen vom Metrik Typ 1 (OSPF Ext T1) werden in RIP übernommen.	`Aktiv, Inaktiv`	`Inaktiv`
Match external 2	Aktiv: Externe OSPF Routen vom Metrik Typ 2 (OSPF Ext T2) werden in RIP übernommen.	`Aktiv, Inaktiv`	`Inaktiv`
Match NSSA external 1	Aktiv: Externe OSPF Routen vom Metrik Typ 1 aus einer NSSA (Not so Stubby Area) werden in RIP übernommen .	`Aktiv, Inaktiv`	`Inaktiv`
Match NSSA external 2	Aktiv: Externe OSPF Routen vom Metrik Typ 2 aus einer NSSA (Not so Stubby Area) werden in RIP übernommen.	`Aktiv, Inaktiv`	`Inaktiv`

Tab. 134: Route Distribution-Tabelle

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 135: Schaltflächen

6.5.3 Statistik

Das RIP-Statistik-Fenster zeigt Zählerstände von Zählern an, die Routing-relevante Ereignisse zählen.

Parameter	Bedeutung
Globale Routenänderungen	Anzahl der durch RIP verursachten Routenänderungen in der Routingtabelle
Globale Anfragen	Anzahl der gesendeten Antworten auf Anfragen anderer Systeme
Modul	Modul des Routers
Port	Port, für den dieser Eintrag gilt
Empfangene verworfene Pakete	Anzahl der empfangenen Routing-Datenpakete, die der Switch aus unterschiedlichen Gründen verworfen hat, z.B. andere Protokollversion, unbekannter Kommandotyp.
Empfangene ignorierte Routen	Anzahl der empfangenen Routing-Informationen, die der Router ignoriert, weil das Eingabeformat ungültig ist.
Gesendete Updates	Anzahl der gesendeten Routingtabellen mit geänderten Routing-Einträgen.

Tab. 136: RIP-Statistiktabelle

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 137: Schaltflächen

6.6 Routingtabelle

Die Routingtabelle enthält alle dem Gerät bekannten Routen.

Bestehen mehrere Routen zu einem Ziel, dann wählt der Router die Route mit dem niedrigsten Wert in der Spalte Metrik.

Unter Routingtabelle finden Sie die Dialoge:

- Aktuell
- Statisch
- Präferenzen

6.6.1 Aktuell

Die aktuelle Routingtabelle enthält alle Routen, zu denen im Moment eine gültige Verbindung besteht.

Parameter	Bedeutung
Modul	Modul des Routers
Port	Router-Interface
Netzadresse	IP-Adresse des Zielnetzes
Netzmaske	Netzmaske zur IP-Adresse des Zielnetzes
Next-Hop IP-Adresse	IP-Adresse des nächsten Routers auf dem Weg in das Zielnetz.
Typ	Zeigt die Art des Eintrags an: – local, das Ziel ist direkt über dieses Router-Interface erreichbar. – remote, der Next Hop ist ein Router

Tab. 138: Aktuelle Routingtabelle

Parameter	Bedeutung
Protokoll	Zeigt an, wie der Eintrag zustande kam: – local, eigenes Router-Interface – netmgmt, statische Route – ospf – rip
Metrik	Metrik dieser Route. Die Route mit dem kleinsten Wert für die Metrik wählt der Switch zur Vermittlung. Besitzen mehrere Routing-Einträge mit identischer Netzadresse/Netzmaske, jedoch mit unterschiedlicher Next Hop IP-Adresse, die gleiche Metrik, dann trägt der Switch all diese in die Routingtabelle ein (ECMP, equal cost multiple path). Der Switch unterstützt bis zu vier ECMP-Routen.

Tab. 138: Aktuelle Routingtabelle

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 139: Schaltflächen

6.6.2 Statisch

Die statische Routingtabelle gibt Ihnen die Möglichkeit, statische Routen einzugeben.
Im Lieferzustand sind die Präferenzen so eingestellt, dass der Switch statisch eingetragenen Routen gegenüber den dynamisch eingetragenen Routen den Vorzug gibt (siehe auf Seite 247 „Präferenzen“).

☐ Klicken Sie auf „Eintrag erzeugen“, um ein Fenster für die Eingabe einer neuen Zeile in der Tabelle zu öffnen.
Nach der Eingabe
– der IP-Adresse des Zielnetzes
– der Netzmaske zur IP-Adresse des Zielnetzes,
– IP-Adresse des nächsten Routers auf dem Weg in das Zielnetz
klicken Sie auf „OK“, um die Eingabe in die Tabelle zu übertragen.
Sie können den Eintrag für die Präferenz direkt in der Tabelle ändern.

☐ Um eine Zeile zu löschen, wählen Sie die Zeile aus und klicken Sie auf „Eintrag löschen.

Parameter	Bedeutung
Zielnetz	IP-Adresse des Zielnetzes
Zielnetzmaske	Netzmaske zur IP-Adresse des Zielnetzes
Next Hop	IP-Adresse des nächsten Routers auf dem Weg in das Zielnetz.
Präferenz	Wichtigkeit dieses Eintrags, mit dem diese Route bei der Wahl der besten Route berücksichtigt wird. Als Voreinstellung übernimmt der Dialog den Wert aus der Tabelle im Präferenz-Dialog (siehe auf Seite 247 „Präferenzen“). Eine Präferenz mit dem Wert 255 bedeutet „nicht erreichbar“, d.h. die Route wird nicht für die Vermittlung verwendet
Track-ID	Identifikationsnummer des Tracking-Objektes, bei dessen Wechsel in den Zustand `down` das Gerät diese Route aus der aktuellen Routingtabelle löscht (siehe auf Seite 244 „Aktuell“).

Tab. 140: Tabelle für statische Routen

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 141: Schaltflächen

6.6.3 Präferenzen

Dieser Dialog bietet Ihnen die Möglichkeit, eine Voreinstellung für die Wichtigkeit (administrative Distanz) eines Eintrages in die Routingtabelle zu treffen. Je kleiner der Wert ist, desto wichtiger ist der Eintrag. Einem neuen Eintrag in die Routingtabelle ordnet der Router automatisch die Wichtigkeit zu, die hier in der Präferenzliste steht.

Anmerkung: Weisen Sie „connected“ stets den kleinsten Wert für administrative Distanz zu.

Quelle	Bedeutung	Voreinstellung
connected	Eintrag für direkt am Switch angeschlossene Routen/Interfaces.	0
static	Eintrag für Routen aus der statischen Routingtabelle.	1
ospf-intra	Eintrag für Routen von OSPF innerhalb einer Area	8
ospf-inter	Eintrag für Routen von OSPF zwischen Areas	10

Tab. 142: Präferenzlisten

Quelle	Bedeutung	Voreinstellung
ospf-ext-t1	Diese Routen wurden von einem Autonomous System Boundary Router (ASBR) in die OSPF-Area importiert. Diese Routen benutzen die Kosten in Bezug auf die Verbindung zwischen dem ASBR und diesem Switch als Teil der Routenkosten.	13
ospf-ext-t2	Diese Routen wurden von einem Autonomous System Boundary Router (ASBR) in die OSPF-Area importiert. Diese Routen benutzen nicht die Kosten in Bezug auf die Verbindung zwischen dem ASBR und diesem Switch als Teil der Routenkosten.	150
rip	Eintrag für Routen vom Routing Information Protokoll.	15

Tab. 142: Präferenzlisten

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 143: Schaltflächen

6.7 Tracking

Die Tracking-Funktion bietet Ihnen die Möglichkeit, bestimmte Objekte wie z.B. die Verfügbarkeit eines Interfaces zu überwachen.
Das Besondere an dieser Funktion ist die Weiterleitung einer Objekt-Zustandsänderung an eine Anwendung wie z.B. VRRP, die sich zuvor als Interessent für diese Information registriert hat.

6.7.1 Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, ein neues Tracking-Objekt anzulegen, ein bestehendes Tracking-Objekt zu ändern oder zu löschen.

Das Gerät bietet Tracking-Objekte des Typs:
- Interface
- Ping
- Logik

Das Gerät unterstützt bis zu 256 Tracking-Objekte (Track ID: 1 bis 256).

Parameter	Bedeutung
Track-ID	Identifikationsnummer dieses Tracking-Objektes.
Aktiv	Aktivieren/Deaktivieren dieses Tracking-Objektes.
Modul.Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.
Link-Up-Verzögerung [s]	Ein Interface-Objekt nimmt den Zustand `up` an, sobald die physikalische Verbindung länger als die Verzögerungszeit anhält.
Link-Down-Verzögerung [s]	Ein Interface-Objekt nimmt den Zustand `down` an, sobald die physikalische Verbindungsunterbrechung länger als die Verzögerungszeit anhält.

Tab. 144: Parameter eines Tracking-Objektes des Typs Interface

Parameter	Bedeutung
Änderungsnachricht senden	Aktivieren/Deaktivieren des Versendens eines Alarms bei einer Änderung des Status dieses Tracking-Objektes.
Status	Anzeige des Status dieses Tracking-Objektes.
Anzahl Änderungen	Anzeige der Anzahl der Statuswechsel.
Zeit seit letzter Änderung	Anzeige der Zeit, die seit dem letzten Statuswechsel verstrichen ist.

Tab. 144: Parameter eines Tracking-Objektes des Typs Interface

Parameter	Bedeutung
Track-ID	Identifikationsnummer dieses Tracking-Objektes.
Aktiv	Aktivieren/Deaktivieren dieses Tracking-Objektes.
IP-Adresse	IP-Adresse des mit Ping zu überwachenden Gerätes.
Modul.Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port 1 des 2. Moduls. Wenn Sie „auto“ auswählen, benutzt das Gerät automatisch das Interface mit der besten Route.
Ping-Intervall [s]	Zeitlicher Abstand zwischen den Ping-Anforderungen in Sekunden.
Ausbleibende Ping-Antworten	Anzahl ausbleibender Ping-Antworten, die zum Status `down` führen.
Ankommende Ping-Antworten	Anzahl aufeinanderfolgend empfangener Ping-Antworten, die zum Status `up` führen.
Ping-Timeout [ms]	Die Zeit, die das Gerät auf eine Ping-Antwort wartet, bevor das Gerät die Ping-Antwort als „Ausbleibende-Ping-Antwort“ wertet.
Ping-TTL	Der TTL-Wert (Time To Live) im IP-Paket-Header, mit dem das Gerät die Ping-Anforderungen sendet.
Änderungsnachricht senden	Aktivieren/Deaktivieren des Versendens eines Alarms bei einer Änderung des Status dieses Tracking-Objektes.
Status	Anzeige des Status dieses Tracking-Objektes.
Anzahl Änderungen	Anzeige der Anzahl der Statuswechsel.
Zeit seit letzter Änderung	Anzeige der Zeit, die seit dem letzten Statuswechsel verstrichen ist.

Tab. 145: Parameter eines Tracking-Objektes des Typs Ping

Parameter	Bedeutung
Track-ID	Identifikationsnummer dieses Tracking-Objektes.
Aktiv	Aktivieren/Deaktivieren dieses Tracking-Objektes.

Tab. 146: Parameter eines Tracking-Objektes des Typs Logisch

Parameter	Bedeutung
Operator	Operator zum Verknüpfen von bis zu 8 Operanden (Tracking-Objekten). Ist das Ergebnis der Verknüpfung wahr, dann ist der Status dieses Tracking-Objektes `up`.
Operand 1 bis n	Operanden für die Verknüpfung mit dem Operator. Die Operanden wählen Sie aus bestehenden Tracking-Objekten aus.
Änderungsnachricht senden	Aktivieren/Deaktivieren des Versendens eines Alarms bei einer Änderung des Status dieses Tracking-Objektes.
Status	Anzeige des Status dieses Tracking-Objektes.
Anzahl Änderungen	Anzeige der Anzahl der Statuswechsel.
Zeit seit letzter Änderung	Anzeige der Zeit, die seit dem letzten Statuswechsel verstrichen ist.

Tab. 146: Parameter eines Tracking-Objektes des Typs Logisch

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Löschen	Entfernt den markierten Tabelleneintrag.
Assistent	Öffnet den „Assistent“. Der „Assistent“ unterstützt Sie beim Erstellen neuer Tabelleneinträge.
Zurück	Zeigt die vorherige Seite wieder an. Änderungen gehen dabei verloren.
Weiter	Übernimmt die Änderungen und öffnet die nächste Seite.
Fertig	Übernimmt die Änderungen und schließt die Konfiguration ab.
Abbrechen	Beendet den Assistenten. Änderungen gehen dabei verloren.
Hilfe	Öffnet die Online-Hilfe.

Tab. 147: Schaltflächen

6.7.2 Applikationen

Diese Tabelle zeigt Ihnen die Tracking-Objekte an, bei denen Anwendungen (Applikationen) registriert sind.

- VRRP registrieren Sie für ein Tracking-Objekt im Dialog `Redundanz:VRRP:Konfiguration` (siehe auf Seite 319 „VRRP-Instanz-Einstellungen“).
- Statische Routen registrieren Sie für ein Tracking-Objekt im Dialog `Routing:Routing-Tabelle:Statisch` (siehe auf Seite 246 „Statisch“).
- Logische Verknüpfungen von Tracking-Objekten registriert das Gerät automatisch für ein Tracking-Objekt.

Parameter	Wert
Track ID	Identifikationsnummer des Tracking-Objektes.
Applikation	Anwendung, die für dieses Tracking-Objekt registriert ist.
Anzahl Änderungen	Anzahl der Zustandsänderungen dieses Tracking-Objektes.
Zeit seit letzter Änderung	Zeit, die seit der letzten Zustandsänderung dieses Tracking-Objektes verstrichen ist.

Tab. 148: Für Tracking-Objekte registrierte Anwendungen

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 149: Schaltflächen

7 Redundanz

Unter Redundanz finden Sie die Dialoge und Ansichten zur Konfiguration und Überwachung der Redundanzfunktionen:

- Link-Aggregation
- Ring-Redundanz
- Ring-/Netzkopplung
- Spanning Tree
- VRRP/HiVRRP

Anmerkung: Das Dokument „Anwender-Handbuch Redundanzkonfiguration“ enthält ausführliche Informationen, die Sie zur Auswahl des geeigneten Redundanzverfahrens und dessen Konfiguration benötigen.

7.1 Link-Aggregation

Dieser Dialog bietet Ihnen die Möglichkeit:
- Eine Übersicht aller vorhandenen Link-Aggregationen anzuzeigen,
- Link-Aggregationen anzulegen,
- Link-Aggregationen zu konfigurieren,
- Statische Link-Aggregationen zuzulassen, und
- Link-Aggregationen zu löschen.

Das LACP (Link-Aggregation Control Protocol nach IEEE 802.3ad) ist ein Netzwerkprotokoll zur dynamischen Bündelung von physikalischen Netzverbindungen. Zur Datenübertragung steht die volle Bandbreite aller Verbindungsleitungen zur Verfügung. Im Falle des Ausfalls einer Verbindung übernehmen die verbleibenden Verbindungen den gesamten Datenverkehr (Redundanz). Die Lastverteilung zwischen den Verbindungsleitungen erfolgt automatisch.
Eine Link-Aggregation konfigurieren Sie, indem Sie zwischen 2 Geräten mindestens 2 vorhandene, parallele redundante Verbindungsleitungen (Leitungsbündel, engl.: Trunk) zu einer logischen Verbindung zusammengefassen. Mit Link-Aggregation können Sie max. 8 (optimal bis zu 4) Verbindungsleitungen zwischen Geräten zu einem Trunk zusammenfassen. Sie können in beliebiger Kombination Twisted-Pair- oder LWL-Kabel als Verbindungsleitungen eines Trunks verwenden. Konfigurieren Sie alle Verbindungen so, dass die Datenrate und die Duplexeinstellungen der beteiligten Ports übereinstimmen.
Von einem Gerät können maximal 7 Trunks ausgehen.

Anmerkung: Schließen Sie eine Kombination von Link-Aggregation mit folgenden Redundanzverfahren aus:
- Netz-/Ringkopplung
- MRP-Ring
- Sub-Ring

Anmerkung: Zu einer Link-Aggregation gehören genau 2 Geräte. Konfigurieren Sie die Link-Aggregation jeweils an beiden beteiligten Geräten. Schließen Sie während der Konfigurationsphase höchstens eine Verbindungsleitung zwischen den Geräten an. Dadurch vermeiden Sie Schleifen (Loops).

Parameter	Bedeutung
Statische Link-Aggregationen zulassen	Wenn Sie Geräte über mehrere Leitungen verbinden, verhindert das Link-Aggregation-Control-Protokoll (LACP) selbstständig die Entstehung von Loops. Wählen Sie `Statische Link-Aggregation zulassen`, wenn das Partner-Gerät LACP nicht unterstützt (z.B. MACH 3000).
Trunk-Port	Diese Spalte zeigt Ihnen den Index an, unter dem das Gerät eine Link-Aggregation als virtuellen Port (8.x) angelegt hat.
Geräte-Ports	Aufzählung der physikalischen Ports, die Mitglied der Link-Aggregation sind.
Name	Hier können Sie der Link-Aggregation einen Namen zuzuweisen.
Aktiv	Diese Spalte ermöglicht Ihnen, eine eingerichtete Link-Aggregation zu aktivieren/deaktivieren.
Link Trap	Wählen Sie „Link-Trap“, dann generiert das Gerät einen Alarm, sobald alle Verbindungen der Link-Aggregation unterbrochen sind.
STP-Modus	In der Spalte „STP-Modus“ wählen Sie `on`, wenn Sie die Link-Aggregation in einen Spanning-Tree eingebunden haben, `off`, wenn nicht.
Typ	`- manuell` Das Partnergerät unterstützt kein LACP und Sie haben „Statische Link-Aggregation zulassen“ angewählt. `- dynamic` Beide Geräte unterstützen LACP und Sie haben „Statische Link-Aggregation zulassen“ nicht angewählt. **Hinweis:** Bestehen die Mehrfachverbindungen zwischen Geräten, die alle LACP unterstützen, zeigt das Gerät `dynamic` an auch wenn „Statische Link-Aggregation zulassen“ angewählt wurde. In diesem Fall schalten die Geräte automatisch auf dynamic um.

Tab. 150: Link-Aggregation

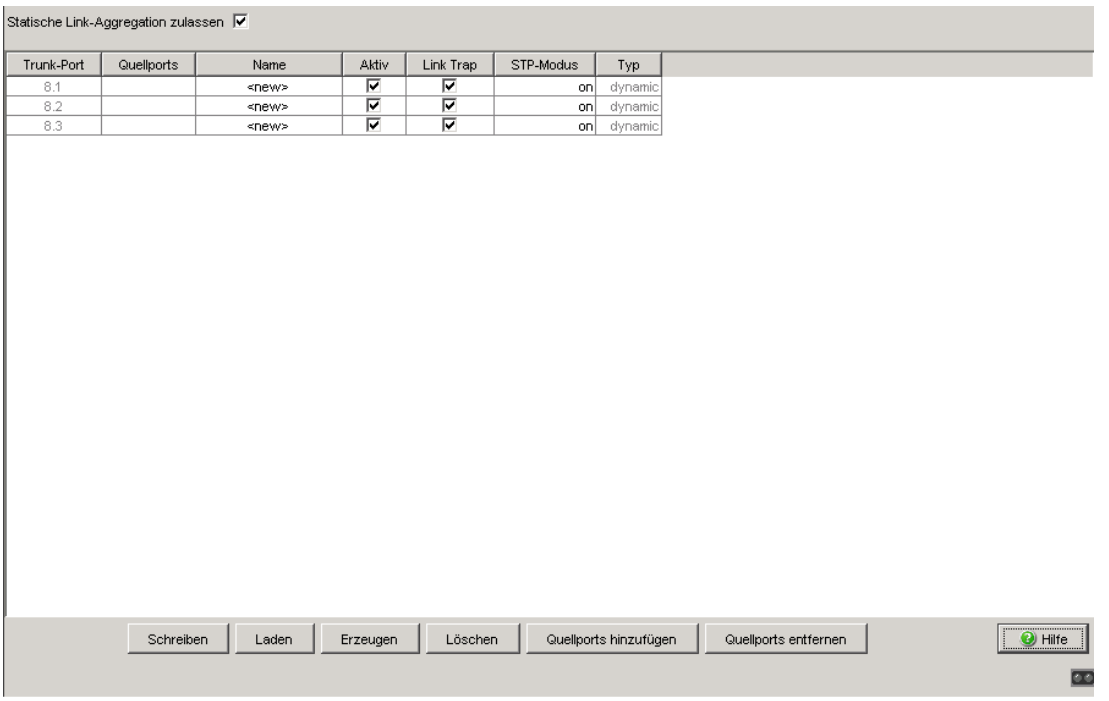


Abb. 61: Link-Aggregation einstellen

Anmerkung: Für PowerMICE und MACH 4000
Zur Erhöhung der Verfügbarkeit besonders wichtiger Verbindungen können Sie HIPER-Ring (siehe auf Seite 258 „Ring-Redundanz“) und Link-Aggregation kombinieren.
Wenn Sie eine Link-Aggregation in einem HIPER-Ring verwenden wollen, konfigurieren Sie zuerst die Link-Aggregation und danach den HIPER-Ring. Geben Sie im HIPER-Ring-Dialog als Wert für Modul und Port den Index der gewünschten Link-Aggregation an (8.x). Beachten Sie, dass der jeweilige Ring-Port zur gewählten Link-Aggregation dazugehört.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Geräte-Ports hinzufügen	Öffnet das Fenster „Hinzuzufügende Ports auswählen“, welches die verfügbaren Ports anzeigt. Um einen Port vom Trunk hinzuzufügen, klicken Sie auf „OK“.
Geräte-Ports entfernen	Öffnet eine Liste der Ports, die in dem Trunk verfügbar sind. Um einen Port vom Trunk zu entfernen, klicken Sie auf „OK“.
OK	Führt die ausgewählte Aktion durch.
Abbrechen	Beendet die ausgewählte Aktion.
Hilfe	Öffnet die Online-Hilfe.

Tab. 151: Schaltflächen

7.2 Ring-Redundanz

Das Konzept der Ring-Redundanz ermöglicht den Aufbau hochverfügbarer, ringförmiger Netzstrukturen.

Beim Ausfall einer Teilstrecke wandelt sich die Ringstruktur eines

- HIPER-(**HI**GH **PE**RFORMANCE **R**EDUNDANCY) Rings mit bis zu 50 Geräten im typischen Fall innerhalb von 80 ms (einstellbar: Standard/Beschleunigt) wieder in eine Linienstruktur zurück.
- MRP (**M**edia **R**edundancy **P**rotocol)-Rings (IEC 62439) bei bis zu 50 Geräten im typischen Fall innerhalb von 80 ms (einstellbar maximal 200 ms/500 ms) wieder in eine Linienstruktur zurück.

Mit Hilfe der **R**ing-**M**anager- (RM-) Funktion eines Gerätes können Sie beide Enden eines Backbones in Linienstruktur zu einem redundanten Ring schließen.

- Innerhalb eines HIPER-Ringes können Sie eine beliebige Mischung der folgenden Geräte einsetzen:
  - RS2-./.
  - RS2-16M
  - RS2-4R
  - RS20, RS30, RS40
  - RSR20, RSR30
  - OCTOPUS
  - MICE
  - MS20, MS30
  - PowerMICE
  - MACH 100

  - MACH 1000
  - MACH 3000
  - MACH 4000
- Innerhalb eines MRP-Rings können Sie Geräte einsetzen, die das MRP-Protokol nach IEC 62439 unterstützen.
- Innerhalb eines Fast HIPER-Ringes können Sie eine beliebige Mischung der folgenden Geräte einsetzen:
  - RSR20, RSR30
  - MACH 1000

Der Ring-Redundanz-Dialog bietet Ihnen abhängig vom Gerätemodell die Möglichkeit:

- Zwischen den verfügbaren Ring-Redundanz-Versionen zu wählen und zu wechseln,
- eine Übersicht der aktuellen Ring-Redundanz Konfiguration anzuzeigen,
- neue Ring-Redundanzen anzulegen,
- vorhandene Ring-Redundanzen zu konfigurieren,
- die Ring-Manager-Funktion ein-/auszuschalten,
- Ringinformationen zu erhalten, und
- die Ring-Redundanz zu löschen.

Anmerkung: Sie können auf einem Gerät zur gleichen Zeit ausschließlich eine Methode der Ring-Redundanz einschalten. Deaktivieren Sie beim Wechsel zu einer anderen Ring-Redundanz-Methode die Funktion.

Anmerkung: Haben Sie ein Gerät als MRP-Ringmanager konfiguriert, bietet Ihnen das Gerät die Möglichkeit, die MRP-Ring-Konfiguration automatisch vorzunehmen (siehe auf Seite 268 „Erweiterte Ringkonfiguration/-diagnose (ARC)“).

Parameter	Bedeutung

Version	Wählen Sie, welche Ring-Redundanz-Version Sie einsetzen:
	`HIPER-Ring`
	`MRP`

Ring-Port Nr.	In einem Ring hat jedes Gerät 2 Nachbarn. Definieren Sie 2 Ports als Ring-Ports, an denen die Nachbargeräte angeschlossen werden.
Modul	Modulbezeichnung der als Ring-Ports verwendeten Ports
Port	Portbezeichnung der als Ring-Ports verwendeten Ports
Funktion	Werte abhängig von gewählter Ring-Redundanz-Version. Beschreibung in den folgenden Abschnitten bei der entsprechenden Ring-Redundanz-Version.

Tab. 152: Ring-Redundanz Basiskonfiguration

7.2.1 HIPER-Ring konfigurieren

Anmerkung: Für die Ring-Ports wählen Sie im Dialog `Grundeinstellungen:Portkonfiguration`) folgende Grundeinstellungen:

Port-Typ	Bitrate	Autonegotiation (Automatische Konfiguration)	Port-Einstellung	Duplex
TX	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
TX	1 Gbit/s	an	an	-
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
Optisch	1 Gbit/s	an	an	-
Optisch	10 Gbit/s	-	an	10 Gbit/s Vollduplex (FDX)

Tab. 153: Port-Einstellungen für Ring-Ports

Anmerkung: Konfigurieren Sie alle Geräte des HIPER-Rings individuell. Warten Sie mit dem Anschließen der redundanten Strecke, bis Sie die Konfiguration aller Geräte des HIPER-Rings abgeschlossen haben. So vermeiden Sie Schleifen während der Konfigurationsphase.

Anmerkung: Alternativ zur Konfiguration des HIPER-Rings per Software, können Sie bei den Switches RS20/30/40, MS20/30 und PowerMICE einige Einstellungen auch mit DIP-Schaltern an den Geräten vornehmen. Mit einem DIP-Schalter können Sie auch einstellen, ob die Konfiguration per DIP-Schalter oder die Konfiguration per Software Vorrang hat. Lieferzustand ist „Software Configuration“ (Konfiguration per Software). Details zu den DIP-Schaltern finden Sie im Anwender-Handbuch Installation.

Parameter	Bedeutung
Ring-Port X.X Operation	Anzeige im Feld „Operation“: `active`: Sie haben diesen Port eingeschaltet und er hat einen Link. `inactive`: Sie haben diesen Port ausgeschaltet oder er hat keinen Link.
Status des Ringmanagers	Statusinformation, keine Eingabe möglich: `Aktiv (redundante Strecke)`: die redundante Strecke wurde geschlossen, weil eine Datenleitung oder Netzkomponente innerhalb des Rings ausgefallen ist. `Inaktiv`: die redundante Strecke ist offen, alle Datenleitungen und Netzkomponenten funktionieren.
Ringmanager-Modus	Schalten Sie bei genau einem Gerät an den Enden der Linie die Ring-Manager-Funktion ein.
Ringrekonfiguration	Die Einstellungen im Rahmen „Ringrekonfiguration“ sind ausschließlich bei Geräten wirksam, die Ring-Manager sind. Wählen Sie bei dem Ring-Manager den gewünschten Wert für den Testpaket-Timeout, den der Ring-Manager nach dem Senden eines Testpakets abwartet, bevor er das Testpaket als verloren-gegangen betrachtet. ▶ `Standard`:Testpakete-Timeout 480 ms ▶ `Beschleunigt`: Testpakete-Timeout 280 ms **Anmerkung:** Hinweis: Die Einstellungen sind insbesondere dann sinnvoll, wenn mindestens eine Strecke im Ring aus einer 1.000MBit/s-Twisted-Pair-Strecke besteht. Die aufgrund der Reaktionscharakteristik von 1.000-MBit/s-Twisted-Pair-Ports bestehende Rekonfigurationszeit bei Verbindungsunter-brechungen kann so deutlich beschleunigt werden.
Information	Wenn das Gerät Ring-Manager ist: Die Anzeigen in diesem Rahmen bedeuten: „Redundanz vorhanden“: Wenn eine Komponente des Rings ausfällt, übernimmt die redundante Strecke deren Funktion. „Konfigurationsfehler“: Sie haben die Funktion falsch konfiguriert oder die Ringportverbindung ist nicht vorhanden.

Tab. 154: HIPER-Ring-Konfiguration

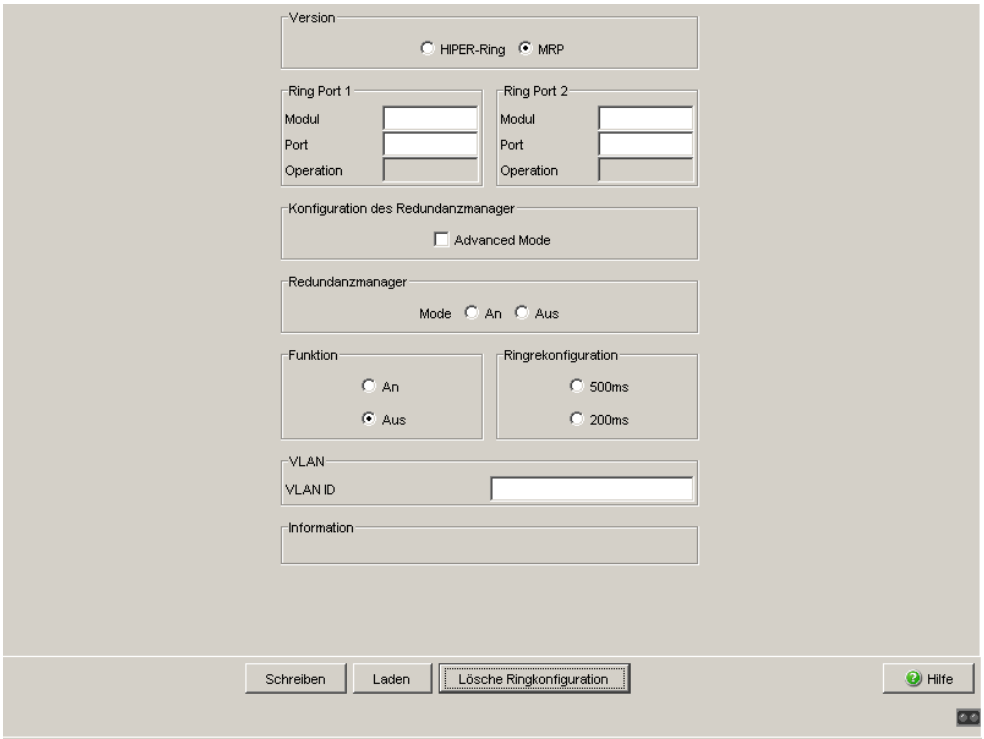


Abb. 62: Ring-Redundanz wählen, Ringports eingeben, Ring-Manager ein-/ausschalten und Ringrekonfiguration wählen.

Anmerkung: Deaktivieren Sie das Spanning-Tree-Protokoll (STP) an den Ports, die an den redundanten Ring angeschlossen sind, da Spanning-Tree und Ring-Redundanz mit unterschiedlichen Reaktionszeiten arbeiten (`Redundanz:Spanning Tree:Port`).
Wenn Sie die Funktion des HIPER-Rings über DIP-Schalter aktiviert haben, schaltet sich STP automatisch ab.

Anmerkung: Haben Sie VLANs konfiguriert, dann beachten Sie die VLAN-Konfiguration der Ringports.
Bei der Konfiguration des HIPER-Rings wählen Sie für die Ringports die
– VLAN-ID 1 und „`Ingress Filtering`“ deaktiviert in der Port-Tabelle und
– VLAN-Zugehörigkeit `U` oder `T` in der statischen VLAN-Tabelle.

Anmerkung: Falls Sie auch redundante Ring-/Netzkopplung verwenden: stellen Sie sicher, dass das Gerät VLAN 1 Pakete getagged auf den beiden Ringports vermittelt.

Anmerkung: Wenn Sie Link-Aggregations-Verbindungen im HIPER-Ring verwenden wollen (PowerMICE und MACH 4000), dann geben Sie für Modul und Port des Ringports den Index des gewünschten Link-Aggregation-Eintrags an.

Anmerkung: Beim Aktivieren der HIPER-Ring-Funktion per Software oder DIP-Schalter setzt das Gerät die entsprechenden Einstellungen für die vordefinierten Ringports in der Konfigurationstabelle (Übertragungsrate und Modus). Schalten Sie die HIPER-Ring-Funktion ab, behalten die zu normalen Ports zurückgewandelten Ports die Ringporteinstellungen bei. Unabhängig von der DIP-Schalter-Stellung können Sie die Port-Einstellungen weiterhin über Software verändern.

7.2.2 MRP-Ring konfigurieren

Anmerkung: Um einen MRP-Ring zu konfigurieren, bauen Sie das Netz nach Ihren Erfordernissen auf. Für die Ring-Ports wählen Sie im Dialog `Grundeinstellungen:Portkonfiguration` folgende Grundeinstellungen:

Port-Typ	Bitrate	Autonegotiation (Automatische Konfiguration)	Port-Einstellung	Duplex
TX	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
TX	1 Gbit/s	an	an	-
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
Optisch	1 Gbit/s	an	an	-
Optisch	10 Gbit/s	-	an	10 Gbit/s Vollduplex (FDX)

Tab. 155: Port-Einstellungen für Ring-Ports

Anmerkung: Konfigurieren Sie alle Geräte des MRP-Rings individuell. Warten Sie mit dem Anschließen der redundanten Strecke, bis Sie die Konfiguration aller Geräte des MRP-Rings abgeschlossen haben. So vermeiden Sie Schleifen während der Konfigurationsphase.

Anmerkung: Wenn Sie VLANs konfiguriert haben und die MRP-Ring-Konfiguration einem VLAN zuordnen wollen:

- ☐ Wählen Sie im Dialog `Redundanz:Ring-Redundanz` im Feld `VLAN` eine VLAN-ID > 0. Wählen Sie bei allen Geräten in diesem MRP-Ring in der MRP-Ring Konfiguration diese VLAN-ID.
- ☐ Prüfen Sie die VLAN-Konfiguration der Ringports: Wählen Sie für alle Ringports in diesem MRP-Ring diese entsprechende VLAN-ID und die VLAN-Zugehörigkeit `T` in der statischen VLAN Tabelle.
- ☐ Vermeiden Sie VLAN-ID = 0.

Anmerkung: Falls Sie auch redundante Ring-/Netzkopplung verwenden: stellen Sie sicher, dass das Gerät VLAN 1 Pakete getagged auf den beiden Ringports vermittelt.

Parameter	Bedeutung
Ring-Port X.X Operation	Anzeige im Feld „Operation“: `forwarding`: Sie haben diesen Port eingeschaltet und er hat einen Link. `blocked`: dieser Port ist blockiert und hat einen Link `disabled`: Sie haben diesen Port ausgeschaltet `not-connected`: dieser Port hat keinen Link.
Konfiguration des Ringmanagers	Schalten Sie den Advanced-Mode aus, wenn ein Gerät im Ring den Advanced-Mode für schnelle Umschaltzeiten nicht unterstützt. Ansonsten schalten Sie den Advanced-Mode ein. **Anmerkung:** Alle Hirschmann-Geräte, die den MRP-Ring unterstützen, unterstützen auch den Advanced-Mode.
Ringmanager-Modus	Schalten Sie bei genau einem Gerät an den Enden der Linie die Ring-Manager-Funktion ein.
Funktion	Wenn Sie alle Parameter für den MRP-Ring konfiguriert haben, schalten Sie hier die Funktion ein. Wenn Sie alle Geräte im MRP-Ring konfiguriert haben, schließen Sie redundante Strecke.
Ringrekonfiguration	Wählen Sie bei dem Gerät, bei dem Sie den Ring-Manager eingeschaltet haben, den Wert 200 ms, wenn die Stabilität des Ringes den Anforderungen an Ihr Netz entspricht. Ansonsten wählen Sie 500 ms. `Hinweis`: Einstellungen im Rahmen „Ringrekonfiguration“ sind lediglich bei Geräten wirksam, die Ring-Manager sind.
VLAN-ID	Wenn Sie VLANs konfiguriert haben, dann wählen Sie hier: ▶ `VLAN-ID 0`, wenn Sie die MRP-Ring-Konfiguration keinem VLAN zuordnen möchten. Beachten Sie die VLAN-Konfiguration der Ringports: Wählen Sie für die Ringports dann die VLAN-ID 1 und VLAN-Zugehörigkeit `U` in der statischen VLAN-Tabelle. ▶ `VLAN-ID > 0`, wenn Sie die MRP-Ring-Konfiguration diesem VLAN zuordnen wollen. Wählen Sie bei allen Geräten in diesem MRP-Ring diese VLAN-ID in der MRP-Ring Konfiguration.Beachten Sie die VLAN-Konfiguration der Ringports: Wählen Sie für alle Ringports in diesem MRP-Ring dann diese entsprechende VLAN-ID und die VLAN-Zugehörigkeit `T` in der statischen VLAN Tabelle.
Information	Wenn das Gerät Ring-Manager ist: Die Anzeigen in diesem Rahmen bedeuten: „Redundanz vorhanden“: Wenn eine Komponente des Rings ausfällt, übernimmt die redundante Strecke deren Funktion. „Konfigurationsfehler“: Sie haben die Funktion falsch konfiguriert oder die Ringportverbindung ist nicht vorhanden.

Tab. 156: MRP-Ring Konfiguration

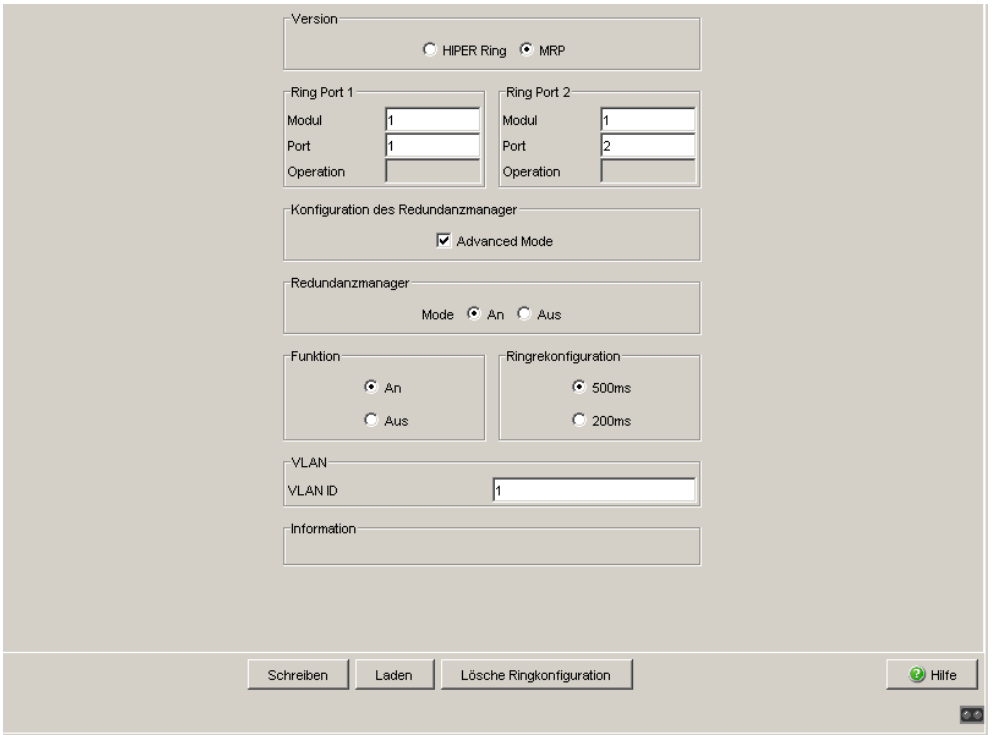


Abb. 63: MRP-Ring-Version wählen, Ringports eingeben und Ring-Manager ein-/ausschalten.

Anmerkung: Schalten Sie bei allen Geräten in einem MRP-Ring im Dialog `Redundanz:Spanning Tree:Global` die MRP-Kompatibilität an, wenn Sie RSTP im MRP-Ring verwenden wollen. Sollte dies nicht möglich sein, etwa weil einzelne Geräte die MRP-Kompatibilität nicht unterstützen, deaktivieren Sie das Spanning-Tree-Protokoll an den Ports, die an den MRP-Ring angeschlossen sind. Spanning-Tree und Ring-Redundanz beeinflussen sich gegenseitig.

Anmerkung: Wenn Sie RSTP mit einem MRP-Ring kombinieren, stellen Sie auf den Geräten im MRP-Ring eine bessere, also numerisch kleinere RSTP-Bridge-Priorität ein als auf den Geräten im angeschlossenen RSTP-Netz. Damit helfen Sie, eine Verbindungsunterbrechung zu Geräten außerhalb des Rings zu vermeiden.

Erweiterte Ringkonfiguration/-diagnose (ARC)

Das Hirschmann-Gerät bietet Ihnen als Besonderheit die Möglichkeit, die Konfiguration aller Geräte in einem MRP-Ring durch das ARC-Protokoll (Advanced Ring Configuration) vorzunehmen.

Zur Konfiguration eines MRP-Rings mit ARC reicht es aus, wenn Sie Hirschmann-Geräte im Lieferzustand zu einem Ring verbinden und an einem Gerät die Erweiterte Ringkonfiguration/ -diagnose ausführen. Lediglich das Gerät, auf dem Sie ARC mit dem Web-based Interface bedienen, benötigt eine IP-Adresse.

Der ARC-Manager sendet zunächst Diagnose-Pakete in den Ring und wertet die Rückmeldungen der Ringteilnehmer aus. Auf diese Weise ermittelt er die Ringports und die momentanen Einstellungen der Ring-Teilnehmer.
Stellt der ARC-Manager fest, dass die Voraussetzungen für die Erweiterte Ringkonfiguration/-diagnose erfüllt sind, bietet er Ihnen die automatische Konfiguration an.
Dabei sendet der ARC-Manager Konfigurations-Pakete in den Ring. Alle Geräte im Ring konfigurieren dabei automatisch ihre Ringredundanz-Einstellungen für einen MRP-Ring nach den Vorgaben des ARC-Managers.
Danach speichern alle Geräte im Ring ihre neue Konfiguration nichtflüchtig ab.

Die Voraussetzungen für die automatische Prüfung und Durchführung der Erweiterten Ringkonfiguration/-diagnose sind:

- Vermeidung von Loops (Schleifen):
  - Auf allen Geräten und Ring-Ports des Rings ist RSTP aktiv (Voreinstellung: global und auf allen Ports aktiv).
- Alle Geräte im Ring unterstützen die Erweiterte Ringkonfiguration/-diagnose:
  - sie arbeiten mit der Software-Variante L2P, L3E oder L3P,
  - sie arbeiten mit der Software-Version 07.0.00 oder höher.
- Alle Geräte, die Sie als MRP-**Ringteilnehmer** vorgesehen haben:
  - Der konfigurierte Modus des Ringmanagers ist `Aus` (Voreinstellung: `Aus`).
  - Die Erweiterte Ringkonfiguration/-diagnose ist `Lesen/Schreiben` (Voreinstellung: `Lesen/Schreiben`).

Anmerkung: Um die Einstellungen im Rahmen Erweiterte Ringkonfiguration/-diagnose abzulesen, setzen Sie im Web-based Interface
- die Version der Ring-Redundanz auf `MRP` und
- die Funktion auf `An`.

– Die Voreinstellung der konfigurierten Version der Ring-Redundanz ist `MRP`. Haben Sie eine andere Version gewählt, setzen die Geräte beim Ausführen der Erweiterten Ringkonfiguration/-diagnose ihre Einstellung automatisch auf `MRP`.
– Die Voreinstellung der Funktion ist `Aus`. Die Geräte setzen beim Ausführen der Erweiterten Ringkonfiguration/-diagnose ihre Einstellung automatisch auf `An`.

▶ Das Gerät, das Sie als MRP-**Ringmanager** vorgesehen haben:
  – Ausschließlich 1 Gerät im Ring ist MRP-Ringmanager,
  – Die konfigurierte Version der Ring-Redundanz ist `MRP` (Voreinstellung: MRP),
  – Die konfigurierten Ring-Ports stimmen mit der Ring-Verkabelung überein (Voreinstellung für beide Ports: 1.1),
  – Der konfigurierte Modus des Ringmanagers ist `An` (Voreinstellung: Aus),
  – Die konfigurierte Funktion ist `An` (Voreinstellung: Aus),
  – Die Erweiterte Ringkonfiguration/-diagnose ist `An` (Voreinstellung: `Aus`),
  – Ausschließlich dieses Gerät führt die Erweiterte Ringkonfiguration/-diagnose aus.

▶ Physikalische Topologie:
  – Sie haben die Geräte zu einem physikalischen Ring verbunden.

Anmerkung: Beachten Sie die folgenden Besonderheiten der Erweiterten Ringkonfiguration/-diagnose:

▶ Die Erweiterte Ringkonfiguration/-diagnose konfiguriert ausschließlich einen MRP-Basis-Ring. Konfigurieren Sie Ringe mit einem anderen Redundanz-Protokoll sowie Sub-Ringe manuell.

▶ Beim Ausführen der Konfiguration der Erweiterten Ringkonfiguration/-diagnose schalten alle Geräte im Ring RSTP auf ihren Ring-Ports ab. Ausnahme: ist auf einem Gerät die Einstellung „MRP-Kompatibilität“ aktiv (siehe auf Seite 291 „Global“), so lässt das Gerät RSTP auf dem Ring-Port eingeschaltet.
Wenn Sie RSTP benötigen, schalten Sie RSTP auf den Ring-Ports manuell ein (siehe auf Seite 305 „Port“).

Haben Sie ein Gerät als Ring-**Teilnehmer** vorgesehen, zeigt es im Dialog Ring-Redundanz den Rahmen „Erweiterte Ringkonfiguration/-diagnose“ mit 3 Auswahlmöglichkeiten an.
Falls nötig, selektieren Sie die Option „Lesen/Schreiben“ und speichern Sie die Einstellung auf dem Gerät.

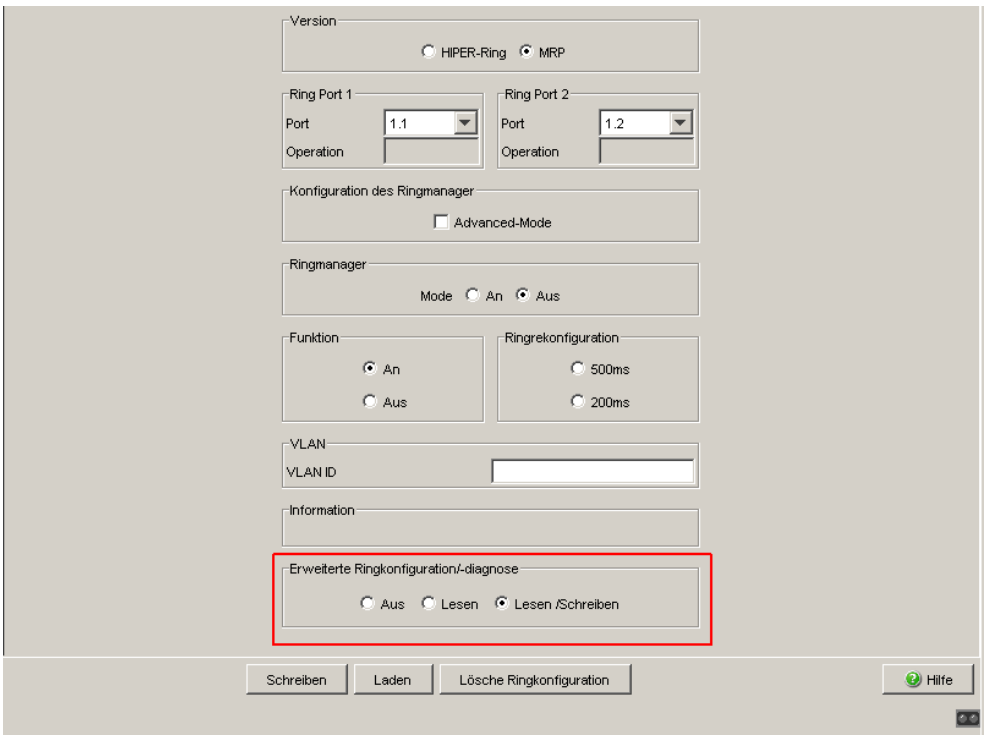


Abb. 64: Dialog Ring-Redundanz, Erweiterte Ringkonfiguration/-diagnose eines MRP-Clients

Haben Sie ein Gerät als Ring-**Manager** vorgesehen, zeigt es im Dialog Ring-Redundanz den Rahmen „Erweiterte Ringkonfiguration/-diagnose“ an. Er enthält 2 Auswahlmöglichkeiten sowie die Schaltflächen „Konfiguration“ und „Diagnose“.
Falls nötig, selektieren Sie die Option „An“ und speichern Sie die Einstellung auf dem Gerät.

Um zu prüfen, ob ARC den Ring automatisch konfigurieren kann, klicken Sie auf „Diagnose“. Um den Ring automatisch mit ARC zu konfigurieren, klicken Sie auf „Konfiguration“. Das Gerät führt Sie mit Hilfe eines Assistenten durch die Diagnose- und Konfigurationsschritte und zeigt Ihnen die Ergebnisse an.

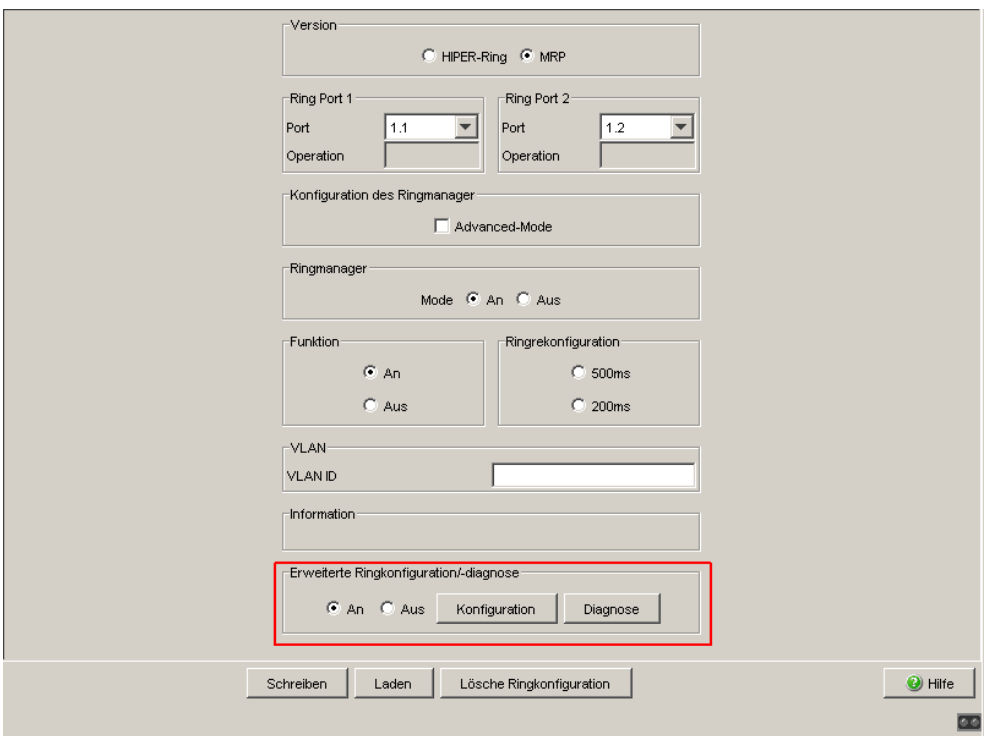


Abb. 65: Dialog Ring-Redundanz, Erweiterte Ringkonfiguration/-diagnose eines MRP-Managers

7.2.3 Fast HIPER-Ring konfigurieren (MACH 1040)

Innerhalb eines Fast HIPER-Ringes können Sie eine beliebige Mischung der folgenden Geräte einsetzen:

- RSR20, RSR30
- MACH 1000

Um einen Fast HIPER-Ring zu konfigurieren, bauen Sie das Netz nach Ihren Erfordernissen auf. Für die Ring-Ports wählen Sie im Dialog `Grundeinstellungen:Portkonfiguration` folgende Grundeinstellungen:

Port-Typ	Bitrate	Autonegotiation (Automatische Konfiguration)	Port-Einstellung	Duplex
TX	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
TX	1 Gbit/s	an	an	-
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
Optisch	1 Gbit/s	an	an	-
Optisch	10 Gbit/s	-	an	10 Gbit/s Vollduplex (FDX)

Tab. 157: Port-Einstellungen für Ring-Ports

Anmerkung: Wenn Sie VLANs konfiguriert haben und die Fast HIPER-Ring-Konfiguration einem VLAN zuordnen wollen:

- ☐ Wählen Sie im Dialog `Redundanz:Ring-Redundanz` im Feld `VLAN` eine VLAN-ID > 0. Wählen Sie bei allen Geräten in diesem Ring in der Fast HIPER-Ring-Konfiguration diese VLAN-ID.
- ☐ Prüfen Sie die VLAN-Konfiguration der Ringports: Wählen Sie für alle Ringports in diesem Ring diese entsprechende VLAN-ID und die VLAN-Zugehörigkeit `T` in der statischen VLAN Tabelle.
- ☐ Vermeiden Sie VLAN-ID = 0.

Anmerkung: Falls Sie auch redundante Ring-/Netzkopplung verwenden: stellen Sie sicher, dass das Gerät VLAN 1 Pakete getagged auf den beiden Ringports vermittelt.

Parameter	Bedeutung
Ring-Port X.X Operation	Anzeige im Feld „Operation“: `forwarding`: Sie haben diesen Port eingeschaltet und er hat einen Link. `blocked`: dieser Port ist blockiert und hat einen Link `disabled`: Sie haben diesen Port ausgeschaltet `not-connected`: dieser Port hat keinen Link.
Ringmanager-Modus	Schalten Sie bei genau einem Gerät an den Enden der Linie die Ring-Manager-Funktion ein.
Funktion	Wenn Sie alle Parameter für den Fast HIPER-Ring konfiguriert haben, schalten Sie hier die Funktion ein. Wenn Sie alle Geräte im Fast HIPER-Ring konfiguriert haben, schließen Sie redundante Strecke.
Ringinformation Ringumlaufzeit	`Ringumlaufzeit`: Vom Ring-Manager gemessene Ringumlaufzeit der Prüfpakete in µs. Die Anzeige beginnt mit 100 µs, in Schritten von 100 µs. Werte um 1000 µs und größer signalisieren, dass der Ring instabil werden kann. Überprüfen Sie in diesem Fall die korrekte Anzahl der Geräte im Rahmen „Switche“ (siehe unten).
VLAN-ID	Wenn Sie VLANs konfiguriert haben, dann wählen Sie hier: `VLAN-ID 0`, wenn Sie die Fast HIPER-Ring-Konfiguration keinem VLAN zuordnen möchten. Beachten Sie die VLAN-Konfiguration der Ringports: Wählen Sie für die Ringports dann die VLAN-ID 1 und VLAN-Zugehörigkeit U in der statischen VLAN-Tabelle. `VLAN-ID >0`, wenn Sie die Fast HIPER-Ring-Konfiguration diesem VLAN zuordnen wollen. Wählen Sie bei allen Geräten in diesem Ring die selbe VLAN-ID in der Fast HIPER-Ring Konfiguration.Beachten Sie die VLAN-Konfiguration der Ringports: Wählen Sie für alle Ringports in diesem Fast HIPER-Ring dann diese entsprechende VLAN-ID und die VLAN-Zugehörigkeit M in der statischen VLAN Tabelle.
Switche / Anzahl	Geben Sie hier die Anzahl der in diesem Fast HIPER-Ring integrierten Geräte an. Dieser Eintrag dient der Optimierung der Rekonfigurationszeit und der Stabilität des Rings.
Information	Wenn das Gerät Ring-Manager ist: Die Anzeigen in diesem Rahmen bedeuten: „Redundanz vorhanden“: Wenn eine Komponente des Rings ausfällt, übernimmt die redundante Strecke deren Funktion. „Konfigurationsfehler“: Sie haben die Funktion falsch konfiguriert oder die Ringportverbindung ist nicht vorhanden.

Tab. 158: Fast HIPER-Ring Konfiguration

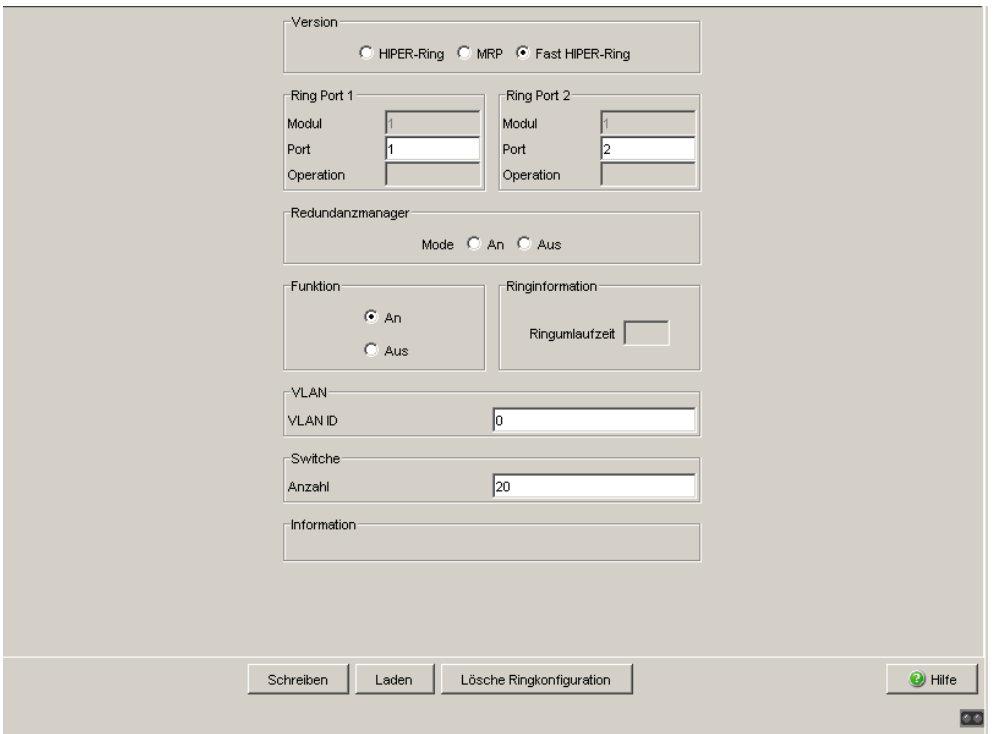


Abb. 66: Fast HIPER-Ring wählen und konfigurieren

Anmerkung: Deaktivieren Sie das Spanning-Tree-Protokoll (STP) an den Ports, die an den redundanten Ring angeschlossen sind, da Spanning-Tree und Ring-Redundanz mit unterschiedlichen Reaktionszeiten arbeiten (`Redundanz:Spanning Tree:Port`).

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Lösche Ringkonfiguration	Schaltet die Redundanzfunktion aus und setzt alle Einstellungen im Dialog in den Lieferzustand zurück.
Hilfe	Öffnet die Online-Hilfe.

Tab. 159: Schaltflächen

7.3 Sub-Ring

Dieser Dialog bietet Ihnen die Möglichkeit:
- Eine Übersicht aller verbundenen Sub-Ringe anzuzeigen,
- Sub-Ringe anzulegen,
- Sub-Ringe zu konfigurieren, und
- Sub-Ringe zu löschen.

Anmerkung: Folgende Geräte unterstützen die Sub-Ring-Manager-Funktion:
– RSR20/RSR30
– PowerMICE
– MACH 1000
– MACH 4000

In einen Sub-Ring können Sie als Teilnehmer die Geräte integrieren, die MRP unterstützen, die Sub-Ring-Manager-Funktion ist nicht notwendig.

Anmerkung: Konfigurieren Sie jedes Gerät im Sub-Ring, bevor Sie die redundante Strecke schließen. So vermeiden Sie Schleifen während der Konfigurationsphase.

Anmerkung: Sub-Ringe nutzen MRP. Sie können Sub-Ringe an bestehende Basis-Ringe mit HIPER-Ring-Protokoll, Fast HIPER-Ring-Protokoll und MRP ankoppeln. Wenn Sie einen Sub-Ring an einen Basis-Ring unter MRP koppeln, dann konfigurieren Sie beide Ringe in unterschiedlichen VLANs. Konfigurieren Sie hierzu
- entweder die Sub-Ring-Ports der Sub-Ring-Manager und die Geräte des Sub-Rings in einem eigenen VLAN. Hierbei können mehrere Sub-Ringe das gleiche VLAN nutzen.
- oder die Geräte des Basis-Rings inklusive der Basis-Ring-Ports der Sub-Ring-Manager in einem eigenen VLAN. Dies verringert den Konfigurationsaufwand, wenn Sie an einen Basis-Ring mehrere Sub-Ringe ankoppeln.

Anmerkung: Im Sub-Ring konfigurieren Sie die Geräte mit ausgeschalteter Sub-Ring-Manager-Funktionen als Teilnehmer an einem MRP-Ring (siehe auf Seite 265 „MRP-Ring konfigurieren“).
Das bedeutet:

- Definieren Sie eine unterschiedliche VLAN-Zugehörigkeit von Basis-Ring und Sub-Ring, wenn auch der Basis-Ring das MRP-Protokoll nutzt; z.B. VLAN-ID 1 für den Basis-Ring und VLAN-ID 2 für den Sub-Ring.
- Schalten Sie die MRP-Ring-Funktion bei allen Geräten ein.
- Schalten Sie die Ring-Manager-Funktion bei allen Geräten aus.
- Konfigurieren Sie keine Link-Aggregation.
- Schalten Sie RSTP für die im Sub-Ring genutzten MRP-Ring-Ports aus.
- Weisen Sie allen Geräten die gleiche MRP-Domänen-ID zu. Verwenden Sie ausschließlich Geräte der Firma Hirschmann Automation and Control GmbH, können Sie den Default-Wert für die MRP-Domänen-ID unverändert lassen.

Anmerkung: Verwenden Sie das Command Line Interface (CLI), um Geräten ohne Sub-Ring-Manager-Funktion eine andere MRP-Domänen-Bezeichnung zuzuweisen. Weitere Informationen hierzu finden Sie im Referenz-Handbuch Command Line Interface.

7.3.1 Sub-Ring-Konfiguration

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Max. Tabellen-einträge	Anzahl der von einem Sub-Ring-Manager gleichzeitig verwaltbaren Sub-Ringe.	4 MACH1040: (16)	-
Sub-Ring-ID	Eindeutige Bezeichnung für diesen Sub-Ring.	0 - 2147483647 (2^{31}-1)	-
Funktion an/aus	Schalten Sie den Sub-Ring erst nach vollständiger Konfiguration an. Schließen Sie dann den Sub-Ring.	`An` `Aus`	`An`
Konfigurations-status	Ein Icon zeigt den aktuellen Status des Sub-Rings an.		

Tab. 160: Sub-Ring Basiskonfiguration

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Redundanz vorhanden	Ein Icon zeigt an, ob die Redundanz vorhanden ist.		
.Port	Bezeichnung des Ports, der das Gerät mit dem Sub-Ring verbindet.	Alle verfügbaren Ports, die nicht bereits zur Ring-Redundanz des Basis-Rings gehören, in der Form X.X (Modul.Port)	
Name	Optionale Benennung des Sub-Rings		
SRM-Modus	Sollzustand: Bestimmen Sie, ob dieser SRM die redundante Verbindung verwalten soll (Modus `redundant Manager`) oder nicht. Wenn Sie bei beiden SRM den gleichen Wert für SRM-Modus eingestellt haben, übernimmt der SRM mit der höheren MAC Adresse die Funktion des redundantManager. `singleManager` beschreibt den Sonderstatus, wenn Sie einen Sub-Ring über 2 Ports eines einzigen Gerätes anschließen. In diesem Fall verwaltet der Port mit der höheren Portnummer die redundante Verbindung.	manager redundantManager singleManager	manager
SRM-Status	Istzustand: Zeigt an, ob dieser SRM die redundante Verbindung verwaltet (Modus `redundant Manager`) oder nicht. Wenn Sie bei beiden SRM den gleichen Wert für SRM-Modus eingestellt haben, übernimmt der SRM mit der höheren MAC Adresse die Funktion des redundantManager. `SingleManager` beschreibt den Sonderstatus, wenn Sie einen Sub-Ring über 2 Ports eines einzigen Gerätes anschließen. In diesem Fall verwaltet der Port mit der höheren Portnummer die redundante Verbindung.	manager redundantManager singleManager	manager
Port-Status	Verbindungsstatus des Sub-Ring-Ports	forwarding disabled blocked not connected	
VLAN	VLAN, dem dieser Sub-Ring zugeordnet ist. Existiert unter der angegebenen VLAN-ID noch kein VLAN, legt das Gerät dieses automatisch an. Möchten Sie für diesen Sub-Ring kein eigenes VLAN benutzen, lassen Sie den Eintrag auf 0.	Entsprechend den Vorgaben im Dialog VLAN	-

Tab. 160: Sub-Ring Basiskonfiguration

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Partner-MAC	Anzeige der MAC-Adresse des Sub-Ring-Managers am anderen Ende des Sub-Rings.	Gültige MAC-Adresse	00 00 00 00 00 00
MRP Domäne	Weisen Sie allen Mitgliedern in einem Sub-Ring die gleiche MRP-Domänen-Bezeichnung zu. Verwenden Sie ausschließlich Geräte der Firma Hirschmann, können Sie den Default-wert übernehmen, anderenfall passen Sie ihn gegebenenfalls an. Bei mehreren Sub-Ringen können alle Sub-Ringe die gleiche MRP-Domänen-Bezeichnung nutzen.	Alle zugelassenen MRP Domänen-Bezeichnungen	255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255
Protokoll		`standardMRP`	`standardMRP`

Tab. 160: Sub-Ring Basiskonfiguration

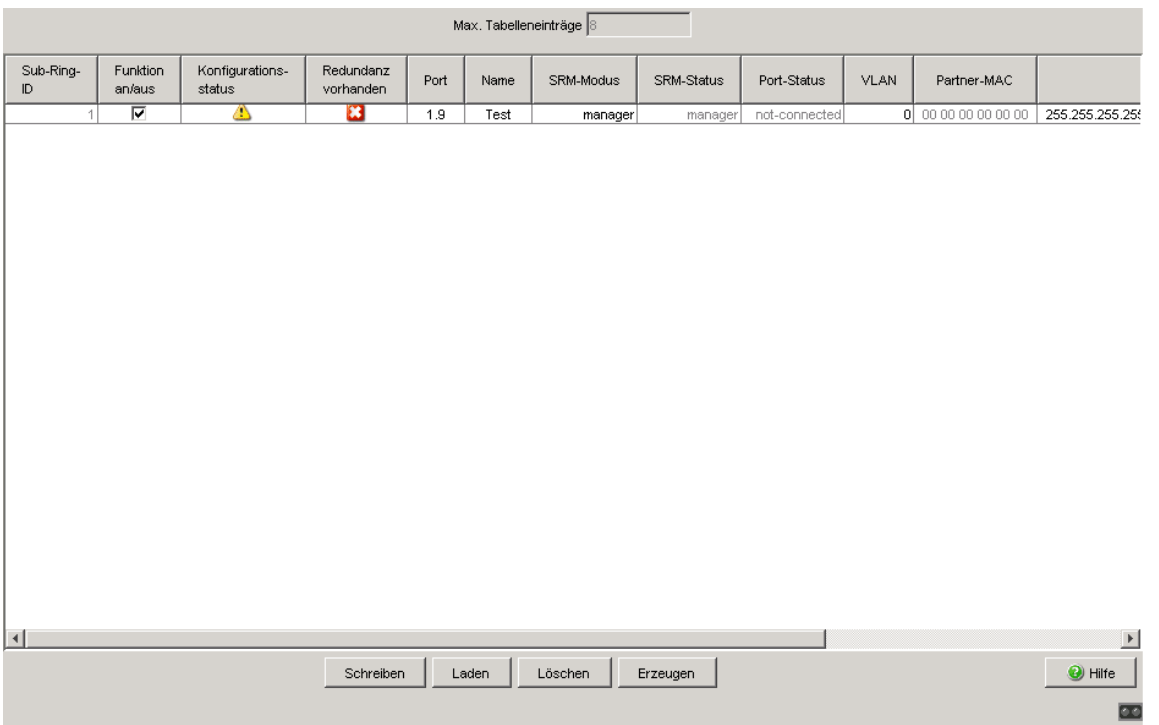


Abb. 67: Sub-Ring Basiskonfiguration

7.3.2 Sub-Ring – Neuer Eintrag

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Sub-Ring-ID	Eindeutige Bezeichnung für diesen Sub-Ring.	0 - 2147483647 (2^{31}-1)	-
.Port	Bezeichnung des Ports, der das Gerät mit dem Sub-Ring verbindet.	Alle verfügbaren Ports, die nicht bereits zur Ring-Redundanz des Basis-Rings gehören, in der Form X.X (Modul.Port)	
Name	Optionale Benennung des Sub-Rings		
SRM-Modus	Sollzustand: Bestimmen Sie, ob dieser SRM die redundante Verbindung verwalten soll (Modus `redundant Manager`) oder nicht. Wenn Sie bei beiden SRM den gleichen Wert für SRM-Modus eingestellt haben, übernimmt der SRM mit der höheren MAC Adresse die Funktion des redundantManager. `singleManager` beschreibt den Sonderstatus, wenn Sie einen Sub-Ring über 2 Ports eines einzigen Gerätes anschließen. In diesem Fall verwaltet der Port mit der höheren Portnummer die redundante Verbindung.	manager redundantManager singleManager	manager
VLAN	VLAN, dem dieser Sub-Ring zugeordnet ist. Existiert unter der angegebenen VLAN-ID noch kein VLAN, legt das Gerät dieses automatisch an. Möchten Sie für diesen Sub-Ring kein eigenes VLAN benutzen, lassen Sie den Eintrag auf 0.	Entsprechend den Vorgaben im Dialog VLAN	-
MRP Domäne	Weisen Sie allen Mitgliedern in einem Sub-Ring die gleiche MRP-Domänen-Bezeichnung zu. Verwenden Sie ausschließlich Geräte der Firma Hirschmann, können Sie den Defaultwert übernehmen, anderenfall passen Sie ihn gegebenenfalls an. Bei mehreren Sub-Ringen können alle Sub-Ringe die gleiche MRP-Domänen-Bezeichnung nutzen.	Alle zugelassenen MRP Domänen-Bezeichnungen	255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255

Tab. 161: Sub-Ring - Neuer Eintrag

Anmerkung: Für einen Sub-Ring im `singleManager`-Modus legen Sie 2 Einträge mit unterschiedlichen Sub-Ring-IDs an.

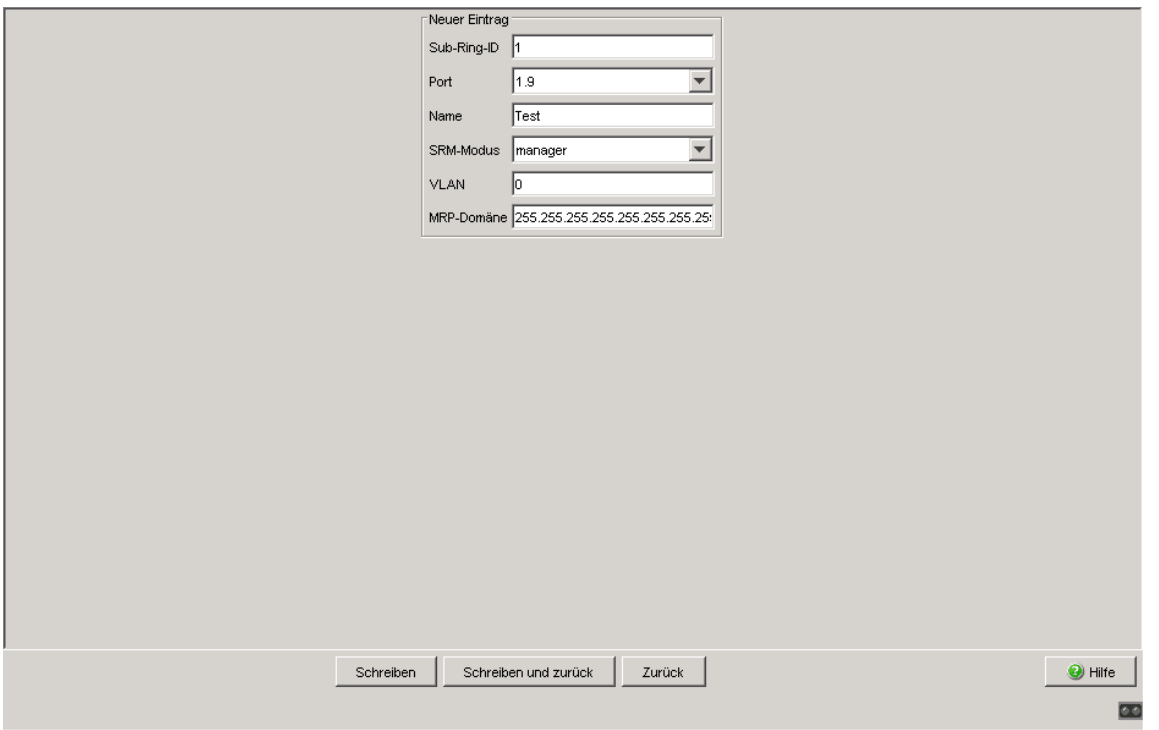


Abb. 68: Sub-Ring - Neuer Eintrag Dialog

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Löschen	Entfernt den markierten Tabelleneintrag.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Schreiben und zurück	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes und kehrt zurück zum vorherigen Dialog.

Tab. 162: Schaltflächen

Schaltfläche	Bedeutung
Zurück	Zeigt die vorherige Seite wieder an. Änderungen gehen dabei verloren.
Hilfe	Öffnet die Online-Hilfe.

Tab. 162: Schaltflächen (Forts.)

7.4 Ring-/Netzkopplung

Verwenden Sie die Ring-/Netzkopplung, um einen vorhandenen Ring (HIPER-Ring, MRP, Fast HIPER-Ring) an ein weiteres Netz oder an einen weiteren Ring redundant zu koppeln. Stellen Sie sicher, dass die Koppelpartner Hirschmann-Geräte sind.

Anmerkung: Zwei-Switch-Kopplung
Stellen Sie sicher, dass Sie einen Ring (HIPER-Ring, MRP, Fast HIPER-Ring) konfiguriert haben, bevor Sie die Ring-/Netzkopplung einrichten.

Dieser Dialog bietet Ihnen die Möglichkeit:
- Eine Übersicht der vorhandenen Ring-/Netzkopplung anzuzeigen,
- eine Ring-/Netzkopplung zu konfigurieren,
- eine Ring-/Netzkopplung ein-/auszuschalten,
- eine neue Ring-/Netzkopplung anzulegen, und
- eine Ring-/Netzkopplungen zu löschen.

7.4.1 Ring-/Netzkopplung vorbereiten

STAND-BY-Schalter

Alle Geräte besitzen einen STAND-BY-Schalter, mit dem Sie die Rolle des Geräts innerhalb einer Ring-/Netzkopplung bestimmen.

Dieser Schalter ist je nach Gerätetyp ausgeführt als ein DIP-Schalter an den Geräten oder ausschließlich als eine Software-Einstellung (Dialog `Redundanz:Ring-/Netzkopplung`). Sie bestimmen durch das Einstellen dieses Schalters, ob das Gerät innerhalb einer Ring-/Netzkopplung die Haupt- oder die redundante Kopplungs-Rolle ausführt. Details zu den DIP-Schaltern finden Sie im Anwender-Handbuch Installation.

Anmerkung: Je nach Ausführung besitzen die Geräte einen DIP-Schalter, mit dem zwischen der Software-Konfiguration und der DIP-Schalter-Konfiguration gewählt werden kann. Wenn Sie die DIP-Schalter so einstellen, dass die Software-Konfiguration gewählt ist, sind die DIP-Schalter im Endeffekt deaktiviert.

Gerätetyp	Ausführung STAND-BY Schalter
RS2-./.	DIP-Schalter
RS2-16M	DIP-Schalter
MICE/PowerMICE	Schaltbar zwischen DIP-Schalter und Software-Einstellung
MACH 3000/MACH 4000	Software-Schalter

Tab. 163: Übersicht Ausführung des STAND-BY Schalters

Setzen Sie den STAND-BY-Schalter abhängig von Gerät und Ausführung anhand der folgenden Tabelle:

Gerät mit	Wahl zwischen Hauptkopplung und redundanter Kopplung
DIP-Schalter	Am DIP-Schalter „STAND-BY“
DIP-Schalter-/Software-Schalter-Alternative	Entsprechend der gewählten Option - am DIP-Schalter „STAND-BY“ oder im - Dialog `Redundanz:Ring-/Netzkopplung` durch Wahl in „Konfiguration auswählen“. **Hinweis:** Diese Geräte besitzen einen DIP-Schalter, mit dem zwischen der Software-Konfiguration und der DIP-Schalter-Konfiguration gewählt werden kann. Details zu den DIP-Schaltern an den Geräten finden Sie im Anwender-Handbuch Installation.
Software-Schalter	Im Dialog `Redundanz:Ring-/Netzkopplung`

Tab. 164: Einstellen des STAND-BY-Schalters

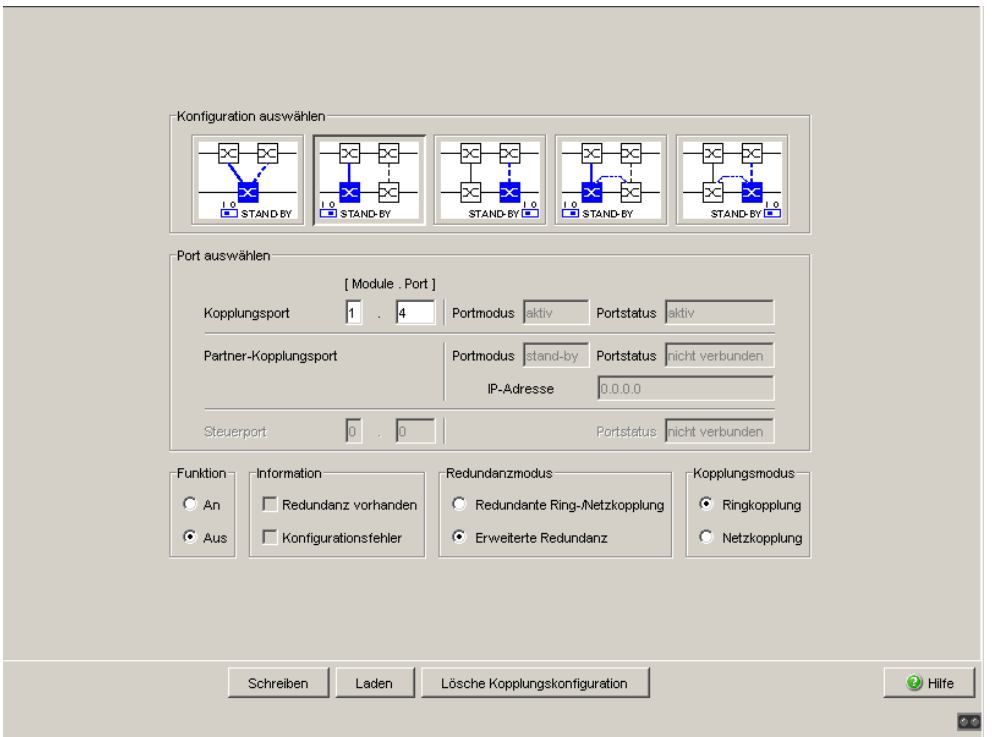


Abb. 69: Software-Konfiguration des STAND-BY-Schalters

Der Dialog zeigt in Abhängigkeit der STAND-BY-DIP-Schalterstellung die nicht möglichen Konfigurationen ausgegraut an. Möchten Sie eine dieser ausgegrauten Konfigurationen wählen, dann bringen Sie den STAND-BY-DIP-Schalter am Switch in die andere Stellung.

Ein-Switch-Kopplung
Ordnen Sie dem Gerät die DIP-Schalter-Einstellung „STAND-BY“ oder über die Software-Konfiguration die Redundanzfunktion zu.

Zwei-Switch-Kopplung
Ordnen Sie dem Gerät in der redundanten Strecke die DIP-Schalter-Einstellung „STAND-BY“ oder über die Softwarekonfiguration die Redundanzfunktion zu

Anmerkung: Schließen Sie aus Gründen der Redundanz-Zuverlässigkeit die Kombination von Rapid Spanning Tree und Ring-/Netzkopplung aus.

Dialog Ring-/Netzkopplung

Parameter	Bedeutung
Konfiguration auswählen	Wählen Sie abhängig von Ihren lokalen Gegebenheiten „Ein-Switch-Kopplung“, „Zwei-Switch-Kopplung, Slave“, „Zwei-Switch-Kopplung, Master“, „Zwei-Switch-Kopplung mit Steuerleitung, Slave“ oder „Zwei-Switch-Kopplung mit Steuerleitung, Master“. Diese Möglichkeiten sind als Buttons von links nach rechts dargestellt. Abhängig vom Gerätetyp (siehe Tabelle 163) nehmen Sie diese Einstellung vor: – ausschließlich mit DIP-Schaltern – ausschließlich per Software – per DIP-Schalter und Software Details zu den DIP-Schaltern an den Geräten finden Sie im Anwender-Handbuch Installation. – Bei Geräten, die ausschließlich mit DIP-Schaltern konfiguriert werden, nehmen sie die Einstellungen über diese vor. Die Buttons im Dialog dienen in diesem Fall lediglich der Anzeige. – Geräte ohne DIP-Schalter stellen Sie ausschließlich per Software ein. Sie können die Konfiguration mit den Buttons auswählen. – Bei Geräten, die per DIP-Schalter und Software konfiguriert werden können, können Sie die DIP-Schalter aktivieren oder deaktivieren. Haben Sie die DIP-Schalter aktiviert, können Sie Einstellungen der DIP-Schalter per Software nicht überscheiben, nicht per Software wählbare Einstellungen sind im Dialog ausgegraut. Zur Konfiguration per Software wählen Sie die zutreffende Ring-/Netzkopplungs-Konstellation durch Drücken des entsprechenden Buttons aus.
Kopplungsport	Dies ist der Port, an dem Sie eine Redundanzverbindung angeschlossen haben. **Hinweis:** Konfigurieren Sie den Kopplungsport und, soweit vorhanden, die Ring-Ports auf unterschiedlichen Ports. **Hinweis:** Um dauerhafte Schleifen (Loops) zu vermeiden, setzt das Gerät den Port-Status des Kopplungsports auf „aus“, wenn Sie die Funktion ausschalten oder die Konfiguration wechseln, während die Verbindungen an diesen Ports in Betrieb sind.
Portmodus	- `aktiv`: Sie haben den Port eingeschaltet. - `stand-by`: Der Port befindet sich im Stand-by-Modus.
Portstatus	- `aktiv`: Sie haben den Port eingeschaltet. - `stand-by`: Der Port befindet sich im Stand-by-Modus. - `nicht verbunden`: Sie haben den Port nicht verbunden.
Partner-Kopplungsport	Dies ist der Port, an dem der Partner seine Verbindung angeschlossen hat. Eine Port-Eingabe ist lediglich bei der Einrichtung einer „Ein-Switch-Kopplung“ möglich und notwendig. **Hinweis:** Konfigurieren Sie den Partner-Kopplungsport und soweit vorhanden, Ring-Ports auf unterschiedlichen Ports.

Tab. 165: Ring-/Netzkopplung Dialog

Parameter	Bedeutung
IP-Adresse	Wenn Sie eine „Zwei-Switch-Kopplung“ gewählt haben, zeigt das Gerät hier die IP-Adresse des Partners an, soweit Sie diesen im Netz schon in Betrieb genommen haben.
Steuerport	Dies ist der Port, an welchem Sie die Steuerleitung anschließen.
Funktion	Schalten Sie hier die Ring-Netzkopplung für dieses Gerät An oder Aus
Information	Wenn das Gerät Ring-Manager ist: Die Anzeigen in diesem Rahmen bedeuten: „Redundanz vorhanden“: Wenn eine Komponente des Rings ausfällt, übernimmt die redundante Strecke deren Funktion. „Konfigurationsfehler“: Sie haben die Funktion falsch konfiguriert oder die Ringportverbindung ist nicht vorhanden.
Redundanzmodus	Bei der Einstellung „Redundante Ring-/Netzkopplung“ ist entweder die Hauptleitung oder die redundante Leitung aktiv. Niemals sind beide Leitungen gleichzeitig aktiv. Bei der Einstellung „Erweiterte Redundanz“ sind Hauptleitung und redundante Leitung gleichzeitig aktiv, wenn die Verbindungsleitung zwischen den Geräten im angekoppelten (d.h im entfernten) Netz ausfällt. Während der Rekonfigurationszeit ist es möglich, dass es zu Paketdoppelungen kommt. Wählen Sie daher diese Einstellung ausschließlich, wenn Ihre Anwendung Paketdoppelungen erkennt.
Kopplungsmodus	Bestimmen Sie hier, ob die Konstellation die Sie konfigurieren, eine Kopplung von Redundanz-Ringen (HIPER-Ring, MRP-Ring) oder von Netzsegmenten ist.

Tab. 165: Ring-/Netzkopplung Dialog

Anmerkung: Für die Kopplungsports wählen Sie im Dialog `Grundeinstellungen:Portkonfiguration` folgende Einstellungen:

Port-Typ	Bitrate	Autonegotiation (Automatische Konfiguration)	Port-Einstellung	Duplex
TX	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
TX	1 Gbit/s	an	an	-
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
Optisch	1 Gbit/s	an	an	-
Optisch	10 Gbit/s	-	an	10 Gbit/s Vollduplex (FDX)

Tab. 166: Port-Einstellungen für Ring-Ports

Anmerkung: Haben Sie VLANs konfiguriert, dann beachten Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports.
Bei der Ring-/Netzkopplungs-Konfiguration wählen Sie für die Kopplungs- und Partner-Kopplungsports die
– VLAN-ID 1 und „`Ingress Filtering`“ deaktiviert in der Port-Tabelle und
– VLAN-Zugehörigkeit `T` in der statischen VLAN-Tabelle.

Anmerkung: Unabhängig von den VLAN-Einstellungen verschickt das Gerät die Ring-Kopplungsframes mit VLAN ID 1 und Priorität 7. Stellen Sie sicher, dass das Gerät VLAN 1 Pakete im lokalen Ring und im angeschlossenen Netz getaggt vermittelt. Damit bleibt die Priorität der Ring-Kopplungsframes erhalten.

Anmerkung: Wenn Sie die Funktionen Ring-Manager und Zwei-Switch-Kopplung gleichzeitig betreiben, besteht die Möglichkeit einer Schleifenbildung (Loop).

Anmerkung: Die Ring-/Netzkopplung arbeitet mit Testpaketen (Layer 2-Frames). Die beteiligten Geräte senden ihre Testpakete stets VLAN-getaggt mit der VLAN-ID 1 und der höchsten VLAN-Priorität 7. Dies gilt auch dann, wenn der Sende-Port ungetaggtes Mitglied in VLAN 1 ist.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Lösche Kopplungs-konfiguration	Entfernt die Kopplungskonfiguration.
Hilfe	Öffnet die Online-Hilfe.

Tab. 167: Schaltflächen

7.5 Spanning Tree

Unter Spanning Tree finden Sie die Dialoge und Ansichten zur Konfiguration und Überwachung der Spanning-Tree-Funktion nach dem Standard IEEE 802.1Q-2005, Rapid Spanning Tree (RSTP) und Multiple Spanning Tree (MSTP).

Anmerkung: Das Spanning-Tree-Protokoll ist ein Protokoll für MAC-Bridges (Brücken). Daher verwendet die folgende Beschreibung den Begriff Bridge für Switch.

Einführung

Lokale Netze werden immer größer. Dies gilt sowohl für die geografische Ausdehnung als auch für die Anzahl der Netzteilnehmer. Deshalb ist der Einsatz mehrerer Bridges vorteilhaft, z. B. um:

- die Netzlast in Teilbereichen zu verringern,
- redundante Verbindungen aufzubauen und
- Entfernungseinschränkungen zu überwinden.

Der Einsatz mehrerer Bridges mit mehrfachen, redundanten Verbindungen zwischen den Teilnetzen kann jedoch zu Schleifen/Loops und zum Verlust der Kommunikation durch das Netz führen. Als Hilfe, um dies zu verhindern, haben Sie die Möglichkeit, Spanning Tree einzusetzen. Spanning Tree erzielt Schleifenfreiheit durch das gezielte Deaktivieren von redundanten Verbindungen. Das gezielte Wieder-Aktivieren einzelner Verbindungen bei Bedarf ermöglicht die Redundanz.

Rapid Spanning Tree Protocol (RSTP)

RSTP ist eine Weiterentwicklung des Spanning-Tree-Protokolls (STP) und ist zu diesem kompatibel. Das STP benötigte bei Betriebsunfähigkeit einer Verbindung oder einer Bridge eine Rekonfigurationszeit von max. 30 s. Dies ist für zeitkritische Anwendungen nicht mehr akzeptabel. RSTP erreicht durchschnittliche Rekonfigurationszeiten von unter einer Sekunde. Wenn Sie RSTP in einer Ringtopologie mit 10 bis 20 Geräten einsetzen, können Sie auch Rekonfigurationszeiten im Millisekundenbereich erreichen.

Anmerkung: RSTP löst eine Layer 2-Netztopologie mit redundanten Pfaden in eine Baumstruktur (Spanning Tree) auf, die keine redundanten Pfade mehr enthält. Einer der Switches übernimmt dabei die Rolle der Root-Bridge. Die maximal erlaubte Anzahl der Geräte in einem aktiven Ast von der Root-Bridge bis zur Astspitze können Sie durch die Variable `Max Age` der aktuellen Root-Bridge vorgeben. Der voreingestellte Wert für `Max Age` ist 20, er kann bis auf 40 erhöht werden.
Wenn das als Root arbeitende Gerät ausfällt und ein anderes Gerät dessen Funktion übernimmt, bestimmt die neue Root-Bridge die größtmögliche erlaubte Anzahl der Geräte in einem Ast durch ihre `Max Age`-Einstellung.

Anmerkung: Sie haben die Möglichkeit, RSTP-Netzsegmente an einen MRP-Ring anzukoppeln. Aktivieren sie dazu die MRP-Kompatibilität. Dies ermöglicht Ihnen, RSTP über einen MRP-Ring zu betreiben.
Liegt die Root-Bridge innerhalb des MRP-Rings, zählen die Geräte im MRP-Ring bei der Berechnung der Astlänge als ein einziges Gerät. Ein Gerät, das an einer beliebigen Ring-Bridge angeschlossen ist, empfängt solche RSTP-Informationen, als wäre es direkt an die Root-Bridge angeschlossen.

Anmerkung: Der RSTP-Standard schreibt vor, dass alle Geräte innerhalb eines Netzes mit dem (Rapid-) Spanning-Tree-Algorithmus arbeiten. Bei gleichzeitigem Einsatz von STP und RSTP gehen in den Netz-Segmenten, die gemischt betrieben werden, die Vorteile der schnelleren Rekonfiguration bei RSTP verloren.
Ein Gerät, das lediglich RSTP unterstützt, arbeitet mit MSTP-Geräten zusammen, indem es sich keiner MST-Region, sondern dem CST (Common Spanning Tree) zuordnet.

Anmerkung: Das Standardisierungskomitee hat bei einer Änderung des RSTP-Standards IEEE 802.1D-2004 den maximalen Wert für „Hello Time“ von 10 auf 2 reduziert. Wenn Sie die Switch-Software von einer Release vor 5.0 auf eine Release 5.0 oder höher aktualisieren, reduziert die neue Software-Release automatisch lokal eingetragene „Hello Time“-Werte, die größer als 2 s sind, auf 2 s.
Ist das Gerät nicht RSTP-Root, so können abhängig von der Software-Release des Root-Gerätes weiterhin „Hello Time“ Werte > 2 s gültig sein.

Multiple Spanning Tree Protocol (MSTP)
MSTP ist eine Erweiterung des Rapid-Spanning-Tree-Protokolls, um den Nutzen von VLANs zu vergrößern. MSTP bietet Ihnen die Möglichkeit, mehrere Gruppen von VLANs zu definieren und für jede Gruppe eine eigene Spanning-Tree-Instanz zu konfigurieren. Diese Spanning-Tree-Instanz verhindert innerhalb der zugehörigen VLAN-Gruppe Schleifen und bietet Redundanz bei einem Ausfall.
Darüber hinaus ermöglicht MSTP bereits im Normalbetrieb, d. h., wenn alle Verbindungen in Betrieb sind, eine bessere Ausnutzung vorhandener Verbindungen. Z.B. kann MSTP eine Verbindung zwischen 2 Bridges für eine bestimmte VLAN-Gruppe in den Zustand „discarding“ setzen; jedoch gleichzeitig dieselbe Verbindung für eine andere VLAN-Gruppe im Zustand „forwarding“ betreiben. So ermöglicht MSTP im Normalbetrieb eine bessere Ausnutzung Ihrer Ressourcen durch Load-Sharing.

Anmerkung: Der folgende Text verwendet den Begriff Spanning Tree (STP), um Einstellungen oder Sachverhalte zu beschreiben, die sowohl auf STP, RSTP oder MSTP zutreffen.

7.5.1 Global

Dieser Dialog bietet Ihnen die Möglichkeit:

- Das Spanning-Tree-Protokoll ein-/auszuschalten und die Protokoll-Version RSTP oder MSTP auszuwählen,
- Bridge-bezogene Informationen zum Spanning-Tree-Protokoll anzuzeigen,
- Bridge-bezogene Parameter des Spanning-Tree-Protokolls zu konfigurieren,
- Bridge-bezogene Zusatzfunktionen einzustellen,
- die Parameter der Root-Bridge anzuzeigen und
- Bridge-bezogene Topologie-Informationen anzuzeigen.

Anmerkung: Rapid Spanning Tree ist als Vorgabe auf dem Gerät eingeschaltet und beginnt eigenständig, die vorgefundene Topologie in eine Baumstruktur aufzulösen. Haben Sie RSTP auf einzelnen Geräten ausgeschaltet, vermeiden Sie Schleifen während der Konfigurationsphase.

Die folgenden Tabellen zeigen Auswahlmöglichkeiten, Voreinstellungen und Informationen für die globalen Spanning-Tree-Einstellungen der Bridge.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Rahmen „Funktion“	Schaltet die Spanning Tree-Funktion für dieses Gerät „An“ oder „Aus“. Schalten Sie Spanning Tree für ein Gerät global aus, so flutet das Gerät empfangene Spanning Tree-Pakete wie normale Multicast-Pakete an den Ports. Das Gerät verhält sich damit transparent gegenüber Spanning Tree-Paketen.	`An`, `Aus`	`An`
Rahmen „Protokoll-Version“	Wählen Sie die Protokollversion: - `RSTP` (IEEE 802.1Q-2005), um Spanning Tree gemeinsam für alle konfigurierten VLANs einzusetzen, - `MSTP` (IEEE 802.1Q-2005), um Spanning Tree getrennt für verschiedene VLAN-Gruppen einzusetzen.	`RSTP`, `MSTP`	RSTP

Tab. 168: Globale Spanning-Tree-Einstellungen, Grundfunktionen

Im Rahmen „Protokoll-Konfiguration / Information“ haben Sie die Möglichkeit, die folgenden Werte zu konfigurieren und Informationen abzulesen.

Im Kontext von MSTP sind dies die Einstellungen für den Common Spanning Tree (CST).

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Spalte „Bridge“	**Informationen und Konfigurations-parameter des lokalen Geräts**		
Bridge-ID (Read-Only)	Die lokale Bridge-ID, zusammengesetzt aus der lokalen Priorität und der eigenen MAC-Adresse. Das Format ist ppppp / mm mm mm mm mm mm, mit: ppppp: Priorität (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).		
Priorität	Stellt die lokale Bridge-Priorität ein. Die Bridge-Priorität und die eigene MAC-Adresse zusammen bilden die eigene `Bridge-ID`. Das Gerät mit dem besten, also numerisch niedrigsten Prioritätswert übernimmt die Rolle der Root-Bridge. Bestimmen Sie das Root-Gerät, indem Sie dem Gerät die beste Priorität in der `Bridge-ID` unter allen Geräten im Netz zuweisen. Geben Sie den Wert als Vielfaches von 4.096 ein.	0 ≤ n*4.096 ≤ 61.440	32.768
Hello Time	Stellt die Hello-Time ein. Die lokale `Hello Time` gibt die Zeit zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Pakete) in Sekunden an. Hat das lokale Gerät die Root-Funktion, übernehmen die anderen Geräte im gesamten Netz diesen Wert. Ansonsten benutzt das lokale Gerät den Wert der Root-Bridge in der rechten Spalte „Root“.	1 - 2	2

Tab. 169: Globale Spanning-Tree-Einstellungen, lokale Bridge-Parameter

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Forward Delay	Stellt den Parameter Forward Delay ein. Beim Vorgängerprotokoll STP wurde der Parameter Forward Delay dazu verwendet, um den Zustandswechsel zwischen den Zuständen `disabled`, `discarding`, `learning`, `forwarding` zu verzögern. Seit der Einführung von RSTP hat dieser Parameter eine untergeordnete Bedeutung, weil die RSTP-Bridges den Zustandswechsel ohne vorgegebene Verzögerung aushandeln. Ist das lokale Gerät Root, übernehmen die anderen Geräte im gesamten Netz diesen Wert. Ansonsten benutzt das lokale Gerät den Wert der Root-Bridge in der rechten Spalte „Root“.	4 - 30 s Beachten Sie den Hinweis, der auf diese Tabelle folgt.	15 s
Max Age	Stellt den Parameter Max. Age ein. Beim Vorgängerprotokoll STP wurde der Parameter Max Age verwendet, um die Gültigkeit von STP-BPDUs in Sekunden anzugeben. Bei RSTP bedeutet Max Age die maximal zulässige Astlänge (Anzahl der Geräte bis zur Root-Bridge). Ist das lokale Gerät Root, übernehmen die anderen Geräte im gesamten Netz diesen Wert. Ansonsten benutzt das lokale Gerät den Wert der Root-Bridge in der rechten Spalte „Root“.	6 - 40 s Beachten Sie den Hinweis, der auf diese Tabelle folgt.	20 s
Tx Hold Count	Stellt den Parameter Tx Hold Count ein. Versendet das Gerät eine BPDU, inkrementiert es an diesem Port einen Zähler. Erreicht der Zähler den Wert des Tx Hold Count, stellt der Port das Senden weiterer BPDUs ein. Der Zähler wird jede Sekunde um 1 dekrementiert. Das Gerät versendet in der folgenden Sekunde maximal 1 neue BPDU.	1 - 40 (nach RSTP-Standard: 1 - 10)	10

Tab. 169: Globale Spanning-Tree-Einstellungen, lokale Bridge-Parameter

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
MRP-Kompatibilität	Schaltet die MRP-Kompatibilität an/aus. Die MRP-Kompatibilität ermöglicht die Nutzung von RSTP innerhalb eines MRP-Rings und bei der Kopplung von RSTP-Segmenten an einen MRP-Ring. Voraussetzung ist, dass alle Geräte im MRP-Ring die MRP-Kompatibilität unterstützen.	`An`, `Aus`	`Aus`
BPDU-Guard	Schaltet die `BPDU-Guard`-Funktion an/aus. Ist `BPDU-Guard` eingeschaltet, aktiviert das Gerät die Funktion für Edge-Ports (mit der Einstellung „Admin-Edge-Port“ `true`). Empfängt ein solcher Port eine beliebige STP-BPDU, setzt das Gerät den Port-Zustand „BPDU Guard Effect“auf `true` und den Vermittlungszustand des Ports in `discarding` (siehe Tabelle 180). So hilft Ihnen das Gerät, Ihr Netz an Endgeräteports vor Fehlkonfigurationen oder Angriffen mit STP-BPDUs zu schützen, die die Topologie zu verändern versuchen.	`An`, `Aus`	`Aus`

Tab. 169: Globale Spanning-Tree-Einstellungen, lokale Bridge-Parameter

Anmerkung: Wenn Sie RSTP mit einem MRP-Ring kombinieren, stellen Sie auf den Geräten im MRP-Ring eine bessere, also numerisch kleinere RSTP-Bridge-Priorität ein als auf den Geräten im angeschlossenen RSTP-Netz. Damit helfen Sie, eine Verbindungsunterbrechung zu Geräten außerhalb des Rings zu vermeiden.

Anmerkung: Die Parameter `Forward Delay` und `Max Age` stehen in folgender Beziehung zueinander:

`Forward Delay` ≥ (`Max Age`/2) + 1

Wenn Sie Werte eingeben, die dieser Beziehung widersprechen, dann ersetzt das Gerät diese Werte durch die zuletzt gültigen Werte oder die Voreinstellung.

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Spalte „Root“	**Informationen des Geräts, das aktuell Root-Bridge ist**		
Bridge-ID	Die `Bridge-ID` der aktuellen Root-Bridge. Das Format ist pppp / mm mm mm mm mm mm, mit: pppp: Priorität (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).		
Priorität	Die `Priorität` der aktuellen Root-Bridge.	0 ≤ n*4.096 ≤ 61.440	32.768
Hello Time	Die `Hello Time` der aktuellen Root-Bridge.	1 - 2	2
Forward Delay	Das `Forward Delay` der aktuellen Root-Bridge.	4 - 30 s	15 s
Max Age	Der Parameter `Max Age` der aktuellen Root-Bridge.	6 - 40 s	20 s

Tab. 170: Globale Spanning-Tree-Einstellungen, Root-Bridge-Informationen

Parameter	Bedeutung	Mögliche Werte
Spalte „Topologie“	**Spanning Tree-Topologie-Informationen**	
Bridge ist Root	Ist das lokale Gerät aktuell die Root-Bridge, zeigt das Gerät dieses Kästchen markiert an, ansonsten leer.	Markiert, nicht markiert.
Root-Port	Derjenige Port des Geräts, von dem der aktuelle Pfad zur Root-Bridge führt. 0: die lokale Bridge ist Root.	Gültige Port-ID oder 0.
Root-Pfadkosten	Pfadkosten vom Root-Port des Geräts zur aktuellen Root-Bridge des gesamten Layer 2-Netzes. 0: die lokale Bridge ist Root.	0-200.000.000
Anzahl Topologieänderungen	Zählt, wie oft das Gerät seit dem Start einen Port durch Spanning Tree in den Zustand `Forwarding` gesetzt hat.	
Zeit seit letzter Änderung	Zeit seit der letzten Topologie-Änderung.	

Tab. 171: Globale Spanning-Tree-Einstellungen, Topologie-Informationen

Haben Sie die Funktion „MRP-Kompatibilität“ aktiviert, zeigt, das Gerät den Rahmen „Information“ mit zusätzlichen Informationen zur MRP-Kompatibilität an:

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Information	Wenn Sie die MRP-Kompatibilität aktiviert haben (RSTP over MRP) und eines der beteiligten Geräte ein Konfigurationsproblem feststellt, zeigt das Gerät „Konflikt mit der Bridge pppp / mm mm mm mm mm“ an. Im Normalbetrieb ist dieses Feld leer.	Meldung mit Bridge-ID oder leer.	-

Tab. 172: Globale Spanning-Tree-Einstellungen, Rahmen Information

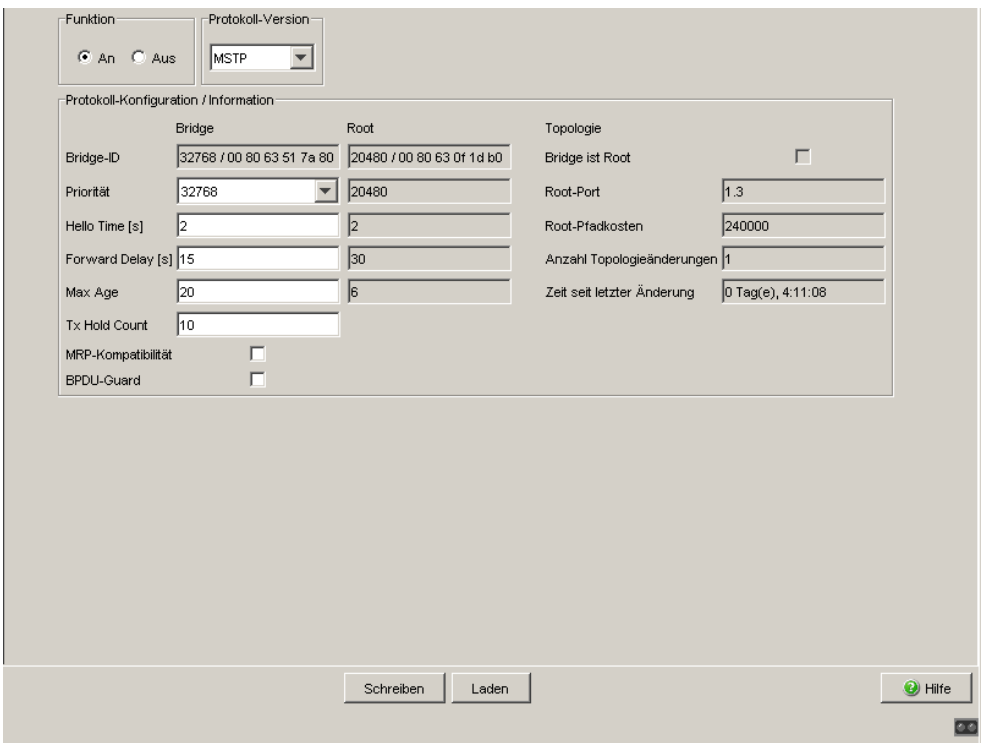


Abb. 70: Dialog Spanning Tree, Global

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 173: Schaltflächen

7.5.2 MSTP (Multiple Spanning Tree)

Dieser Dialog bietet Ihnen die Möglichkeit:
- die globale Multiple Spanning Tree-Instanz zu verwalten,
- eine Multiple Spanning Tree-Instanz zu erzeugen oder zu löschen,
- einer Multiple Spanning Tree-Instanz VLANs zuzuordnen und die MSTI zu verwalten.

Der Karteikartenreiter (Tab) für die globale Multiple-Spanning-Tree-Instanz trägt den Namen „MST Global (CIST)“. Diese Instanz ist stets vorhanden und kann nicht gelöscht werden. Sie enthält alle konfigurierten VLANs, die nicht explizit einer MSTI zugeordnet sind. Zu den Einstellungen gehört der MST-Region-Identifizierer, die Maximalanzahl an Hops für den Internal Spanning Tree (IST) sowie Informationen zu IST und CST (diese werden zusammen als CIST bezeichnet).

Die Karteikartenreiter (Tabs) für die MSTIs tragen den Namen MSTI, gefolgt von der Nr. der Instanz, z.B. „MSTI 2“. Hier können Sie die einzelnen Multiple-Spanning-Tree-Instanzen (MSTIs) zu verwalten. Das Gerät bietet Ihnen die Möglichkeit, bis zu 16 Multiple Spanning Tree-Instanzen (MSTIs) zu erzeugen. Voraussetzung für den Einsatz von MSTP ist, dass alle Bridges im Netz, die einen MSTP-Bereich bilden sollen, ebenfalls MSTP unterstützen.

Anmerkung: Um mstp zu nutzen, deaktivieren Sie die anderen Redundanzprotokolle auf diesem Gerät.

Anmerkung: Beachten Sie bei der Kombination von MSTP mit dem Management-VLAN 0 folgende Einschränkung: der DHCP-Clients des Gerätes versendet seine DHCP-Broadcasts ausschließlich in VLAN 1.

Dialog-Karteikartenreiter (Tab) MSTP Global (CIST)

Dieser Karteikartenreiter des Dialogs bietet Ihnen die Möglichkeit, die MST-Region und die globale Multiple Spanning Tree-Instanz (IST) innerhalb der MST-Region zu konfigurieren sowie Informationen zu IST und CST anzuzeigen.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Rahmen „MST Region Identifier“	Informationen zur MST-Region		
Name	Der Name der MSTP-Region, zu der das Gerät gehört.	Max. 32 Zeichen, Wert 0x21 (!) bis inkl. 0x7e (~)	Die MAC-Adresse des Geräts.
Revision Level	Versionsnummer der MSTP-Region, zu der das Gerät gehört.	0 -65.535	0
Digest	Die MD5-Prüfsumme der MSTP-Konfiguration.	16 Bytes in Hex-Darstellung.	

Tab. 174: Dialog Multiple Spanning-Tree-Einstellungen, MST Global (CIST), MST-Region

Anmerkung: Konfigurieren Sie alle Bridges einer MST-Region mit identischen Werten für:
– den Namen der MST-Region,
– den Revision-Level, und
– die Zuordnung der VLANs zu den MSTP-Instanzen.

Anmerkung: Nehmen Sie die Ports, die die Bridges einer MST-Region verbinden, als Tagged-Member in alle VLANs auf, die auf den Bridges eingerichtet sind. So vermeiden Sie mögliche Verbindungsunterbrechungen bei Topologieänderungen innerhalb der MST-Region.
Nehmen Sie auch die Ports, die eine MST-Region mit anderen MST-Regionen oder der CST-Region verbinden (sogenannte Boundary-Ports) in als Tagged-Member in alle VLANs auf, die auf beiden Regionen eingerichtet sind. So vermeiden Sie mögliche Verbindungsunterbrechungen bei Topologieänderungen, die die Boundary-Ports betreffen.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Rahmen „Globale CIST-Parameter“	Detail-Informationen zur globalen MST-Instanz (IST) der Region und CST.		
Maximum Hops	Maximale Anzahl von Bridges innerhalb der MST-Region in einem Ast zur Root-Bridge.	6 -40	20
Zugeordnete VLANs	Liste aller VLANs, die ausschließlich der globalen MST-Instanz und keiner anderen MSTI zugeordnet sind.	Liste aller statischen VLANs.	1;
Bridge-ID (Read-Only)	Die lokale Bridge-ID, zusammengesetzt aus der lokalen Priorität und der eigenen MAC-Adresse. Das Format ist ppppp / mm mm mm mm mm mm, mit: ppppp: Priorität (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).		
Root-ID	Die `Bridge-ID` der aktuellen Root-Bridge des gesamten Layer 2-Netzes.[a] Das Format ist ppppp / mm mm mm mm mm mm, mit: ppppp: Priorität (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).		
Regional-Root-ID	Die `Bridge-ID` der aktuellen Root-Bridge der der globalen Instanz (IST) der MST-Region, zu der dieses Gerät gehört.[b] Das Format ist ppppp / mm mm mm mm mm mm, mit: ppppp: Priorität (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).		
Root-Port	Derjenige Port des Geräts, von dem aus der aktuelle Pfad zur Root-Bridge des gesamten Layer 2-Netzes (CIST-Root) führt. 0: lokale Bridge ist CIST-Root.	Gültige Port-ID oder 0	-

Tab. 175: Dialog Multiple Spanning-Tree-Einstellungen, MST Global (CIST), Globale MST-Parameter

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Root-Pfadkosten	Externe Pfadkosten von der Regional-Root-Bridge der MST-Region des Geräts zur aktuellen Root-Bridge des gesamten Layer 2-Netzes (CIST-Root).[c] Diese sind für alle Geräte innerhalb einer MST-Region die selben. 0: Regional-Root-Bridge ist gleichzeitig CIST-Root-Bridge	0-200.000.000	
Interne Root-Pfad-kosten	Interne Pfadkosten vom Root-Port des Geräts zur aktuellen Regional-Root-Bridge der MST-Region des Geräts. 0: lokale Bridge ist Root.	0-200.000.000	-

Tab. 175: Dialog Multiple Spanning-Tree-Einstellungen, MST Global (CIST), Globale MST-Parameter

- [a] Diese Bridge heißt auch CIST-Root-Bridge (CIST: Common and Internal Spanning Tree). Sie hat die beste Bridge-ID aller Bridges - sowohl derer, die keiner MSTP-Region angehören (CST, Common Spanning Tree), als auch derer, die der globalen Instanz einer MSTP-Region angehören (Internal Spanning Tree, IST). Alle Bridges im gesamten Layer 2-Netz verwenden die Zeitparameter der CIST-Root-Bridge, z.B. die Hello Time.
- [b] Die IST-Regional-Root-ID kann für die MST-Region des Geräts mit der obigen CIST-Root-ID identisch sein, wenn die IST-Regional-Root-Bridge die beste Bridge-ID im gesamten Layer 2-Netz besitzt.
- [c] Diese sind identisch mit den Root-Pfadkosten von Spanning Tree oder Rapid Spanning Tree, wenn Sie kein MSTP einsetzen (in diesen Fällen betrachtet sich jedes Gerät als eine eigene Region).

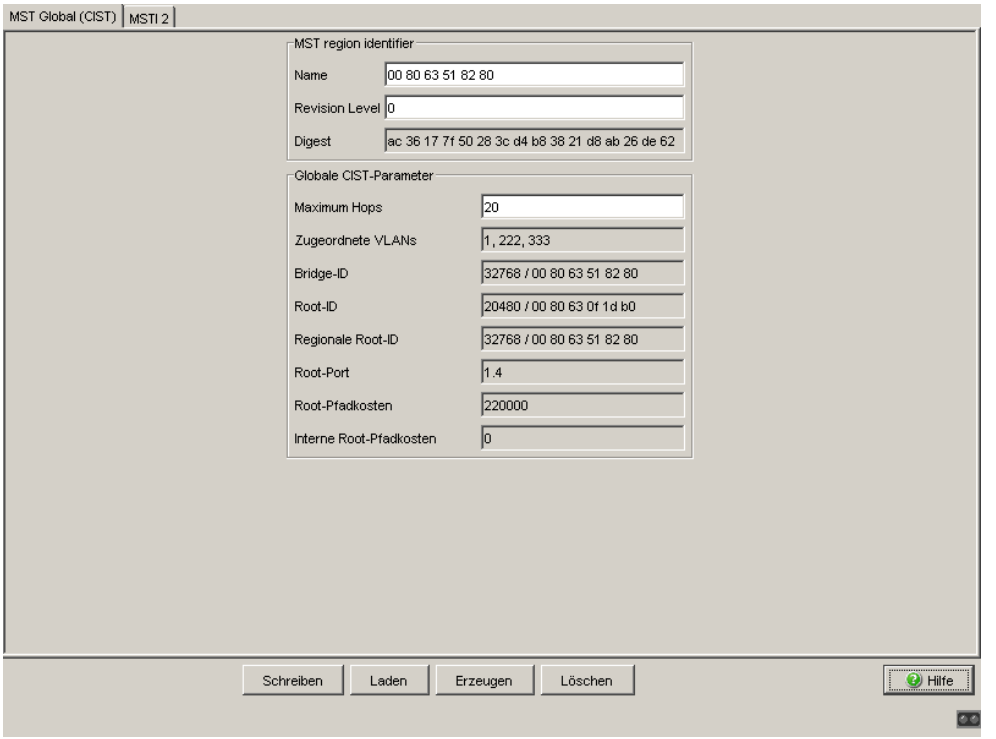


Abb. 71: Dialog Multiple Spanning Tree, MST Global (CIST)

Dialog-Karteikartenreiter MSTI (Multiple Spanning Tree Instance)

Die MSTI-Karteikartenreiter (Tabs) des Dialogs bieten Ihnen die Möglichkeit, die einzelnen Multiple Spanning Tree-Instanzen zu verwalten. Der Karteikartenreiter trägt den Namen MSTI, gefolgt von der Nr. der Instanz, z. B. „MSTI 2“.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Rahmen „VLANs“	Verwalten der VLANs, die dieser Multiple Spanning Tree-Instanz zugeordnet sind.		
Zugeordnete VLANs	Liste aller VLANs, die dieser MSTI momentan zugeordnet sind.	Teilmenge aller statisch eingerichteten VLANs.	Keine VLANs.

Tab. 176: Multiple Spanning-Tree-Einstellungen, MST-Instanz, VLANs

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Bedientaste „VLAN hinzufügen“	Öffnet einen Dialog zur Auswahl einer VLAN-ID aus den statisch eingerichteten VLANs des Geräts. Wählen Sie die gewünschte VLAN-ID aus und klicken Sie auf „OK“.	Eines der statischen VLANs.	
Bedientaste „VLAN entfernen“	Öffnet einen Dialog zur Auswahl einer VLAN-ID. Wählen Sie die gewünschte VLAN-ID aus und klicken Sie auf „OK“.	Ein VLAN, das der MSTI momentan zugeordnet ist	

Tab. 176: Multiple Spanning-Tree-Einstellungen, MST-Instanz, VLANs

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Rahmen „Instance-Parameter“	Detail-Informationen zur ausgewählten Multiple Spanning Tree-Instanz		
Priorität	Die lokale Bridge-`Priorität` für die ausgewählte MST-Instanz. Die Bridge-Priorität und die eigene MAC-Adresse zusammen bilden die eigene `Bridge-ID`. Das Gerät mit dem besten, also numerisch niedrigsten Prioritätswert wird zum Root-Gerät des ausgewählten MST-Bereichs. Bestimmen Sie das Root-Gerät, indem Sie diesem Gerät die beste Priorität in der `Bridge-ID` unter allen Geräten in dem ausgewählten MST-Bereich zuweisen. Geben Sie den Wert als Vielfaches von 4.096 ein.	0 ≤ n*4.096 ≤ 61.440	32.768
Bridge-ID	Die lokale `Bridge-ID`, zusammengesetzt aus der lokalen `Priorität` + MSTI, gefolgt von der eigenen MAC-Adresse. Das Format ist ppppp / mm mm mm mm mm mm, mit: ppppp: Priorität+MSTI (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).	0 - 65.534; Summe aus Priorität (0 - 61.440 in Schritten von 4.096) und MSTI (1 - 4.094)	32.768 + MSTI
Zeit seit letzter Änderung	Zeit seit der letzten Topologie-Änderung für diese MST-Instanz		
Topologie-Änderungen	Zählt, wie oft das Gerät seit dem Start der ausgewählten MST-Instanz einen Port durch Spanning Tree in den Zustand `forwarding` gesetzt hat.		

Tab. 177: Multiple Spanning-Tree-Einstellungen, MST-Instanz, Parameter

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Root-ID	Die `Bridge-ID` der aktuellen Root-Bridge des ausgewählten MST-Bereichs. Das Format ist ppppp / mm mm mm mm mm mm, mit: ppppp: Priorität (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).	0 - 65.534; Summe aus Priorität (0 - 61.440 in Schritten von 4.096) und MSTI (1 - 4.094)	
Root-Pfadkosten	Pfadkosten vom Root-Port zur aktuellen Root-Bridge des ausgewählten MST-Bereichs. 0: Bridge ist Root für diesen MST-Bereich.	0-200.000.000	
Root-Port	Derjenige Port des Geräts, von dem der aktuelle Pfad zur Root-Bridge des ausgewählten MST-Bereichs führt. 0: Bridge ist Root für diesen MST-Bereich.	Gültige Port-ID oder 0	

Tab. 177: Multiple Spanning-Tree-Einstellungen, MST-Instanz, Parameter

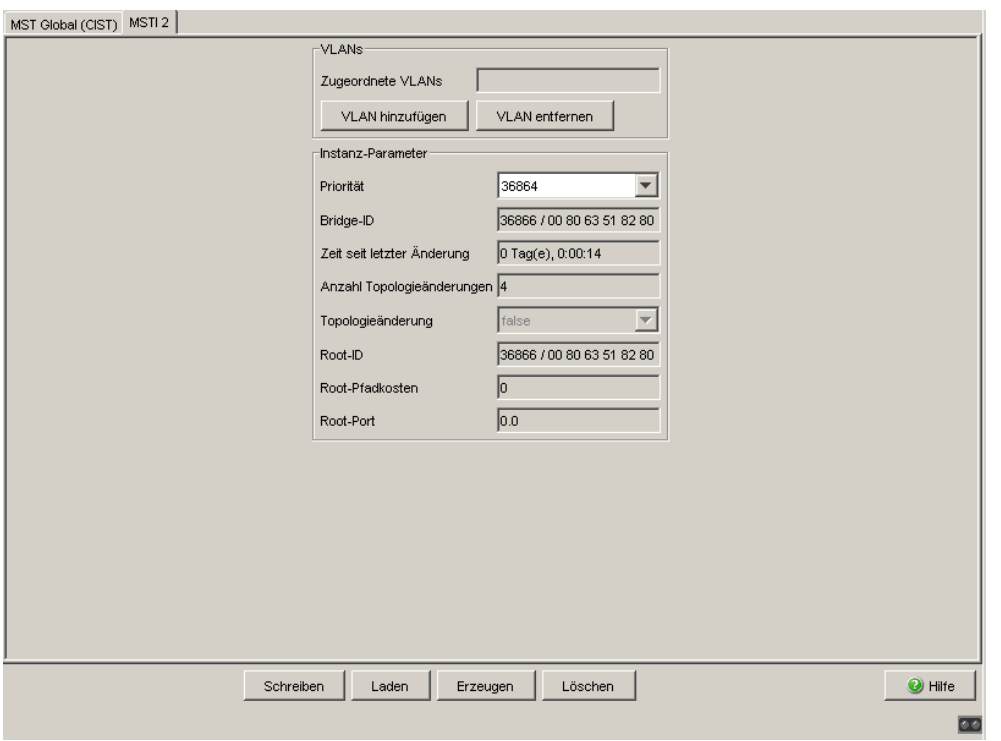


Abb. 72: Dialog Multiple Spanning Tree, MSTI <ID>

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Erzeugen	Fügt eine MSTP-Instanz hinzu.
Löschen	Entfernt eine MSTP-Instanz.
Hilfe	Öffnet die Online-Hilfe.

Tab. 178: Schaltflächen

7.5.3 Port

Anmerkung: Deaktivieren Sie das Spanning-Tree-Protokoll an den Ports, die an einen HIPER-Ring, Fast HIPER-Ring oder eine Ring-/Netzkopplung angeschlossen sind, da Spanning-Tree und Ring-Redundanz oder Ring-/Netzkopplung sich gegenseitig beeinflussen.
Schalten Sie in einem MRP-Ring die MRP-Kompatibilität an, wenn Sie RSTP und MRP in Kombination verwenden wollen.
Wenn Sie RSTP mit einem MRP-Ring kombinieren, stellen Sie auf den Geräten im MRP-Ring eine bessere, also numerisch kleinere RSTP-Bridge-Priorität ein als auf den Geräten im angeschlossenen RSTP-Netz. Damit helfen Sie, eine Verbindungsunterbrechung zu Geräten außerhalb des Rings zu vermeiden.

Die MSTI-Karteikartenreiter (Tabs) des Dialogs bieten Ihnen die Möglichkeit, die einzelnen Multiple Spanning Tree-Instanzen zu verwalten. Der Karteikartenreiter trägt den Namen MSTI, gefolgt von der Nr. der Instanz, z. B. „MSTI 2“.

- Spanning Tree an den einzelnen Ports aus- oder einzuschalten, die Ports für die globale MST-Instanz (CIST) zu konfigurieren und Informationen über den Port-Zustand anzuzeigen,
- verschiedene Schutzfunktionen an den Ports einzustellen,
- die Ports für eine existierende MST-Instanz zu konfigurieren (Port-Pfadkosten und Port-Priorität) und Informationen über den Port-Zustand abzulesen für die ausgewählte MSTI anzuzeigen.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Karteikartenreiter „CIST“	Port-Konfiguration und -Informationen zur globalen MSTI (IST) sowie der CST.		
Modul.Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.		
STP aktiv	Hier können Sie Spanning Tree für diesen Port ein- oder ausschalten. Ist Spanning Tree global eingeschaltet und an einem Port ausgeschaltet, sendet dieser Port keine STP-BPDUs und verwirft empfangene STP-BPDUs. **Anmerkung:** Möchten Sie parallel zu Spanning Tree andere Layer 2-Redundanzprotokolle wie HIPER-Ring oder Ring-/Netzkopplung einsetzen, achten Sie darauf, die Ports, die an diesen Protokollen beteiligt sind, in diesem Dialog für Spanning Tree auszuschalten. Andernfalls arbeitet die Redundanz möglicherweise nicht wie vorgesehen oder es kann zu Loops kommen.	`An`, `Aus`	`An`

Tab. 179: Port-bezogene STP-Einstellungen und -Anzeigen, CIST

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Port-Status (read-only)	Zeigt den STP-Port-Status bezüglich der globalen MSTI (IST) an.	`discarding`, `learning`, `forwarding`, `disabled`, `manualForwarding`, `notParticipate`	-
Port-Rolle (read-only)	Zeigt die STP-Port-Rolle bezüglich der globalen MSTI (IST) an.	`root` `alternate` `designated` `backup` `master` `disabled`	-
Port-Pfadkosten	Eingabe der Pfadkosten bezüglich der globalen MSTI (IST) zur Bevorzugung redundanter Pfade. Beim Wert 0 ermittelt der Switch für die globale MSTI (IST) automatisch die Pfadkosten abhängig von der Übertragungsrate.	0 - 200.000.000	0 (automatisch)
Port-Priorität	Geben Sie hier die Port-Priorität (die vier obersten Bits der Port-Identifikation ein) bezüglich der globalen MSTI (IST) ein, als Dezimalzahl des obersten Bytes der Port-ID.	16 ≤ n·16 ≤ 240	128
Empfangene Bridge-ID (read-only)	Zeigt die entfernte Bridge-ID an, von der dieser Port zuletzt eine STP-BPDU empfangen hat.[a]	Bridge-Identifikation (Format ppppp / mm mm mm mm mm mm)	-
Empfangene Port-ID (read-only)	Zeigt die Port-ID auf der entfernten Bridge an, von der dieser Port zuletzt eine STP-BPDU empfangen hat.[a]	Port-Identifikation, Format pn nn, mit p: Port-Priorität / 16, nnn: Port-Nr., (beide hexadezimal)	-
Empfangene Pfadkosten (read-only)	Zeigt die Pfadkosten der entfernten Bridge an, die diese von ihrem Root-Port zur CIST-Root-Bridge hat.[a]	0-200.000.000	-

Tab. 179: Port-bezogene STP-Einstellungen und -Anzeigen, CIST

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Admin-Edge-Port	Aktivieren Sie diese Einstellung ausschließlich dann, wenn ein Endgerät an den Port angeschlossen ist (Administrativ: vorgegebene Einstellung) . Dann geht der Port nach Aufbau eines Links sofort in den Forwarding-Status, ohne zuerst die STP-Stati zu durchlaufen. Empfängt der Port trotzdem eine STP-BPDU, blockiert das Gerät den Port und klärt dessen STP-Port-Rolle. Der Port kann dabei in einem anderen Status übergehen, z.B. `forwarding`, `discarding`, `learning`. Deaktivieren Sie die Einstellung, wenn der Port an eine Bridge angeschlossen ist. Der Port durchläuft nach Aufbau eines Links dann zuerst die STP-Stati, bevor er ggf. in den Zustand `forwarding` geht. Diese Einstellung gilt für alle MSTIs.	`aktiv` (Kästchen markiert), `inaktiv` (Kästchen leer)	`inaktiv`
Auto-Edge-Port	Die Einstellung Auto-Edge-Port berücksichtigt das Gerät ausschließlich, wenn der Parameter Admin-Edge-Port deaktiviert ist. Ist Auto-Edge-Port aktiv, setzt das Gerät den Port nach dem Aufbau eines Links nach 1,5 · `Hello Time` (in der Voreinstellung 3 s) in den Zustand forwarding. Ist Auto-Edge-Port deaktiviert, wartet das Gerät statt dessen `Max Age` (in der Voreinstellung 20 s). Diese Einstellung gilt für alle MSTIs.	`aktiv` (Kästchen markiert), `inaktiv` (Kästchen leer)	`aktiv`

Tab. 179: Port-bezogene STP-Einstellungen und -Anzeigen, CIST

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Oper-Edge-Port	Das Gerät setzt den Zustand „Oper-Edge-Port“ (Operational: in Betrieb) auf `true`, wenn es keine STP-BPDUs empfangen hat, also ein Endgerät angeschlossen ist. Es setzt den Zustand auf `false`, wenn es eine STP-BPDUs empfangen hat, also eine Bridge angeschlossen ist. Dieser Zustand gilt für alle MSTIs.	`true`, `false`	-
Ist Punkt-zu-Punkt	Das Gerät setzt den Zustand „Oper Punkt-zu-Punkt“ (Operational: in Betrieb) auf `true`, wenn dieser Port eine Vollduplex-Verbindung zu einem STP-Gerät hat. Ansonsten setzt es den Zustand auf `false` (z.B. wenn ein Hub angeschlossen ist). Die Punkt-zu-Punkt-Verbindung ist eine direkte Verbindung zwischen 2 RSTP-Geräten. Die direkte, dezentrale Kommunikation zwischen den beiden Bridges es bewirkt eine kurze Rekonfigurationszeit. Dieser Zustand gilt für alle MSTIs.	`true`, `false` Das Gerät bestimmt diesen Zustand aus dem Duplex-Modus: FDX: `true` HDX: `false`	

Tab. 179: Port-bezogene STP-Einstellungen und -Anzeigen, CIST

– [a] Diese Spalten zeigen Ihnen Detail-Informationen, die über die bisher üblichen Details hinausgehen:
Für Designated-Ports zeigt das Gerät die Information der STP-BPDU an, die der Port zuletzt empfangene hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz.
Für die Port-Rollen Alternate-, Backup-, Master- und Root sind diese

Informationen im stationären Zustand (statische Topologie) identisch mit den Designated-Informationen.
Hat ein Port keinen Link oder hat er noch keine STP-BDPU der aktuellen MSTI empfangen, zeigt das Gerät die Werte an, die der Port als Designated-Port senden würde.

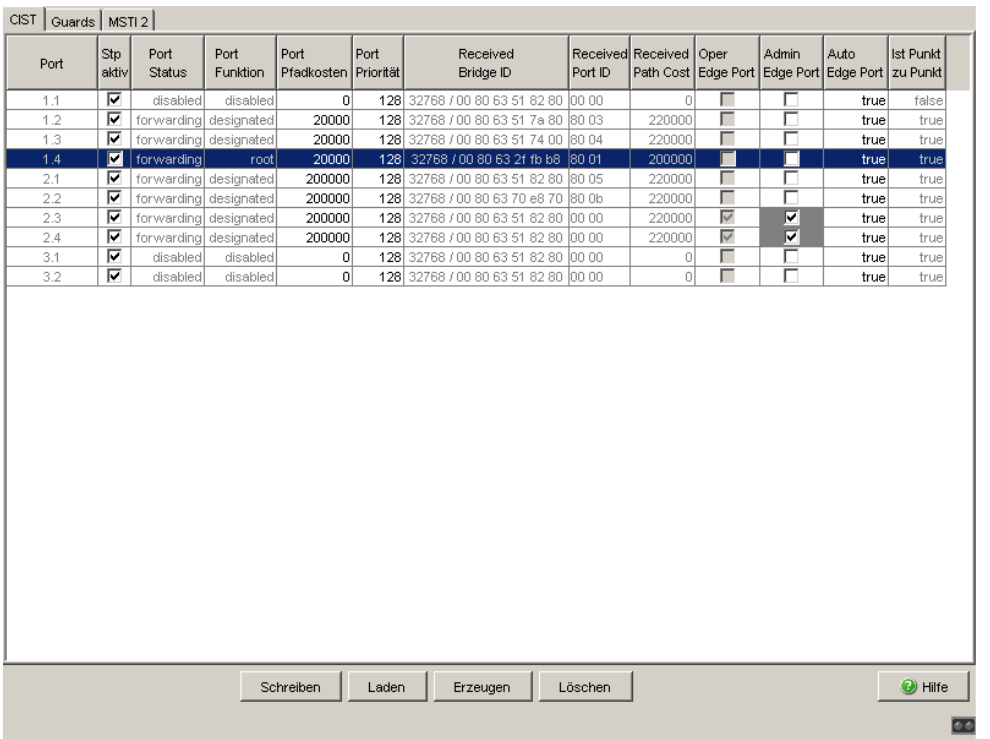


Abb. 73: Dialog Multiple Spanning Tree, Port, Karteikartenreiter CIST

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Karteikarten-reiter „Guards“	Schutzeinstellungen für die Ports.		
Modul.Port	Portbezeichnung durch Modul- und Port-nummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.		

Tab. 180: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Root-Guard	Die Einstellung „Root-Guard“ ist ausschließlich für Ports in der STP-Rolle `designated` relevant. Empfängt ein solcher Port eine STP-BPDU mit einer besseren Pfadinformation zur Root als die dem Gerät bekannte, dann verwirft das Gerät die BPDU und setzt den Port-Zustand in `discarding`, statt dem Port die STP-Port-Rolle `root` zuzuweisen. So hilft das Gerät, Ihr Netz vor Angriffen mit STP-BPDUs, die die Topologie zu verändern versuchen, und vor Fehlkonfigurationen zu schützen. Bleiben STP-BPDUs mit einer besseren Pfad-information zur Root aus, dann setzt das Gerät den Vermittlungszustand des Ports wieder entsprechend der Port-Rolle. **Anmerkung:** Die Einstellungen „Root-Guard“ und „Loop Guard“ schließen sich gegenseitig aus. Wenn Sie eine Einstellung aktivieren, während die andere bereits aktiv ist, schaltet das Gerät die andere ab.	`aktiv` (Kästchen markiert), `inaktiv` (Kästchen leer)	`inaktiv`

Tab. 180: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
TCN-Guard	Ist die Einstellung „TCN-Guard“ aktiv (TCN: Topology Change Notification), ignoriert der Port in empfangenen STP-BPDUs das Topology-Change-Flag, das eine Topologie-Änderung ankündigt. So schützt das Gerät Ihr Netz vor Angriffen mit STP-BPDUs, die die Topologie zu verändern versuchen. Ist die Einstellung „TCN-Guard“ inaktiv, reagiert das Gerät gemäß dem Protokoll auf empfangene STP-BPDUs: es löscht seine Adresstabelle und leitet die TCN-Information weiter. **Anmerkung:** Enthält die empfangene BPDU außer dem Topology-Change-Flag weitere Informationen, die eine Topologie-Änderung bewirken, verarbeitet das Gerät diese auch bei aktiviertem TCN-Guard. Beispiel: das Gerät empfängt eine bessere Pfadinformation zur Root als die bereits bekannte.	`aktiv` (Kästchen markiert), `inaktiv` (Kästchen leer)	`inaktiv`

Tab. 180: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Loop-Guard	Die Einstellung „Loop-Guard“ ist ausschließlich sinnvoll für Ports in der STP-Rolle `alternate`, `backup` oder `root`. Ist die Einstellung „Loop-Guard“ aktiv und empfängt der Port eine Zeitlang keine STP-BPDUs mehr, setzt das Gerät den Port in den Zustand `discarding` (Port sendet keine Daten mehr). Das Gerät setzt den Port zusätzlich in den sogenannten „Loop-inkonsistenten Zustand“ und zeigt dies in der Spalte „Loop-Zustand“ an. Das Gerät verhindert einen möglichen Loop, wenn keine STP-BPDUs mehr empfangen werden, z.B., wenn Sie STP auf dem entfernten Gerät abschalten oder der Link lediglich in der Empfangsrichtung betriebsunfähig wird. Empfängt der Port wieder BPDUs, setzt das Gerät den Loop-inkonsistenten Zustand des Ports zurück auf `false` und den Vermittlungszustand des Ports entsprechend der Port-Rolle. Ist die Einstellung „Loop-Guard“ inaktiv, setzt das Gerät den Port dagegen nach dem Ausbleiben von STP-BPDUs in den Zustand `forwarding`. **Anmerkung:** Die Einstellungen „Root-Guard“ und „Loop Guard“ schließen sich gegenseitig aus. Wenn Sie eine Einstellung aktivieren, während die andere bereits aktiv ist, schaltet das Gerät die andere ab.	`aktiv` (Kästchen markiert), `inaktiv` (Kästchen leer)	`inaktiv`
Loop-Zustand (read-only)	Anzeige des Status des Loop-inkonsistenten Zustands. Das Gerät setzt den Loop-inkonsistenten Zustand eines Ports auf `true`, wenn an dem Port die Einstellung „Loop-Guard“ aktiv ist und der Port keine STP-BPDUs mehr empfängt. Das Gerät lässt dabei den Port im Vermittlungszustand `discarding`, und hilft so, einen möglichen Loop zu verhindern. Empfängt der Port wieder STP-BPDUs, setzt das Gerät den Loop-inkonsistenten Zustand zurück auf `false`.	`true`, `false`	-

Tab. 180: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Übergänge in Loop-Zustand (read-only)	Zählt, wie oft das Gerät den Port in den Loop-inkonsistenten Zustand (Spalte „Loop-Zustand“ `true`) gesetzt hat.	0 - 4.294.967.295 (2^{32}-1)	0
Übergänge aus Loop-Zustand	Zählt, wie oft das Gerät den Port aus dem Loop-inkonsistenten Zustand (Spalte „Loop-Zustand“ `true`) zurückgesetzt hat.	0 - 4.294.967.295 (2^{32}-1)	0
BPDU-Guard-Effect (read-only)	Der Zustand „BPDU-Guard-Effect“ ist ausschließlich für Edge-Ports relevant (Ports mit der Einstellung „Admin-Edge-Port“ `true`) und lediglich dann, wenn die globale Funktion „BPDU Guard“ aktiv ist (siehe Tabelle 169). Empfängt ein solcher Port eine beliebige STP-BPDU, setzt das Gerät den Port-Zustand „BPDU Guard Effect“auf `true` und seinen Vermittlungszustand in `discarding`. So hilft Ihnen das Gerät, Ihr Netz an Endgeräteports vor Fehlkonfigurationen oder Angriffen mit STP-BPDUs zu schützen, die die Topologie zu verändern versuchen. Um den Port aus dem gesperrten Zustand wieder in einen normalen Vermittlungszustand zu bringen, ziehen und stecken Sie den Link oder schalten Sie die Port-Einstellung „Admin-Edge-Port“ aus und wieder ein.	`true`, `false`	-

Tab. 180: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

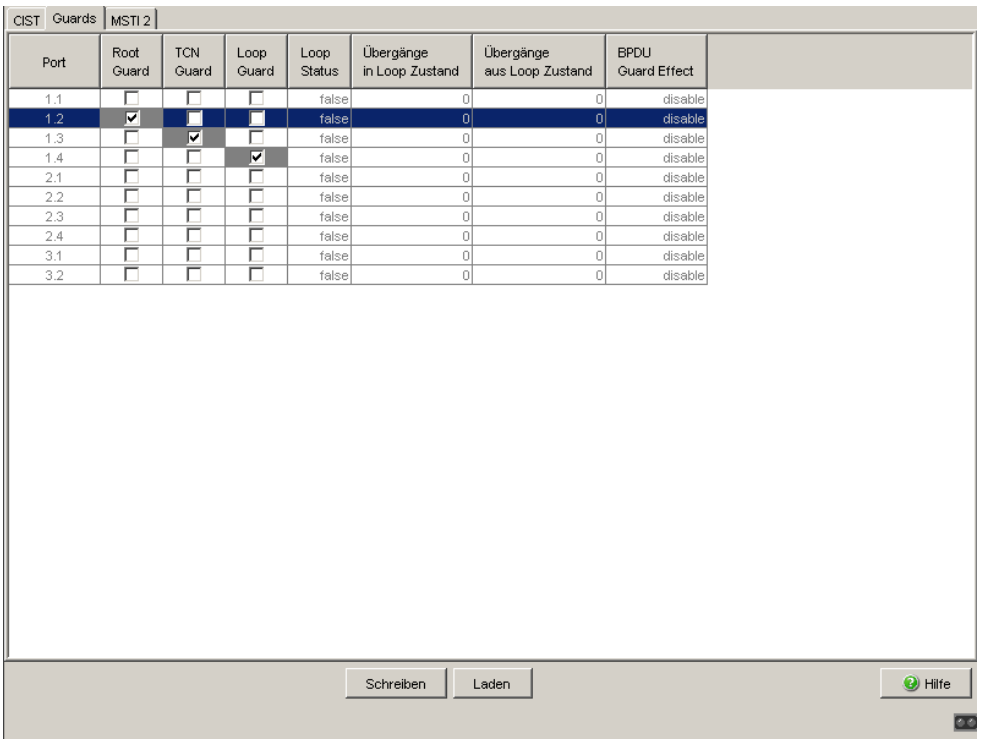


Abb. 74: Dialog Multiple Spanning Tree, Port, Karteikartenreiter Guards

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Karteikarten-reiter „MSTI <ID>“	Port-Konfiguration und -Informationen zur ausgewählten MSTI. **Anmerkung:** Anmerkung: das Gerät zeigt die Karteikartenreiter MSTI ... ausschließlich dann an, wenn Sie mindestens 1 MST-Instanz konfiguriert haben.		
Port-Status (read-only)	Zeigt den STP-Port-Status bezüglich der aktuellen MSTI an.	`discarding`, `learning`, `forwarding`, `disabled`, `manualForwarding`, `notParticipate`	-

Tab. 181: Port-bezogene STP-Einstellungen und -Anzeigen, pro MSTI

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Port-Rolle (read-only)	Zeigt die STP-Port-Rolle bezüglich der aktuellen MSTI an.	`root, alternate, designated, backup, master, disabled`	-
Port-Pfadkosten	Eingabe der Pfadkosten bezüglich der aktuellen MSTI zur Bevorzugung redundanter Pfade. Beim Wert 0 ermittelt der Switch automatisch die Pfadkosten abhängig von der Übertragungsrate.	0 - 200.000.000	0 (automatisch)
Port-Priorität	Geben Sie hier die Port-Priorität (die vier obersten Bits der Port-Identifikation ein) bezüglich der aktuellen MSTI ein, als Dezimalzahl des obersten Bytes der Port-D.	16 ≤ n*16 ≤ 240	128
Empfangene Bridge-ID (read-only)	Zeigt die entfernte Bridge-ID der aktuellen MSTI an, von der dieser Port zuletzt eine BPDU empfangen hat.[a].	Bridge-Identifikation (Format ppppp / mm mm mm mm mm mm)	-
Empfangene Port-ID (read-only)	Zeigt die Port-ID auf der entfernten Bridge der aktuellen MSTI an, von der dieser Port zuletzt eine BPDU empfangen hat.[a]	Port-Identifikation, Format pn nn, mit p: Port-Priorität / 16, nnn: Port-Nr., (beide hexadezimal)	-
Empfangene Pfadkosten (read-only)	Zeigt die Pfadkosten der entfernten Bridge an, die diese von ihrem Root-Port zur Root-Bridge der aktuellen MSTI hat.[a].	0-200.000.000	-

Tab. 181: Port-bezogene STP-Einstellungen und -Anzeigen, pro MSTI

– [a] Diese Spalten zeigen Ihnen Detail-Informationen, die über die bisher üblichen Details hinausgehen:
  Für Designated-Ports zeigt das Gerät die Information der STP-BPDU an, die der Port zuletzt empfangene hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz.
  Für die Port-Rollen Alternate-, Backup-, Master- und Root sind diese

Informationen im stationären Zustand (statische Topologie) identisch mit den Designated-Informationen.
Hat ein Port keinen Link oder hat er noch keine STP-BDPU der aktuellen MSTI empfangen, zeigt das Gerät die Werte an, die der Port als Designated-Port senden würde.

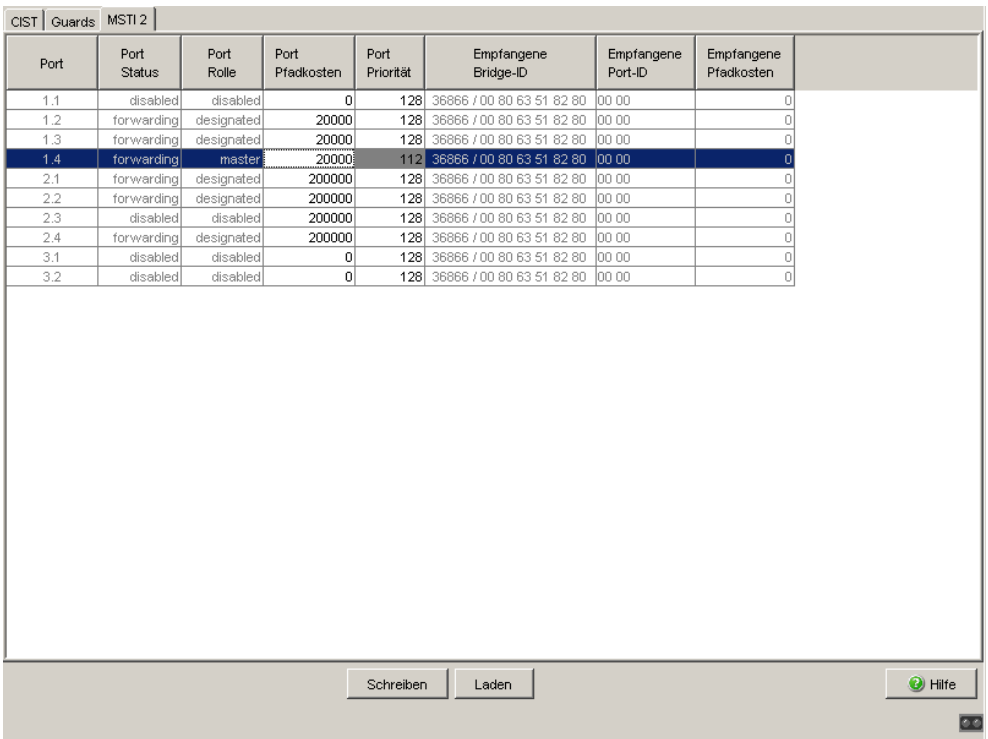


Abb. 75: Dialog Multiple Spanning Tree, Port, Karteikartenreiter MSTI <ID>

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 182: Schaltflächen

7.6 VRRP/HiVRRP

Das Virtual Router Redundancy Protocol (VRRP) beschreibt ein Verfahren, das es ermöglicht, auf den Ausfall eines Routers zu reagieren.
VRRP findet seine Anwendung in Netzen mit Endgeräten, die lediglich einen Eintrag für das „Default Gateway“ unterstützen. Fällt das „Default Gateway“ aus, dann sorgt VRRP dafür, dass die Endgeräte ein redundantes Gateway finden.
Die Firma Hirschmann hat das VRRP weiterentwickelt zum Hirschmann Virtual Router Redundancy Protocol (HiVRRP). HiVRRP bietet bei entsprechender Konfiguration Umschaltzeiten von unter 400 ms.

Anmerkung: Detaillierte Informationen zu VRRP und HiVRRP finden Sie im Anwender-Handbuch „Routing-Konfiguration“.

7.6.1 VRRP/HiVRRP Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, generelle Einstellungen und Einstellungen pro Port für das VRRP vorzunehmen.
Sie können:
– bis zu 8 virtuelle Router pro Port und
– bis zu 16 Einträge mit HiVRRP pro Router
konfigurieren.

Generelle Einstellungen

Parameter	Bedeutung
Funktion	Ein-/Ausschalten der VRRP-Funktion
Version	Anzeige der VRRP-Version
VRRP-Master-Trap senden	Sobald der Router die VRRP-Master-Funktion übernimmt, sendet er einen Master-Trap
VRRP-Authentifizierungsfehler-Trap senden	Sobald der Router eine VRRP-Information mit falscher Authentifizierung empfängt, sendet er einen VRRP-Authentifizierungsfehler-Trap.

Tab. 183: VRRP Generelle Einstellungen

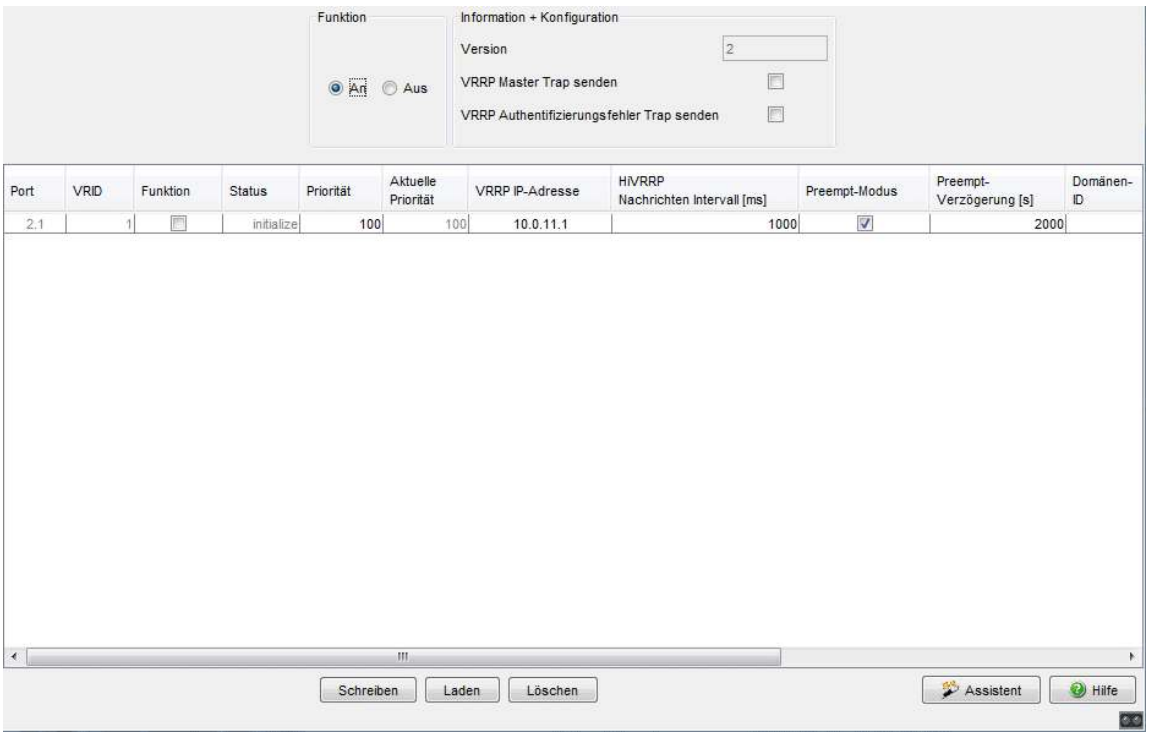


Abb. 76: Dialog VRRP/HiVRRP-Konfiguration

VRRP-Instanz-Einstellungen

Parameter	Bedeutung
Modul	Modul des Gerätes
Port	Port, für den dieser Eintrag gilt
VRID	Virtuelle Router-Identifikation (Wert 1-255)
Funktion	Ein-/Ausschalten der VRRP-Instanzen

Tab. 184: VRRP-Konfigurationstabelle

Parameter	Bedeutung
Status	VRRP-Status – `initialize`: VRRP ist in der Initialisierungsphase. Bisher ist kein Master benannt. – `backup`: Der Router beobachtet die Möglichkeit, Master zu werden. – `master`: Der Router ist Master.
Priorität	Eingestellte VRRP-Priorität (Wert: 1-255, Voreinstellung: 100). Der Router mit dem höchsten Wert übernimmt die Master-Funktion. Ist die virtuelle Router-IP-Adresse gleich der IP-Adresse des Router-Interfaces, dann heißt dieser Router „Owner“. Existiert ein Owner, dann weist VRRP ihm die VRRP-Priorität 255 zu und deklariert ihn so zum Master.
Aktuelle Priorität	Tatsächlich verwendete VRRP-Priorität (Wert: 1-255). Dieser Wert ist normalerweise gleich der eingestellten VRRP-Priorität, kann aber kleiner sein, wenn überwachte Tracking-Objekte im Zustand „down“ sind.
VRRP IP-Adresse	Primäre virtuelle Router-IP-Adresse.
HiVRRP Nachrichten-Intervall	Intervall für die Aussendung von Nachrichten (Advertisement) als Master (Wert: bei VRRP: `1-255 s`, Wert bei HiVRRP: `100-255.000 ms`, Voreinstellung: `1 s`).
Preempt-Modus	Diese Einstellung legt fest, ob dieser Router als Backup-Router einem Master-Router mit niedrigerer VRRP-Priorität die Master-Rolle entzieht. Bei ausgeschaltetem Preempt-Modus beansprucht dieser Router die Master-Rolle erst, wenn die IP-Multicast-Nachricht des existierenden Masters ausbleibt.
Preempt-Verzögerung	Der Preempt-Modus im Zusammenwirken mit VRRP-Tracking kann das Umschalten auf einen besseren Router ermöglichen. Dynamische Routing-Verfahren benötigen aber eine gewisse Zeit, auf geänderte Routen zu reagieren und ihre Routingtabelle neu zu befüllen. Um während dieser Zeit Paketverluste zu vermeiden, bietet die verzögerte Umschaltung (Preempt-Verzögerung) vom Master- auf den Backup-Router den dynamischen Routingverfahren die Möglichkeit, ihre Routingtabellen zu befüllen (Wert: 0-65.535 s, Voreinstellung 0 s).
Domänen-ID	Die Domänen-ID ist eine Nummer zur Identifizierung der Domäne (siehe auf Seite 323 „HiVRRP-Domänen“). Wert: 0-8, Voreinstellung 0 = keine Domäne.
Domänen-Rolle	`none`: kein Mitglied einer Domäne `member`: übernimmt das Verhalten des Supervisors `supervisor`: bestimmt das Verhalten der Domäne
Authentifizierung	Die Art der angewendeten Authentifizierung: – `noAuthentication`: Austausch von VRRP-Informationen ohne Authentifizierung. – `simpleTextPassword`: Austausch von VRRP-Informationen mit Klartext-Passwort-Authentifizierung.
Schlüssel	Passwort für Authentifizierung. Zur Kommunikation benötigen die Router mit der gleichen virtuellen Router-IP-Adresse die gleiche Authentifizierungseinstellung.
Master-IP-Adresse	Tatsächliche Router-Interface-IP-Adresse des Masters.

Tab. 184: VRRP-Konfigurationstabelle

VRRP-Router-Instanz einrichten

☐ Klicken Sie im Dialog `Redundanz:VRRP/HiVRRP:Konfiguration` auf „Assistent“ rechts unten.

☐ Wählen Sie in der Tabelle des Assistenten-Dialogs eine Port-Zeile aus und geben Sie in der Zeile VRID die Virtuelle Router-Identifikation ein. Sie können bis zu 8 virtuelle Router je Interface konfigurieren.

☐ Klicken Sie „Weiter“.

☐ Geben Sie unter „Eintrag bearbeiten“ im Rahmen „Grundkonfiguration“ ein:

- die IP-Adresse des virtuellen Routers
- die VRRP-Priorität
- die Art der Authentifizierung
- den Schlüssel für die Authentifizierung
- die Preempt-Verzögerung
- das Nachrichten-Intervall.

Wählen Sie nach Bedarf den Preempt-Modus.

Schalten Sie die VRRP-Funktion ein.

Wenn Sie

- Umschaltzeiten unter 3 s erzielen wollen,
- erreichen wollen, dass die Router miteinander mittels Unicasts kommunizieren,
- Domänen einrichten wollen oder
- Link-Down Meldungen verschicken wollen,

aktivieren Sie das Feld "HiVRRP".

Geben Sie im Rahmen „HiVRRP“ ein:

- das "Nachrichten-Intervall"
- die "Zieladresse". Die HiVRRP-Zieladresse ist die IP-Adresse des Partner-HiVRRP-Routers.
- die IP-Adresse des zweiten Routers an den die Link-Down-Meldungen verschickt werden. Diese Funktion kann verwendet werden, wenn der virtuelle Router aus zwei VRRP-Routern besteht.
- die Domänen-ID
- die Domänen-Rolle

☐ Klicken Sie auf „Fertig“, um das VRRP-Router-Interface in die VRRP-Router-Interface-Tabelle zu übernehmen
oder
☐ Klicken Sie auf „Weiter", um unter „Tracking" dem virtuellen Router Tracking-Objekte zuzuordnen. Der Wechsel eines Tracking-Objektes in den Zustand „Down” führt zur Dekrementierung der VRRP-Priorität. Wählen sich einen bestehenden Tracking-Eintrag aus und klicken Sie auf „Hinzufügen”. Sie können bis zu 8 Tracking-Objekte hinzufügen. Achten Sie darauf, dass die Summe der Dekremente aller zugewiesenen Tracking-Einträge kleiner ist als die VRRP-Priorität dieses VRRP-Interfaces.

Anmerkung: Da der IP-Adress-Owner per Definition die feste VRRP-Priorität 255 besitzt, setzt die VRRP-Tracking-Funktion voraus, dass die IP-Adressen der VRRP-Router-Interfaces ungleich der virtuellen Router-IP-Adresse sind.

Anmerkung: Damit nach der Dekrementierung der VRRP-Priorität des Masters durch die Tracking-Funktion der Backup-Router die Master-Rolle übernehmen kann, aktivieren Sie den Preempt-Modus.

☐ Klicken Sie auf „Fertig“, um das VRRP-Router-Interface in die VRRP-Router-Interface-Tabelle zu übernehmen
oder
☐ Klicken Sie auf „Weiter", falls Sie unter „Assoziierte IP-Adressen" (Multinetting) weitere IP-Adressen eintragen möchten.
☐ Klicken Sie auf „Fertig“, um das VRRP-Router-Interface in die VRRP-Router-Interface-Tabelle zu übernehmen.

VRRP-Router-Instanz konfigurieren

☐ Doppelklicken Sie im Dialog `Redundanz:VRRP/HiVRRP:Konfiguration` in eine Zelle der Tabelle und bearbeiten Sie den Eintrag oder klicken Sie mit der rechten Maustaste in eine Zelle und wählen einen Wert aus.
☐ Alternativ zur direkten Bearbeitung in der Tabelle können Sie eine Zeile in der Tabelle markieren und mit Hilfe des Assistenten bearbeiten.

VRRP-Router-Instanz löschen

☐ Wählen Sie im Dialog `Redundanz:VRRP/HiVRRP:Konfiguration` eine Zeile aus und klicken Sie auf „Eintrag löschen“. Damit löschen Sie die Zeile.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Löschen	Entfernt den markierten Tabelleneintrag.
Assistent	Öffnet den „Assistenten“. Mit dem „Assistenten“ weisen Sie einem Port die zulässigen MAC-Adressen zu.
Zurück	Zeigt die vorherige Seite wieder an. Änderungen gehen dabei verloren.
Weiter	Übernimmt die Änderungen und öffnet die nächste Seite.
Fertig	Übernimmt die Änderungen und schließt die Konfiguration ab.
Abbrechen	Beendet den Assistenten. Änderungen gehen dabei verloren.
Hilfe	Öffnet die Online-Hilfe.

Tab. 185: Schaltflächen

7.6.2 HiVRRP-Domänen

Eine HiVRRP-Instanz ist eine als HiVRRP konfigurierte Router-Instanz mit Funktionen, die das HiVRRP beinhaltet. In einer HiVRRP-Domäne fassen Sie mehrere HiVRRP-Instanzen eines Routers zu einer Management-Einheit zusammen. Eine HiVRRP-Instanz ernennen Sie zum Supervisor der HiVRRP-Domäne. Dieser Supervisor regelt das Verhalten aller HiVRRP-Instanzen seiner Domäne.
Der Router unterstützt bis zu 8 Domänen.

HiVRRP-Domänen anzeigen

Parameter	Bedeutung
Domain-ID	Identifikationsnummer der Domänen
Status	Status des Supervisors der Domäne `noError`: Supervisor ist aktiv `SupervisorDown`: Supervisor ist nicht aktiv `noSupervisor`: kein Supervisor festgelegt
Supervisor-Port	HiVRRP-Instanz (Modul und Port, in der Schreibweise <Slot>.<Port>), die zum Supervisor bestimmt wurde
Supervisor-VRID	VRID des Supervisors
Supervisor Status	Status des Supervisors – `Initialisieren`: VRRP ist in der Initialisierungsphase. Bisher ist kein Master benannt – `Backup`: Der Router beobachtet die Möglichkeit, Master zu werden – `Master`: Der Router ist Master – `unknown`: Kein Supervisor
Aktuelle Priorität	Aktuelle VRRP-Priorität
Redundanz-Überprüfung für Teilnehmer	Aktiviert die Funktion für die ausgewählte Domäne.

Tab. 186: HiVRRP-Domänen anzeigen

HiVRRP-Domänen-Instanzen auf verschiedenen Ports

Sind Domänen-Instanzen (Member) auf verschiedene physikalische Ports verteilt, überwacht der Router per Voreinstellung ausschließlich die Verbindung des Supervisors auf Leitungsunterbrechung („Redundancy-Check per Member“ ausgeschaltet).
Sie haben die Möglichkeit, die Überwachung der weiteren Verbindungen innerhalb der Domäne auf Leitungsunterbrechung einzuschalten. Überwachen bedeutet, dass der Router zur Erkennung einer Leitungsunterbrechung HiVRRP-Nachrichten sendet. Wählen Sie bei geringer Wahr-

scheinlichkeit für eine Leitungsunterbrechung ein langes HiVRRP Nachrichten-Intervall (siehe auf Seite 319 „VRRP-Instanz-Einstellungen“), um die Netzlast gering zu halten.

☐ Schalten Sie in der Spalte „Redundancy-Check per Member“ für die gewünschte Domäne die Funktion bei Bedarf ein.

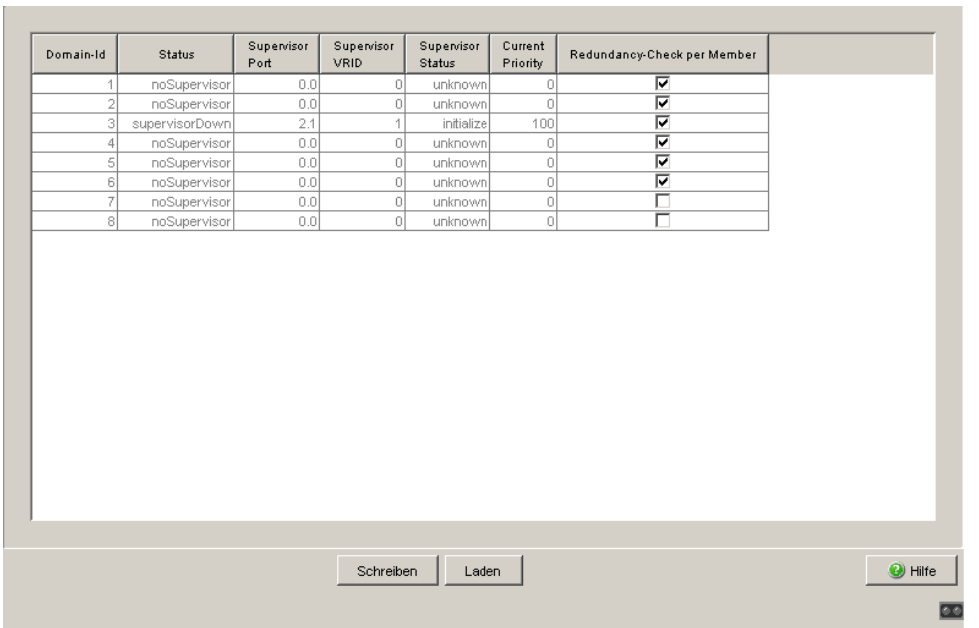


Abb. 77: Dialog HiVRRP-Domänen

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 187: Schaltflächen

7.6.3 Statistik

Das VRRP-Statistik-Fenster zeigt Zählerstände von Zählern an, die VRRP-relevante Ereignisse zählen.

Parameter	Bedeutung
Prüfsummenfehler	Anzahl empfangener VRRP-Nachrichten mit falscher Prüfsumme.
Versionsfehler	Anzahl empfangener VRRP-Nachrichten mit unbekannter oder nicht unterstützter Versionsnummer.
VRID-Fehler	Anzahl empfangener VRRP-Nachrichten mit einer ungültigen VRID für diesen virtuellen Router.

Tab. 188: VRRP-Statistik über alle Ports

Parameter	Bedeutung
Port	Port des Moduls des Gerätes.
VRID	Virtuelle Router-ID
Master geworden	Anzahl, wie oft der Switch schon Master wurde.
Nachrichten empfangen	Anzahl der empfangenen VRRP-Nachrichten.
Intervall-Fehler	Anzahl der vom Router außerhalb des Nachrichtenintervalls empfangenen VRRP-Nachrichten.
Authentifizierungsfehler	Anzahl empfangener VRRP-Nachrichten mit Authentifizierungsfehler.
IP TTL-Fehler	Anzahl der empfangenen VRRP-Nachrichten mit einer IP-TTL ungleich 255.
Null-Prioritätspakete empfangen	Anzahl der VRRP-Nachrichten, über einen VRRP-Teilnehmer mit der Priorität 0.
Null Prioritätspakete gesendet	Anzahl der VRRP-Nachrichten, die der Switch mit der Priorität 0 verschickt hat.
Empfangene ungültige Pakete	Anzahl der empfangenen VRRP-Nachrichten mit ungültigem Typ.
Adressfehler	Anzahl der empfangenen VRRP-Nachrichten, für die die Adressliste nicht mit der lokal für den virtuellen Router konfigurierten Adressliste übereinstimmt.
Ungültiger Authentifizierungstyp	Anzahl empfangener VRRP-Nachrichten mit ungültigem Authentifizierungstyp.
Unpassender Authentifizierungstyp	Anzahl empfangener VRRP-Nachrichten mit falschem Authentifizierungstyp.
Paketlängenfehler	Anzahl der empfangenen VRRP-Nachrichten mit falscher Paketlänge.

Tab. 189: VRRP-Port-Statistiktabelle

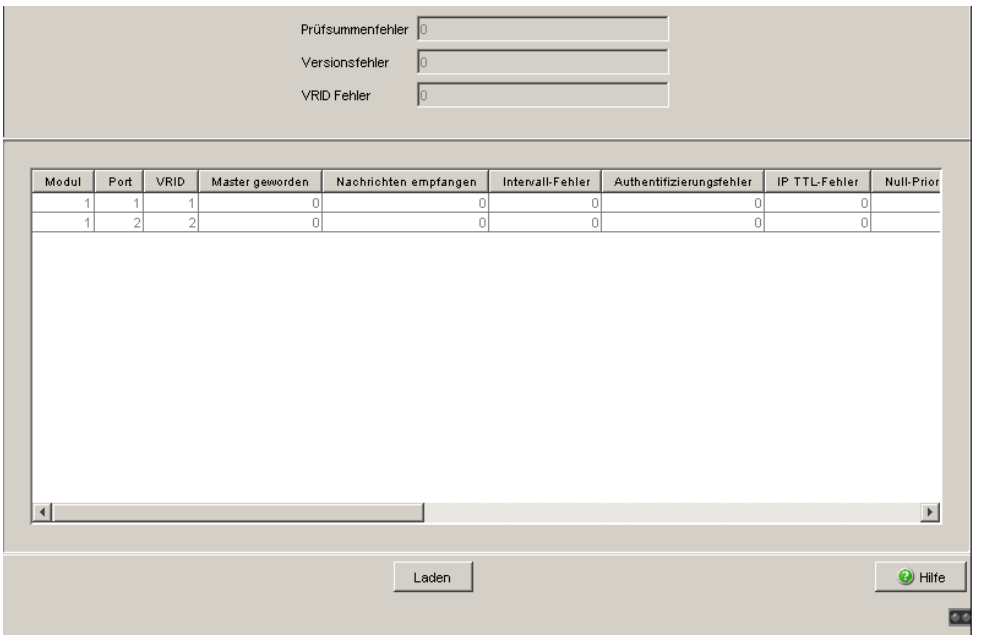


Abb. 78: Dialog VRRP-Statistiken

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 190: Schaltflächen

7.6.4 Tracking

Das VRRP-Tracking-Fenster zeigt den Zustand aller zu VRRP-Objekten zugeordneten Tracking-Objekte an.

Parameter	Bedeutung
Port	Port, für den dieser Eintrag gilt, in der Schreibweise <Slot>.<Port>
VRID	Virtuelle Router-Identifikation des zugeordneten virtuellen Routers.
Track-ID	Identifikationsnummer des Tracking-Objekts, bei dem Sie diesen Eintrag registrieren (siehe auf Seite 252 „Applikationen“).
Dekrement	Wert, um den der lokale Router die aktuelle VRRP-Priorität des zugeordneten VRRP-Routers erniedrigt, wenn das Tracking-Objekt den Zustand „down“ annimmt.
Status	Momentaner Zustand des Tracking-Objekts: „up“ oder „down“.
Aktiv	Anzeige des Eintrags als „aktiv“, wenn das Tracking-Objekt vollständig eingerichtet und aktiviert ist. Mehr Informationen zu aktiven Einträgen: (siehe Abbildung 79). Ist der Eintrag nicht aktiv, ist sein Zustand immer „up“.

Tab. 191: VRRP-Tracking-Tabelle

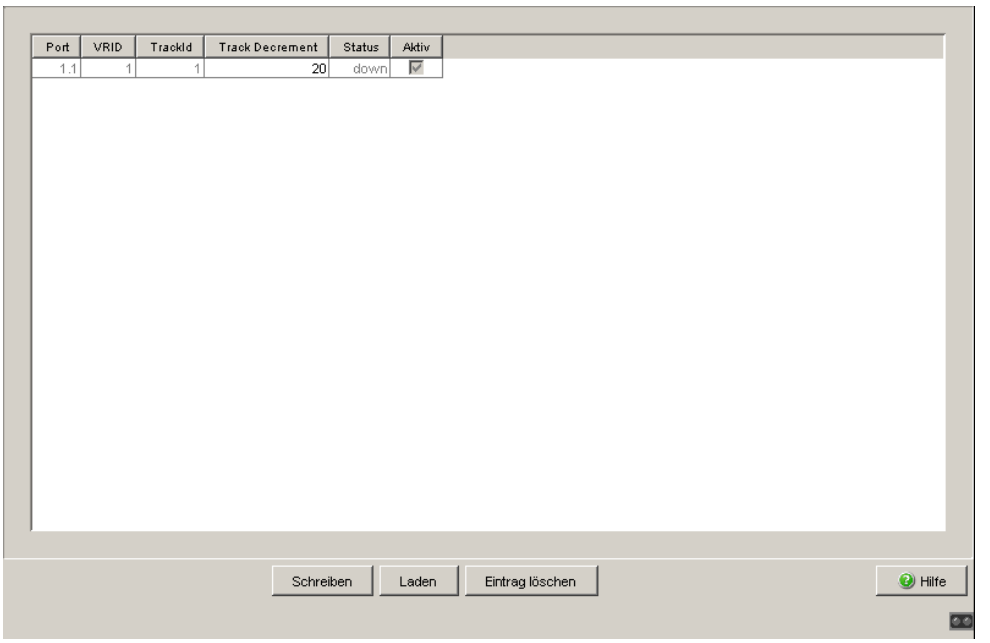


Abb. 79: Dialog Tracking

Tracking-Objekt löschen

☐ Wählen Sie im Dialog `Redundanz:VRRP:Tracking` eine Zeile aus und klicken Sie auf „Eintrag löschen“. Damit löschen Sie die Zeile.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 192: Schaltflächen

8 Diagnose

Das Diagnose-Menü enthält folgende Tabellen und Dialoge:

- Syslog
- Trap-Log
- Ports (Statistiken, Netzlast, SFP-Module, TP-Kabeldiagnose, Port-Monitor)
- Auto-Disable
- Konfigurations-Check
- Topologie-Erkennung
- Port-Mirroring
- Gerätestatus
- Meldekontakt
- Alarme (Traps)
- Bericht (Log-Datei, Systeminformation)
- IP-Adressen Konflikterkennung
- Selbsttest

Diese geben im Service-Fall dem Techniker die notwendigen Informationen zur Diagnose.

8.1 Syslog

Der Dialog „Syslog“ bietet Ihnen die Möglichkeit, die Ereignisse, die das Gerät in seinen Trap-Log oder Event-Log schreibt, zusätzlich an einen oder mehrere Syslog-Server zu senden. Sie können die Funktion ein-/ausschalten und eine Liste von bis zu 8 Syslog-Server-Einträgen verwalten. Dabei haben Sie die Möglichkeit, vorzugeben, dass das Gerät abhängig vom Mindest-Schweregrad des Ereignisses verschiedene Syslog-Server informiert.

Zusätzlich können Sie die SNMP-Anfragen an das Gerät als Ereignisse an einen oder mehrere Syslog-Server senden. Dabei haben Sie die Möglichkeit, GET- und SET-Anfragen getrennt zu behandeln und den zu loggenden Anfragen einen Schweregrad zuzuweisen.

Anmerkung: Die Ereignisse selbst, die das Gerät geloggt hat, finden Sie im Dialog „Trap-Log“ (siehe auf Seite 336 „Trap-Log“) und in der Log-Datei (siehe auf Seite 389 „Event-Log“). Das Gerät wertet SNMP-Anfragen als Ereignis, wenn Sie "Log SNMP-Set/Get Request" aktivieren (siehe Tabelle 194).

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Rahmen „Funktion“	Schaltet die Syslog-Funktion für dieses Gerät „An“ oder „Aus“.	`An` `Aus`	`Aus`
Rahmen „SNMP-Logging“	Einstellungen, um SNMP-Anfragen an das Gerät als Ereignisse an die Liste der Syslog-Server zu senden.		
Log SNMP-Get-Requests.	Erzeugt bei SNMP-Get-Anfragen Ereignisse für den Syslog mit dem vorgegebenen Schweregrad.	`Aktiv` `inaktiv`	`inaktiv`

Tab. 193: Syslog- und SNMP-Logging-Einstellungen

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand

Schweregrad (für Logs von SNMP-Get-Requests)	Gibt den Schweregrad vor, mit dem das Gerät das Ereignis „SNMP-Get-Request erhalten“ für die Liste der Syslog-Server erzeugt.	`debug`
		`informational`
		`notice`
		`warning`
		`error`
		`critical`
		`alert`
		`emergency`
			`notice`

Log SNMP-Set-Requests.	Erzeugt bei SNMP-Set-Anfragen Ereignisse für den Syslog mit dem vorgegebenen Schweregrad.	`Aktiv` `inaktiv`	`inaktiv`

Schweregrad (für Logs von SNMP-Set-Requests)	Gibt den Schweregrad vor, mit dem das Gerät das Ereignis „SNMP-Set-Request erhalten“ für die Liste der Syslog-Server erzeugt.	`debug`
		`informational`
		`notice`
		`warning`
		`error`
		`critical`
		`alert`
		`emergency`
			`notice`

Tab. 193: Syslog- und SNMP-Logging-Einstellungen

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Syslog-Server-Einträge			
Index	Laufende Nummer des Syslog-Server-Eintrags in der Tabelle. Wenn Sie einen Eintrag löschen, bleibt eine Nummerierungslücke. Wenn Sie einen Eintrag erzeugen, schließt das Gerät die 1. Lücke.	1 - 8	-
IP-Adresse	Adresse eines Syslog-Servers, an den das Gerät seine Log-Einträge sendet.	Gültige IPv4-Adresse	0.0.0.0
Port	UDP-Port, auf dem Ihr Syslog-Server Einträge annimmt.	1 - 65.535	514

Tab. 194: Syslog-Server-Einträge

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand

Mindest-Schwere-grad	Mindest-Schweregrad für ein Ereignis, damit das Gerät dafür einen Log-Eintrag an diesen Syslog-Server schickt.	`debug`
		`informational`
		`notice`
		`warning`
		`error`
		`critical`
		`alert`
		`emercency`
			critical

Aktiv	Aktivieren oder Deaktivieren des aktu-ellen Syslog-Server-Eintrags in dieser Zeile.	`aktiv`
		(Kästchen markiert)
		`inaktiv`
		(Kästchen leer)
			inaktiv

Tab. 194: Syslog-Server-Einträge

Anmerkung: Wenn Sie das Logging von SNMP-Anfragen aktivieren, sendet das Gerät diese als Ereignisse mit dem voreingestellten Schweregrad `notice` an die Liste der Syslog-Server. Der voreingestellte Mindest-Schweregrad für einen Syslog-Server-Eintrag ist `critical`.

Um SNMP-Anfragen an einen Syslog-Server zu senden, haben Sie mehrere Möglichkeiten, die Voreinstellungen zu ändern. Wählen Sie diejenige, die am besten zu Ihren Anforderungen passt.

- Setzen Sie den Schweregrad, mit dem das Gerät SNMP-Anfragen als Ereignisse erzeugt, auf `warning` oder `error` und ändern Sie den Mindest-Schweregrad für einen Syslog-Eintrag bei einem oder mehreren Syslog-Servern auf den gleichen Wert.
  Sie haben auch die Möglichkeit, dafür einen eigenen Syslog-Server-Eintrag zu erzeugen.
- Setzen Sie ausschließlich den Schweregrad der SNMP-Anfragen auf `critical` oder höher. Das Gerät sendet dann SNMP-Anfragen als Ereignisse mit dem Schweregrad `critical` oder schwerer an die Syslog-Server.
- Setzen Sie ausschließlich den Mindest-Schweregrad bei einem oder mehreren Syslog-Server-Einträgen auf `notice` oder niedriger. Das Gerät sendet dann u. U. sehr viele Ereignisse an die Syslog-Server.

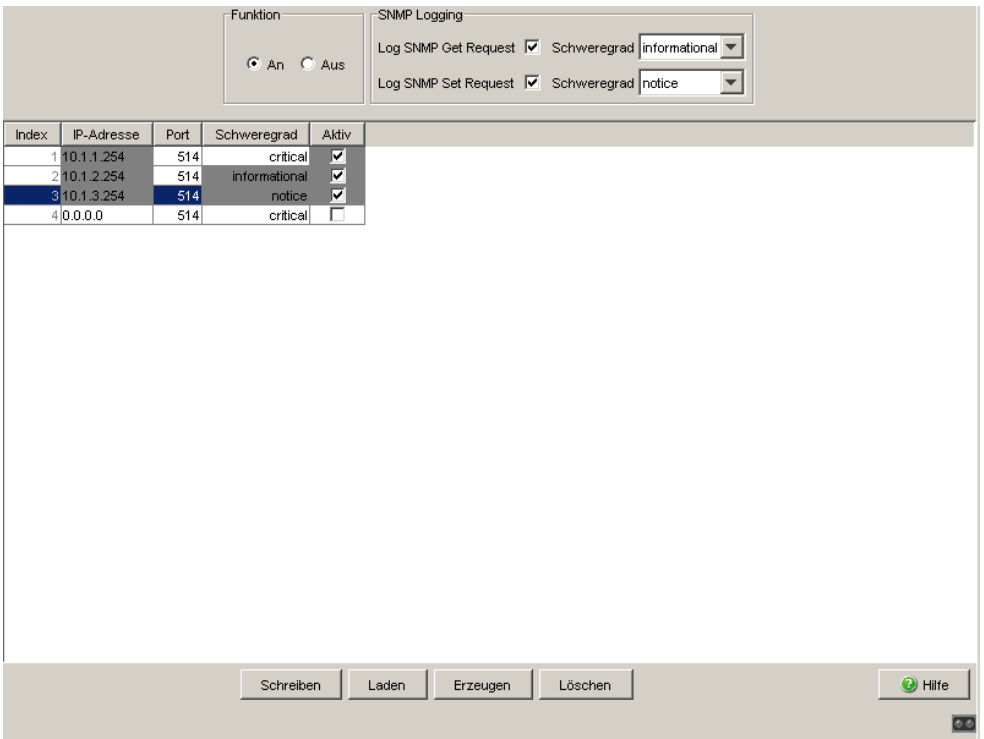


Abb. 80: Dialog Syslog

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 195: Schaltflächen

8.2 Trap-Log

Die Tabelle listet die geloggten Ereignisse mit Zeitstempel auf. Mit der Bedientaste „Laden“ aktualisieren Sie den Inhalt des Trap-Logs. Mit der Bedientaste „Löschen“ löschen Sie den Inhalt des Trap-Logs.

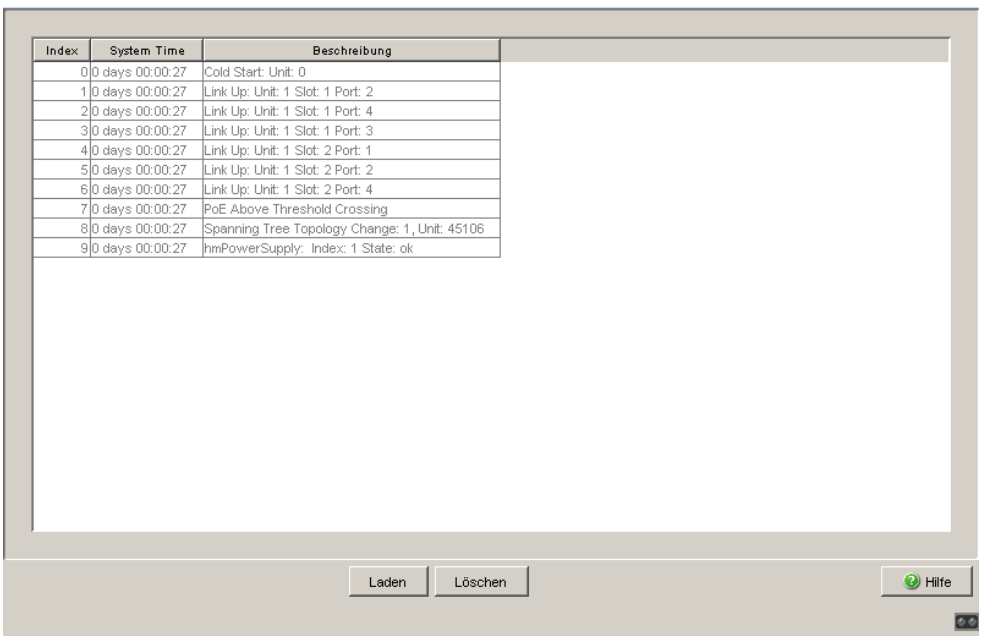


Abb. 81: Trap-Log Tabelle

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Index	Zeigt eine fortlaufende Nummer, auf die sich der Tabelleneintrag bezieht. Das Gerät legt diese Nummer automatisch fest.	0, 1, 2, ...	
System Time	Zeigt die Zeit an, die seit dem geloggten Ereignis vergangen ist.	d days hh:mm:ss	
Beschreibung	Zeigt eine Kurzbeschreibung des geloggten Ereignisses an.	-	

Tab. 196: Trap-Log Tabelle

Sie haben die Möglichkeit, die geloggten Ereignisse zusätzlich an einen oder mehrere Syslog-Server zu senden (siehe auf Seite 332 „Syslog“).

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Löschen	Löscht die Tabelleneinträge.
Hilfe	Öffnet die Online-Hilfe.

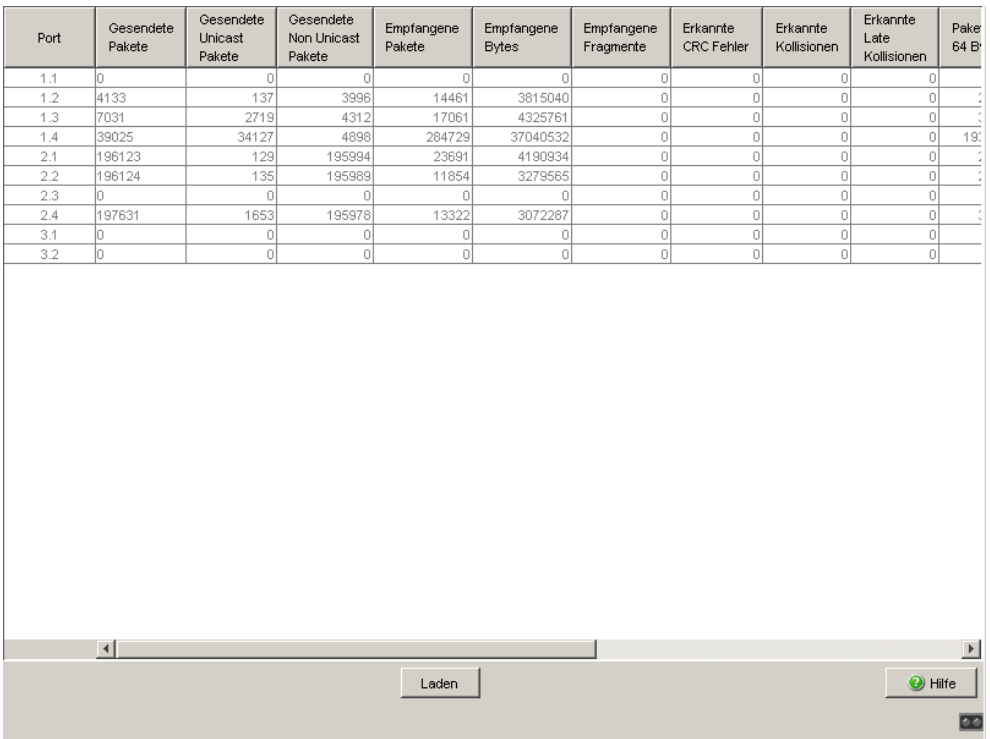
Tab. 197: Schaltflächen

8.3 Ports

Das Port-Menü enthält Anzeigen und Tabellen zu den einzelnen Ports:
- Statistiktabelle
- Netzlast
- SFP-Module
- TP-Kabeldiagnose
- Port-Monitor

8.3.1 Portstatistiken

Diese Tabelle zeigt Ihnen die Inhalte verschiedener Ereigniszähler an. Im Menüpunkt Neustart können Sie mit „Warmstart“, „Kaltstart“ oder „Portzähler zurücksetzen“ die Ereigniszähler auf 0 zurücksetzen.
Die Paketzähler summieren die Ereignisse aus Sende- und Empfangsrichtung.



Port	Gesendete Pakete	Gesendete Unicast Pakete	Gesendete Non Unicast Pakete	Empfangene Pakete	Empfangene Bytes	Empfangene Fragmente	Erkannte CRC Fehler	Erkannte Kollisionen	Erkannte Late Kollisionen	Pake 64 B
1.1	0	0	0	0	0	0	0	0	0	
1.2	4133	137	3996	14461	3815040	0	0	0	0	
1.3	7031	2719	4312	17061	4325761	0	0	0	0	
1.4	39025	34127	4898	284729	37040532	0	0	0	0	19
2.1	196123	129	195994	23691	4190934	0	0	0	0	
2.2	196124	135	195989	11854	3279565	0	0	0	0	
2.3	0	0	0	0	0	0	0	0	0	
2.4	197631	1653	195978	13322	3072287	0	0	0	0	
3.1	0	0	0	0	0	0	0	0	0	
3.2	0	0	0	0	0	0	0	0	0	

Abb. 82: Portstatistiken, Tabelle

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Portzähler zurücksetzen	Setzt die Zähler der Portstatistik auf `0`.
Hilfe	Öffnet die Online-Hilfe.

Tab. 198: Schaltflächen

8.3.2 Auslastung (Netzlast)

Diese Tabelle zeigt Ihnen die Auslastung (Netzlast) der einzelnen Ports an. Die Auslastung ist die Datenmenge, die der Port in den zurückliegenden 30 s empfangen hat, im Vergleich zu der maximal möglichen Datenmenge bei seiner aktuell konfigurierten Datenrate.

Der obere und der untere Grenzwert kontrollieren die Netzlast-Alarme für einen Port. Übersteigt die Netzlast den oberen Grenzwert, sendet das Gerät einen Alarm. Sobald die Netzlast den unteren Grenzwert unterschreitet, endet der Alarm. Ist der Bereich zwischen dem oberen und dem unteren Grenzwert großzügig gewählt, verringert sich die Anzahl der mehrfach gesendeten Alarme.

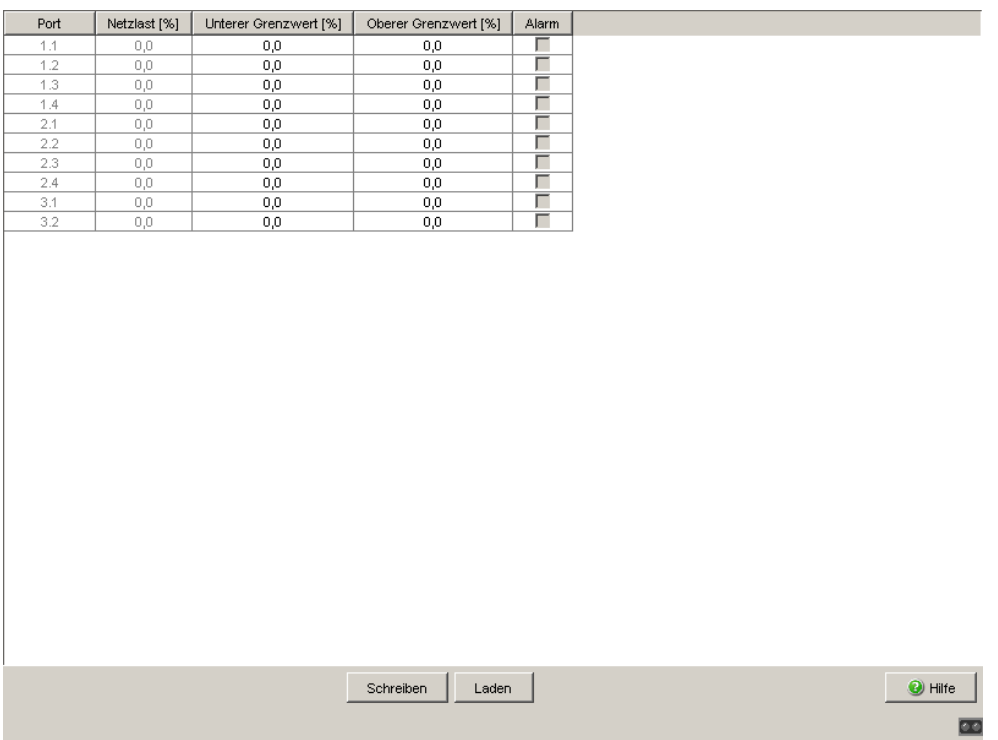


Abb. 83: Dialog Auslastung (Netzlast)

Parameter	Bedeutung	Mögliche Werte	Liefer-zustand
Port	Zeigt die Nummer des Geräte-Ports, auf den sich der Tabelleneintrag bezieht.	1.1, 1.2, 1.3 etc.	
Netzlast [%]	Zeigt die aktuelle Netzlast in Prozent, die der Geräte-Port in den zurückliegenden 30 s empfangen hat. Die Netzlast ist das Verhältnis der empfangen Datenmenge zur maximal möglichen Datenmenge bei der aktuell konfigurierten Datenrate.	0,00..100,00	0,00
Unterer Grenzwert [%]	Definiert den unteren Grenzwert für die Netzlast. Unterschreitet die Netzlast über den Geräte-Port diesen Wert, endet der Alarm. Der Wert 0 deaktiviert den unteren Grenzwert.	0.00..100.00	0.00
Oberer Grenzwert [%]	Legt einen oberen Grenzwert für die Netzlast fest. Überschreitet die Netzlast des Geräte-Ports diesen Wert, zeigt das Feld Alarm einen Alarm. Der Wert 0 deaktiviert den oberen Grenzwert.	0,00..100,00	0,00
Alarm	Kennzeichnet den Alarmzustand für die Netzlast. – markiert Die Netzlast des Geräte-Ports liegt unter dem im Feld Unterer Grenzwert [%] oder über dem im Feld Oberer Grenzwert [%] festgelegten Wert. Das Gerät sendet eine SNMP-Nachricht (Trap). – unmarkiert Die Netzlast des Geräte-Ports liegt über dem im Feld Unterer Grenzwert [%] und unter dem im Feld Oberer Grenzwert [%] festgelegten Wert.	markiert unmarkiert	unmar-kiert

Tab. 199: Auslastung (Netzlast) Tabelle

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 200: Schaltflächen

8.3.3 SFP-Transceiver

Die SFP-Zustandsanzeige bietet Ihnen die Möglichkeit, die aktuelle Bestückung der SFP-Module und deren Eigenschaften einzusehen. Zu den Eigenschaften zählen:

Parameter	Bedeutung
Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.
Modultyp	Typ des SFP-Moduls, z.B. M-SFP-SX/LC.
Unterstützt	Zeigt an, ob das Medienmodul das SFP-Modul unterstützt.
Temperatur in °C	Anzeige der Betriebstemperatur des SFPs.
Sendeleistung in mW	Anzeige der Sendeleistung in mW.
Empfangsleistung in mW	Anzeige der Empfangsleistung in mW.
Sendeleistung in dBm	Anzeige der Sendeleistung in dBm.
Empfangsleistung in dBm	Anzeige der Empfangsleistung in dBm.

Tab. 201: Dialog SFP-Module

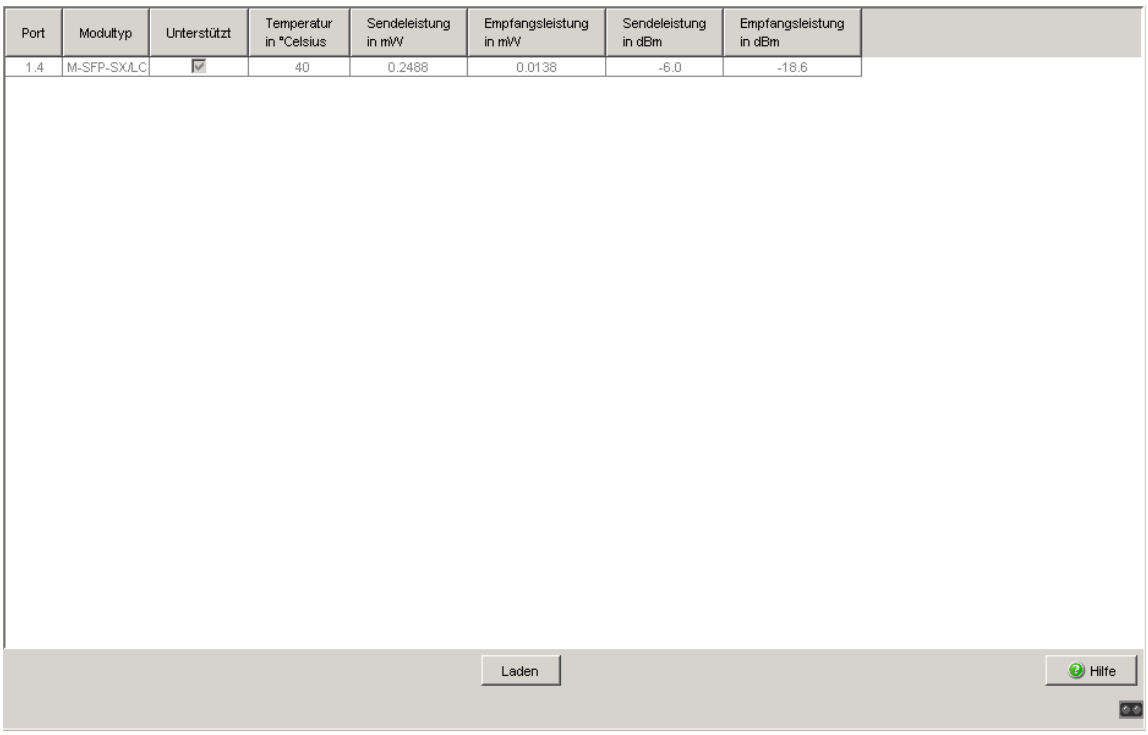


Abb. 84: Dialog SFP-Module

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 202: Schaltflächen

8.3.4 TP-Kabeldiagnose

Die TP-Kabeldiagnose ermöglicht Ihnen, das angeschlossene Kabel auf Kurzschluss oder Unterbrechung zu prüfen.

Anmerkung: Während der Überprüfung ruht der Datenverkehr an diesem Port.

☐ Wählen Sie den TP-Port aus, an dem Sie die Prüfung durchführen wollen.

☐ Klicken Sie auf „Schreiben“, um die Prüfung zu starten.

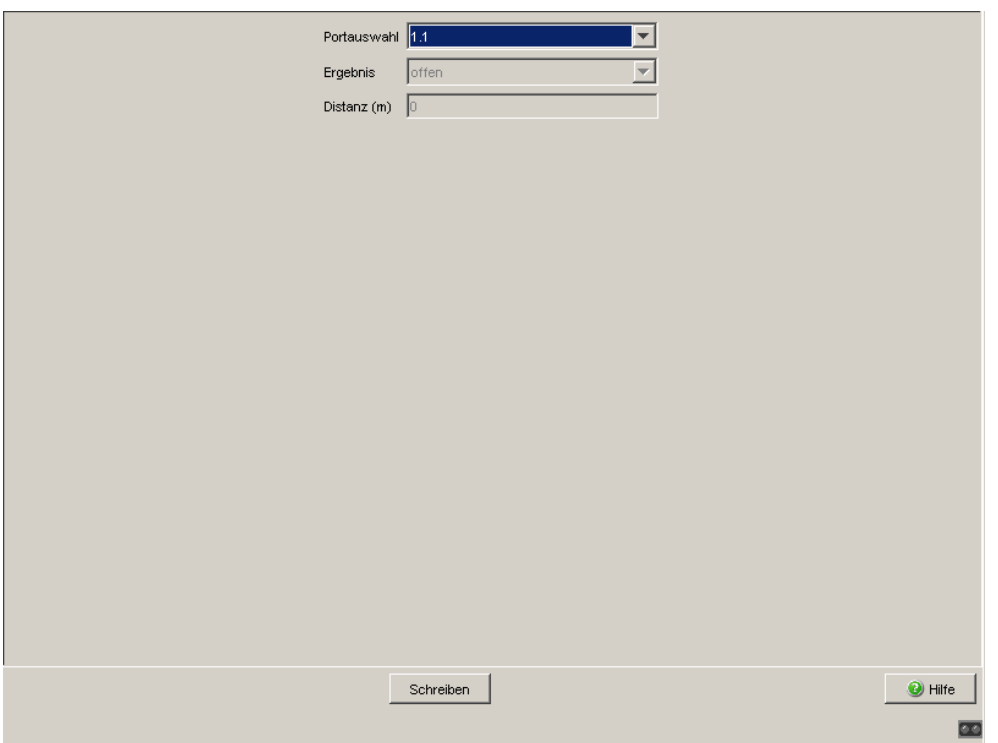


Abb. 85: Dialog TP-Kabeldiagnose

Die Prüfung dauert wenige Sekunden. Nach der Prüfung finden Sie in der Zeile „Ergebnis“ das Prüfergebnis der Kabeldiagnose. Ergibt das Prüfergebnis einen Kabelfehler, dann finden Sie in der Zeile „Distanz“ die Entfernung vom Port zum Kabelfehler.

Ergebnis	Bedeutung
normal	Das Kabel ist in Ordnung.
offen	Das Kabel ist unterbrochen.
Kurzschluss	Das Kabel weist einen Kurzschluss auf.
Unbekannt	Sie haben noch keine Kabelprüfung durchgeführt oder diese läuft gerade.

Tab. 203: Bedeutung der möglichen Ergebnisse

Voraussetzungen für eine korrekte TP-Kabeldiagnose:
- 1000BASE-T-Port, über 8-adriges Kabel mit 1000BASE-T-Port verbunden oder
- 10BASE-T/100BASE-TX-Port, mit 10BASE-T/100BASE-TX-Port verbunden.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Hilfe	Öffnet die Online-Hilfe.

Tab. 204: Schaltflächen

8.3.5 Port Monitor

Der Port-Monitor überwacht die Ports des Gerätes. Beim Eintritt eines Ereignisses führt das Gerät eine Aktion für den Port aus, z. B. bei zu vielen Verbindungsabbrüchen auf Grund eines Wackelkontaktes.

Global

In der Registerkarte „Global“ legen Sie für die zu überwachenden Ports die auslösenden Ereignisse sowie eine Aktion fest:

- ☐ Schalten Sie die Funktion im Rahmen „Funktion“ global ein.
- ☐ Markieren Sie für jeden zu überwachenden Port das Kontrollkästchen in der Spalte „Port Monitor an“.
- ☐ Legen Sie für jeden zu überwachenden Port das auslösende Ereignis fest. Markieren Sie dazu die Kontrollkästchen in den Spalten „Linkänderungen an“ bis „Link Speed und Duplex Modus an“.
- ☐ Legen Sie die Parameter für das auslösende Ereignis in der zugehörigen Registerkarte fest.
- ☐ Wählen Sie für jeden zu überwachenden Port in der Spalte „Aktion“ die Aktion aus, die das Gerät ausführen soll.
- ☐ Speichern Sie die Einstellungen.

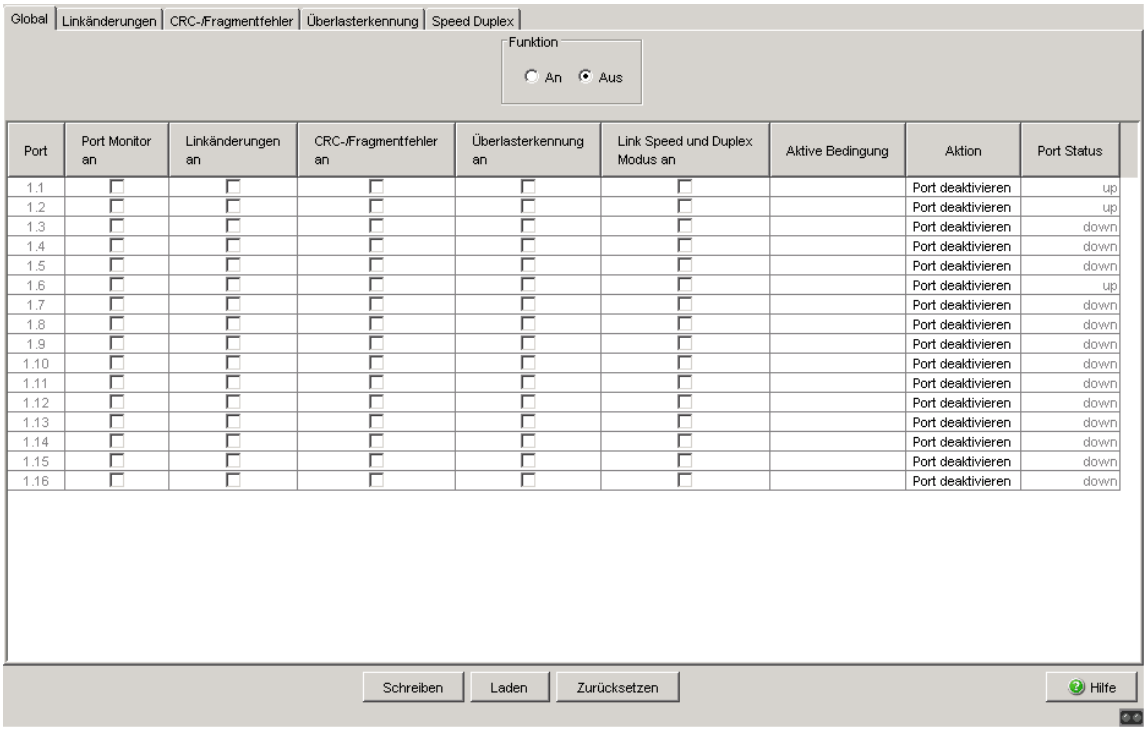


Abb. 86: Dialog Port-Monitor Global

Parameter	Bedeutung
Rahmen „Funktion“	Schaltet die Funktion „Port-Monitor“ für das Gerät an oder aus.
Port-Tabelle	
Port	Liste der verfügbaren Ports des Gerätes.
Port-Monitor an	Hier wählen Sie die zu überwachenden Ports aus.
Linkänderungen an	Hier wählen Sie aus, ob Linkänderungen eine Aktion auslösen. Als Linkänderungen gelten Wechsel vom Zustand „Link down“ nach „Link up“.
CRC-/Fragmentfehler an	Hier wählen Sie aus, ob auftretende CRC- bzw Fragmentfehler eine Aktion auslösen.
Überlasterkennung an	Hier wählen Sie aus, ob die Überlasterkennung eine Aktion auslöst.
Link Speed und Duplex Modus an	Hier wählen Sie aus, ob eine falsche Kombination von Duplex-Modus und Übertragungsgeschwindigkeit eine Aktion auslöst.
Aktive Bedingung	Zeigt die Bedingung aufgrund der das Gerät eine Aktion an diesem Port ausgeführt hat.

Tab. 205: Tabelle Port-Monitor Global

Parameter	Bedeutung
Aktion	Hier wählen Sie die Aktion, die das Gerät ausführt, wenn das auslösende Ereignis eintritt. Folgende Aktionen sind möglich: ▶ `Port deaktivieren` Deaktiviert den Port. Danach blinkt die Port-LED auf dem Gerät 3 mal grün je Periode. Das Gerät re-aktiviert den Port, wenn Sie im Dialog `Diagnose:Ports:Auto-Disable` folgende Einstellungen festgelegt haben: – Im Rahmen „Konfiguration“ ist das Kontrollkästchen für das auslösende Ereignis markiert, das den Port deaktiviert hat. – Der Reset-Timer ist für den Port >0 festgelegt. ▶ `Trap senden` Sendet einen SNMP-Trap. Der Port bleibt aktiviert. ▶ `Auto Disable` Deaktiviert den Port abhängig von den Einstellungen im Dialog `Diagnose:Ports:Auto-Disable`, Rahmen „Konfiguration“. – Das Gerät deaktiviert den Port, wenn das Kontrollkästchen für das auslösende Ereignis markiert ist. Danach blinkt die Port-LED auf dem Gerät 3 mal grün je Periode. Das Gerät re-aktiviert den Port, wenn im Dialog `Diagnose:Ports:Auto-Disable` für den Port der Reset-Timer für den Port >0 festgelegt ist. Wenn das Gerät den Port auf Grund von Überlast deaktiviert hat, gelten für das Re-Aktivieren des Ports weitere Voraussetzungen (siehe auf Seite 352 „Überlasterkennung“). – Der Port bleibt aktiviert, wenn das Kontrollkästchen für das auslösende Ereignis unmarkiert ist.
Port-Status	Zeigt den aktuellen Port-Status an. – `up`: Datenübertragung über den Port ist möglich. – `down`: Datenübertragung über den Ports ist unterbrochen. – `notPresent`: Kein physischer Port vorhanden.

Tab. 205: Tabelle Port-Monitor Global

Linkänderungen

In der Registerkarte „Linkänderungen“ legen Sie die Parameter fest, anhand der das Gerät bei zu vielen Linkänderungen eine Aktion für den betreffenden Port auslöst:

☐ Öffnen Sie die Registerkarte „Linkänderungen“.

☐ Legen Sie im Rahmen „Parameter“ die Anzahl der Linkänderungen und das zugehörige Intervall fest.
Diese Parameter gelten für sämtliche Ports, bei denen in der Registerkarte „Global“, Spalte „Linkänderung an“ das Kontrollkästchen markiert ist.

☐ Speichern Sie die Einstellungen.

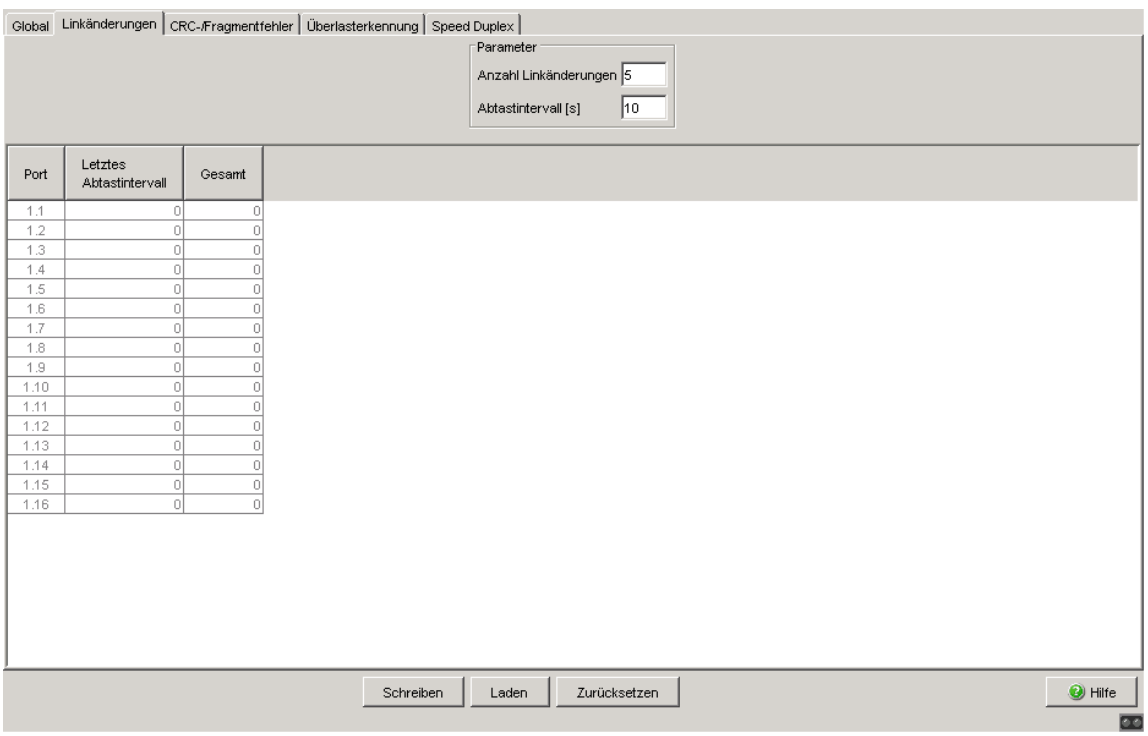


Abb. 87: Dialog Port-Monitor Linkänderungen

Anmerkung: Beachten Sie für Ports, bei denen Sie die Anzahl der Link-Änderungen auf den Wert 1 gesetzt haben, die folgende Besonderheit: Haben Sie die Aktion „Port deaktivieren“ gewählt, schaltet das Gerät den Port bereits nach der 1. Link-Änderung ab. Dazu zählt auch die „Link Up“-Änderung in den folgenden Fällen:

- beim Neustart des Gerätes, wenn an dem Port bereits ein Kommunikationspartner angeschlossen ist,
- beim 1. Anschließen eines Kommunikationspartners und
- beim Laden einer Konfiguration (siehe auf Seite 53 „Konfiguration laden“).

Hat das Gerät alle Ports deaktiviert, ist ein Zugriff auf den Switch ausschließlich über den V.24-Zugang möglich.

Parameter	Bedeutung
Anzahl Linkänderungen	Anzahl der Linkänderungen im abgeschlossenen Abtastintervall, der zu einer Aktion des Gerätes führt.
Abtastintervall [s]	Länge eines Abtastintervalls, in dem das Gerät die Anzahl der Linkänderungen bestimmt.
Port-Tabelle	
Port	Liste der verfügbaren Ports des Gerätes.
Letztes Abtastintervall	Anzahl der Linkänderungen im letzten Abtastintervall. Die Linkänderungen werden auch nach dem Deaktivieren des Ports weitergezählt.
Gesamt	Summe aller bisher aufgetretener Linkänderungen. Die Linkänderungen werden auch nach dem Deaktivieren des Ports weitergezählt.

Tab. 206: Port-Monitor Linkänderungen Tabelle

CRC-/Fragmentfehler

In der Registerkarte „CRC-/Fragmentfehler“ legen Sie die Parameter fest, anhand der das Gerät bei zu vielen empfangenen fehlerhaften Ethernet-Paketen eine Aktion für den betreffenden Port auslöst:

☐ Öffnen Sie die Registerkarte „CRC-/Fragmentfehler“.

☐ Legen Sie im Rahmen „Parameter“ die Rate der fehlerhaften Pakete (in Parts per million) und das zugehörige Intervall fest.
Diese Parameter gelten für sämtliche Ports, bei denen in der Registerkarte „Global“, Spalte „CRC-/Fragmentfehler an“ das Kontrollkästchen markiert ist.

☐ Speichern Sie die Einstellungen.

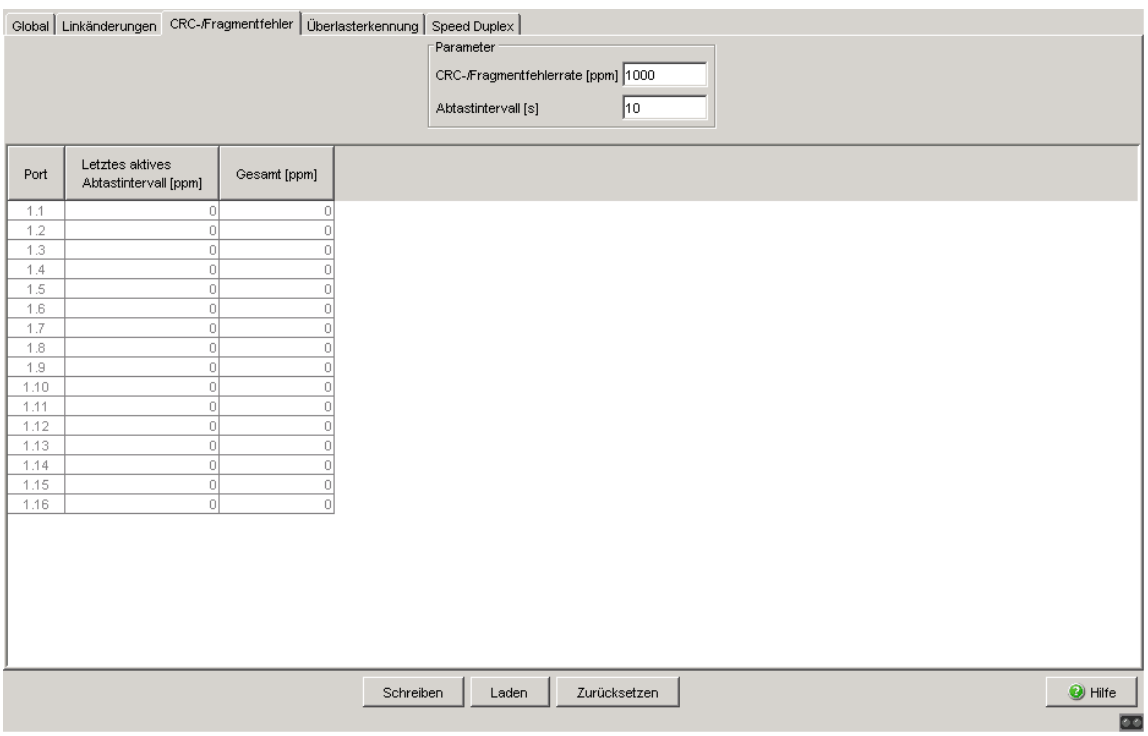


Abb. 88: Dialog Port-Monitor CRC-/Fragmentfehler

Parameter	Bedeutung
CRC-/Fragment-fehlerrate [ppm]	Fragmentfehleranteil im abgeschlossenen Abtastintervall, der zu einer Aktion des Gerätes führt.
Abtastintervall [s]	Länge eines Abtastintervalls, in dem das Gerät den CRC-/Fragment-fehleranteil bestimmt.
Port-Tabelle	
Port	Liste der verfügbaren Ports des Gerätes.

Tab. 207: Port-Monitor CRC-/Fragmentfehler Tabelle

Parameter	Bedeutung
Letztes aktives Abtastintervall [ppm]	Erkannter Fehleranteil im letzten aktiven Abtastintervall, der die Aktion auslöste.
Gesamt [ppm]	Bisher aufgetretener Gesamtfehleranteil in ppm (parts per million).

Tab. 207: Port-Monitor CRC-/Fragmentfehler Tabelle

Überlasterkennung

In der Registerkarte „Überlasterkennung“ legen Sie die Parameter fest, anhand der das Gerät bei Überlast eine Aktion für den betreffenden Port auslöst:

☐ Öffnen Sie die Registerkarte „Überlasterkennung“.

☐ Legen Sie im Rahmen „Parameter“ das Intervall fest.
Dieser Parameter gilt für sämtliche Ports, bei denen in der Registerkarte „Global“, Spalte „Überlasterkennung an“ das Kontrollkästchen markiert ist.

☐ Legen Sie in der Spalte „Traffic-Typ“fest, welche Pakete das Gerät bei der Lasterkennung berücksichtigt.

☐ Legen Sie in der Spalte „Oberer Grenzwert“ den gewünschten Wert in `pps` (Pakete pro Sekunde) fest.
Übersteigt die Datenrate auf dem Port diesen Wert, führt das Gerät die in der Registerkarte „Global“ festgelegte Aktion für den Port aus.

☐ Legen Sie in der Spalte „Unterer Grenzwert“ den gewünschten Wert in `pps` (Pakete pro Sekunde) fest, wenn Sie auf dem Port die Aktion `Trap senden` oder `Auto Disable` verwenden.
Die Auto-Disable-Funktion re-aktiviert einen deaktivierten Port, wenn folgende Voraussetzungen erfüllt sind:
- In den Auto-Disable-Einstellungen ist der „Reset-Timer“-Wert für den Port >0 festgelegt.
- Die im „Reset-Timer“ festgelegte Zeit ist abgelaufen.
- Die Last auf dem Port ist niedriger als der in der Spalte „Unterer Grenzwert“ festgelegte Wert.

- ☐ Auf den Geräten MACH104 und MACH1040 haben Sie die Möglichkeit, die in der Spalte „Grenzwert-Typ“ voreingestellte Einheit `pps` (Pakete pro Sekunde) zu ändern:
  - Mit der Einheit `kbps` legen Sie die Last in den Spalten „Oberer Grenzwert“ und „Unterer Grenzwert“ im Bereich `0..10000000` kbit/s fest.
  - Mit der Einheit `link-capacity` legen Sie die Last in den Spalten „Oberer Grenzwert“ und „Unterer Grenzwert“ im Bereich 0..100% der Bandbreite fest.
- ☐ Speichern Sie die Einstellungen.

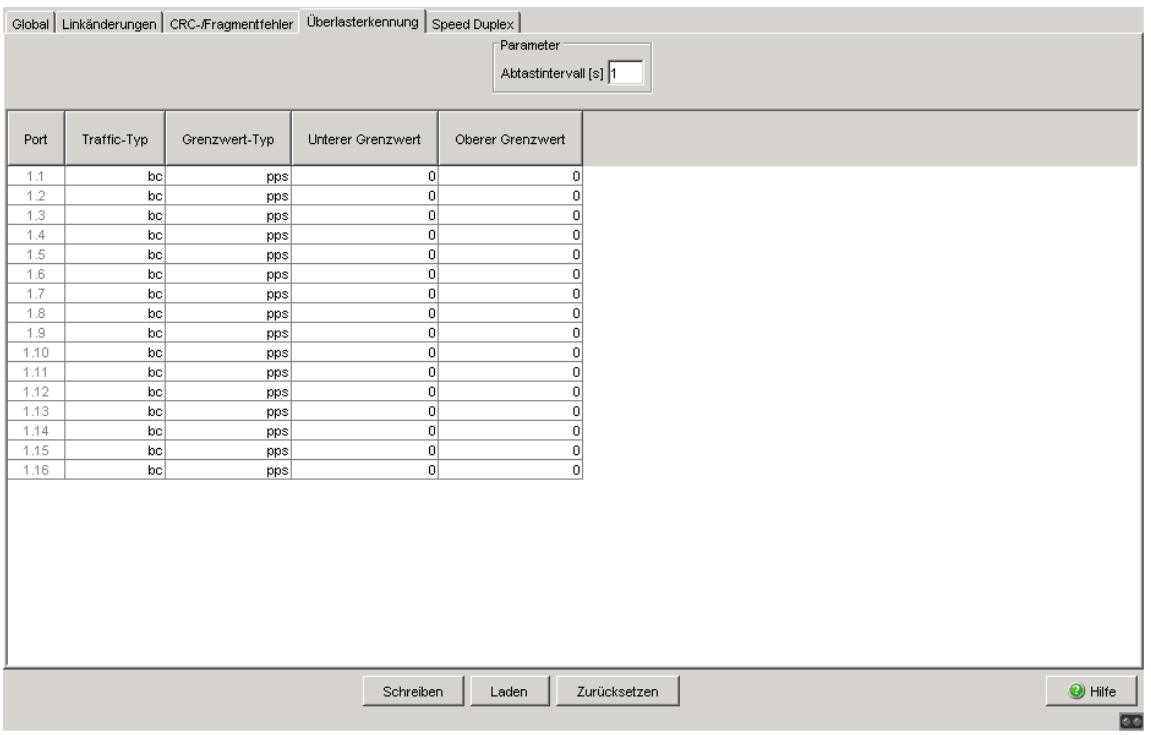


Abb. 89: Dialog Port-Monitor Überlasterkennung

Parameter	Bedeutung
Abtastintervall [s]	Länge eines Abtastintervalls, in dem das Gerät die Anzahl der Unter- und Überschreitungen der zulässigen Grenzwerte ermittelt.
Port-Tabelle	
Port	Liste der verfügbaren Ports des Gerätes.

Tab. 208: Tabelle Port-Monitor CRC-/Fragmentfehler

Parameter	Bedeutung
Traffic-Typ	Legt den Traffic-Typ für die Überlasterkennung fest. Folgende Aktionen sind möglich: – all: Die Überlasterkennung nutzt den Unicast-, Broadcast- Multicast-Datenverkehr, um die Grenzwerte zu erkennen. – bc: Die Überlasterkennung nutzt den Broadcast-Datenverkehr, um die Grenzwerte zu erkennen. – bc-mc: Die Überlasterkennung nutzt den Broadcast- und den Multicast-Datenverkehr, um die Grenzwerte zu erkennen.
Grenzwert-Typ	Legt den Grenzwert-Typ für die Überlasterkennung fest. Folgende Aktionen sind möglich: – pps - Pakete pro Sekunde Verfügbar auf den Geräten MACH1040 und MACH104: – kbps - Kilobits pro Sekunde – link-capacity - Prozentwert der Link-Kapazität
Unterer Grenzwert	Beschreibt den Wert, ab dem das Gerät den Port automatisch aktiviert.
Oberer Grenzwert	Beschreibt den Wert, ab dem das Gerät den Port automatisch deaktiviert.

Tab. 208: Tabelle Port-Monitor CRC-/Fragmentfehler

Speed Duplex

In der Registerkarte „Speed Duplex“ legen Sie die erlaubten Kombinationen von Geschwindigkeit und Duplex-Modus fest. Erkennt das Gerät eine unerlaubte Kombinationen von Geschwindigkeit und Duplex-Modus, löst es eine Aktion für den betreffenden Port aus:

☐ Öffnen Sie die Registerkarte „Speed Duplex“.

☐ Legen Sie für jeden Port individuell fest, welcher Duplex-Modus bei welcher Geschwindigkeit erlaubt ist.

☐ Speichern Sie die Einstellungen.

Anmerkung: Der Port-Monitor überwacht Geschwindigkeit und Duplex-Modus ausschließlich auf eingeschalteten physischen Ports.

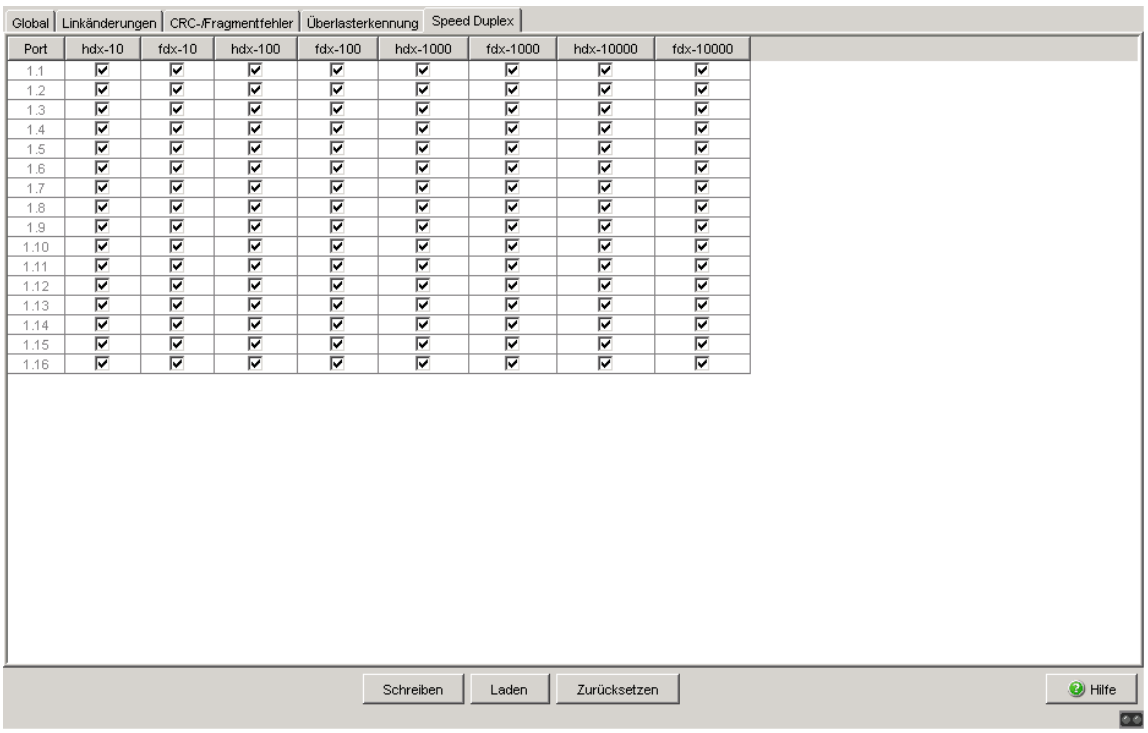


Abb. 90: Dialog Port-Monitor Speed Duplex

Parameter	Bedeutung
Port	Liste der verfügbaren Ports des Gerätes.
hdx-10	Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ `unmarkiert` Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte „Global“ festgelegte Aktion aus.
fdx-10	Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ `unmarkiert` Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte „Global“ festgelegte Aktion aus.

Tab. 209: Tabelle Port-Monitor Speed Duplex

Parameter	Bedeutung
hdx-100	Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ `unmarkiert` Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte „Global“ festgelegte Aktion aus.
fdx-100	Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ `unmarkiert` Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte „Global“ festgelegte Aktion aus.
hdx-1000	Aktiviert/deaktiviert das Akzeptieren der Kombination von 1 Gbit/s und Halbduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ `unmarkiert` Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte „Global“ festgelegte Aktion aus.

Tab. 209: Tabelle Port-Monitor Speed Duplex

Parameter	Bedeutung
fdx-1000	Aktiviert/deaktiviert das Akzeptieren der Kombination von 1 Gbit/s und Vollduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ `unmarkiert` Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte „Global“ festgelegte Aktion aus.
fdx-10000	Verfügbar auf den Geräten MACH4002 24G/48G und MACH104: Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Gbit/s und Vollduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ `unmarkiert` Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte „Global“ festgelegte Aktion aus.

Tab. 209: Tabelle Port-Monitor Speed Duplex

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Zurücksetzen	Setzt die Port-Überwachungsfunktion für das ausgewählte Interface zurück und aktiviert den Port, falls die Überwachungsfunktion den Port deaktiviert hat.
Hilfe	Öffnet die Online-Hilfe.

Tab. 210: Schaltflächen

8.3.6 Auto-Disable

Die Auto-Disable-Funktion bietet Ihnen die Möglichkeit, Ports, die der Port-Monitor deaktiviert hat, nach einer benutzerdefinierten Zeitspanne automatisch zu re-aktivieren. Dabei erlaubt das Gerät, mehrere auslösende Ereignisse zu berücksichtigen.

Die auslösenden Ereignisse, auf Grund der das Gerät die Ports deaktiviert, legen Sie fest in den Einstellungen der Portsicherheit (siehe auf Seite 89 „Portsicherheit“) und des Port-Monitors (siehe auf Seite 346 „Port Monitor“).

Wenn der Port-Monitor für einen Port die Aktion `Auto Disable` ausführt, entscheiden die Einstellungen im Dialog „Auto-Disable“, Rahmen „Konfiguration“ darüber, was mit dem Port passiert:

- Das Gerät deaktiviert den Port, wenn das Kontrollkästchen für die Auslöse-Bedingung markiert ist. Danach blinkt die Port-LED auf dem Gerät 3 mal grün je Periode.
  Das Gerät re-aktiviert den Port, wenn der „Reset-Timer“-Wert für den Port >0 festgelegt ist.
- Der Port bleibt aktiviert, wenn das Kontrollkästchen für das auslösende Ereignis unmarkiert ist.

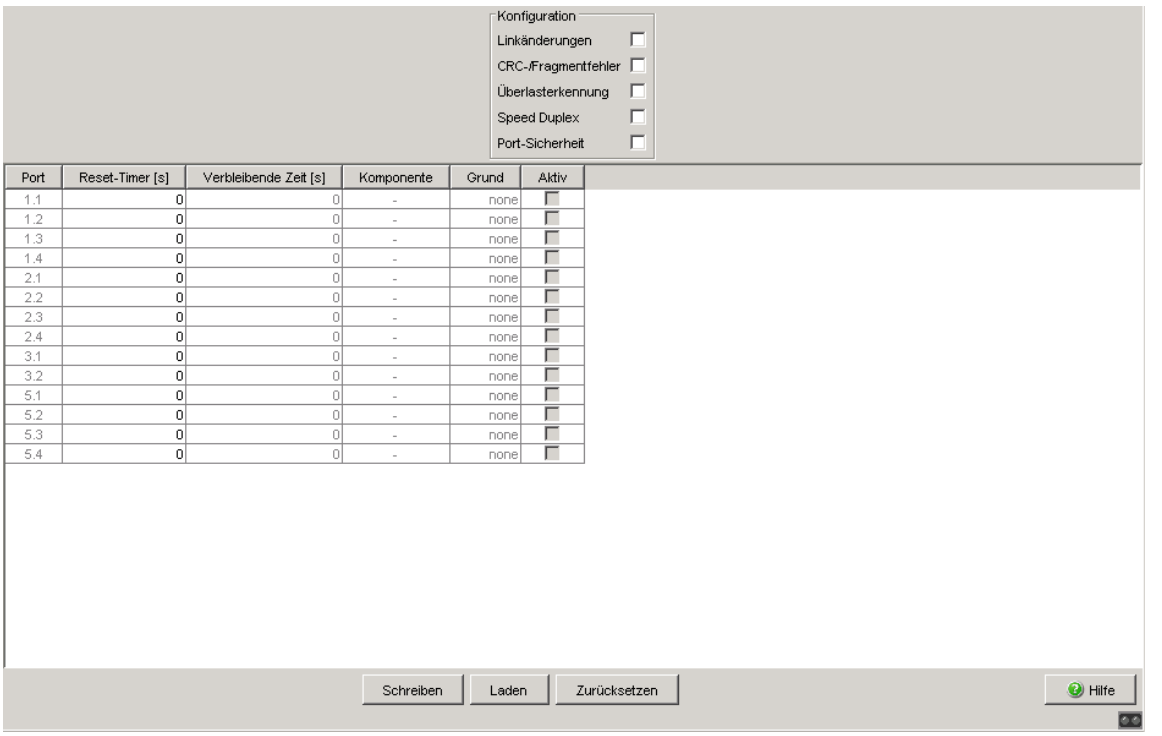


Abb. 91: Dialog „Auto-Disable“

Konfiguration

Parameter	Bedeutung
Linkänderungen	Aktiviert/deaktiviert das Überwachen von Linkänderungen auf den Ports. Mögliche Werte: ▶ `markiert` Die Auto-Disable-Funktion überwacht Linkänderungen auf den Ports. Wenn der Port-Monitor einen Port auf Grund von zu vielen Linkänderungen deaktiviert, re-aktiviert das Gerät den Port nach Ablauf der im Feld „Reset-Timer“ festgelegten Zeit. Voraussetzung ist, dass der „Reset-Timer“-Wert für den Port >0 ist. ▶ `unmarkiert` (Voreinstellung) Die Auto-Disable-Funktion ignoriert Linkänderungen auf den Ports.
CRC-/Fragmentfehler	Aktiviert/deaktiviert das Überwachen von CRC-/Fragmentfehlern auf den Ports. Mögliche Werte: ▶ `markiert` Die Auto-Disable-Funktion überwacht CRC-/Fragmentfehler auf den Ports. Wenn der Port-Monitor einen Port auf Grund von zu vielen CRC-/Fragmentfehlern deaktiviert, re-aktiviert das Gerät den Port nach Ablauf der im Feld „Reset-Timer“ festgelegten Zeit. Voraussetzung ist, dass der „Reset-Timer“-Wert für den Port >0 ist. ▶ `unmarkiert` (Voreinstellung) Die Auto-Disable-Funktion ignoriert CRC-/Fragmentfehler auf den Ports.
Überlasterkennung	Aktiviert/deaktiviert das Überwachen der Last auf den Ports. Mögliche Werte: ▶ `markiert` Die Auto-Disable-Funktion überwacht die Last auf den Ports. Wenn der Port-Monitor einen Port auf Grund von Überlast deaktiviert, re-aktiviert das Gerät den Port nach Ablauf der im Feld „Reset-Timer“ festgelegten Zeit. Voraussetzung ist, dass der „Reset-Timer“-Wert für den Port >0 ist. Für weitere Voraussetzungen siehe „Überlasterkennung” auf Seite 352. ▶ `unmarkiert` (Voreinstellung) Die Auto-Disable-Funktion ignoriert die Last auf den Ports.

Tab. 211: Rahmen „Konfiguration“ im Dialog `Diagnose:Ports:Auto-Disable`

Parameter	Bedeutung
Speed Duplex	Aktiviert/deaktiviert das Überwachen der Geschwindigkeits- und Duplex-Kombination auf den Ports. Mögliche Werte: ▶ `markiert` Die Auto-Disable-Funktion überwacht die Geschwindigkeits- und Duplex-Kombination auf den Ports. Wenn der Port-Monitor einen Port auf Grund einer unerlaubten Kombinationen von Geschwindigkeit und Duplex-Modus deaktiviert, re-aktiviert das Gerät den Port nach Ablauf der im Feld „Reset-Timer“ festgelegten Zeit. Voraussetzung ist, dass der „Reset-Timer“-Wert für den Port >0 ist. ▶ `unmarkiert` (Voreinstellung) Die Auto-Disable-Funktion ignoriert die Geschwindigkeits- und Duplex-Kombination auf den Ports.
Port-Sicherheit	Aktiviert/deaktiviert das Überwachen von unberechtigten Zugriffen auf den Ports im Zusammenarbeit mit der Funktion „Port-Sicherheit“ (siehe auf Seite 89 „Portsicherheit“). Mögliche Werte: ▶ `markiert` Die Auto-Disable-Funktion überwacht unberechtigte Zugriffe auf den Ports. Wenn der Port-Monitor einen Port auf Grund von zu vielen CRC-/Fragmentfehlern deaktiviert, re-aktiviert das Gerät den Port nach Ablauf der im Feld „Reset-Timer“ festgelegten Zeit. Voraussetzung ist, dass der „Reset-Timer“-Wert für den Port >0 ist. ▶ `unmarkiert` (Voreinstellung) Die Auto-Disable-Funktion ignoriert unberechtigte Zugriffe auf den Ports.

Tab. 211: Rahmen „Konfiguration“ im Dialog `Diagnose:Ports:Auto-Disable` (Forts.)

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Geräte-Ports, auf den sich der Tabelleneintrag bezieht.
Reset-Timer [s]	Legt die Zeitspanne in Sekunden fest, nach der das Gerät den durch den Port-Monitor deaktivierten Port automatisch re-aktiviert. Mögliche Werte: ▶ `0` (Voreinstellung) Timer ist deaktiviert. Der Port bleibt deaktiviert. ▶ `30...2147483` Wenn der Port-Monitor den Port auf Grund von Überlast deaktiviert hat, gelten für das Re-Aktivieren des Ports weitere Voraussetzungen (siehe auf Seite 352 „Überlasterkennung“).
Verbleibende Zeit [s]	Verbleibende Zeit in Sekunden bis zur automatischen Re-Aktivierung des Ports.
Komponente	Zeigt den Namen der Funktion, die den Port deaktiviert hat.
Grund	Zeigt das auslösende Ereignis, auf Grund dessen der Port-Monitor den Port deaktiviert hat.
Aktiv	Zeigt, ob die Auto-Disable-Funktion auf dem betreffenden Port aktiv ist. Mögliche Werte: ▶ `markiert` Die Auto-Disable-Funktion ist auf dem Port aktiv. Der Port ist im Augenblick deaktiviert. Nach Ablauf der im Feld „Reset-Timer“ festgelegten Zeit re-aktiviert die Auto-Disable-Funktion den Port. ▶ `unmarkiert` (Voreinstellung) Die Auto-Disable-Funktion ist auf dem Port inaktiv.

Tab. 212: Tabelle im Dialog `Diagnose:Ports:Auto-Disable`

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Zurücksetzen	Aktiviert den Port nach Deaktivierung durch die Port-Monitor- oder Port-Sicherheit-Funktion.
Hilfe	Öffnet die Online-Hilfe.

Tab. 213: Schaltflächen

8.4 Konfigurations-Check

Das Gerät bietet Ihnen die Möglichkeit, seine Konfiguration mit denen seiner Nachbar-Geräte zu vergleichen.
Dazu verwendet es die Daten, die es mittels Topologie-Erkennung (LLDP) von seinen Nachbargeräten empfangen hat.
Der Dialog listet die erkannten Abweichungen auf, die die Leistungsfähigkeit der Kommunikation zwischen dem Gerät und den erkannten Nachbargeräten beeinflussen.

☐ Mit der „Laden“-Bedientaste aktualisieren Sie den Inhalt der Tabelle. Bleibt die Tabelle leer, war der Konfigurations-Check erfolgreich und die Konfiguration des Gerätes ist kompatibel zu den erkannten Nachbargeräten.

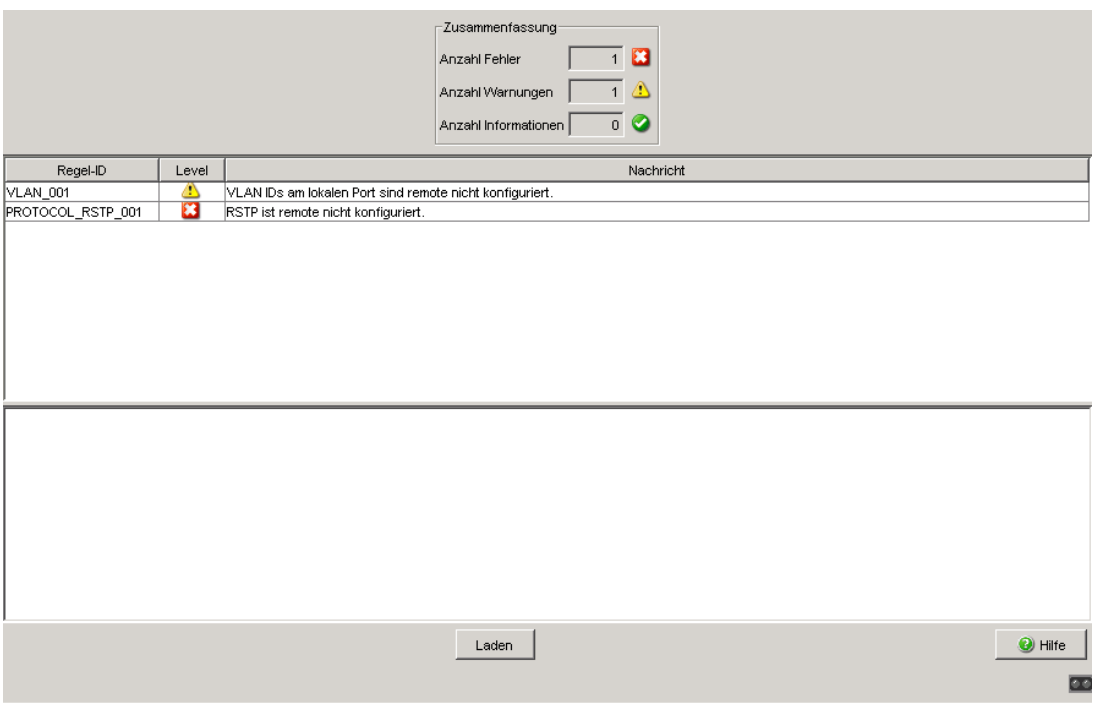


Abb. 92: Dialog Konfigurations-Check

Parameter	Bedeutung
Anzahl Fehler	Zeigt die Anzahl der Fehler an, die das Gerät beim Konfigurations-Check erkannt hat.
Anzahl Warnungen	Zeigt die Anzahl der Warnungen an, die das Gerät beim Konfigurations-Check erkannt hat.
Anzahl Informationen	Zeigt die Anzahl der Informationen an, die das Gerät beim Konfigurations-Check erkannt hat.

Tab. 214: Konfigurations-Check Zusammenfassung

Parameter	Bedeutung
Regel-ID	Regel-ID der aufgetretenen Abweichungen. Der Dialog fasst mehrere Abweichungen mit der gleichen Regel-ID unter einer Regel-ID zusammen.
Level	Grad der Abweichung zwischen der Konfiguration dieses Gerätes und den erkannten Nachbargeräten. Der Regel-Level kann 3 Zustände annehmen: Information: Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten ist nicht beeinträchtigt. Warnung: Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten kann beeinträchtigt sein. Fehler: Die Kommunikation zwischen den beiden Geräten ist beeinträchtigt.
Nachricht	Der Dialog spezifiziert die aufgetretenen Informationen, Warnungen und Fehler genauer.

Tab. 215: Tabelle Konfigurations-Check

☐ Wählen Sie in der Konfigurations-Check-Tabelle eine Zeile aus, zeigt das Gerät im darunterliegenden Fenster weitere Informationen an.

Anmerkung: Ein Nachbargerät ohne LLDP-Unterstützung, das LLDP-Pakete weiterleitet, kann im Dialog mehrdeutige Meldungen verursachen. Dies tritt auf, wenn das Nachbargerät ein Hub oder ein Switch ohne Management ist, der die Norm IEEE 802.1D-2004 ignoriert.
Der Dialog stellt in dem Fall die am Nachbargerät angeschlossenen und erkannten Geräte als direkt mit dem Gerät verbunden dar, obwohl diese am Nachbargerät angeschlossen sind.

Anmerkung: Haben Sie auf dem Gerät mehr als 39 VLANs eingerichtet, zeigt der Dialog stets eine Warnung an. Der Grund ist die begrenzte Anzahl der möglichen VLAN-Informationen in LLDP-Frames mit begrenzter Länge. Das Gerät vergleicht die ersten 39 VLANs automatisch.
Haben Sie 40 oder mehr VLANs eingerichtet, prüfen Sie die Übereinstimmung der weiteren VLANs nötigenfalls manuell.

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 216: Schaltflächen

8.5 Topologie-Erkennung

Dieser Dialog bietet Ihnen die Möglichkeit, die Funktion zur Topologie-Erkennung (LLDP) ein/auszuschalten und die empfangenen LLDP-Informationen in Form von 2 Tabellen anzuzeigen, gruppiert nach allgemeinen LLDP-Informationen und LLDP-MED-Informationen.

8.5.1 LLDP-Informationen von Nachbargeräten

Die Tabelle des Karteikartenreiters „LLDP“ zeigt Ihnen die gesammelten LLDP-Informationen zu Nachbargeräten an. Mit diesen Informationen ist eine Netzmanagement-Station in der Lage, die Struktur Ihres Netzes darzustellen.

Das Aktivieren der Einstellung „FDB-Einträge anzeigen“ unterhalb der Tabelle bietet Ihnen die Möglichkeit, die Tabelleneinträge um Einträge von Geräten ohne aktive LLDP-Unterstützung zu erweitern. Das Gerät nimmt in diesem Fall auch Informationen aus seiner FDB (Forwarding Database) auf.

Die Tabelle zeigt Ihnen an, welche LLDP-Informationen das Gerät an seinen Ports von anderen Geräten empfangen hat.

Parameter	Bedeutung
Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.
Nachbar-Bezeichner	Chassis-ID des Nachbargerätes. Diese kann z.B. die Basis-MAC-Adresse des Nachbargerätes sein.
Nachbar-IP-Adresse	Management-Adresse des Nachbargerätes. Diese kann z.B. eine IPv4-Adresse sein.
Nachbar-Port-Beschreibung	Port-Beschreibung des Nachbargerätes. Die Port-Beschreibung ist eine alphanumerische Zeichenkette.

Tab. 217: Topologie-Erkennung (LLDP-Informationen)

Parameter	Bedeutung
Nachbar-System-name	Systemname des Nachbargerätes. Der Systemname ist eine alpha-numerische Zeichenkette.
Nachbar-Systembeschreibung	Systembeschreibung des Nachbargerätes gemäß IEEE 802.1AB.

Tab. 217: Topologie-Erkennung (LLDP-Informationen)

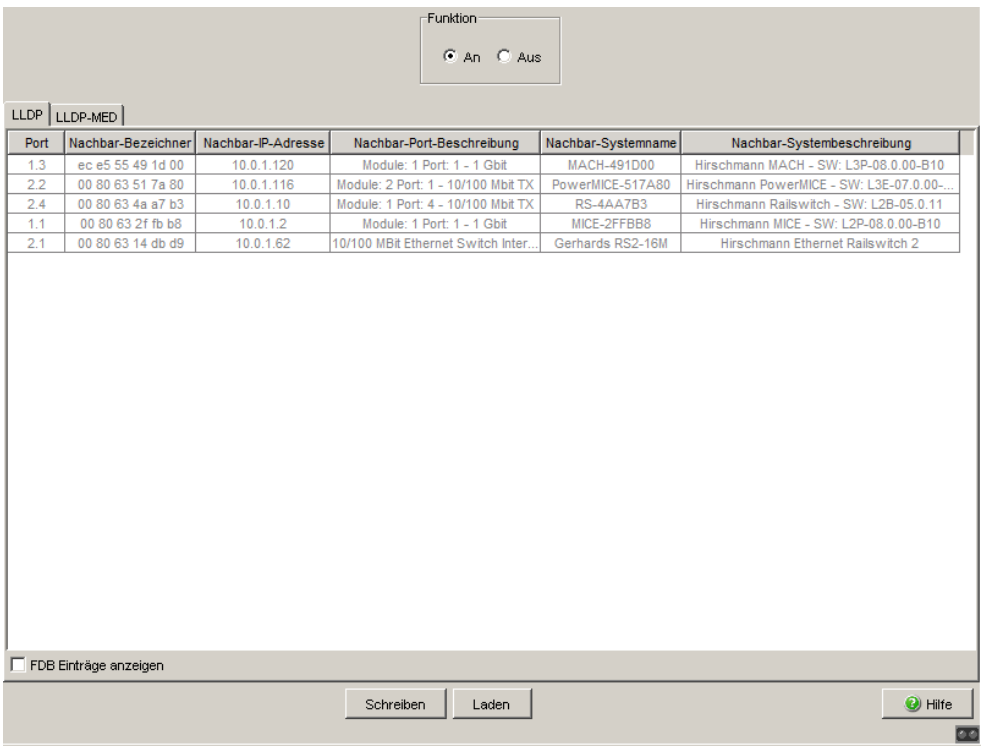


Abb. 93: Topologie-Erkennung

Sind an einem Port, z. B. über einen Hub, mehrere Geräte angeschlossen, dann zeigt die Tabelle pro angeschlossenem Gerät eine Zeile an.

Wenn an einem Port sowohl Geräte mit als auch ohne aktive Topologie-Erkennungs-Funktion angeschlossen sind, dann blendet die Topologie-Tabelle die Geräte ohne aktive Topologie-Erkennung aus.

Wenn ausschließlich Geräte ohne aktive Topologie-Erkennung an einem Port angeschlossen sind, dann enthält die Tabelle stellvertretend für alle Geräte eine Zeile für diesen Port. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.
MAC-Adressen von Geräten, die die Topologie-Tabelle übersichtshalber ausblendet, finden Sie in der Adress-Tabelle (FDB), (siehe auf Seite 169 „Filter für MAC-Adressen“).

8.5.2 LLDP-MED (Media Endpoint Discovery)

Die Tabelle des Karteikartenreiters „LLDP-MED“ zeigt Ihnen ausgewählte LLDP-MED-Informationen zu Nachbargeräten an. Voraussetzung dafür ist, dass sowohl die LLDP-MED-Funktion als auch die LLDP-Funktion (siehe auf Seite 365 „LLDP-Informationen von Nachbargeräten“) eingeschaltet sind.

Das Gerät unterstützt die folgenden Subtypen der Netz-Konnektivitäts-Nachrichten:

- LLDP-MED Capabilities TLV (Subtyp 1)
- LLDP-MED Network Policy TLV (Subtyp 2)

Die Tabelle zeigt Ihnen an, welche LLDP-MED-Informationen das Gerät an seinen Ports von anderen Geräten empfangen hat.

Parameter	Bedeutung
Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.
Device Class	LLDP-MED-Geräteklasse des entfernten Geräts: – 0: undefiniert (Eigenschaften in keiner definierten Klasse enthalten) – 1: Endgeräte-Klasse I – 2: Endgeräte-Klasse II – 3: Endgeräte-Klasse III – 4: Netzwerk-Gerät
VLAN-ID	VLAN-ID der Netz-Richtlinie für den Port des entfernten Gerätes (0 - 4.094), 0: Prioritäts-getaggte Frames
Priority	Layer 2- (IEEE 802.1p-) Priorität der Netz-Richtlinie für den Port des entfernten Gerätes (0 - 7)
DSCP	Wert des Differentiated Services Code Point (nach RFC 2474 und 2475) der Netz-Richtlinie für den Port des entfernten Gerätes (0 - 63)
Unknown Bit Status	– `true`: die Netz-Richtlinie für den Applikations-Typ des entfernten Gerätes ist momentan unbekannt. Die Werte für VLAN ID, Priority und DSCP sind in diesem Fall ohne Bedeutung. – false: die Netz-Richtlinie für den Applikations-Typ des entfernten Gerätes ist bekannt
Tagged Bit Status	– `true`: die Applikation des entfernten Gerätes verwendet VLAN-getaggte Frames – `false`: die Applikation des entfernten Gerätes verwendet ungetaggte Frames oder unterstützt keinen Port-VLAN-basierten Betrieb. Die Werte für VLAN ID und Priority sind in diesem Fall ohne Bedeutung.
Hardware-Revision	Hersteller-spezifischer String mit der Hardware-Version des Endgerätes (max. 32 Zeichen)
Firmware-Revision	Hersteller-spezifischer String mit der Firmware-Version des Endgerätes (max. 32 Zeichen)
Software-Revision	Hersteller-spezifischer String mit der Software-Version des Endgerätes (max. 32 Zeichen)
Serial Number	Hersteller-spezifischer String mit der Seriennummer des Endgerätes (max. 32 Zeichen)
Herstellername	Hersteller-spezifischer String mit dem Namen des Endgeräte-Herstellers (max. 32 Zeichen)

Tab. 218: Topologie-Erkennung (LLDP-MED-Informationen)

Parameter	Bedeutung
Modell-Name	Hersteller-spezifischer String mit dem Namen des Endgeräte-Modells (max. 32 Zeichen)
Asset ID	Hersteller-spezifischer String mit der ID zur Inventarisierung des Endgerätes (max. 32 Zeichen)

Tab. 218: Topologie-Erkennung (LLDP-MED-Informationen)

Anmerkung: Wenn Sie die Funktion LLDP-MED aktivieren, sendet der Switch Informationen über seine Eigenschaften in Form von LLDP-MED-Frames aus. Dazu gehören auch Informationen über die im Switch konfigurierten Voice-VLANs (siehe auf Seite 202 „Voice-VLAN“). Aktivieren Sie daher die Funktion LLDP-MED, wenn Sie an dem Switch Geräte wie z.B. ein VoIP-Telefon per Plug-and-Play betreiben möchten, da dafür beide Geräte Informationen über ihr jeweiliges Nachbargerät benötigen.

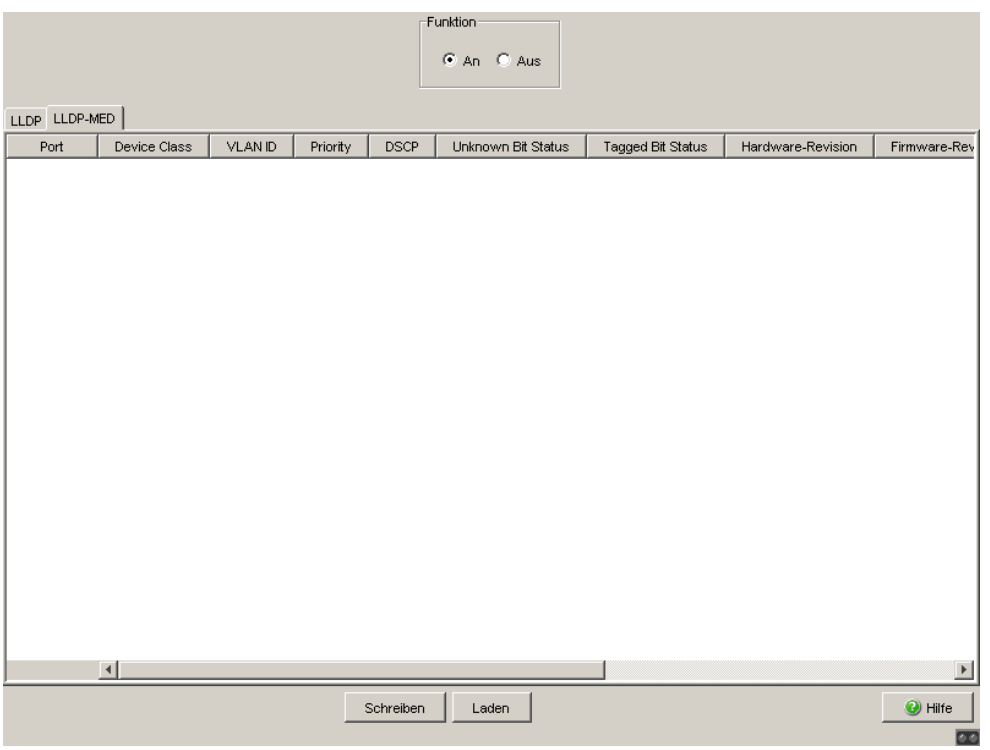


Abb. 94: LLDP-MED-Informationen

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 219: Schaltflächen

8.6 Port-Mirroring

Die Funktion Port-Mirroring bietet Ihnen die Möglichkeit, den Datenverkehr einer Gruppe von Ports des Gerätes zu Diagnosezwecken zu untersuchen. Dabei spiegelt (kopiert) das Gerät die Daten eines oder mehrerer Quellports an den Zielport. Ein am Zielport angeschlossenes Management-Werkzeug, z.B. eine RMON-Probe, kann so den Datenverkehr der Quellports in Sende- und Empfangsrichtung beobachten. Der Datenverkehr an den Quellports bleibt dadurch unbeeinflusst.

Anmerkung: Der Zielport benötigt ausreichend Bandbreite, um den Datenstrom aufzunehmen. Wenn der kopierte Datenstrom die Bandbreite des Zielports überschreitet, verwirft das Gerät überschüssige Datenpakete auf dem Zielport.

Als Quell- oder Zielport sind physikalische Ports verwendbar.
Die Geräte MACH4002 24/48 + 4G und Power MICE unterstützen bis zu 8 Quellports.

☐ Wählen Sie aus der Liste der physikalischen Ports die Quell-Ports aus, deren Datenverkehr sie beobachten möchten. Markieren Sie die entsprechenden Kontrollkästchen.
Das Gerät stellt in der Tabelle den Port, der sich momentan als „Ziel-Port“ in Verwendung befindet, ausgegraut dar. Voreinstellung: (keine Quell-Ports)

☐ Wählen Sie im Rahmen „Ziel-Port“ den Ziel-Port, an dem Sie Ihr Management-Werkzeug angeschlossen haben.
Die Dropdown-Liste zeigt ausschließlich die verfügbaren Ports an. Ports, die momentan als Quell-Ports in Benutzung sind, sind nicht auswählbar. Voreinstellung: (kein Ziel-Port)

☐ Legen Sie die zu überwachende Richtung des Datenverkehrs fest.
  – Wenn Sie „RX“ festlegen, spiegelt das Gerät ausschließlich die am Quellport empfangenen Frames an den Zielport (Eingangsüberwachung).
  – Wenn Sie „TX“ festlegen, spiegelt das Gerät ausschließlich die am Quellport gesendeten Frames an den Zielport (Ausgangsüberwachung).

☐ Um die Funktion einzuschalten, wählen Sie `An` im Rahmen `Funktion` und klicken Sie „Schreiben“. Voreinstellung: `Aus`.

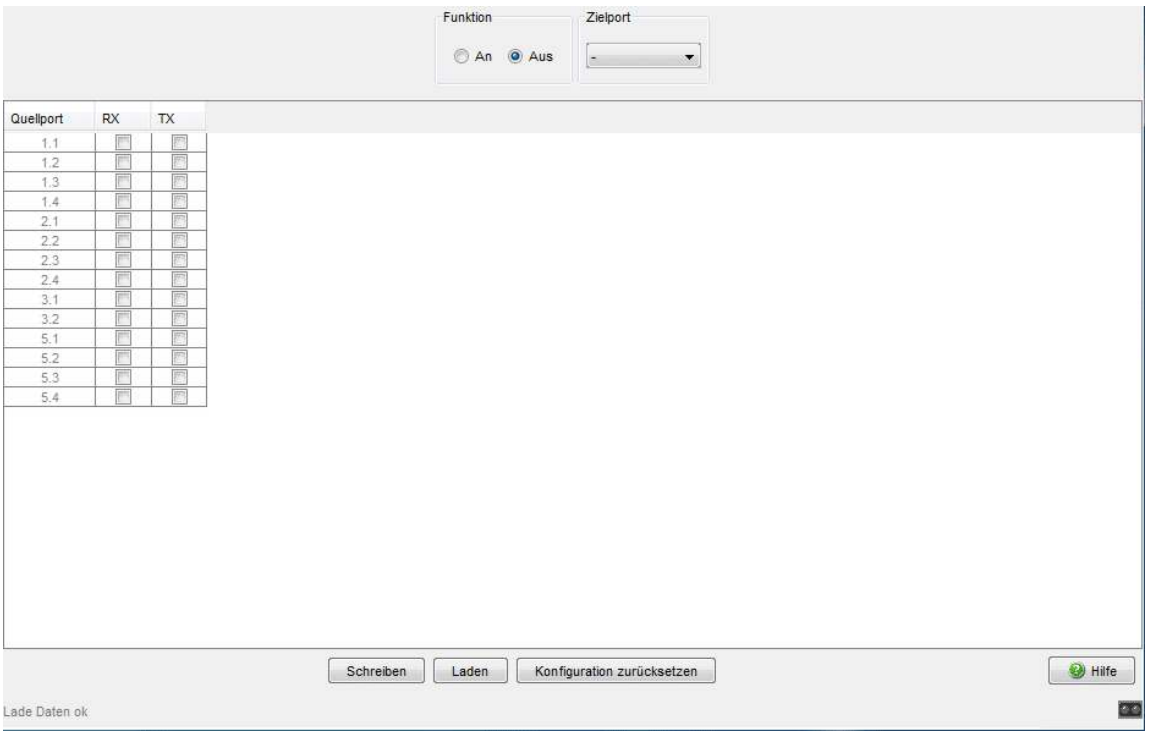


Abb. 95: Dialog `Diagnose:Port-Mirroring N:1`

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Konfiguration zurücksetzen	Setzt die Einstellungen des Dialogs in den Lieferzustand zurück.
Hilfe	Öffnet die Online-Hilfe.

Tab. 220: Schaltflächen

8.7 Gerätestatus

Der Gerätestatus gibt einen Überblick über den Gesamtzustand des Gerätes. Viele Prozessvisualisierungssysteme erfassen den Gerätestatus eines Gerätes, um seinen Zustand grafisch darzustellen.

Das Gerät zeigt seinen aktuellen Status als „Fehler“ oder „Ok“ im Rahmen „Gerätestatus“ an. Das Gerät bestimmt diesen Status aus den einzelnen Überwachungsergebnissen.

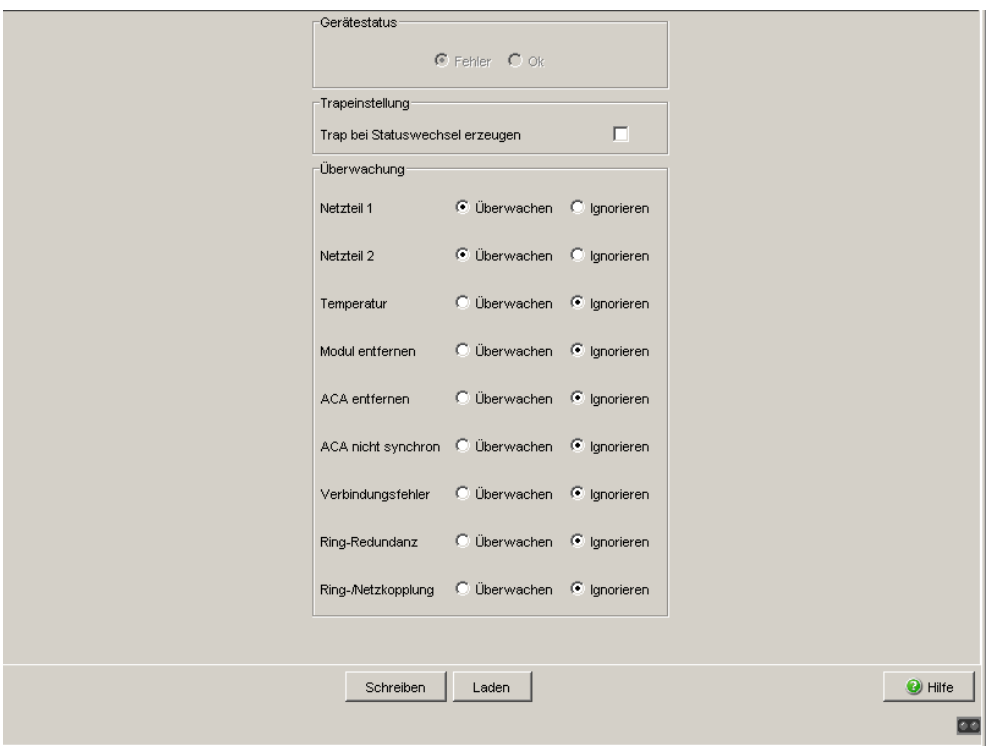


Abb. 96: Dialog Gerätestatus (bei PowerMICE)

☐ Wählen Sie im Feld „Überwachung“ die Ereignisse, die Sie überwachen möchten.
☐ Zur Temperaturüberwachung stellen Sie zusätzlich die Temperatur-schwellen im Dialog `Grundeinstellungen:System` am Ende der Systemdaten ein .

Die auswählbaren Ereignisse haben folgende Bedeutung:

Name	Bedeutung
Rahmen „Gerätestatus“	Das Gerät bestimmt diesen Status aus den einzelnen Überwachungsergebnissen. Er kann die Werte „Fehler“ oder „Ok“ annehmen.
Rahmen „Trapeinstellungen“	-
Trap bei Statuswechsel erzeugen.	Aktivieren Sie diese Einstellung, damit das Gerät einen Traps versendet, wenn es seinen Gerätestatus ändert.
Rahmen „Überwachung“	-
Netzteil ...	Versorgungsspannung(en) überwachen/ignorieren
Temperatur (°C)	Eingestellte Temperaturschwelle (siehe auf Seite 22 „System“) auf Über- und Unterschreiten überwachen/ignorieren
Modul entfernen	Entfernen eines Moduls überwachen/ignorieren (bei modularen Geräten).
ACA entfernen	Entfernen des ACA überwachen/ignorieren.
ACA nicht synchron	Nichtübereinstimmung der Konfiguration im Gerät und auf dem ACA[a] überwachen/ignorieren.
Verbindungsfehler	Den fehlerhaften Linkstatus mindestens eines Ports überwachen/ignorieren. Die Meldung des Linkstatus kann pro Port über das Management maskiert werden (siehe auf Seite 37 „Portkonfiguration“). Im Lieferzustand erfolgt keine Verbindungsüberwachung.
Ring-Redundanz	Ring-Redundanz überwachen/ignorieren (bei HIPER-Ring nur im Ring-Manager-Betrieb). Im Lieferzustand erfolgt keine Überwachung der Ring-Redundanz. Ist das Gerät normaler Ring-Teilnehmer und nicht Ring-Manager, meldet es folgendes: ▶ nichts (beim HIPER-Ring) ▶ erkannte Fehler in der lokalen Konfiguration (beim Fast HIPER-Ring und bei MRP)

Tab. 221: Gerätestatus

Name	Bedeutung
Ring-/Netzkopplung	Überwachen/ignorieren der Kopplungs-Redundanz-Funktion. Im Lieferzustand erfolgt keine Überwachung der Kopplungs-Redundanz. Bei der Zwei-Switch-Kopplung mit Steuerleitung meldet der Slave zusätzlich folgende Zustände: – fehlerhafter Linkstatus der Steuerleitung – Partnergerät ist ebenfalls Slave (im Stand-by-Modus). **Anmerkung:** Bei der Zwei-Switch-Kopplung ist Voraussetzung, dass beide Switches ihren jeweiligen Partner gefunden haben.
Lüfter	Funktion des Lüfters überwachen/ignorieren (bei Geräten mit Lüfter).

Tab. 221: Gerätestatus

a. Die Konfigurationen stimmen dann nicht überein, wenn nur eine Datei existiert oder die 2 Dateien nicht den gleichen Inhalt haben.

Anmerkung: Bei nicht redundanter Zuführung der Versorgungsspannung meldet das Gerät das Fehlen einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder die Überwachung ausschalten (siehe auf Seite 377 „Meldekontakt“).

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 222: Schaltflächen

8.8 Meldekontakt

Die Meldekontakte ermöglichen Ihnen

- die Steuerung externer Geräte durch die manuelle Einstellung der Meldekontakte,
- die Funktionsüberwachung des Gerätes,
- die Signalisierung des Gerätestatus des Gerätes.

8.8.1 Manuelle Einstellung

☐ Wählen Sie die Karteikarte „Meldekontakt 1“ oder „Meldekontakt 2“ (bei Geräten mit 2 Meldekontakten).
☐ Wählen Sie im Feld „Modus Meldekontakt“ den Modus „Manuelle Einstellung“. Dieser Modus bietet Ihnen die Möglichkeit, diesen Meldekontakt fernzubedienen.
☐ Wählen Sie „Offen“ im Feld „Manuelle Einstellung“, um den Kontakt zu öffnen.
☐ Wählen Sie „Geschlossen“ im Feld „Manuelle Einstellung“, um den Kontakt zu schließen.

Anwendungsmöglichkeiten:

- Simulation eines Fehlers bei einer SPS-Fehlerüberwachung.
- Fernbedienung eines Gerätes über SNMP, wie z.B. das Einschalten einer Kamera.

8.8.2 Funktionsüberwachung

☐ Wählen Sie die Karteikarte „Meldekontakt 1“ oder „Meldekontakt 2“ (bei Geräten mit 2 Meldekontakten).

☐ Wählen Sie im Feld „Modus Meldekontakt“ den Modus „Funktionsüberwachung“. Die Meldekontakte dienen in diesem Modus der Funktionsüberwachung des Gerätes und ermöglichen damit eine Ferndiagnose. Über die potentialfreien Meldekontakte (Relaiskontakt, Ruhestromschaltung) werden durch Kontaktunterbrechung die folgenden Zustände gemeldet.

- Der Ausfall der Versorgungsspannung 1/2 (entweder der externen Versorgungsspannung oder der internen Spannung).[1] Wählen Sie „Netzteil überwachen", wenn der Meldekontakt den Ausfall der Versorgungsspannung oder der geräteinternen Spannung, die aus den Versorgungsspannungen erzeugt wird, melden soll.
- Über- oder Unterschreiten der eingestellten Temperaturschwelle (siehe auf Seite 23 „Systemdaten“). Wählen Sie Temperatur „überwachen", wenn der Meldekontakt eine unzulässige Temperatur melden soll.
- Das Entfernen eines Moduls. Wählen Sie Modul entfernen „überwachen“, wenn der Meldekontakt das Entfernen eines Moduls melden soll (bei modularen Geräten).
- Lüfter funktioniert nicht mehr (bei Geräten mit Lüfter).
- Das Entfernen des ACA. Wählen Sie ACA entfernen „überwachen“, wenn der Meldekontakt das Entfernen des ACA melden soll (bei Geräten mit Unterstützung des ACA).
- Nichtübereinstimmung der Konfiguration im Gerät und auf dem ACA[2]. Wählen Sie ACA nicht synchron „überwachen“, wenn der Meldekontakt die Nichtübereinstimmung der Konfiguration melden soll (bei Geräten mit Unterstützung des ACA).

1. In einem MACH4000-Gerät können Sie zusätzliche Netzteile installieren, die das Gerät in den Bedienoberflächen als P3-1, P3-2, P4-1 und P4-2 anzeigt. Details zu den Netzteilen finden Sie im Dokument Installations-Handbuch.
2. Die Konfigurationen stimmen dann nicht überein, wenn nur eine Datei existiert oder die 2 Dateien nicht den gleichen Inhalt haben.

- Der Verbindungsfehler (funktionsunfähiger Linkstatus) mindestens eines Ports. Die Meldung des Linkstatus kann beim Gerät pro Port über das Management maskiert werden. Im Lieferzustand ist die Verbindungsüberwachung inaktiv. Wählen Sie Verbindungsfehler „überwachen“, wenn das Gerät über den Meldekontakt einen fehlerhaften Linkstatus mindestens eines Ports melden soll.

- Wenn das Gerät Teil eines redundanten Rings ist: der Entfall der Redundanz-Reserve (d.h., die Redundanzfunktion hat sich tatsächlich eingeschaltet), (siehe auf Seite 258 „Ring-Redundanz“).
  - ☐ Wählen Sie Ring-Redundanz „Überwachen“, wenn der Meldekontakt den Entfall der Redundanz-Reserve im redundanten Ring melden soll.
  - ☐ Wählen Sie Sub-Ring-Redundanz „Überwachen“, wenn der Meldekontakt den Entfall der Redundanz-Reserve im redundanten Sub-Ring melden soll.

  Lieferzustand: keine Überwachung.

  Anmerkung: Ist das Gerät normaler Ring-Teilnehmer und nicht Ring-Manager, meldet es beim HIPER-Ring nichts, beim Fast HIPER-Ring und bei MRP nur erkannte Fehler in der lokalen Konfiguration.

- Der Entfall der Redundanz-Reserve bei der Ring-/Netzkopplung (d. h., die Redundanzfunktion hat sich tatsächlich eingeschaltet). Wählen Sie Ring-/Netzkopplung "überwachen", wenn der Meldekontakt einen Entfall der Redundanz-Reserve bei der Ring-/Netzkopplung melden soll (siehe auf Seite 258 „Ring-Redundanz“).
  Lieferzustand: keine Überwachung.

  Anmerkung: Bei der Zwei-Switch-Kopplung ist Voraussetzung, dass beide Switches ihren jeweiligen Partner gefunden haben.

8.8.3 Gerätestatus

☐ Wählen Sie die Karteikarte „Meldekontakt 1“ oder „Meldekontakt 2“ (bei Geräten mit zwei Meldekontakten).
☐ Wählen Sie im Feld „Modus Meldekontakt“ den Modus „Gerätestatus“.
Der Meldekontakt dient in diesem Modus der Überwachung des Status des Gerätes (siehe auf Seite 22 „Gerätestatus“) und ermöglicht damit eine Ferndiagnose.
Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung der Gerätestatus „Fehler detektiert“ (siehe auf Seite 22 „Gerätestatus“) gemeldet.

8.8.4 Trapeinstellung

☐ Wählen Sie `Trap bei Statuswechsel erzeugen`, damit das Gerät ein Trap erzeugt, sobald sich bei aktiver Funktionsüberwachung die Stellung eines Meldekontaktes ändert.

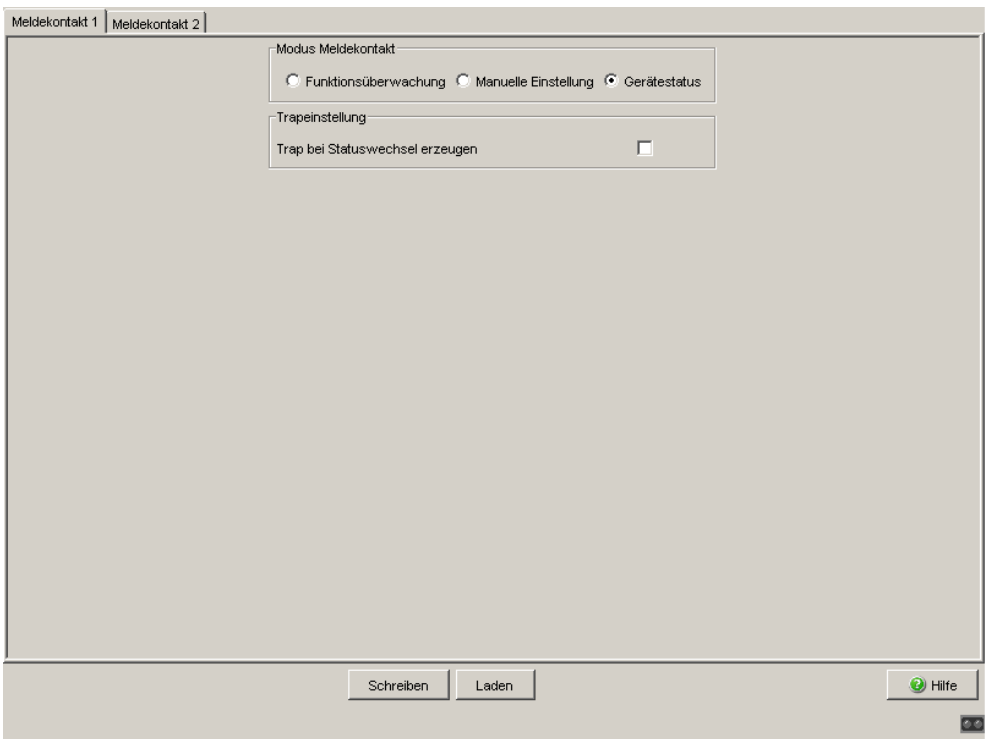


Abb. 97: Dialog Meldekontakt

Der Dialog Meldekontakt enthält 1 Karteikarte („Meldekontakt 1“), wenn das Gerät 1 Meldekontakt besitzt.

Der Dialog Meldekontakt enthält 2 Karteikarten („Meldekontakt 1“ und „Meldekontakt 2“), wenn das Gerät 2 Meldekontakte besitzt.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 223: Schaltflächen

8.9 Alarme (Traps)

Dieser Dialog bietet Ihnen die Möglichkeit festzulegen, welche Ereignisse einen Alarm (Trap) auslösen und an wen diese Alarme gesendet werden sollen.

Die folgenden Gerätetypen unterstützen 6 Trap-Ziele:
- PowerMICE
- MACH 104
- MACH 1040
- MACH 4000

☐ Im Rahmen „Konfiguration“ wählen Sie die Trap-Kategorien aus, von denen Sie Traps versenden wollen. Voreinstellung: alle Trap-Kategorien sind aktiv.

☐ Klicken Sie „Erzeugen“.
☐ In der Spalte „IP-Adresse“ geben Sie die IP-Adresse des Empfängers an, an den die Traps geschickt werden sollen.
☐ In der Spalte „Passwort“ geben Sie den Community-Namen an, den das Gerät verwendet, um sich als Quelle des Traps zu identifizieren.
☐ In der Spalte „Aktiv“ kreuzen Sie die Einträge an, die das Gerät beim Versenden von Traps berücksichtigen sollen. Voreinstellung: inaktiv.

Die auswählbaren Ereignisse haben folgende Bedeutung:

Name	Bedeutung
Authentifizierung	Das Gerät hat einen unerlaubten Zugriff zurückgewiesen (siehe auf Seite 76 „SNMPv1/v2-Zugriffs-Einstellungen“).
Link Up/Down	An einem Port des Gerätes wurde die Verbindung zu einem anderen Gerät hergestellt/unterbrochen.
Spanning Tree	Die Topologie des Rapid Spanning Tree hat sich geändert

Tab. 224: Trap-Kategorien

Name	Bedeutung
Chassis	Fasst die folgenden Ereignisse zusammen: ▶ Der Status einer Versorgungsspannung hat sich geändert (siehe Dialog `System`). ▶ Der Status des Meldekontakts hat sich geändert. Um dieses Ereignis zu berücksichtigen, aktivieren Sie „Trap bei Statuswechsel erzeugen“ im Dialog `Diagnose:Meldekontakt 1/2`. ▶ Der AutoConfiguration Adapter (ACA) wurde hinzugefügt oder entfernt. ▶ Die Konfiguration auf dem AutoConfiguration Adapter (ACA) unterscheidet sich von der im Gerät. ▶ Die Temperaturschwellen wurden unter- oder überschritten. ▶ Der Empfangsleistungs-Status eines Ports mit SFP-Modul hat sich geändert (siehe Dialog `Diagnose:Ports:SFP-Module`). ▶ Die Konfiguration wurde erfolgreich im Gerät und in einem ggf. vorhandenen AutoConfiguration Adapter (ACA) abgespeichert. ▶ Die Konfiguration wurde nach dem Speichern im Gerät zum 1. Mal verändert.
Redundanz	Der Redundanzzustand der Ring-Redundanz (redundante Strecke aktiv/inaktiv) oder (bei Geräten, die redundante Ring-/Netzkopplung unterstützen) der redundanten Ring-/Netzkopplung (Redundanz vorhanden) hat sich geändert.
Portsicherheit	An einem Port wurde ein Datenpaket von einem nicht erlaubten Endgerät empfangen (siehe Dialog `Portsicherheit`).

Tab. 224: Trap-Kategorien

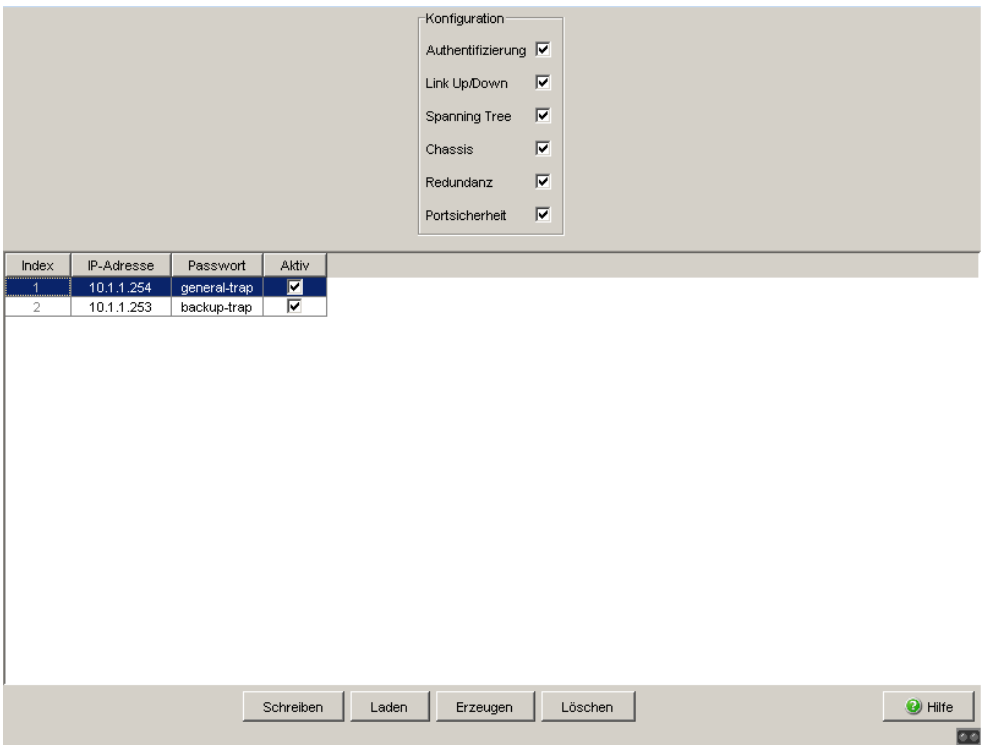


Abb. 98: Dialog Alarme

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 225: Schaltflächen

8.10 Bericht

Folgende Berichte stehen zur Diagnose zur Verfügung:

- System Information (siehe auf Seite 389 „Systeminformationen“).
  Die Systeminformation ist eine HTML-Datei mit systemrelevanten Daten. Das Gerät zeigt die Systeminformation in seinem eigenen Dialogfenster an.
- Event Log (siehe auf Seite 389 „Event-Log“).
  Das Event-Log ist eine HTML-Datei, in die das Gerät wichtige geräteinterne Ereignisse schreibt. Das Gerät zeigt die Log-Datei in seinem eigenen Dialogfenster an.

Anmerkung: Sie haben die Möglichkeit, die geloggten Ereignisse zusätzlich an einen oder mehrere Syslog-Server zu senden (siehe auf Seite 332 „Syslog“).

Folgende Bedientasten stehen zur Verfügung:

- Download Switch-Dump.
  Diese Bedientaste bietet Ihnen die Möglichkeit, Systeminformationen als Dateien in einem ZIP-Archiv herunterzuladen (siehe Tabelle 226).
  - ☐ Wählen Sie das Verzeichnis aus, in dem Sie den Switch-Dump speichern möchten.
  - ☐ Klicken Sie auf „Speichern“.

Das Gerät erzeugt den Dateinamen des Switch-Dumps automatisch nach dem Muster <IP-Adresse>_<Systemname>.zip, für ein Gerät vom Typ PowerMICE z.B. „10.0.1.112_PowerMICE-517A80.zip“.

- Download JAR-File.
  Diese Bedientaste bietet Ihnen die Möglichkeit, das Applet des Web-based Interface als JAR-Datei herunterzuladen. Sie haben danach die Möglichkeit, das Applet außerhalb eines Browsers zu starten.
  Dies ermöglicht Ihnen die Administration des Gerätes auch dann, wenn Sie dessen Web-Server aus Sicherheitsgründen abgeschaltet haben.

  ☐ Wählen Sie das Verzeichnis aus, in dem Sie das Applet speichern möchten.

  ☐ Klicken Sie auf „Speichern“.

Das Gerät erzeugt den Dateinamen des Applets automatisch nach dem Muster <Gerätetyp><Software-Variante><Software-Version)>_<Software-Revision des Applets>.jar, für ein Gerät von Typ PowerMICE mit der Software-Variante L3P z.B. „pmL3P06000_00.jar“.

Datei	Name	Format	Bemerkungen
Log-Datei	event_log.html	HTML	
System-Informationen	systemInfo.html	HTML	
Trap-Log	traplog.txt	Text	
Geräte-Konfiguration (binär)	switch.cfg, powermice.cfg oder .mach.cfg	Binär	Dateiname abhängig vom Gerätetyp.
Geräte-Konfiguration (als Skript)	switch.cli, powermice.cli oder mach.cli	Skript	Dateiname abhängig vom Gerätetyp.
Interner Speicherauszug zur Produktverbesserung durch den Hersteller	dump.hmd	Binär	

Tab. 226: Dateien im Switch-Dump-Archiv
a: Voraussetzung: eine Telnet-Verbindung ist verfügbar.
b: Voraussetzung: Sie sind als Benutzer mit Schreibrechten angemeldet.

Datei	Name	Format	Bemerkungen
Exception-Log	exception_log.html	HTML	
Ausgaben der CLI-Kommandos[a]: – show running-config[b] – show port all – show sysinfo – show mac-address-table – show mac-filter-table igmpsnooping	clicommands.txt	Text	

Tab. 226: Dateien im Switch-Dump-Archiv
a: Voraussetzung: eine Telnet-Verbindung ist verfügbar.
b: Voraussetzung: Sie sind als Benutzer mit Schreibrechten angemeldet.

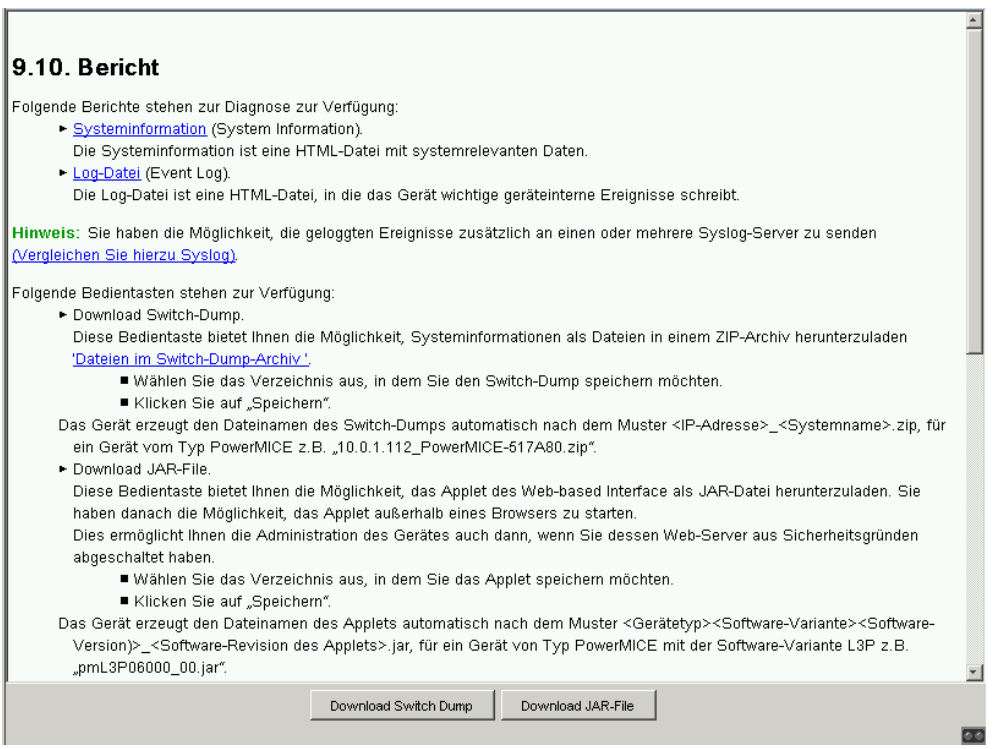


Abb. 99: Dialog Bericht

8.10.1 Systeminformationen

Die Systeminformation ist eine HTML-Datei mit systemrelevanten Daten.

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Suchen	Öffnet den Dialog „Finden“. Der Dialog bietet Ihnen die Möglichkeit, die Log-Datei nach Suchbegriffen oder regulären Ausdrücken zu durchsuchen.
Speichern	Öffnet den Dialog „Speichern“. Der Dialog bietet Ihnen die Möglichkeit, die Log-Datei im HTML-Format auf Ihrem PC zu speichern.
Hilfe	Öffnet die Online-Hilfe.

Tab. 227: Schaltflächen

8.10.2 Event-Log

Die Log-Datei (Event Log) ist eine HTML-Datei, in die das Gerät wichtige geräteinterne Ereignisse schreibt.

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Suchen	Öffnet den Dialog „Finden“. Der Dialog bietet Ihnen die Möglichkeit, die Log-Datei nach Suchbegriffen oder regulären Ausdrücken zu durchsuchen.

Tab. 228: Schaltflächen

Schaltfläche	Bedeutung
Speichern	Öffnet den Dialog „Speichern“. Der Dialog bietet Ihnen die Möglichkeit, die Log-Datei im HTML-Format auf Ihrem PC zu speichern.
Logdatei löschen	Entfernt die protokollierten Einträge aus der Log-Datei.
Hilfe	Öffnet die Online-Hilfe.

Tab. 228: Schaltflächen (Forts.)

8.11 IP-Adressen-Konflikterkennung

Dieser Dialog bietet Ihnen die Möglichkeit, Adresskonflikte des Gerätes mit seiner eigenen IP-Adresse zu erkennen und zu beheben (Address Conflict Detection, ACD).

☐ Wählen Sie in „Status“ die Betriebsart der IP-Adresskonflikt-Erkennung (siehe Tabelle 229). Die Voreinstellung ist `disable`.

☐ Im Feld „Fehlerzustand“ zeigt das Gerät das aktuelle Ergebnis der IP-Adresskonflikt-Erkennung an.
Mögliche Werte sind:
- `false`: die Erkennung ist ausgeschaltet oder das Gerät hat kein Problem festgestellt; oder
- `true`: das Gerät hat ein Problem festgestellt.

Modus	Bedeutung
Feld „Status“	Legt den Status für die IP-Adressen-Konflikterkennung fest. Der Status kann die Werte „enable“, „disable“, „activeDetectionOnly“ oder „passiveDetectionOnly“ annehmen.
`enable`	Aktive und passive Erkennung einschalten.
`disable`	Funktion ausschalten
`activeDetectionOnly`	Ausschließlich aktive Detektion einschalten. Das Gerät überprüft unmittelbar nach dem Anschluss an ein Netz oder nach einer Änderung der IP-Konfiguration, ob seine eigene IP-Adresse schon im Netz vorhanden ist. Ist die IP-Adresse bereits vorhanden, dann wechselt es, falls möglich, wieder zurück zur vorhergehenden Konfiguration und startet nach 15 Sekunden einen erneuten Versuch. Das Gerät vermeidet so, am Netzverkehr mit einer doppelten IP-Adresse teilzunehmen.

Tab. 229: Mögliche Adresskonflikt-Betriebsmodi

Modus	Bedeutung
`passiveDetectio-nOnly`	Ausschließlich passive Detektion einschalten. Das Gerät lauscht passiv am Netz, ob seine IP-Adresse noch einmal vorhanden ist. Erkennt es eine doppelte IP-Adresse, dann verteidigt es mit Hilfe des ACD-Mechanismus´ zuerst seine Adresse durch Aussenden von Gratituous ARPs. Geht die Gegenstelle daraufhin nicht vom Netz, dann geht das Management-Interface des lokalen Gerätes vom Netz. Zyklisch nach 15 Sekunden startet es erneut eine Erkennung, ob der Adresskonflikt noch vorliegt. Falls nicht, geht es wieder ans Netz.
Feld „Fehler“	Zeigt an, ob das Gerät einen IP-Adressen-Konflikt erkannt hat. In diesem Fall hat das Feld den Wert „false“.

Tab. 229: Mögliche Adresskonflikt-Betriebsmodi

- In der Tabelle protokolliert das Gerät IP-Adresskonflikte mit seiner IP-Adresse. Zu jedem Konflikt protokolliert das Gerät folgende Informationen:
  - die Uhrzeit (Spalte „Timestamp“),
  - die IP-Adresse, mit der der Konflikt bestand (Spalte „IP-Adresse“),
  - die MAC-Adresse des Gerätes, mit dem der IP-Adresskonflikt bestand (Spalte „Mac-Adresse“).

  Je IP-Adresse protokolliert das Gerät eine Zeile, und zwar die mit dem letzten Konflikt.

☐ Bei einem Neustart löscht das Gerät die Tabelle.

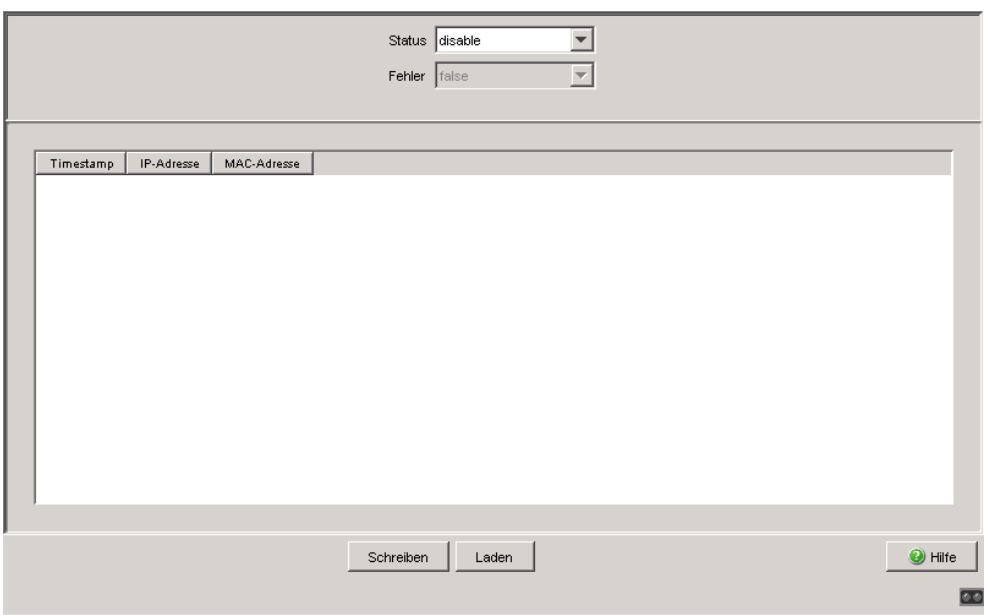


Abb. 100: Dialog IP-Adressen Konflikterkennung

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 230: Schaltflächen

8.12 MAC-Benachrichtigung

Das Gerät bietet Ihnen die Möglichkeit, Änderungen im Netz anhand der MAC-Adresse der Endgeräte zu verfolgen. Wenn sich an einem Port die MAC-Adresse des angeschlossenen Endgerätes ändert, sendet das Gerät periodisch einen SNMP-Trap.

Diese Funktion ist ausschließlich für Ports gedacht, an denen Endgeräte angeschlossen sind und sich demzufolge die MAC-Adresse selten ändert.

8.12.1 Funktion

Parameter	Bedeutung
Funktion	Schaltet die MAC-Benachrichtigungsfunktion des Gerätes global ein oder aus. Mögliche Werte: ▶ `An` Das Gerät sendet Traps für die aktiven Zeilen an die im Dialog `Diagnose:Statuskonfiguration:Alarme (Traps)` konfigurierten aktiven Managementstationen. ▶ `Aus` (Lieferzustand)

Tab. 231: Rahmen „Funktion“ im Dialog `Diagnose:Statuskonfiguration:MAC Benachrichtigung`

8.12.2 Konfiguration

Parameter	Bedeutung
Intervall [s]	Legt die Zeitspanne zwischen Benachrichtigungen in Sekunden fest. Der Gerätepuffer enthält bis zu 20 Adressen. Wenn der Puffer vor Ablauf der Zeitspanne voll ist, sendet das Gerät einen Trap an die Managementstation. Mögliche Werte: ▶ `0..2147483647`

Tab. 232: Rahmen „Konfiguration“ im Dialog `Diagnose:Statuskonfiguration:MAC Benachrichtigung`

8.12.3 Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Geräte-Ports, auf den sich der Tabelleneintrag bezieht.
Aktiv	Schaltet die MAC-Benachrichtigungsfunktion dieses Ports ein oder aus. Mögliche Werte: ▶ `markiert` Sofern global aktiviert, sendet das Gerät Traps für diese Zeile an die im Dialog `Diagnose:Statuskonfiguration:Alarme (Traps)` konfigurierten aktiven Managementstationen. ▶ `unmarkiert` (Voreinstellung)

Tab. 233: Tabelle im Dialog `Diagnose:Statuskonfiguration:MAC Benachrichtigung`

Parameter	Bedeutung
Modus	Legt fest, wann das Gerät für MAC-Adressereignisse an einer bestimmten Schnittstelle einen Trap sendet. Mögliche Werte: ▶ `add` Das Gerät sendet Benachrichtigungen über neue Einträge in der FDB. ▶ `remove` Das Gerät sendet Benachrichtigungen über gelöschte Einträge aus der FDB. ▶ `add + remove` (Voreinstellung) Das Gerät sendet Benachrichtigungen über neue und gelöschte Einträge in/aus der FDB.
Letzte MAC-Addresse	Zeigt für dieses Interface die letzte MAC-Addresse, die der Adresstabelle hinzugefügt oder von ihr entfernt wurde.
Letzter MAC-Status	Zeigt den Status der letzten MAC-Adresse an diesem Interface an. Mögliche Werte: ▶ `other` ▶ `added` ▶ `removed`

Tab. 233: Tabelle im Dialog `Diagnose:Statuskonfiguration:MAC Benachrichtigung` (Forts.)

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 234: Schaltflächen

8.13 Selbsttest

Dieser Dialog bietet Ihnen die Möglichkeit:

- den RAM-Test beim Kaltstart des Gerätes ein-/auszuschalten. Das Ausschalten des RAM-Tests verkürzt die Bootzeit beim Kaltstart des Gerätes.
  Voreinstellung: eingeschaltet.
- das Durchführen eines Neustarts auf Grund eines undefinierten Software- oder Hardwarezustandes ein-/auszuschalten.
  Voreinstellung: eingeschaltet.
- das Wechseln in den System-Monitor während des Systemstarts zu ermöglichen/zu unterbinden.
  Voreinstellung: eingeschaltet, das Wechseln in den System-Monitor ist beim Systemstart über eine V.24-Verbindung möglich.
  Diese Funktion arbeitet ausschließlich in Verbindung mit einem Bootcode in Version 09.0.00 oder höher. Für ein Update des Bootcodes wenden Sie sich an Ihren Vertriebspartner.

  Anmerkung: Wenn das Wechseln in den System-Monitor unterbunden ist und Sie das Passwort vergessen, haben Sie dauerhaft keinen Zugriff auf das Gerät. Um das Gerät wieder entsperren zu lassen, wenden Sie sich an Ihren Vertriebspartner.

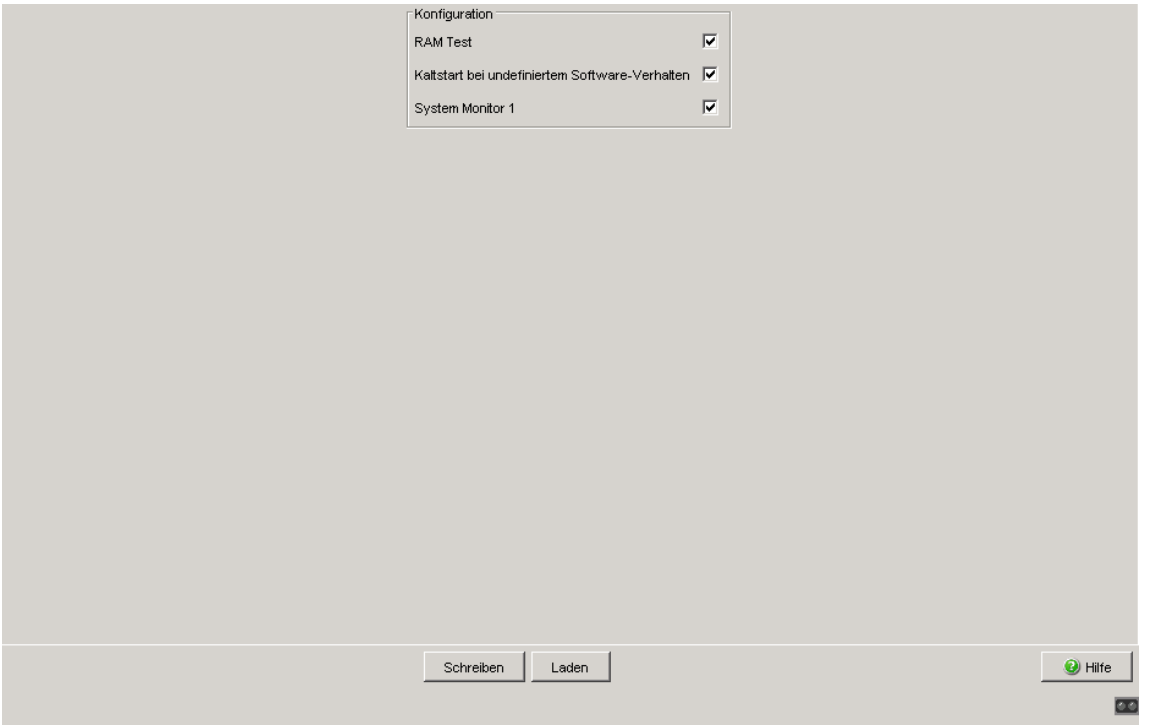


Abb. 101: Dialog Selbsttest

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 235: Schaltflächen

9 Erweitert

Das Menü enthält Dialoge, Anzeigen und Tabellen zu:

- DHCP-Relay-Agent
- DHCP-Server
- Industrieprotokolle
- Command Line Interface

9.1 DHCP-Relay-Agent

Dieses Menü bietet Ihnen die Möglichkeit, den DHCP-Relay-Agenten zu konfigurieren.

Der DHCP-Relay-Agent leitet die DHCP-Anfragen angeschlossener Endgeräte an einen DHCP-Server weiter. Die Weiterleitung an einen bestimmten DHCP-Server geschieht abhängig davon, auf welchem Port oder Interface das Gerät die DHCP-Anfrage empfängt. Die erforderlichen Einstellungen dafür legen Sie im Dialog `Erweitert:DHCP-Relay-Agent:Server` fest. Dort haben Sie die Möglichkeit, bis zu 16 DHCP-Server festzulegen.

9.1.1 Global

Dieser Dialog ermöglicht Ihnen, den DHCP-Relay-Agenten zu konfigurieren.

- Die Tabellenspalte „Circuit-ID“ zeigt Ihnen den Wert an, den Sie bei der Konfiguration Ihres DHCP-Servers eintragen. Die „Circuit-ID“ enthält neben der Portnummer auch die ID des VLANs, aus dem das DHCP-Relay die DHCP-Anfrage empfangen hat.

  Anmerkung: Die VLAN-ID befindet sich im 4. und 5. Oktett der Circuit-ID. Die angezeigte Circuit-ID gilt für ungetaggte Frames. Empfängt das DHCP-Relay einen VLAN-getaggten Frame, kann die Circuit-ID, die das Gerät tatsächlich an den DHCP-Server sendet, von der angezeigten abweichen.

Das Kapitel „Netz“ beinhaltet weitere Informationen über VLAN 0.

Beispiel für die Konfiguration Ihres DHCP-Servers:
Typ: `mac`
Remote–ID-Eintrag für DHCP-Server: `00 06 00 80 63 00 06 1E`
Circuit-ID:B3 06 00 00 01 00 01 01

Hieraus resultiert der Eintrag für die „Hardwareadresse“ im DHCP-Server:
`B3060000010001010006008063000061E`

☐ Die Spalte „DHCP-Relay ein“ aktiviert das Relay über den Port. Clienten, die an einen aktivierten Port angeschlossen sind, kommunizieren direkt mit dem DHCP-Server.

☐ Die Spalte „DHCP-Relay Status“ zeigt an, ob Relay über den Port ein- oder ausgeschaltet ist.

☐ Die Tabellenspalte „Option 82 ein“ bietet Ihnen die Möglichkeit, diese Funktion pro Port ein-/auszuschalten.

☐ In der Spalte „Hirschmann-Gerät“ kreuzen Sie die Ports an, an denen ein Gerät von Hirschmann angeschlossen ist.

Anmerkung: Die DHCP-Relay-Funktion benötigt mindestens 2 Ports. Verbinden Sie einen Port mit dem DHCP-Clienten und einen Port mit dem DHCP-Server. Aktivieren Sie die DHCP-Relay-Funktion sowohl global als auch über die Relay-Ports. Die DHCP-Server-Funktion ist höher priorisiert als die von DHCP-Relay. Schalten Sie deshalb den DHCP-Server für die Client- und Server-Ports ab.

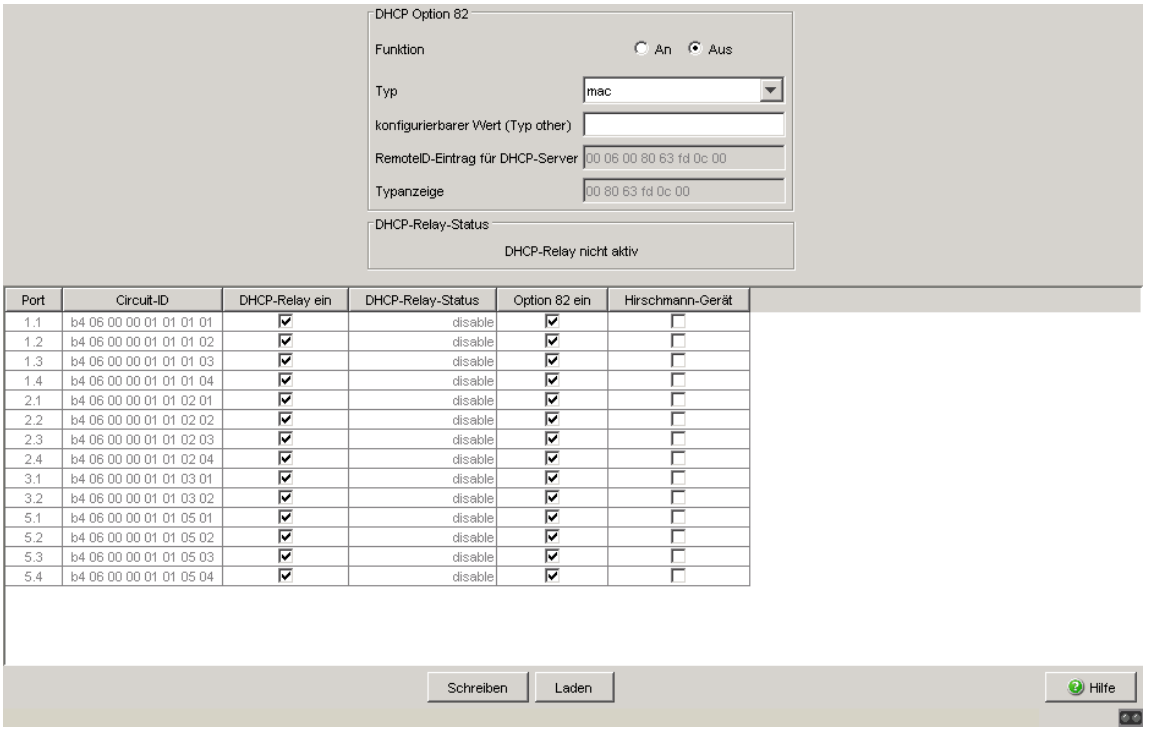


Abb. 102: Dialog DHCP-Relay-Agent

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 236: Schaltflächen

9.1.2 Server

Dieser Dialog bietet Ihnen die Möglichkeit, bis zu 16 DHCP-Server festzulegen, an die der DHCP-Relay-Agent die DHCP-Anfragen weiterleitet.
Das Gerät leitet entweder jede DHCP-Anfrage an einen Server weiter oder ausschließlich Anfragen, die es auf einem bestimmten Port oder Interface empfängt.

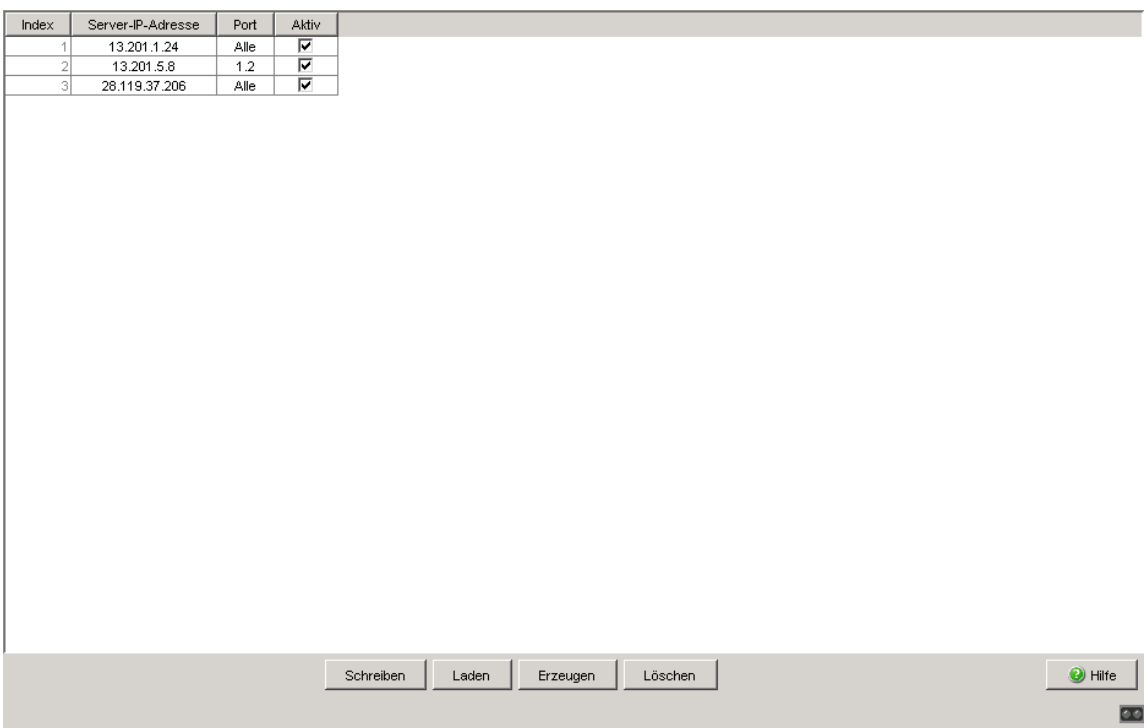


Abb. 103: Dialog `Erweitert:DHCP-Relay-Agent:Port`

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Zeigt eine fortlaufende Nummer, auf die sich der Tabelleneintrag bezieht. Das Gerät legt diese Nummer automatisch fest.	`1..16`	–
Server-IP-Adresse	Legt die IP-Adresse des DHCP-Servers fest.	Gültige IPv4-Adresse	`0.0.0.0`

Tab. 237: Rahmen „DHCP-Server Mode“ im Dialog `Erweitert:DHCP-Server:Global`

Parameter	Bedeutung	Wertebereich	Voreinstellung
Port	Legt fest, ob das Gerät jede DHCP-Anfrage an den Server weiterleitet oder ausschließlich Anfragen, die es auf einem Port oder Interface empfängt.	`Alle` <Portnummer>	`Alle`
Aktiv	Aktiviert/deaktiviert die Weiterleitung von DHCP-Anfragen an diesen DHCP-Server.	`aktiviert` `deaktiviert`	`deaktiviert`

Tab. 237: Rahmen „DHCP-Server Mode“ im Dialog `Erweitert:DHCP-Server:Global`

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 238: Schaltflächen

9.2 DHCP-Server

Die DHCP-Server-Dialoge bieten Ihnen die Möglichkeit, einfach Geräte (Clients) neu in Ihr Netz einzubinden oder in Ihrem Netz auszutauschen: Durch die Wahl von DHCP als Konfigurationsmodus beim Client holt sich dieser die Konfigurationsdaten von dem DHCP-Server.

Der DHCP-Server vergibt an den Client:

– eine fest eingestellte IP-Adresse (statisch) oder eine Adresse aus einem Adressbereich (dynamisch),
– die Netzmaske,
– die Gateway-Adresse,
– die DNS-Server-Adresse,
– die WINS-Server-Adresse und
– die Lease-Zeit.

Zusätzlich können Sie global oder pro Port einen URL zur Übertragung von weiteren Konfigurationsparametern auf den Client angeben.

9.2.1 Global

Dieser Dialog bietet Ihnen die Möglichkeit, den DHCP-Server des Gerätes global und pro Port ein- oder auszuschalten.

Parameter	Bedeutung	Wertebereich	Voreinstellung
DHCP-Server-Modus	Globales Ein-/Ausschalten des DCHP-Servers auf dem Gerät.	`An`, `Aus`	`Aus`

Tab. 239: Rahmen „DHCP-Server Mode“ im Dialog `Erweitert:DHCP-Server:Global`

Parameter	Bedeutung	Wertebereich	Voreinstellung
IP-Überprüfung	Aktivert/deaktiviert die Überprüfung von einzigartigen IP-Adressen. Die Server prüfen beim Vergeben einer neuen Adresse, ob die gewählte Netzwerkadresse einmalig im Netzwerk ist. Der Server verifiziert die angebotene Adresse beispielsweise mit einem ICMP-Echo-Request.	`An`, `Aus`	`An`

Tab. 240: Rahmen „Konfiguration“ im Dialog `Erweitert:DHCP-Server:Global`

Parameter	Bedeutung	Wertebereich	Voreinstellung
Port	Modul- und Port-Nummer, für die dieser Eintrag gilt.	-	-
DHCP-Server aktiv	Ein-/Ausschalten des DHCP-Servers an diesem Port. Um den DHCP-Server an einem Port zu aktivieren, schalten Sie außerdem den DHCP-Server-Modus global ein.	`An`, `Aus`	`An`

Tab. 241: Tabelle im Dialog `Erweitert:DHCP-Server:Global`

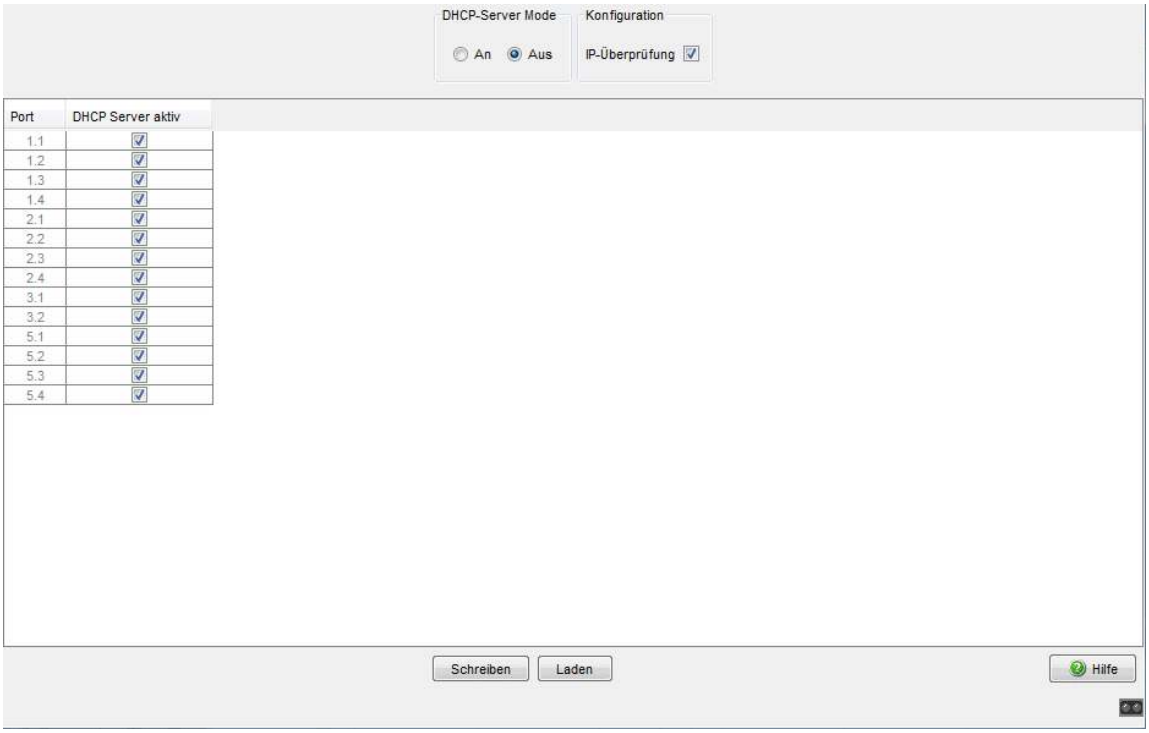


Abb. 104: Dialog DHCP-Server Global

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 242: Schaltflächen

9.2.2 Pool

Dieser Dialog bietet Ihnen die Möglichkeit, die Vergabe von IP-Adressen detailliert zu steuern. Sie können den DHCP-Server pro Port oder pro VLAN ein- bzw. ausschalten. Der DHCP-Server bietet dazu einen sogenannten IP-Adress-Pool (kurz „Pool“), aus dem er IP-Adressen an Clients vergibt. Der Pool besteht aus einer Liste von Einträgen. Ein Eintrag kann eine bestimmte IP-Adresse oder einen zusammenhängenden IP-Adressbereich definieren. Sie haben die Wahl zwischen einer dynamischen und einer statischen Vergabe.

- Ein Eintrag für die dynamische Vergabe gilt für alle Ports des Geräts, für die Sie den DHCP-Server aktivieren. Meldet sich ein Client an einem Port, dann weist der DHCP-Server eine noch freie IP-Adresse aus einem Pool-Eintrag für diesen Port zu.
  Für eine dynamische Zuteilung erstellen Sie einen Pool-Eintrag für alle Ports und tragen die 1. und die letzte IP-Adresse des IP-Adressbereichs ein. Lassen Sie die Felder MAC-Adresse, Client-ID, Remote-ID und Circuit-ID frei.
  Sie haben die Möglichkeit, mehrere Pool-Einträge zu erzeugen. Damit können Sie z.B. IP-Adressbereiche realisieren, die Lücken enthalten.
- Bei einer statischen Vergabe weist der DHCP-Server stets die selbe IP-Adresse an einen Client zu. Der DHCP-Server identifiziert den Client über eine eindeutige Hardware-ID.
  Ein statischer Adress-Eintrag kann ausschließlich 1 IP-Adresse enthalten und kann für alle Ports oder für einen bestimmten Port des Gerätes gelten.
  Für eine statische Zuteilung erstellen Sie einen Pool-Eintrag für alle Ports oder einen bestimmten Port, tragen die IP-Adresse ein und lassen das Feld „Letzte IP-Adresse“ frei. Geben Sie eine Hardware-ID an, mit der der DHCP-Server den Client eindeutig identifiziert. Diese ID kann eine MAC-Adresse, eine Client-ID, eine Remote-ID oder eine Circuit-ID sein. Meldet sich ein Client mit einer bekannten Hardware-ID, dann weist der DHCP-Server die statische IP-Adresse zu.

Die Tabelle zeigt Ihnen die konfigurierten Einträge des DHCP-Server-Pools an. Sie haben die Möglichkeit, einen Eintrag neu zu erzeugen, einen bestehenden Eintrag zu editieren oder Einträge zu löschen.
Sie haben die Möglichkeit, bis zu 128 Pool-Einträge zu erzeugen.

Um einen neuen Eintrag zu erzeugen, klicken Sie auf „Erzeugen“. Füllen Sie die Felder aus, die Sie benötigen und klicken Sie anschließend auf „Schreiben“.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Index	Zeigt eine fortlaufende Nummer, auf die sich der Tabelleneintrag bezieht. Das Gerät legt diese Nummer automatisch fest.	0, 1, 2, ...	
Aktiv	Aktiviert oder deaktiviert den Pool-Eintrag.	`An`, `Aus`	`Aus`
IP-Adresse	▶ Für einen dynamischen Adress-Eintrag: Die 1. Adresse des IP-Adress-Pools, die der DHCP-Server an einen Client vergibt. ▶ Für einen statischen Adress-Eintrag: Die IP-Adresse, die der Server stets an den selben Client vergibt.	Gültige IPv4-Adresse	-
Letzte IP-Adresse	Für einen dynamischen Adress-Eintrag: Die letzte Adresse des IP-Adress-Pools, die der DHCP-Server an einen Client vergibt.	Gültige IPv4-Adresse	-
Port	Modul- und Port-Nummer, für die dieser Eintrag gilt. ▶ Für einen dynamischen Adress-Eintrag wählen Sie `all`. ▶ Für einen statischen Adress-Eintrag wählen Sie all oder eine gültige Modul- und Port-Nr.	Gültige Modul- und Port-Nr. oder `all`.	`all`
VLAN	VLAN-Nummer, für die dieser Eintrag gilt. **Anmerkung:** Diese Spalte ist verfügbar für die Geräte MS, Octopus, RS, RSR, MACH102 und MACH1020/1030.	Gültige VLAN-Nr.	-
MAC-Adresse	Für einen statischen Adress-Eintrag: MAC-Adresse, mit der sich der Client identifiziert.	MAC-Adresse des Clients, der die statische IP-Adresse erhält	-
DHCP-Relay	IP-Adresse des DHCP-Relays, über das der Client seine Anfrage stellt. Empfängt der DHCP-Server eine Anfrage über ein anderes DHCP-Relay, ignoriert er diese. Befindet sich zwischen dem Client und dem DHCP-Server kein DHCP-Relay, lassen Sie dieses Feld leer.	IPv4-Adresse des DHCP-Relays.	-

Tab. 243: DHCP-Server-Pool-Einstellungen, IP-Adress-Grundeinstellungen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Client-ID	Für einen statischen Adress-Eintrag: Client-ID, mit der sich der Client identifiziert.	Client-ID des Clients, der die statische IP-Adresse erhält[a]	-
Remote-ID	Für einen statischen Adress-Eintrag: Remote-ID, mit der sich der Client identifiziert.	Remote-ID des Clients, der die statische IP-Adresse erhält[a]	-
Circuit-ID	Für einen statischen Adress-Eintrag: Circuit-ID, mit der sich der Client identifiziert.	Circuit-ID des Clients, der die statische IP-Adresse erhält[a]	-
Hirschmann-Gerät	Aktivieren Sie diese Einstellung, wenn das Gerät aus diesem Eintrag ausschließlich Geräte von Hirschmann bedient.	`An` `Aus`	`Aus`
Konfigurations-URL	TFTP-URL, von dem der Client weitere Konfigurationsinformationen beziehen soll. Geben Sie den URL an im Format tftp://servername-oder-ip-addresse/verzeichnis/datei.	Gültiger TFTP-URL	-
Lease-Time [s]	Zeit in s, für die der DHCP-Server die Adresse dem Client zuteilt. Innerhalb der Lease-Zeit kann der Client eine Verlängerung beantragen. Beantragt der Client keine Verlängerung, nimmt der DHCP-Server die IP-Adresse nach ihrem Ablaufen wieder in den Pool auf und teilt sie bei Bedarf einen beliebigen Client zu.	1 s - 4.294.967.295 s (2^{32}-1 s)	86.400 s (1 Tag)
Default-Gateway	Default-Gateway-Eintrag für den Client.	Gültige IPv4-Adresse	-
Netzmaske	Netzmasken-Eintrag für den Client.	Gültige IPv4-Netzmaske	-
WINS-Server	WINS- (Windows Internet Name Service-) Eintrag für den Client.	Gültige IPv4-Adresse	-
DNS-Server	DNS-Server-Eintrag für den Client.	Gültige IPv4-Adresse	-

Tab. 243: DHCP-Server-Pool-Einstellungen, IP-Adress-Grundeinstellungen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Hostname	Hostname für den Client. Ist dieser Name angegeben, überschreibt er den Systemnamen des Clients (siehe auf Seite 23 „Systemdaten“).	Max. 64 ASCII-Zeichen im Bereich 0x21 (!) - 0x7e (~).	- (Kein Hostname)
Vendor-specific	Beinhaltet herstellerspezifische Informationen, eingegeben als Hex-String in einem TLV-Format (Type Length Value). **Anmerkung:** Z. B. Herstellerspezifische Information, „f1 08 0a 7e 7e 02 0a 7f 7f 02“. Beschreibt einen spezifischen Typ des Herstellers f1 mit einer Feldlänge von 08. Die nächsten 8 Oktetten beinhalten die eigentlichen Händlerdaten. Falls vorhanden, behandelt das Gerät die nächsten 2 Oktetten als Typ- und Längenfelder. Geben Sie darum einen gültigen Hex-String ein, der die korrekten Längen-Werte beinhaltet.	Gültiger Hex-String.	-

Tab. 243: DHCP-Server-Pool-Einstellungen, IP-Adress-Grundeinstellungen

[a] Eine Client-, Remote- oder Circuit-ID besteht aus 1 - 255 Bytes in Hexadezimalschreibweise (00 - ff), durch Leerzeichen getrennt.

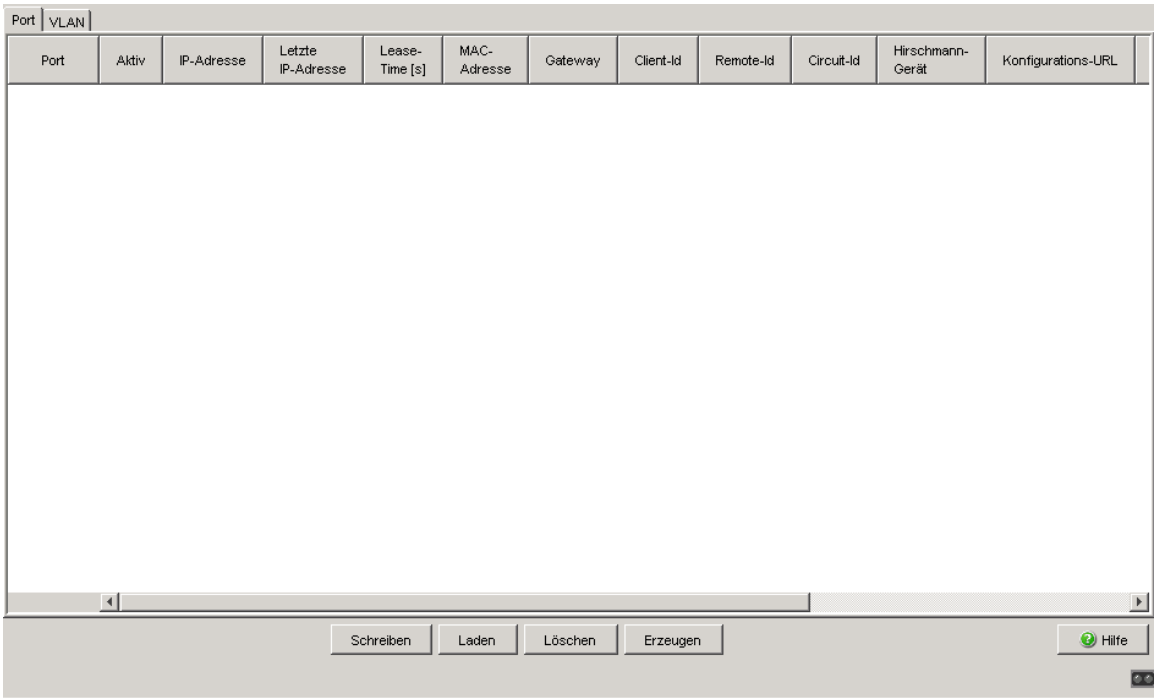


Abb. 105: Dialog DHCP-Server-Pool pro Port

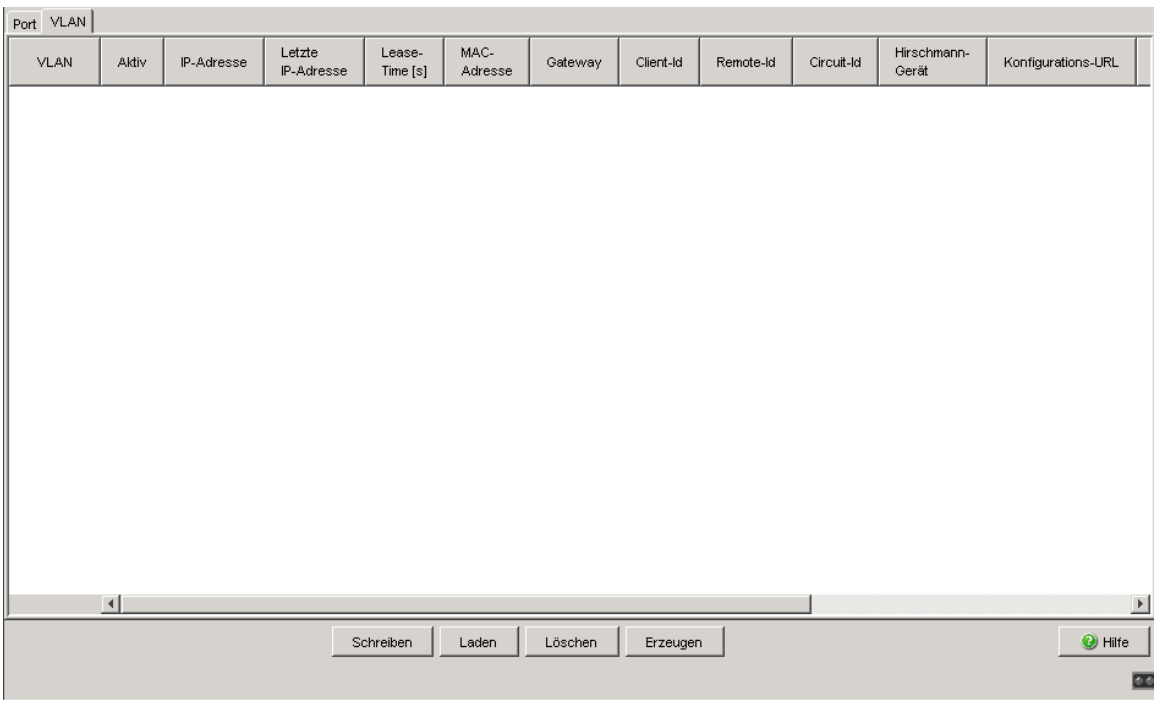


Abb. 106: Dialog DHCP-Server-Pool pro VLAN

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Erzeugen	Fügt einen neuen Tabelleneintrag hinzu.
Löschen	Entfernt den markierten Tabelleneintrag.
Hilfe	Öffnet die Online-Hilfe.

Tab. 244: Schaltflächen

9.2.3 Lease-Tabelle

Die Lease-Tabelle (engl. Lease: Vermietung) zeigt Ihnen die IP-Adressen an, die der DHCP-Server aktuell vergeben hat.
Zu jeder vergebenen IP-Adresse zeigt das Gerät die zugehörigen Details an.

Parameter	Bedeutung	Mögliche Werte
Port	Modul- und Port-Nummer, für die dieser Eintrag gilt.	-
IP-Adresse	IP-Adresse, die der DHCP-Server an das Gerät mit der angegebenen MAC-Adresse vergeben hat.	Eine IPv4-Adresse aus dem Pool.
Status	Zustand der DHCP-Adressvergabe gemäß dem Dynamic Host Configuration Protocol.	`bootp`, `offering`, `requesting`, `bound`, `renewing`, `rebinding`, `declined`, `released`
Remaining Lifetime	Verbleibende Zeit in Sekunden, bis die Gültigkeit der IP-Adresse abläuft, es sei denn, der Client beantragt eine Verlängerung.	-

Tab. 245: DHCP-Lease-Tabelle

Parameter	Bedeutung	Mögliche Werte
Vergeben an (MAC-Adresse)	MAC-Adresse des Clients, der die IP-Adresse aktuell geleast hat.	Format xx:xx:xx:xx:xx
DHCP-Relay	IP-Adresse des DHCP-Relay, über das der Client die Anfrage gestellt hat.	IPv4-Adresse oder leer
Lokale ID	Die Client-ID, die der Client bei der DHCP-Anfrage angegeben hat.	[a]
Entfernte ID	Die Remote-ID, die der Client bei der DHCP-Anfrage angegeben hat.	[a]
Circuit ID	Die Circuit-ID, die der Client bei der DHCP-Anfrage angegeben hat.	[a]

Tab. 245: DHCP-Lease-Tabelle

– [a] Eine Client-, Remote- oder Circuit-ID besteht aus 1 - 255 Bytes in Hexadezimalschreibweise (00 - ff), durch Leerzeichen getrennt.

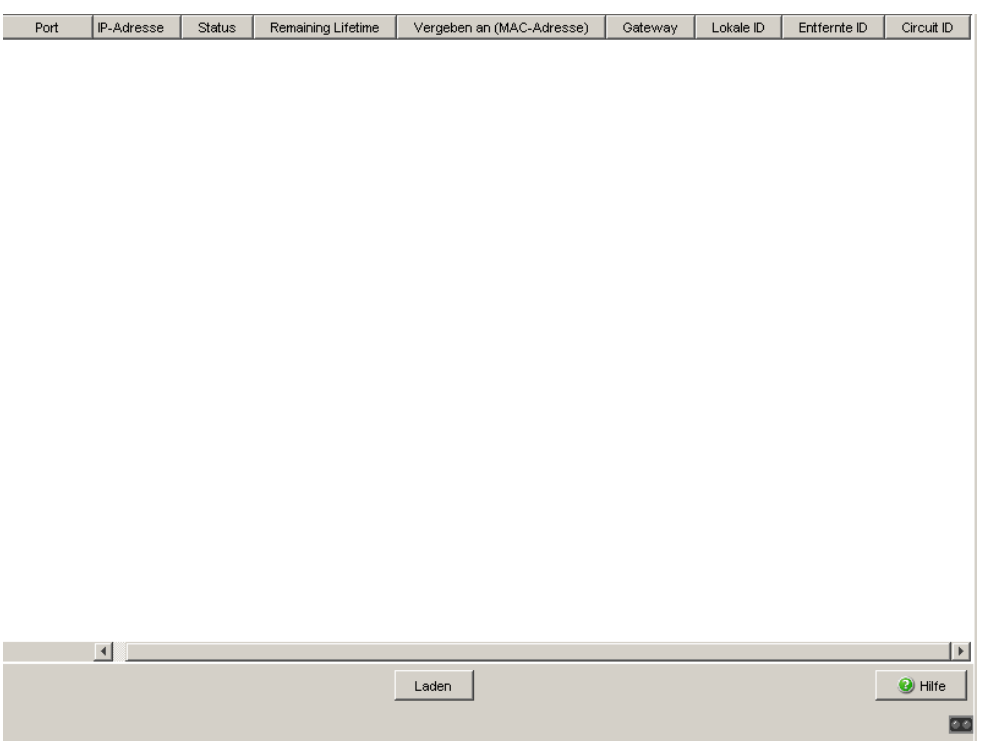


Abb. 107: Dialog DHCP-Server-Lease-Tabelle

Schaltflächen

Schaltfläche	Bedeutung
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 246: Schaltflächen

9.3 Industrieprotokolle

Das Industrieprotokolle-Menü bietet Ihnen die Möglichkeit,
- das Protokoll PROFINET IO zu konfigurieren, sowie
- das Protokoll EtherNet/IP zu konfigurieren.

Detaillierte Angaben zu den Industrieprotokollen und zur Konfiguration der SPS finden Sie im Anwender-Handbuch „Industrie-Protokolle“.

9.3.1 PROFINET IO

Dieser Dialog bietet Ihnen die Möglichkeit, das Protokoll PROFINET IO zu konfigurieren. Zur Integration in ein Steuerungssystem führen Sie die folgenden Schritte durch.

Allgemeine Einstellungen:

☐ Prüfen Sie im Dialog `Grundeinstellungen:System`, ob im Feld „Name“ ein gültiger Systemname für das Gerät festgelegt ist.
Der Systemname darf ausschließlich alphanumerische Zeichen, Bindestriche und Punkte enthalten.

☐ Prüfen Sie im Dialog `Grundeinstellungen:Netz`, ob im Rahmen „Modus“ `Lokal` ausgewählt ist (siehe auf Seite 29 „Netz“).

☐ Prüfen Sie im Dialog `Switching:VLAN:Global`, ob „VLAN 0-Transparent-Modus“ markiert ist (siehe auf Seite 187 „VLAN Global“).

Anmerkung: Schließen Sie eine Kombination des VLAN 0-Transparent-Modus mit dem Einsatz von MSTP (Multiple Spanning Tree) oder Routing aus.

☐ Konfigurieren Sie die Alarmeinstellungen und die Schwellwerte für die Alarme, die Sie überwachen wollen (siehe auf Seite 374 „Gerätestatus“).

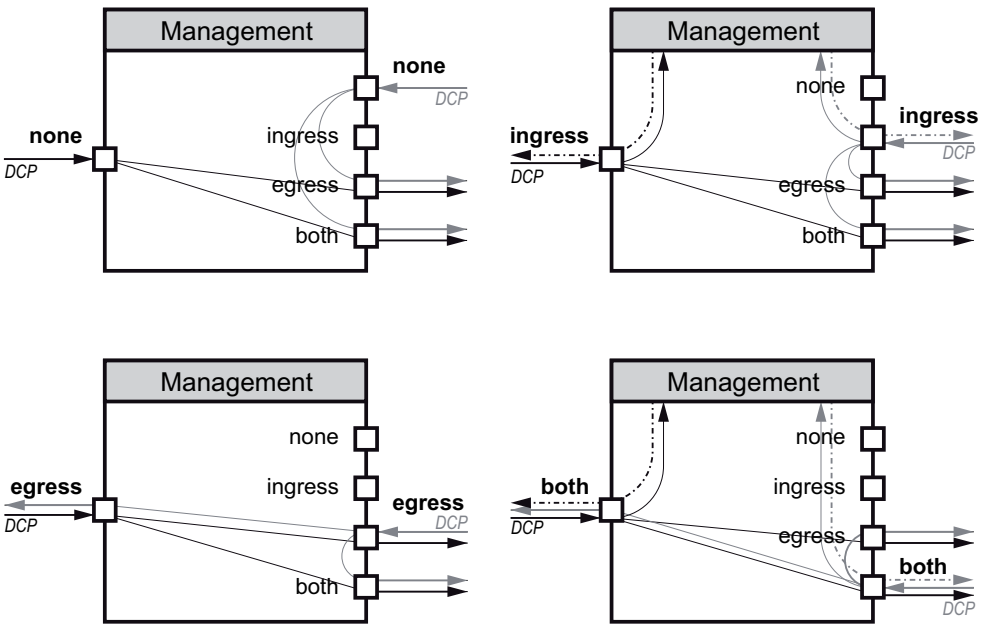
Globale PROFINET IO-Einstellungen:

☐ Schalten Sie PROFINET IO im Rahmen „Funktion“ ein.

☐ Laden Sie durch Klicken auf „Download GSDML File“ die GSDML-Datei auf Ihren PC.

PROFINET IO-Port-Einstellungen:

☐ Legen Sie für jeden Port in der Spalte `DCP Mode` die gewünschte Einstellung fest. DCP-Pakete sind Multicasts, Antworten des Managements sind Unicasts. In jeder der Einstellungen vermittelt das Gerät empfangene DCP-Frames an Ports mit der Einstellung `egress` und `both`.



- `none`:
  Keine Antwort des Managements auf empfangene DCP-Frames.
  Port sendet keine DCP-Frames.
- `ingress`:
  Der Agent antwortet auf DCP-Frames.
  Port sendet keine DCP-Frames.
- `egress`:
  Keine Antwort des Managements auf empfangene DCP-Frames.
  Port sendet DCP-Frames.
- `both`:
  Der Agent antwortet auf DCP-Frames.
  Port sendet DCP-Frames.

Die Voreinstellung ist `both`.

Anmerkung: Wenn Sie 2 Switches verbinden, die in getrennten DCP-Domänen liegen sollen, schalten Sie auf **beiden** Switches den DCP-Modus der beteiligten Ports auf `none` oder auf `ingress`. So erreichen Sie, dass keiner der Switches DCP-Frames an das andere Gerät sendet.

☐ Wählen Sie den Port, für dessen PHY-Baustein Sie den schnellen Start-Modus einstellen möchten, und wählen Sie in der Spalte `Fast Start Up`:
- `disable`, um den normalen Start-Modus einzustellen,
- `enable`, um den schnellen Start-Modus einzustellen.

Anmerkung: Die Einstellung `enable` wirkt sich nur aus, wenn die automatische Konfiguration des Ports (Autoneg) abgeschaltet ist (siehe auf Seite).

Die Voreinstellung ist `disable`. Unterstützt ein Port den schnellen Start-Modus nicht, zeigt das Gerät in dieser Spalte `unsupported` an.

Einstellungen für die SPS:

☐ Konfigurieren Sie die SPS wie im Anwender-Handbuch „Industrie-Protokolle“ beschrieben.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 247: Schaltflächen

9.3.2 EtherNet/IP

Dieser Dialog bietet Ihnen die Möglichkeit, das Protokoll EtherNet/IP zu aktivieren. Zur Integration in ein Steuerungssystem führen Sie die folgenden Schritte durch.

Allgemeine Einstellungen:

☐ Prüfen Sie im Dialog `Switching:Multicast:IGMP`, ob IGMP eingeschaltet ist (siehe auf Seite 176 „IGMP (Internet Group Management Protocol)“).

EtherNet/IP-Einstellungen:

☐ Schalten Sie EtherNet/IP im Rahmen „Funktion“ ein (Voreinstellung: aus).

☐ Laden Sie durch Klicken auf „Download EDS File...“ die EDS-Datei auf Ihren PC.

Einstellungen für die SPS:

☐ Konfigurieren Sie die SPS wie im Anwender-Handbuch „Industrie-Protokolle“ beschrieben.

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 248: Schaltflächen

9.3.3 IEC61850 MMS Protokoll (RSR, MACH 1000)

Das IEC61850 ist ein von der International Electrotechnical Commission (IEC) standardisiertes Protokoll für die industrielle Kommunikation. So nutzen z. B. automatische Netzumschalter dieses Protokoll, um mit der Infrastruktur eines Kraftwerks kommunizieren.

Das paketorientierte Protokoll definiert eine einheitliche Kommunikationssprache auf Basis des Transportprotokolls TCP/IP. Für die Client-Server-Kommunikation nutzt das Protokoll einen MMS-Server (Manufacturing Message Specification). Das Protokoll beherbergt Funktionen für SCADA (Supervisory Control and Data Acquisition), IED (Intelligent Electronic Device) und andere Netzwerk-Kontrollsysteme.

Dieser Dialog bietet Ihnen die Möglichkeit, folgende MMS-Server-Funktionen konfigurieren:
- Aktivieren/deaktivieren des MMS-Servers
- Aktivieren/deaktivieren des Schreibzugriffs auf den MMS-Server

Parameter	Bedeutung	Wertebereich	Voreinstellung
Funktion	Aktivieren/deaktivieren des MMS-Servers.	An, Aus	Aus

Tab. 249: Rahmen „Funktion“ im Dialog `Erweitert:Industrie-Protokolle:IEC61850`

Parameter	Bedeutung	Wertebereich	Voreinstellung
Schreibzugriff	Aktivieren/deaktivieren des Schreibzugriffs auf den MMS-Servers.	markiert, unmarkiert	unmarkiert
Technical Key	Legt den IED-Namen fest. Der IED-Name ist somit unabhängig vom System-Namen einstellbar.	a..z A..Z _ 0..9	KEY

Tab. 250: Rahmen „Konfiguration“ im Dialog `Erweitert:Industrie-Protokolle:IEC61850`

Parameter	Bedeutung	Wertebereich	Voreinstellung
Download ICD-Datei	Diese Schaltfläche kopiert die ICD-Datei auf Ihren PC.	-	-

Tab. 251: Rahmen „Download“ im Dialog `Erweitert:Industrie-Protokolle:IEC61850`

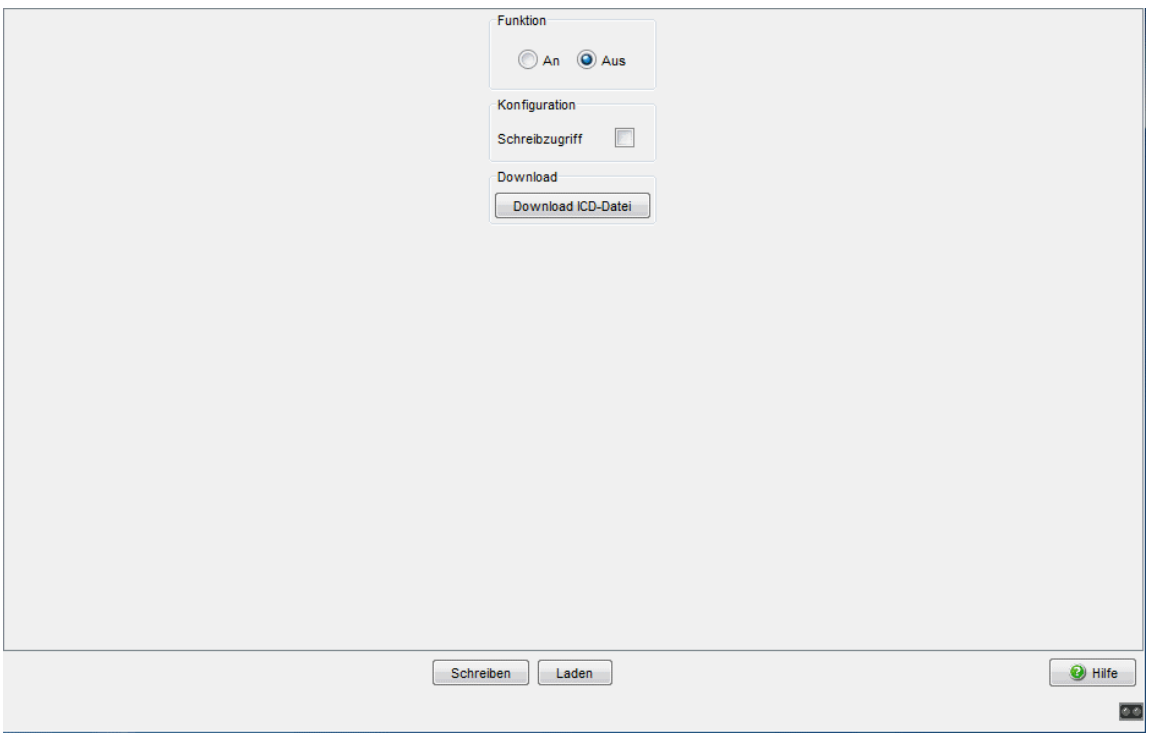


Abb. 108: Dialog `Erweitert:Industrie-Protokolle:IEC61850`

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern`, wählen den Speicherort für die Gerätekonfiguration und klicken auf „Sichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 252: Schaltflächen

9.3.4 Digital IO-Module

Das Digital I/O MICE-Medienmodul MM24-IOIOIOIO bietet Ihnen die Möglichkeit, Statusmeldungen auf einfache Weise von einer Stelle Ihres Netzes zu einer anderen Stelle übertragen. Diese Module montieren Sie auf (Power)MICE-Grundgeräten an der gewünschten Stelle in Ihrem Netz.

Die 4 digitalen Eingänge des Digital I/O MICE-Medienmoduls bieten Ihnen die Möglichkeit, digitale Sensorsignale zu erfassen und weiterzuleiten.
Die 4 digitalen Ausgänge des Digital I/O MICE-Medienmoduls bieten Ihnen die Möglichkeit, Aktoren zu schalten.

Die 24 VDC-Ausgangsspannung des Digital I/O MICE-Medienmoduls bietet Ihnen die Möglichkeit, beispielsweise Aktoren oder Kontrollleuchten zu betreiben.

Die Software unterstützt die logische Funktion 1 auf n. Sie können einen digitalen Eingang (Input) eines Digital I/O MICE-Medienmoduls abfragen und damit praktisch beliebig viele (n) Ausgänge setzen. Diese Ausgänge können sich an folgenden Stellen befinden:

- auf dem selben Digital I/O MICE-Medienmodul auf dem selben (Power)MICE-Grundgerät,
- auf einem anderen Digital I/O MICE-Medienmodul auf dem selben (Power)MICE-Grundgerät,
- auf einem Digital I/O MICE-Medienmodul auf einem anderen (Power)MICE-Grundgerät.

In der „Beschreibung und Betriebsanleitung Industrial ETHERNET Digital I/O MICE-MedienmodulDigital I/O MICE-MedienmodulDigital I/O MICE-Medienmodul MM24-IOIOIOIO“ finden Sie:

- Sicherheitshinweise
- eine Gerätebeschreibung
- Informationen zur Belegung der Anschlussklemmen des Digital I/O MICE-Medienmoduls
- eine Beschreibung der Anzeigeelemente
- und weitere Informationen, die Sie zur Installation des Gerätes benötigen, bevor Sie mit der Konfiguration des Gerätes beginnen

Das Menü „Digital IO-Module“ enthält die Dialoge, Anzeigen und Tabellen zur Konfiguration von Digital I/O MICE-Medienmodulen:

- IO-Input
  - Funktion (An-/Ausschalten)
  - Konfiguration (Aktualisierungsintervall konfigurieren)
  - Input-ID und Wert anzeigen
  - Log Event und SNMP-Trap konfigurieren
- IO-Output
  - Funktion (An-/Ausschalten)
  - Konfiguration (Aktualisierungsintervall und Anzahl der Wiederholungsversuche konfigurieren)
  - Output ID und Wert anzeigen
  - Source-IP-Adresse, Input-ID, Log Event und SNMP-Trap konfigurieren

IO-Input

Dieses Menü bietet Ihnen die Möglichkeit, die 4 digitalen Eingänge (Inputs) eines Digital I/O MICE-Medienmoduls MM24-IOIOIOIO zu konfigurieren.

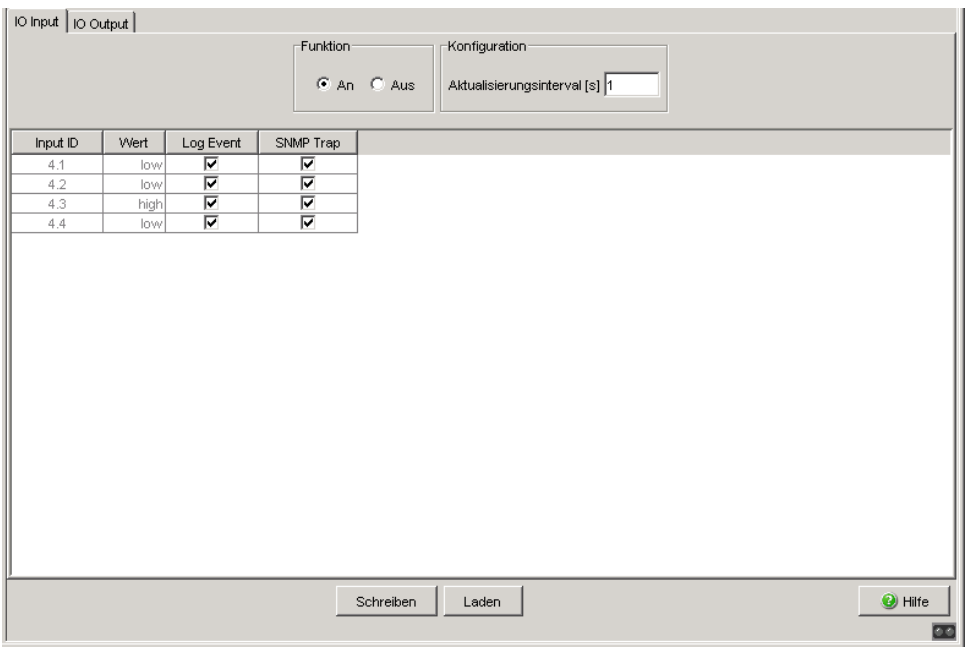


Abb. 109: Dialog IO Input

Funktion

Parameter	Bedeutung	Wertebereich	Voreinstellung
Funktion	Schaltet das zyklische Abfragen der digitalen Eingänge (IO Input) an oder aus.	`An`, Aus	`Aus`

Tab. 253: IO-Input - Funktion

Konfiguration

Parameter	Bedeutung	Wertebereich	Voreinstellung
Aktualisierungsintervall [s]	Das Intervall für die Aktualisierung des IO-Input-Status konfigurieren. Mit dieser Angabe legen Sie fest, in welchen Zeitabständen das Gerät die Werte der digitalen Eingänge des Digital I/O MICE-Medienmodul abfragt.	1 - 10 Sekunden	1 Sekunde

Tab. 254: IO-Input - Konfiguration

IO Input

In der Tabelle „IO Input“ bietet Ihnen die Möglichkeit,

- Input ID und zugehörigen Wert anzuzeigen.
- Log Event und SNMP Trap für diesen Eintrag zu konfigurieren.

Nachdem Sie die digitalen Eingänge des Digital I/O MICE-Medienmoduls konfiguriert haben, listet der Dialog die Werte der konfigurierten digitalen Eingänge auf.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Input ID	Steckplatznummer des Digital I/O MICE-Medienmoduls (x) und Nummer des digitalen Eingangs (i), für den dieser Eintrag gilt. Notation: x.i	x = 1 - 7 i = 1 - 4	-
Wert	Pegel des digitalen Inputs. – `low`: Zustand „0“, Eingangsspannung am digitalen Input 0 V – `high`: Zustand „1“, Eingangsspannung am digitalen Input +24 VDC – `not-available`: Zustand „undefiniert“. Eingangsspannung am digitalen Input entspricht weder dem high- noch dem low-Pegel. Mögliche Ursache: Das zyklische Abfragen der digitalen Eingänge ist ausgeschaltet.	low, high, not-available	not-available

Tab. 255: IO Input-Tabelle

Parameter	Bedeutung	Wertebereich	Voreinstellung
Log Event	Aktiviert/deaktiviert die Logging-Funktion für Input-Statusänderungen. – `An`: Das Gerät prüft den Status der digitalen Eingänge des Digital I/O MICE-Medienmoduls in regelmäßigen Zeitabständen gemäß Ihrer Einstellung im Eingabefeld „Aktualisierungsinterval [s]“. Wenn das Gerät eine Änderung bei einem dieser IO-Input Werte erkennt, schreibt es einen Eintrag in seinen Ereignis-Log. Der Dialog `Diagnose:Bericht:EventLog` zeigt diese Einträge an. – `Aus`: Das Gerät schreibt bei einer Input-Statusänderung keinen Eintrag in seinen Ereignis-Log.	`An`, `Aus`	`Aus`
SNMP Trap	Aktiviert oder deaktiviert das Senden von SNMP-Traps bei Input-Statusänderungen. – An: Das Gerät prüft den Status der digitalen Eingänge des Digital I/O MICE-Medienmoduls in regelmäßigen Zeitabständen gemäß Ihrer Einstellung im Eingabefeld „Aktualisierungsinterval [s]“. Wenn das Gerät eine Änderung bei einem dieser IO-Input Werte erkennt, sendet es einen SNMP-Trap. Der Dialog Diagnose:Trap-Log zeigt diese Traps an. – Aus: Das Gerät sendet bei einer Input-Statusänderung keinen SNMP-Trap.	`An`, `Aus`	`Aus`

Tab. 255: IO Input-Tabelle

IO-Output

Dieses Menü bietet Ihnen die Möglichkeit, die 4 digitalen Ausgänge (Outputs) eines Digital I/O MICE-Medienmoduls MM24-IOIOIOIO auf den Wert „High“ (Relais Position 1) oder „Low“ (Relais Position 2) zu setzen (siehe Tabelle 258).

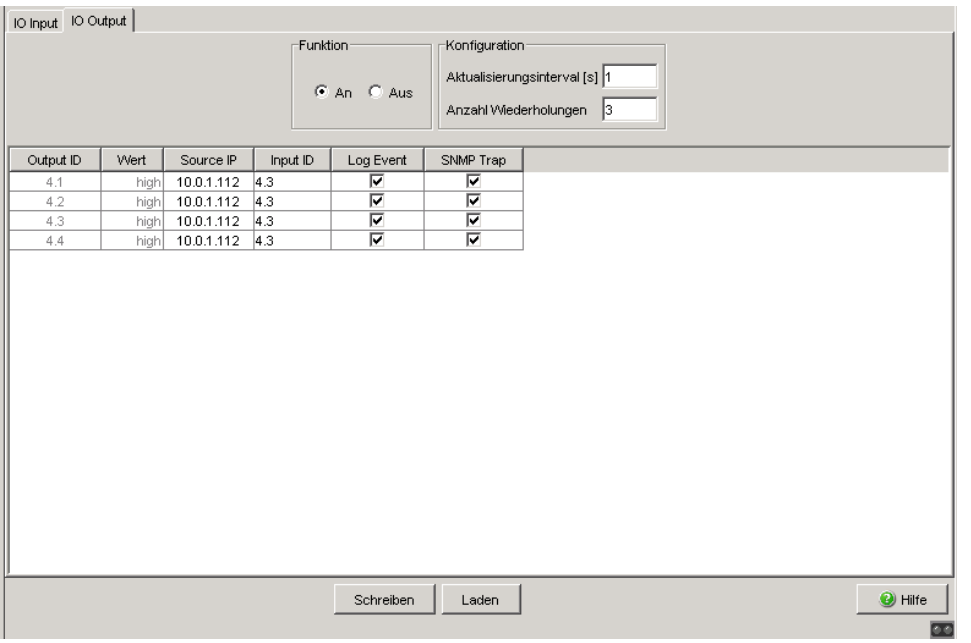


Abb. 110: Dialog IO Output

Funktion

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Funktion	Schaltet das zyklische Setzen der digitalen Ausgänge (IO Output) an oder aus.	`An` `Aus`	`Aus`

Tab. 256: IO-Output - Funktion

Konfiguration

Anmerkung: Wenn das Gerät nach der Anzahl der konfigurierten Wiederholungsversuche keine Antwort auf seine Anfragen bekommt, setzt es den digitalen Ausgang auf den Default-Wert (low). Dies gilt für alle digitalen Ausgänge, für die Sie eine Eingangsüberwachung konfiguriert haben.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Aktualisierungs-intervall [s]	Das Intervall für die Aktualisierung des IO-Output-Status konfigurieren. Mit dieser Angabe legen Sie fest, in welchen Zeitabständen das Gerät die Werte der digitalen Ausgänge des Digital I/O MICE-Medienmoduls setzt.	1 - 10 Sekunden	1 Sekunde
Anzahl Wiederholungen	Die Anzahl der Wiederholungsversuche angeben, die das Gerät unternimmt, um die digitalen Ausgänge des Digital I/O MICE-Medienmoduls zu setzen.	1 - 10	3

Tab. 257: IO-Output - Konfiguration

IO Output

In der Tabelle „IO Output“ bietet Ihnen die Möglichkeit,

- Output ID und zugehörigen Wert anzuzeigen.
- Source-IP-Adresse, Input-ID, Log Event und SNMP-Trap für diesen Eintrag zu konfigurieren.

☐ Geben Sie im Feld „Source IP“ die IP-Adresse des (Power)MICE-Gerätes ein, auf dem Sie das Digital I/O MICE-Medienmodul montiert haben, dessen digitale Eingänge Sie zum Setzen von digitalen Ausgängen verwenden wollen.

☐ Wählen Sie im Feld „Input ID“ die Steckplatznummer des Digital I/O MICE-Medienmoduls und die Nummer des digitalen Inputs aus, dessen Status Sie zum Setzen des digitalen Ausgangs verwenden wollen.

☐ Setzen Sie im Feld „Log Event“ durch Anklicken einen Haken, um im Gerät für diesen digitalen Ausgang die Funktion Ereignis-Logs zu aktivieren.

☐ Setzen Sie im Feld „SNMP Trap“ durch Anklicken einen Haken, um im Gerät für diesen digitalen Ausgang das Senden von SNMP Traps zu aktivieren.

☐ Klicken Sie auf „Schreiben“, um Ihre Einstellungen zu speichern.

☐ Klicken Sie auf „Laden“, um die aktuellen Werte an den digitalen Ausgängen des Gerätes in der Tabelle anzuzeigen.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Output ID	Steckplatznummer Digital I/O MICE-Medienmoduls (x) und Nummer des digitalen Outputs (o), für den dieser Eintrag gilt. Notation: x.o	x = 1 - 7 o = 1 - 4	-
Wert	Pegel des digitalen Outputs. – `low`: Zustand „0", Relais am digitalen Ausgang ist in Position 2 (Mittelkontakt ist mit Ruhekontakt verbunden). – `high`: Zustand „1", Relais am digitalen Ausgang ist in Position 1 (Mittelkontakt ist mit Arbeitskontakt verbunden). – `not-available`: Zustand „undefiniert". Spannung am digitalen Output entspricht weder dem high- noch dem low-Pegel. Mögliche Ursache: Das zyklische Setzen der digitalen Ausgänge ist ausgeschaltet.	`low`, `high`, `not-available`	`not-available`
Source IP	IP-Adresse des (Power)MICE-Gerätes mit einem Digital I/O MICE-Medienmodul, von dem Sie einen digitalen Eingang zum Setzen des digitalen Ausgangs auswerten wollen.	Gültige IPv4-Adresse	0.0.0.0
Input ID	Steckplatznummer des Digital I/O MICE-Medienmoduls (x) und Nummer des digitalen Inputs (i), den Sie zum Setzen des digitalen Ausgangs verwenden. Notation: x.i	x = 1 - 7 i = 1 - 4	1.1

Tab. 258: IO Output-Tabelle

Parameter	Bedeutung	Wertebereich	Voreinstellung
Log Event	Aktiviert/deaktiviert die Logging-Funktion für Output-Statusänderungen. – `An`: Das Gerät prüft den Status der digitalen Eingänge des Digital I/O MICE-Medienmoduls in regelmäßigen Zeitabständen gemäß der Einstellung im Eingabefeld „Aktualisierungsinterval [s]“. Wenn das Gerät eine Änderung bei einem dieser IO-Output Werte erkennt, schreibt es einen Eintrag in seinen Ereignis-Log. Der Dialog `Diagnose:Bericht:EventLog` zeigt diese Einträge an. – `Aus`: Das Gerät schreibt bei einer Ouput-Statusänderung keinen Eintrag in seinen Ereignis-Log.	`An`, `Aus`	`Aus`
SNMP Trap	Aktiviert oder deaktiviert das Senden von SNMP-Traps bei Output-Statusänderungen. – An: Das Gerät prüft den Status der digitalen Eingänge des Digital I/O MICE-Medienmoduls in regelmäßigen Zeitabständen gemäß der Einstellung im Eingabefeld „Aktualisierungsinterval [s]“. Wenn das Gerät eine Änderung bei einem dieser IO-Output Werte erkennt, sendet es einen SNMP-Trap. – Aus: Das Gerät sendet bei einer Ouput-Statusänderung keinen SNMP-Trap.	`An`, `Aus`	`Aus`

Tab. 258: IO Output-Tabelle

Anmerkung: Wenn das Gerät den digitalen Eingang des Digital I/O MICE-Medienmoduls nicht einlesen kann, schreibt es einen Eintrag in seien Ereignis-Log. Mögliche Ursache: Das Gerät ist nicht erreichbar oder die Konfiguration ist inkorrekt.

9.4 DIP-Switch via Software überschreiben (PowerMICE)

Dieser Dialog bietet Ihnen die Möglichkeit, die Einstellungen der DIP-Switches auf dem Gerät anzuzeigen. Bei Bedarf können Sie die Einstellungen der DIP-Switches deaktivieren oder mit Software-Einstellungen überschreiben.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Funktion	Aktiviert/deaktiviert die DIP-Switches auf dem Gerät. `An`: Das Gerät verwendet die mit den DIP-Switches festgelegten Einstellungen. Voraussetzung ist, dass „DIP-Switch An“ aktiv ist. `Aus`: Das Gerät ignoriert die Einstellungen der DIP-Switches.	`An`, `Aus`	`An`

Tab. 259: Rahmen „Funktion“ im Dialog `Erweitert:DIP-Switch`

Parameter	Bedeutung	Wertebereich	Voreinstellung
Konflikt mit Hardware-Einstellungen	Zeigt Konflikte zwischen den Einstellungen der DIP-Switches auf dem Gerät und den Software-Einstellungen. `Aktiv`: Konflikt zwischen den Einstellungen der DIP-Switches auf dem Gerät und den Software-Einstellungen. `Inaktiv`: Kein Konflikt.	Aktiv, inaktiv	-

Tab. 260: Rahmen „DIP-Switch Zustand“ im Dialog `Erweitert:DIP-Switch`

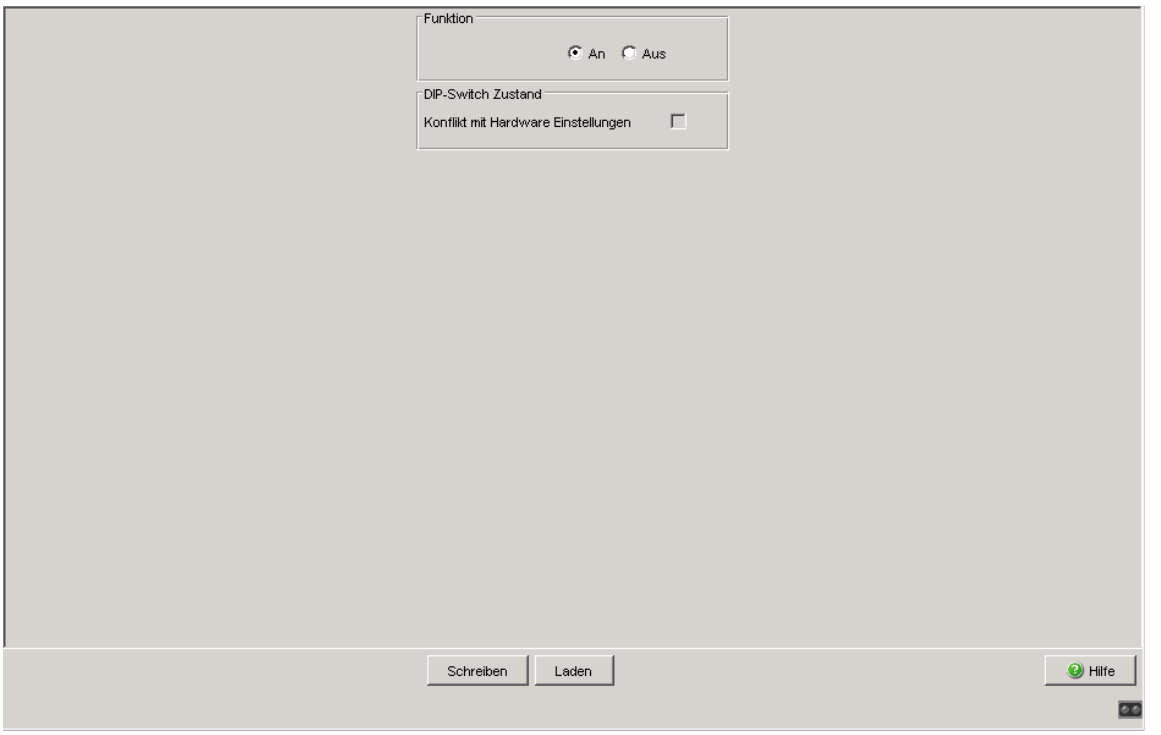


Abb. 111: Dialog `Erweitert:DIP-Switch`

Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (`RAM`) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog `Grundeinstellungen:Laden/Speichern` und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (`RAM`) des Gerätes gespeichert sind.
Hilfe	Öffnet die Online-Hilfe.

Tab. 261: Schaltflächen

9.5 Command Line

Dieses Fenster ermöglicht Ihnen, mit Hilfe des Web-Interfaces auf das Command Line Interface (CLI) zuzugreifen.

Detaillierte Angaben zum CLI finden Sie im Reference Manual „Command Line Interface“.

Schaltflächen

Schaltfläche	Bedeutung
Hilfe	Öffnet die Online-Hilfe.

Tab. 262: Schaltflächen

A Anhang

A.1 Technische Daten

Switching	
Größe MAC-Adresstabelle (inkl. statische Filter)	8.000 (16.000 bei PowerMICE und MACH 4000)
Max. Anzahl statisch konfigurierter MAC-Adressfilter	100
Max. Anzahl über GMRP/IGMP-Snooping lernbarer MAC-Adressfilter	1.000
Max. Länge überlanger Pakete	1.552 Bytes
Latenz, abhängig von der Port-Datenrate 10.000 Mbit/s 1.000 Mbit/s 100 Mbit/s 10 Mbit/s	 Layer 2: typ. 3,0 µs; Layer 3: typ. 3,0 µs Layer 2: typ. 3,5 µs; Layer 3: typ. 4,5 µs Layer 2: typ. 4,5 µs; Layer 3: typ. 5,5 µs Layer 2: typ. 19 µs; Layer 3: typ. 20 µs
Max. Anzahl statischer Adresseinträge	100 (im RM-Modus: 0 Unicast-Einträge)

VLAN	
VLAN-ID	1 bis 4.042
Anzahl VLANs	max. 256 gleichzeitig pro Gerät max. 256 gleichzeitig pro Port
Anzahl VLANs im GMRP in VLAN 1	max. 256 gleichzeitig pro Gerät max. 256 gleichzeitig pro Port

Access Control Lists (ACLs)	
Anzahl ACL-Einträge	100
Anzahl möglicher Regeln	1.000
Anzahl Regeln pro ACL-Eintrag	10
Anzahl Regeln pro Interface	100
Anzahl Switch-Queues	8
Einstellbare Port-Prioritäten	0-7

Router	
ARP-Einträge	bis zu 2.000
Routing-Einträge	bis zu 4.000 (1.500 bei MACH 4002-24G/48G)

Router	
Anzahl VLAN-Interfaces	bis zu 128
Statische Routen	256
Statische ARP-Einträge	64
Multicast-Routen	512
Anzahl Tracking-Objekte	256

A.2 Liste der RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 951	BOOTP
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1769	SNTP
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1907	Management Information Base for SNMP v2
RFC 1908	Coexistence between SNMP v1 and SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2271	SNMP Framework MIB
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped Boundaries
RFC 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Service
RFC 2570	Introduction to SNMP v3
RFC 2571	Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for SNMP
RFC 2573	SNMP v3 Applications
RFC 2574	User Based Security Model for SNMP v3
RFC 2575	View Based Access Control Model for SNMP
RFC 2576	Coexistence between SNMP v1, v2 & v3
RFC 2578	SMIv2

RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2865	RADIUS Client
RFC 3164	The BSD Syslog Protocol
RFC 3580	(802.1X RADIUS Usage Guidelines)
RFC 4188	(Definitions of Managed Objects for Bridges)

A.3 Zugrundeliegende IEEE-Normen

IEEE 802.1AB	Topology Discovery (LLDP)
IEEE 802.1af	Power over Ethernet
IEEE 802.1D-1998, IEEE 802.1D-2004	Media access control (MAC) bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
IEEE 802.1Q-1998	Virtual Bridged Local Area Networks (VLAN Tagging, Port Based VLANs, GVRP)
IEEE 802.1Q-2005	Spanning Tree (STP), Rapid Spanning Tree (RSTP), Multiple Spanning Tree (MSTP)
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3ad	Link Aggregation with Static LAG and LACP Support
IEEE 802.3af-2003	Power over Ethernet (PoE)
IEEE 802.3x	Flow Control

A.4 Zugrundeliegende IEC-Normen

IEC 62439	High availability automation networks; insbesondere: Kap. 5, MRP – Media Redundancy Protocol based on a ring topology

A.5 Zugrundeliegende ANSI-Normen

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

A.6 Literaturhinweise

- „TCP/IP Illustrated“, Vol. 1
  W.R. Stevens
  Addison Wesley 1994
  ISBN 0-201-63346-9
- Hirschmann Anwender-Handbuch „Installation“
- Hirschmann Anwender-Handbuch „Grundkonfiguration“
- Hirschmann Anwender-Handbuch „Redundanzkonfiguration“
- Hirschmann Anwender-Handbuch „Routing-Konfiguration“
- Hirschmann Referenz-Handbuch „Grafische Benutzeroberfläche (GUI)“
- Hirschmann Referenz-Handbuch „Command Line Interface“

A.7 Copyright integrierter Software

A.7.1 Bouncy Castle Crypto APIs (Java)

The Legion Of The Bouncy Castle
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle
(http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A.7.2 Broadcom Corporation

(c) Copyright 1999-2012 Broadcom Corporation. All Rights Reserved.

B Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, damit der Einsatz dieses Produkts problemlos erfolgen kann. Ihre Kommentare und Anregungen unterstützen uns, die Qualität und den Informationsgrad dieser Dokumentation noch zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	**gut**	**befriedigend**	**mäßig**	**schlecht**
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Leserkritik

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer +49 (0)7127 14-1600 oder
- per Post an

  Hirschmann Automation and Control GmbH
  Abteilung 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

C Stichwortverzeichnis

1
802.1D/p-Mapping 216
802.1X 98
802.1X-Authentifizierung (Voice-VLAN) 203

A
ACA (AutoConfiguration Adapter) 52, 384
Acceptable Frame Types 198
Access Control Lists (ACL) 129
Address Conflict Detection (ACD) 391
Address Resolution Protocol (ARP) 232
Administrative Distanz 247
AF 219
Aging Time 164
Alarm 383
Anforderungsintervall (SNTP) 136
ARP-Parameter 232
ARP-Statistik 234
ARP-Tabelle 234
Assured Forwarding 219
Authentifizierung 321
AutoConfiguration Adapter (ACA) 384
Auto-Summary 238

B
Bedienhinweise (GUI) 18
Bericht 386
BPDU-Guard 294
Broadcast-Limiter 174

C
Cable-Crossing 38
CLI 433
Class Selector 218
Command Line Interface 433
Count-to-Infinity 239

D
DHCP-Relay-Agent 400
DHCP-Server 405
DHCP-Server (Lease-Tabelle) 413
DHCP-Server-Pool 408
DIP-Schalter 261
Diagnose 331
DiffServ 207
Discovery 237
Distanzvektor 238
DSCP 207

E
EF 218
Eingeschränkter Management-Zugriff 85
Ein-Switch-Kopplung 284
Empfangsleistungs-Status 384
Ereignis-Log 336
Erweitert 399
EtherNet/IP 419
Expedited Forwarding 218

F
FAQ 453
Fast HIPER-Ring konfigurieren 272
Filter für MAC-Adressen 169
Forward Delay 293, 295

G
Grafische Benutzeroberfläche starten 15
Grafische Benutzeroberfläche (GUI) 15
Grandmaster 152
Grundeinstellungen 21

H
Hardware-Uhr (gepuffert) 132
Hello Time 292, 295
HIPER-Ring 197, 261
HIPER-Ring konfigurieren 261
HIPER-Ring (Quelle für Alarme) 384
HiView 15
HiVRRP 318
HiVRRP-Domänen 323
Host Routes Accept 238

I
ICMP 237
IGMP-Einstellungen 177
IGMP-Querier 177
IGMP-Snooping 177
Independent VLAN 190
Industrial HiVision 12
Industrieprotokolle 11, 416
Ingress Filtering 198
IP-DSCP Wert 208
IP-DSCP-Mapping 207, 218

J
Java Runtime Environment 21

K

Kaltstart 68
Kaltstart (nach dem Software-Update) 34, 35
Konfigurationprofil speichern (GUI) 19
Konfigurations-Check 362

L

LACP Link Aggregation Control Protocol 254
Lastbegrenzer Einstellungen 174
Lieferzustand wiederherstellen 52
Link Aggregation 253, 256
LLDP 362, 365
LLDP-MED (Voice-VLAN) 202
Login Banner 125
Login-Banner 124
Login-Fenster 17

M

Maximale Bandbreite 224
Max Age 293, 295
Medienmodul (bei modularen Geräten) 23
Meldekontakt 377
Meldekontakt (Quelle für Alarm) 384
MRP-Domäne 278, 279
MRP-Ring 197, 254, 265
MRP-Ring konfigurieren 265
Multicasts 176
Multinetting 227
Multiple Spanning Tree (MSTP) 288

N

Netdirected Broadcasts 227, 229, 230
Netzlast 288, 340
Netzmanagementstation 365
Neustart 68

O

OSPF Routen 241

P

Passwort 72, 74
Per-Hop-Behavior (PHB) 218
PHY Fast Startup pro Port 418
Portkonfiguration 37
Portkonfiguration (QoS/Priorität) 210
Ports 338
Portsicherheit (802.1X-basiert) 98
Portsicherheit (IP-/MAC-basiert) 89
Portsicherheit (Quelle für Alarme) 92, 96
Portstatistiken 338
Port-Mirroring 371
Port-Monitor 346
Port-Priorität 210, 212
Port-VLAN-ID 198
Port-Zustand (Link) 37
PROFINET IO 11, 416
Precedence 218
Precision Time Protocol 139
Pre-Login-Banner 124
Prioritäts-Queue 208
Proxy-ARP 229, 230
PTP 139

Q

QoS/Priorität 207
Queue-Management 207, 221

R

RADIUS 116
RAM-Test 397
Rapid Spanning Tree (RSTP) 288, 305
Reboot 68
Redundanz 11, 253, 288
Redundanzmanager 258
Referenzuhr 152
Restricted Management Access 85
RFC 438
RIP 238
RIP (Konfiguration) 238
RIP-Statistik 243
Ring 258
Ringmanager 258
Ringport 261
Ringstruktur 258
Ring-Redundanz 253
Ring-/Netzkopplung 197, 253, 282, 376
Ring-/Netzkopplung (Quelle für Alarme) 384
RMON-Probe 371
RM-Funktion 258
Root-Bridge 289
Routenverteilung 241
Router 11, 225
Router Discovery 237
Route Distribution 241
Routingtabelle 244
Routing Information Protocol (RIP) 238
Routing (Globale Einstellungen) 226
Routing-Funktion 227

S

Schulungsangebote 453
Selbsttest 397
SFP-Modul 342
SFP-Zustandsanzeige 342
Shaping Rate 210, 214
Shared VLAN 190
Sicherheit 71
SNMPv1/v2-Zugriffs-Einstellungen 76

SNMP-Logging 332
SNTP-Broadcasts 136
SNTP-Server 403
Software-Update 32
Spanning Tree (STP) 288
Split-Horizon 239
SSH-Zugriff 80
Statische Routingtabelle 246
Statistiktabelle 338
Statusleiste über Menü 18
Strict-Priority 222
Sub-Ring konfigurieren 275, 276, 279
Switching 163
Symbol 13
Syslog 332
Systemvoraussetzungen (GUI) 15
Systemzeit 136

T

Technische Fragen 453
Telnet-Zugriff 80
Temperatur (Gerät) 23
Temperatur (SFPs) 342
Time To Live 226
Topologie 365
Topologie-Erkennung 362
ToS 207
TP-Kabeldiagnose 343
Tracking 249, 327
Tracking (VRRP/HiVRRP) 246
Tracking-Applikationen 252
Tracking-Konfiguration 249
Traffic Class 221
Trap 383
Trunk 254
TrustDot1p (globaler Trust-Modus) 213
TrustIpDscp 213
Trust Modus 210, 213
TTL 226
TX Hold Count 293
Type-of-Service 207

U

Uhr 139
Untrusted Traffic Class 210, 214
Untrusted (globaler Trust-Modus) 213

V

Verbindungs-Zustand (Link) 37
Versorgungsspannung 384
Video 223
Virtual Router Redundancy Protocol 318
VLAN 187
VLAN Aktuell Dialog 193
VLAN Global-Dialog 187
VLAN Modus 190
VLAN Port Dialog 198
VLAN Priorität 208
VLAN Statisch Dialog 195
VLAN und GOOSE Protokoll 189
VLAN und GVRP 199
VLAN und Redundanzringe 200
VLAN (HIPER-Ring) 263
VLAN (Router-Interface) 227
VLAN-ID (Netzparameter) 29
VLAN-Mapping 207
VoIP 223
Voice-VLAN 202
Voreinstellungen wiederherstellen 52
VRRP 318
VRRP-Instanz 319
VRRP-Nachrichten-Intervall 321
VRRP-Router-Instanz 321
VRRP-Statistik 326
VRRP-Tracking 252, 327

W

Warteschlange 222
Web-Zugriff 80
Weighted Fair Queuing 214, 223, 223
Weighted Round Robin 223

Z

Zeit 131, 132
Zeitmanagement 139
Zeitstempeleinheit 140
Zwei-Switch-Kopplung 284

D Weitere Unterstützung

Technische Fragen

Bei technischen Fragen wenden Sie sich bitte an den Hirschmann-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann.

Die Adressen unserer Vertragspartner finden Sie im Internet unter http://www.hirschmann.com

Unser Support steht Ihnen zur Verfügung unter https://hirschmann-support.belden.eu.com

Sie erreichen uns

in der Region EMEA unter
- Tel.: +49 (0)1805 14-1538
- E-Mail: hac.support@belden.com

in der Region Amerika unter
- Tel.: +1 (717) 217-2270
- E-Mail: inet-support.us@belden.com

in der Region Asien-Pazifik unter
- Tel.: +65 6854 9860
- E-Mail: inet-ap@belden.com

Hirschmann Competence Center

Das Hirschmann Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen hat vor den Wettbewerbern gleich dreifach die Nase vorn:

- Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
  Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter http://www.hicomcenter.com
- Der Support reicht von der Inbetriebnahme über den Bereitschafts-service bis zu Wartungskonzepten.

Mit dem Hirschmann Competence Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

Reference Manual

CLI Command Line Interface
Industrial ETHERNET (Gigabit) Switch
PowerMICE, MACH 104, MACH 1040, MACH 4000

L3P Rel. 9.0

Technical Support
HAC-Support@belden.com

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.

© 2015 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. For devices with embedded software, the end-user license agreement on the enclosed CD/DVD applies.

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 (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Germany
Tel.: +49 1805 141538

Rel. 9.0 - 02/2015 – 2/19/15

Content

Content 3

About this Manual 27

Maintenance 29

Service Shell 31
Permanently disabling the Service Shell 31

1 Command Structure 33

1.1 Format 34
1.1.1 Command 35
1.1.2 Parameters 35
1.1.3 Values 36
1.1.4 Conventions 38
1.1.5 Annotations 39
1.1.6 Special keys 40
1.1.7 Special characters in scripts 41
1.1.8 Secrets in scripts 43
1.1.9 Slot-Port Naming Convention 45

2 Quick Start up 47

2.1 Quick Starting the Switch 48

2.2 System Info and System Setup 49

3 Mode-based CLI 55

3.1 Mode-based Topology 57

3.2 Mode-based Command Hierarchy 58

3.3 Flow of Operation 61

3.4 “No” Form of a Command 63
3.4.1 Support for “No” Form 63
3.4.2 Behavior of Command Help ("?") 63

4 CLI Commands: Base 65

4.1 System Information and Statistics 66
4.1.1 show 66
4.1.2 show address-conflict 66
4.1.3 show arp switch 67
4.1.4 show bridge address-learning 67
4.1.5 show bridge address-relearn-detect 68
4.1.6 show bridge aging-time 68
4.1.7 show bridge duplex-mismatch-detect 69
4.1.8 show bridge fast-link-detection 69
4.1.9 show bridge framesize 69
4.1.10 show bridge vlan-learning 70
4.1.11 bridge framesize 70
4.1.12 show config-watchdog 71
4.1.13 show device-status 71
4.1.14 show authentication 72
4.1.15 show eventlog 73
4.1.16 show interface 74
4.1.17 show interface ethernet 76
4.1.18 show interface switchport 83
4.1.19 show interface utilization 84
4.1.20 show logging 85
4.1.21 show mac-address-conflict 86
4.1.22 show mac-addr-table 87
4.1.23 show signal-contact 88
4.1.24 show slot 90
4.1.25 show running-config 91
4.1.26 show sysinfo 92
4.1.27 show temperature 95
4.1.28 utilization alarm-threshold 95

4.2 Debug Commands 96
4.2.1 debug tcpdump help 96
4.2.2 debug tcpdump start cpu 96
4.2.3 debug tcpdump start cpu filter 97
4.2.4 debug tcpdump stop 97
4.2.5 debug tcpdump filter show 98
4.2.6 debug tcpdump filter list 98
4.2.7 debug tcpdump filter delete 99

4.3 Management VLAN Commands 100

4.3.1 network mgmt_vlan 100

4.4 Class of Service (CoS) Commands 101
4.4.1 classofservice dot1p-mapping 102
4.4.2 classofservice ip-dscp-mapping 103
4.4.3 classofservice trust 104
4.4.4 show classofservice dot1p-mapping 105
4.4.5 show classofservice ip-dscp-mapping 106
4.4.6 show classofservice trust 107
4.4.7 vlan port priority all 107
4.4.8 vlan priority 108
4.4.9 dvlan-tunnel ethertype 108
4.4.10 mode dvlan-tunnel 110
4.4.11 show dvlan-tunnel 111

4.5 Link Aggregation(802.3ad) Commands 112
4.5.1 link-aggregation staticcapability 112
4.5.2 show link-aggregation brief 113

4.6 Management Commands 114
4.6.1 telnet 114
4.6.2 transport input telnet 115
4.6.3 transport output telnet 116
4.6.4 session-limit 117
4.6.5 session-timeout 118
4.6.6 bridge address-learning 118
4.6.7 bridge address-relearn detect operation 119
4.6.8 bridge address-relearn detect threshold 119
4.6.9 bridge aging-time 120
4.6.10 bridge fast-link-detection 121
4.6.11 bridge duplex-mismatch-detect operation 121
4.6.12 bridge vlan-learning 122
4.6.13 digital-input 122
4.6.14 digital-output 124
4.6.15 show digital-input 127
4.6.16 show digital-input config 128
4.6.17 show digital-input all 129
4.6.18 show digital-input <slot/input> 130
4.6.19 show digital-output 131
4.6.20 show digital-output config 132
4.6.21 show digital-output all 133
4.6.22 show digital-output <slot/output> 134

4.6.23	ethernet-ip	135
4.6.24	network mgmt-access add	136
4.6.25	network mgmt-access delete	136
4.6.26	network mgmt-access modify	137
4.6.27	network mgmt-access operation	138
4.6.28	network mgmt-access status	139
4.6.29	network parms	139
4.6.30	network protocol	140
4.6.31	network priority	141
4.6.32	profinetio	142
4.6.33	serial timeout	143
4.6.34	set prompt	143
4.6.35	show ethernet-ip	144
4.6.36	show network	144
4.6.37	show network mgmt-access	146
4.6.38	show profinetio	147
4.6.39	show serial	147
4.6.40	show snmp-access	148
4.6.41	show snmpcommunity	149
4.6.42	show snmp sync	150
4.6.43	show snmptrap	151
4.6.44	show telnet	152
4.6.45	show telnetcon	153
4.6.46	show trapflags	154
4.6.47	snmp-access global	155
4.6.48	snmp-access version	156
4.6.49	snmp-access version v3-encryption	157
4.6.50	snmp-server	158
4.6.51	snmp-server community	159
4.6.52	snmp-server contact	160
4.6.53	snmp-server community ipaddr	161
4.6.54	snmp-server community ipmask	162
4.6.55	snmp-server community mode	163
4.6.56	snmp-server community ro	164
4.6.57	snmp-server community rw	164
4.6.58	snmp-server location	164
4.6.59	snmp-server sysname	165
4.6.60	snmp-server enable traps	165
4.6.61	snmp-server enable traps chassis	166
4.6.62	snmp-server enable traps l2redundancy	167
4.6.63	snmp-server enable traps linkmode	168

4.6.64 snmp-server enable traps multiusers 169
4.6.65 snmp-server enable traps port-sec 170
4.6.66 snmp-server enable traps stpmode 171
4.6.67 snmptrap 172
4.6.68 snmptrap ipaddr 173
4.6.69 snmptrap mode 174
4.6.70 snmptrap snmpversion 175
4.6.71 telnetcon maxsessions 176
4.6.72 telnetcon timeout 177

4.7 Syslog Commands 178
4.7.1 logging buffered 178
4.7.2 logging buffered wrap 179
4.7.3 logging cli-command 180
4.7.4 logging console 181
4.7.5 logging host 182
4.7.6 logging host reconfigure 183
4.7.7 logging host remove 183
4.7.8 logging snmp-requests get operation 183
4.7.9 logging snmp-requests set operation 184
4.7.10 logging snmp-requests get severity 184
4.7.11 logging snmp-requests set severity 185
4.7.12 logging syslog 186
4.7.13 logging syslog port 186

4.8 Scripting Commands 187
4.8.1 script apply 187
4.8.2 script delete 188
4.8.3 script list 188
4.8.4 script show 189
4.8.5 script validate 189

4.9 Device Configuration Commands 191
4.9.1 addport 191
4.9.2 adminmode 192
4.9.3 auto-disable reason 193
4.9.4 auto-disable reset 195
4.9.5 auto-disable timer 195
4.9.6 auto-negotiate 196
4.9.7 auto-negotiate all 197
4.9.8 cable-crossing 198
4.9.9 media-module 199

4.9.10	deleteport	200
4.9.11	deleteport all	200
4.9.12	dip-switch operation	201
4.9.13	macfilter	202
4.9.14	macfilter adddest	203
4.9.15	macfilter adddest all	204
4.9.16	mac notification (Global Config)	205
4.9.17	mac notification (Interface Config)	206
4.9.18	monitor session <session-id>	207
4.9.19	monitor session <session-id> mode	209
4.9.20	monitor session <session-id> source/destination	210
4.9.21	link-aggregation	211
4.9.22	link-aggregation adminmode	212
4.9.23	link-aggregation linktrap	213
4.9.24	link-aggregation name	214
4.9.25	rmon-alarm add	214
4.9.26	rmon-alarm delete	215
4.9.27	rmon-alarm enable	215
4.9.28	rmon-alarm disable	216
4.9.29	rmon-alarm modify mib-variable	216
4.9.30	rmon-alarm modify thresholds	217
4.9.31	rmon-alarm modify interval	217
4.9.32	rmon-alarm modify sample-type	218
4.9.33	rmon-alarm modify startup-alarm	218
4.9.34	rmon-alarm modify rising-event	219
4.9.35	rmon-alarm modify falling-event	219
4.9.36	set garp timer join	220
4.9.37	set garp timer leave	221
4.9.38	set garp timer leaveall	222
4.9.39	set gmrp adminmode	223
4.9.40	set gmrp interfacemode	224
4.9.41	set gmrp interfacemode	225
4.9.42	set gmrp forward-all-groups	226
4.9.43	set gmrp forward-unknown	227
4.9.44	set igmp	228
4.9.45	set igmp	229
4.9.46	set igmp aging-time-unknown	229
4.9.47	set igmp automatic-mode	230
4.9.48	set igmp forward-all	231
4.9.49	set igmp static-query-port	232
4.9.50	set igmp groupmembershipinterval	233

4.9.51	set igmp interfacemode	234
4.9.52	set igmp lookup-interval-unknown	235
4.9.53	set igmp lookup-resp-time-unknown	235
4.9.54	set igmp maxresponse	236
4.9.55	set igmp querier max-response-time	237
4.9.56	set igmp querier protocol-version	237
4.9.57	set igmp querier status	238
4.9.58	set igmp querier tx-interval	238
4.9.59	set igmp query-ports-to-filter	239
4.9.60	selftest ramtest	239
4.9.61	selftest reboot-on-error	240
4.9.62	serviceshell	241
4.9.63	update module-configuration	241
4.9.64	show auto-disable brief	242
4.9.65	show auto-disable reasons	243
4.9.66	show dip-switch	244
4.9.67	show garp	245
4.9.68	show gmrp configuration	245
4.9.69	show igmpsnooping	246
4.9.70	show mac-filter-table gmrp	248
4.9.71	show mac-filter-table igmpsnooping	249
4.9.72	show mac-filter-table multicast	250
4.9.73	show mac-filter-table static	251
4.9.74	show mac-filter-table staticfiltering	252
4.9.75	show mac-filter-table stats	253
4.9.76	show mac notification	253
4.9.77	show monitor session	255
4.9.78	show port	256
4.9.79	show link-aggregation	257
4.9.80	show rmon-alarm	258
4.9.81	show selftest	259
4.9.82	show serviceshell	259
4.9.83	show storm-control	260
4.9.84	show storm-control limiters port	260
4.9.85	show vlan	261
4.9.86	show vlan brief	263
4.9.87	show vlan port	264
4.9.88	show voice vlan	265
4.9.89	show voice vlan interface	266
4.9.90	shutdown	267
4.9.91	shutdown all	268

4.9.92 snmp sync community-to-v3 269
4.9.93 snmp sync v3-to-community 270
4.9.94 snmp trap link-status 270
4.9.95 snmp trap link-status all 271
4.9.96 spanning-tree bpdumigrationcheck 272
4.9.97 speed 273
4.9.98 storm-control broadcast 274
4.9.99 storm-control egress-limiting 274
4.9.100 storm-control ingress-limiting 275
4.9.101 storm-control ingress-mode 275
4.9.102 storm-control broadcast (port-related) 276
4.9.103 storm-control egress-limit 276
4.9.104 storm-control ingress-limit 277
4.9.105 storm-control ingress-mode 277
4.9.106 storm-control flowcontrol 278
4.9.107 storm-control flowcontrol per port 279
4.9.108 vlan 280
4.9.109 vlan0-transparent-mode 281
4.9.110 vlan acceptframe 282
4.9.111 vlan database 283
4.9.112 vlan ingressfilter 284
4.9.113 vlan name 285
4.9.114 vlan participation 286
4.9.115 vlan participation all 287
4.9.116 vlan port acceptframe all 288
4.9.117 vlan port ingressfilter all 289
4.9.118 vlan port pvid all 290
4.9.119 vlan port tagging all 291
4.9.120 vlan pvid 292
4.9.121 vlan tagging 293
4.9.122 voice vlan (Global Config Mode) 294
4.9.123 voice vlan <id> 295
4.9.124 voice vlan dot1p 296
4.9.125 voice vlan none 296
4.9.126 voice vlan untagged 297
4.9.127 voice vlan auth 297

4.10 User Account Management Commands 298
4.10.1 disconnect 298
4.10.2 show loginsession 299
4.10.3 show users 300

4.10.4 users defaultlogin 301
4.10.5 users login <user> 302
4.10.6 users access 303
4.10.7 users name 304
4.10.8 users passwd 305
4.10.9 users snmpv3 accessmode 306
4.10.10 users snmpv3 authentication 307
4.10.11 users snmpv3 encryption 308

4.11 System Utilities 309
4.11.1 address-conflict 309
4.11.2 boot skip-aca-on-boot 310
4.11.3 show boot skip-aca-on-boot 310
4.11.4 cablestatus 311
4.11.5 clear eventlog 311
4.11.6 traceroute 312
4.11.7 clear arp-table-switch 312
4.11.8 clear config 313
4.11.9 clear config factory 313
4.11.10 clear counters 313
4.11.11 clear hiper-ring 314
4.11.12 clear igmpsnooping 314
4.11.13 clear mac-addr-table 315
4.11.14 clear pass 315
4.11.15 clear link-aggregation 316
4.11.16 clear signal-contact 316
4.11.17 clear traplog 317
4.11.18 clear ring-coupling 317
4.11.19 clear vlan 317
4.11.20 config-watchdog 318
4.11.21 copy 318
4.11.22 device-status connection-error 327
4.11.23 device-status monitor 328
4.11.24 logout 329
4.11.25 mac-address conflict operation 329
4.11.26 ping 330
4.11.27 signal-contact connection-error 330
4.11.28 signal-contact 331
4.11.29 temperature 332
4.11.30 reboot 333
4.11.31 show reboot 334

4.11.32 reload 335
4.11.33 show reload 336
4.11.34 set clibanner 337
4.11.35 set pre-login-banner 339

4.12 LLDP - Link Layer Discovery Protocol 341
4.12.1 show lldp 341
4.12.2 show lldp config 341
4.12.3 show lldp config chassis 342
4.12.4 show lldp config chassis admin-state 342
4.12.5 show lldp config chassis notification-interval 342
4.12.6 show lldp config chassis re-init-delay 343
4.12.7 show lldp config chassis tx-delay 343
4.12.8 show lldp config chassis tx-hold-mult 343
4.12.9 show lldp config chassis tx-interval 344
4.12.10 show lldp config port 345
4.12.11 show lldp config port tlv 346
4.12.12 show lldp med 347
4.12.13 show lldp med interface 348
4.12.14 show lldp med local-device detail 349
4.12.15 show lldp med remote-device 350
4.12.16 show lldp med remote-device detail 351
4.12.17 show lldp remote-data 351
4.12.18 lldp 353
4.12.19 lldp config chassis admin-state 354
4.12.20 lldp config chassis notification-interval 354
4.12.21 lldp config chassis re-init-delay 355
4.12.22 lldp config chassis tx-delay 355
4.12.23 lldp config chassis tx-hold-mult 356
4.12.24 lldp chassis tx-interval 356
4.12.25 clear lldp config all 357
4.12.26 lldp admin-state 357
4.12.27 lldp fdb-mode 358
4.12.28 lldp hm-mode 358
4.12.29 lldp max-neighbors 359
4.12.30 lldp med 360
4.12.31 lldp med all 361
4.12.32 lldp med confignotification 361
4.12.33 lldp med confignotification all 362
4.12.34 lldp med faststartrepeatcount 363
4.12.35 lldp med transmit-tlv 364

4.12.36 lldp med transmit-tlv all 365
4.12.37 lldp notification 366
4.12.38 lldp tlv link-aggregation 366
4.12.39 lldp tlv mac-phy-config-state 366
4.12.40 lldp tlv max-frame-size 367
4.12.41 lldp tlv mgmt-addr 367
4.12.42 lldp tlv pnio 367
4.12.43 lldp tlv pnio-alias 368
4.12.44 lldp tlv pnio-mrp 368
4.12.45 lldp tlv port-desc 368
4.12.46 lldp tlv port-vlan 369
4.12.47 lldp tlv gmrp 369
4.12.48 lldp tlv igmp 369
4.12.49 lldp tlv portsec 370
4.12.50 lldp tlv ptp 370
4.12.51 lldp tlv protocol 370
4.12.52 lldp tlv sys-cap 371
4.12.53 lldp tlv sys-desc 371
4.12.54 lldp tlv sys-name 371
4.12.55 lldp tlv vlan-name 372
4.12.56 name 372

4.13 SNTP - Simple Network Time Protocol 373
4.13.1 show sntp 373
4.13.2 show sntp anycast 375
4.13.3 show sntp client 375
4.13.4 show sntp operation 376
4.13.5 show sntp server 377
4.13.6 show sntp status 377
4.13.7 show sntp time 378
4.13.8 no sntp 378
4.13.9 sntp anycast address 379
4.13.10 sntp anycast transmit-interval 379
4.13.11 sntp anycast vlan 380
4.13.12 sntp client accept-broadcast 380
4.13.13 sntp client disable-after-sync 381
4.13.14 sntp client offset 381
4.13.15 sntp client request-interval 382
4.13.16 no sntp client server 382
4.13.17 sntp client server primary 383
4.13.18 sntp client server secondary 384

4.13.19 sntp client threshold 385
4.13.20 sntp operation 386
4.13.21 sntp server disable-if-local 387
4.13.22 sntp time system 387

4.14 PTP - Precision Time Protocol 388
4.14.1 show ptp 388
4.14.2 show ptp configuration 391
4.14.3 show ptp operation 391
4.14.4 show ptp port 392
4.14.5 show ptp status 393
4.14.6 ptp clock-mode 394
4.14.7 ptp operation 395
4.14.8 ptp sync-lower-bound 395
4.14.9 ptp sync-upper-bound 396
4.14.10 ptp v1 preferred-master 396
4.14.11 ptp v1 re-initialize 397
4.14.12 ptp v1 subdomain-name 397
4.14.13 ptp v1 sync-interval 398
4.14.14 ptp v2bc priority1 399
4.14.15 ptp v2bc priority2 399
4.14.16 ptp v2bc domain 400
4.14.17 ptp v2bc utc-offset 400
4.14.18 ptp v2bc utc-offset-valid 400
4.14.19 ptp v2bc vlan 401
4.14.20 ptp v2bc vlan-priority 401
4.14.21 ptp v1 burst 402
4.14.22 ptp v1 operation 402
4.14.23 ptp v2bc operation 403
4.14.24 ptp v2bc announce-interval 403
4.14.25 ptp v2bc announce-timeout 404
4.14.26 ptp v2bc sync-interval 404
4.14.27 ptp v2bc delay-mechanism 404
4.14.28 ptp v2bc pdelay-interval 405
4.14.29 ptp v2bc network-protocol 405
4.14.30 ptp v2bc v1-compatibility-mode 405
4.14.31 ptp v2bc asymmetry 406
4.14.32 ptp v2tc asymmetry 406
4.14.33 ptp v2tc delay-mechanism 406
4.14.34 ptp v2tc management 407
4.14.35 ptp v2tc multi-domain-mode 407

4.14.36 ptp v2tc network-protocol 408
4.14.37 ptp v2tc operation 408
4.14.38 ptp v2tc pdelay-interval 409
4.14.39 ptp v2tc primary-domain 409
4.14.40 ptp v2tc profile 410
4.14.41 ptp v2tc syntonization 410
4.14.42 ptp v2tc vlan 411
4.14.43 ptp v2tc power-tlv-check 411
4.14.44 ptp v2tc vlan-priority 412
4.14.45 ptp v2tc sync-local-clock 412

4.15 PoE - Power over Ethernet 413
4.15.1 show inlinepower 413
4.15.2 show inlinepower port 414
4.15.3 inlinepower (Global Config) 417
4.15.4 inlinepower (Interface Config) 418
4.15.5 clear inlinepower 419

4.16 PoE+ - Power over Ethernet Plus 420
4.16.1 show inlinepower slot 420
4.16.2 inlinepower budget slot 421
4.16.3 inlinepower threshold slot 422
4.16.4 inlinepower trap slot 422

4.17 Port monitor 423
4.17.1 show port-monitor 424
4.17.2 show port-monitor <slot/port> 424
4.17.3 show port-monitor brief 426
4.17.4 show port-monitor crc-fragment 427
4.17.5 show port-monitor link-flap 427
4.17.6 show port-monitor overload-detection 428
4.17.7 show port-monitor speed-duplex 429
4.17.8 port-monitor (Global Config) 430
4.17.9 port-monitor (Interface Config) 430
4.17.10 port-monitor action 431
4.17.11 port-monitor condition link-flap (Global Config) 432
4.17.12 port-monitor condition link-flap (Interface Config) 432
4.17.13 port-monitor condition crc-fragment (Global Config) 433
4.17.14 port-monitor condition crc-fragment (Interface Config) 434
4.17.15 port-monitor condition speed-duplex-monitor (Interface Config) 434

4.17.16 port-monitor condition speed-duplex-monitor speed (Interface Config) 435
4.17.17 port-monitor condition speed-duplex-monitor clear (Interface Config) 435

5 CLI Commands: Switching 437

5.1 Spanning Tree Commands 439
5.1.1 show spanning-tree 439
5.1.2 show spanning-tree interface 442
5.1.3 show spanning-tree mst detailed 443
5.1.4 show spanning-tree mst port detailed 444
5.1.5 show spanning-tree mst port summary 447
5.1.6 show spanning-tree mst summary 448
5.1.7 show spanning-tree summary 449
5.1.8 show spanning-tree vlan 450
5.1.9 spanning-tree 451
5.1.10 spanning-tree auto-edgeport 452
5.1.11 spanning-tree bpduguard 453
5.1.12 spanning-tree configuration name 454
5.1.13 spanning-tree configuration revision 455
5.1.14 spanning-tree edgeport 456
5.1.15 spanning-tree forceversion 457
5.1.16 spanning-tree forward-time 458
5.1.17 spanning-tree guard loop 459
5.1.18 spanning-tree guard none 460
5.1.19 spanning-tree guard root 461
5.1.20 spanning-tree hello-time 462
5.1.21 spanning-tree hold-count 462
5.1.22 spanning-tree max-age 463
5.1.23 spanning-tree max-hops 464
5.1.24 spanning-tree mst 465
5.1.25 spanning-tree mst priority 467
5.1.26 spanning-tree mst vlan 468
5.1.27 spanning-tree mst instance 469
5.1.28 spanning-tree port mode 470
5.1.29 spanning-tree port mode all 471
5.1.30 spanning-tree stp-mrp-mode 472
5.1.31 spanning-tree tcnguard 473

5.2 MRP 474
5.2.1 show mrp 474

5.2.2 show mrp current-domain 475
5.2.3 mrp current-domain 476
5.2.4 mrp delete-domain 478
5.2.5 mrp new-domain 478
5.2.6 arc 479
5.2.7 show arc 480

5.3 HIPER-Ring 482
5.3.1 show hiper-ring 483
5.3.2 hiper-ring 484
5.3.3 hiper-ring mode 484
5.3.4 hiper-ring port primary 485
5.3.5 hiper-ring port secondary 485
5.3.6 hiper-ring recovery-delay 486

5.4 Fast-HIPER-Ring 487
5.4.1 fast-hiper-ring 490

5.5 Redundant Coupling 492
5.5.1 show ring-coupling 493
5.5.2 ring-coupling 495
5.5.3 ring-coupling config 496
5.5.4 ring-coupling net-coupling 497
5.5.5 ring-coupling operation 497
5.5.6 ring-coupling port 498
5.5.7 ring-coupling redundancy-mode 498

5.6 Port Security 499
5.6.1 show port-sec dynamic 499
5.6.2 show port-sec mode 500
5.6.3 show port-sec port 501
5.6.4 port-sec mode 501
5.6.5 port-sec action 502
5.6.6 port-sec allowed-ip 503
5.6.7 port-sec allowed-ip add 503
5.6.8 port-sec allowed-ip remove 504
5.6.9 port-sec allowed-mac 504
5.6.10 port-sec allowed-mac add 505
5.6.11 port-sec allowed-mac remove 505
5.6.12 port-sec dynamic 506
5.6.13 clear port-sec 506

5.7 DHCP Relay Commands 507
5.7.1 dhcp-relay 508

5.7.2 dhcp-relay 509
5.7.3 show dhcp-relay 510

5.8 DHCP Server Commands 512
5.8.1 DHCP server configuration example 512
5.8.2 show dhcp-server 514
5.8.3 show dhcp-server operation 515
5.8.4 show dhcp-server port 515
5.8.5 show dhcp-server pool 516
5.8.6 dhcp-server addr-probe 516
5.8.7 dhcp-server operation 517
5.8.8 dhcp-server pool add <id> 517
5.8.9 dhcp-server pool modify <id> mode 518
5.8.10 dhcp-server pool modify <id> option 520
5.8.11 dhcp-server pool modify leasetime 521
5.8.12 dhcp-server pool modify <id> hirschmann-device 521
5.8.13 dhcp-server pool enable 522
5.8.14 dhcp-server pool disable 522
5.8.15 dhcp-server pool delete 522

5.9 Sub-Ring Commands 523
5.9.1 show sub-ring 523
5.9.2 sub-ring <id> mode 525
5.9.3 sub-ring <id> operation 526
5.9.4 sub-ring <id> protocol 526
5.9.5 sub-ring <id> port 527
5.9.6 sub-ring <id> ring-name 527
5.9.7 sub-ring <id> vlan 528
5.9.8 sub-ring <id> mrp-domainID 529
5.9.9 sub-ring delete-ring 530
5.9.10 sub-ring new-ring 530

6 CLI Commands: Security 531

6.1 Security Commands 533
6.1.1 authentication login 533
6.1.2 authorization network radius 535
6.1.3 clear dot1x statistics 535
6.1.4 clear radius statistics 536
6.1.5 dot1x defaultlogin 536
6.1.6 dot1x dynamic-vlan enable 537
6.1.7 dot1x guest-vlan 538

6.1.8 dot1x initialize 539
6.1.9 dot1x login 539
6.1.10 dot1x mac-auth-bypass 540
6.1.11 dot1x max-req 541
6.1.12 dot1x max-users 542
6.1.13 dot1x port-control 543
6.1.14 dot1x port-control all 544
6.1.15 dot1x re-authenticate 545
6.1.16 dot1x re-authentication 545
6.1.17 dot1x safe-vlan 546
6.1.18 dot1x system-auth-control 547
6.1.19 dot1x timeout 547
6.1.20 dot1x timeout guest-vlan-period 549
6.1.21 dot1x unauthenticated-vlan 550
6.1.22 dot1x user 551
6.1.23 ip ssh protocol 552
6.1.24 radius accounting mode 553
6.1.25 radius server host 553
6.1.26 radius server key 555
6.1.27 radius server msgauth 555
6.1.28 radius server primary 556
6.1.29 radius server retransmit 557
6.1.30 radius server timeout 558
6.1.31 show radius accounting 558
6.1.32 show authentication 561
6.1.33 show authentication users 562
6.1.34 show dot1x 562
6.1.35 show dot1x users 567
6.1.36 show dot1x clients 568
6.1.37 show ip ssh 569
6.1.38 show radius 570
6.1.39 show radius statistics 571
6.1.40 show users authentication 573
6.1.41 users login 574

6.2 HTTP Commands 575
6.2.1 ip http server 575
6.2.2 show ip http 576
6.2.3 ip https server 577
6.2.4 ip https port 578
6.2.5 ip https certgen 578

6.2.6 show ip https 579

7 Appendix- VLAN Example 581

7.1 SOLUTION 1 583

7.2 SOLUTION 2 585

8 Routing Commands 587

8.1 ARP Commands 589
8.1.1 arp 590
8.1.2 ip proxy-arp 591
8.1.3 arp cachesize 592
8.1.4 arp dynamicrenew 593
8.1.5 arp purge 593
8.1.6 arp resptime 594
8.1.7 arp retries 595
8.1.8 arp selective-learning 596
8.1.9 arp timeout 597
8.1.10 clear arp-cache 597
8.1.11 show arp 598
8.1.12 show arp brief 600
8.1.13 show arp switch 601

8.2 IP Routing 602
8.2.1 routing 603
8.2.2 ip routing 604
8.2.3 ip address 605
8.2.4 ip mtu 606
8.2.5 ip netdirbcast 607
8.2.6 ip route 608
8.2.7 ip route default 610
8.2.8 ip route distance 611
8.2.9 ip forwarding 612
8.2.10 ip vlan-single-mac 613
8.2.11 show ip brief 614
8.2.12 ip table-sizes 615
8.2.13 ip table-sizes arp-entries 616
8.2.14 ip table-sizes unicast-routes 617
8.2.15 ip table-sizes multicast-routes 618
8.2.16 show ip interface 619
8.2.17 show ip interface brief 621

8.2.18 show ip route 622
8.2.19 show ip route bestroutes 623
8.2.20 show ip route entry 624
8.2.21 show ip route preferences 625
8.2.22 show ip route static 626
8.2.23 show ip stats 627

8.3 Router Discovery Protocol Commands 633
8.3.1 ip irdp 634
8.3.2 ip irdp address 635
8.3.3 ip irdp holdtime 636
8.3.4 ip irdp maxadvertinterval 637
8.3.5 ip irdp minadvertinterval 638
8.3.6 ip irdp preference 639
8.3.7 show ip irdp 639

8.4 Virtual LAN Routing Commands 641
8.4.1 vlan routing 642
8.4.2 show ip vlan 643

8.5 Tracking Commands 644
8.5.1 track interface 644
8.5.2 track logical 645
8.5.3 track mode 645
8.5.4 track ping 646
8.5.5 track trap 647
8.5.6 show track 647
8.5.7 show track <id> 649
8.5.8 show track applications 651

8.6 VRRP Commands 652
8.6.1 ip vrrp 653
8.6.2 ip vrrp domain send-member-advertisements 654
8.6.3 ip vrrp trap 655
8.6.4 ip vrrp 656
8.6.5 ip vrrp mode 657
8.6.6 ip vrrp ip 658
8.6.7 ip vrrp authentication 659
8.6.8 ip vrrp preempt 660
8.6.9 ip vrrp delay-preemption 661
8.6.10 ip vrrp priority 662
8.6.11 ip vrrp timers advertise 663
8.6.12 ip vrrp advertisement-address 664

8.6.13 ip vrrp link-down-notification 665
8.6.14 ip vrrp track 666
8.6.15 ip vrrp domain 667
8.6.16 show ip vrrp interface stats 668
8.6.17 show ip vrrp 670
8.6.18 show ip vrrp domain 671
8.6.19 show ip vrrp interface 672
8.6.20 show ip vrrp interface brief 674

8.7 OSPF Commands 675
8.7.1 enable (OSPF) 676
8.7.2 ip ospf 677
8.7.3 1583compatibility 678
8.7.4 area default-cost 678
8.7.5 area nssa 679
8.7.6 area nssa default-info-originate 679
8.7.7 area nssa no-redistribute (OSPF) 680
8.7.8 area nssa no-summary (OSPF) 680
8.7.9 area nssa translator-role (OSPF) 680
8.7.10 area nssa translator-stab-intv 681
8.7.11 area range 681
8.7.12 area stub 682
8.7.13 area stub summarylsa 683
8.7.14 area virtual-link 684
8.7.15 area virtual-link authentication 685
8.7.16 area virtual-link dead-interval 686
8.7.17 area virtual-link hello-interval 687
8.7.18 area virtual-link retransmit-interval 688
8.7.19 area virtual-link transmit-delay 689
8.7.20 default-information originate (OSPF) 690
8.7.21 default-metric (OSPF) 691
8.7.22 distance ospf 692
8.7.23 distribute-list out 693
8.7.24 exit-overflow-interval 694
8.7.25 external-lsdb-limit 695
8.7.26 ip ospf areaid 696
8.7.27 ip ospf authentication 697
8.7.28 ip ospf cost 698
8.7.29 ip ospf dead-interval 699
8.7.30 ip ospf hello-interval 700
8.7.31 ip ospf priority 701

8.7.32 ip ospf retransmit-interval 702
8.7.33 ip ospf transmit-delay 703
8.7.34 ip ospf mtu-ignore 704
8.7.35 router-id 704
8.7.36 redistribute 705
8.7.37 maximum-paths 706
8.7.38 trapflags 707
8.7.39 show ip ospf 707
8.7.40 show ip ospf area 710
8.7.41 show ip ospf database 711
8.7.42 show ip ospf interface 713
8.7.43 show ip ospf interface brief 715
8.7.44 show ip ospf interface stats 716
8.7.45 show ip ospf neighbor 717
8.7.46 show ip ospf neighbor brief 720
8.7.47 show ip ospf range 721
8.7.48 show ip ospf stub table 722
8.7.49 show ip ospf virtual-link 723
8.7.50 show ip ospf virtual-link brief 724

8.8 RIP Commands 725
8.8.1 enable (RIP) 725
8.8.2 ip rip 726
8.8.3 auto-summary 727
8.8.4 default-information originate (RIP) 728
8.8.5 default-metric (RIP) 729
8.8.6 distance rip 730
8.8.7 distribute-list out 731
8.8.8 ip rip authentication 732
8.8.9 ip rip receive version 733
8.8.10 ip rip send version 734
8.8.11 hostroutesaccept 735
8.8.12 redistribute 736
8.8.13 split-horizon 737
8.8.14 update-timer 738
8.8.15 show ip rip 738
8.8.16 show ip rip interface brief 740
8.8.17 show ip rip interface 741

9 IP Multicast Commands 743

9.1 Multicast Commands 744

9.1.1 ip mcast boundary 744
9.1.2 ip multicast 745
9.1.3 ip multicast staticroute 746
9.1.4 ip multicast ttl-threshold 747
9.1.5 disable ip multicast mdebug mtrace 748
9.1.6 mrinfo 749
9.1.7 mstat 750
9.1.8 mtrace 751
9.1.9 no ip mcast mroute 752
9.1.10 show ip mcast 753
9.1.11 show ip mcast boundary 754
9.1.12 show ip mcast interface 754
9.1.13 show ip mcast mroute 755
9.1.14 show ip mcast mroute group 756
9.1.15 show ip mcast mroute source 757
9.1.16 show ip mcast mroute static 758
9.1.17 show mrinfo 759
9.1.18 show mstat 760
9.1.19 show mtrace 761

9.2 DVMRP Commands 762
9.2.1 ip dvmrp 763
9.2.2 ip dvmrp metric 764
9.2.3 ip dvmrp trapflags 765
9.2.4 ip dvmrp 766
9.2.5 show ip dvmrp 767
9.2.6 show ip dvmrp interface 768
9.2.7 show ip dvmrp neighbor 769
9.2.8 show ip dvmrp nexthop 770
9.2.9 show ip dvmrp prune 771
9.2.10 show ip dvmrp route 772

9.3 IGMP Commands 773
9.3.1 ip igmp 773
9.3.2 ip igmp version 774
9.3.3 ip igmp last-member-query-count 775
9.3.4 ip igmp last-member-query-interval 776
9.3.5 ip igmp query-interval 777
9.3.6 ip igmp query-max-response-time 778
9.3.7 ip igmp robustness 779
9.3.8 ip igmp startup-query-count 780
9.3.9 ip igmp startup-query-interval 781

9.3.10 show ip igmp 782
9.3.11 show ip igmp groups 782
9.3.12 show ip igmp interface 784
9.3.13 show ip igmp interface membership 786
9.3.14 show ip igmp interface stats 788

9.4 PIM-DM Commands 789
9.4.1 ip pimdm 790
9.4.2 ip pimdm holdtimes 791
9.4.3 ip pimdm mode 792
9.4.4 ip pimdm hello-interval 793
9.4.5 show ip pimdm 794
9.4.6 show ip pimdm interface 795
9.4.7 show ip pimdm interface stats 796
9.4.8 show ip pimdm neighbor 797
9.4.9 ip pim-trapflags 798

9.5 PIM-SM Commands 799
9.5.1 ip pimsm mode 800
9.5.2 ip pimsm bsr-border 801
9.5.3 ip pimsm dr-priority 802
9.5.4 ip pimsm join-prune-interval 803
9.5.5 ip pimsm hello-interval 804
9.5.6 ip pimsm bsr-candidate 805
9.5.7 ip pimsm register-threshold 806
9.5.8 ip pimsm rp-address 807
9.5.9 ip pimsm rp-candidate 808
9.5.10 ip pimsm ssm default 808
9.5.11 ip pimsm ssm 809
9.5.12 show ip pimsm 810
9.5.13 show ip pimsm bsr 811
9.5.14 show ip pimsm interface 811
9.5.15 show ip pimsm neighbor 811
9.5.16 show ip pimsm rp mapping 812
9.5.17 show ip pimsm rphash 812
9.5.18 show ip pimsm candidate 813

10 Quality of Service (QoS) Commands 815

10.1 MAC ACL Commands 816
10.1.1 mac access-list extended 817
10.1.2 mac access-list extended rename 818

10.1.3 {deny|permit} 819
10.1.4 mac access-group 821
10.1.5 show mac access-lists 822

10.2 IP ACL Commands 824
10.2.1 access-list 825
10.2.2 access-list fragments 827
10.2.3 ip access-group 828
10.2.4 show ip access-lists 829
10.2.5 show access-lists global 831
10.2.6 show access-lists 832

10.3 CoS Commands 833
10.3.1 cos-queue max-bandwidth 834
10.3.2 cos-queue min-bandwidth 835
10.3.3 cos-queue strict 836
10.3.4 traffic-shape 837
10.3.5 show interfaces cos-queue 837

11 Protocol-based VLAN Commands 839

11.1 Show Commands 840
11.1.1 show port protocol 840

11.2 Configuration Commands 841
11.2.1 vlan protocol group 841
11.2.2 vlan protocol group add protocol 842
11.2.3 vlan protocol group remove 843
11.2.4 protocol group 843
11.2.5 protocol vlan group 844
11.2.6 protocol vlan group all 845

12 Index 847

13 Glossary 859

14 Further support 877

About this Manual

The “GUI” reference manual contains detailed information on using the graphical user interface (web-based interface) to operate the individual functions of the device.

The "Command Line Interface" reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The "Installation" user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The "Basic 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.

The "Redundancy Configuration" user manual contains the information you need to select a suitable redundancy procedure and configure that procedure.

The "Industry Protocols" user manual describes how the device is connected by means of a communication protocol commonly used in the industry, such as EtherNet/IP or PROFINET IO.

The "Routing Configuration User Manual" document contains the information you need to start operating the routing function. It takes you step-by-step from a small router application through to the router configuration of a complex network. ƒn The manual enables you to configure your router by following the examples.

The HiVision Network Management Software provides you with additional options for smooth configuration and monitoring:

- Simultaneous configuration of multiple devices
- Graphic interface with network layout
- Auto-topology recognition
- Event log
- Event handling
- Client/server structure
- Browser interface

- ActiveX control for SCADA integration
- SNMP/OPC gateway.

Maintenance

Hirschmann are continually working on improving and developing their software. You should regularly check whether there is a new version of the software that provides you with additional benefits. You will find software information and downloads on the product pages of the Hirschmann website

Service Shell

A service technician uses the Service Shell function for maintenance of your functioning device. If you need service support, this function allows the service technician to access internal functions of your device from an external location.

Note: The Service Shell function is for service purposes exclusively. This function allows the access on internal functions of the device. In no case, execute internal functions without service technician instructions. Executing internal functions such as deleting the content of the NVM (non-volatile memory) possibly leads to inoperability of your device.

Permanently disabling the Service Shell

If you do not need the Service Shell, the device allows you to disable the function. In this case you still have the option to configure the device. Though, the service technician has no possibilities to access internal functions of your device to call up additional required information.

Note: Disabling the Service Shell function produces a permanent effect. This process is irreversible.

To reactivate the Service Shell function, send the device back to the manufacturer.

- ☐ To display the Service Shell function, enter `serviceshell` and a space, and then a question mark `?`
- ☐ To permanently deactivate the Shell Service function, enter `serviceshell deactivate` and a space, and press the enter key.

1 Command Structure

The Command Line Interface (CLI) syntax, conventions and terminology are described in this section. Each CLI command is illustrated using the structure outlined below.

1.1 Format

Some commands, such as **`clear vlan,`** do not require parameters. Other commands, such as **`network parms`**, have parameters for which you must supply a value. Parameters are positional — you must type the values in the correct order. Optional parameters will follow required parameters. For example:

Example 1

```
network parms <ipaddr> <netmask> [gateway]
```

- `network parms`
  is the command name.
- `<ipaddr> <netmask>`
  are the required values for the command.
- `[gateway]`
  is the optional value for the command.

Example 2

```
snmp-server location <loc>
```

- `snmp-server location`
  is the command name.
- `<loc>`
  is the required parameter for the command.

Example 3

```
clear vlan
```

- `clear vlan`
  is the command name.

1.1.1 Command

The following conventions apply to the command name:

- The command name is displayed in this document in courier font and is to be typed exactly as shown.
- Once you have entered enough letters of a command name to uniquely identify the command, pressing the ***<Space bar>*** or ***<Tab key>*** will cause the system to complete the word.
- Entering Ctrl-Z will return you to the root level command prompt.

1.1.2 Parameters

Parameters are order dependent.

Parameters are displayed in this document in *italic font*, which are to be replaced with a name or number.

To use spaces as part of parameter name, enclose it in double quotes. For example, the expression "System Name with Spaces" forces the system to accept the spaces.

Parameters may be mandatory values, optional values, choices, or a combination.

- <parameter>. The <> angle brackets indicate that a mandatory parameter is to be entered in place of the brackets and text inside them.
- [parameter]. The [] square brackets indicate that an optional parameter may be entered in place of the brackets and text inside them.
- choice1 | choice2. Vertical bars '|' separate alternative, mutually exclusive, elements.
- The {} curly braces indicate that a parameter must be chosen from the list of choices.
- Braces within square brackets [{}] indicate a required choice within an optional element.

1.1.3 Values

ipaddr

This parameter is a valid IP address. Presently the IP address can be entered in following formats:

a (32 bits)

a.b (8.24 bits)

a.b.c (8.8.16 bits)

a.b.c.d (8.8.8.8 bits)

In addition to these formats, decimal, hexadecimal and octal formats are supported through the following input formats (where n is any valid hexadecimal, octal or decimal number):

0xn (CLI assumes hexadecimal format)

0n (CLI assumes octal format with leading zeros)

n (CLI assumes decimal format)

macaddr

The MAC address format is six hexadecimal numbers separated by colons, for example 00:06:29:32:81:40.

areaid

Area IDs may be entered in dotted-decimal notation (for example, 0.0.0.1). An area ID of 0.0.0.0 is reserved for the backbone. Area IDs have the same form as IP addresses, but are distinct from IP addresses. The IP network address of the sub-netted network may be used for the area ID.

routerid

The value of <router id> must be entered in 4-digit dotted-decimal notation (for example, 0.0.0.1). A router ID of 0.0.0.0 is invalid.

Interface

Valid slot and port number separated by forward slashes. For example, 0/1 represents slot number 0 and port number 1. See “Slot-Port Naming Convention” on

page 45.

Logical Interface Logical slot and port number. This is applicable in the case of a port-channel (LAG) and vlan router interfaces (9/x). The operator can use the logical slot/port to configure the port-channel. See “Slot-Port Naming Convention” on page 45.

Character strings Use double quotation marks to identify character strings, for example, “System Name with Spaces”. An empty string (“”) is not valid.

1.1.4 Conventions

Network addresses are used to define a link to a remote host, workstation or network. Network addresses are shown using the following syntax:

Address Type	Format	Range
ipaddr	192.168.11.110	0.0.0.0 to 255.255.255.255 (decimal)
macaddr	A7:C9:89:DD:A9:B3	hexadecimal digit pairs

Table 1: Network Address Syntax

Double quotation marks such as "System Name with Spaces" set off user defined strings. If the operator wishes to use spaces as part of a name parameter then it must be enclosed in double quotation marks.

Empty strings (““) are not valid user defined strings.

Command completion finishes spelling the command when enough letters of a command are typed to uniquely identify the command word. The command may be executed by typing <enter> (command abbreviation) or the command word may be completed by typing the <tab> or <space bar> (command completion).

The value 'Err' designates that the requested value was not internally accessible.

The value of '-----' designates that the value is unknown.

1.1.5 Annotations

The CLI allows the user to type single-line annotations at the command prompt for use when writing test or configuration scripts and for better readability. The exclamation point (‘!’) character flags the beginning of a comment. The comment flag character can begin a word anywhere on the command line and all input following this character is ignored. Any command line that begins with the character ‘!’ is recognized as a comment line and ignored by the parser.

Some examples are provided below:

```
! Script file for setting the CLI prompt
set prompt example-switch
! End of the script file
```

1.1.6 Special keys

Certain special key combinations speed up use of the CLI. They are listed in this section. Also, help is available for the CLI by typing **HELP:**

BS	delete previous character
Ctrl-A Ctrl-E	go to beginning of line go to end of line
Ctrl-F Ctrl-B	go forward one character go backward one character
Ctrl-D	delete current character
Ctrl-H	display command history or retrieve a command
Ctrl-U, X Ctrl-K	delete to beginning of line delete to end of line
Ctrl-W	delete previous word
Ctrl-T	transpose previous character
Ctrl-P	go to previous line in history buffer
Ctrl-N	go to next line in history buffer
Ctrl-Z	return to root command prompt
Tab, <SPACE>	command-line completion
Exit	go to next lower command prompt
?	list choices

1.1.7 Special characters in scripts

Some of the configuration parameters are strings that can contain special characters. When the switch creates a script from the running configuration (by use of the command #show running-config <scriptname.cli>), these special characters are written to the script with a so-called escape character preceding them. This ensures that when applying the script, these characters are regarded as a normal part of the configuration parameter, not having the special meaning they usually have.

Character (plain)	Meaning, when entered in the CLI
!	Begin of a comment, ! and the rest of the line will be ignored
"	Begin or end of a string that may contain space characters
'	Begin or end of a string that may contain space characters
?	Shows possible command keywords or parameters
\	The backslash is used as an escape character to mask characters that normally have a special meaning

Tab. 2: Special characters

Character (escaped)	Meaning, when entered in the CLI
\!	! becomes part of the string
\"	" becomes part of the string
\'	' becomes part of the string
\?	? becomes part of the string
\\	\ becomes part of the string

Tab. 3: Special characters escaped

The commands with strings that may contain these special characters are listed below.

Note: Not every string is allowed to contain special characters. The string that is output with the escape characters (if necessary) is shown as "...".

Command	Note
!System Description "..."	"At the beginning of the script
!System Version "..."	"At the beginning of the script

Tab. 4: Commands in Privileged Exec mode

Command	Note
snmp-server location "..."	
snmp-server contact "..."	
snmp-server community "..."	
snmp-server community ipaddr <ip> "..."	
snmp-server community ipmask <ip> "..."	
snmp-server community ro "..."	
snmp-server community rw "..."	
no snmp-server community mode "..."	
no snmp-server community "..."	
link-aggregation "..."	
spanning-tree configuration name "..."	
ptp subdomain-name "..."	

Tab. 5: Commands in Global Config mode

Command	Note
name "..."	

Tab. 6: Commands in Interface Config mode

Command	Note
vlan name <n> "..."	

Tab. 7: Commands in VLAN Database mode

When a device creates a script, a human-readable header is included that lists the special characters and the escape characters:

```
!Parameter string escape handling \, 1
!Characters to be preceded with escape char (\): \, !, ", ', ?
```

1.1.8 Secrets in scripts

A configuration may include secrets (e. g., passwords). When creating a script, these secrets are written to it in a scrambled form, not in clear text. These secrets may be up to 31 characters long. The format for a scrambled secret is: ":v1:<scrambled secret>:" (without the quotes (), they were added for readability). v1 denotes the scrambling method (v1 in this case), the value of the scrambled secret is a 64-digit hex string.

The following commands produce scrambled secrets (if necessary):

Command	Note
ip ospf authentication encrypt <secret> <id>	Software L3P
ip ospf authentication simple <secret>	Software L3P
ip rip authentication encrypt <secret> <id>	Software L3E and L3P
ip rip authentication simple <secret>	Software L3E and L3P
ip vrrp <id> authentication simple <secret>	Software L3E and L3P
radius server key acct <ip> <password>	
radius server key auth <ip> <password>	
users passwd <username> <password>	
users snmpv3 encryption <username> des <password>	

Tab. 8: Commands in Global Config mode

Command	Note
area <ip> virtual-link <ip> authentication encrypt <secret> <id>	Encrypted Authentication
area <ip> virtual-link <ip> authentication simple <secret>	Simple Authentication

Tab. 9: Commands in Router OSPF mode (software L3P)

Applying or validating a script requires the following conditions for a scrambled secret, else it will be considered invalid (usually only relevant if a script is edited manually):

- string must not be longer than 64 hex digits
- string must only contain the digits 0-9 and the characters A-F (or a-f)
- string length must be even

1.1.9 Slot-Port Naming Convention

Switch software references physical entities such as cards and ports using a Slot/Port naming convention. This convention is also used to identify certain logical entities such as Link Aggregation (LAG) interfaces.
The slot number has two uses. In the case of physical ports it identifies the card containing the ports. In the case of logical ports it also identifies the type of interface or port.

Physical slot numbers

Physical slot numbers begin with one, and are allocated up to the maximum number of physical slots

Logical slot numbers

Logical slots immediately follow physical slots and identify LAG or router interfaces. For LAG the slot number 8 is used. For VLAN-based interfaces the slot number 9 is used.

The port identifies the specific physical port or logical interface being managed on a given slot.

Physical Ports

The physical ports for each slot are numbered sequentially starting from one.

Logical Interfaces

There are two types of logical interfaces: LAG and VLAN-based routing interfaces.

- LAG interfaces are only used for bridging functions. Each LAG interface consists of a set of up to eight physical ports and is identified by its own slot/port designation.
- VLAN routing interfaces are only used for routing functions.

2 Quick Start up

The CLI Quick Start up details procedures to quickly become acquainted with the software.

2.1 Quick Starting the Switch

- Read the device Installation Guide for the connectivity procedure. In-band connectivity allows access to the software locally or from a remote workstation. The device must be configured with IP information (IP address, subnet mask, and default gateway).
- Turn the Power on.
- Allow the device to load the software until the login prompt appears. The device‘s initial state is called the default mode.
- When the prompt asks for operator login, execute the following steps:
  - Type the word `admin` in the login area. Since a number of the Quick Setup commands require administrator account rights, we recommend logging into an administrator account. Press the enter key.
  - Enter the state on delivery password `private`.
  - Press the enter key.
  - The CLI User EXEC prompt will be displayed.
    User EXEC prompt:
    `(Hirschmann Product) >`
  - Use “enable” to switch to the Privileged EXEC mode from User EXEC.
    Privileged EXEC prompt:
    `(Hirschmann Product) #`
  - Use “configure” to switch to the Global Config mode from Privileged EXEC.
    Global Config prompt:
    `(Hirschmann Product) (Config)#`
  - Use “exit” to return to the previous mode.

2.2 System Info and System Setup

This chapter informs you about:

- Quick Start up Software Version Information
- Quick Start up Physical Port Data
- Quick Start up User Account Management
- Quick Start up IP Address
- Quick Start up Uploading from Switch to Out-of-Band PC Only XMODEM)
- Quick Start up Downloading from Out-of-Band PC to Switch (Only XMODEM)
- Quick Start up Downloading from TFTP Server
- Quick Start up Factory Defaults

Quick Start up Physical Port Data

Command	Details
`show port all` (in Privileged EXEC)	Displays the Ports
	slot/port
	Type - Indicates if the port is a special type of port
	Admin Mode - Selects the Port Control Administration State
	Physical Mode - Selects the desired port speed and duplex mode
	Physical Status - Indicates the port speed and duplex mode
	Link Status - Indicates whether the link is up or down
	Link Trap - Determines whether or not to send a trap when link status changes
	LACP Mode - Displays whether LACP is enabled or disabled on this port.

Table 10: Quick Start up Physical Port Data

Quick Start up User Account Management

Command	Details
`show users` (in Privileged EXEC)	Displays all of the users that are allowed to access the switch
	Access Mode - Shows whether the user is able to change parameters on the switch(Read/Write) or is only able to view them (Read Only). As a factory default, the ‘admin’ user has Read/Write access and the ‘user’ user has Read Only access. There can only be one Read/Write user and up to five Read Only users.
`show loginsession` (in User EXEC)	Displays all of the login session information

Table 11: Quick Start up User Account Management

Command	Details
`users passwd <user-name>` (in Global Config)	Allows the user to set passwords or change passwords needed to login A prompt will appear after the command is entered requesting the users old password. In the absence of an old password leave the area blank. The operator must press enter to execute the command. The system then prompts the user for a new password then a prompt to confirm the new password. If the new password and the confirmed password match a message will be displayed. User password should not be more than eight characters in length. Make sure, that the passwords of the users differ from each other. If two or more users try to choose the same password, the CLI will display an error message.
`copy system:running-config nvram:startup-config` (in Privileged EXEC)	This will save passwords and all other changes to the device. If you do not save the configuration by doing this command, all configurations will be lost when a power cycle is performed on the switch or when the switch is reset.
`logout` (in User EXEC and Privileged EXEC)	Logs the user out of the switch

Table 11: Quick Start up User Account Management

Quick Start up IP Address

To view the network parametes the operator can access the device by the following methods.

- Simple Network Management Protocol - SNMP
- Web Browser

Note: After configuring the network parameters it is advisable to execute the command '`copy system:running-config nvram:startup-config`' to ensure that the configurations are not lost.

Command	Details
`show network` (in User EXEC)	Displays the Network Configurations
	IP Address - IP Address of the switch Default IP is 0.0.0.0
	Subnet Mask - IP Subnet Mask for the switch Default is 0.0.0.0
	Default Gateway - The default Gateway for this switch Default value is 0.0.0.0
	Burned in MAC Address - The Burned in MAC Address used for in-band connectivity
	Network Configurations Protocol (BOOTP/DHCP) - Indicates which network protocol is being used Default is DHCP
	Network Configurations Protocol HiDiscovery - Indicates the status of the HiDiscovery protocol. Default is read-write
	Management VLAN Id - Specifies VLAN id
	Web Mode - Indicates whether HTTP/Web is enabled.
	JavaScript Mode - Indicates whether java mode is enabled. When the user accesses the switch's graphical user interface (web interface) and JavaScript Mode is enabled, the switch's web server will deliver a HTML page that contains JavaScript. Some browsers do not support JavaScript. In this case, a HTML page without JavaScript is necessary. In this case, set JavaScript Mode to disabled. Default: enabled.
`network parms <ipaddr> <net-mask> [gateway]` (in Privileged EXEC)	Sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.
	IP Address range from 0.0.0.0 to 255.255.255.255
	Subnet Mask range from 0.0.0.0 to 255.255.255.255

Table 12: Quick Start up IP Address

Command	Details
	Gateway Address range from 0.0.0.0 to 255.255.255.255

Table 12: Quick Start up IP Address

Quick Start up Downloading from TFTP Server

Before starting a TFTP server download, the operator must complete the Quick Start up for the IP Address.

Command	Details
`copy <url> {nvram:startup-config | system:image}`	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: tftp://ipAddr/filepath/fileName. The nvram:startup-config option downloads the configuration file using tftp and system:image option downloads the code file.

Table 13: Quick Start up Downloading from TFTP Server

Quick Start up Factory Defaults

Command	Details
`clear config` (in Privileged EXEC Mode)	Enter yes when the prompt pops up to clear all the configurations made to the switch.
`copy system:running-config nvram:startup-config`	Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.
`reboot` (or cold boot the switch) (in Privileged EXEC Mode)	Enter yes when the prompt pops up that asks if you want to reset the system. This is the users choice either reset the switch or cold boot the switch, both work effectively.

Table 14: Quick Start up Factory Defaults

3 Mode-based CLI

The CLI groups all the commands in appropriate modes according to the nature of the command. A sample of the CLI command modes are described below. Each of the command modes support specific software commands.

- User Exec Mode
- Privileged Exec Mode
- Global Config Mode
- Vlan Mode
- Interface Config Mode
- Line Config Mode
- Router OSPF Config Mode
- Router RIP Config Mode
- MAC Access-list Config Mode

The Command Mode table captures the command modes, the prompts visible in that mode and the exit method from that mode.

Command Mode	Access Method	Prompt	Exit or Access Next Mode
`User Exec Mode`	This is the first level of access. Perform basic tasks and list system information	`(Hirschmann Product)>`	Enter Logout command
`Privileged Exec Mode`	From the User Exec Mode, enter the `enable` command	`(Hirschmann Product)#`	To exit to the User Exec mode, enter exit or press Ctrl-Z.
`VLAN Mode`	From the Privileged User Exec mode, enter the `vlan database` command	`(Hirschmann Product) (Vlan) #`	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to User Exec mode.
`Global Config Mode`	From the Privileged Exec mode, enter the `configure` command	`(Hirschmann Product) (Config)#`	To exit to the Privileged Exec mode, enter the exit command, or press Ctrl-Z to switch to user exec mode.
`Interface Config Mode`	From the Global Configuration mode, enter the `interface <slot/port>` command	`(Hirschmann Product) (Interface-"if number")#`	To exit to the Global Config mode enter exit. To return to user EXEC mode enter ctrl-Z.

Table 15: Command Mode

Command Mode	Access Method	Prompt	Exit or Access Next Mode
`Line Config Mode`	From the Global Configuration mode, enter the `lineconfig` command	`(Hirschmann Product) (line) #`	To exit to the Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.
`Router OSPF Config Mode`	From the Global Configuration mode, enter the `router ospf` command	`(Hirschmann Product) (Config-router)#`	To exit to the Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.
`Router RIP Config Mode`	From the Global Config mode, enter the `router rip` command	`(Hirschmann Product) (Config-router)#`	To exit to the Global Config mode enter exit. To return to User Exec mode enter ctrl-Z.
`MAC Access-list Config Mode`	From the Global Config mode enter the `mac access-list extended <name>` command.	`(Hirschmann Product) (Config mac-access-list)#`	To exit to the Global Config mode, enter the exit command. To return to the User EXEC mode, enter Ctrl-Z.

Table 15: Command Mode

3.1 Mode-based Topology

The CLI tree is built on a mode concept where the commands are available according to the interface. Some of the modes are depicted in the following figure.

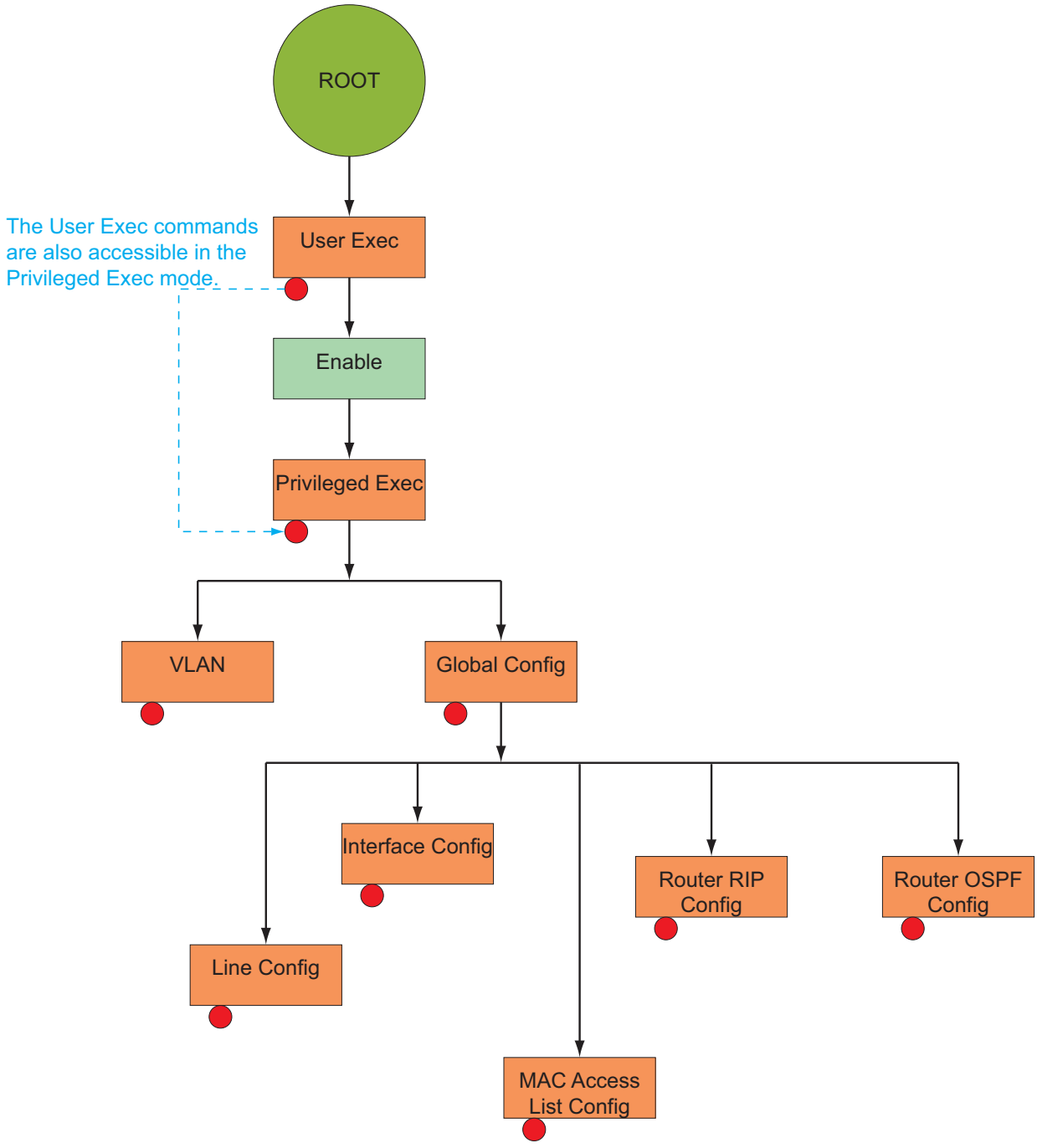


Fig. 1: Mode-based CLI

3.2 Mode-based Command Hierarchy

The CLI is divided into various modes. The Commands in one mode are not available until the operator switches to that particular mode, with the exception of the User Exec mode commands. The User Exec mode commands may also be executed in the Privileged Exec mode.
The commands available to the operator at any point in time depend upon the mode. Entering a question mark (?) at the CLI prompt, displays a list of the available commands and descriptions of the commands.

The CLI provides the following modes:

User Exec Mode

When the operator logs into the CLI, the User Exec mode is the initial mode. The User Exec mode contains a limited set of commands. The command prompt shown at this level is:

```
Command Prompt: (Hirschmann Product)>
```

Privileged Exec Mode

To have access to the full suite of commands, the operator must enter the Privileged Exec mode. Privileged users authenticated by login are able to enter the Privileged EXEC mode. From Privileged Exec mode, the operator can issue any Exec command, enter the VLAN mode orenter the Global Configuration mode . The command prompt shown at this level is:

```
Command Prompt: (Hirschmann Product)#
```

VLAN Mode

This mode groups all the commands pertaining to VLANs. The command prompt shown at this level is:

```
Command Prompt: (Hirschmann Product)(VLAN)#
```

Global Config Mode

This mode permits the operator to make modifications to the running configuration. General setup commands are grouped in this mode. From the Global Configuration mode, the operator can enter the System Configuration mode, the Physical Port Configuration mode, the

Interface Configuration mode, or the Protocol Specific modes specified below. The command prompt at this level is:

```
Command Prompt: (Hirschmann Product)(Config)#
```

From the Global Config mode, the operator may enter the following configuration modes:

Interface Config Mode

Many features are enabled for a particular interface. The Interface commands enable or modify the operation of an interface.

In this mode, a physical port is set up for a specific logical connection operation. The Interface Config mode provides access to the router interface configuration commands. The command prompt at this level is:

```
Command Prompt: (Hirschmann Product)(Interface
<slot/port>)#
```

The resulting prompt for the interface configuration command entered in the Global Configuration mode is shown below:

```
(Hirschmann Product)(Config)# interface 2/1
(Hirschmann Product)(Interface 2/1)#
```

Line Config Mode

This mode allows the operator to configure the console interface. The operator may configure the interface from the directly connected console or the virtual terminal used with Telnet. The command prompt at this level is:

```
Command Prompt: (Hirschmann Product)(Line)#
```

Router OSPF Config Mode:

In this mode, the operator is allowed to access the router OSPF configuration commands. The command prompt at this level is:

```
(Hirschmann Product)(Config)# router ospf
Command Prompt: (Hirschmann Product)(Config
router)#
```

Router RIP Config Mode:

In this mode, the operator is allowed to access the router RIP configuration commands. The command prompt at this level is:

```
(Hirschmann Product)(Config)# router rip
Command Prompt: (Hirschmann Prodct)(Config router)#
```

MAC Access-List Config Mode

Use the MAC Access-List Config mode to create a MAC Access-List and to enter the mode containing Mac Access-List configuration commands.

```
(Hirschmann Product)(Config)# mac-access-list extended <name>
```

```
Command Prompt: (Hirschmann Product)(Config mac-access-list)#
```

3.3 Flow of Operation

This section captures the flow of operation for the CLI:

- The operator logs into the CLI session and enters the User Exec mode. In the User Exec mode the `(Hirschmann Product)`(exec)> prompt is displayed on the screen.

The parsing process is initiated whenever the operator types a command and presses <ENTER>. The command tree is searched for the command of interest. If the command is not found, the output message indicates where the offending entry begins. For instance, command node A has the command `"show spanning-tree"` but the operator attempts to execute the command `"show arpp brief"` then the output message would be `(Hirschmann Product)(exec)> show sspanning-tree^.` `(Hirschmann Product)%Invalid input detected at '^' marker`. If the operator has given an invalid input parameter in the command, then the message conveys to the operator an invalid input was detected. The layout of the output is depicted below:

```
(Hirschmann Product)(exec) #show sspanning-tree
                                              ^
(Hirschmann Product)Invalid input detected at '^' marker.
```

Fig. 2: Syntax Error Message

After all the mandatory parameters are entered, any additional parameters entered are treated as optional parameters. If any of the parameters are not recognized a syntax error message will be displayed.

- After the command is successfully parsed and validated, the control of execution goes to the corresponding CLI callback function.

- For mandatory parameters, the command tree extends till the mandatory parameters make the leaf of the branch. The callback function is only invoked when all the mandatory parameters are provided. For optional parameters, the command tree extends till the mandatory parameters and the optional parameters make the leaf of the branch. However, the call back function is associated with the node where the mandatory parameters are fetched. The call back function then takes care of the optional parameters.
- Once the control has reached the callback function, the callback function has complete information about the parameters entered by the operator.

3.4 “No” Form of a Command

“No” is a specific form of an existing command and does not represent a new or distinct command. Only the configuration commands are available in the “no” form. The behavior and the support details of the “no” form is captured as part of the mapping sheets.

3.4.1 Support for “No” Form

Almost every configuration command has a “no” form. In general, use the no form to reverse the action of a command or reset a value back to the default. For example, the `no shutdown interface` configuration command reverses the shutdown of an interface. Use the command without the keyword ”no“ to re-enable a disabled feature or to enable a feature that is disabled by default.

3.4.2 Behavior of Command Help ("?")

The “no” form is treated as a specific form of an existing command and does not represent a new or distinct command. However, the behavior of the “?” and help text differ for the “no” form (the help message shows only options that apply to the “no” form).

- The help message is the same for all forms of the command. The help string may be augmented with details about the “no” form behavior.
- For the (`no interface`?) and (`no inte`?) cases of the “?”, the options displayed are identical to the case when the “no” token is not specified as in (`interface`) and (`inte`?).

4 CLI Commands: Base

This chapter provides detailed explanation of the Switching commands. The commands are divided into five functional groups:

- Show commands display switch settings, statistics, and other information.
- Configuration commands configure features and options of the switch. For every configuration command, there is a show command that displays the configuration setting.
- Copy commands transfer or save configuration and informational files to and from the switch.
- Clear commands clear
  - some
    (e.g. the ”clear arp-table-switch” command which clears the agent´s ARP table) or
  - all
    (e.g. the ”clear config” command which resets the whole configuration to the factory defaults

This chapter includes the following configuration types:

- System information and statistics commands
- Management commands
- Device configuration commands
- User account management commands
- Security commands
- System utilities
- Link Layer Discovery Protocol Commands
- Simple Network Time Protocol Commands
- Precision Time Protocol Commands
- Power over Ethernet Commands

4.1 System Information and Statistics

4.1.1 show

This command displays the interface's configuration.

Format

```
show [all]
```

Mode

```
Interface Config
```

all

Show all the running configuration parameters on this interface. The configuration parameters will be displayed even if their value is the default value.

4.1.2 show address-conflict

This command displays address-conflict settings.

Format

```
show address-conflict
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.3 show arp switch

This command displays the Address Resolution Protocol cache of the switch.

Format

```
show arp switch
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.4 show bridge address-learning

This command displays the address-learning setting.
The setting can be enable or disable.

Format

```
show bridge address-learning
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.5 show bridge address-relearn-detect

This command displays the Bridge Address Relearn Detection setting and the Bridge Address Relearn Threshold.

Format

```
show bridge address-relearn-detect
```

Mode

```
Privileged EXEC and User EXEC
```

Bridge Address Relearn Detection

Setting can be enable or disable.

Bridge Address Relearn Threshold

The threshold can be 1 to 1024.

4.1.6 show bridge aging-time

This command displays the timeout for address aging.

Format

```
show bridge aging-time
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.7 show bridge duplex-mismatch-detect

This command displays the Bridge Duplex Mismatch Detection setting (Enabled or Disabled).

Format

```
show bridge duplex-mismatch-detect
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.8 show bridge fast-link-detection

This command displays the Bridge Fast Link Detection setting.

Format

```
show bridge fast-link-detection
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.9 show bridge framesize

This command displays the maximum size of frame (packet size) setting.

Format

```
show bridge framesize
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.10 show bridge vlan-learning

This command displays the bridge vlan-learning mode.

Format

```
show bridge vlan-learning
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.11 bridge framesize

Activation of long frames. Configure 1522 or 1632[1)] or 9022[2)] as maximum size of frame (packet size).

Default

```
1522
```

Format

```
bridge framesize { 1522 | 1632[1)] | 9022[2)] }
```

Mode

```
Global Config
```

bridge framesize 1522

Configure 1522 as maximum size of frame (packet size).

bridge framesize 1632 [1)]

Configure 1632 [1)] as maximum size of frame (packet size).

bridge framesize 9022 [1)]

Configure 9022 [2)] as maximum size of frame (packet size, jumbo frames).

[1)] On MACH4000, MACH100, MACH1000 and PowerMICE: `1552`
[2)] Available for the MACH104 and MACH1040 devices.

4.1.12 show config-watchdog

Activating the watchdog enables you to return automatically to the last configuration after a set time period has elapsed. This gives you back your access to the Switch.

Format

```
show config-watchdog
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.13 show device-status

The signal device status is for displaying

- the monitoring functions of the switch,
- the device status trap setting.

Format

```
show device-status
[monitor|state|trap]
```

Mode

```
Privileged EXEC and User EXEC
```

Device status monitor

Displays the possible monitored events and which of them are monitored:
– the detected failure of at least one of the supply voltages.
– the removal of the ACA

– the removal of a media module
– the temperature limits
– the defective link status of at least one port. With the switch, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.
– the loss of Redundancy guarantee.
Ring/network coupling:
– The following conditions are reported in Stand-by mode:
– interrupted control line
– partner device running in Stand-by mode.
HIPER-Ring:
– The following condition is reported in RM mode additionally:
– Ring redundancy guaranteed. Ring redundancy is not monitored in the delivery condition.

Device status state

`Error` The current device status is error.

`No Error` The current device status is no error.

Device status trap

`enabled` A trap is sent if the device status changes.

`disabled` No trap is sent if the device status changes.

4.1.14 show authentication

This command displays users assigned to authentication login lists.

Format

```
show authentication [users <listname>]
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.15 show eventlog

This command displays the event log, which contains error messages from the system. The event log is not cleared on a system reset.

Format

```
show eventlog
```

Mode

```
Privileged EXEC and User EXEC
```

File

The file in which the event originated.

Line

The line number of the event

Task Id

The task ID of the event.

Code

The event code.

Time

The time this event occurred.

Note: Event log information is retained across a switch reset.

4.1.16 show interface

This command displays a summary of statistics for a specific port or a count of all CPU traffic based upon the argument.

Format

```
show interface {<slot/port> |
                ethernet{<slot/port>|switchport} |
                switchport}
```

Mode

```
Privileged EXEC and User EXEC
```

The display parameters, when the argument is ' <slot/port>', is as follows :

Packets Received Without Error

The total number of packets (including broadcast packets and multicast packets) received by the processor.

Packets Received With Error

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Broadcast Packets Received

The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Transmitted Without Error

The total number of packets transmitted out of the interface.

Transmit Packets Errors

The number of outbound packets that could not be transmitted because of errors.

Collisions Frames

The best estimate of the total number of collisions on this Ethernet segment.

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is 'switchport', is as follows :

Packets Received Without Error

The total number of packets (including broadcast packets and multicast packets) received by the processor.

Broadcast Packets Received

The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received With Error

The number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Packets Transmitted Without Error

The total number of packets transmitted out of the interface.

Broadcast Packets Transmitted

The total number of packets that higher-level protocols requested to be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packet Errors

The number of outbound packets that could not be transmitted because of errors.

Address Entries Currently In Use

The total number of Forwarding Database Address Table entries now active on the switch, including learned and static entries.

VLAN Entries Currently In Use

The number of VLAN entries presently occupying the VLAN table.

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds since the statistics for this switch were last cleared.

4.1.17 show interface ethernet

This command displays detailed statistics for a specific port or for all CPU traffic based upon the argument.

Format

```
show interface ethernet {<slot/port> | switchport}
```

Mode

```
Privileged EXEC and User EXEC
```

The display parameters, when the argument is '<slot/port>', are as follows :

Packets Received

Octets Received - The total number of octets of data (including those in bad packets) received on the network (excluding framing bits but including Frame Check Sequence (FCS) octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. ----- The result of this equation is the value Utilization which is the percent utilization of the ethernet segment on a scale of 0 to 100 percent.

Packets Received < 64 Octets - The total number of packets (including bad packets) received that were < 64 octets in length (excluding framing bits but including FCS octets).

Packets Received 64 Octets - The total number of packets (including bad packets) received that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Received 65-127 Octets - The total number of packets (including bad packets) received that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 128-255 Octets - The total number of packets (including bad packets) received that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 256-511 Octets - The total number of packets (including bad packets) received that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 512-1023 Octets - The total number of packets (including bad packets) received that were between 512 and 1023

octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 1024-1518 Octets - The total number of packets (including bad packets) received that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received 1519-1522 Octets - The total number of packets (including bad packets) received that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Received > 1522 Octets - The total number of packets received that were longer than 1522 octets (excluding framing bits, but including FCS octets) and were otherwise well formed.

Packets Received Successfully

Total - The total number of packets received that were without errors.

Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received - The total number of good packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received - The total number of good packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Packets Received with MAC Errors

Total - The total number of inbound packets that contained errors preventing them from being deliverable to a higher-layer protocol.

Jabbers Received - The total number of packets received that were longer than 1518 octets (excluding framing bits, but including FCS octets), and had either a bad Frame Check Sequence (FCS) with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). Note that this definition of jabber is different than the definition in IEEE-802.3 section 8.2.1.5 (10BASE5) and section 10.3.1.4 (10BASE2). These documents define jabber as the condition where any packet exceeds 20 ms. The allowed range to detect jabber is between 20 ms and 150 ms.

Fragments/Undersize Received - The total number of packets received that were less than 64 octets in length (excluding framing bits but including FCS octets).

Alignment Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with a non-integral number of octets.

Rx FCS Errors - The total number of packets received that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

Overruns - The total number of frames discarded as this port was overloaded with incoming packets, and could not keep up with the inflow.

Received Packets not forwarded

Total - A count of valid frames received which were discarded (i.e. filtered) by the forwarding process.

Local Traffic Frames - The total number of frames dropped in the forwarding process because the destination address was located off of this port.

802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

Unacceptable Frame Type - The number of frames discarded from this port due to being an unacceptable frame type.

VLAN Membership Mismatch - The number of frames discarded on this port due to ingress filtering.

VLAN Viable Discards - The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.

Multicast Tree Viable Discards - The number of frames discarded when a lookup in the multicast tree for a VLAN occurs while that tree is being modified.

Reserved Address Discards - The number of frames discarded that are destined to an IEEE 802.1 reserved address and are not supported by the system.

Broadcast Storm Recovery - The number of frames discarded that are destined for FF:FF:FF:FF:FF:FF when Broadcast Storm Recovery is enabled.

CFI Discards - The number of frames discarded that have CFI bit set and the addresses in RIF are in non-canonical format.

Upstream Threshold - The number of frames discarded due to lack of cell descriptors available for that packet's priority level.

Packets Transmitted Octets

Total Bytes - The total number of octets of data (including those in bad packets) transmitted into the network (excluding framing bits but including FCS octets). This object can be used as a reasonable estimate of ethernet utilization. If greater precision is desired, the etherStatsPkts and etherStatsOctets objects should be sampled before and after a common interval. -----

Packets Transmitted 64 Octets - The total number of packets (including bad packets) transmitted that were 64 octets in length (excluding framing bits but including FCS octets).

Packets Transmitted 65-127 Octets - The total number of packets (including bad packets) transmitted that were between 65 and 127 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 128-255 Octets - The total number of packets (including bad packets) transmitted that were between 128 and 255 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 256-511 Octets - The total number of packets (including bad packets) transmitted that were between 256 and 511 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 512-1023 Octets - The total number of packets (including bad packets) transmitted that were between 512 and 1023 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 1024-1518 Octets - The total number of packets (including bad packets) transmitted that were between 1024 and 1518 octets in length inclusive (excluding framing bits but including FCS octets).

Packets Transmitted 1519-1522 Octets - The total number of packets (including bad packets) transmitted that were between 1519 and 1522 octets in length inclusive (excluding framing bits but including FCS octets).

Max Info - The maximum size of the Info (non-MAC) field that this port will receive or transmit.

Packets Transmitted Successfully

Total - The number of frames that have been transmitted by this port to its segment.

Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Errors

Total Errors - The sum of Single, Multiple, and Excessive Collisions.

Tx FCS Errors - The total number of packets transmitted that had a length (excluding framing bits, but including FCS octets) of between 64 and 1518 octets, inclusive, but had a bad Frame Check Sequence (FCS) with an integral number of octets

Oversized - The total number of frames that exceeded the max permitted frame size. This counter has a max increment rate of 815 counts per sec. at 10 Mb/s.

Underrun Errors - The total number of frames discarded because the transmit FIFO buffer became empty during frame transmission.

Transmit Discards

Total Discards - The sum of single collision frames discarded, multiple collision frames discarded, and excessive frames discarded.

Single Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by exactly one collision.

Multiple Collision Frames - A count of the number of successfully transmitted frames on a particular interface for which transmission is inhibited by more than one collision.

Excessive Collisions - A count of frames for which transmission on a particular interface is discontinued due to excessive collisions.

Port Membership - The number of frames discarded on egress for this port due to egress filtering being enabled.

VLAN Viable Discards - The number of frames discarded on this port when a lookup on a particular VLAN occurs while that entry in the VLAN table is being modified, or if the VLAN has not been configured.

Protocol Statistics

BPDUs received - The count of BPDUs (Bridge Protocol Data Units) received in the spanning tree layer.

BPDUs Transmitted - The count of BPDUs (Bridge Protocol Data Units) transmitted from the spanning tree layer.

802.3x Pause Frames Received - A count of MAC Control frames received on this interface with an opcode indicating the PAUSE operation. This counter does not increment when the interface is operating in half-duplex mode.

GVRP PDU's Received - The count of GVRP PDU's received in the GARP layer.

GMRP PDU's received - The count of GMRP PDU's received in the GARP layer.

GMRP PDU's Transmitted - The count of GMRP PDU's transmitted from the GARP layer.

GMRP Failed Registrations - The number of times attempted GMRP registrations could not be completed.

STP BPDUs Transmitted - Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received - Spanning Tree Protocol Bridge Protocol Data Units received

RST BPDUs Transmitted - Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RSTP BPDUs Received - Rapid Spanning Tree Protocol Bridge Protocol Data Units received

MSTP BPDUs Transmitted - Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received - Multiple Spanning Tree Protocol Bridge Protocol Data Units received

Dot1x Statistics

EAPOL Frames Received- The number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted - The number of EAPOL frames of any type that have been transmitted by this authenticator.

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds since the statistics for this port were last cleared.

The display parameters, when the argument is ‘switchport, are as follows :

Octets Received - The total number of octets of data received by the processor (excluding framing bits but including FCS octets).

Total Packets Received Without Error- The total number of packets (including broadcast packets and multicast packets) received by the processor.

Unicast Packets Received - The number of subnetwork-unicast packets delivered to a higher-layer protocol.

Multicast Packets Received - The total number of packets received that were directed to a multicast address. Note that this number does not include packets directed to the broadcast address.

Broadcast Packets Received - The total number of packets received that were directed to the broadcast address. Note that this does not include multicast packets.

Receive Packets Discarded - The number of inbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Octets Transmitted - The total number of octets transmitted out of the interface, including framing characters.

Packets Transmitted without Errors - The total number of packets transmitted out of the interface.

Unicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a subnetwork-unicast address, including those that were discarded or not sent.

Multicast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to a Multicast address, including those that were discarded or not sent.

Broadcast Packets Transmitted - The total number of packets that higher-level protocols requested be transmitted to the Broadcast address, including those that were discarded or not sent.

Transmit Packets Discarded - The number of outbound packets which were chosen to be discarded even though no errors had been detected to prevent their being deliverable to a higher-layer protocol. A possible reason for discarding a packet could be to free up buffer space.

Most Address Entries Ever Used - The highest number of Forwarding Database Address Table entries that have been learned by this switch since the most recent reboot.

Address Entries in Use - The number of Learned and static entries in the Forwarding Database Address Table for this switch.

Maximum VLAN Entries - The maximum number of Virtual LANs (VLANs) allowed on this switch.

Most VLAN Entries Ever Used - The largest number of VLANs that have been active on this switch since the last reboot.

Static VLAN Entries - The number of presently active VLAN entries on this switch that have been created statically.

Dynamic VLAN Entries - The number of presently active VLAN entries on this switch that have been created by GVRP registration.

VLAN Deletes - The number of VLANs on this switch that have been created and then deleted since the last reboot.

Time Since Counters Last Cleared

The elapsed time, in days, hours, minutes, and seconds, since the statistics for this switch were last cleared.

4.1.18 show interface switchport

This command displays data concerning the internal port to the management agent.

Format

```
show interface switchport
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.19 show interface utilization

This command displays the utilization statistics for the entire device.

Format

`show interface utilization`

Mode

`Global Config`

Interface

Display port number in `<slot/port>` notation.

Utilization

Display the utilization on this port.
Possible values: `0..100.00%`

Lower threshold

Display the lower threshold setting for the utilization statistics on this port.
Possible values: `0..100.00%`

Upper threshold

Display the upper threshold setting for the utilization statistics on this port.
Possible values: `0..100.00%`

Alarm condition

Display the alarm condition setting for the utilization statistics on this port.
Possible values: `true`, `false`

4.1.20 show logging

This command displays the trap log maintained by the switch. The trap log contains a maximum of 256 entries that wrap.

Format

```
show logging [buffered | hosts | traplogs |
snmp-requests]
```

Mode

```
Privileged EXEC and User EXEC
```

buffered

Display buffered (in-memory) log entries.

hosts

Display logging hosts.

traplogs

Display trap records.

snmp-requests

Display logging SNMP requests and severity level.

4.1.21 show mac-address-conflict

This command displays the mac-address-conflict configuration.

Format

`show mac-address-conflict`

Mode

`Privileged EXEC and User EXEC`

MAC Address Conflict Detection

The status of the mac-address-conflict configuration.

MAC Address Conflict Detection Operation

Possible values: `enabled`, `disabled`
Default value: `enabled`
The meanings of the values are:
enabled MAC Address Conflict Detection enabled.
The device sends a trap if it detects a packet with its own MAC address in the network.
disabled MAC Address Conflict Detection disabled.
The device disclaims sending a trap if it detects a packet with its own MAC address in the network.

4.1.22 show mac-addr-table

This command displays the forwarding database entries. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional *all* parameter. Alternatively, the administrator can enter a MAC Address to display the table entry for the requested MAC address and all entries following the requested MAC address.

Note: This command displays only learned unicast addresses. For other addresses use the command show mac-filter-table.
See “show mac-filter-table gmrp” on page 248.

Format

```
show mac-addr-table [<macaddr> <1-4042> | all]
```

Mode

```
Privileged EXEC and User EXEC
```

Mac Address

A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Slot/Port

The port which this address was learned.

if Index

This object indicates the ifIndex of the interface table entry associated with this port.

Status

The status of this entry. The meanings of the values are:

Learned The value of the corresponding instance was learned by observing the source MAC addresses of incoming traffic, and is currently in use.

Management The value of the corresponding instance (system MAC address) is also the value of an existing instance of dot1dStaticAddress.

4.1.23 show signal-contact

The signal contact is for displaying

- the manual setting and the current state of the signal contact,
- the monitoring functions of the switch,
- the signal-contacts trap setting.

Format

```
show signal-contact
  [1|2|all [mode|monitor|state|trap]]
```

Mode

`Privileged EXEC and User EXEC`

Signal contact mode

`Auto` The signal contact monitors the functions of the switch which makes it possible to perform remote diagnostics.
A break in contact is reported via the zero-potential signal contact (relay contact, closed circuit).

`Device Status` The signal contact monitors the device-status.

`Manual` This command gives you the option of remote switching the signal contact.

Signal contact monitor

Displays the possible monitored events and which of them are monitored:
– the detected failure of at least one of the supply voltages.
– the removal of the ACA
– the removal of a media module
– the temperature limits
– the defective link status of at least one port. With the switch, the indication of link status can be masked by the management for each port. Link status is not monitored in the delivery condition.
– the loss of Redundancy guarantee.
Ring/network coupling:
– The following conditions are reported in Stand-by mode:
– interrupted control line
– partner device running in Stand-by mode.
HIPER-Ring:
– The following condition is reported in RM mode additionally:
– Ring redundancy guaranteed. Ring redundancy is not monitored in the delivery condition.

Signal contact manual setting

`closed` The signal contact´s manual setting is closed.

`open` The signal contact´s manual setting is open.

Signal contact operating state

`closed` The signal contact is currently closed.

`open` The signal contact is currently open.

Signal contact trap

`enabled` A trap is sent if the signal contact state changes.

`disabled` No trap is sent if the signal contact state changes.

Note: To show the signal contact´s port related settings, use the command show port {<slot/port> | all} (see “show port” on page 256).

4.1.24 show slot

This command is used to display information about slot(s).
For `[slot]` enter the slot ID.

Format

`show slot [slot]`

Mode

`Privileged EXEC`, `Global Config`

Slot

Display the number of the media module slot.

Status

`Full` The media module slot is equipped with a module.
`Empty` The media module slot is not equipped.

Admin State

Note: This feature is available for MS20/MS30, PowerMICE, MACH102 and MACH4000 devices.
`Enable` The media module slot is logically enabled.
`Disable` The media module slot is logically disabled.

Configured Card Model ID

Display the type of the media module.

Card Description

Display the type of the media module.

Product Code

Display the type of the media module.

Pluggable

`Yes` The module is pluggable.
`No` The module is not pluggable.

4.1.25 show running-config

This command is used to display the current setting of different protocol packages supported on the switch. This command displays only those parameters, the values of which differ from default value. The output is displayed in the script format, which can be used to configure another switch with the same configuration.

Format

```
show running-config [all | <scriptname>]
```

Mode

```
Privileged EXEC
```

all

Show all the running configuration on the switch. All configuration parameters will be output even if their value is the default value.

<scriptname>

Script file name for writing active configuration.
Note: Make sure that the file extension is cli, that the file name does not exceed 16 characters, does not start with a dot (.) and does not contain a directory.

4.1.26 show sysinfo

Use this command to display system information for the device, including system-up time.

Format

```
show sysinfo
```

Mode

```
Privileged EXEC and User EXEC
```

Device Status

Displays the latest status for this device.

Alarms

Displays the latest present Alarm for a signal contact.

System Description

Text used to identify this switch.

System Name

Name used to identify the switch.

System Location

Text used to identify the location of the switch. May be up to 31 alpha-numeric characters. The factory default is blank.

System Contact

Text used to identify a contact person for this switch. May be up to 31 alpha-numeric characters. The factory default is blank.

System UpTime

The time in days, hours and minutes since the last switch reboot.

System Date and Time

The system clock´s date and time in local time zone.

System IP Address

The system´s IP address.

Boot Software Release

The boot code´s version number.

Boot Software Build Date

The boot code´s build date.

Operating system Software Release

The operating system´s software version number.

Operating system Software Build Date
The operating system´s software build date.

Running Software Release
The operating system´s software version number.

Running Software Build Date
The operating system´s software build date.

Stored Software Release
The stored operating system´s software version number.

Stored Software Build Date
The stored operating system´s software build date.

Backup Software Release
The backup operating system´s software version number.

Backup Software Build Date
The backup operating system´s software build date.

Backplane Hardware Revision
The hardware´s revision number.

Backplane Hardware Description
The hardware´s device description.

Serial Number (Backplane)
The hardware´s serial number.

Base MAC Address (Backplane)
The hardware´s base MAC address.

Number of MAC Addresses (Backplane)
The number of hardware MAC addresses.

Configuration state
The state of the actual configuration.

Configuration signature
The signature (watermark) of the stored configuration. The signature changes each time the configuration is saved.

Auto Config Adapter, State
The Auto Configuration Adapter's state.

Auto Config Adapter, Serial Number

The Auto Configuration Adapter's serial number (if present and operative).

Factory Hardware Description

The product code (factory hardware description) of the device, e.g. MAR1020-99TTTTMMMMTTTTTTTTTTTTTTTTUC9HPHH

Fan Status

The status of the MACH4000 fan.

Power Supply Information

The status of the power supplies.

Media Module Information

The description of each media module
– Description: media module type,
– Serial Number of the media modul (if available),
SFP Information:
– SFP Part ID: SFP type (if available),
– SFP Serial No. of the SFP module (if available),
– SFP Supported: yes/no,
– SFP Temperature (°C, F),
– SFP Tx Pwr, SFP transmit power (dBm / mW),
– SFP Rx Pwr, SFP receive power (dBm / mW)

CPU Utilization

The utilization of the central processing unit.

Average CPU Utilization

The average utilization of the central processing unit.

Flashdisk

Free memory on flashdisk (in Kbytes).

4.1.27 show temperature

Note: The command is available for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH100, MACH1000, PowerMICE, MACH4000 and OCTOPUS devices.

This command displays the lower and upper temperature limit for sending a trap.

Format

```
show temperature
```

Mode

```
Privileged EXEC and User EXEC
```

4.1.28 utilization alarm-threshold

Use this command to add the alarm threshold value for monitoring bandwidth utilization of the interface.

Format

```
utilization alarm-threshold
     {lower <0..10000> | upper <0..10000>}
```

Mode

```
Interface Config
```

lower

Enter lower utilization alarm threshold in the range of `0..10000` where `10000` represents 100%.

upper

Enter upper utilization alarm threshold in the range of `0..10000` where `10000` represents 100%.

4.2 Debug Commands

4.2.1 debug tcpdump help

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.
This command displays the supported options and expressions for the tcpdump command.

Format

```
debug tcpdump help
```

Mode

```
Privileged EXEC
```

4.2.2 debug tcpdump start cpu

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.
This command starts a capture on the CPU interface with the options and expressions in the <command> parameter.
Without the <command> parameter this command starts a capture on the CPU interface using default options and no explicit filtering.

Format

```
debug tcpdump start cpu <command>
```

Mode

```
Privileged EXEC
```

4.2.3 debug tcpdump start cpu filter

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.
This command starts a capture on the CPU interface with the options and expressions in the filter file.

Format

```
debug tcpdump start cpu filter <capturefilter>
```

Mode

```
Privileged EXEC
```

4.2.4 debug tcpdump stop

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.
This command stops a running capture on the CPU interface.

Format

```
debug tcpdump stop
```

Mode

```
Privileged EXEC
```

4.2.5 debug tcpdump filter show

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.
This command shows a saved filter file stored in flash memory.

Format

```
debug tcpdump filter show <capturefilter>
```

Mode

```
Privileged EXEC
```

4.2.6 debug tcpdump filter list

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.
This command lists all saved filter files stored in flash memory.

Format

```
debug tcpdump filter list
```

Mode

```
Privileged EXEC
```

4.2.7 debug tcpdump filter delete

Run diagnostics commands. With the TCP dump you run a packet analyzer for capturing network traffic.
This command removes a saved filter file from the flash memory.

Format

```
debug tcpdump filter delete <capturefilter>
```

Mode

```
Privileged EXEC
```

4.3 Management VLAN Commands

4.3.1 network mgmt_vlan

This command configures the Management VLAN ID. If you enter the VLAN ID “0” , the agent can be accessed by all VLANs.

Default

1

Format

```
network mgmt_vlan <0-4042>
```

Mode

```
Privileged EXEC
```

4.4 Class of Service (CoS) Commands

This chapter provides a detailed explanation of the QoS CoS commands. The following commands are available.

The commands are divided into these different groups:

- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display device settings, statistics and other information.

Note: The 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode is applied to all interfaces.

4.4.1 classofservice dot1p-mapping

This command maps an 802.1p priority to an internal traffic class for a device when in ‘Global Config’ mode. The number of available traffic classes may vary with the platform. Userpriority and trafficclass can both be the range from 0-7. The command is only available on platforms that support priority to traffic class mapping on a ‘per-port’ basis, and the number of available traffic classes may vary with the platform.

Format

```
classofservice dot1p-mapping
       <userpriority> <trafficclass>
```

Mode

```
Global Config or Interface Config
```

userpriority

Enter the 802.1p priority (0-7).

trafficclass

Enter the traffic class to map the 802.1p priority (0-3).

no classofservice dot1p-mapping

This command restores the default mapping of the 802.1p priority to an internal traffic class.

Format

```
no classofservice dot1p-mapping
```

Modes

```
Global Config or Interface Config
```

4.4.2 classofservice ip-dscp-mapping

This command maps an IP DSCP value to an internal traffic class. The <ipdscp> value is specified as either an integer from 0 to 63, or symbolically through one of the following keywords: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef.

Format

```
classofservice ip-dscp-mapping
                              <ipdscp> <trafficclass>
```

Mode

```
Global Config
```

ipdscp

Enter the IP DSCP value in the range of 0 to 63 or an IP DSCP keyword (af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, be, cs0, cs1, cs2, cs3, cs4, cs5, cs6, cs7, ef).

trafficclass

Enter the traffic class to map the 802.1p priority (0-3).

no classofservice ip-dscp-mapping

This command restores the default mapping of the IP DSCP value to an internal traffic class.

Format

```
no classofservice dot1p-mapping
```

Modes

```
Global Config
```

4.4.3 classofservice trust

This command sets the class of service trust mode of an interface. The mode can be set to trust one of the Dot1p (802.1p) or IP DSCP packet markings.

Note: In `trust ip-dscp` mode the switch modifies the vlan priority for outgoing frames according to
– the DSCP mapping and VLAN mapping table
(PowerMICE, MACH104, MACH1040, MACH4000)
– the fix mapping table
(see Reference Manual „GUI Graphical User Interface“ (Web-based Interface) for further details).

Format

`classofservice trust dot1p | ip-dscp`

Mode

`Global Config` or
`Interface Config`
(PowerMICE, MACH104, MACH1040, MACH4000)

no classofservice trust

This command sets the interface mode to untrusted, i.e. the packet priority marking is ignored and the default port priority is used instead.

Format

`no classofservice trust`

Modes

`Global Config` or
`Interface Config`
(PowerMICE, MACH104, MACH1040, MACH4000)

4.4.4 show classofservice dot1p-mapping

This command displays the current 802.1p priority mapping to internal traffic classes for a specific interface. The slot/port parameter is required on platforms that support priority to traffic class mapping on a ‘per-port’ basis.

Platforms that support priority to traffic class mapping on a per-port basis:

Format

```
show classofservice dot1p-mapping
```

Platforms that do not support priority to traffic class mapping on a per-port basis:

Format

```
Show classofservice dot1p-mapping
```

Mode

```
Privileged EXEC and User EXEC
```

4.4.5 show classofservice ip-dscp-mapping

This command displays the current IP DSCP mapping to internal traffic classes for the global configuration settings.

Format

```
show classofservice ip-dscp-mapping [<slot/port>]
```

Mode

```
Privileged EXEC
```

The following information is repeated for each user priority.

IP DSCP

The IP DSCP value.

Traffic Class

The traffic class internal queue identifier to which the IP DSCP value is mapped.

slot/port

Valid slot and port number separated by forward slashes.

4.4.6 show classofservice trust

This command displays the current trust mode for the specified interface. The slot/port parameter is optional. If specified, the trust mode of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format

```
show classofservice trust [slot/port]
```

Mode

```
Privileged EXEC
```

Class of Service Trust Mode

The current trust mode: Dot1p, IP DSCP, or Untrusted.

Untrusted Traffic Class

The traffic class used for all untrusted traffic. This is only displayed when the COS trust mode is set to 'untrusted'.

slot/port

Valid slot and port number separated by forward slashes.

4.4.7 vlan port priority all

This command configures the port priority assigned for untagged packets for all ports presently plugged into the device. The range for the *priority* is 0..7. Any subsequent per port configuration will override this configuration setting.

Format

```
vlan port priority all <priority>
```

Mode

```
Global Config
```

4.4.8 vlan priority

This command configures the default 802.1p port priority assigned for untagged packets for a specific interface. The range for the *priority* is 0..7.

Default

0

Format

```
vlan priority <priority>
```

Mode

```
Interface Config
```

4.4.9 dvlan-tunnel ethertype

Note: This command is available for the RS20/RS30/RS40, RSB20, MS20/MS30, RSR20/RSR30, MACH100, MACH104, MACH1000, MACH1040,

MACH4002-24G/48G (XG), OCTOPUS, OS20/OS30 devices.

This command configures the ethertype for all core ports. The ethertype may have the values of 802.1q, vMAN or custom. The configured ethertype is used for VLAN classification on all ports which are configured as core ports.

Default

```
802.1Q
```

Format

```
dvlan-tunnel ethertype
                  {802.1Q | vman | custom <0-65535>}
```

Mode

```
Global Config
```

802.1Q

Configure the etherType as 0x8100.

custom

Custom configure the etherType for the DVlan tunnel.
Range for the optional value of the custom ethertype: 0 to 65535.

vman

Configure the etherType as 0x88A8.

4.4.10 mode dvlan-tunnel

Note: This command is available for the RS20/RS30/RS40, RSB20, MS20/MS30, RSR20/RSR30, MACH100, MACH104, MACH1000, MACH1040, MACH4002-24G/48G (XG), OCTOPUS, OS20/OS30 devices.

Use this command to configure the port either as core port or access port.

Default

```
Disabled
```

Format

```
mode dvlan-tunnel {access | core}
```

Mode

```
Interface Config
```

access

Configure this port as a customer port.

core

Configure this port as a provider network port.

no mode dvlan-tunnel

Use this command to configure the port as normal switch port and to disable the DVLAN tunneling.

Default

```
Disabled
```

Format

```
no mode dvlan-tunnel
```

Mode

```
Interface Config
```

4.4.11 show dvlan-tunnel

Note: This command is available for the RS20/RS30/RS40, RSB20, MS20/MS30, RSR20/RSR30, MACH100, MACH104, MACH1000, MACH1040, MACH4002-24G/48G (XG), OCTOPUS, OS20/OS30 devices.

Use this command to display the DVLAN-Tunnel mode and used ether-type for the specified interface(s).

Format

```
show dvlan-tunnel [interface {slot/port} | all]
```

Modes

```
Privileged EXEC
User EXEC
```

<slot/port>

Enter an interface in slot/port format.

all

Enter 'all' for all interfaces.

Interface

Display the number of the interface (slot/port).
Possible values (example): `1/1, 1/2, 2/1, 2/2, 2/3`.

Mode

Display the DVLAN-Tunnel mode.
Possible values: `normal`, ...

EtherType

Display the used ether-type.
Possible values: `802.1Q, vman, custom`.

4.5 Link Aggregation(802.3ad) Commands

4.5.1 link-aggregation staticcapability

This command enables the support of link-aggregations (static LAGs) on the device. By default, the static capability for all link-aggregations is disabled.

Default

disabled

Format

```
link-aggregation staticcapability
```

Mode

```
Global Config
```

- **no link-aggregation staticcapability**
  This command disables the support of static link-aggregations (LAGs) on the device.

Default

disabled

Format

```
no link-aggregation staticcapability
```

Mode

```
Global Config
```

4.5.2 show link-aggregation brief

This command displays the static capability of all link-aggregations (LAGs) on the device as well as a summary of individual link-aggregations.

Format

```
show link-aggregation brief
```

Mode

```
Privileged EXEC and User EXEC
```

Static Capability

This field displays whether or not the device has static capability enabled.

For each link-aggregation the following information is displayed:

Name

This field displays the name of the link-aggregation.

Link State

This field indicates whether the link is up or down.

Mbr Ports

This field lists the ports that are members of this link-aggregation, in <slot/port> notation.

Max. num. of LAGs

Displays the maximum number of concurrently configured link aggregations on this device.

Slot no. for LAGs

Displays the slot number for all configured link aggregations on this device.

4.6 Management Commands

These commands manage the switch and show current management settings.

4.6.1 telnet

This command establishes a new outbound telnet connection to a remote host. The host value must be a valid IP address. Valid values for port should be a valid decimal integer in the range of 0 to 65535, where the default value is `23`. If [debug] is used, the current telnet options enabled is displayed. The optional line parameter sets the outbound telnet operational mode as 'line-mode', where by default, the operational mode is 'character mode'. The echo option enables local echo and only takes effect when the local switch is accessed via the serial connection (V.24).

Format

```
telnet <host> <port> [debug] [line] [echo]
```

Mode

```
Privileged EXEC and User EXEC
```

4.6.2 transport input telnet

This command regulates new telnet sessions. If sessions are enabled, new telnet sessions can be established until there are no more sessions available. If sessions are disabled, no new telnet sessions are established. An established session remains active until the session is ended or an abnormal network error ends the session.

Default

enabled

Format

```
transport input telnet
```

Mode

```
Line Config
```

no transport input telnet

This command disables telnet sessions. If sessions are disabled, no new telnet sessions are established.

Format

```
no transport input telnet
```

Mode

```
Line Config
```

4.6.3 transport output telnet

This command regulates new outbound telnet connections. If enabled, new outbound telnet sessions can be established until it reaches the maximum number of simultaneous outbound telnet sessions allowed.
If disabled, no new outbound telnet session can be established. An established session remains active until the session is ended or an abnormal network error ends it.

Default

enabled

Format

```
transport output telnet
```

Mode

```
Line Config
```

no transport output telnet

This command disables new outbound telnet connections. If disabled, no new outbound telnet connection can be established.

Format

```
no transport output telnet
```

Mode

```
Line Config
```

4.6.4 session-limit

This command specifies the maximum number of simultaneous outbound telnet sessions. A value of 0 indicates that no outbound telnet session can be established.

Default

4

Format

`session-limit <0-5>`

Mode

`Line Config`

no session-limit

This command sets the maximum number of simultaneous outbound telnet sessions to the default value.

Format

`no session-limit`

Mode

`Line Config`

4.6.5 session-timeout

This command sets the telnet session timeout value.The timeout value unit of time is minutes.

Default

`5`

Format

`session-timeout <1-160>`

Mode

`Line Config`

no session-timeout

This command sets the telnet session timeout value to the default. The timeout value unit of time is minutes.

Format

`no session-timeout`

Mode

`Line Config`

4.6.6 bridge address-learning

To enable you to observe the data at all the ports, the Switch allows you to disable the learning of addresses. When the learning of addresses is disabled, the Switch transfers all the data from all ports to all ports. The default value is `enable`.

Format

`bridge address-learning {disable|enable}`

Mode

`Global Config`

4.6.7 bridge address-relearn detect operation

This command enables or disables Bridge Address Relearn Detection. The default value is `disable`.

Default

Disabled

Format

```
bridge address-relearn detect operation
{disable|enable}
```

Mode

`Global Config`

4.6.8 bridge address-relearn detect threshold

This command defines the value of relearned addresses to signal address relearn threshold exceeded.
The default relearn threshold is 1. Possible values to configure threshold count are `1` to `1024`.

Default

1

Format

```
bridge address-relearn-detect threshold <value>
```

Mode

`Global Config`

value

`1` to `1024`

4.6.9 bridge aging-time

This command configures the forwarding database address aging timeout in seconds.

Default

30

Format

`bridge aging-time <10-630>`

Mode

`Global Config`

Seconds

The <seconds> parameter must be within the range of 10 to 630 seconds.

no bridge aging-time

This command sets the forwarding database address aging timeout to 30 seconds.

Format

`no bridge aging-time`

Mode

`Global Config`

4.6.10 bridge fast-link-detection

This command enables or disables the Bridge Fast Link Detection.

Default

Enabled

Format

```
bridge fast-link-detection {disable|enable}
```

Mode

```
Global Config
```

4.6.11 bridge duplex-mismatch-detect operation

This command enables or disables Bridge Duplex Mismatch Detection.

Reasons for Duplex Mismatch can be:
- A local port is configured to fix full-duplex.
- A port is configured to auto-negotiation and has negotiated HalfDuplex-Mode.

Duplex Mismatch can be excluded, when the local port is configured to auto-negotiation and duplex mode is negotiated to full-duplex.

Note: If counters and configuration settings indicate a Duplex Mismatch, the reason can also be a bad cable and/or EMI.

Default

Enabled

Format

```
bridge duplex-mismatch-detect operation
{disable|enable}
```

Mode

```
Global Config
```

4.6.12 bridge vlan-learning

With ”independent” you set the Shared VLAN Learning mode to Independent. The switch will treat equal MAC source addresses from different VLANs as separate addresses.
With ”shared” you set the Shared VLAN Learning mode to Shared. The switch will treat equal MAC source addresses from different VLANs as the same adress.

Format

```
bridge vlan-learning {independent|shared}
```

Mode

```
Global Config
```

4.6.13 digital-input

This command configures the MICE IO-Module digital inputs.

Format

```
digital-input
  admin-state {enable | disable}
  refresh-interval <refresh-interval>
  log-event {all | <slot/input>} {enable|disable}
  snmp-trap {all | <slot/input>} {enable|disable}
```

Mode

```
Global Config
```

admin-state

This command enables or disables the polling task for digital inputs of the MICE IO-Module. When disabled, no event logging or SNMP traps will work. Default value: `disable`.

`disable` Disable the IO-Module digital inputs admin state.

`enable` Enable the IO-Module digital inputs admin state.

refresh-interval

This command configures the digital inputs refresh interval. Each input configured for event logging or SNMP traps is polled with this interval.

`<refresh-interval>` The refresh interval is in the range of 1..10 seconds. Default value: `1`.

log-event

This command enables or disables the event logging of input status changes for one or all digital inputs. Default value: `disable`.
The input state will be checked according to the interval set with IO-`<refresh-interval>`.

`all` Configure the IO-Module event logging for all digital inputs.

`<slot/input>` Configure the IO-Module event logging for a single digital input.

`disable` Disable event logging for digital input status changes.

`enable` Enable event logging for digital input status changes.

snmp-trap

This command enables or disables the sending of SNMP traps in case of input status changes for one or all digital inputs. Default value: `disable`.
The trap will be sent to all SNMP trap receivers configured with snmptrap.
The input state will be checked according to the interval set with IO-`<refresh-interval>`.

`all` Configure the IO-Module SNMP trap for all digital inputs.

`<slot/input>` Configure the IO-Module SNMP trap for a single digital input.

`disable` Disable SNMP traps for digital input status changes.

`enable` Enable SNMP traps for digital input status changes.

4.6.14 digital-output

This command configures the IO-Module digital outputs.

Format

```
digital-output
  admin-state {enable | disable}
  refresh-interval <refresh-interval>
  retry-count <refresh-interval>
  log-event {all | <slot/output>} {enable|disable}
  snmp-trap {all | <slot/output>} {enable|disable}
  mirror all | <slot>/<output> {disable |
                  from <IPaddress> <slot>/<input>}
```

Mode

`Global Config`

admin-state

This command enables or disables the polling task for digital outputs of the MICE IO-Module. When disabled, no event logging or SNMP traps will work. Default value: `disable`.

`disable` Disable the IO-Module digital outputs admin state.

`enable` Enable the IO-Module digital outputs admin state.

refresh-interval

This command configures the IO-Module digital outputs refresh interval. Each output configured for input mirroring is refreshed (input is polled) with this interval.

`<refresh-interval>` The refresh interval is in the range of 1..10 seconds. Default value: `1`.

retry-count

This command configures the number of retry counts for setting digital outputs of the MICE IO-Module. Each output configured for input mirroring is set to the default value (low) when after the number of configured retries no SNMP get request was answered.

`<refresh-interval>` The refresh interval is in the range of 1..10 seconds. Default value: `1`.

log-event

This command enables or disables the event logging of output status changes for one or all digital outputs. Default value: `disable`.
The output state will be checked according to the interval set with IO-

`<refresh-interval>`.
Configure the IO-Module event logging for one or all digital outputs.
`all` Configure the IO-Module event logging for all digital outputs.
`<slot/output>` Configure the IO-Module event logging for a single digital output.
`disable` Disable event logging for digital output status changes.
`enable` Enable event logging for digital output status changes.

snmp-trap

This command enables or disables the sending of SNMP traps in case of output status changes for one or all digital outputs. Default value: `disable`.
The trap will be sent to all SNMP trap receivers configured with snmptrap.
The output state will be checked according to the interval set with IO-`<refresh-interval>`.
`all` Configure the IO-Module SNMP trap for all digital outputs.
`<slot/output>` Configure the IO-Module SNMP trap for a single digital output.
`disable` Disable SNMP traps for digital output status changes.
`enable` Enable SNMP traps for digital output status changes.

mirror

Configure the IO-Module mirroring for one or all digital outputs.
This command determines the input mirrored to the currently selected output.
To disable mirroring, the following commands are equivalent:

```
digital-output mirror 1/2 disable
digital-output mirror 1/2 from 0.0.0.0 1/1
```

`<all>`: Configure the IO-Module mirroring for all digital outputs.

`<slot/output>`: Configure the IO-Module mirroring for a single digital output. The <slot> value determines the IO-module slot number on the device with the selected IP address.

`disable`: Disable the IO-Module mirroring for a single digital output.

`from`: Enable the IO-Module mirroring for a single digital output from <IP-address> <slot/input>

`<IPaddress>`: The IP address value determines the IP address used for reading the input value. Use IP address 127.0.0.1 or the system IP address to mirror inputs from a local IO module. When IP address is 0.0.0.0 no input is mirrored to the output (the output value is set to 'low'). Default value: `0.0.0.0`.

`<slot/input>`: The <input> value determines the input number on this device. Default value: `1/1`.

4.6.15 show digital-input

This command shows the input value or configuration from all available digital inputs of the MICE I/O Module.

Format

`show digital-input`

Mode

`Global Config`

Digital Input System Information:

Admin State

Show the IO-Module digital inputs Admin State.
Possible values: `Disabled, Enabled`.

Refresh Interval [s]

Show the IO-Module digital inputs Refresh Interval in seconds.
Value range: `1..10`.

Digital Input Information:

Input

Show numbers of the IO-Module digital input.
Possible values (example): `1/1, 1/2, 1/3, 1/4, 3/1, 3/2, 3/3, 3/4`

Value

Show the value of the IO-Module digital inputs.
Possible values: `Not available, High, Low`.

Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital inputs.
Possible values: `Disabled, Enabled`.

SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital inputs.
Possible values: `Disabled, Enabled`.

4.6.16 show digital-input config

This command shows the IO-Module digital inputs global configuration.

Format

```
show digital-input config
```

Mode

```
Global Config
```

Digital Input System Information:

Admin State

Show the IO-Module digital inputs Admin State.
Possible values: `Disabled, Enabled`.

Refresh Interval [s]

Show the IO-Module digital inputs Refresh Interval in seconds.
Value range: `1..10`.

4.6.17 show digital-input all

This command shows the IO-Module value or configuration for all inputs.

Format

```
show digital-input all {all | config | value}
```

Mode

```
Global Config
```

all

Show the IO-Module configuration and value for all inputs

config

Show the IO-Module configuration for all inputs.

value

Show the IO-Module value for all inputs.

Digital Input Information:

Input

Show numbers of the IO-Module digital input.
Possible values (example): `1/1, 1/2, 1/3, 1/4, 3/1, 3/2, 3/3, 3/4`

Value

Show the value of the IO-Module digital inputs.
Possible values: `Not available, High, Low`.

Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital inputs. Possible values: `Disabled, Enabled`.

SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital inputs. Possible values: `Disabled, Enabled`.

4.6.18 show digital-input <slot/input>

This command shows the IO-Module value or configuration for a single input.

Format

```
show digital-input <slot/input>
                                {all | config | value}
```

Mode

`Global Config`

all

Show the IO-Module configuration and value for one input.

config

Show the IO-Module configuration for one input.

value

Show the IO-Module value for one input.

Digital Input <slot/input> Value

Show the value of the IO-Module digital input.
Possible values: `Not available, High, Low`.

Digital Input <slot/input> Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital input. Possible values: `Disabled, Enabled`.

Digital Input <slot/input> SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital input. Possible values: `Disabled, Enabled`.

4.6.19 show digital-output

This command shows the output value or configuration from all available digital outputs of the MICE I/O Module.

Format

```
show digital-output
```

Mode

```
Global Config
```

Digital output System Information:

Admin State

Show the IO-Module digital outputs Admin State.
Possible values: `Disabled, Enabled`.

Refresh Interval [s]

Show the IO-Module digital outputs Refresh Interval in seconds.
Value range: `1..10`.

Retry Count

Show the value of the IO-Module digital outputs Retry count.
Value range: `1..10`.

Digital output Information:

Output

Show numbers of the IO-Module digital output.
Possible values (example): `1/1, 1/2, 1/3, 1/4, 3/1, 3/2, 3/3, 3/4`

Value

Show the value of the IO-Module digital outputs.
Possible values: `Not available, High, Low`.

Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital outputs.
Possible values: `Disabled, Enabled`.

SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital outputs.
Possible values: `Disabled, Enabled`.

Mirror from IP

Show the IP address used for reading the input value.
Possible values: `None, a.b.c.d` (valid IP address).

Input

Show the input number of the device used for reading the input value.
Possible values (example): `1/1, 1/2, 1/3, 1/4, 3/1, 3/2, 3/3, 3/4`

4.6.20 show digital-output config

This command shows the IO-Module digital outputs global configuration.

Format

```
show digital-output config
```

Mode

```
Global Config
```

Digital output System Information:

Admin State

Show the IO-Module digital outputs Admin State.
Possible values: `Disabled, Enabled`.

Refresh Interval [s]

Show the IO-Module digital outputs Refresh Interval in seconds.
Value range: `1..10`.

Retry Count

Show the value of the IO-Module digital outputs Retry count.
Value range: `1..10`.

4.6.21 show digital-output all

This command shows the IO-Module value or configuration for all outputs.

Format

```
show digital-output all {all | config | value}
```

Mode

```
Global Config
```

all

Show the IO-Module configuration and value for all outputs

config

Show the IO-Module configuration for all outputs.

value

Show the IO-Module value for all outputs.

Digital output Information:

output

Show numbers of the IO-Module digital output.
Possible values (example): `1/1, 1/2, 1/3, 1/4, 3/1, 3/2, 3/3, 3/4`

Value

Show the value of the IO-Module digital outputs.
Possible values: `Not available, High, Low`.

Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital outputs. Possible values: `Disabled, Enabled`.

SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital outputs. Possible values: `Disabled, Enabled`.

Mirror from IP

Show the IP address used for reading the input value.
Possible values: `None, a.b.c.d` (valid IP address).

Input

Show the input number of the device used for reading the input value.
Possible values (example): 1`/1, 1/2, 1/3, 1/4, 3/1, 3/2, 3/3, 3/4`

4.6.22 show digital-output <slot/output>

This command shows the IO-Module value or configuration for a single output.

Format

```
show digital-output <slot/output>
                                {all | config | value}
```

Mode

`Global Config`

all

Show the IO-Module configuration and value for one output.

config

Show the IO-Module configuration for one output.

value

Show the IO-Module value for one output.

Digital output <slot/output> Value

Show the value of the IO-Module digital output.
Possible values: `Not available, High, Low, Invalid`.

Digital output <slot/output> Log-Event

Show if Event logging is enabled or disabled for the IO-Module digital output.
Possible values: `Disabled, Enabled`.

Digital output <slot/output> SNMP-trap

Show if SNMP traps are enabled or disabled for the IO-Module digital output.
Possible values: `Disabled, Enabled`.

Digital Output <slot/output> Mirror from IP

Show the IP address used for reading the input value.
Possible values: `Not configured, a.b.c.d` (valid IP address).

4.6.23 ethernet-ip

This command controls the EtherNet/IP function on the switch.
Detailed information you can find in the User Manual Industrial Protocols.

Default

depends on the order code (standard = disable)

Format

`ethernet-ip admin-state {enable | disable}`

Mode

`Global Config`

Admin-state

`disable:` Disables the EtherNet/IP function on this device.
Note: The relevant MIB objects are still accessible.
`enable:` Enables the EtherNet/IP function on this device.

4.6.24 network mgmt-access add

This command is used to configure the restricted management access feature (RMA).
It creates a new empty entry at the <index> (if you enter the command with parameter <index>) or at the next free index (if you enter the command without parameter <index>).

Format

```
network mgmt-access add [index]
```

Mode

```
Global Config
```

[index]

Index of the entry in the range 1..16.

4.6.25 network mgmt-access delete

This command is used to configure the restricted management access feature (RMA).
It deletes an existing entry with <index>.

Format

```
network mgmt-access delete <index>
```

Mode

```
Global Config
```

<index>

Index of the entry in the range 1..16.

4.6.26 network mgmt-access modify

This command is used to configure the restricted management access feature (RMA).
The command modifies an existing rule with <index> to change IP address, net mask and allowed services.

Format

```
network mgmt-access modify <index>
                        { ip <address> |
                          mask <netmask> |
                          http {enable | disable} |
                          https {enable | disable} |
                          snmp {enable | disable} |
                          telnet {enable | disable} |
                          ssh {enable |disable } }
```

Mode

Global Config

<index>

Index of the entry in the range 1..16.

<ip>

Configure IP address which should have access to management

<mask>

Configure network mask to allow a subnet for management access.

<http>

Configure if HTTP is allowed to have management access.

<https>

Configure if HTTPS is allowed to have management access.

<snmp>

Configure if SNMP is allowed to have management access.

<telnet>

Configure if TELNET is allowed to have management access.

<ssh>

Configure if SSH is allowed to have management access.

enable

Allow the service to have management access.

disable

Do not allow the service to have management access.

4.6.27 network mgmt-access operation

This command is used to configure the restricted management access feature (RMA).
It enables or disables the service to have management access. The default value is `disable`.

Format

```
network mgmt-access operation {disable|enable}
```

Mode

```
Global Config
```

enable

Enable the restricted management access function globally.

disable

Disable the restricted management access function globally.

4.6.28 network mgmt-access status

This command is used to configure the restricted management access feature (RMA).
It activates/deactivates an existing rule with `<index>`.

Format

```
network mgmt-access status <index>
                                    {enable | disable}
```

Mode

```
Global Config
```

<index>

Index of the entry in the range 1..16.

enable

Allow the service to have management access.

disable

Do not allow the service to have management access.

4.6.29 network parms

This command sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.

Format

```
network parms <ipaddr> <netmask> [gateway]
```

Mode

```
Privileged EXEC
```

4.6.30 network protocol

This command specifies the network configuration protocol to be used.
If you modify this value, change is effective immediately after you saved your changes.
The parameter `bootp` indicates that the switch periodically sends requests to a Bootstrap Protocol (BootP) server or a DHCP server until a response is received.
`none` indicates that the switch should be manually configured with IP information.

Independently of the BootP and DHCP settings, HiDiscovery can be configured as an additional protocol.

Default

DHCP

Format

```
network protocol {none | bootp | dhcp | hidiscovery
{off | read-only | read-write}}
```

Mode

`Privileged EXEC`

4.6.31 network priority

This command configures the VLAN priority or the IP DSCP value for outgoing management packets. The <ipdscp> is specified as either an integer from 0-63, or symbolically through one of the following keywords: af11,af12,af13,af21,af22,af23,af31,af32,af33,af41,af42,af43,be,cs0, cs1, cs2,cs3,cs4,cs5,cs6,cs7,ef.

Default

0 for both values

Format

```
network priority {dot1p-vlan <0-7> |
ip-dscp <ipdscp> }
```

Mode

```
Privileged EXEC
```

no network priority

This command sets the VLAN priority or the IP DSCP value for outgoing management packets to default which means VLAN priority 0 or IP DSCP value 0 (Best effort).

Format

```
no network priority {dot1p-vlan | ip-dscp }
```

Mode

```
Privileged EXEC
```

4.6.32 profinetio

This command controls the PROFINET IO function on the switch.
Detailed information you can find in the User Manual Industrial Protocols.

Default

depends on the order code (standard = disable)

Format

`profinetio admin-state {enable | disable}`

Mode

`Global Config`

Admin-state

`disable` Disables the PROFINET IO function on this device.
Note: The relevant MIB objects are still accessible.

`enable` Enables the PROFINET IO function on this device.

4.6.33 serial timeout

This command specifies the maximum connect time (in minutes) without console activity. A value of 0 indicates that a console can be connected indefinitely. The time range is 0 to 160.

Default

5

Format

```
serial timeout <0-160>
```

Mode

```
Line Config
```

- **no serial timeout**
  This command sets the maximum connect time without console activity (in minutes) back to the default value.

Format

```
no serial timeout
```

Mode

```
Line Config
```

4.6.34 set prompt

This command changes the name of the prompt. The length of name may be up to 64 alphanumeric characters.

Format

```
set prompt <prompt string>
```

Mode

```
Privileged EXEC
```

4.6.35 show ethernet-ip

This command displays the admin state of the EtherNet/IP function.

Format

```
show ethernet-ip
```

Mode

```
Privileged EXEC and User EXEC
```

4.6.36 show network

This command displays configuration settings associated with the switch's network interface. The network interface is the logical interface used for in-band connectivity with the switch via any of the switch's front panel ports. The configuration parameters associated with the switch's network interface do not affect the configuration of the front panel ports through which traffic is switched or routed.

Format

```
show network
```

Mode

```
Privileged EXEC and User EXEC
```

System IP Address

The IP address of the interface. The factory default value is `0.0.0.0`

Subnet Mask

The IP subnet mask for this interface. The factory default value is `0.0.0.0`

Default Gateway

The default gateway for this IP interface. The factory default value is `0.0.0.0`

Burned In MAC Address

The burned in MAC address used for in-band connectivity.

Network Configuration Protocol (BootP/DHCP)

Indicates which network protocol is being used. Possible values: `bootp` | `dhcp` | `none`.

DHCP Client ID (same as SNMP System Name)

Displays the DHCP Client ID.

Network Configuration Protocol HiDiscovery

Indicates in which way the HiDiscovery protocol is being used. Possible values: `off` | `read-only` | `read-write`.

HiDiscovery Version

Indicates the supported HiDiscovery protocol version.
Possible values: `v1` | `v2`.

Management VLAN ID

Specifies the management VLAN ID.

Management VLAN Priority

Specifies the management VLAN Priority.

Management VLAN IP-DSCP Value

Specifies the management VLAN IP-DSCP value.

Web Mode

Specifies if the switch will use Java Script to start the Management Applet. The factory default is `Enable`.

4.6.37 show network mgmt-access

This command displays the operating status and entries for restricted management access (RMA).

Format

`show network mgmt-access`

Mode

`Privileged EXEC and User EXEC`

Operation

Indicates whether the operation for RMA is enabled or not.
Possible values: `Enabled` | `Disabled`.

ID

Index of the entry for restricted management access (`1` to max. `16`).

IP address

The IP address which should have access to management.
The factory default value is `0.0.0.0`.

Netmask

The network mask to allow a subnet for management access.
The factory default value is `0.0.0.0`.

HTTP

Indicates whether HTTP is allowed to have management access or not. Possible values: `Yes` | `No`.

HTTPS

Indicates whether HTTPS is allowed to have management access or not. Possible values: `Yes` | `No`.

SNMP

Indicates whether SNMP is allowed to have management access or not. Possible values: `Yes` | `No`.

TELNET

Indicates whether TELNET is allowed to have management access or not. Possible values: `Yes` | `No`.

SSH

Indicates whether SSH is allowed to have management access or not. Possible values: `Yes` | `No`.

Active

Indicates whether the feature is active or not.
Possible values: `[x]` | `[ ]`.

4.6.38 show profinetio

This command displays the admin state of the PROFINET IO function.

Format

```
show profinetio
```

Mode

```
Privileged EXEC and User EXEC
```

4.6.39 show serial

This command displays serial communication settings for the switch.

Format

```
show serial
```

Mode

```
Privileged EXEC and User EXEC
```

Serial Port Login Timeout (minutes)

Specifies the time, in minutes, of inactivity on a Serial port connection, after which the Switch will close the connection. Any numeric value between 0 and 160 is allowed, the factory default is 5. A value of 0 disables the timeout.

4.6.40 show snmp-access

This command displays SNMP access information related to global and SNMP version settings. SNMPv3 is always enabled.

Format

```
show snmp-access
```

Mode

```
Privileged EXEC
```

4.6.41 show snmpcommunity

This command displays SNMP community information. Six communities are supported. You can add, change, or delete communities. The switch does not have to be reset for changes to take effect.
The SNMP agent of the switch complies with SNMP Version 1 (for more about the SNMP specification, see the SNMP RFCs). The SNMP agent sends traps through TCP/IP to an external SNMP manager based on the SNMP configuration (the trap receiver and other SNMP community parameters).

Format

```
show snmpcommunity
```

Mode

```
Privileged EXEC
```

SNMP Community Name

The community string to which this entry grants access. A valid entry is a case-sensitive alphanumeric string of up to 32 characters. Each row of this table must contain a unique community name.

Client IP Address -

An IP address (or portion thereof) from which this device will accept SNMP packets with the associated community. The requesting entity's IP address is ANDed with the Subnet Mask before being compared to the IP Address. Note that if the Subnet Mask is set to 0.0.0.0, an IP Address of 0.0.0.0 matches all IP addresses. The default value is 0.0.0.0

Client IP Mask -

A mask to be ANDed with the requesting entity's IP address before comparison with IP Address. If the result matches with IP Address then the address is an authenticated IP address. For example, if the IP Address = 9.47.128.0 and the corresponding Subnet Mask = 255.255.255.0 a range of incoming IP addresses would match, i.e. the incoming IP Address could equal 9.47.128.0 - 9.47.128.255. The default value is 0.0.0.0

Access Mode

The access level for this community string.

Status

The status of this community access entry.

4.6.42 show snmp sync

This command displays the status of the synchronization between the SNMPv1/v2 community table and the SNMPv3 password table and reverse.

Format

```
show snmp sync
```

Mode

```
Privileged EXEC
```

V1/V2 community to V3 password

Display the status of the synchronization between the SNMPv1/v2 community table and the SNMPv3 password table.

Enabled - Synchronization enabled.

Disabled - Synchronization disabled.

V3 password to V1/V2 community

Display the status of the synchronization between the SNMPv3 password table and the SNMPv1/v2 community table.

Enabled - Synchronization enabled.

Disabled - Synchronization disabled.

4.6.43 show snmptrap

This command displays SNMP trap receivers. Trap messages are sent across a network to an SNMP Network Manager. These messages alert the manager to events occurring within the switch or on the network. Six trap receivers are simultaneously supported.

Format

```
show snmptrap
```

Mode

```
Privileged EXEC
```

SNMP Trap Name

The community string of the SNMP trap packet sent to the trap manager. This may be up to 32 alphanumeric characters. This string is case sensitive.

IP Address

The IP address to receive SNMP traps from this device. Enter four numbers between `0` and `255` separated by periods.

Status

A pull down menu that indicates the receiver's status (enabled or disabled) and allows the administrator/user to perform actions on this user entry:

Enable - send traps to the receiver

Disable - do not send traps to the receiver.

Delete - remove the table entry.

4.6.44 show telnet

This command displays outbound telnet settings.

Format

`show telnet`

Mode

`Privileged EXEC and User EXEC`

Outbound Telnet Connection Login Timeout (minutes)

This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from `1` to `160`. The factory default is `5`.

Maximum Number of Outbound Telnet Sessions

This object indicates the number of simultaneous outbound connection sessions allowed. The factory default is `5`.

Allow New Outbound Telnet Sessions

Indicates that new outbound telnet sessions will not be allowed when set to no. The factory default value is `yes`.

4.6.45 show telnetcon

This command displays inbound telnet settings.

Format

`show telnetcon`

Mode

`Privileged EXEC and User EXEC`

Telnet Connection Login Timeout (minutes)

This object indicates the number of minutes a remote connection session is allowed to remain inactive before being logged off. May be specified as a number from `1` to `160`. The factory default is `4`.

Maximum Number of Remote Telnet Sessions

This object indicates the number of simultaneous remote connection sessions allowed. The factory default is `2` (`4` for version L2P)

Allow New Telnet Sessions

Indicates that new telnet sessions will not be allowed when set to no. The factory default value is `yes`.

4.6.46 show trapflags

This command displays trap conditions. Configure which traps the switch should generate by enabling or disabling the trap condition. If a trap condition is enabled and the condition is detected, the switch's SNMP agent sends the trap to all enabled trap receivers. The switch does not have to be reset to implement the changes. Cold and warm start traps are always generated and cannot be disabled.

Format

```
show trapflags
```

Mode

```
Privileged EXEC and User EXEC
```

Authentication Flag

May be enabled or disabled. The factory default is enabled. Indicates whether authentication failure traps will be sent.

Chassis

Indicates whether traps that are related to the chassis functionality of the switch will be sent. These functions include the signal contacts, the ACA, temperature limits exceeded, changes in the module map, addition or removal of SFP modules, status of power supply has changed and the LLDP and SNTP features. May be enabled or disabled.
Default value: enabled.

Layer 2 Redundancy

Indicates whether traps that are related to the layer 2 redundancy features of the switch will be sent. The HiPER-Ring and the Redundant Coupling will tell you with these traps when the main line has become inoperative or returned. May be enabled or disabled.
Default value: enabled.

Link Up/Down Flag

May be enabled or disabled. The factory default is enabled. Indicates whether link status traps will be sent.

Multiple Users Flag

May be enabled or disabled. The factory default is enabled. Indicates whether a trap will be sent when the same user ID is logged into the switch more than once at the same time (either via telnet or serial port).

Port Security (MAC, IP and 802.1X)

Enable/disable sending port security event traps (for MAC/IP port security as well as for 802.1X).

Spanning Tree Flag

May be enabled or disabled. The factory default is enabled. Indicates whether spanning tree traps will be sent.

4.6.47 snmp-access global

This command configures the global SNMP access setting (for all SNMP versions).

Format

```
snmp-access global {disable|enable|read-only}
```

Mode

```
Global Config
```

disable

Disable SNMP access to this switch, regardless of the SNMP version used.

enable

Enable SNMP read and write access to this switch, regardless of the SNMP version used.

read-only

Enable SNMP read-only access to this switch (disable write access), regardless of the SNMP version used.

4.6.48 snmp-access version

This command configures the SNMP version specific access mode for SNMPv1 and SNMPv2.

Format

```
snmp-access version {all|v1|v2} {disable|enable}
```

Mode

```
Global Config
```

all

Enable or disable SNMP access by all protocol versions (v1 and v2).

v1

Enable or disable SNMP access by v1.

v2

Enable or disable SNMP access by v2.

4.6.49 snmp-access version v3-encryption

Use this command to activate/deactivate SNMPv3 data encryption.

Format

```
snmp-access version v3-encryption
          {readonly | readwrite} {enable | disable}
```

Mode

```
Global Config
```

disable

Disable SNMP access to this switch by SNMPv3 protocol version.

enable

Enable SNMP read and write access to this switch by SNMPv3 protocol version.

readonly

Enable SNMP read-only access to this switch (disable write access) by SNMPv33 protocol version.

readwrite

Enable SNMP read-write access to this switch (enable write access) by SNMPv3 protocol version.

4.6.50 snmp-server

This command sets the name and the physical location of the switch, and the organization responsible for the network.The range for *name*, *location* and *contact* is from 0 to 64 alphanumeric characters.

Default

None

Format

```
snmp-server
 {community <name> |
  ipaddr <ipaddr> <name> |
  ipmask <ipmask> <name> |
  mode <name> |
  ro <name> |
  rw <name> |
  contact <con> |
  enable traps { chassis | l2redundancy |
    linkmode | multiusers | port-sec | stpmode }
  location <loc> |
  sysname <name> }
```

Mode

```
Global Config
```

4.6.51 snmp-server community

This command adds a new SNMP community name. A community name is a name associated with the switch and with a set of SNMP managers that manage it with a specified privileged level. The length of name can be up to 32 case-sensitive characters.

Note: Community names in the SNMP community table must be unique. When making multiple entries using the same community name, the first entry is kept and processed and all duplicate entries are ignored.

Default

Two default community names: Public and Private. You can replace these default community names with unique identifiers for each community. The default values for the remaining four community names are blank.

Format

```
snmp-server community <name>
```

Mode

```
Global Config
```

no snmp-server community

This command removes this community name from the table. The name is the community name to be deleted.

Format

```
no snmp-server community <name>
```

Mode

```
Global Config
```

4.6.52 snmp-server contact

This command adds a new SNMP server contact.

Format

```
snmp-server contact <con>
```

Mode

```
Global Config
```

con

Enter system contact up to 63 characters in length.
If the name contains spaces, enclose it in quotation marks (").

no snmp-server contact

This command removes this SNMP server contact from the table.
<con> is the SNMP server contact to be deleted.

Format

```
no snmp-server contact <con>
```

Mode

```
Global Config
```

4.6.53 snmp-server community ipaddr

This command sets a client IP address for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP mask value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 0.0.0.0 allows access from any IP address. Otherwise, this value is ANDed with the mask to determine the range of allowed client IP addresses. The name is the applicable community name.

Default

0.0.0.0

Format

```
snmp-server community ipaddr <ipaddr> <name>
```

Mode

```
Global Config
```

- **no snmp-server community ipaddr**
  This command sets a client IP address for an SNMP community to 0.0.0.0. The name is the applicable community name.

Format

```
no snmp-server community ipaddr <name>
```

Mode

```
Global Config
```

4.6.54 snmp-server community ipmask

This command sets a client IP mask for an SNMP community. The address is the associated community SNMP packet sending address and is used along with the client IP address value to denote a range of IP addresses from which SNMP clients may use that community to access the device. A value of 255.255.255.255 will allow access from only one station, and will use that machine's IP address for the client IP Address. A value of 0.0.0.0 will allow access from any IP address. The name is the applicable community name.

Default

0.0.0.0

Format

```
snmp-server community ipmask <ipmask> <name>
```

Mode

```
Global Config
```

no snmp-server community ipmask

This command sets a client IP mask for an SNMP community to 0.0.0.0. The name is the applicable community name. The community name may be up to 32 alphanumeric characters.

Format

```
no snmp-server community ipmask <name>
```

Mode

```
Global Config
```

4.6.55 snmp-server community mode

This command activates an SNMP community. If a community is enabled, an SNMP manager associated with this community manages the switch according to its access right. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Default

The default private and public communities are enabled by default. The four undefined communities are disabled by default.

Format

```
snmp-server community mode <name>
```

Mode

```
Global Config
```

no snmp-server community mode

This command deactivates an SNMP community. If the community is disabled, no SNMP requests using this community are accepted. In this case the SNMP manager associated with this community cannot manage the switch until the Status is changed back to Enable.

Format

```
no snmp-server community mode <name>
```

Mode

```
Global Config
```

4.6.56 snmp-server community ro

This command restricts access to switch information. The access mode is read-only (also called public).

Format

```
snmp-server community ro <name>
```

Mode

```
Global Config
```

4.6.57 snmp-server community rw

This command restricts access to switch information. The access mode is read/write (also called private).

Format

```
snmp-server community rw <name>
```

Mode

```
Global Config
```

4.6.58 snmp-server location

This command configures the system location.

Format

```
snmp-server location <system location>
```

Mode

```
Global Config
```

4.6.59 snmp-server sysname

This command configures the system name.

Format

```
snmp-server sysname <system name>
```

Mode

```
Global Config
```

4.6.60 snmp-server enable traps

This command enables the Authentication Trap Flag.

Default

enabled

Format

```
snmp-server enable traps
```

Mode

```
Global Config
```

no snmp-server enable traps

This command disables the Authentication Trap Flag.

Format

```
no snmp-server enable traps
```

Mode

```
Global Config
```

4.6.61 snmp-server enable traps chassis

Configures whether traps that are related to the chassis functionality of the switch will be sent. These functions include the signal contacts, the ACA, temperature limits exceeded, changes in the module map, addition or removal of SFP modules, status of power supply has changed and the LLDP and SNTP features. May be enabled or disabled.
Default value: enabled.

Default

enabled

Format

```
snmp-server enable traps chassis
```

Mode

```
Global Config
```

no snmp-server enable traps chassis

This command disables chassis traps for the entire switch.

Format

```
no snmp-server enable traps chassis
```

Mode

```
Global Config
```

4.6.62 snmp-server enable traps l2redundancy

Indicates whether traps that are related to the layer 2 redundancy features of the switch will be sent. The HiPER-Ring and the Redundant Coupling will tell you with these traps when the main line has become inoperative or returned. May be enabled or disabled.
Default value: enabled.

Default

enabled

Format

```
snmp-server enable traps l2redundancy
```

Mode

```
Global Config
```

- **no snmp-server enable traps l2redundancy**
  This command disables layer 2 redundancy traps for the entire switch.

Format

```
no snmp-server enable traps l2redundancy
```

Mode

```
Global Config
```

4.6.63 snmp-server enable traps linkmode

This command enables Link Up/Down traps for the entire switch. When enabled, link traps are sent only if the Link Trap flag setting associated with the port is enabled (see ‘snmp trap link-status’ command).

Default

enabled

Format

```
snmp-server enable traps linkmode
```

Mode

```
Global Config
```

no snmp-server enable traps linkmode

This command disables Link Up/Down traps for the entire switch.

Format

```
no snmp-server enable traps linkmode
```

Mode

```
Global Config
```

4.6.64 snmp-server enable traps multiusers

This command enables Multiple User traps. When the traps are enabled, a Multiple User Trap is sent when a user logs in to the terminal interface (EIA 232 (serial port) or telnet) and there is an existing terminal interface session.

Default

enabled

Format

```
snmp-server enable traps multiusers
```

Mode

```
Global Config
```

no snmp-server enable traps multiusers

This command disables Multiple User traps.

Format

```
no snmp-server enable traps multiusers
```

Mode

```
Global Config
```

4.6.65 snmp-server enable traps port-sec

This command enables port security traps. When the traps are enabled, a Port Security Trap is sent if a port security event occurs (applies to MAC/IP Port Security as well as to 802.1X Port Security).

Default

enabled

Format

```
snmp-server enable traps port-sec
```

Mode

```
Global Config
```

no snmp-server enable traps port-sec

This command disables Port Security traps.

Format

```
no snmp-server enable traps port-sec
```

Mode

```
Global Config
```

4.6.66 snmp-server enable traps stpmode

This command enables the sending of new root traps and topology change notification traps.

Default

enabled

Format

```
snmp-server enable traps stpmode
```

Mode

```
Global Config
```

- **no snmp-server enable traps stpmode**
  This command disables the sending of new root traps and topology change notification traps.

Format

```
no snmp-server enable traps stpmode
```

Mode

```
Global Config
```

4.6.67 snmptrap

This command adds an SNMP trap name. The maximum length of name is 32 case-sensitive alphanumeric characters.

Default

The default name for the six undefined community names is Delete.

Format

```
snmptrap <name> <ipaddr> [snmpversion snmpv1]
```

Mode

```
Global Config
```

no snmptrap

This command deletes trap receivers for a community.

Format

```
no snmptrap <name> <ipaddr>
```

Mode

```
Global Config
```

4.6.68 snmptrap ipaddr

This command assigns an IP address to a specified community name. The maximum length of name is 32 case-sensitive alphanumeric characters.

Note: IP addresses in the SNMP trap receiver table must be unique. If you make multiple entries using the same IP address, the first entry is retained and processed. All duplicate entries are ignored.

Format

```
snmptrap ipaddr <name> <ipaddr> <ipaddrnew>
```

Mode

```
Global Config
```

ipaddr

Enter the old IP Address.

ipaddrnew

Enter the new IP Address.

4.6.69 snmptrap mode

This command activates or deactivates an SNMP trap. Enabled trap receivers are active (able to receive traps). Disabled trap receivers are inactive (not able to receive traps).

Format

```
snmptrap mode <name> <ipaddr>
```

Mode

```
Global Config
```

no snmptrap mode

This command deactivates an SNMP trap. Disabled trap receivers are inactive (not able to receive traps).

Format

```
no snmptrap mode <name> <ipaddr>
```

Mode

```
Global Config
```

4.6.70 snmptrap snmpversion

This command configures SNMP trap version for a specified community.

Format

```
snmptrap snmpversion <name> <ipAddr>
 {snmpv1 | snmpv2}
```

Mode

```
Global Config
```

name

Enter the community name.

ipAaddr

Enter the IP Address.

snmpv1

Use SNMP v1 to send traps.

snmpv2

Use SNMP v2 to send traps.

4.6.71 telnetcon maxsessions

Configure the number of remote telnet connections allowed.

Default

5

Format

```
telnetcon maxsessions <0-5>
```

Mode

```
Privileged EXEC
```

no telnetcon maxsessions

This command sets the maximum number of telnet connection sessions that can be established to the default value.

Format

```
no telnetcon maxsessions
```

Mode

```
Privileged EXEC
```

4.6.72 telnetcon timeout

This command sets the telnet connection session timeout value, in minutes. A session is active as long as the session has not been idle for the value set. The time is a decimal value from 1 to 160.

Default

5

Format

```
telnetcon timeout <1-160>
```

Mode

```
Privileged EXEC
```

no telnetcon timeout

This command sets the telnet connection session timeout value to the default.

Changing the timeout value for active sessions does not become effective until the session is reaccessed. Also, any keystroke activates the new timeout duration.

Format

```
no telnetcon timeout
```

Mode

```
Privileged EXEC
```

4.7 Syslog Commands

This section provides a detailed explanation of the Syslog commands. The commands are divided into two functional groups:

- Show commands display spanning tree settings, statistics, and other information.
- Configuration Commands configure features and options of the device. For every configuration command there is a show command that displays the configuration setting.

4.7.1 logging buffered

This command enables logging to an in-memory log where up to 128 logs are kept.

Default

`enabled`

Format

`logging buffered`

Mode

`Global Config`

no logging buffered

This command disables logging to in-memory log.

Format

`no logging buffered`

4.7.2 logging buffered wrap

This command enables wrapping of in-memory logging when full capacity reached. Otherwise when full capacity is reached, logging stops.

Default

`wrap`

Format

`logging buffered wrap`

Mode

`Privileged EXEC`

no logging buffered wrap

This command disables wrapping of in-memory logging and configures logging to stop when capacity is full.

Format

`no logging buffered wrap`

4.7.3 logging cli-command

This command enables the CLI command Logging feature. The Command Logging component enables the switch software to log all Command Line Interface (CLI) commands issued on the system.

Default

```
disabled
```

Format

```
logging cli-command
```

Mode

```
Global Config
```

no logging cli-command

This command disables the CLI command Logging feature.

Format

```
no logging cli-command
```

4.7.4 logging console

This command enables logging to the console. The <severitylevel> value is specified as either an integer from 0 to 7 or symbolically through one of the following keywords: emergency (0), alert (1), critical (2), error (3), warning (4), notice (5), informational (6), debug (7).

Default

```
disabled; alert
```

Format

```
logging console [severitylevel] | <[0-7]>
```

Mode

```
Global Config
```

severitylevel | [0-7]

Enter Logging Severity Level (emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7).
Note: Selecting a lower severity level (larger number) will include all messages from higher severity levels (smaller numbers).
Possible severity levels: see Table 16

no logging console

This command disables logging to the console.

Format

```
no logging console
```

4.7.5 logging host

This command enables logging to a host where up to eight hosts can be configured.

Default

```
Port – 514; Level – Critical;
```

Format

```
logging host <hostaddress>
 [<port> [<severitylevel>]]
```

Mode

```
Global Config
```

Severity number	Severity name	Meaning
0	emergency	Minimum severity to be logged is 0. This is the highest level and will result in all other messages of lower levels not being logged.
1	alert	Minimum severity to be logged is 1.
2	critical	Minimum severity to be logged is 2.
3	error	Minimum severity to be logged is 3.
4	warning	Minimum severity to be logged is 4.
5	notice	Minimum severity to be logged is 5.
6	info	Minimum severity to be logged is 6.
7	debug	Minimum severity to be logged is 7. This is the lowest level and will result in messages of all levels being logged.

Tab. 16: Possible severity levels

4.7.6 logging host reconfigure

The Logging Host Index for which to change the IP Address.

Format

```
logging host reconfigure <hostindex> <hostaddress>
```

Mode

```
Global Config
```

4.7.7 logging host remove

The Logging Host Index to be removed.

Format

```
logging host remove <hostindex>
```

Mode

```
Global Config
```

4.7.8 logging snmp-requests get operation

This command enables or disables the logging of SNMP GET requests.

Default

```
Disabled
```

Format

```
logging snmp-requests get operation
  { enable | disable }
```

Mode

```
Global Config
```

4.7.9 logging snmp-requests set operation

This command enables or disables the logging of SNMP SET requests.

Default

`Disabled`

Format

```
logging snmp-requests set operation
  { enable | disable }
```

Mode

`Global Config`

4.7.10 logging snmp-requests get severity

With this command you can define the severity level of logging SNMP GET requests.

Default

`Disabled`

Format

```
logging snmp-requests get severity <level|[0-7]>
```

Mode

`Global Config`

level | [0-7]

Enter Logging Severity Level (`emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7`).

Note: Selecting a lower severity level (larger number) will include all messages from higher severity levels (smaller numbers).

4.7.11 logging snmp-requests set severity

With this command you can define the severity level of logging SNMP SET requests.

Default

`Disabled`

Format

`logging snmp-requests set severity <level|[0-7]>`

Mode

`Global Config`

level | [0-7]

Enter Logging Severity Level (`emergency|0, alert|1, critical|2, error|3, warning|4, notice|5, info|6, debug|7`).

Note: Selecting a lower severity level (larger number) will include all messages from higher severity levels (smaller numbers).

4.7.12 logging syslog

This command enables syslog logging.

Default

`disabled`

Format

`logging syslog`

Mode

`Global Config`

no logging syslog

This command disables syslog logging.

Format

`no logging syslog`

4.7.13 logging syslog port

Enter the port number of the syslog server.

Default

`514`

Format

`logging syslog port <portid>`

Mode

`Global Config`

4.8 Scripting Commands

Configuration Scripting allows the user to generate text-formatted script files representing the current configuration. These configuration script files can be uploaded to a PC and edited, downloaded to the system and applied to the system. Configuration scripts can be applied to one or more switches with no/minor modifications.

Use the show running-config command to capture the running configuration into a script. Use the copy command to transfer the configuration script to and from the switch.

Scripts are intended to be used on systems with default configuration but users are not prevented from applying scripts on systems with non-default configurations.

Note:
- The file extension must be “.cli”.
- A maximum of ten scripts are allowed on the switch.
- The combined size of all script files on the switch shall not exceed 1024 KB.

4.8.1 script apply

This command applies the commands in the script to the switch. We recommend that the system have default configurations but users are not prevented from applying scripts on systems with non-default configurations. The <scriptname> parameter is the name of the script to apply.

Format

```
script apply <scriptname>
```

Mode

```
Privileged EXEC
```

4.8.2 script delete

This command deletes a specified script where the <scriptname> parameter is the name of the script to be deleted. The ‘all’ option deletes all the scripts present on the switch.

Format

```
script delete {<scriptname> | all}
```

Mode

```
Privileged EXEC
```

4.8.3 script list

This command lists all scripts present on the switch as well as the remaining available space.

Format

```
script list [aca]
```

Mode

```
Privileged EXEC
```

Configuration Script

Name of the script.
Without the optional ACA parameter: Listing of the scripts in the switch´s flash memory.
With the optional ACA parameter: Listing of the scripts on the external ACA 21-USB.

Size

Size of the script.

4.8.4 script show

This command displays the contents of a script file. The parameter <script-name> is the name of the script file.

Format

```
script show <scriptname>
```

Mode

```
Privileged EXEC
```

The format of display is
`Line <no>: <Line contents>`

4.8.5 script validate

This command validates a script file by parsing each line in the script file where <scriptname> is the name of the script to validate.The validate option is intended to be used as a tool for script development.
Validation helps to identify potential errors concerning a script on the device.

Format

```
script validate <scriptname>
```

Mode

```
Privileged EXEC
```

4.9 Device Configuration Commands

4.9.1 addport

This command adds one port to the Link Aggregation (LAG). The given interface is a logical slot and port number of a configured Link Aggregation.

Note: Before adding a port to a Link Aggregation, set the physical mode of the port. See ‘speed’ command.

Format

addport <logical slot/port>

Mode

Interface Config

4.9.2 adminmode

This command enables the whole Link Aggregation as one single port.

Note: Before adding a port to a Link Aggregation, set the physical mode of the port. See ‘speed’ command.

Format

```
adminmode
```

Mode

```
Interface Config
```

no adminmode

This command disables the whole Link Aggregation as one single port.

Format

```
no adminmode
```

Mode

```
Interface Config
```

4.9.3 auto-disable reason

This command enables the port disabling on this device by reason.

Default

```
Disabled
```

Format

```
auto-disable reason {link-flap | crc-error |
overload-detection | speed-duplex | port-security}
```

Mode

```
Global Config
```

link-flap

Enable the port disabling on this device by link flap.

crc-error

Enable the port disabling on this device by CRC error.

overload-detection

Enable the port disabling on this device by overload detection.

speed-duplex

Enable the port disabling on this device by speed-duplex.

port-security

Enable the port disabling on this device by port-security.

no auto-disable reason

This command disables the port disabling on this device by reason.

Default

```
Disabled
```

Format

```
no auto-disable reason {link-flap | crc-error |
                overload-detection | speed-duplex}
```

Mode

```
Global Config
```

link-flap

Disable the port disabling on this device by link flap.

crc-error

Disable the port disabling on this device by CRC error.

overload-detection

Disable the port disabling on this device by overload detection.

port-security

Disable the port disabling on this device by port-security.

speed-duplex

Disable the port disabling on this device by speed-duplex.

4.9.4 auto-disable reset

Use this command to reset the specific interface and reactivate the port.

Format

```
auto-disable reset
```

Mode

```
Interface Config
```

4.9.5 auto-disable timer

This command defines the time after which a deactivated port is activated again.

Default

```
0
```

Format

```
auto-disable timer {0 | 30..2147483}
```

Mode

```
Interface Config
```

{0 | 30..2147483}

Timer value in seconds after a deactivated port is activated again.
Possible values:
`0` The value `0` disables the timer.
`30..2147483`.

4.9.6 auto-negotiate

This command enables automatic negotiation on a port. The default value is `enable`.

Format

```
auto-negotiate
```

Mode

```
Interface Config
```

no auto-negotiate
This command disables automatic negotiation on a port.

Format

```
no auto-negotiate
```

Mode

```
Interface Config
```

4.9.7 auto-negotiate all

This command enables automatic negotiation on all ports.
The default value is `enable`.

Format

```
auto-negotiate all
```

Mode

```
Global Config
```

no auto-negotiate all

This command disables automatic negotiation on all ports.

Format

```
no auto-negotiate all
```

Mode

```
Global Config
```

4.9.8 cable-crossing

Note: This function is available for the RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH1000, PowerMICE and OCTOPUS devices.

Use this command to enable or disable the cable crossing function.

Note: The `cable-crossing` settings become effective for a certain port, if `auto-negotiate` is disabled for this port.
The `cable-crossing` settings are irrelevant for a certain port, if `auto-negotiate` is enabled for this port.

Format

`cable-crossing {enable|disable}`

Mode

`Interface Config`

cable-crossing enable

The device swaps the port output and port input of the TP port.

cable-crossing disable

The device does not swap the port output and port input of the TP port.

4.9.9 media-module

Use this command to logically configure media modules.

Default

```
media-module enable all
```

Format

```
media-module { remove <1-7> |
               enable { <1-7> | all } |
               disable { <1-7> | all } }
```

Mode

```
Global Config
```

remove

Logically remove a media-module that has already been physically removed.

<1-7>

Enter the number of a media module that has already been physically removed but is logically still present in the configuration.

enable

Enable a media-module slot.

<1-7>

Enter the number of the media module to be enabled.

all

Enable all media modules on the device.

disable

Disable a media-module slot.

<1-7>

Enter the number of the media module to be disabled.

all

Disable all media modules on the device.

4.9.10 deleteport

This command deletes the port from the link-aggregation (LAG). The interface is a logical slot and port number of a configured link aggregation.

Note: This command has to be issued in the member port's interface config mode.

Format

```
deleteport <logical slot/port>
```

Mode

```
Interface Config
```

4.9.11 deleteport all

This command deletes all configured ports from the link-aggregation (LAG). The interface is a logical slot and port number of a configured link-aggregation.

Format

```
deleteport <logical slot/port> all
```

Mode

```
Global Config
```

4.9.12 dip-switch operation

Note: This command is available for the MICE, PowerMICE and RS20/ RS30/RS40 devices.

Use this command to enable/disable the DIP switch configuration.

Default

`disabled`

Format

`dip-switch operation { enable | disable }`

Mode

`Global Config`

enable

Enable the DIP switch configuration.

disable

Disable the DIP switch configuration.
The device ignores DIP switch settings.

4.9.13 macfilter

This command adds a static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The restricted MAC Addresses are: 00:00:00:00:00:00, 01:80:C2:00:00:00 to 01:80:C2:00:00:0F, 01:80:C2:00:00:20 to 01:80:C2:00:00:21, and FF:FF:FF:FF:FF:FF.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Up to 100 static MAC filters may be created.

Format

```
macfilter <macaddr> <vlanid>
```

Mode

```
Global Config
```

no macfilter

This command removes all filtering restrictions and the static MAC filter entry for the MAC address <macaddr> on the VLAN <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Format

```
no macfilter <macaddr> <vlanid>
```

Mode

```
Global Config
```

4.9.14 macfilter adddest

This command adds the interface to the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.
The <vlanid> parameter must identify a valid VLAN (1-4042).

Format

```
macfilter adddest <macaddr> <vlanid>
```

Mode

```
Interface Config
```

no macfilter adddest

This command removes a port from the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1-4042).

Format

```
no macfilter adddest <macaddr> <vlanid>
```

Mode

```
Interface Config
```

4.9.15 macfilter adddest all

This command adds all interfaces to the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Format

```
macfilter adddest {all | <macaddr> <vlanid>}
```

Mode

```
Global Config
```

no macfilter adddest all

This command removes all ports from the destination filter set for the MAC filter with the given <macaddr> and VLAN of <vlanid>. The <macaddr> parameter must be specified as a 6-byte hexadecimal number in the format of b1:b2:b3:b4:b5:b6.

The <vlanid> parameter must identify a valid VLAN (1 to 4042).

Format

```
no macfilter adddest [all | <macaddr> <vlanid>}
```

Mode

```
Global Config
```

4.9.16 mac notification (Global Config)

Use this command to change the settings for MAC address change notification globally on the device. This command enables the sending of MAC notification traps or sets the MAC notification interval in seconds.

Format

```
mac notification {operation |
                 interval <0..2147483647> }
```

Mode

Global Config

operation

Enable sending of MAC notification traps.

interval

Set the MAC notification interval.

<0..2147483647>

MAC notification interval in seconds.

no mac notification operation

This command disables sending of MAC notification traps globally.

Format

```
no mac notification operation
```

Mode

Global Config

4.9.17 mac notification (Interface Config)

Use this command to change the settings for MAC address change notification for one port. This command enables MAC notification for this port or sets the mode for which action the device sends a MAC notification.

Format

```
mac notification {operation |
                  mode { add | remove | all } }
```

Mode

```
Interface Config
```

operation

Enable sending of MAC notification traps.

mode

Set the mode for which action the device sends a MAC notification.

add

The device sends MAC notification traps when entries are added to the FDB.

remove

The device sends MAC notification traps when entries are removed from the FDB.

all

The device sends MAC notification traps when entries are changed in the FDB.

no mac notification operation

This command disables sending of MAC notification traps for this port.

Format

```
no mac notification operation
```

Mode

```
Interface Config
```

4.9.18 monitor session <session-id>

This command configures a probe port and a monitored port for monitor session (port monitoring). The first slot/port is the source monitored port and the second slot/port is the destination probe port. If this command is executed while port monitoring is enabled, it will have the effect of changing the probe and monitored port values.

Format

```
monitor session <session-id>
 [ mode |
   source interface <slot/port>
              [direction { rx | tx | tx/rx } ] |
   destination interface <slot/port> ]
```

Mode

`Global Config`

session-id

Session number (currently, session number 1 is supported).

mode

Enable/Disable port mirroring session.
Note: does not affect the source or destination interfaces.

source interface <slot/port>

Configure the source interface (in `slot/port` notation).

direction

Configure the direction of the interface.´

rx

Configure the direction of the interface as rx (receive).

tx

Configure the direction of the interface as tx (transmit).

rx/tx

Configure the direction of the interface as rx/tx (receive and transmit).

destination interface <slot/port>

Configure the probe interface (in `slot/port` notation).

- **no monitor session<session-id>**
  This command removes the monitor session (port monitoring) designation from both the source probe port and the destination monitored portand removes the probe port from all VLANs. The port must be manually re-added to any desired VLANs.

Format

```
no monitor session <session-id> [mode]
```

Mode

```
Global Config
```

session-id

Session number (currently, session number 1 is supported).

4.9.19 monitor session <session-id> mode

This command configures the monitor session (port monitoring) mode to enable. The probe and monitored ports must be configured before monitor session (port monitoring) can be enabled. If enabled, the probe port will monitor all traffic received and transmitted on the physical monitored port. It is not necessary to disable port monitoring before modifying the probe and monitored ports.

Default

`disabled`

Format

`monitor session <session-id> mode`

Mode

`Global Config`

session-id

Session number (currently, session number 1 is supported).

no monitor session <session-id> mode

This command sets the monitor session (port monitoring) mode to disable.

Format

`no monitor session <session-id> mode`

Mode

`Global Config`

session-id

Session number (currently, session number 1 is supported).

4.9.20 monitor session <session-id> source/ destination

This command allows you to configure and activate the port mirroring function of the switch. Port mirroring is when the data traffic of a source port is copied to a specified destination port. The data traffic at the source port is not influenced by port mirroring. A management tool connected at the specified port, e.g., an RMON probe, can thus monitor the data traffic of the source port.
This command can be called multiple times with different ports to add more than one source port to the session.
It is possible to add/remove ports to/from an active session.

Note:
- The device supports a maximum of one session.
- The maximum number of source ports is 8.
- Ports configured as mirror source or destination ports have to be physical ports.

Note: In active port mirroring, the specified destination port is used solely for observation purposes.

Default

```
none
```

Format

```
monitor session <session-id> {source | destination}
interface <slot/port>
```

Mode

```
Global Config
```

session-id

Session number (currently, session number 1 is supported).

- **no monitor session <session-id> source/destination**
  This command resets the monitor session (port monitoring) source/destination. The port will be removed from port mirroring

Format

```
no monitor session <session-id> {source | destination} interface
```

Mode

```
Global Config
```

session-id

Session number (currently, session number 1 is supported).

4.9.21 link-aggregation

This command configures a new Link Aggregation (LAG) and generates a logical slot/port number for the Link Aggregation. Display this number using the “show link-aggregation”.

Note: Before including a port in a Link Aggregation, set the port physical mode. See ‘speed’ command.

Format

```
link-aggregation <name>
```

Mode

```
Global Config
```

4.9.22 link-aggregation adminmode

This command enables a Link Aggregation (LAG). The interface is a logical slot/port for a configured Link Aggregation. The option `all` sets every configured Link Aggregation with the same administrative mode setting.

Format

```
link-aggregation adminmode all
```

Mode

```
Global Config
```

- **no link-aggregation adminmode**
  This command disables a Link Aggregation (LAG). The interface is a logical slot/port for a configured Link Aggregation. The option `all` sets every configured Link Aggregation with the same administrative mode setting.

Format

```
no link-aggregation adminmode all
```

Mode

```
Global Config
```

4.9.23 link-aggregation linktrap

This command enables link trap notifications for the link-aggregation (LAG). The interface is a logical slot/port for a configured link-aggregation. The option `all` sets every configured link-aggregation with the same administrative mode setting.

Default

`enabled`

Format

`link-aggregation linktrap {<logical slot/port> | all}`

Mode

`Global Config`

no link-aggregation linktrap

This command disables link trap notifications for the link-aggregation (LAG). The interface is a logical unit, slot and port slot and port for a configured link-aggregation. The option `all` sets every configured link-aggregation with the same administrative mode setting.

Format

`no link-aggregation linktrap {<logical slot/port> | all]`

Mode

`GlobalConfig`

4.9.24 link-aggregation name

This command defines a name for the link-aggregation (LAG). The interface is a logical slot/port for a configured link-aggregation, and name is an alpha-numeric string up to 15 characters. This command is used to modify the name that was associated with the link-aggregation when it was created.

Format

```
link-aggregation name {<logical slot/port> | all |
<name>}
```

Mode

```
Global Config
```

4.9.25 rmon-alarm add

This command adds an RMON alarm.

Format

```
rmon-alarm add <index>
              [<mib-variable>
               <rising-threshold>
               <falling-threshold>]
```

Mode

```
Global Config
```

index

```
Enter the index of the RMON alarm.
```

mib-variable

```
Enter the MIB variable.
```

rising-threshold

```
Enter the rising threshold for the RMON alarm.
```

falling-threshold

```
Enter the falling threshold for the RMON alarm.
```

4.9.26 rmon-alarm delete

This command deletes an RMON alarm.

Format

```
rmon-alarm delete <index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

4.9.27 rmon-alarm enable

This command enables an RMON alarm.

Format

```
rmon-alarm enable <index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

4.9.28 rmon-alarm disable

This command disables an RMON alarm.

Format

```
rmon-alarm disable <index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

4.9.29 rmon-alarm modify mib-variable

This command modifies the mib-variable of an RMON alarm.

Format

```
rmon-alarm modify <index> mib-variable <mib-variable>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

mib-variable

Enter the MIB variable.

4.9.30 rmon-alarm modify thresholds

This command modifies the thresholds of an RMON alarm.

Format

```
rmon-alarm modify <index> thresholds
                          <rising-threshold>
                          <falling-threshold>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

rising-threshold

Enter the rising threshold for the RMON alarm.

falling-threshold

Enter the falling threshold for the RMON alarm.

4.9.31 rmon-alarm modify interval

This command modifies the interval of an RMON alarm.

Format

```
rmon-alarm modify <index> interval <interval>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

interval

Enter the interval for the RMON alarm.

4.9.32 rmon-alarm modify sample-type

This command modifies the sample-type of an RMON alarm.

Format

```
rmon-alarm modify <index> sample-type {absolute|delta}
```

Mode

Global Config

index

Enter the index of the RMON alarm.

absolute

Sample-type for RMON alarm is absolute.

delta

Sample-type for RMON alarm is delta.

4.9.33 rmon-alarm modify startup-alarm

This command modifies the startup-alarm of an RMON alarm.

Format

```
rmon-alarm modify <index> startup-alarm
                  {rising | falling | risingorfalling}
```

Mode

Global Config

index

Enter the index of the RMON alarm.

rising

Start-up alarm if the value is rising.

falling

Start-up alarm if the value is falling.

risingorfalling

Start-up alarm if the value is rising or falling.

4.9.34 rmon-alarm modify rising-event

This command modifies the rising-event of an RMON alarm.

Format

```
rmon-alarm modify <index> rising-event
                          <rising-event-index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

rising-event-index

Enter the index for the rising event for the RMON alarm.

4.9.35 rmon-alarm modify falling-event

This command modifies the falling-event of an RMON alarm.

Format

```
rmon-alarm modify <index> falling-event
                          <falling-event-index>
```

Mode

Global Config

index

Enter the index of the RMON alarm.

falling-event-index

Enter the index for the falling event for the RMON alarm.

4.9.36 set garp timer join

This command sets the GVRP join time per port and per GARP. Join time is the interval between the transmission of GARP Protocol Data Units (PDUs) registering (or re-registering) membership for a VLAN or multicast group. This command has an effect only when GVRP is enabled. The time is from 10 to 100 (centiseconds). The value `20` centiseconds is 0.2 seconds.

Default

```
20
```

Format

```
set garp timer join <10-100>
```

Mode

```
Global Config
Interface Config
```

no set garp timer join

This command sets the GVRP join time per port and per GARP to 20 centiseconds (0.2 seconds). This command has an effect only when GVRP is enabled.

Format

```
no set garp-timer join
```

Mode

```
Global Config
Interface Config
```

4.9.37 set garp timer leave

This command sets the GVRP leave time per port. Leave time is the time to wait after receiving an unregister request for a VLAN or a multicast group before deleting the VLAN entry. This can be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service.time is 20 to 600 (centiseconds). The value `60` centiseconds is 0.6 seconds.

Note: This command has an effect only when GVRP is enabled.

Default

```
60
```

Format

```
set garp timer leave <20-600>
```

Mode

```
Global Config
Interface Config
```

no set garp timer leave

TThis command sets the GVRP leave time per port to 60 centiseconds (0.6 seconds).

Note: This command has an effect only when GVRP is enabled.

Format

```
no set garp timer leave
```

Mode

```
Global Config
Interface Config
```

4.9.38 set garp timer leaveall

This command sets how frequently *Leave All PDUs* are generated per port. A *Leave All PDU* indicates that all registrations will be unregistered. Participants would need to rejoin in order to maintain registration. The value applies per port and per GARP participation. The time may range from `200` to `6000` (centiseconds). The value `1000` centiseconds is 10 seconds.

Note: This command has an effect only when GVRP is enabled.

Default

`1000`

Format

`set garp timer leaveall <200-6000>`

Mode

`Global Config`
`Interface Config`

no set garp timer leaveall

This command sets how frequently *Leave All PDUs* are generated per port to 1000 centiseconds (10 seconds).

Note: This command has an effect only when GVRP is enabled.

Format

`no set garp timer leaveall`

Mode

`Global Config`
`Interface Config`

4.9.39 set gmrp adminmode

This command enables GARP Multicast Registration Protocol (GMRP) on the system. The default value is `disable`.

Format

```
set gmrp adminmode
```

Mode

```
Privileged EXEC and Global Config
```

no set gmrp adminmode
This command disables GARP Multicast Registration Protocol (GMRP) on the system.

Format

```
no set gmrp adminmode
```

Mode

```
Privileged EXEC and Global Config
```

4.9.40 set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enlisted as a member of a Link Aggregation (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if Link Aggregation (LAG) membership is removed from an interface that has GARP enabled.

Default

```
enabled
```

Format

```
set gmrp interfacemode
```

Mode

```
Interface Config
```

no set gmrp interfacemode

This command disables GARP Multicast Registration Protocol on a selected interface. If an interface which has GARP enabled is enlisted as a member of a Link Aggregation (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if Link Aggregation (LAG) membership is removed from an interface that has GARP enabled.

Format

```
no set gmrp interfacemode
```

Mode

```
Interface Config
```

4.9.41 set gmrp interfacemode

This command enables GARP Multicast Registration Protocol on all interfaces. If an interface which has GARP enabled is enabled for routing or is enlisted as a member of a link-aggregation (LAG), GARP functionality will be disabled on that interface. GARP functionality will subsequently be re-enabled if routing is disabled and link-aggregation (LAG) membership is removed from an interface that has GARP enabled.

Default

```
disabled
```

Format

```
set gmrp interfacemode
```

Mode

```
Global Config
```

- **no set gmrp interfacemode**
  This command disables GARP Multicast Registration Protocol on a selected interface.

Format

```
no set gmrp interfacemode
```

Mode

```
Global Config
```

4.9.42 set gmrp forward-all-groups

This command enables the GMRP Multicast Registration Protocol feature 'Forward All Groups' for all ports.

Default

```
disabled
```

Format

```
set gmrp forward-all-groups
```

Mode

```
Interface Config
Global Config
```

no set gmrp forward-all-groups

This command disables the GMRP Multicast Registration Protocol feature 'Forward All Groups' for all ports.

Format

```
no set gmrp forward-all-groups
```

Mode

```
Interface Config
Global Config
```

4.9.43 set gmrp forward-unknown

Note: This command is available for the devices of the MS20/MS30, RS20/RS30/RS40, MACH102, MACH104, MACH1000, MACH1040, OCTOPUS, RSR20/RSR30 family.

Use this command to configure if the device should forward unknown GMRP multicast packets. The setting can be discard or flood. The default is flood.

Default

```
flood
```

Format

```
set gmrp forward-unknown {discard | flood}
```

Mode

```
Global Config
```

discard

The device discards unknown GMRP multicast packets.

flood

The device floods unknown GMRP multicast packets.

no set gmrp forward-unknown

This command disables the GMRP Multicast Registration Protocol feature 'Forward Unknown' for all ports.

Format

```
no set gmrp forward-unknown
```

Mode

```
Global Config
```

4.9.44 set igmp

This command enables IGMP Snooping on the system. The default value is `disable`.

Note: The IGMP snooping application supports the following:
- Global configuration or per interface configuration.
- Validation of the IP header checksum (as well as the IGMP header checksum) and discarding of the frame upon checksum error.
- Maintenance of the forwarding table entries based on the MAC address versus the IP address.
- Flooding of unregistered multicast data packets to all ports in the VLAN.

Format

```
set igmp
```

Mode

```
Global Config
```

no set igmp

This command disables IGMP Snooping on the system.

Format

```
no set igmp
```

Mode

```
Global Config
```

4.9.45 set igmp

This command enables IGMP Snooping on a selected interface.

Default

`enabled`

Format

`set igmp`

Mode

`Interface Config`

no set igmp

This command disables IGMP Snooping on a selected interface.

Format

`no set igmp`

Mode

`Interface Config`

4.9.46 set igmp aging-time-unknown

This command configures the IGMP Snooping aging time for unknown multicast frames (unit: seconds, min.: `3`, max.: `3600`, Default value: `260`).

Format

`set igmp aging-time-unknown <3-3600>`

Mode

`Global Config`

4.9.47 set igmp automatic-mode

If enabled, this port is allowed to be set as static query port automatically, if the LLDP protocol has found a switch or router connected to this port. Use the command's normal form to enable the feature, the 'no' form to disable it.

Default

```
disabled
```

Format

```
set igmp automatic-mode
```

Mode

```
Interface Config
```

4.9.48 set igmp forward-all

This command activates the forwarding of multicast frames to this interface even if the given interface has not received any reports by hosts. N. B.: this applies only to frames that have been learned via IGMP Snooping. The purpose is that an interface (e. g. a HIPER Ring's ring port) may need to forward all such frames even if no reports have been received on it. This enables faster recovery from ring interruptions for multicast frames.

Default

```
disabled
```

Format

```
set igmp forward-all
```

Mode

```
Interface Config
```

- **no set igmp forward-all**
  This command disables the forwarding of all multicast frames learned via IGMP Snooping on a selected interface.

Format

```
no set igmp forward-all
```

Mode

```
Interface Config
```

4.9.49 set igmp static-query-port

This command activates the forwarding of IGMP membership report frames to this interface even if the given interface has not received any queries. The purpose is that a port may need to forward such frames even if no queries have been received on it (e. g., if a router is connected to the interface that sends no queries).

Default

```
disabled
```

Format

```
set igmp static-query-port
```

Mode

```
Interface Config
```

- **no set igmp**
  This command disables the unconditional forwarding of IGMP membership report frames to this interface.

Format

```
no set igmp static-query-port
```

Mode

```
Interface Config
```

4.9.50 set igmp groupmembershipinterval

This command sets the IGMP Group Membership Interval time on the system. The Group Membership Interval time is the amount of time in seconds that a switch will wait for a report from a particular group on a particular interface before deleting the interface from the entry. This value must be greater than the IGMP Maximum Response time value. The range is `3` to `3,600` seconds.

Default

`260`

Format

`set igmp groupmembershipinterval <3-3600>`

Mode

`Global Config`

- **no set igmp groupmembershipinterval**
  This command sets the IGMP Group Membership Interval time on the system to 260 seconds.

Format

`no set igmp groupmembershipinterval`

Mode

`Global Config`

4.9.51 set igmp interfacemode

This command enables IGMP Snooping on all interfaces. If an interface which has IGMP Snooping enabled is enabled for port-based routing or is enlisted as a member of a link-aggregation (LAG), IGMP Snooping functionality will be disabled on that interface. IGMP Snooping functionality will subsequently be re-enabled if routing is disabled or link-aggregation (LAG) membership is removed from an interface that has IGMP Snooping enabled.

Format

```
set igmp interfacemode
```

Mode

```
Global Config
```

- **no set igmp interfacemode**
  This command disables IGMP Snooping on all interfaces.

Format

```
no set igmp interfacemode
```

Mode

```
Global Config
```

4.9.52 set igmp lookup-interval-unknown

This command configures the IGMP Snooping lookup response time for unknown multicast frames (unit: seconds, min.: 2, max.: 3599, Default value: 125).

Format

```
set igmp lookup-interval-unknown <2-3599>
```

Mode

```
Global Config
```

<2-3599>

Enter the IGMP Snooping lookup response time for unknown multicast frames (unit: seconds, min.: 2, max.: 3599, Default value: 125).

4.9.53 set igmp lookup-resp-time-unknown

This command configures the IGMP Snooping lookup interval for unknown multicast frames (unit: seconds, min.: 1, max.: 3,598, Default value: 10).

Format

```
set igmp lookup-resp-time-unknown <1-3598>
```

Mode

```
Global Config
```

<2-3598>

Enter the IGMP Snooping lookup interval for unknown multicast frames (unit: seconds, min.: 1, max.: 3598, Default value: 10).

4.9.54 set igmp maxresponse

This command sets the IGMP Maximum Response time on the system. The Maximum Response time is the amount of time in seconds that a switch will wait after sending a query in response to a received leave message, before deleting the multicast group received in the leave message. If the switch receives a report in response to the query within the maxresponse time, then the multicast group is not deleted. This value must be less than the IGMP Query Interval time value. The range is `1` to `3,598` seconds.

Default

`10`

Format

`set igmp maxresponse <1-3598>`

Mode

`Global Config`

Note: the IGMP Querier's max. response time was also set. It is always the same value as the IGMP Snooping max. response time.

no set igmp maxresponse

This command sets the IGMP Maximum Response time on the system to 10 seconds.

Format

`no set igmp maxresponse`

Mode

`Global Config`

4.9.55 set igmp querier max-response-time

Configure the IGMP Snooping Querier's maximum response time. The range is `1` to `3,598` seconds. The default value is `10` seconds.

Default

```
10
```

Format

```
set igmp querier max-response-time <1-3598>
```

Mode

```
Global Config
```

Note: The IGMP Snooping max. response time was also set. It is always the same value as the IGMP Querier´s max. response time.

4.9.56 set igmp querier protocol-version

Configure the IGMP Snooping Querier's protocol version (1, 2 or 3).

Default

```
2
```

Format

```
set igmp querier protocol-version {1 | 2 | 3}
```

Mode

```
Global Config
```

4.9.57 set igmp querier status

Configure the IGMP Snooping Querier's administrative status (enable or disable).

Default

```
disable
```

Format

```
set igmp querier status {enable | disable}
```

Mode

```
Global Config
```

4.9.58 set igmp querier tx-interval

Configure the IGMP Snooping Querier's transmit interval. The range is 2 to 3,599 seconds.

Default

```
125
```

Format

```
set igmp querier tx-interval <2-3599>
```

Mode

```
Global Config
```

4.9.59 set igmp query-ports-to-filter

This command enables or disables the addition of query ports to multicast filter portmasks. The setting can be enable or disable.

Default

`Disable`

Format

`set igmp query-ports-to-filter {enable | disable}`

Mode

`Global Config`

enable

Addition of query ports to multicast filter portmasks.

disable

No addition of query ports to multicast filter portmasks.

4.9.60 selftest ramtest

Enable or disable the RAM test for a cold start of the device.
Deactivating the RAM test reduces the booting time for a cold start of the device.
Default value: `enabled`.

Format

`selftest ramtest {disable|enable}`

Mode

`Global Config`

selftest ramtest disable

Disable the ramtest.

selftest ramtest enable

Enable the ramtest. This is the default.

4.9.61 selftest reboot-on-error

Enable or disable a restart due to an undefined software or hardware state. Default value: `disabled`.

Format

```
selftest reboot-on-error
        {disable | enable | seriousOnly}
```

Mode

`Global Config`

selftest reboot-on-error disable

Disable the reboot-on-error function. This is the default.

selftest reboot-on-error enable

Enable the reboot-on-error function.

selftest reboot-on-error seriousOnly

The device will only reboot on errors considered to be critical.

Note: Duplex mismatch errors are considered to be non-critical. In case of a detected duplex mismatch error, the device will not reboot. Reset the device to restore ports to an usable state.

4.9.62 serviceshell

Use this command to execute a service shell command.

Format

```
serviceshell [deactivate]
```

Mode

```
Privileged EXEC
```

deactivate

Disable the service shell access permanently **(Cannot be undone)**.

Note: If you execute this command the system asks for confirmation: When you disable the service shell function it is permanently disabled. Please see the Basic Configuration Manual for details.

4.9.63 update module-configuration

Note: This command is available for the MACH1020 and MACH1030 devices.

Use this command to update the product code of the device.

Format

```
update module-configuration
```

Mode

```
Global Config
```

Note: Update the product code specifically after you replaced or added a module to the device.

4.9.64 show auto-disable brief

Use this command to display the Auto Disable summary.

Format

`show auto-disable brief`

Mode

`Global Config`

Intf

Display the number of the interface in slot/port format.

Error reason

Display the error reason for auto-disable.
Possible values: `no error` | `link-flap` | `crc-error` | `overload-detection` | `port-security` | `speed-duplex`.

Component name

Display the name of the component for auto-disable.
Possible values: `PORTSEC` | `PORTMON`.

Remaining time (sec.)

Display the remaining time in seconds for auto-disable.
Possible values: `0` | `30..2147483`.

Auto-Disable time (sec.)

Display the time for auto-disable in seconds.
Possible values: `0` | `30..2147483`.

Auto-Disable oper state

Display the operational state of the auto-disable function.
Possible values: `active` | `inactive`.

4.9.65 show auto-disable reasons

Use this command to display the reasons for port auto-disable on this device.

Format

`show auto-disable reasons`

Mode

`Global Config`

Error reason

Display the error reasons of the port auto-disable function
Possible values: `link-flap` | `crc-error` | `overload-detection` | `port-security` | `speed-duplex`.

State

Display the state of the port auto-disable function.
Possible values: `enabled` | `disabled`.

4.9.66 show dip-switch

This command displays the DIP switch operation configuration.

Format

`show dip-switch`

Mode

`Global Config`

DIP Switch operation

This field displays the DIP Switch operation status.
Possible values: `Enabled`, `Disabled`

DIP Switch conflict

This field displays the DIP Switch conflict status.
Possible values: `True`, `False`

DIP Switch Red. Manager

This field displays the DIP Switch Redundancy Manager status.
Possible values: `Enabled`, `Disabled`

DIP Switch Standby

This field displays the DIP Switch Standby status.
Possible values: `Enabled`, `Disabled`

DIP Switch RingPort

Note: This command is available for the MICE devices.
This field displays the DIP Switch RingPort numbers.
Possible values: Interface number in `slot/port` notation.

DIP Switch SW config

Note: This command is available for the MICE devices.
This field displays the DIP Switch SW config status.
Possible values: `Enabled`, `Disabled`

4.9.67 show garp

This command displays Generic Attributes Registration Protocol (GARP) information.

Format

```
show garp
```

Mode

```
Privileged EXEC and User EXEC
```

GMRP Admin Mode

This displays the administrative mode of GARP Multicast Registration Protocol (GMRP) for the system.

4.9.68 show gmrp configuration

This command displays Generic Attributes Registration Protocol (GARP) information for one or all interfaces.

Format

```
show gmrp configuration {<slot/port> | all}
```

Mode

```
Privileged EXEC and User EXEC
```

Interface

This displays the slot/port of the interface that this row in the table describes.

Join Timer

Specifies the interval between the transmission of GARP PDUs registering (or re-registering) membership for an attribute. Current attributes are a VLAN or multicast group. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are `10..100` centiseconds (0.1 to 1.0 seconds). The factory default is `20` centiseconds (0.2 seconds). The finest granularity of specification is `1` centisecond (0.01 seconds).

Leave Timer

Specifies the period of time to wait after receiving an unregister request for an attribute before deleting the attribute. Current attributes are a VLAN or multicast group. This may be considered a buffer time for another station to assert registration for the same attribute in order to maintain uninterrupted service. There is an instance of this timer on a per-Port, per-GARP participant basis. Permissible values are `20..600` centiseconds (0.2 to 6.0 seconds). The factory default is `60` centiseconds (0.6 seconds). The finest granularity of specification is `1` centisecond (0.01 seconds).

LeaveAll Timer

This Leave All Time controls how frequently LeaveAll PDUs are generated. A LeaveAll PDU indicates that all registrations will shortly be deregistered. Participants will need to rejoin in order to maintain registration. There is an instance of this timer on a per-Port, per-GARP participant basis. The Leave All Period Timer is set to a random value in the range of LeaveAllTime to 1.5*LeaveAllTime. Permissible values are `200..6000` centiseconds (2 to 60 seconds). The factory default is `1000` centiseconds (10 seconds). The finest granularity of specification is `1` centisecond (0.01 seconds).

Port GMRP Mode

Indicates the GMRP administrative mode for the port. It may be enabled or disabled. If this parameter is disabled, Join Time, Leave Time and Leave All Time have no effect. The factory default is disabled.

4.9.69 show igmpsnooping

This command displays IGMP Snooping information. Configured information is displayed whether or not IGMP Snooping is enabled. Status information is only displayed when IGMP Snooping is enabled.

Format

```
show igmpsnooping
```

Mode

`Privileged EXEC and User EXEC`

Admin Mode

This indicates whether or not IGMP Snooping is globally enabled on the switch.

Forwarding of Unknown Frames

This displays if and how unknown multicasts are forwarded.
The setting can be Discard, Flood or Query Ports.
The default is Query Ports.

Group Membership Interval

This displays the IGMP Group Membership Interval. This is the amount of time a switch will wait for a report for a particular group on a particular interface before it sends a query on that interface. This value may be configured.

Multicast Control Frame Count

This displays the number of multicast control frames that are processed by the CPU.

Interfaces Enabled for IGMP Snooping

This is the list of interfaces on which IGMP Snooping is enabled. Additionally, if a port has a special function, it will be shown to the right of its slot/port number. There are 3 special functions: `Forward All`, `Static Query Port` and `Learned Query Port`.

Querier Status (the administrative state).

This displays the IGMP Snooping Querier's administrative status.

Querier Mode (the actual state, read only)

This displays the IGMP Snooping Querier's operating status.

Querier Transmit Interval

This displays the IGMP Snooping Querier's transmit interval in seconds.

Querier Max. Response Time

This displays the IGMP Snooping Querier's maximum response time in seconds.

Querier Protocol Version

This displays the IGMP Snooping Querier's protocol version number.

4.9.70 show mac-filter-table gmrp

This command displays the GARP Multicast Registration Protocol (GMRP) entries in the Multicast Forwarding Database (MFDB) table.

Format

```
show mac-filter-table gmrp
```

Mode

```
Privileged EXEC and User EXEC
```

Mac Address

A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB. In an IVL system the MAC address will be displayed as 8 bytes.

Type

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description

The text description of this multicast table entry.

Interfaces

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

4.9.71 show mac-filter-table igmpsnooping

This command displays the IGMP Snooping entries in the Multicast Forwarding Database (MFDB) table.

Format

```
show mac-filter-table igmpsnooping
```

Mode

```
Privileged EXEC and User EXEC
```

Mac Address

A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Type

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description

The text description of this multicast table entry.

Interfaces

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

4.9.72 show mac-filter-table multicast

This command displays the Multicast Forwarding Database (MFDB) information. If the command is entered with no parameter, the entire table is displayed. This is the same as entering the optional `all` parameter. The user can display the table entry for one MAC Address by specifying the MAC address as an optional parameter.

Format

```
show mac-filter-table multicast
            [<macaddr> <1-4042>]
```

Mode

`Privileged EXEC and User EXEC`

Mac Address

A multicast MAC address for which the switch has forwarding and or filtering information. The format is two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Type

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Component

The component that is responsible for this entry in the Multicast Forwarding Database. Possible values are `IGMP Snooping`, `GMRP` and `Static Filtering`.

Description

The text description of this multicast table entry.

Interfaces

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

Forwarding Interfaces

The resultant forwarding list is derived from combining all the component's forwarding interfaces and removing the interfaces that are listed as the static filtering interfaces.

4.9.73 show mac-filter-table static

This command displays the Static MAC Filtering information for all Static MAC Filters. If `all` is selected, all the Static MAC Filters in the system are displayed. If a macaddr is entered, a vlan must also be entered and the Static MAC Filter information will be displayed only for that MAC address and VLAN.

Format

```
show mac-filter-table static {<macaddr> <vlanid> | all}
```

Mode

`Privileged EXEC and User EXEC`

MAC Address

Is the MAC Address of the static MAC filter entry.

VLAN ID

Is the VLAN ID of the static MAC filter entry.

Source Port(s)

Indicates the source port filter set's slot and port(s).

Destination Port(s)

Indicates the destination port filter set's slot and port(s).

4.9.74 show mac-filter-table staticfiltering

This command displays the Static Filtering entries in the Multicast Forwarding Database (MFDB) table.

Format

```
show mac-filter-table staticfiltering
```

Mode

```
Privileged EXEC and User EXEC
```

Mac Address

A unicast MAC address for which the switch has forwarding and or filtering information. The format is 6 or 8 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB.

Type

This displays the type of the entry. Static entries are those that are configured by the end user. Dynamic entries are added to the table as a result of a learning process or protocol.

Description

The text description of this multicast table entry.

Interfaces

The list of interfaces that are designated for forwarding (Fwd:) and filtering (Flt:).

4.9.75 show mac-filter-table stats

This command displays the Multicast Forwarding Database (MFDB) statistics.

Format

```
show mac-filter-table stats
```

Mode

```
Privileged EXEC and User EXEC
```

Total Entries

This displays the total number of entries that can possibly be in the Multicast Forwarding Database table.

Most MFDB Entries Ever Used

This displays the largest number of entries that have been present in the Multicast Forwarding Database table. This value is also known as the MFDB high-water mark.

Current Entries

This displays the current number of entries in the Multicast Forwarding Database table.

4.9.76 show mac notification

This command displays the MAC address change notification configuration.

Format

```
show mac notification
```

Mode

```
Privileged EXEC
```

MAC notification settings

This table displays the MAC notification settings (status and interval) for the device.

MAC notification status

This field displays the status of MAC notification traps for the device.
Possible values: `enabled`, `disabled`.

MAC notification interval

This field displays the MAC notification interval for the device.
Possible values: `1..2147483647`.

Interface

This field displays the number of the interface in `slot/port` format.

MAC notify

This field displays the status of MAC notification traps for this port.
Possible values: `enabled`, `disabled`

Mode

This field displays the mode for which action the device sends a MAC notification trap.
Possible values: `add, remove, all`

Last MAC address

This field displays the last MAC address added or removed from the address table for this interface.
Possible values: Valid MAC address in `aa:bb:cc:dd:ee:ff` notation.

Last MAC status

This field displays the status of the last MAC address on this interface.
Possible values: `added`, `removed`, `other`.

4.9.77 show monitor session

This command displays the port monitoring information for the system.

Format

`show monitor session <Session Number>`

Mode

`Global Config, Privileged EXEC, User EXEC`

Session

Display port monitor session settings.

Session Number

Session number. Enter `1` for the session number.

Session ID

Displays the session number of the port monitor session.
Possible values: `1`.

Admin Mode

Displays the status of the port monitoring feature.
Possible values: `Enable`, `Disable`.

Probe Port

Displays the interface configured as the probe port (in slot/port notation). If this value has not been configured, '`Not Configured`' will be displayed.

Mirrored Port

Displays the interface configured as the mirrored port (in slot/port notation). If this value has not been configured, '`Not Configured`' will be displayed.

Direction

Displays the direction which has been configured for the port.
Possible values: `rx` (receive), `tx` (transmit), `rx/tx` (receive and transmit)
If this value has not been configured, '`Not Configured`' will be displayed.

4.9.78 show port

This command displays port information.

Format

```
show port {<slot/port> | all} [name]
```

Mode

```
Privileged EXEC and User EXEC
```

Slot/Port

Valid slot and port number separated by forward slashes.

Name

When the optional command parameter `name` was specified, the output is different. It specifically includes the Interface Name as the second column, followed by other basic settings that are also shown by the normal command without the command parameter `name`.

Type

If not blank, this field indicates that this port is a special type of port. The possible values are:

`Mon` – this port is a monitoring port. Look at the Port Monitoring screens to find out more information.

`LA Mbr` – this port is a member of a Link Aggregation (LAG).

`Probe` – this port is a probe port.

Admin Mode

Indicates the Port control administration state. The port must be enabled in order for it to be allowed into the network. - May be enabled or disabled. The factory default is enabled.

Physical Mode

Indicates the desired port speed and duplex mode. If auto-negotiation support is selected, then the duplex mode and speed will be set from the auto-negotiation process. Note that the port's maximum capability (full duplex -100M) will be advertised. Otherwise, this object will determine the port's duplex mode and transmission rate. The factory default is Auto.

Physical Status

Indicates the port speed and duplex mode.

Link Status

Indicates whether the Link is up or down.

Link Trap

This object determines whether or not to send a trap when link status changes. The factory default is enabled.

Flow

Indicates if enable flow control is enabled on this port.

Device Status

Indicates whether or not the given port's link status is monitored by the device status.

VLAN Prio

This object displays the port VLAN priority.

4.9.79 show link-aggregation

This command displays an overview of all link-aggregations (LAGs) on the switch.

Format

```
show link-aggregation {<logical slot/port> | all}
```

Mode

```
Privileged EXEC and User EXEC
```

Logical slot/port

Valid slot and port number separated by forward slashes.

Name

The name of this link-aggregation (LAG). You may enter any string of up to 15 alphanumeric characters.

Link State

Indicates whether the Link is up or down.

Admin Mode

May be enabled or disabled. The factory default is enabled.

Link Trap Mode

This object determines whether or not to send a trap when link status changes. The factory default is enabled.

STP Mode

The Spanning Tree Protocol Administrative Mode associated with the port or link-aggregation (LAG). The possible values are:

`Disable` – Spanning tree is disabled for this port.

`Enable` – Spanning tree is enabled for this port.

Mbr Ports

A listing of the ports that are members of this link-aggregation (LAG), in slot/port notation. There can be a maximum of eight ports assigned to a given link-aggregation (LAG).

Port Speed

Speed of the link-aggregation port.

Type

This field displays the status designating whether a particular link-aggregation (LAG) is statically or dynamically maintained. The possible values of this field are `Static`, indicating that the link-aggregation is statically maintained; and `Dynamic`, indicating that the link-aggregation is dynamically maintained.

Active Ports

This field lists the ports that are actively participating in the link-aggregation (LAG).

4.9.80 show rmon-alarm

This command displays switch configuration information.

Format

```
show rmon-alarm
```

Mode

```
Privileged EXEC and User EXEC
```

4.9.81 show selftest

This command displays switch configuration information.

Format

```
show selftest
```

Mode

```
Privileged EXEC and User EXEC
```

Ramtest state

May be enabled or disabled. The factory default is enabled.

Reboot on error

May be enabled, disabled or seriousOnly. The factory default is enabled.

4.9.82 show serviceshell

This command displays the admin state of the service shell access.

Format

```
show serviceshell
```

Mode

```
Privileged EXEC and User EXEC
```

Admin state of service shell

Display the admin state of the service shell access
Possible values: Disabled, Enabled.

4.9.83 show storm-control

This command displays switch configuration information.

Format

```
show storm-control
```

Mode

```
Privileged EXEC and User EXEC
```

Ingress Limiting

May be enabled or disabled. The factory default is disabled.

Ingress Limiter Mode

Note: This command is available for the MACH4000 and PowerMICE devices.
Sets the global mode for the ingress limiter. The factory default is: Broadcasts only.

Egress Broadcast Limiting

May be enabled or disabled. The factory default is disabled.

Egress Limiting (all traffic)

May be enabled or disabled. The factory default is disabled.

802.3x Flow Control Mode

May be enabled or disabled. The factory default is disabled.

4.9.84 show storm-control limiters port

This command displays the limiter settings per port. "0" means that the respective limiter is disabled.

Format

```
show storm-control limiters port {<slot/port>|all}
```

Mode

```
Privileged EXEC and User EXEC
```

Ingress Mode

Note: This command is available for the devices RS20/RS30/RS40, MS20/MS30 and OCTOPUS.
Shows the mode for the ingress limiter. The factory default is: Broadcasts only.

Ingress Limit

Shows the ingress rate limit. The factory default is: 0.

Egress Broadcast Limit

Shows the egress broadcast rate limit. The factory default is: 0.

Egress Limit (all traffic)

Note: This command is available for the devices RS20/RS30/RS40, MS20/MS30 and OCTOPUS.
Shows the egress rate limit for all frame types.
The factory default is: 0.

4.9.85 show vlan

This command displays detailed information, including interface information, for a specific VLAN. The ID is a valid VLAN identification number

Format

```
show vlan <vlanid>
```

Mode

```
Privileged EXEC and User EXEC
```

VLAN ID

There is a VLAN Identifier (VID) associated with each VLAN. The range of the VLAN ID is 1 to 4042.

VLAN Name

A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of `Default`. This field is optional.

VLAN Type

Type of VLAN, which can be Default, (VLAN ID = 1), a static (one that is configured and permanently defined), or Dynamic (one that is created by GVRP registration).

VLAN Creation Time

Time since VLAN has been created:
d days, hh:mm:ss (System Uptime).

Interface

Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.

Current

Determines the degree of participation of this port in this VLAN. The permissible values are:

`Include` – This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

`Exclude` – This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

`Autodetect` – Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Configured

Determines the configured degree of participation of this port in this VLAN. The permissible values are:

`Include` – This port is always a member of this VLAN. This is equivalent to registration fixed in the IEEE 802.1Q standard.

`Exclude` – This port is never a member of this VLAN. This is equivalent to registration forbidden in the IEEE 802.1Q standard.

`Autodetect` – Specifies to allow the port to be dynamically registered in this VLAN via GVRP. The port will not participate in this VLAN unless a join request is received on this port. This is equivalent to registration normal in the IEEE 802.1Q standard.

Tagging

Select the tagging behavior for this port in this VLAN.

`Tagged -` specifies to transmit traffic for this VLAN as tagged frames.

`Untagged -` specifies to transmit traffic for this VLAN as untagged frames.

4.9.86 show vlan brief

This command displays a list of all configured VLANs.

Format

```
show vlan brief
```

Mode

```
Privileged EXEC and User EXEC
```

VLAN ID

There is a VLAN Identifier (vlanid)associated with each VLAN. The range of the VLAN ID is 1 to 4042.

VLAN Name

A string associated with this VLAN as a convenience. It can be up to 32 alphanumeric characters long, including blanks. The default is blank. VLAN ID 1 always has a name of `Default`. This field is optional.

VLAN Type

Type of VLAN, which can be Default, (VLAN ID = 1), a static (one that is configured and permanently defined), or a Dynamic (one that is created by GVRP registration).

VLAN Creation Time

Displays the time (as the system time up time) when the VLAN was created.

4.9.87 show vlan port

This command displays VLAN port information.

Format

```
show vlan port {<slot/port> | all}
```

Mode

```
Privileged EXEC and User EXEC
```

Slot/Port

Valid slot and port number separated by forward slashes. It is possible to set the parameters for all ports by using the selectors on the top line.

Port VLAN ID

The VLAN ID that this port will assign to untagged frames or priority tagged frames received on this port. The value must be for an existing VLAN. The factory default is `1`.

Acceptable Frame Types

Specifies the types of frames that may be received on this port. The options are 'VLAN only' and 'Admit All'. When set to 'VLAN only', untagged frames or priority tagged frames received on this port are discarded. When set to 'Admit All', untagged frames or priority tagged frames received on this port are accepted and assigned the value of the Port VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance to the 802.1Q VLAN specification.

Ingress Filtering

May be enabled or disabled. When enabled, the frame is discarded if this port is not a member of the VLAN with which this frame is associated. In a tagged frame, the VLAN is identified by the VLAN ID in the tag. In an untagged frame, the VLAN is the Port VLAN ID specified for the port that received this frame. When disabled, all frames are forwarded in accordance with the 802.1Q VLAN bridge specification. The factory default is disabled.

GVRP

The protocol for VLAN administration, GVRP (GARP VLAN Registration Protocol) is particularly used for the adjustment of terminal devices and VLAN switches. In realtime, it traces users log-in and log-off and provides updated configuration data to the network management system. In order to be able to use this protocol, GVRP has

to be supported by every switch.
GVRP may be enabled or disabled. The factory default is disabled.

Default Priority

The 802.1p priority assigned to tagged packets arriving on the port.

4.9.88 show voice vlan

Use this command to display the current global Voice VLAN Administrative Mode.
Voice VLAN is a feature used to automatically separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of using Voice VLAN is to ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high.

Format

```
show voice vlan
```

Mode

```
Privileged EXEC
```

Administrative Mode

Possible values: `Disable, Enable`

4.9.89 show voice vlan interface

Use this command to display Use this command to display a summary of the current Voice VLAN configuration for a specific interface.
`<slot/port>` indicates a specific physical interface.
all indicates all valid interfaces.

Format

```
show voice vlan interface {<slot/port> | all}
```

Mode

```
Privileged EXEC
```

<slot/port>

Indicates a specific physical interface.

all

Indicates all valid interfaces.

Interface

Displays the physical interface.

Voice VLAN Interface Mode

Displays the Voice VLAN Interface Mode.
Possible values: `Disabled, Enabled`.

Voice VLAN Authentication

Displays the Voice VLAN Authentication.
Possible values: `Disabled, Enabled`.

Voice VLAN Port Status

Displays the Voice VLAN Port Status.
Possible values: `Disabled, Enabled`.

4.9.90 shutdown

This command disables a port.

Default

`enabled`

Format

`shutdown`

Mode

`Interface Config`

no shutdown

This command enables a port.

Format

`no shutdown`

Mode

`Interface Config`

4.9.91 shutdown all

This command disables all ports.

Default

`enabled`

Format

`shutdown all`

Mode

`Global Config`

no shutdown all

This command enables all ports.

Format

`no shutdown all`

Mode

`Global Config`

4.9.92 snmp sync community-to-v3

This command enables the synchronization between the SNMPv1/v2 community table and the SNMPv3 password table.

Format

```
snmp sync community-to-v3
```

Mode

```
Global Config
```

- **no snmp sync community-to-v3**
  This command disables the synchronization between the SNMPv1/v2 community table and the SNMPv3 password table.

Format

```
no snmp sync community-to-v3
```

Mode

```
Global Config
```

4.9.93 snmp sync v3-to-community

This command enables the synchronization between the SNMPv3 password table and the SNMPv1/v2 community table.

Format

```
snmp sync v3-to-community
```

Mode

```
Global Config
```

- **no snmp sync v3-to-community**
  This command disables the synchronization between the SNMPv3 password table and the SNMPv1/v2 community table.

Format

```
no snmp sync v3-to-community
```

Mode

```
Global Config
```

4.9.94 snmp trap link-status

This command enables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See ‘snmp-server enable traps linkmode’ command.

Format

```
snmp trap link-status
```

Mode

```
Interface Config
```

no snmp trap link-status
This command disables link status traps by interface.

Note: This command is valid only when the Link Up/Down Flag is enabled. See ‘snmp-server enable traps linkmode’ command).

Format

```
no snmp trap link-status
```

Mode

```
Interface Config
```

4.9.95 snmp trap link-status all

This command enables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see “snmp-server enable traps linkmode”).

Format

```
snmp trap link-status all
```

Mode

```
Global Config
```

no snmp trap link-status all
This command disables link status traps for all interfaces.

Note: This command is valid only when the Link Up/Down Flag is enabled (see “snmp-server enable traps linkmode”).

Format

```
no snmp trap link-status all
```

Mode

```
Global Config
```

4.9.96 spanning-tree bpdumigrationcheck

This command enables BPDU migration check on a given interface.
This will force the specified port to transmit RST or MST BPDUs.
The **all** option enables BPDU migration check on all interfaces.

Format

```
spanning-tree bpdumigrationcheck {<slot/port>|all}
```

Mode

```
Global Config
```

no spanning-tree bpdumigrationcheck
This command disables BPDU migration check on a given interface. The `all` option disables BPDU migration check on all interfaces.

Format

```
no spanning-tree bpdumigrationcheck {<slot/
port>|all}
```

Mode

```
Global Config
```

4.9.97 speed

This command sets the speed and duplex setting for the interface.

Format

```
speed {<100 | 10> <half-duplex | full-duplex> |
       1000 full-duplex}
```

Mode

```
Interface Config
```

Acceptable values are:

1000 full-duplex

Set speed for the interface to `1000 Mbps`.
Set duplex mode for the interface to `full duplex`.

100 full-duplex

Set speed for the interface to `100 Mbps`.
Set duplex mode for the interface to `full duplex`.

100 half-duplex

Set speed for the interface to `100 Mbps`.
Set duplex mode for the interface to `half duplex`.

10 full-duplex

Set speed for the interface to `10 Mbps`.
Set duplex mode for the interface to `full duplex`.

10 half-duplex

Set speed for the interface to `10 Mbps`.
Set duplex mode for the interface to `half duplex`.

4.9.98 storm-control broadcast

This command enables the egress broadcast limiter globally.

Format

```
storm-control broadcast
```

Mode

```
Global Config
```

no storm-control broadcast

This command disables the egress broadcast limiter globally.

Format

```
no storm-control broadcast
```

Mode

```
Global Config
```

4.9.99 storm-control egress-limiting

This command enables or disables the egress limiter globally for all frame types.

Format

```
storm-control egress-limiting {disable | enable}
```

Mode

```
Global Config
```

4.9.100 storm-control ingress-limiting

This command enables or disables the ingress limiter globally.

Format

```
storm-control ingress-limiting {disable | enable}
```

Mode

```
Global Config
```

4.9.101 storm-control ingress-mode

Note: This command is available for the MACH4000 and PowerMICE devices.

This command sets the frame type for the ingress limiter globally to: BC or BC+MC.

Format

```
storm-control ingress-mode {bc | mc+bc}
```

Mode

```
Global Config
```

4.9.102 storm-control broadcast (port-related)

This command enables the broadcast limiter per port.
Enter the maximum number of broadcasts that the given port is allowed to send (unit: frames per second, min.: `0` (no limit), Default value: `0` (no limit)).

Format

```
storm-control broadcast <max. broadcast rate>
```

Mode

```
Interface Config
```

4.9.103 storm-control egress-limit

Note: This command is available for the RS20/RS30/RS40, MS20/MS30 and OCTOPUS devices.

Sets the egress rate limit in kbit/s. "0" means: no limit.

Format

```
storm-control egress-limit <max. egress rate>
```

Mode

```
Interface Config
```

4.9.104 storm-control ingress-limit

Sets the ingress rate limit in kbit/s. "0" means: no limit.

Format

```
storm-control ingress-limit <max. ingress rate>
```

Mode

```
Interface Config
```

4.9.105 storm-control ingress-mode

Note: This command is available for the RS20/RS30/RS40, MS20/MS30, OCTOPUS devices.

This command sets the frame type for the ingress limiter to:
All, BC, BC+MC, BC+MC+uUC.

Format

```
storm-control ingress-mode {all | bc | mc+bc |
uuc+mc+bc}
```

Mode

```
Interface Config
```

4.9.106 storm-control flowcontrol

This command enables 802.3x flow control for the switch.

Note: This command only applies to full-duplex mode ports.

Default

```
disabled
```

Format

```
storm-control flowcontrol
```

Mode

```
Interface Config
Global Config
```

no storm-control flowcontrol

This command disables 802.3x flow control for the switch.

Note: This command only applies to full-duplex mode ports.

Format

```
no storm-control flowcontrol
```

Mode

```
Interface Config
Global Config
```

4.9.107 storm-control flowcontrol per port

This command enables 802.3x flow control for the port.

Note: This command only applies to full-duplex mode ports.

Default

`enabled`

Format

`storm-control flowcontrol`

Mode

`Interface Config`

no storm-control flowcontrol per port

This command disables 802.3x flow control for the port.

Note: This command only applies to full-duplex mode ports.

Format

`no storm-control flowcontrol`

Mode

`Interface Config`

4.9.108 vlan

This command creates a new VLAN and assigns it an ID. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 1-4042.

Format

```
vlan <1-4042>
```

Mode

```
VLAN database
```

no vlan

This command deletes an existing VLAN. The ID is a valid VLAN identification number (ID 1 is reserved for the default VLAN). VLAN range is 1-4042.

Format

```
no vlan <1-4042>
```

Mode

```
VLAN database
```

4.9.109 vlan0-transparent-mode

Activate the “Transparent Mode“ to be able to switch priority tagged frames without a VLAN affiliation thus with VLAN-ID “0”.
In this mode the VLAN-ID “0” persists in the frame, irrespective of the Port VLAN ID setting in the “VLAN Port“ dialog.

Note: For PowerMICE, MACH100, MACH1000 and MACH4000:
In transparency mode devices ignore received vlan tags. Set the vlan membership of the ports to untagged for all vlans.

Note: For RS20/RS30/RS40, MS20/MS30 and OCTOPUS:
In transparency mode devices ignore the configured port vlan id. Set the vlan membership of the ports from vlan 1 to untagged or member.

Format

```
vlan0-transparent-mode {disable|enable}
```

Mode

```
VLAN database
```

4.9.110 vlan acceptframe

This command sets the frame acceptance mode per interface. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default

`Admit All`

Format

`vlan acceptframe <vlanonly | all | untaggedonly>`

Mode

`Interface Config`

all

Untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port.

vlanonly

Only frames received with a VLAN tag will be forwarded. Other frames will be dropped.

untaggedonly

Only frames received without a VLAN tag will be forwarded. Other frames will be dropped.

Note: This command is available for devices of the RS20/RS30/RS40, MS20/MS30, MACH102, RSR20/RSR30, MACH1020/MACH1030 and OCTOPUS family.

- **no vlan acceptframe**
  This command sets the frame acceptance mode per interface to `Admit All`. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format

```
no vlan acceptframe
```

Mode

```
Interface Config
```

4.9.111 vlan database

This command switches into the global VLAN mode.

Default

```
Admit All
```

Format

```
vlan database
```

Mode

```
Privileged EXEC
```

4.9.112 vlan ingressfilter

This command enables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default

```
disabled
```

Format

```
vlan ingressfilter
```

Mode

```
Interface Config
```

- **no vlan ingressfilter**
  This command disables ingress filtering. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format

```
no vlan ingressfilter
```

Mode

```
Interface Config
```

4.9.113 vlan name

This command changes the name of a VLAN. The name is an alphanumeric string of up to 32 characters, and the ID is a valid VLAN identification number. ID range is 1-4042.

Default

The name for VLAN ID 1 is always Default. The name for other VLANs is defaulted to a blank string.

Format

```
vlan name <1-4042> <newname>
```

Mode

```
VLAN database
```

no vlan name

This command sets the name of a VLAN to a blank string. The VLAN ID is a valid VLAN identification number. ID range is 1-4042.

Format

```
no vlan name <1-4042>
```

Mode

```
VLAN database
```

4.9.114 vlan participation

This command configures the degree of participation for a specific interface in a VLAN. The ID is a valid VLAN identification number, and the interface is a valid interface number.

Format

```
vlan participation
  <exclude | include | auto> <1-4042>
```

Mode

```
Interface Config
```

Participation options are:

include

The interface is always a member of this VLAN. This is equivalent to registration fixed.

exclude

The interface is never a member of this VLAN. This is equivalent to registration forbidden.

auto

The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

4.9.115 vlan participation all

This command configures the degree of participation for all interfaces in a VLAN. The ID is a valid VLAN identification number.

Format

```
vlan participation all <exclude | include | auto>
<1-4042>
```

Mode

```
Global Config
```

Participation options are:

include

The interface is always a member of this VLAN. This is equivalent to registration fixed.

exclude

The interface is never a member of this VLAN. This is equivalent to registration forbidden.

auto

The interface is dynamically registered in this VLAN by GVRP. The interface will not participate in this VLAN unless a join request is received on this interface. This is equivalent to registration normal.

4.9.116 vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces. For VLAN Only mode, untagged frames or priority frames received on this interface are discarded. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Default

`Admit All`

Format

`vlan port acceptframe all <vlanonly | all>`

Mode

`Global Config`

no vlan port acceptframe all

This command sets the frame acceptance mode for all interfaces to `Admit All`. For Admit All mode, untagged frames or priority frames received on this interface are accepted and assigned the value of the interface VLAN ID for this port. With either option, VLAN tagged frames are forwarded in accordance with the IEEE 802.1Q VLAN Specification.

Format

`no vlan port acceptframe all`

Mode

`Global Config`

4.9.117 vlan port ingressfilter all

This command enables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Default

```
disabled
```

Format

```
vlan port ingressfilter all
```

Mode

```
Global Config
```

- **no vlan port ingressfilter all**
  This command disables ingress filtering for all ports. If ingress filtering is disabled, frames received with VLAN IDs that do not match the VLAN membership of the receiving interface are admitted and forwarded to ports that are members of that VLAN.

Format

```
no vlan port ingressfilter all
```

Mode

```
Global Config
```

4.9.118 vlan port pvid all

This command changes the VLAN ID for all interface.

Default

`1`

Format

`vlan port pvid all <1-4042>`

Mode

`Global Config`

no vlan port pvid all

This command sets the VLAN ID for all interfaces to 1.

Format

`no vlan port pvid all <1-4042>`

Mode

`Global Config`

4.9.119 vlan port tagging all

This command configures the tagging behavior for all interfaces in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format

```
vlan port tagging all <1-4042>
```

Mode

```
Global Config
```

- **no vlan port tagging all**
  This command configures the tagging behavior for all interfaces in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format

```
no vlan port tagging all <1-4042>
```

Mode

```
Global Config
```

4.9.120 vlan pvid

This command changes the VLAN ID per interface.

Default

```
1
```

Format

```
vlan pvid <1-4042>
```

Mode

```
Interface Config
```

no vlan pvid

This command sets the VLAN ID per interface to 1.

Format

```
no vlan pvid <1-4042>
```

Mode

```
Interface Config
```

4.9.121 vlan tagging

This command configures the tagging behavior for a specific interface in a VLAN to enabled. If tagging is enabled, traffic is transmitted as tagged frames. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format

```
vlan tagging <1-4042>
```

Mode

```
Interface Config
```

- **no vlan tagging**
  This command configures the tagging behavior for a specific interface in a VLAN to disabled. If tagging is disabled, traffic is transmitted as untagged frames. The ID is a valid VLAN identification number.

Format

```
no vlan tagging <1-4042>
```

Mode

```
Interface Config
```

4.9.122 voice vlan (Global Config Mode)

This command enables the Voice VLAN feature.

Voice VLAN is a feature used to automatically separate voice and data traffic on a port, by VLAN and/or priority. A primary benefit of using Voice VLAN is to ensure that the sound quality of an IP phone is safeguarded from deteriorating when the data traffic on the port is high.

Default

```
Disabled
```

Format

```
voice vlan
```

Mode

```
Global Config
```

no voice vlan

This command disables the Voice VLAN feature.

Default

```
Disabled
```

Format

```
no voice vlan
```

Mode

```
Global Config
```

4.9.123 voice vlan <id>

Use this command to configure VLAN tagging and 802.1p priority.

Format

```
voice vlan <id> [dot1p <priority>] }
```

Mode

```
Interface Config
```

<id>

Enter the Voice VLAN ID.

dot1p

Configure Voice VLAN 802.1p priority tagging for voice traffic.

<priority>

The priority tag range is 0–7.

no voice vlan

This command disables the Voice VLAN feature on the interface.

Default

```
Disabled
```

Format

```
no voice vlan
```

Mode

```
Interface Config
```

4.9.124 voice vlan dot1p

Use this command to configure Voice VLAN 802.1p priority tagging for voice traffic.

Format

```
voice vlan dot1p <priority>
```

Mode

```
Interface Config
```

<priority>

Configure Voice VLAN 802.1p priority tagging for voice traffic. The priority tag range is 0–7.

4.9.125 voice vlan none

Use this command to allow the IP phone to use its own configuration to send untagged voice traffic.

Format

```
voice vlan none
```

Mode

```
Interface Config
```

4.9.126 voice vlan untagged

Use this command to configure the phone to send untagged voice traffic.

Format

```
voice vlan untagged
```

Mode

```
Interface Config
```

4.9.127 voice vlan auth

Use this command to set Voice VLAN Authentication Mode. If disabled, VOIP devices which are detected via LLDP-med will have access to the Voice VLAN without authentication.

Default

```
Enabled
```

Format

```
voice vlan auth [enabled | disabled]
```

Mode

```
Interface Config
```

disable

VOIP devices which are detected via LLDP-MED will have access to the Voice VLAN without authentication.

enable

VOIP devices which are detected via LLDP-MED will not have access to the Voice VLAN without authentication.

4.10 User Account Management Commands

These commands manage user accounts.

4.10.1 disconnect

This command closes a telnet session.

Format

```
disconnect {<sessionID> | all}
```

Mode

```
Privileged EXEC
```

Session ID

Enter the session ID (1-11).

4.10.2 show loginsession

This command displays current telnet and serial port connections to the switch.

Format

```
show loginsession
```

Mode

```
Privileged EXEC and User EXEC
```

ID

```
Login Session ID
```

User Name

The name the user will use to login using the serial port or Telnet. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to 8 characters, and is not case sensitive. Two users are included as the factory default, ‘admin’ and ‘user’.

Connection From

IP address of the telnet client machine or EIA-232 for the serial port connection.

Idle Time

Time this session has been idle.

Session Time

Total time this session has been connected.

4.10.3 show users

This command displays the configured user names and their settings. This command is only available for users with readwrite privileges. The SNMPv3 fields will only be displayed if SNMP is available on the system.

Format

```
show users
```

Mode

```
Privileged EXEC
```

User Name

The name the user will use to login using the serial port, Telnet or Web. A new user may be added to the switch by entering a name in a blank entry. The user name may be up to eight characters, and is not case sensitive. Two users are included as the factory default, ‘admin’ and ‘user’

Access Mode

Shows whether the operator is able to change parameters on the switch (Read/Write) or is only able to view them (Read Only). As a factory default, the ‘admin’ user has Read/Write access and the ‘user’ has Read Only access. There can only be one Read/Write user and up to five Read Only users.

SNMPv3 AccessMode

This field displays the SNMPv3 Access Mode. If the value is set to ReadWrite, the SNMPv3 user will be able to set and retrieve parameters on the system. If the value is set to ReadOnly, the SNMPv3 user will only be able to retrieve parameter information. The SNMPv3 access mode may be different than the CLI and Web access mode.

SNMPv3 Authentication

This field displays the authentication protocol to be used for the specified login user.

SNMPv3 Encryption

This field displays the encryption protocol to be used for the specified login user.

4.10.4 users defaultlogin

This command assigns the authentication login list to use for non-configured users when attempting to log in to the system. This setting is overridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format

```
users defaultlogin <listname>
```

Mode

```
Global Config
```

listname

Enter an alphanumeric string of not more than 15 characters.

4.10.5 users login <user>

Enter user name.

Format

```
users login <user> <listname>
```

Mode

```
Global Config
```

Note:

When assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable (use 'authentication login <listname> [method1 [method2 [method3]]]').

no users login <user>

This command removes an operator.

Format

```
no users login <user> <listname>
```

Mode

```
Global Config
```

Note:

The ‘admin’ user account cannot be deleted.

4.10.6 users access

This command sets access for a user: readonly/readwrite.

Format

```
users access <username> {readonly | readwrite}
```

Mode

```
Global Config
```

<username>

Enter a name up to 32 alphanumeric characters in length.

readonly

Enter the access mode as readonly.

readwrite

Enter the access mode as readwrite.

no users access

This command deletes access for a user.

Format

```
no users access <username>
```

Mode

```
Global Config
```

4.10.7 users name

This command adds a new user (account) if space permits. The account <username> can be up to eight characters in length. The name may be comprised of alphanumeric characters as well as the dash (‘-’) and underscore (‘_’). The <username> is not case-sensitive.
Six user names can be defined.

Format

```
users name <username>
```

Mode

```
Global Config
```

no users name

This command removes an operator.

Format

```
no users name <username>
```

Mode

```
Global Config
```

Note:

The ‘admin’ user account cannot be deleted.

4.10.8 users passwd

This command is used to change a password. The password should not be more than eight alphanumeric characters in length. If a user is authorized for authentication or encryption is enabled, the password must be at least eight alphanumeric characters in length. The username and password are case-sensitive. When a password is changed, a prompt will ask for the former password. If none, press enter.
Note: Make sure, that the passwords of the users differ from each other. If two or more users try to choose the same password, the CLI will display an error message.

Default

```
No Password
```

Format

```
users passwd <username> {<password>}
```

Mode

```
Global Config
```

no users passwd
This command sets the password of an existing operator to blank. When a password is changed, a prompt will ask for the operator's former password. If none, press enter.

Format

```
no users passwd <username> {<password>}
```

Mode

```
Global Config
```

4.10.9 users snmpv3 accessmode

This command specifies the snmpv3 access privileges for the specified login user. The valid accessmode values are `readonly` or `readwrite`. The `<username>` is the login user name for which the specified access mode applies. The default is `readwrite` for 'admin' user; `readonly` for all other users

Default

`admin -- readwrite; other -- readonly`

Format

`users snmpv3 accessmode <username> <readonly | readwrite>`

Mode

`Global Config`

no users snmpv3 accessmode

This command sets the snmpv3 access privileges for the specified login user as `readwrite` for the 'admin' user; `readonly` for all other users. The <username> is the login user name for which the specified access mode will apply.

Format

`no users snmpv3 accessmode <username>`

Mode

`Global Config`

4.10.10 users snmpv3 authentication

This command specifies the authentication protocol to be used for the specified login user. The valid authentication protocols are `none`, `md5` or `sha`. If md5 or sha are specified, the user login password is also used as the snmpv3 authentication password and therefore must be at least eight characters in length. The <username> is the login user name associated with the authentication protocol.

Default

```
no authentication
```

Format

```
users snmpv3 authentication <username> <none | md5 | sha>
```

Mode

```
Global Config
```

no users snmpv3 authentication

This command sets the authentication protocol to be used for the specified login user to `none`. The <username> is the login user name for which the specified authentication protocol will be used.

Format

```
users snmpv3 authentication <username>
```

Mode

```
Global Config
```

4.10.11 users snmpv3 encryption

This command specifies the encryption protocol to be used for the specified login user. The valid encryption protocols are des or `none`.
If des is specified, the required key may be specified on the command line. The `key` may be up to 16 characters long. If the `des` protocol is specified but a key is not provided, the user will be prompted for the key. When using the des protocol, the user login password is also used as the snmpv3 encryption password and therefore must be at least eight characters in length.
If `none` is specified, a key must not be provided. The `<username>` is the login user name associated with the specified encryption.

Default

```
no encryption
```

Format

```
users snmpv3 encryption <username> <none |
des[key]>
```

Mode

```
Global Config
```

no users snmpv3 encryption

This command sets the encryption protocol to `none`. The <username> is the login user name for which the specified encryption protocol will be used.

Format

```
no users snmpv3 encryption <username>
```

Mode

```
Global Config
```

4.11 System Utilities

This section describes system utilities.

4.11.1 address-conflict

This command configures the setting for detection possible address conflicts of the agent´s IP address with other devices´ IP addresses in the network.

Format

```
address-conflict
  {detection-mode { active-only | disable |
   enable | passive-only}|
   ongoing-detection { disable | enable } }
```

Mode

```
Global Config
```

detection mode

Configure the device's address conflict detection mode (active-only, disable, enable or passive-only). Default value: `enable`.

ongoing detection

Disable or enable the ongoing address conflict detection. Default value: `enable`.

4.11.2 boot skip-aca-on-boot

Use this command to skip external memory (AutoConfiguration Adapter ACA21) during boot phase to shorten startup duration.
The ACA21 functionality will be available after the boot phase.

Format

```
boot skip-aca-on-boot {disable | enable}
```

Mode

```
Global Config
```

Default

```
disabled
```

enable

Enable ACA21 skip during boot phase.

disable

Disable ACA21 skip during boot phase.

4.11.3 show boot skip-aca-on-boot

Use this command display the status of the option of skipping external memory (AutoConfiguration Adapter ACA21) during boot phase.

Format

```
show boot skip-aca-on-boot
```

Mode

```
Global Config
```

Default

```
disabled
```

Enabled

ACA21 skip during boot phase is enabled.

Disabled

ACA21 skip during boot phase is disabled.

4.11.4 cablestatus

This command tests the cable attached to an interface for short or open circuit. During the test the traffic is interrupted on this port.

Format

```
cablestatus <slot/port>
```

Mode

```
Privileged EXEC
```

4.11.5 clear eventlog

Clear the event log. The CLI will ask for confirmation.
Answer `y` (yes) or `n` (no).
The CLI displays the end of this operation.

Format

```
clear eventlog
```

Mode

```
Privileged EXEC
```

4.11.6 traceroute

This command is used to discover the routes that packets actually take when traveling to their destination through the network on a hop-by-hop basis. <ipaddr> should be a valid IP address.
The optional port parameter is the UDP port used as the destination of packets sent as part of the traceroute. This port should be an unused port on the destination system. [port] should be a valid decimal integer in the range of 0 (zero) to 65,535. The default value is `33434`.

Format

```
traceroute <ipaddr> [port]
```

Mode

```
Privileged EXEC
```

4.11.7 clear arp-table-switch

This command clears the agent´s ARP table (cache).

Format

```
clear arp-table-switch
```

Mode

```
Privileged EXEC
```

4.11.8 clear config

This command resets the configuration in RAM to the factory defaults without powering off the switch.

Format

```
clear config
```

Mode

```
Privileged EXEC
```

4.11.9 clear config factory

This command resets the whole configuration to the factory defaults. Configuration data and scripts stored in nonvolatile memory will also be deleted.

Format

```
clear config factory
```

Mode

```
Privileged EXEC
```

4.11.10 clear counters

This command clears the stats for a specified <slot/port>or for all the ports or for the entire switch based upon the argument.

Format

```
clear counters {<slot/port> | all}
```

Mode

```
Privileged EXEC
```

4.11.11 clear hiper-ring

This command clears the HIPER Ring configuration (deletes it).

Format

```
clear hiper-ring
```

Mode

```
Privileged EXEC
```

4.11.12 clear igmpsnooping

This command clears the tables managed by the IGMP Snooping function and will attempt to delete these entries from the Multicast Forwarding Database.

Format

```
clear igmpsnooping
```

Mode

```
Privileged EXEC
```

4.11.13 clear mac-addr-table

This command clears the switch's MAC address table (the forwarding database that contains the learned MAC addresses).

Note: this command does not affect the MAC filtering table.

Format

```
clear mac-addr-table
```

Mode

```
Privileged EXEC
```

4.11.14 clear pass

This command resets all user passwords to the factory defaults without powering off the switch. You are prompted to confirm that the password reset should proceed.

Format

```
clear pass
```

Mode

```
Privileged EXEC
```

4.11.15 clear link-aggregation

This command clears all link-aggregations (LAGs).

Format

```
clear link-aggregation
```

Mode

```
Privileged EXEC
```

4.11.16 clear signal-contact

This command clears the signal-contact output configuration.
Switches the signal contact 1´s mode to `auto` and its manual setting to `open`.
Switches the signal contact 2´s mode to `manual` and its manual setting to `closed`.
Enables the monitoring of the power supplies for signal contact 1 only.
Disables the sending of signal contact traps.

Format

```
clear signal-contact
```

Mode

```
Privileged EXEC
```

4.11.17 clear traplog

This command clears the trap log.

Format

```
clear traplog
```

Mode

```
Privileged EXEC
```

4.11.18 clear ring-coupling

This command clears the ring-coupling configuration.

Format

```
clear ring-coupling
```

Mode

```
Privileged EXEC
```

4.11.19 clear vlan

This command resets VLAN configuration parameters to the factory defaults.

Format

```
clear vlan
```

Mode

```
Privileged EXEC
```

4.11.20 config-watchdog

If the function is enabled and the connection to the switch is interrupted for longer than the time specified in “timeout [s]”, the switch then loads the last configuration saved.

Format

```
config-watchdog {admin-state {disable|enable}|
timeout <10..600>}
```

Mode

```
Global Config
```

admin-state

Enable or disable the Auto Configuration Undo feature
Default value: `disabled`.

timeout

Configure the Auto Configuration Undo timeout (unit: seconds).

4.11.21 copy

This command uploads and downloads to/from the switch. Remote URLs can be specified using tftp.
`copy` (without parameters) displays a brief explanation of the most important copy commands. A list of valid commands is provided below.
The command can be used to the save the running configuration to nvram by specifying the source as `system:running-config` and the destination as `nvram:startup-config`.

Default

```
none
```

Format

```
copy
copy aca:script <sourcefilename> nvram:script
  [targetfilename]
copy aca:capturefilter <sourcefilename>
  nvram:capturefilter [targetfilename]
```

```
copy aca:sfp-white-list <sourcefilename>
  nvram:sfp-white-list
copy nvram:backup-image system:image
copy nvram:clibanner <url>
copy nvram:capture aca:capture
copy nvram:capture <url>
copy nvram:capturefilter <sourcefilename>
  aca:capturefilter <targetfilename>
copy nvram:capturefilter <sourcefilename>
copy nvram:errorlog <url>
copy nvram:script <sourcefilename> aca:script
  [targetfilename]
copy nvram:script <sourcefilename> <url>
copy nvram:startup-config <url>
copy nvram:startup-config system:running-config
copy nvram:traplog <url>
copy system:running-config nvram:startup-config
<url>
copy system:running-config <url>
copy <tftp://ip/filepath/fileName>
  nvram:sfp-white-list
copy tftp://<server_ip>/<path_to_pem>
     nvram:httpscert
copy <url> nvram:clibanner
copy <url> nvram:capturefilter <destfilename>
copy aca:capturefilter <sourcefilename>
  nvram:capturefilter <destfilename>
copy <url> nvram:script <destfilename>
copy <url> nvram:startup-config
copy <url> system:image
copy <url> system:running-config
copy <url> system:bootcode
```

Mode

Privileged EXEC

- **copy aca:script <sourcefilename> nvram:script [targetfilename]**

  Copies the script from the Auto Configuration Adapter.

  – `sourcefilename`: Filename of source configuration Script. Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.

  – `targetfilename`: Filename on the switch's NVRAM. Filename length may be max. 20 characters, including extension '.cli'.

- **copy aca:capturefilter <sourcefilename> nvram:capturefilter [targetfilename]**

  Copies a capture filter file from the Auto Configuration Adapter.

  – `sourcefilename`: Filename of source capture filter expressions file.

  – `targetfilename`: Filename on the switch's NVRAM.

- **copy aca:sfp-white-list <sourcefilename> nvram:sfp-white-list**

  Use this command to load the SFP white list file from a ACA21.
  Note: In order to delete the SFP white list file from the flash memory: use the command `clear sfp-white-list`.
  The `clear config factory` command deletes the SFP white list, too.

- **copy nvram:backup-image system:image**

  Use this command to swap current and backup images. The backup image (backup.bin) and current image (main.bin) will exchange the file name, after reboot the both OS and configuration files will be swapped.

- **copy <tftp://ip/filepath/fileName> nvram:sfp-white-list**

  Use this command to load the SFP white list file from a TFTP server.
  Note: In order to delete the SFP white list file from the flash memory: use the command `clear sfp-white-list`.
  The `clear config factory` command deletes the SFP white list, too.

- **copy tftp://<server_ip>/<path_to_pem> nvram:httpscert**

  Use this command for uploading a PEM certificate for HTTPS over TFTP
  Note: Reboot the device or re-enable the HTTPS server after uploading a PEM certificate.

- **copy nvram:clibanner <url>**

  Downloads the CLI banner file via TFTP using <tftp://ip/filepath/fileName>.

- **copy nvram:capture aca:capture**

  Save the internal packet capture file to the Auto Configuration Adapter ACA21 (file name: "capture.cap").

- **copy nvram:capture <url>**

  Save the internal packet capture file to a tftp URL using <tftp://ip/filepath/fileName>.

copy nvram:capturefilter <sourcefilename> aca:capturefilter <targetfilename>

Save a capture filter file from the flash memory to the Auto Configuration Adapter.

– sourcefilename: Filename of source capture filter expressions file.

– targetfilename: Filename of target capture filter expressions file.

copy nvram:capturefilter <sourcefilename> <url>

Save the internal packet capture filter file from the flash memory to a tftp URL using <tftp://ip/filepath/fileName>.

– sourcefilename: Filename of source capture filter expressions file.

copy nvram:errorlog <url>

Uploads Errorlog file.

– <url>: Uploads Error log file using <tftp://ip/filepath/fileName>.

copy nvram:script <sourcefilename> aca:script [targetfilename]

Uploads configuration script file. Save the script to the AutoConfiguration Adapter.

– `sourcefilename`: Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.

– `targetfilename`: Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.

copy nvram:script <sourcefilename> <url>

Uploads Configuration Script file using <tftp://ip/filepath/fileName>. Filename length may be max. 20 characters, including extension '.cli'.

– `sourcefilename`: Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.

- **copy nvram:startup-config <url>**

  Uploads config file using <tftp://ip/filepath/fileName>.

- **copy nvram:startup-config system:running-config**

  Uploads/Copies config file. The target is the currently running configuration.

- **copy nvram:traplog <url>**

  Uploads Trap log file. Uploads Trap log file using <tftp://ip/filepath/fileName>.

- **copy system:running-config nvram:startup-config**

  Copies system config file. Save the running configuration to NVRAM.

- **copy system:running-config <url>**

  Copies system config file. Uploads system running-config via tftp using <tftp://ip/filepath/fileName>.

copy <url> nvram:clibanner

This feature provides a privileged user the capability to change the CLI default banner:

```
-------------------------------------------------
Copyright (c) 2004-2015 <Company Name>

          All rights reserved

     <Product Name> Release L3P-09.0.00

     (Build date 2015-02-02 02:02)


     System Name:  <Product Name>
     Mgmt-IP    :  a.b.c.d
     1.Router-IP:  0.0.0.0
     Base-MAC   :  aa:bb:cc:dd:ee:ff
     System Time:  2015-02-02 15:15:15
-------------------------------------------------
```

The command uploads the CLI banner file by tftp using `<tftp://ip/filepath/fileName>`.

After the upload you logout from CLI and the new CLI banner file will be displayed at the next login.

– `url`: Upload CLI banner file using <tftp://ip/filepath/fileName>.

If no cli banner file is defined, the default cli banner is displayed (see above).

Note: Note that the CLI banner file you created has the following properties:

- Use ASCII format (character codes `0x20` .. `0x7F`, `\n` and `\t` as C-like sequences)
- Do not use regular expressions
- Do not exeed the limit of 2048 byte
- Do not exceed the limit of 20 lines
- Do not exceed the limit of 80 characters per line
- A device can only have one banner file at the moment
- Save the CLI banner file as *.bnr.

Note: Alternatively, use the following command to define the text for the CLI login banner. This banner replaces the banner before login.
`set clibanner text <Max. 2048 characters>`
See “set clibanner” on page 337

no clibanner

This command deletes an existing CLI banner file.

copy <url> nvram:capturefilter <destfilename>

Load a Capture Filter file from a tftp URL into the flash memory using `<tftp://ip/filepath/fileName>`.
– `destfilename`: Destination filename of capture filter expressions file.

copy aca:capturefilter <sourcefilename> nvram:capturefilter <targetfilename>

Load a capture filter file from AutoConfiguration Adapter ACA21 into the flash memory.

– `sourcefilename`: Filename of source capture filter expressions file.

– `targetfilename`: Specify the file name on the switch's NVRAM.

copy <url> nvram:script <destfilename>

Downloads Configuration Script file using <tftp://ip/filepath/fileName>.
– `destfilename`: Filename length may be max. 20 characters, including extension '.cli' or '.CLI'.

copy <url> nvram:sshkey-dsa

Downloads IP secure shell (SSH) DSA key file by tftp using <tftp://ip/filepath/fileName>.

- **copy <url> nvram:sshkey-rsa1**

  Downloads IP secure shell (SSH) RSA1 key file by tftp using <tftp://ip/filepath/fileName>.

- **copy <url> nvram:sshkey-rsa2**

  Downloads IP secure shell (SSH) RSA2 key file by tftp using <tftp://ip/filepath/fileName>.

- **copy <url> nvram:startup-config**

  Downloads Config file by tftp using <tftp://ip/filepath/fileName>.

- **copy <url> system:image**

  Downloads code file by tftp using <tftp://ip/filepath/fileName>.

- **copy <url> system:running-config**

  Downloads Code/Config file using <tftp://ip/filepath/fileName>.
  The target is the currently running configuration.

- **copy <url> system:bootcode**

  Use the "copy <url> system:bootcode" command to load the boot-code file via tftp into the device. For <url> enter the path of the tftp server using the following notation: "<tftp://ip/filepath/fileName>", e.g. "tftp://10.1.112.214/switch/switch01.cfg".

- **clear sfp-white-list**

  Use this command to delete the SFP white list file from the flash memory.
  Note: The `clear config factory` command deletes the SFP white list, too.

4.11.22 device-status connection-error

This command configures the device status link error monitoring for this port.

Default

```
ignore
```

Format

```
device-status connection-error {ignore|propagate}
```

Mode

```
Interface Config
```

4.11.23 device-status monitor

This command configures the device-status.

Format

```
device-status monitor
 {aca-removal | all | connection-error |
hiper-ring |
  module-removal | power-supply-1 |
  power-supply-2 | power-supply-3-1 |
  power-supply-3-2 | power-supply-4-1 |
  power-supply-4-2 | ring-coupling | temperature }
   {error|ignore}
device-status trap {disable|enable}
```

Mode

`Global Config`

monitor

Determines the monitoring of the selected event or all events.
– `error` If the given event signals an error, the device state will also signal `error`,
– `ignore` Ignore the given event - even if it signals an error, the device state will not signal 'error' because of that.

trap

Configure if a trap is sent when the device status changes its state.
– `enable` enables sending traps,
– `disable` disables sending traps.

4.11.24 logout

This command closes the current telnet connection or resets the current serial connection.

Note: Save configuration changes before logging out.

Format

```
logout
```

Mode

```
Privileged EXEC
```

4.11.25 mac-address conflict operation

Use this command to enable sending a trap if the device detects a packet with its own MAC address in the network.
Possible values: `enabled`, `disabled`
Default value: `enabled`

Format

```
mac-address-conflict operation
```

Mode

```
Privileged EXEC
```

no mac-address conflict operation

Use this command to disable sending a trap if the device detects a packet with its own MAC address in the network.

Format

```
no mac-address conflict operation
```

Mode

```
Privileged EXEC
```

4.11.26 ping

This command checks if another computer is on the network and listens for connections. To use this command, configure the switch for network (in-band) connection. The source and target devices must have the ping utility enabled and running on top of TCP/IP. The switch can be pinged from any IP workstation with which the switch is connected through the default VLAN (VLAN 1), as long as there is a physical path between the switch and the workstation. The terminal interface sends, three pings to the target station.

Format

```
ping <ipaddr>
```

Mode

```
Privileged EXEC and User EXEC
```

4.11.27 signal-contact connection-error

This command configures the signal contact link error monitoring for this port.

Format

```
signal-contact connection-error {disable|enable}
```

Mode

```
Interface Config
```

disable

A link down event on this port will be not monitored by a signal contact (default).

enable

A link down event on this port will be monitored by a signal contact.

4.11.28 signal-contact

This command configures the signal contacts.

Format

```
signal-contact {1|2|all}
 {mode {auto|device-status|manual}
 |monitor {aca-removal|
   all|
   connection-error|hiper-ring|module-removal
   |power-supply-1| power-supply-2
   |power-supply-3-1|power-supply-3-2
   |power-supply-4-1|power-supply-4-2
   |ring-coupling|temperature} {disable|enable}
 |state {closed|open}
 |trap {disable|enable} }
```

Mode

`Global Config`

Contact No.

Selection of the signal contact:
– `1` signal contact 1,
– `2` signal contact 2,
– `all` signal contact 1 and signal contact 2.

mode

Selection of the operational mode:
– `auto` function monitoring,
– `device-status` the device-status determines the signal contact´s status.
– `manual` manually setting the signal contact.

monitor

Enables or disables the monitoring of the selected event or all events.
– `enable` monitoring,
– `disable` no monitoring.

state

Set the manual setting of the signal contact:
– `closed` ,
– `open`.
Only takes immediate effect in manual mode.

trap

Configures the sending of traps concerning the signal contact.
– `enable` enables sending traps,
– `disable` disables sending traps.

4.11.29 temperature

Note: The command is available for RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH100, MACH1000, PowerMICE, MACH4000 and OCTOPUS devices.

This command configures the lower and upper temperature limit for the device. If these limits are exceeded, a trap is sent. The unit for the temperature limit is °C (Celsius), the minimum value is `-99`, the maximum value is 99. The default for the lower limit is 0, for the upper limit, it is `70`.

Note: To give the temperature in Fahrenheit, use the suffix f.

Format

```
temperature {lower-limit|upper-limit} <temperature
value> [c|f]
```

Mode

`Global Config`

lower-limit

Configure the lower temperature limit.

upper-limit

Configure the upper temperature limit.

4.11.30 reboot

This command resets the switch (cold start) after a given time delay, for warm start See “reload” on page 335. Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Format

```
reboot {delay <seconds>}
```

Mode

```
Privileged EXEC
```

<seconds>

The number of seconds after which the switch will reboot.
Value range: `None` (no reboot sceduled), `0 .. 2147483` sec (= 596 h + 31 min + 23 sec).

clear reboot

This command cancels a scheduled reboot.

4.11.31 show reboot

This command displays if a reboot is scheduled for the device. If scheduled, the command displays the number of seconds after which the switch will reboot.

Format

```
show reboot
```

Modes

```
Privileged EXEC
User Exec
```

<seconds>

The number of seconds after which the switch will reboot.
Value range: `None` (no reboot scheduled), `0 .. 2147483` sec (= 596 h + 31 min + 23 sec).

4.11.32 reload

This command enables you to reset the switch (warm start) after a given time delay, for cold start See “reboot” on page 333.
Note: First, the device is checking the software in the flash memory and then it resets. If a warm start is not possible, the device automatically executes a cold start.
Reset means that all network connections are terminated and the boot code executes. The switch uses the stored configuration to initialize the switch. You are prompted to confirm that the reset should proceed. A successful reset is indicated by the LEDs on the switch.

Format

```
reload {delay <seconds>}
```

Mode

```
Privileged EXEC
```

<seconds>

The number of seconds after which the switch will reload.
Value range: `0..2147483` sec.

clear reload

This command cancels a scheduled reload.

4.11.33 show reload

This command displays if a reload is scheduled for the device. If scheduled, the command displays the number of seconds after which the switch will reload.

Format

```
show reload
```

Modes

```
Privileged EXEC
User Exec
```

<seconds>

The number of seconds after which the switch will reload.
Possible values: `None` (no reload scheduled), `0..2147483` sec.

4.11.34 set clibanner

Use this command to set the preferences for the CLI login banner. Enable or disable the CLI login banner and define the text for the login banner.
This banner replaces the CLI banner before login.

Format

```
set clibanner {operation |
               text <Max. 2048 characters>}
```

Modes

```
Privileged EXEC
```

operation

Enable the CLI login banner.

text

Define the text for the CLI login banner.

Possible values: Max. 2048 characters in the range ASCII code 0x20 (space character, “ ”) to ASCII code 0x7E (tilde, “~”), except ASCII code 0x25 (percent sign, "`%`").

Use `\\n`: for new line and `\\t` for horizontal tabulator.

Enter the text with quotes, e.g.
`"This is a login banner text."`

Example:

```
**************************************************
*                                                *
*    Site:      <Name of the location>           *
*    Equipment: <Device name>                    *
*                                                *
*    Unauthorized access will be prosecuted.     *
*                                                *
**************************************************
```

no set clibanner operation

Use this command to disable the CLI login banner.

Format

```
no set clibanner operation
```

Mode

```
Privileged EXEC
```

4.11.35 set pre-login-banner

Use this command to set the preferences for the CLI pre-login banner. Enable or disable the CLI pre-login banner and define the text for the pre-login banner.
The device displays this banner additionally before login in CLI and Graphical User Interface.

Format

```
set pre-login-banner { operation |
                       text <max. 255 characters> }
```

Modes

```
Privileged EXEC
```

operation

Enable the CLI login banner.

text

Define the text for the CLI pre-login banner.

Default: `Empty string`
Possible values: Max. 255 characters in the range ASCII code 0x20 (space character, “ ”) to ASCII code 0x7E (tilde, “~”), except ASCII code 0x25 (percent sign, "%").

Use `\\n`: for new line and `\\t` for horizontal tabulator.

Enter the text within quotes, e.g.
`"This is a pre-login banner text."`

Example:

```
**************************************************
*                                                *
*    Site:      Name of the location             *
*    Equipment: Device name                      *
*                                                *
*    Unauthorized access will be prosecuted.     *
*                                                *
**************************************************
```

no set pre-login-banner operation

Use this command to disable the CLI pre-login banner.

Format

```
no set pre-login-banner operation
```

Mode

Privileged EXEC

4.12 LLDP - Link Layer Discovery Protocol

These commands show and configure the LLDP parameters in compliance with IEEE 802.1 AB.

4.12.1 show lldp

This command shows all LLDP settings.

Format

```
show lldp
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.2 show lldp config

This command shows all LLDP configuration settings.

Format

```
show lldp config
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.3 show lldp config chassis

This command shows all LLDP configuration settings concerning the entire device.

Format

```
show lldp config chassis
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.4 show lldp config chassis admin-state

Display the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol is inactive but the LLDP MIBs can still be accessed.

Format

```
show lldp config chassis admin-state
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.5 show lldp config chassis notification-interval

Display the LLDP minimum notification trap interval (unit: seconds).

Format

```
show lldp config chassis notification-interval
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.6 show lldp config chassis re-init-delay

Display the LLDP configuration's chassis re-initialization delay (unit: seconds).

Format

```
show lldp config chassis re-init-delay
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.7 show lldp config chassis tx-delay

Display the LLDP transmit delay (unit: seconds). It indicates the delay between successive LLDP frame transmissions.

Format

```
show lldp config chassis tx-delay
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.8 show lldp config chassis tx-hold-mult

Display the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval).

Format

```
show lldp config chassis tx-hold-mult
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.9 show lldp config chassis tx-interval

Display the interval (unit: seconds) at which LLDP frames are transmitted on behalf of this LLDP agent.

Format

```
show lldp config chassis tx-interval
```

Mode

```
Privileged EXEC and User EXEC
```

4.12.10 show lldp config port

This command shows all LLDP configuration settings and states concerning one or all ports.

Format

```
show lldp config port <{slot/port|all}>
  admin-state | fdb-mode | hm-mode |
  max-neighbors | notification | tlv
```

Mode

```
Privileged EXEC and User EXEC
```

admin-state

Display the port's LLDP admin state (if LLDP/IEEE802.1AB frames will be transmitted and/or received).

fdb-mode

Display the port's LLDP FDB mode.

hm-mode

Display the port's LLDP Hirschmann mode.

.**max-neighbors**

Display the port's max. no. of LLDP neighbors.

notification

Display the port's LLDP notification (trap) setting.

tlv

Display the port's LLDP TLV settings (they determine which information is included in the LLDP frames that are sent). The command is a group command and will output several lines of data.

4.12.11 show lldp config port tlv

This command shows all LLDP TLV configuration settings (if the given information is included in the sent LLDP frames or not) concerning one or all ports.

Format

```
show lldp config port <{slot/port|all}> tlv
```

Mode

```
Privileged EXEC and User EXEC
```

inlinepower

Enable or disable the sending of the port's Power over Ethernet capabilities (PoE, IEEE 802.3af).
Note: This command is available for devices supporting PoE.

link-aggregation

Display the port's LLDP TLV inclusion of Link Aggregation.

mac-phy-config-state

Display the port's LLDP TLV inclusion of MAC Phy. Cfg. State.

max-frame-size

Display the port's LLDP TLV inclusion of Max. Frame Size.

PROFINET IO Status

Display the port's LLDP TLV inclusion of PROFINET IO Status.

PROFINET IO Alias

Display the port's LLDP TLV inclusion of PROFINET IO Alias.

PROFINET IO MRP

Display the port's LLDP TLV inclusion of PROFINET IO MRP.

mgmt-addr

Display the port's LLDP TLV inclusion of Management Address.

port-desc

Display the port's LLDP TLV inclusion of Port Description.

port-vlan

Display the port's LLDP TLV inclusion of Port VLAN.

protocol

Display the port's LLDP TLV inclusion of Protocol.

sys-cap

Display the port's LLDP TLV inclusion of System Capabilities.

sys-desc

Display the port's LLDP TLV inclusion of System Description.

sys-name

Display the port's LLDP TLV inclusion of System Name.

vlan-name

Display the port's LLDP TLV inclusion of VLAN Name.

4.12.12 show lldp med

Use this command to display a summary of the current LLDP MED global configuration.

Format

```
show lldp med
```

Mode

```
Privileged EXEC
```

Fast Start Repeat Count

Display the Fast Start Repeat Count, e.g. the number of LLDP PDUs that will be transmitted when the product is enabled.
Value range: `1..10`.

Device class

Display the Device class.

4.12.13 show lldp med interface

Use this command to display a summary of the current LLDP MED configuration for a specific interface.

Format

`show lldp med interface {<unit/slot/port> | all}`

Mode

`Privileged EXEC`

<unit/slot/port>

Indicates a specific physical interface.

all

Indicates all valid LLDP interfaces.

Interface

Displays the physical interface.

Link

Displays the link status.
Possible values: `Up, Down`.

configMED

Displays if confignotification for the Media Endpoint Devices is `Enabled/Disabled`.

operMED

Displays if operation for the Media Endpoint Devices is `Enabled/Disabled`.

ConfigNotify

Displays the ConfigNotify.
Possible values: `Enabled, Disabled`.

TLVsTx

Displays the TLVsTx.

4.12.14 show lldp med local-device detail

Use this command to display detailed information about the LLDP MED data that a specific interface transmits. `<unit/slot/port>` indicates a specific physical interface.

Format

```
show lldp med local-device detail {<slot/port>}
```

Mode

```
Privileged EXEC
```

<slot/port>

Indicates a specific physical interface.

Interface

Displays the physical interface.

Network Policies

Displays the Network Policies.

4.12.15 show lldp med remote-device

Use this command to display the summary information about remote devices that transmit current LLDP MED data to the system. You can show information about LLDP MED remote data received on all valid LLDP interfaces or on a specific physical interface.

Format

```
show lldp med remote-device{<slot/port> | all}
```

Mode

```
Privileged EXEC
```

<slot/port>

Indicates a specific physical interface.

all

Indicates all valid LLDP interfaces.

Local Interface

Displays the local interface.

RemoteID

Displays the RemoteID.

Device Class

Displays the Device Class.

4.12.16 show lldp med remote-device detail

Use this command to display detailed information about remote devices that transmit current LLDP MED data to an interface on the system.

Format

```
show lldp med remote-device detail <slot/port>
```

Mode

```
Privileged EXEC
```

Local Interface

Displays the local interface.

4.12.17 show lldp remote-data

This command shows all LLDP remote-data settings and states concerning one or all ports.

Format

```
show lldp remote-data <{slot/port|all}>
  chassis-id | detailed | ether-port-info |
  inlinepower | link-aggregation-info |
  mgmt-addr | profinetio-port-info |
  port-desc | port-id | summary | sys-desc |
  sys-name | vlan-info
```

Mode

```
Privileged EXEC and User EXEC
```

chassis-id

Display the remote data's chassis ID only.

detailed

Display remote data in detailed format (i. e., all available data).
Note: most important data is output first (not in alphabetic order of command names). This is the default command if no specific command is given.

ether-port-info

Display the remote data's port Ethernet properties only (group command, outputs: Port Autoneg. Supported, Port Autoneg. Enabled, Port Autoneg. Advertized Capabilities and Port Operational MAU Type).

inlinepower

Displays the remote port's Power over Ethernet capabilities (PoE, IEEE 802.3af). Included are if the remote device is a PSE (Power Source Device) or a PD (Powered Device), if PoE is supported and if the power pairs are selectable.

link-aggregation-info

Display the remote data's link aggregation information only (group command, outputs: Link Agg. Status and Link Agg. Port ID).

mgmt-addr

Display the remote data's management address only.

profinetio-port-info

Display the remote data's Port ProfinetIO properties only.

port-desc

Display the port's LLDP TLV inclusion of Port Description.

port-id

Display the remote data's port ID only.

summary

Display remote data in summary format (table with most important data only, strings will be truncated if necessary, indicated by an appended '>' character).

sys-desc

Display the remote data's system description only.

sys-name

Display the remote data's system name only.

vlan-info

Display the remote data's VLAN information only (group command, outputs: Port VLAN ID, Membership VLAN IDs and their respective names).

4.12.18 lldp

Enable/disable the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol will become inactive, but the LLDP MIBs can still be accessed. This command is a shorthand notation for `lldp config chassis admin-state {off|on}` (see “lldp config chassis admin-state” on page 354).

The default setting is `on`.

Format

```
lldp
```

Mode

```
Global Config
```

- **no lldp**
  Disable the LLDP/IEEE802.1AB functionality on this device.

Format

```
no lldp
```

Mode

```
Global Config
```

4.12.19 lldp config chassis admin-state

Configure the LLDP/IEEE802.1AB functionality on this device. If disabled, the LLDP protocol will become inactive, but the LLDP MIBs can still be accessed.

- `off`: Disable the LLDP/IEEE802.1AB functionality.
- `on`: Enable the LLDP/IEEE802.1AB functionality.

The default setting is `on`.

Format

```
lldp config chassis admin-state {off|on}
```

Mode

```
Global Config
```

4.12.20 lldp config chassis notification-interval

Configure the LLDP minimum notification interval (the minimum time after a notification trap has been sent until a new trap can be sent, unit: seconds, min.: `5` sec., max.: `3600` sec., Default value: `5` sec.).

Format

```
lldp config chassis notification-interval
 <notification interval>
```

Mode

```
Global Config
```

Notification interval

Configure the LLDP minimum notification interval (the minimum time after a notification trap has been sent until a new trap can be sent, unit: seconds, min.: `5` sec., max.: `3600` sec., Default value: `5` sec.).

4.12.21 lldp config chassis re-init-delay

Configure the LLDP re-initialization delay (unit: seconds, min.: 1 sec., max.: 10 sec., Default value: 2 sec.).

Format

```
lldp config chassis re-init-delay <re-init delay>
```

Mode

```
Global Config
```

Re-init-delay

Configure the LLDP re-initialization delay (unit: seconds, min.: 1 sec., max.: 10 sec., Default value: 2 sec.).

4.12.22 lldp config chassis tx-delay

Configure the LLDP transmit delay, the delay between successive LLDP frame transmissions (unit: seconds, min.: 1 sec., max.: 8192 sec., Default value: 2 sec.).

Format

```
lldp config chassis tx-delay <tx delay>
```

Mode

```
Global Config
```

Tx-delay

Configure the LLDP transmit delay, the delay between successive LLDP frame transmissions (unit: seconds, min.: 1 sec., max.: 8192 sec., Default value: 2 sec.).

4.12.23 lldp config chassis tx-hold-mult

Configure the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval), min.: 2, max.: 10, Default value: 4.

Format

```
lldp config chassis tx-hold-mult
                                <tx hold multiplier>
```

Mode

Global Config

Tx-hold-mult

Configure the LLDP transmit hold multiplier, a time-to-live value expressed as a multiple of the LLDP Message Tx Interval (tx-interval), min.: 2, max.: 10, Default value: 4.

4.12.24 lldp chassis tx-interval

Configure the interval at which LLDP frames are transmitted on behalf of this LLDP agent (unit: seconds, min.: 5 sec., max.: 32768 sec., Default value: 30 sec.)

Format

```
lldp chassis tx-interval <tx interval>
```

Mode

Global Config

Tx-interval

Configure the interval at which LLDP frames are transmitted on behalf of this LLDP agent (unit: seconds, min.: 5 sec., max.: 32768 sec., Default value: 30 sec.).

4.12.25 clear lldp config all

Clear the LLDP configuration, i. e., set all configurable parameters to default values (all chassis- as well as port-specific parameters at once).
Note: LLDP Remote data remains unaffected.

Format

```
clear lldp config all
```

Mode

```
Privileged EXEC
```

4.12.26 lldp admin-state

Configure the port's LLDP admin state (if LLDP/IEEE802.1AB frames will be transmitted to and/or received from the standard IEEE multicast address 01:80:c2:00:00:0e).

The default setting is `tx-and-rx`.

Format

```
lldp admin-state <{tx-only|rx-only|tx-and-rx|off}>
```

Mode

```
Interface Config
```

4.12.27 lldp fdb-mode

Configure the port's LLDP FDB mode.

The default setting is `autodetect`.

Format

```
lldp fdb-mode <{lldp-only|mac-only|lldp-and-
mac|autodetect}>
```

Mode

```
Interface Config
```

4.12.28 lldp hm-mode

Configure the port's LLDP Hirschmann mode (if LLDP/IEEE802.1AB frames will be transmitted to and/or received from the Hirschmann-specific multicast address 01:80:63:2f:ff:0b).

The default setting is `tx-and-rx`.

Format

```
lldp hm-mode <{tx-only|rx-only|tx-and-rx|off}>
```

Mode

```
Interface Config
```

4.12.29 lldp max-neighbors

Configure the port's LLDP max. no. of neighbors (min.: `1`, max.: `50`, Default value: `10`).

Format

```
lldp max-neighbors <1..50>
```

Mode

```
Interface Config
```

4.12.30 lldp med

LLDP for Media Endpoint Devices (LLDP-MED) is an extension to LLDP that operates between endpoint devices such as IP phones, Voice / Media Gateways, Media Servers, IP Communications Controllers or other VoIP devices or servers, and network devices such as switches. It specifically provides support for voice over IP (VoIP) applications. In this purpose, it provides an additional set of common advertisement messages (TLVs), for capabilities discovery, network policy, Power over Ethernet, inventory management and location information.
Use this command to enable MED. By enabling MED, you will be effectively enabling the transmit and receive function of LLDP.

Default

```
Enabled
```

Format

```
lldp med
```

Mode

```
Interface Config
```

no lldp med

Use this command to disable MED.

Format

```
no lldp med
```

Mode

```
Interface Config
```

4.12.31 lldp med all

Use this command to configure LLDP-MED on all the ports.

Default

Enabled

Format

lldp med all

Mode

Global Config

4.12.32 lldp med confignotification

Use this command to configure all the ports to send the topology change notification.

Default

Disabled

Format

lldp med confignotification

Mode

Interface Config

no lldp med confignotification

Use this command to disable notifications.

Format

no lldp med confignotification

Mode

Interface Config

4.12.33 lldp med confignotification all

Use this command to configure all the ports to send the topology change notification.

Default

```
Disabled
```

Format

```
lldp med confignotification all
```

Mode

```
Global Config
```

4.12.34 lldp med faststartrepeatcount

Use this command to set the value of the fast start repeat count.

Default

`3`

Format

`lldp med faststartrepeatcount [count]`

Mode

`Global Config`

[count]

The number of LLDP PDUs that will be transmitted when the product is enabled. The range is `1` to `10`.

no lldp med faststartrepeatcount

Use this command to return to the factory default value.

Format

`no lldp med faststartrepeatcount`

Mode

`Global Config`

4.12.35 lldp med transmit-tlv

Use this command to specify which optional Type Length Values (TLVs) in the LLDP-MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default

```
By default, the capabilities and network policy
TLVs are included.
```

Format

```
lldp med transmit-tlv [capabilities]
                                    [network-policy]
```

Mode

```
Interface Config
```

capabilities

Include/Exclude LLDP capabilities TLV.

network-policy

Include/Exclude LLDP network policy TLV.

no lldp med transmit-tlv

Use this command to remove a TLV.

Format

```
no lldp med transmit-tlv [capabilities]
                                    [network-policy]
```

Mode

```
Interface Config
```

4.12.36 lldp med transmit-tlv all

Use this command to specify which optional Type Length Values (TLVs) in the LLDP MED set will be transmitted in the Link Layer Discovery Protocol Data Units (LLDPDUs).

Default

By default, the capabilities and network policy TLVs are included.

Format

```
lldp med transmit-tlv all [capabilities]
                                    [network-policy]
```

Mode

Global Config

capabilities

Include/Exclude LLDP capabilities TLV.

network-policy

Include/Exclude LLDP network policy TLV.

no lldp med med transmit-tlv all

Use this command to remove a TLV.

Format

```
no lldp med transmit-tlv all [capabilities]
                                    [network-policy]
```

Mode

Global Config

4.12.37 lldp notification

Configure the port's LLDP notification setting (on or off, Default value: off).

Format

```
lldp notification <{off|on}>
```

Mode

```
Interface Config
```

4.12.38 lldp tlv link-aggregation

Configure the port's LLDP TLV inclusion of Link Aggregation (on or off, default: on).

Format

```
lldp tlv link-aggregation <{off|on}>
```

Mode

```
Interface Config
```

4.12.39 lldp tlv mac-phy-config-state

Configure the port's LLDP TLV inclusion of MAC Phy. Cfg. State (on or off, default: on).

Format

```
lldp tlv mac-phy-config-state <{off|on}>
```

Mode

```
Interface Config
```

4.12.40 lldp tlv max-frame-size

Configure the port's LLDP TLV inclusion of Max. Frame Size (on or off, default: on).

Format

```
lldp tlv max-frame-size <{off|on}>
```

Mode

```
Interface Config
```

4.12.41 lldp tlv mgmt-addr

Configure the port's LLDP TLV inclusion of Management Address (on or off, default: on).

Format

```
lldp tlv mgmt-addr <{off|on}>
```

Mode

```
Interface Config
```

4.12.42 lldp tlv pnio

Configure the port's LLDP TLV inclusion of PROFINET IO Status (on or off, default: on).

Format

```
lldp tlv pnio <{off|on}>
```

Mode

```
Interface Config
```

4.12.43 lldp tlv pnio-alias

Configure the port's LLDP TLV inclusion of PROFINET IO Alias (on or off, default: on).

Format

```
lldp tlv pnio-alias <{off|on}>
```

Mode

```
Interface Config
```

4.12.44 lldp tlv pnio-mrp

Configure the port's LLDP TLV inclusion of PROFINET IO MRP (on or off, default: on).

Format

```
lldp tlv pnio-mrp <{off|on}>
```

Mode

```
Interface Config
```

4.12.45 lldp tlv port-desc

Configure the port's LLDP TLV inclusion of Port Description (on or off, default: on).

Format

```
lldp tlv port-desc <{off|on}>
```

Mode

```
Interface Config
```

4.12.46 lldp tlv port-vlan

Configure the port's LLDP TLV inclusion of Port VLAN (on or off, default: on).

Format

```
lldp tlv port-vlan <{off|on}>
```

Mode

```
Interface Config
```

4.12.47 lldp tlv gmrp

Configure the port's LLDP TLV inclusion of GMRP (on or off, default: on).

Format

```
lldp tlv gmrp <{off|on (on)}>
```

Mode

```
Interface Config
```

4.12.48 lldp tlv igmp

Configure the port's LLDP TLV inclusion of IGMP (on or off, default: on).

Format

```
lldp tlv igmp <{off|on (on)}>
```

Mode

```
Interface Config
```

4.12.49 lldp tlv portsec

Configure the port's LLDP TLV inclusion of PortSec (on or off, default: on).

Format

```
lldp tlv portsec <{off|on (on)}>
```

Mode

```
Interface Config
```

4.12.50 lldp tlv ptp

Configure the port's LLDP TLV inclusion of PTP (on or off, default: on).

Format

```
lldp tlv ptp <{off|on (on)}>
```

Mode

```
Interface Config
```

4.12.51 lldp tlv protocol

Configure the port's LLDP TLV inclusion of Protocol (on or off, default: on).

Format

```
lldp tlv protocol <{off|on (on)}>
```

Mode

```
Interface Config
```

4.12.52 lldp tlv sys-cap

Configure the port's LLDP TLV inclusion of System Capabilities (on or off, default: on).

Format

```
lldp tlv sys-cap <{off|on}>
```

Mode

```
Interface Config
```

4.12.53 lldp tlv sys-desc

Configure the port's LLDP TLV inclusion of System Description (on or off, default: on).

Format

```
lldp tlv sys-desc <{off|on}>
```

Mode

```
Interface Config
```

4.12.54 lldp tlv sys-name

Configure the port's LLDP TLV inclusion of System Name (on or off, default: on).

Format

```
lldp tlv sys-name <{off|on}>
```

Mode

```
Interface Config
```

4.12.55 lldp tlv vlan-name

Configure the port's LLDP TLV inclusion of VLAN Name.

Format

```
lldp tlv vlan-name <{off|on}>
```

Mode

```
Interface Config
```

4.12.56 name

Set or remove a descriptive name for the current interface (physical ports only).

Format

```
name <descriptive name>
```

Mode

```
Interface Config
```

<descriptive name>

Enter a descriptive name for the current interface (physical ports only). Max. length is 20 characters.

Note: If it contains blanks or exclamation marks (!), enclose it in quotation marks ("). The description itself must not contain any quotation marks (' or "), question marks (?) or backslashes (\).

no name

Delete the descriptive name for the current interface (physical ports only).

Format

```
no name
```

Mode

```
Interface Config
```

4.13 SNTP - Simple Network Time Protocol

These commands show and configure the SNTP parameters.

4.13.1 show sntp

This command shows all SNTP settings.

Format

```
show sntp
```

Mode

```
Privileged EXEC and User EXEC
```

SNTP Server Anycast Address

Show SNTP Server Anycast Address (a.b.c.d).

SNTP Server Anycast Transmit Interval

Show SNTP Anycast Transmit Interval (in seconds).

SNTP Server Anycast VLAN

Show SNTP Server Anycast VLAN.

SNTP Server Disable if Timesource is local

Show SNTP Server Disable if Timesource is local (Yes/No).

SNTP Client Accepts Broadcasts

Show SNTP Client Accepts Broadcasts (Yes/No).

SNTP Client Disable after Synchronization

Show SNTP Client Disable after Synchronization (Yes/No).

SNTP Client Request Interval

Show SNTP Client Request Interval (in seconds).

SNTP Client Local Time Offset

Show SNTP Client Local Time Offset (in minutes).

SNTP Client Primary Server IP Address

Show SNTP Client Primary Server IP Address (a.b.c.d).

SNTP Client Secondary Server IP Address

Show SNTP Client Secondary Server IP Address (a.b.c.d).

SNTP Client Threshold to Server Time

Show SNTP Client Threshold to Server Time (in milliseconds).

SNTP Operation Global

Show SNTP Operation Global (Disabled or Enabled).

SNTP Operation Server

Show SNTP Operation Server (Disabled or Enabled).

SNTP Operation Client

Show SNTP Operation Client (Disabled or Enabled).

SNTP Status

Show SNTP Status

SNTP Time

Show SNTP Time (yyyy-mm-dd hh:mm:ss).

SNTP System Time

Show SNTP system Time (yyyy-mm-dd hh:mm:ss).

4.13.2 show sntp anycast

This command shows all SNTP anycast configuration settings.

Format

```
show sntp anycast [address|transmit-interval|vlan]
```

Mode

```
Privileged EXEC and User EXEC
```

address

Show the SNTP server's anycast destination IP Address.

transmit-interval

Show the SNTP Server's interval for sending Anycast messages (unit: seconds).

vlan

Show the SNTP server's Anycast VLAN ID (used for sending Anycast messages).

4.13.3 show sntp client

This command shows all SNTP anycast configuration settings.

Format

```
show sntp client [accept-broadcast|
                  disable-after-sync|
                  offset|
                  request-interval|
                  server<primary|secondary>|
                  threshold]
```

Mode

```
Privileged EXEC and User EXEC
```

accept-broadcast

Show if the SNTP Client accepts SNTP broadcasts.

disable-after-sync

Show if the SNTP client will be disabled once it is synchronized to the time server.

offset

Show the local time's offset (in minutes) with respect to UTC (positive values for locations east of Greenwich).

request-interval

Show the SNTP Client's request interval (unit: seconds).

server

Show the SNTP Client's server IP addresses.

server primary

Show the SNTP Client's primary server IP addresses.

server secondary

Show the SNTP Client's redundant server IP addresses.

server threshold

Show the SNTP Client's threshold in milliseconds.

4.13.4 show sntp operation

This command shows if the SNTP function is enabled or disabled.

Format

```
show sntp operation
```

Mode

```
Privileged EXEC and User EXEC
```

4.13.5 show sntp server

This command shows the SNTP Server's configuration parameters.

Format

```
show sntp server [disable-if-local]
```

Mode

```
Privileged EXEC and User EXEC
```

disable-if-local

Show if the server will be disabled if the time is running from the local clock and not synchronized to an external time source.

4.13.6 show sntp status

This command shows the SNTP state, synchronization and error messages.

Format

```
show sntp status
```

Mode

```
Privileged EXEC and User EXEC
```

4.13.7 show sntp time

This command shows time and date.

Format

```
show sntp time [sntp|system]
```

Mode

```
Privileged EXEC and User EXEC
```

sntp

Show the current SNTP date and UTC time.

system

Show the local system's current date and time.

4.13.8 no sntp

This command disables sntp.

Format

```
no sntp
```

Mode

```
Global Config
```

4.13.9 sntp anycast address

Set the SNTP server's anycast destination IP Address, default: 0.0.0.0 (none).

Format

```
sntp anycast address <IPAddress>
```

Mode

```
Global Config
```

no sntp anycast address
Set the SNTP server's anycast destination IP Address to 0.0.0.0.

Format

```
no sntp anycast address
```

Mode

```
Global Config
```

4.13.10 sntp anycast transmit-interval

The transmit interval in seconds, default: 120.

Format

```
sntp anycast transmit-interval <1-3600>
```

Mode

```
Global Config
```

4.13.11 sntp anycast vlan

Set the SNTP server's Anycast VLAN ID used for sending Anycast messages, default: 1.

Format

```
sntp anycast vlan <1-4042>
```

Mode

```
Global Config
```

4.13.12 sntp client accept-broadcast

Enable/Disable that the SNTP Client accepts SNTP broadcasts.

Format

```
sntp client accept-broadcast <on | off>
```

Mode

```
Global Config
```

- **no sntp accept-broadcast**
  Disable the SNTP Client accepts SNTP broadcasts.

Format

```
no sntp client accept-broadcast
```

Mode

```
Global Config
```

4.13.13 sntp client disable-after-sync

If this option is activated, the SNTP client disables itself once it is synchronized to a server.

Format

```
sntp client disable-after-sync <on | off>
```

Mode

```
Global Config
```

off

Do not disable SNTP client when it is synchronized to a time server.

on

Disable SNTP client as soon as it is synchronized to a time server.

4.13.14 sntp client offset

The offset between UTC and local time in minutes, default: 60.

Format

```
sntp client offset <-1000 to 1000>
```

Mode

```
Global Config
```

4.13.15 sntp client request-interval

The synchronization interval in seconds, default: 30.

Format

```
sntp client request-interval <1-3600>
```

Mode

```
Global Config
```

4.13.16 no sntp client server

Disable the SNTP client servers.

Format

```
no sntp client server
```

Mode

```
Global Config
```

4.13.17 sntp client server primary

Set the SNTP Client's primary server IP Address, default: 0.0.0.0 (none).

Format

```
sntp client server primary <IP-Address>
```

Mode

```
Global Config
```

- **no sntp client server primary**
  Disable the primary SNTP client server.

Format

```
no sntp client server primary
```

Mode

```
Global Config
```

4.13.18 sntp client server secondary

Set the SNTP Client's secondary server IP Address, default: 0.0.0.0 (none).

Format

```
sntp client server secondary <IP-Address>
```

Mode

```
Global Config
```

no sntp client server secondary

Disable the secondary SNTP client server.

Format

```
no sntp client server secondary
```

Mode

```
Global Config
```

4.13.19 sntp client threshold

With this option you can reduce the frequency of time alterations. Enter this threshold as a positive integer value in milliseconds. The switch obtains the server timer as soon as the deviation to the server time is above this threshold.

Format

```
sntp client threshold <milliseconds>
```

Mode

```
Global Config
```

Milliseconds

```
Enter the allowed deviation to the server time as a
positive integer value in milliseconds.
```

no sntp client threshold
Disable the sntp client threshold.

Format

```
no sntp client threshold
```

Mode

```
Global Config
```

4.13.20 sntp operation

Enable/Disable the SNTP function.

Format

```
sntp operation <on | off> |
               client { on | off } |
               server { on | off }
```

Mode

```
Global Config
```

client

Enable or disable SNTP Client.

server

Enable or disable SNTP Server.

no sntp operation

Disable the SNTP Client and Server.

Format

```
no sntp operation
```

Mode

```
Global Config
```

4.13.21 sntp server disable-if-local

With this option enabled, the switch disables the SNTP Server Function if it is not synchronized to a time server itself.

Format

```
sntp server disable-if-local <on | off>
```

Mode

```
Global Config
```

off

Enable the SNTP Server even if it is not synchronized to a time server itself.

on

Disable the SNTP Server if it is not synchronized to a time server itself.

4.13.22 sntp time system

Set the current sntp time.

Format

```
sntp time system <YYYY-MM-DD HH:MM:SS>
```

Mode

```
Global Config
```

4.14 PTP - Precision Time Protocol

These commands show and configure the PTP (IEEE 1588) parameters.

Note: The operation parameter is available for all devices.
All other parameters are additionally available for MS20/MS30, MACH1040, MACH104 and PowerMICE.

4.14.1 show ptp

This command shows all PTP settings.

Format

`show ptp`

Mode

`Privileged EXEC and User EXEC`

PTP (Global) Operation

Show the global PTP (IEEE 1588) operation setting. This field shows if PTP is enabled/disabled on this device.
Possible values: `Enabled`, `Disabled`

PTP (Global) Clock Mode

Show which PTP clock mode is currently configured.
Possible values: `v1-simple-mode, v2-simple-mode, v1-boundary-clock, v2-boundary-clock-onestep, v2-boundary-clock-twostep, v2-transparent-clock}`

PTP (Global) Sync. Upper Bound

Show the upper bound for the PTP clock synchronization status (unit: nanoseconds).
Possible values: `31..1000000000 nsec`

PTP (Global) Sync. Lower Bound

Show the lower bound for the PTP clock synchronization status (unit: nanoseconds).
Possible values: `0..999999999 nsec`

PTP Preferred Master

Show if the local switch shall be regarded as a preferred master clock or not.
Possible values: `False`, `True`

PTP Subdomain Name

Show the PTP subdomain name.
Possible values: Up to 16 characters from ASCII hex value 0x21 (`!`) up to and including hex value 0x7e (~).

PTP Sync. Interval

Show the configured Precision Time Protocol sync interval.
The sync interval is the interval (in seconds) between successive sync messages issued by a master clock.
Possible values: `sec-1`, `sec-2`, `sec-8`, `sec-16`, `sec-64`

PTP Status, Is Synchronized

Show if the device is synchronized (true or false).
Possible values: `False`, `True`

PTP Status, Offset From Master

Show the device's offset from the master (unit: nanoseconds), i.e. the deviation of the local clock from the reference clock.

PTP Status, Max. Offset Absolute

Show the device's maximum offset absolute (unit: nanoseconds).

PTP Status, Delay To Master

Show the device's delay to the master (unit: nanoseconds), i.e. the single signal runtime between the local device and reference clock.

PTP Status, Grandmaster UUID

Show grandmaster Universally Unique IDentifier, i.e. the MAC address of the grandmaster clock (Unique Universal Identifier).
Possible values: 32 hexadecimal numbers (`hh hh hh hh hh hh hh hh`).

PTP Status, Parent UUID

Show parent Universally Unique IDentifier, i.e. the MAC address of the master clock with which the local time is directly synchronized.
Possible values: 32 hexadecimal numbers (`hh hh hh hh hh hh hh hh`).

PTP Status, Clock Stratum

Show the qualification of the local clock.

PTP Status, Clock Identifier

Show the device's clock properties (e.g. accuracy, epoch, etc.).

PTPv1 Boundary Clock Ports

Show port number, operation status, burst status of the PTPv1 Boundary Clock Ports.

Port

Show the number of the interface (in `slot/port` notation).

Operation

Show if sending and receiving / processing PTP synchronization messages is enabled or disabled on the device.
Possible values: `Enabled`, `Disabled`

Burst

Show the status of the burst feature for synchronization running during a synchronization interval.
Possible values: `Enabled`, `Disabled`

Status

Show the ports PTP status.
Possible values: `Initializing`, `faulty`, `disabled`, `listening`, `pre-master`, `master`, `passive`, `uncalibrated`, `slave`.

4.14.2 show ptp configuration

This command shows the configured PTP (IEEE 1588) values depending on the currently configured clock mode.

Format

```
show ptp configuration
```

Mode

```
Privileged EXEC and User EXEC
```

PTP (Global) Clock Mode

Show which PTP clock mode is currently configured.

PTP (Global) Sync. Upper Bound

Show the upper bound for the PTP clock synchronization status (unit: nanoseconds).

PTP (Global) Sync. Lower Bound

Show the lower bound for the PTP clock synchronization status (unit: nanoseconds).

4.14.3 show ptp operation

Show the global PTP (IEEE 1588) operation setting (the administrative setting).This command shows if PTP is enabled/disabled on this device.

Format

```
show ptp operation
```

Mode

```
Privileged EXEC and User EXEC
```

4.14.4 show ptp port

This command shows the PTP (IEEE 1588) port configuration settings depending on the currently configured clock mode.

Format

```
show port [<slot/port>|all]
```

Mode

```
Privileged EXEC and User EXEC
```

<slot/port>

Show the port-related PTP (IEEE 1588) settings for the given port.

all

Show the port-related PTP (IEEE 1588) settings for all ports.

4.14.5 show ptp status

This command shows the device´s global PTP (IEEE 1588) status (the operating states).

Format

```
show ptp status
```

Mode

```
Privileged EXEC and User EXEC
```

PTP Status, Is Synchronized

Show if the device is synchronized (true or false).

PTP Status, Offset From Master

Show the device's offset from the master (unit: nanoseconds).

PTP Status, Max. Offset Absolute

Show the device's maximum offset absolute (unit: nanoseconds).

PTP Status, Delay To Master

Show the device's delay to the master (unit: nanoseconds).

PTP Status, Grandmaster UUID

Show grandmaster Universally Unique IDentifier
(32 hexadecimal numbers).

PTP Status, Parent UUID

Show parent Universally Unique IDentifier
(32 hexadecimal numbers).

PTP Status, Clock Stratum

Show the device's clock stratum.

PTP Status, Clock Identifier

Show the device's clock identifier.

4.14.6 ptp clock-mode

Configure the Precision Time Protocol (PTP, IEEE 1588) clock mode. If the clock mode is changed, PTP will be initialized. The default is `disable`.

Format

```
ptp clock-mode {v1-simple-mode
               |v2-simple-mode
               |v1-boundary-clock
               |v2-boundary-clock-onestep
               |v2-boundary-clock-twostep
               |v2-transparent-clock}
```

Mode

`Global Config`

v1-simple-mode

Set the clock mode to 'v1 Simple Mode'. This is a client only mode without hardware support. The device only accepts PTPv1 sync messages and sets the time directly. No BMC algorithm will run.

v2-simple-mode

Set the clock mode to 'v2 Simple Mode'. This is a client only mode without hardware support. The device only accepts PTPv2 sync (or follow_up) messages and sets the time directly. No BMC algorithm will run.

v1-boundary-clock

Set the clock mode to 'v1 Boundary Clock'. This specifies the mode as described in the IEEE1588 standard.

v2-boundary-clock-onestep

Set the clock mode to 'v2 Boundary Clock one-step'. This specifies the boundary-clock mode as described in the IEEE1588-2008 (PTPv2) standard. The precise timestamp is inserted directly into the sync-packet (one-step Mode).

v2-boundary-clock-twostep

Set the clock mode to 'v2 Boundary Clock two-step'. This specifies the boundary-clock mode as described in the IEEE1588-2008 (PTPv2) standard. The precise timestamp is transmitted via a follow-up packet (two-step Mode).

v2-transparent-clock

Set the clock mode to 'v2 Transparent Clock'. This specifies the transparent-clock mode (one-step) as described in the IEEE1588-2008 (PTPv2) standard.

4.14.7 ptp operation

Enable or disable the Precision Time Protocol (IEEE 1588).
The default is "disable"

Format

```
ptp operation {disable|enable}
```

Mode

```
Global Config
```

disable

Disable the Precision Time Protocol (IEEE 1588).

enable

Enable the Precision Time Protocol (IEEE 1588).

4.14.8 ptp sync-lower-bound

Configure the lower bound for the PTP clock synchronization
(unit: nanoseconds, min.: 0, max.: 999999999 (10^9-1), default: 30).
Note: The lower bound always has to be smaller than the upper bound.

Format

```
ptp sync-lower-bound <0-999999999>
```

Mode

```
Global Config
```

4.14.9 ptp sync-upper-bound

Configure the upper bound for the PTP clock synchronization (unit: nanoseconds, min.: 31, max.: 1000000000 (10^9), default: 5000).
Note: The upper bound always has to be larger than the lower bound.

Format

```
ptp sync-upper-bound <31-1000000000>
```

Mode

```
Global Config
```

4.14.10 ptp v1 preferred-master

Configure the PTPv1 (IEEE1588-2002) specific settings.
Specify if the local switch shall be regarded as a preferred master clock (i. e., if it will remain master in the presence of disconnection or connection of other clocks).

Format

```
ptp v1 preferred-master {true|false}
```

Mode

```
Global Config
```

true

The local switch shall be regarded as a preferred master clock.

false

The local switch shall not be regarded as a preferred master clock.

4.14.11 ptp v1 re-initialize

Configure the PTPv1 (IEEE1588-2002) specific settings.
Re-initialize the clocks in the local subdomain with the currently configured settings. Changes in the subdomain name or the sync interval will only take effect after this command.

Format

```
ptp v1 re-initialize
```

Mode

```
Global Config
```

4.14.12 ptp v1 subdomain-name

Configure the PTPv1 (IEEE1588-2002) specific settings.
Enter a Precision Time Protocol subdomain name. The default is "_DFLT".
Note: Changes are only applied after the 're-initialize' command or after a re-boot if the configuration was saved.

Format

```
ptp v1 subdomain-name <subdomain name>
```

Mode

```
Global Config
```

<subdomain name>

Enter a PTP subdomain name (up to 16 characters). Valid characters range from hex value 0x21 (!) up to and including hex value 0x7e (~). Enter special characters (\, !, ', ", ?) by preceding them with the escape character (\), e. g., as \\, \!, \', \", \?. The subdomain name must not be empty. The default is "_DFLT".

4.14.13 ptp v1 sync-interval

Configure the PTPv1 (IEEE1588-2002) specific settings.
Configure the Precision Time Protocol sync interval. The sync interval is the interval (in seconds) between successive sync messages issued by a master clock.
Valid values are: `sec-1, sec-2, sec-8, sec-16`, and `sec-64`.
Default is `sec-2`.

Note: Changes are only applied after the 're-initialize' command or after a reboot if the configuration was saved.

Format

```
ptp v1 sync-interval {sec-1|sec-2|sec-8|sec-16|
                      sec-64}
```

Mode

`Global Config`

sec-1

Set the PTP sync interval to sec-1 (1 sec).

sec-2

Set the PTP sync interval to sec-2 (2 sec).

sec-8

Set the PTP sync interval to sec-8 (8 sec).

sec-16

Set the PTP sync interval to sec-16 (16 sec).

sec-64

Set the PTP sync interval to sec-64 (64 sec).

4.14.14 ptp v2bc priority1

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the priority1 value (`0..255`) for the BMC as described in IEEE1588-2008.

Format

```
ptp v2bc priority1 <0-255>
```

Mode

```
Global Config
```

4.14.15 ptp v2bc priority2

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the priority2 value (`0..255`) for the BMC as described in IEEE1588-2008.

Format

```
ptp v2bc priority2 <0-255>
```

Mode

```
Global Config
```

4.14.16 ptp v2bc domain

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the domain number (0..255) as described in IEEE1588-2008.

Format

```
ptp v2bc domain <0-255>
```

Mode

```
Global Config
```

4.14.17 ptp v2bc utc-offset

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the current UTC offset in seconds.

Format

```
ptp v2bc utc-offset <seconds>
```

Mode

```
Global Config
```

4.14.18 ptp v2bc utc-offset-valid

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Configure the UTC offset valid flag.

Format

```
ptp v2bc utc-offset-valid {true|false}
```

Mode

```
Global Config
```

4.14.19 ptp v2bc vlan

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Use this command to configure the VLAN in which PTP packets are send. With a value of none all packets are send untagged.

Format

```
ptp v2bc vlan {none | <0-4042>}
```

Mode

```
Interface Config
```

4.14.20 ptp v2bc vlan-priority

Configure the PTPv2 Boundary Clock (IEEE1588-2008) specific settings. Use this command to configure the VLAN priority.

Format

```
ptp v2bc vlan-priority <0-7>
```

Mode

```
Interface Config
```

4.14.21 ptp v1 burst

Enable or disable the burst feature for synchronization runs during a synchronization interval. Default is disable.

Format

```
ptp v1 burst {enable|disable}
```

Mode

```
Interface Config
```

enable

During a synchronization interval, there are 2 to 8 synchronization runs. This permits faster synchronization when the network load is high.

disable

During a synchronization interval, there is only one synchronization run.

4.14.22 ptp v1 operation

Enable or disable the sending and receiving / processing of PTP synchronization messages. Default is enable.

Format

```
ptp v1 operation {enable|disable}
```

Mode

```
Interface Config
```

enable

Port sends and receives/ processes PTP synchronization messages.

disable

Port blocks PTP synchronization messages.

4.14.23 ptp v2bc operation

Enable or disable the sending and receiving / processing of PTP synchronization messages.

Format

```
ptp v2bc operation {disable|enable}
```

Mode

```
Interface Config
```

enable

Port sends and receives/ processes PTP synchronization messages.

disable

Port blocks PTP synchronization messages.

4.14.24 ptp v2bc announce-interval

Configure the Announce Interval in seconds {1|2|4|8|16}.

Format

```
ptp v2bc announce-interval {1|2|4|8|16}
```

Mode

```
Interface Config
```

4.14.25 ptp v2bc announce-timeout

Configure the Announce Receipt Timeout (2..10).

Format

```
ptp v2bc announce-timeout <2-10>
```

Mode

```
Interface Config
```

4.14.26 ptp v2bc sync-interval

Configure the Sync Interval in seconds {0.5|1|2}.

Format

```
ptp v2bc sync-interval {0.25|0.5|1|2}
```

Mode

```
Interface Config
```

4.14.27 ptp v2bc delay-mechanism

Configure the delay mechanism {e2e|p2p|disabled} of the transparent-clock.

Format

```
ptp v2bc delay-mechanism {e2e|p2p|disabled}
```

Mode

```
Interface Config
```

4.14.28 ptp v2bc pdelay-interval

Configure the Peer Delay Interval in seconds {1|2|4|8|16|32}.
This interval is used if delay-mechanism is set to p2p.

Format

```
ptp v2bc pdelay-interval {1|2|4|8|16|32}
```

Mode

```
Interface Config
```

4.14.29 ptp v2bc network-protocol

Configure the network-protocol {ieee802_3|udp_ipv4} of the transparent-clock.

Format

```
ptp v2bc network-protocol {ieee802_3 | udp_ipv4}
```

Mode

```
Interface Config
```

4.14.30 ptp v2bc v1-compatibility-mode

Set the PTPv1 Hardware compatibility mode {auto|on|off}.

Format

```
ptp v2bc v1-compatibility-mode {auto|on|off}
```

Mode

```
Interface Config
```

4.14.31 ptp v2bc asymmetry

Specifies the asymmetrie in nanoseconds of the link connected to this port {+-1000000000}.

Format

```
ptp v2bc asymmetry <value in ns>
```

Mode

```
Interface Config
```

4.14.32 ptp v2tc asymmetry

Specifies the asymmetrie in nanoseconds of the link connected to this port {+-1000000000}.

Format

```
ptp v2tc asymmetry <value in ns>
```

Mode

```
Interface Config
```

4.14.33 ptp v2tc delay-mechanism

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Configure the delay mechanism {e2e | p2p | disabled} of the transparent-clock.

Format

```
ptp v2tc delay-mechanism {e2e|p2p}
```

Mode

```
Global Config
```

4.14.34 ptp v2tc management

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Enable or disable the management of the transparent-clock (disable for fast packet rates).

Format

```
ptp v2tc management {enable|disable}
```

Mode

```
Global Config
```

4.14.35 ptp v2tc multi-domain-mode

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Enable or disable the transparent-clock for one (primary-domain) or all domain numbers.

Format

```
ptp v2tc multi-domain-mode {enable|disable}
```

Mode

```
Global Config
```

4.14.36 ptp v2tc network-protocol

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Configure the network-protocol {ieee802_3|udp_ipv4} of the transparent-clock.

Format

```
ptp v2tc network-protocol {ieee802_3|udp_ipv4}
```

Mode

```
Global Config
```

4.14.37 ptp v2tc operation

Enable or disable the sending and receiving/ processing of PTP synchronization messages.

Format

```
ptp v2tc operation {disable|enable}
```

Mode

```
Interface Config
```

enable

Port sends and receives/ processes PTP synchronization messages.

disable

Port blocks PTP synchronization messages.

4.14.38 ptp v2tc pdelay-interval

Configure the Peer Delay Interval in seconds {1|2|4|8|16|32}. This interval is used if delay-mechanism is set to p2p.

Format

```
ptp v2tc pdelay-interval {1|2|4|8|16|32}
```

Mode

```
Interface Config
```

4.14.39 ptp v2tc primary-domain

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Configure the primary-domain {for syntonization} of the transparent-clock.

Format

```
ptp v2tc primary-domain <0-255>
```

Mode

```
Global Config
```

4.14.40 ptp v2tc profile

Note: This command is available for the devices of the MACH104, MACH1040, PowerMICE and MS20/MS30 family.

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use this command to configure the PTP v2TC parameters to match the default of a profile.

Format

```
ptp v2tc profile
            { power | default-e2e | default-p2p }
```

Mode

```
Global Config
```

default-e2e

Configure the PTP v2TC parameters to match the default of a profile (end-to-end transparent clock).

default-p2p

Configure the PTP v2TC parameters to match the default of a profile (peer-to-peer transparent clock).

power

Configure the PTP v2TC parameters to match the default of a profile (power profile C37.238).

4.14.41 ptp v2tc syntonization

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Enable or disable the syntonization of the transparent-clock.

Format

```
ptp v2tc syntonization {enable|disable}
```

Mode

```
Global Config
```

4.14.42 ptp v2tc vlan

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use the command to configure the VLAN in which PTP packets are send. With a value of none all packets are send untagged.

Format

```
ptp v2tc vlan {none | <0-4042>}
```

Mode

```
Global Config
```

4.14.43 ptp v2tc power-tlv-check

Note: This command is available for the devices of the MACH104, MACH1040, PowerMICE and MS20/MS30 family.

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use the command to configure the Power TLV Check.

Default

```
Disable
```

Format

```
ptp v2tc power-tlv-check {enable | disable}
```

Mode

```
Global Config
```

enable

Only announce messages including the TLVs specified in the power profile (C37.238) are accepted for syntonization.

disable

Disable v2tc power-tlv-check.

4.14.44 ptp v2tc vlan-priority

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use the command to configure the VLAN priority of tagged ptp packets.

Format

```
ptp v2tc vlan-priority <0-7>
```

Mode

```
Global Config
```

4.14.45 ptp v2tc sync-local-clock

Configure the PTPv2 Transparent Clock (IEEE1588-2008) specific settings. Use the command to enable or disable synchronization of the local clock (only valid if syntonization is enabled).

Format

```
ptp v2tc sync-local-clock {enable | disable}
```

Mode

```
Global Config
```

4.15 PoE - Power over Ethernet

These commands show and configure the Power over Ethernet (IEEE 802.3af) parameters.

4.15.1 show inlinepower

This command shows global PoE inline power settings.

Format

```
show inlinepower
```

Mode

```
Privileged EXEC and User EXEC
```

4.15.2 show inlinepower port

This command shows the configuration settings and states per port.

Format

`show inlinepower port [<slot/port> | all]`

Mode

`Privileged EXEC and User EXEC`

<slot/port>

Enter the interface (in `<slot/port>` notation).

Admin Mode

Display the PoE inline power administrative settings on the specific interface.
- Possible values: `Enabled`, `Disabled`
- Default value: `Enabled`

Status

Display the PoE inline power status on the specific interface.
- Possible values: `Delivering Power`, `Disabled`

Class

Display the PoE class of the specific interface.
- Value range: `0..4`
- Default value: `0`

Current Power

Display the PoE power in Watts on the specific interface being currently delivered by the device.

Max Observed

Display the maximum PoE power in Watts on the specific interface which has been observed by the device.

Power Limit

Display the maximum PoE power that can be reserved on the specific interface. The power limit is ignored if the maximum observed power consumption exceeds this limit.
- Possible values: `0..30.000` (in Watts)
- Default value: `0`. (disable the limitation of PoE inline power)

Interface Name

Display the name of the specific interface.
- Possible values: `<None>`, ...
- Default value: `<None>`

all

Display the global PoE inline power configuration settings and states for the interfaces of the device.

Intf

Display the interface (in `<slot/port>` notation).

Admin Mode

Display the PoE inline power administrative settings for each interface of the device.
- Possible values: `Enabled`, `Disabled`
- Default value: `Enabled`

Operating Status

Display the PoE inline power status for each interface of the device.
- Possible values: `Delivering Power`, `Disabled`

Priority

Display the PoE inline power priority for each interface of the device. In case of power scarcity, inline power on ports configured with the lowest priority is dropped first.
- Possible values: `Critical, High, Low`.
- Default value: `Low`
  The highest priority is `critical`.

Note: This parameter is available for MACH1000, MACH4000 and devices which support Power over Ethernet Plus (MACH104-16TX-PoEP devices and MACH102 devices with media module M1-8TP-RJ45 PoE).

Class

Display the PoE class for each interface of the device.
- Value range: `0..4`
- Default value: `0`

Curr. Power

Display the PoE power in Watts being currently delivered by the device for each interface.

Max. Observed

Display the maximum PoE power in Watts for each interface which has been observed by the device.

Power Limit

Display the maximum PoE power that can be reserved for each interface of the device. The power limit is ignored if the maximum observed power consumption exceeds this limit.
- Possible values: `0..30.000` (in Watts)
- Default value: `0`. (disable the limitation of PoE inline power)

4.15.3 inlinepower (Global Config)

Configure the global inline power parameters.

Format

```
inlinepower {admin-mode {disable|enable} |
trap {disable|enable} | threshold <1-99> |
fast-startup {enable|disable} }
```

Mode

```
Global Config
```

admin-mode

Configure the global inline power administrative setting.
- Possible values: `enable` or `disable`.
- Default value: `enable`.

trap

Configure the inline power notification (trap) setting.
- Possible values: `enable` or `disable`.
- Default value: `disable`.

threshold

Configure the inline power notification (trap) threshold (unit: percent of maximum rated power.
- Value range: `1..99`.
- Default value: `90`.

fast-startup

Configure the inline power to be enabled at the beginning of the start phase.
- Possible values: `enable` or `disable`.
- Default value: `disable`.

4.15.4 inlinepower (Interface Config)

Configure the port related inline power parameters.
Note: The interface name you enter in the `name`-command.

Format

```
inlinepower {admin-mode {disable|enable} |
             power-limit <watts> | priority
             {critical|high|low} }|
```

Mode

`Interface Config`

admin-mode

Configure the port-related inline power administrative setting
- Possible values: `enable` or `disable`.
- Default value: `enable`.

power-limit

Configure the maximum power that can be reserved on the port. If set to `0` then the limitation is disabled. The power limit is ignored if the maximum observed power consumption exceeds this limit.
- Possible values: `0…30.000` (in watts)
- Default value: `0`. (disable the limitation of inline power)

priority

Configure the inline power priority for this port. In case of power scarcity, inline power on ports configured with the lowest priority is dropped first.
- Possible values: `critical, high` or `low`.
  The highest priority is `critical`.
- Default value: `low`.

Note: This parameter is available for MACH1000, MACH4000 and devices which support Power over Ethernet Plus (MACH104-16TX-PoEP devices and MACH102 devices with media module M1-8TP-RJ45 PoE).

4.15.5 clear inlinepower

Reset the inline power parameters to default settings.

Format

```
clear inlinepower
```

Mode

```
Privileged EXEC
```

4.16 PoE+ - Power over Ethernet Plus

Additionally to the PoE (Power over Ethernet) commands, these commands show and configure the Power over Ethernet Plus (IEEE 802.3at) parameters.

Note: PoE+ is available for:
- MACH104-16TX-PoEP devices
- MACH 102 devices with media module M1-8TP-RJ45 PoEP

4.16.1 show inlinepower slot

This command shows the PoE+ configuration settings and states per slot.

Format

```
show inlinepower slot [<slot> | all]
```

Mode

```
Privileged EXEC and User EXEC
```

Slot

For MACH102 devices with M1-8TP-RJ45 PoEP media modules:
Slot = Slot number of the PoE+ module (valid range: 1 - 2)
For MACH104-16TX-PoEP devices: Slot = 1

Nominal Power

Shows the configured nominal power budget which the device provides for the PoE+ ports of the PoE+ module.

Maximum Power

Shows the nominal power which the device provides for the PoE+ ports of the PoE+ module (valid range: 0 - 248 W).

Reserved Power

Shows the maximum power which the device provides for all PoE+ devices together which are connected to the PoE+ module, based on their classification.

Delivered Power

Shows the current demand for power on all PoE+ ports of the module (valid range: 0 - 248 W).

Send Traps

Shows, if the function is enabled/disabled. If send traps is enabled, the device will send a trap if the power threshold exceeds or falls below the power limit or if the PoE+ power supply is switched on/off on one or more ports.

Power Threshold

Power threshold in per cent of the nominal power. If the power is exceeding/falling below this threshold, the device will send a trap.

4.16.2 inlinepower budget slot

Configure the available power budget per slot in Watts.

Format

```
inlinepower budget slot <slot> <0..1000>
```

Mode

```
Global Config
```

Slot

For MACH102 devices with M1-8TP-RJ45 PoEP media modules:
Slot = Slot number of the PoE+ module (valid range: 1 - 2)
For MACH104-16TX-PoEP devices: Slot = 1

4.16.3 inlinepower threshold slot

Configure the usage power threshold expressed in per cents for comparing the measured power for this slot and initiating an alarm if the threshold is exceeded.

Format

```
inlinepower threshold slot <slot> <0..99>
```

Mode

```
Global Config
```

Slot

For MACH102 devices with M1-8TP-RJ45 PoEP media modules:
Slot = Slot number of the PoE+ module (valid range: 1 - 2)
For MACH104-16TX-PoEP devices: Slot = 1

4.16.4 inlinepower trap slot

Configure the alarm that is send if the configured threshold for this slot is exceeded.

Format

```
inlinepower trap slot <slot> {enable | disable}
```

Mode

```
Global Config
```

Slot

For MACH102 devices with M1-8TP-RJ45 PoEP media modules:
Slot = Slot number of the PoE+ module (valid range: 1 - 2)
For MACH104-16TX-PoEP devices: Slot = 1

4.17 Port monitor

These commands show and configure the port monitor parameters.

The port monitor feature monitors certain port (or global) states or changes and performs a certain action, when the specified condition occurs.

Using this commands, you can disable a port and send a trap (see "port admin shutdown").

Disabling a port by condition will not modify the configuration and therefore not keep the port in disabled state after reload/reboot.

To enable the action if a port state occurs
- enable the port monitor globally,
- enable the port monitor on the port,
- configure condition(s) that is (are) performed in port state on a port and
- an action that is performed on that port, when the condition complies.

The condition can be link flapping or CRC/Fragments error, an action can be sending a trap or disabling that port (and send a trap).

If a port was disabled by the Port-Monitor the port can be enabled again with a port monitor reset command (see “port-monitor reset”).

4.17.1 show port-monitor

Use this command to display the global Port Monitor settings.

Format

```
show port-monitor
```

Mode

```
Global Config
```

Port Monitor

Display if Port Monitor function is enabled or disabled.

Condition crc-fragment interval (seconds)

Display the condition of the CRC fragment interval in seconds.

Condition crc-fragment count

Display the condition of the CRC fragment count.

Condition link flap interval (seconds)

Display the condition of the link flap interval in seconds.

Condition link flap count

Display the condition of the link flap count.

4.17.2 show port-monitor <slot/port>

Use this command to display the Port Monitor details for the port.

Format

```
show port-monitor <slot/port>
```

Mode

```
Global Config
```

Port Monitor

Display if Port Monitor is enabled or disabled.

Link Flap

Display if Link Flap is enabled or disabled.

Crc-Fragment

Display if CRC Fragment is enabled or disabled.

Speed-duplex

Display the link speed and duplex condition for the port.
Possible values: `Enabled, Disabled`.

Active Condition

Display the active condition for the port.
Possible values: `Link-Flap, None`.

Action

Display the action (disable port or send trap) to be triggered on the port. Possible values: Disable-Port, Trap-Only.

Port Oper State

Display the link state of the port. Possible values: `Up, Down`.

4.17.3 show port-monitor brief

Use this command to display the Port Monitor brief summary.

Format

`show port-monitor brief`

Mode

`Global Config`

Intf

Display the number of the interface (`slot/port`).

Admin Mode

Display if Port Monitor is enabled or disabled.

Link Flap

Display if Link Flap is enabled or disabled.

Crc Fragment

Display if CRC Fragment is enabled or disabled.

Speed duplex

Display the link speed and duplex condition for the port.
Possible values: `Enabled, Disabled`.

Active Condition

Display the active condition for the port.
Possible values: `Link-Flap, None`.

Action

Display the action (disable port or send trap) to be triggered on the port. Possible values: `Disable-Port, Trap-Only`.

Port Oper State

Display the link state of the port. Possible values: `Up, Down`.

4.17.4 show port-monitor crc-fragment

Use this command to display the CRC fragment counter.

Format

```
show port-monitor crc-fragment <slot/port>
```

Mode

```
Global Config
```

<slot/port>

Display the Port Monitor interface details.

Crc_fragments in last interval

Display the CRC fragments in last interval.

Crc_fragments total

Display the CRC fragments total.

4.17.5 show port-monitor link-flap

Use this command to display the Link Flap counter for the port.

Format

```
show port-monitor link-flap <slot/port>
```

Mode

```
Global Config
```

<slot/port>

Display the Port Monitor interface details.

Link flaps in last interval

Display the Link flaps in last interval.

Link flaps total

Display the Link flaps total.

4.17.6 show port-monitor overload-detection

Use this command to display the overload detection details for the port.

Format

```
show port-monitor overload-detection <slot/port>
```

Mode

```
Global Config
```

<slot/port>

Display the Port Monitor interface details.

Overload-detection traffic type

Display the overload-detection traffic type for the interface.

Overload-detection threshold type

Display the overload-detection threshold type for the interface.

Overload-detection lower threshold

Display the overload-detection lower threshold for the interface.

Overload-detection upper threshold

Display the overload-detection upper threshold for the interface.

4.17.7 show port-monitor speed-duplex

Use this command to display the link speed and duplex configured modes.

Format

`show port-monitor speed-duplex <slot/port>`

Mode

`Global Config`

<slot/port>

Display the Port Monitor interface details for link speed and duplex condition.

Intf

Display the number of the interface (`slot/port`).

Allowed values

Display the allowed values for link speed and duplex combinations for the interfaces of the device.
Possible values: `hdx-10, fdx-10, hdx-100, fdx-100, hdx-1000, fdx-1000, fdx-10000`.

Allowed modes

Speed-duplex

Display the allowed link speed and duplex combinations for the specific interface.
Possible values: `hdx-10, fdx-10, hdx-100, fdx-100, hdx-1000, fdx-1000, fdx-10000`.

4.17.8 port-monitor (Global Config)

Use this command to enable or disable the Port Monitor globally.
Note: This command does not reset the port disable states.

Default

```
Disable
```

Format

```
port-monitor {enable | disable}
```

Mode

```
Global Config
```

4.17.9 port-monitor (Interface Config)

Use this command to enable or disable the Port Monitor on the port.
Note: This command does not reset the port disable states.

Default

```
Disable
```

Format

```
port-monitor {enable | disable}
```

Mode

```
Interface Config
```

4.17.10 port-monitor action

Use this command to configure the Port Monitor action (disable a port or send a trap).
Note: Disable the Port Monitor action will reset the port from port-state.

Default

```
auto-disable
```

Format

```
port-monitor action
          {port-disable | trap-only | auto-disable}
```

Mode

```
Interface Config
```

port-disable

Disable the port when the configured Port Monitor condition triggers.

trap-only

Send a trap when the configured Port Monitor condition triggers.

auto-disable

Notify Auto Disable when the configured Port Monitor condition triggers.

4.17.11 port-monitor condition link-flap (Global Config)

Use this command to configure the Link Flap settings (Link Flap counter and interval for Link Flap detection).

Default

`Disable`

Format

```
port-monitor condition link-flap
            {count <1..100>| interval <1..180>}
```

Mode

`Global Config`

count

Configure the Link Flap counter.
Default: `5`. Value range: `1 ..100`.

interval

Configure the measure interval in seconds for Link Flap detection.
Default: `10` seconds. Value range: `1 ..180` seconds.

4.17.12 port-monitor condition link-flap (Interface Config)

Use this command to enable or disable Link Flap condition on a port to trigger an action.

Default

`Disable`

Format

`port-monitor condition link-flap {enable | disable}`

Mode

`Interface Config`

4.17.13 port-monitor condition crc-fragment (Global Config)

Use this command to configure the crc-fragment settings (crc-fragment counter and interval for crc-fragment detection).

Default

`Disable`

Format

```
port-monitor condition crc-fragment
     {count <1..1000000> | interval <5..180>}
```

Mode

`Global Config`

count

Configure the crc-fragment counter.
Default: `1000`. Value range: `1..1000000`.

interval

Configure the measure interval in seconds for crc-fragment detection.
Default: `10` seconds. Value range: `5..180` seconds.

4.17.14 port-monitor condition crc-fragment (Interface Config)

Use this command to enable or disable crc-fragment settings on a port to trigger an action.

Default

```
Disable
```

Format

```
port-monitor condition crc-fragment
             {enable | disable}
```

Mode

```
Interface Config
```

4.17.15 port-monitor condition speed-duplex-monitor (Interface Config)

Use this command to enable or disable the link speed and duplex condition on a port to trigger an action.

Default

```
Disable
```

Format

```
port-monitor condition speed-duplex-monitor
                       {enable | disable}
```

Mode

```
Interface Config
```

4.17.16 port-monitor condition speed-duplex-monitor speed (Interface Config)

Use this command to configure the allowed link speed and duplex combinations on a port.

Default

```
{hdx-10, fdx-10, hdx-100, fdx-100, hdx-1000,
 fdx-1000, fdx-10000}
```

Format

```
port-monitor condition speed-duplex-monitor speed
  <speed-duplex1>
   [<speed-duplex2>
     [<speed-duplex3>
       [<speed-duplex4>
         [<speed-duplex5>
           [<speed-duplex6>
             [<speed-duplex7>]]]]]]
```

Mode

```
Interface Config
```

4.17.17 port-monitor condition speed-duplex-monitor clear (Interface Config)

Use this command to clear the allowed link speed and duplex combinations on a port. This will trigger the configured action if the link speed and duplex condition is enabled.

Default

```
{hdx-10, fdx-10, hdx-100, fdx-100, hdx-1000,
 fdx-1000, fdx-10000}
```

Format

```
port-monitor condition speed-duplex-monitor clear
```

Mode

```
Interface Config
```

5 CLI Commands: Switching

This section provides detailed explanation of the Switching commands. The commands are divided into two functional groups:

- Show commands display spanning tree settings, statistics, and other information.
- Configuration Commands configure features and options of the switch. For every configuration command there is a show command that displays the configuration setting.

5.1 Spanning Tree Commands

5.1.1 show spanning-tree

This command displays spanning tree settings for the common and internal spanning tree, when the optional parameter “brief” is not included in the command. The following details are displayed.

Format

```
show spanning-tree [brief]
```

Mode

Privileged EXEC and User EXEC

Spanning Tree Adminmode

```
Enabled or Disabled
```

Bridge Priority

```
Configured value.
```

Bridge Identifier

The bridge identifier for the CST (CST = Classical Spanning Tree IEEE 802.1d). It is made up using the bridge priority and the base MAC address of the bridge.

Time Since Topology Change

in seconds

Topology Change Count

Number of times changed.

Topology Change

Boolean value of the Topology Change parameter for the switch indicating if a topology change is in progress on any port assigned to the common and internal spanning tree.

Designated Root

The bridge identifier of the root bridge. It is made up from the bridge priority and the base MAC address of the bridge.

Root Path Cost

Value of the Root Path Cost parameter for the common and internal spanning tree.

Root Port Identifier

Identifier of the port to access the Designated Root for the CST.

Root Port Max Age

Derived value

Root Port Bridge Forward Delay

Derived value

Hello Time

Configured value

Bridge Hold Time

Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

CST Regional Root

Bridge Identifier of the CST Regional Root. It is made up using the bridge priority and the base MAC address of the bridge.

Regional Root Path Cost

Path Cost to the CST Regional Root.

Associated FIDs

List of forwarding database identifiers currently associated with this instance.

Associated VLANs

List of VLAN IDs currently associated with this instance.

show spanning-tree brief

When the “brief” optional parameter is included, this command displays a brief overview of the spanning tree settings for the bridge. In this case, the following details are displayed.

Bridge Priority

Configured value.

Bridge Identifier

The bridge identifier for the selected MST instance. It is made up using the bridge priority and the base MAC address of the bridge.

Bridge Max Age

Configured value.

Bridge Hello Time

Configured value.

Bridge Forward Delay

Configured value.

Bridge Hold Time

Minimum time between transmission of Configuration Bridge Protocol Data Units (BPDUs)

Rstp Mrp Mode

Rapid spanning tree mrp (Media Redundancy Protocol) mode (Enabled/Disabled)

Rstp Mrp configuration error

Configuration error in Rapid spanning tree mrp (Media Redundancy Protocol) (No/Yes)

5.1.2 show spanning-tree interface

This command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. The following details are displayed on execution of the command.

Format

```
show spanning-tree interface <slot/port>
```

Mode

Privileged EXEC and User EXEC

Port mode

Enabled or disabled.

Port Up Time Since Counters Last Cleared

Time since port was reset, displayed in days, hours, minutes, and seconds.

STP BPDUs Transmitted

Spanning Tree Protocol Bridge Protocol Data Units sent

STP BPDUs Received

Spanning Tree Protocol Bridge Protocol Data Units received.

RST BPDUs Transmitted

Rapid Spanning Tree Protocol Bridge Protocol Data Units sent

RST BPDUs Received

Rapid Spanning Tree Protocol Bridge Protocol Data Units received.

MSTP BPDUs Transmitted

Multiple Spanning Tree Protocol Bridge Protocol Data Units sent

MSTP BPDUs Received

Multiple Spanning Tree Protocol Bridge Protocol Data Units received.

5.1.3 show spanning-tree mst detailed

This command displays settings and parameters for the specified multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance ID. The following details are displayed.

Format

```
show spanning-tree mst detailed <mstid>
```

Mode

Privileged EXEC and User EXEC

mstid

Enter a multiple spanning tree instance identifier.
Valid values: 0 - 4094.

MST Instance ID

Valid value: 0

MST Bridge Priority

Valid values: 0-61440 in increments of 4096.

Time Since Topology Change

in seconds

Topology Change Count

Number of times the topology has changed for this multiple spanning tree instance.

Topology Change in Progress

Value of the Topology Change parameter for the multiple spanning tree instance.

Designated Root

Identifier of the Regional Root for this multiple spanning tree instance.

Root Path Cost

Path Cost to the Designated Root for this multiple spanning tree instance

Root Port Identifier

Port to access the Designated Root for this multiple spanning tree instance

Associated FIDs

List of forwarding database identifiers associated with this instance.

Associated VLANs

List of VLAN IDs associated with this instance.

5.1.4 show spanning-tree mst port detailed

This command displays the detailed settings and parameters for a specific switch port within a particular multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <slot/port> is the desired switch port.

Format

```
show spanning-tree mst port detailed <mstid> <slot/
port>
```

Mode

Privileged EXEC and User EXEC

MST Instance ID

Valid value: 0

Port Identifier

Port priority as a two digit hex number followed by the port number as a two digit hex number.

Port Priority

Decimal number.

Port Forwarding State

Current spanning tree state of this port

Port Role

The port´s current RSTP port role.

Port Path Cost

Configured value of the Internal Port Path Cost parameter

Designated Root

The Identifier of the designated root for this port.

Designated Port Cost

Path Cost offered to the LAN by the Designated Port

Designated Bridge

Bridge Identifier of the bridge with the Designated Port.

Designated Port Identifier

Port on the Designated Bridge that offers the lowest cost to the LAN

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command displays the settings and parameters for a specific switch port within the common and internal spanning tree. The <slot/port> is the desired switch port. In this case, the following are displayed.

Port Identifier

The port identifier for this port within the CST.

Port Priority

The priority of the port within the CST.

Port Forwarding State

The forwarding state of the port within the CST.

Port Role

The role of the specified interface within the CST.

Port Path Cost

The configured path cost for the specified interface.

Designated Root

Identifier of the designated root for this port within the CST.

Designated Port Cost

Path Cost offered to the LAN by the Designated Port.

Designated Bridge

The bridge containing the designated port

Designated Port Identifier

Port on the Designated Bridge that offers the lowest cost to the LAN

Topology Change Acknowledgement

Value of flag in next Configuration Bridge Protocol Data Unit (BPDU) transmission indicating if a topology change is in progress for this port.

Hello Time

The hello time in use for this port.

Edge Port

The configured value indicating if this port is an edge port.

Edge Port Status

The derived value of the edge port status. True if operating as an edge port; false otherwise.

Point To Point MAC Status

Derived value indicating if this port is part of a point to point link.

CST Regional Root

The regional root identifier in use for this port.

CST Port Cost

The configured path cost for this port.

5.1.5 show spanning-tree mst port summary

This command displays the settings of one or all ports within the specified multiple spanning tree instance. The parameter <mstid> indicates a particular MST instance. The parameter {<slot/port> | all} indicates the desired switch port or all ports.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then the status summary is displayed for one or all ports within the common and internal spanning tree.

Format

```
show spanning-tree mst port summary <mstid> {<slot/
port> | all}
```

Mode

Privileged EXEC and User EXEC

MST Instance ID

The MST instance associated with this port. Valid value: 0.

Interface

Valid slot and port number separated by forward slashes.

STP Mode

Current STP mode of this port in the specified spanning tree instance.

Type

Currently not used.

Port Forwarding State

The forwarding state of the port in the specified spanning tree instance

Port Role

The role of the specified port within the spanning tree.

5.1.6 show spanning-tree mst summary

This command displays settings and parameters for the specified multiple spanning tree instance. The following details are displayed.

Format

```
show spanning-tree mst summary
```

Mode

Privileged EXEC and User EXEC

MST Instance ID

Valid value: 0

Associated FIDs

List of forwarding database identifiers associated with this instance.

Associated VLANs

List of VLAN IDs associated with this instance.

5.1.7 show spanning-tree summary

This command displays spanning tree settings and parameters for the switch. The following details are displayed on execution of the command.

Format

```
show spanning-tree summary
```

Mode

Privileged EXEC and User EXEC

Spanning Tree Adminmode

Enabled or disabled.

Spanning Tree Version

Version of 802.1 currently supported (IEEE 802.1Q-2005, IEEE 802.1D-2004) based upon the Force Protocol Version parameter

Configuration Name

Configured name.

Configuration Revision Level

Configured value.

Configuration Digest Key

Calculated value.

Configuration Format Selector

Configured value.

MST Instances

List of all multiple spanning tree instances configured on the switch

5.1.8 show spanning-tree vlan

This command displays the association between a VLAN and a multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID (1-4042).

Format

```
show spanning-tree vlan <vlanid>
```

Mode

Privileged EXEC and User EXEC

vlanid

Enter a VLAN identifier (1 - 4042).

VLAN Identifier

The VLANs associated with the selected MST instance.

Associated Instance

Identifier for the associated multiple spanning tree instance or "CST" if associated with the common and internal spanning tree

5.1.9 spanning-tree

This command sets the spanning-tree operational mode to enabled.

Default

```
disabled
```

Format

```
spanning-tree
```

Mode

```
Global Config
```

no spanning-tree

This command sets the spanning-tree operational mode to disabled. While disabled, the spanning-tree configuration is retained and can be changed, but is not activated.

Format

```
no spanning-tree
```

Mode

```
Global Config
```

5.1.10 spanning-tree auto-edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

Format

```
spanning-tree auto-edgeport
```

Mode

```
Interface Config
```

- **no spanning-tree auto-edgeport**
  This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format

```
no spanning-tree auto-edgeport
```

Mode

```
Interface Config
```

5.1.11 spanning-tree bpduguard

This command sets the BPDU (Bridge Protocol Data Units) Guard on the switch to enabled.

Default

```
disabled
```

Format

```
spanning-tree bpduguard
```

Mode

```
Global Config
```

- **no spanning-tree bpduguard**
  This command sets the BPDU (Bridge Protocol Data Units) Guard to disabled.

Format

```
no spanning-tree bpduguard
```

Mode

```
Global Config
```

5.1.12 spanning-tree configuration name

This command sets the Configuration Identifier Name for use in identifying the configuration that this switch is currently using. The <name> is a string of at most 32 characters.

Default

The base MAC address displayed using hexadecimal notation as specified in IEEE 802 standard.

Format

```
spanning-tree configuration name <name>
```

Mode

```
Global Config
```

no spanning-tree configuration name

This command resets the Configuration Identifier Name to its default.

Format

```
no spanning-tree configuration name
```

Mode

```
Global Config
```

5.1.13 spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using. The Configuration Identifier Revision Level is a number in the range of 0 to 65535.

Default

```
0
```

Format

```
spanning-tree configuration revision <0-65535>
```

Mode

```
Global Config
```

no spanning-tree configuration revision

This command sets the Configuration Identifier Revision Level for use in identifying the configuration that this switch is currently using to the default value, i.e. 0.

Format

```
no spanning-tree configuration revision
```

Mode

```
Global Config
```

5.1.14 spanning-tree edgeport

This command specifies that this port is an Edge Port within the common and internal spanning tree. This will allow this port to transition to Forwarding State without delay.

Format

```
spanning-tree edgeport
```

Mode

```
Interface Config
```

no spanning-tree edgeport

This command specifies that this port is not an Edge Port within the common and internal spanning tree.

Format

```
no spanning-tree edgeport
```

Mode

```
Interface Config
```

5.1.15 spanning-tree forceversion

This command sets the Force Protocol Version parameter to a new value. The Force Protocol Version can be one of the following:

- 802.1d - ST BPDUs are transmitted (802.1Q-2005 functionality supported)
- 802.1s - ST BPDUs are transmitted (802.1Q-2005 functionality supported)
- 802.1w - RST BPDUs are transmitted (802.1Q-2005 functionality supported)

Default

```
802.1w
```

Format

```
spanning-tree forceversion
                          <802.1d | 802.1s | 802.1w>
```

Mode

```
Global Config
```

no spanning-tree forceversion

This command sets the Force Protocol Version parameter to the default value, i.e. 802.1w.

Format

```
no spanning-tree forceversion
```

Mode

```
Global Config
```

5.1.16 spanning-tree forward-time

This command sets the Bridge Forward Delay parameter to a new value for the common and internal spanning tree. The forward-time value is in seconds within a range of 4 to 30, with the value being greater than or equal to "(Bridge Max Age / 2) + 1".

Default

```
15
```

Format

```
spanning-tree forward-time <4-30>
```

Mode

```
Global Config
```

no spanning-tree forward-time

This command sets the Bridge Forward Delay parameter for the common and internal spanning tree to the default value, i.e. 15.

Format

```
no spanning-tree forward-time
```

Mode

```
Global Config
```

5.1.17 spanning-tree guard loop

This command enables loop guard and disables root guard on an interface.

Default

```
disabled
```

Format

```
spanning-tree guard loop
```

Mode

```
Interface Config
```

- **no spanning-tree guard**
  This command disables the guard for this port.

Format

```
no spanning-tree guard
```

Mode

```
Interface Config
```

5.1.18 spanning-tree guard none

This command disables root guard and disables loop guard on an interface.

Default

```
disabled
```

Format

```
spanning-tree guard none
```

Mode

```
Interface Config
```

no spanning-tree guard

This command disables the guard for this port.

Format

```
no spanning-tree guard
```

Mode

```
Interface Config
```

5.1.19 spanning-tree guard root

This command enables root guard and disables loop guard on an interface.

Default

```
disabled
```

Format

```
spanning-tree guard root
```

Mode

```
Interface Config
```

- **no spanning-tree guard**
  This command disables the guard for this port.

Format

```
no spanning-tree guard
```

Mode

```
Interface Config
```

5.1.20 spanning-tree hello-time

This command sets the Hello Time parameter to a new value for the common and internal spanning tree. The hellotime <value> is in whole seconds within a range of 1 to 2 with the value being less than or equal to "(Bridge Max Age / 2) - 1".

Default

```
2
```

Format

```
spanning-tree hello-time <1-2>
```

Mode

```
Interface Config
Global Config
```

no spanning-tree hello-time
This command sets the Hello Time parameter for the common and internal spanning tree to the default value, i.e. 2.

Format

```
no spanning-tree hello-time
```

Mode

```
Interface Config
Global Config
```

5.1.21 spanning-tree hold-count

This command sets the bridge hold count parameter.

Default

```
disabled
```

Format

```
spanning-tree hold-count <1-40>
```

Mode

`Global Config`

<1-40>

Enter the bridge parameter for hold count as an integer in the range 1 - 40.

no spanning-tree hold-count

This command sets bridge hold count to disabled.

Format

`no spanning-tree hold-count`

Mode

`Global Config`

5.1.22 spanning-tree max-age

This command sets the Bridge Max Age parameter to a new value for the common and internal spanning tree. The max-age value is in seconds within a range of 6 to 40, with the value being less than or equal to "2 times (Bridge Forward Delay - 1)".

Default

`20`

Format

`spanning-tree max-age <6-40>`

Mode

`Global Config`

no spanning-tree max-age

This command sets the Bridge Max Age parameter for the common and internal spanning tree to the default value, i.e. 20.

Format

```
no spanning-tree max-age
```

Mode

```
Global Config
```

5.1.23 spanning-tree max-hops

This command sets the Bridge Max Hops parameter to a new value for the common and internal spanning tree. The max-hops value is an integer within a range of 1 to127.

Format

```
spanning-tree max-hops <1-127>
```

Mode

```
Global Config
```

no spanning-tree max-hops

This command sets the Bridge Max Hops parameter for the common and internal spanning tree to the default value, i.e. 20.

Format

```
no spanning-tree max-age
```

Mode

```
Global Config
```

5.1.24 spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.
This command accepts the value 0 for the mstid, meaning the common and internal spanning tree.

If the ‘cost’ token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. The pathcost can be specified as a number in the range of 1 to 200000000 or auto. If "auto" is specified, the pathcost value will be set based on Link Speed.

If the ‘port-priority’ token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter. The port-priority value is a number in the range of 0 to 240 in increments of 16.

Default

```
cost : auto; external-cost : auto;
port-priority : 128
```

Format

```
spanning-tree mst <mstid>
     {{cost <1-200000000> | auto } |
      {external-cost <1-200000000> | auto } |
       port-priority <0-240>}
```

Mode

```
Interface Config
```

no spanning-tree mst

This command sets the Path Cost or Port Priority for this port within the multiple spanning tree instance or in the common and internal spanning tree to the respective default values. If the <mstid> parameter corresponds to an existing multiple spanning tree instance, then the configurations are done for that multiple spanning tree instance. If however 0 (defined as the default CIST ID) is passed as the <mstid>, then the configurations are performed for the common and internal spanning tree instance.
This command accepts the value 0 for the mstid, meaning the common and internal spanning tree.
If the ‘cost’ token is specified, this command sets the path cost for this port within a multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. a pathcost value based on the Link Speed.
If the ‘port-priority’ token is specified, this command sets the priority for this port within a specific multiple spanning tree instance or the common and internal spanning tree instance, depending on the <mstid> parameter, to the default value, i.e. 128.

Format

```
no spanning-tree mst <mstid> <cost | port-priority>
```

Mode

```
Interface Config
```

5.1.25 spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The priority value is a number within a range of 0 to 61440 in increments of 4096.
This command accepts the value 0 for the mstid.

If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter to a new value for the common and internal spanning tree. The bridge priority value again is a number within a range of 0 to 61440. The twelve least significant bits will be masked according to the 802.1s specification. This will cause the priority to be rounded down to the next lower valid priority.

Default

```
32768
```

Format

```
spanning-tree mst priority <mstid> <0-61440>
```

Mode

```
Global Config
```

no spanning-tree mst priority

This command sets the bridge priority for a specific multiple spanning tree instance to the default value, i.e. 32768. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance.
This command accepts the value 0 for the mstid.
If 0 (defined as the default CIST ID) is passed as the <mstid>, then this command sets the Bridge Priority parameter for the common and internal spanning tree to the default value, i.e. 32768.

Format

```
spanning-tree mst priority <mstid>
```

Mode

```
Global Config
```

5.1.26 spanning-tree mst vlan

This command adds an association between a multiple spanning tree instance and a VLAN. The VLAN will no longer be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID (1-4042).
This command accepts the value 0 for the mstid.

Format

```
spanning-tree mst vlan <mstid> <vlanid>
```

Mode

```
Global Config
```

no spanning-tree mst vlan

This command removes an association between a multiple spanning tree instance and a VLAN. The VLAN will again be associated with the common and internal spanning tree. The instance <mstid> is a number that corresponds to the desired existing multiple spanning tree instance. The <vlanid> corresponds to an existing VLAN ID.
This command accepts the value 0 for the mstid.

Format

```
no spanning-tree mst vlan <mstid> <vlanid>
```

Mode

```
Global Config
```

5.1.27 spanning-tree mst instance

This command creates a MST instance.

Format

```
spanning-tree mst instance <1-4094>
```

Mode

```
Global Config
```

<1-4094>

Enter a multiple spanning tree instance identifier.

no spanning-tree mst instance

This command removes a MST instance.

Format

```
no spanning-tree mst instance <1-4094>
```

Mode

```
Global Config
```

<1-4094>

Enter a multiple spanning tree instance identifier.

5.1.28 spanning-tree port mode

This command sets the Administrative Switch Port State for this port to enabled.

Default

```
disabled
```

Format

```
spanning-tree port mode
```

Mode

```
Interface Config
```

- **no spanning-tree port mode**
  This command sets the Administrative Switch Port State for this port to disabled.

Format

```
no spanning-tree port mode
```

Mode

```
Interface Config
```

5.1.29 spanning-tree port mode all

This command sets the Administrative Switch Port State for all ports to enabled.

Default

disabled

Format

```
spanning-tree port mode all
```

Mode

Global Config

- **no spanning-tree port mode all**
  This command sets the Administrative Switch Port State for all ports to disabled.

Format

```
no spanning-tree port mode all
```

Mode

Global Config

5.1.30 spanning-tree stp-mrp-mode

This command sets the spanning tree mrp (Media Redundancy Protocol) mode to enabled.

Default

disabled

Format

```
spanning-tree stp-mrp-mode
```

Mode

Global Config

- **no spanning-tree stp-mrp-mode**
  This command sets the spanning tree mrp (Medium Redundancy Protocol) mode to disabled.

Format

```
no spanning-tree stp-mrp-mode
```

Mode

Global Config

5.1.31 spanning-tree tcnguard

This command enables tcn guard on an interface.

Default

```
disabled
```

Format

```
spanning-tree guard tcnguard
```

Mode

```
Interface Config
```

no spanning-tree tcnguard

This command disables tcn guard for this port.

Format

```
no spanning-tree tcnguard
```

Mode

```
Interface Config
```

5.2 MRP

The concept of the MRP-Ring enables the construction of high-availability, ring-shaped network structures.

The two ends of a backbone in a line-type configuration can be closed to form a redundant ring - the MRP-Ring - by using the RM function (Redundancy Manager) of the Switch.

It is possible to mix the devices that support this function in any combination within the MRP ring.

If a line section becomes inoperable, the ring structure of up to 50 switches typically transforms back to a line-type configuration within 150 ms (maximum 500 ms).

5.2.1 show mrp

This command displays the settings and states of the MRP-Ring. The following details are displayed on execution of the command.

Format

show mrp [current-domain]

Mode

Privileged EXEC and User EXEC

current-domain

Specify the optional keyword "current-domain" to show the current MRP domain's settings. If you omit the keyword "current-domain", the show command will display the settings of all existing MRP domains. **Note:** Currently, it is only possible to configure one MRP domain, so the keyword keyword "current-domain" can be omitted (it exists for future compatibility reasons).

5.2.2 show mrp current-domain

This command displays the settings and states of the MRP-Ring´s current domain. The following details are displayed on execution of the command. If you omit the optional keywords (e. g., advanced-mode), all settings will be displayed.

Format

```
show mrp current-domain [advanced-mode |
  domain-id | info | manager-priority | mode |
  name | recovery-delay | operation |
  port [primary | secondary] | summary | vlan]
```

Mode

Privileged EXEC and User EXEC

advanced mode

Show the switch's advanced mode setting for the given MRP domain.

domain-id

Show the given MRP domain's ID.

info

Show status information for the given MRP domain.
Note: The information displayed depends on the switch's mode (Client or Manager) because only a subset of them are useful for each mode.

manager-priority

Show the switch's manager priority for the given MRP domain.

mode

Show the switch's mode for the given MRP domain.

name

Show the given MRP domain's name.

recovery-delay

Show the given MRP domain's recovery delay.

operation

Show the switch's administrative setting for the given MRP domain (enabled or disabled).

port

Show the ports for the given MRP domain

port primary

Show the primary port for the given MRP domain.

port secondary

Show the secondary port for the given MRP domain.

summary

Show a summary for the given MRP domain.

vlan

Show the VLAN ID for the given MRP domain.

5.2.3 mrp current-domain

Specify that you want to configure the current MRP domain's settings.

Default

```
none
```

Format

```
mrp current-domain {advanced-mode {disable|enable}
| manager-priority <0-65535>
| mode {client|manager} | name <domain-name>
| recovery-delay {500ms|200ms}
| operation {disable|enable}
| port {primary|secondary} <slot/port>
| vlan <0-4042>}
```

Mode

```
Global Config
```

advanced-mode

Enable or disable the switch's advanced mode for the given MRP domain.

manager-priority

Configure the given MRP domain's manager priority (0-65535).

mode

Configure the switch's MRP mode for the given domain (client or manager).
`client`: Switch is client for the given MRP domain.
`manager`: Switch is manager for the given MRP domain.

name

Set a name for the given MRP domain.

recovery-delay

Configure the MRP recovery delay for the given domain.
`500ms`: Recovery delay is 500 ms for the given MRP domain.
`200ms`: Recovery delay is 200 ms for the given MRP domain.

operation

Enable or disable the switch for the given MRP domain.

port

Specify the switch's ports for the given MRP domain (in slot/port notation).
`primary`: Specify the switch's primary port for the given MRP domain.

`secondary`: Specify the switch's secondary port for the given MRP domain.

vlan

Enter the VLAN for the given MRP domain
Possible values: `0..4042`
Default Value: `0`

5.2.4 mrp delete-domain

Delete current MRP domain.

Format

```
mrp delete-domain current-domain
```

Mode

```
Global Config
```

5.2.5 mrp new-domain

Create a new MRP domain. The configuration will consist of default parameters and its operation will be disabled.

Default

`n/a` not set

Format

```
mrp new-domain (<domain-id> | default-domain)
```

Mode

```
Global Config
```

domain-id

Enter a new MRP domain id. Format: 16 bytes in decimal notation, example: 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16
The MRP domain id 0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0 is invalid.

default-domain

Create a default MRP domain (ID: 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255).

5.2.6 arc

Use this command to configure ARC (Automatic Ring Configuration). ARC supports MRP.

The ARC protocol is a simple protocol that checks a ring configuration and, if suitable, configures all clients of this ring automatically.

The check cycle includes an analysis of the ARC devices for an already active ring configuration and wrong ring configuration values. The ARC devices can detect loop situations and other ARC Managers in the ring. Errors are reported to the ARC Manager. With this information the ARC Manager can decide whether a configuration of the ring clients is possible or not.

Format

```
arc { manager {enable | disable} |
      client {enable | disable | checkOnly} |
      check |
      configure}
```

Mode

Global Config

client

Configure the ARC client.
- `enable`: Enable the ARC client for configuring and checking.
- `disable`: Disable the ARC client for configuring and checking.
- `checkOnly`: The device can only be checked but not configured by ARC.

manager

Configure the ARC manager.
- `enable`: Enable the ARC manager for configuring and checking.
- `disable`: Disable the ARC manager for configuring and checking.

check

Check the topology. All important values will be taken from the current ring configuration on the devices.

configure

Configure the topology. All important values will be taken from the current ring configuration of the ARC manager.

5.2.7 show arc

This command displays the current ARC configuration and the result of the last action.

Format

```
show arc
```

Mode

```
Global Config
```

Client Settings:

Display the Client Settings for the current ARC configuration.

Admin Status

Display if the ARC client is enabled or disabled.

MAC address of the ARC Manager

Display the MAC address of the ARC Client.

IP address of the ARC Manager

Display the IP address of the ARC Client.

Port 1

Display the number of Ring Port 1 for the client (slot/port).

Port 2

Display the number of Ring Port 2 for the client (slot/port).

Manager Settings:

Display the Manager Settings for the current ARC configuration.

Admin Status

Display the ARC manager is enabled or disabled

Protocol

Display the Protocol. Possible values: mrp, ...

Port 1

Display the number of Ring Port 1 for the manager (slot/port).

Port 2

Display the number of Ring Port 2 for the manager (slot/port).

VLAN ID

Display the VLAN ID. Possible values: 0 - ....

Last Action Result

Display the Result of the Last Action.
Possible values: Ring is open, Already Configured, Loop Source, Multiple RM, Configuration failed, Port not in full duplex mode, ARC not supported by the ring devices.

Last Check result:

Display the Result of the last check.
- `Nr:` Display the number of the check result.
- `Mac Address:` Display the concerned MAC address.
- `IP Address:` Display the concerned IP address.
- `Type:` Display the type of the result. Possible values: `Error, Warning.`

Possible check results (examples):

```
Error - Ring is open
Warning - Already Configured - HIPER Ring - Port1: 1.1 - Port2: 1.2
Warning - Already Configured - MRP - Port1: 1.9 - Port2: 1.10 - VLAN ID: 0
Warning - Already Configured - Fast HIPER Ring - Port1: 1.3 - Port2: 1.4
Error - Loop Source - Hop count: 1 - Port1: 1.1 - Port2: 1.4 - Port3: 1.15
Error - Multiple RM - MRP
Error - Configuration failed - MRP
Warning - Port not in full duplex mode - Port1: 1.1 Half - Port2: 1.2 Full
Warning - ARC not supported by the ring devices
```

5.3 HIPER-Ring

The concept of the HIPER-Ring enables the construction of high-availability, ring-shaped network structures. Within such a ring topology, network components supporting the HIPER-Ring are connected with each other via their ring ports. Exactly one redundancy manager assumes control of the ring. These commands are for configuring the Hirschmann High Performance Redundancy Ring.

Further information concerning this function you will find in the User Manual ”Redundancy Configuration”.

5.3.1 show hiper-ring

This command displays the settings and states of the HIPER-Ring. The following details are displayed on execution of the command.

Format

```
show hiper-ring
  {info | mode | port [primary | secondary] |
  redundancy-state | rm-state | recovery-delay}
```

Mode

Privileged EXEC and User EXEC

info

Display the information about the HIPER-Ring configuration (cabling).

mode

Display the HIPER-Ring mode settings.

port

Display the HIPER-Ring's primary and secondary port properties.

port primary

Display the HIPER Ring's primary port properties.

port secondary

Display the HIPER Ring's secondary port properties.

redundancy-state

Display the actual state of the HIPER-Ring redundancy.

rm-state

Display the state of the HIPER Ring redundancy manager.

recovery-delay

Display the value of the recovery delay.

5.3.2 hiper-ring

Configure the HIPER-Ring.
Press Enter for a list of valid commands and their recommended order.

Format

```
hiper-ring
```

Mode

```
Global Config
```

- **no hiper-ring**
  Clear the HIPER Ring configuration (delete it).

Format

```
no hiper-ring
```

Mode

```
Global Config
```

5.3.3 hiper-ring mode

This command sets the HIPER-Ring mode. Possible values are:

- `ring-manager` Set the switch's HIPER Ring mode to Ring Manager.
- `rm` Abbreviation of Ring Manager.
- `ring-switch` Set the switch's HIPER Ring mode to Ring Switch.
- `rs` Abbreviation of Ring Switch.

Default

```
none
```

Format

```
hiper-ring mode <{ring-manager|ring-switch|rm|rs}>
```

Mode

```
Global Config
```

5.3.4 hiper-ring port primary

Enter the switch's primary HIPER Ring port.

Default

`n/a` (not set)

Format

`hiper-ring port primary <primary ring port>`

Mode

`Global Config`

primary ring port

Enter the switch's primary HIPER Ring port (`<slot/port>`).

5.3.5 hiper-ring port secondary

Enter the switch's secondary HIPER Ring port.

Default

`n/a` not set

Format

`hiper-ring port secondary <secondary ring port>`

Mode

`Global Config`

secondary ring port

Enter the switch's secondary HIPER Ring port (`<slot/port>`).

5.3.6 hiper-ring recovery-delay

Defines the maximum recovery delay of ring recovery in the HIPER Ring (`500` or `300` ms).

Default

`n/a` not set

Format

```
hiper-ring recovery-delay (<500/300>)
```

Mode

```
Global Config
```

5.4 Fast-HIPER-Ring

The concept of the Fast-HIPER-Ring enables the construction of high-availability, ring-shaped network structures. Within such a ring topology, network components supporting the Fast-HIPER-Ring are connected with each other via their ring ports. Exactly one redundancy manager assumes control of the ring.
These commands are for configuring the Hirschmann Fast High Performance Redundancy Ring.

Further information concerning this function you will find in the User Manual ”Redundancy Configuration”.

This command displays the settings and states of the HIPER-Ring. The following details are displayed on execution of the command.

Format

```
show fast-hiper-ring
```

Mode

Privileged EXEC and User EXEC

Ring ID

Display the Ring ID.

Mode of Switch (administrative setting)

Display the HIPER-Ring mode administrative settings.

Mode of Switch (real operating state)

Display the HIPER-Ring operation mode.

Ring Name

Display theFast-HIPER-Ring's name.

Number of nodes in the ring

Display the number of nodes in the ring.

Port Number, Primary

Display the HIPER-Ring's primary port number and its properties.

Port Number, Secondary

Display the HIPER-Ring's secondary port number and its properties.

Operation

Display the admin state of the HIPER-Ring configuration.

General Operating States

Display general information concerning the fast-hiper-ring state.

Specify that you want to show the current Fast HIPER-Ring ID's settings.

Format

```
show fast-hiper-ring current-id
  {id | info | mode | operation | port |
  port [primary |secondary] | summary |
  ring-name | nodes | vlan}
```

Mode

Privileged EXEC and User EXEC

id

Display the given Fast HIPER-Ring's ID.

info

Display status information for the given Fast HIPER-Ring ID.

mode

Display the switch's mode for the given Fast HIPER-Ring ID.

operation

Display the switch's operative setting for the given Fast HIPER-Ring ID.
Note: In case of configuration problems, this value may differ from the administrative setting (may become 'Disabled').

port

Display the ports for the given Fast HIPER-Ring ID.

port primary

Display the primary port for the given Fast HIPER-Ring ID.

port secondary

Display the secondary port for the given Fast HIPER-Ring ID.

summary

Display a summary for the given Fast HIPER-Ring ID.

ring-name

Display the ring name for the given Fast HIPER-Ring ID.

nodes

Display the number of nodes in the ring for the given Fast HIPER-Ring ID.

vlan

Display the VLAN ID for the given Fast HIPER-Ring ID.

5.4.1 fast-hiper-ring

Configure the Fast-HIPER-Ring.

Format

```
fast-hiper-ring {current-id
 {mode {ring-manager|ring-switch|rm|rs} |
 operation {disable|enable} |
 port {primary|secondary} <slot/port> |
 ring-name <ring-name> |
 nodes <1-n> |
 vlan <0-4042>} |
delete-id current-id |
new-id {<id>|default-id}}
```

Mode

Global Config

current-id

Specify that you want to configure the current Fast-HIPER-Ring ID's settings.

mode

Configure the switch's Fast HIPER-Ring mode for the given ID (ring-manager or ring-switch).
rm: Abbreviation for 'ring-manager'.
rs: Abbreviation for 'ring-switch'.

mode ring-manager

Switch is ring-manager for the given Fast HIPER-Ring ID.

mode ring-switch

Switch is ring-switch for the given Fast HIPER-Ring ID.

mode rm

Abbreviation for 'ring-manager'.

mode rs

Abbreviation for 'ring-switch'.

operation

Enable or disable the switch for the given Fast-HIPER-Ring ID.

port

Specify the switch's ports for the given Fast-HIPER-Ring ID.

ring-name

Set a ring name for the given Fast HIPER-Ring ID.

nodes

Specify the number of nodes in the ring for the given Fast HIPER-Ring ID.

vlan

Specify the VLAN for the given Fast HIPER-Ring ID.

delete-id

Delete the given Fast HIPER-Ring ID.

new-id

Create a new Fast HIPER-Ring ID. The configuration will consist of default parameters and its operation will be disabled.

<id>

Enter a new Fast HIPER-Ring ID. Format: a number in the range 1-2147483647 (2^31 - 1). An ID of 0 is invalid.

default-id

Create a default Fast HIPER-Ring ID (1).

5.5 Redundant Coupling

The control intelligence built into the switch allows the redundant coupling of HIPER-Rings and network segments. Two network segments can be connected via two separate paths with one of the following switches:

- RS2-16M
- RS20/RS30/RS40
- RSR20/RSR30
- MICE (Rel. 3.0 or higher)
- MS20/MS30
- PowerMICE
- MACH1000
- MACH3000 (Rel. 3.3 or higher)
- MACH4000

The switch in the redundant line and the switch in the main line inform each other about their operating states by using control frames via the ethernet or via the control line.

Note: For redundancy security reasons, the Rapid Spanning Tree protocol and redundant network/ring coupling may not be enabled simultaneously.

Note: The network that connects the master and the slave must always be a HiPER-Ring. The coupling switch in single mode also must have a HiPER-Ring Configured.

Further information concerning this function you will find in the User Manual ”Redundancy Configuration”.

These commands allow you to configure the redundant coupling of network segments.

5.5.1 show ring-coupling

This command displays the settings and states of the network coupling / ring coupling.

To set up a new Ring Coupling configuration when no configuration is currently present (e. g., after a clear command), always set the local port first. Please refer to: ring-coupling port local <slot/port>.

The following details are displayed on execution of the command.

Format

```
show ring-coupling <config | info |
net-coupling | operation | partner-ip |
port [ all | control | local | partner] |
redundancy-mode>
```

Mode

Privileged EXEC and User EXEC

config

Display the Ring Coupling's configuration
- single
- dual-master-inband
- dual-master-outband
- dual-slave-inband
- dual-slave-outband.

info

Display information about the Ring Coupling's states:
- configuration failure,
- Extended diagnosis,
- redundancy guaranteed.

net-coupling

Display the Ring Coupling's ring/network coupling setting (network/ring-only).

operation

Display the Ring Coupling's operation setting
- on
- off

partner IP

Display the switch's Ring Coupling partner IP address (only valid for remote configurations).

port

Display the switch's Ring Coupling ports
– `all`
– `local`
– `partner` (only takes effect in dual configurations)
– `control` (only takes effect in outband configurations).

redundancy-mode

Display the Ring Coupling's redundancy mode
– `normal`
– `extended`.

Ring/Network Coupling Mode

Display the Ring/Network Coupling mode
– `ring-only` if you wish to couple a HIPER-Ring.
– `network` if you wish to couple a line-type configuration.

5.5.2 ring-coupling

Configure the redundant coupling of HIPER-Rings / network segments. This command, if called without arguments, lists the available subcommands, their recommended order and tips how to set up a new configuration.

Format

```
ring-coupling
```

Mode

```
Global Config
```

- **no ring-coupling**
  Clear the ring-coupling configuration (delete it).

Format

```
no ring-coupling
```

Mode

```
Global Config
```

5.5.3 ring-coupling config

This command sets the Ring Coupling configuration.

Possible values are:

- `single` Configure the Ring Coupling's basic setting to single (both coupling ports are local to the switch, switch performs master and slave functions).
- `dual-master-inband` Configure the Ring Coupling's basic setting to dual-master-inband (2nd coupling port is on a remote switch, local switch is master, communication over network).
- `dual-master-outband` Configure the Ring Coupling's basic setting to dual-master-outband (2nd coupling port is on a remote switch, local switch is master, communication over dedicated control port).
- `dual-slave-inband` Configure the Ring Coupling's basic setting to dual-slave-inband (2nd coupling port is on a remote switch, local switch is slave, communication over network).
- `dual-slave-outband` Configure the Ring Coupling's basic setting to dual-slave-outband (2nd coupling port is on a remote switch, local switch is slave, communication over dedicated control port).
- `dmi` Abbreviation for `dual-master-inband`.
- `dmo` Abbreviation for `dual-master-outband`.
- `dsi` Abbreviation for `dual-slave-inband`.
- `dso` Abbreviation for `dual-slave-outband`.

Default

```
none
```

Format

```
ring-coupling config <{ single |
dual-master-inband | dual-master-outband |
dual-slave-inband | dual-slave-outband |
dmi | dmo | dsi | dso }>
```

Mode

```
Global Config
```

5.5.4 ring-coupling net-coupling

Coupling mode refers to the type of coupled network.

Possible values are:

- `network` ,if you wish to couple a line-type configuration.
- `ring-only` ,if you wish to couple a HIPER-Ring.

Default

`none`

Format

`ring-coupling net-coupling <{network|ring-only}>`

Mode

`Global Config`

5.5.5 ring-coupling operation

Configure the Ring Coupling's operation setting. Possible values are:

- `on` Enable the current Ring Coupling configuration.
- `off` Disable the current Ring Coupling configuration.

Default

`off`

Format

`ring-coupling operation <{off|on}>`

Mode

`Global Config`

5.5.6 ring-coupling port

Configure the Ring Coupling's ports. Possible values are:

- `control` Enter the Ring Coupling's control coupling port in outband configurations.
- `local` Enter the Ring Coupling's local coupling port.
- `partner` Enter the Ring Coupling's partner coupling port in single mode configuration.

Default

`none`

Format

`ring-coupling port <{control|local|partner}> <slot/port>`

Mode

`Global Config`

5.5.7 ring-coupling redundancy-mode

Configure the Ring Coupling's redundancy mode. Possible values are:

- `extended` Slave responds to a failure in the remote ring or network.
- `normal` Slave does not respond to a failure in the remote ring or network.

Default

`extended`

Format

`ring-coupling redundancy-mode <{extended|normal}>`

Mode

`Global Config`

5.6 Port Security

With the Port Securitiy function you can specify for each port from which terminal devices data can be received and sent to other ports. This function helps to protect the network from unauthorized access.

5.6.1 show port-sec dynamic

Use this command to display the dynamic MAC limit port-related settings (dynamic limit,current MAC count, current action and current port state).

Format

`show port-sec dynamic {all | <slot/port>}`

Mode

`Global Config`

all

Display information for each port.

<slot|port>

Display information for one specific port.

Port

Display the number of the port (`slot/port`).
Possible values: `1/1`, `1/2`, ...

State

Display state of dynamic MAC limit port-related settings.
Possible values: `Disabled`, `Enabled`
Default value: `Enabled`

Limit

Display the currently configured dynamic limit of MAC addresses allowed to be learned on the interface.

Possible values: `0..50`
Default value: `0`

Current

Display current number of MAC addresses learned on the interface.
Possible values: `0..50`
Default value: `0`

Action

Display the currently configured action to be taken if port security is violated at this port.
Possible values: `None, Auto Disable, Port Disable, Trap Only`
Default value: `Auto Disable`

5.6.2 show port-sec mode

Display the MAC/IP Based Port Security global setting for all ports.

Format

```
show port-sec mode
```

Mode

Privileged EXEC and User EXEC

5.6.3 show port-sec port

Display the MAC/IP Based Port Security port-related settings (allowed MAC address, current MAC address, allowed IP address, current action and current port state).

Format

```
show port-sec port <{all|<slot/port>}>
```

Mode

Privileged EXEC and User EXEC

5.6.4 port-sec mode

Configure the global MAC/IP Based Port Security mode:

- `ip-based` Port security is based on a given, allowed source IP address.
- `mac-based` Port security is based on a given, allowed source MAC address.

Format

```
port-sec mode <{ip-based|mac-based}>
```

Mode

```
Global Config
```

5.6.5 port-sec action

Configure the action to be taken if port security is violated at this port.

- `none`
  No action is taken if port security is violated at this port.
- `auto-disable`
  The port is auto-disabled for traffic if port security is violated
- `port-disable`
  The port is disabled for traffic if port security is violated.
- `trap-only`
  A trap is sent if port security is violated at this port (this port remains open for traffic).

Configure the allowed IP source address for this port.
Configure the allowed MAC source address for this port.

Format

```
port-sec {action {none | auto-disable |
          port-disable | trap-only}
         |allowed-ip <IP1> [IP2 [IP3 [IP4 [IP5
              [IP6 [IP7 [IP8 [IP9 [IP10]]]]]]]]]
         |allowed-mac <MAC1> [MAC2 [MAC3 [MAC4
              [MAC5 [MAC6 [MAC7 [MAC8 [MAC9
              [MAC10]]]]]]]] }
```

Mode

`Interface Config`

- **no port-sec**
  No action is taken if port security is violated at this port.

Format

```
no port-sec
```

Mode

`Interface Config`

5.6.6 port-sec allowed-ip

Enter the allowed IP source address for this port, format: nnn.nnn.nnn.nnn (nnn: decimal number 0..255) (up to 10).

Format

```
port-sec allowed-ip <IP Address 1> <IP Address 2>
... <IP Address 10>
```

Mode

```
Interface Config
```

5.6.7 port-sec allowed-ip add

Enter the allowed IP source address for this port, format: nnn.nnn.nnn.nnn (nnn: decimal number 0..255) (up to 50).

Format

```
port-sec allowed-ip add <IP Address 1>
                  <IP Address 2> ... <IP Address 50>
```

Mode

```
Interface Config
```

5.6.8 port-sec allowed-ip remove

Enter the allowed IP source address for this port, format: nnn.nnn.nnn.nnn (nnn: decimal number 0..255) (up to 50).

Format

```
port-sec allowed-ip remove <IP Address 1>
                  <IP Address 2> ... <IP Address 50>
```

Mode

```
Interface Config
```

5.6.9 port-sec allowed-mac

Enter the allowed MAC source address for this port, format: nn:nn:nn:nn:nn:nn (n: hexadecimal digit) or format: nn:nn:nn:nn:nn:nn/m (n: hexadecimal digit) (m: decimal digit (1..48)) (up to 10).

Format

```
port-sec allowed-mac <MAC Address 1>
<MAC Address 2> ... <MAC Address 10>
```

Mode

```
Interface Config
```

5.6.10 port-sec allowed-mac add

Enter the allowed MAC source address for this port,
format: nn:nn:nn:nn:nn:nn (n: hexadecimal digit) or
format: nn:nn:nn:nn:nn:nn/m
n: hexadecimal digit, m: decimal digit (1..48)
(up to 50).

Format

```
port-sec allowed-mac add <MAC Address 1>
             <MAC Address 2> ... <MAC Address 50>
```

Mode

```
Interface Config
```

5.6.11 port-sec allowed-mac remove

Enter the allowed MAC source address for this port,
format: nn:nn:nn:nn:nn:nn (n: hexadecimal digit) or
format: nn:nn:nn:nn:nn:nn/m
n: hexadecimal digit, m: decimal digit (1..48)
(up to 50).

Format

```
port-sec allowed-mac remove <MAC Address 1>
             <MAC Address 2> ... <MAC Address 50>
```

Mode

```
Interface Config
```

5.6.12 port-sec dynamic

Use this command to configure the dynamic limit of MAC addresses allowed to be learned on the interface. A value of `0` disables the dynamic limit.

Format

```
port-sec dynamic <max-count>
```

Mode

```
Interface Config
```

<max-count>

Enter the maximum number of dynamically learned allowed MAC addresses
– Possible values: `0..50`
– Default: `0`
– A value of `0` disables the dynamic limit.

5.6.13 clear port-sec

Clear the MAC/IP Based Port Security by setting each port's security action (applied when port security is violated) to None. Additionally, the global mode is set to MAC Based.

Note: This does not clear the 802.1X Port Security.

Format

```
clear port-sec
```

Mode

```
User EXEC and Global Config
```

5.7 DHCP Relay Commands

These commands configure the DHCP Relay parameters. The commands are divided by functionality into these different groups:

- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display switch settings, statistics and other information.
- Commands that start with the keyword ’no’ (so-called ’no commands’) are used to clear some or all of the settings to factory defaults.

5.7.1 dhcp-relay

Set different options for BOOTP/DHCP relay and option 82 inclusion.

Format

```
dhcp-relay
 {opt82
   {operation {disable|enable}|
    man-id <Manual Remote ID>|
    remote-id-type {client-id|ip|mac|other}}|
  server-address <Server-ID (1..16)>
      <Server IP Address> [<slot/port> | all] }
```

Mode

Global Config

dhcp-relay opt82 operation {disable|enable}

Enable/Disable option 82 globally. Default: enable.

dhcp-relay opt82 man-id <Manual Remote ID>

Configure the DCHP Relay's Option 82 Manual Value for the Remote ID Type (only effective, if Remote ID is set to ”other“). Default: no ID.

dhcp-relay opt82 remote-id-type {client-id|ip|mac|other}

Configure the DCHP Relay's Option 82 Remote ID Type.
Default: mac

dhcp-relay server-address
<Server ID (1..16)> <Server IP Address> [<slot/port> | all]

Set the server IP address for one of the 16 possible server IDs.
Default: 0.0.0.0.
Optionally, configure this entry to a specific interface. If an interface is set, only DHCP packets from this interface are relayed to the server.

no dhcp-relay

Clear the DCHP Relay configuration (set all server addresses to 0.0.0.0).

Format

```
no dhcp-relay
```

Mode

Global Config

5.7.2 dhcp-relay

Set different port specific options for option 82 inclusion.

Format

```
dhcp-relay {admin-state {disable|enable} |
            operation {disable|enable} |
            hirschmann-device {disable|enable} |
            hirschmann-agent {disable|enable}}
```

Mode

```
Interface Config
```

dhcp-relay admin-state {disable|enable}

Enable or disable the DHCP Realy's Admin State on this port. Default: enable.
Note: Make sure that "Active Protocol" is "Relay" for both ports involved in DHCP Relaying (the one connected to DHCP client and the one connected to DHCP server).

dhcp-relay operation {disable|enable}

Enable or disable the DHCP Relay's Option 82 on this port. Default: enable.

dhcp-relay hirschmann-device {disable|enable}

Enable this parameter if a Hirschmann DHCP client is connected to this port.
- It disables the forwarding of DHCP multicast requests that are received on this port.
- It will send its own DHCP multicast requests to be relayed by the DHCP relay; this will reduce the load in your network.

Disable this parameter if a Non-Hirschmann DHCP client is connected to this port (these devices send normal broadcast DHCP requests; this enables the relaying of DHCP broadcast requests that are received on this port).

dhcp-relay hirschmann-agent {disable|enable}

Enable or disable the forwarding of DHCP requests that are received on this port. Enable this parameter if a Hirschmann DHCP client is connected to this port. Default: disable.
Disable this parameter if a Non-Hirschmann DHCP client is connected to this port (these devices send normal broadcast DHCP requests; this enables the relaying of DHCP broadcast requests that

are received on this port)
Enable this parameter if a Hirschmann DHCP client is connected to this port (it will send its own DHCP multicast requests to be relayed by the DHCP relay; this will reduce the load in your network).

5.7.3 show dhcp-relay

Display the settings of the BOOTP/DHCP relay.

Format

```
show dhcp-relay [opt82 | port {<slot/port>|all} |
server-address]
```

Mode

Privileged EXEC and User EXEC

opt82

Show the DHCP Relay's Option 82 settings exclusively.

port

Display the DHCP Relay's port-related settings for the specified port exclusively.

<slot/port>

Show the DHCP Relay's port-related settings for the specified port exclusively.

all

Show the DHCP Relay's port-related settings for all ports.

server-address

Display the DHCP Relay's server address settings exclusively.
`ID:` The ID of the DHCP server `(1..16)`.
`Server IP:` The DHCP server's IP address (`a.b.c.d`).
`Interface:` The number of the interface (`<slot/port>` or `all`).
`Operation:` The operational status (`Enabled`, `Disabled`).

Port

Display the port number in `<slot/port>` notation.

Admin State

Display the DHCP Relay's admin state settings.
Possible values: `Disabled`, `Enabled`

Active Protocol

Display the DHCP Relay's active protocol settings.
Possible values: `Relay`, `Disabled`, `Server`, `Inaccessible`

Option 82

Display the DHCP Relay's option 82 settings.
Possible values: `Disabled`, `Enabled`

Hirschmann Device

Display the DHCP Relay's Hirschmann device settings.
Possible values: `Disabled`, `Enabled`

5.8 DHCP Server Commands

These commands configure the DHCP server parameters. The commands are divided by functionality into these different groups:

- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display switch settings, statistics and other information.
- Commands that start with the keyword ’no’ (so-called ’no commands’) clear some or all of the settings to factory defaults.

5.8.1 DHCP server configuration example

The example shown below has the following task: The IP address is only to be served, if a request is coming via interface 1/1 with specified Mac address.

```
<Hirschmann PowerMICE> >enable
<Hirschmann PowerMICE> #configure
<Hirschmann PowerMICE> <Config>#dhcp-server operation
enable
<Hirschmann PowerMICE> <Config>#dhcp-server pool add 1
static 192.168.0.10
<Hirschmann PowerMICE> <Config>#dhcp-server pool modify
1 mode interface 1/1
<Hirschmann PowerMICE> <Config>#dhcp-server pool modify
1 mode mac 00:80:63:12:34:56
<Hirschmann PowerMICE> <Config>#dhcp-server pool modify
1 option gateway 192.168.0.1
<Hirschmann PowerMICE> <Config>#dhcp-server pool enable
1
<Hirschmann PowerMICE> <Config>#interface 1/1
<Hirschmann PowerMICE> <interface 1/1>#dhcp-server oper-
ation enable
```

```
<Hirschmann PowerMICE> <config>#dhcp-server pool modify
1 option vendor-specific <f1 08 0a 7e 7e 02 0a 7f 7f 02>
```

This configuration leads to the following result:

```
<Hirschmann PowerMICE> #show dhcp-server pool 1

ID.............................. 1
Status.......................... Enabled
Start Address................... 192.168.0.10
End Address..................... 192.168.0.10
Leasetime....................... 86400
Hirschmann Device............... Disabled
Mode............................ Interface(1/1)
MAC............................. 00:80:63:12:34:56
Options:
Configpath.....................
Gateway......................... 192.168.0.1
Subnet Mask..................... 255.255.255.0
WINS............................ 0.0.0.0
DNS............................. 0.0.0.0
Hostname.......................
Vendor Specific Information..... "f1 08 0a 7e 7e 02 0a
7f 7f 02"
```

5.8.2 show dhcp-server

Display DHCP Server global and interface information.

Format

`show dhcp-server`

Mode

Privileged EXEC and User EXEC

DHCP Server

Display the DCHP server operation setting.
Possible values: `Enabled`, `Disabled`

DHCP Address Probe

Display the DCHP server address probe setting.
Possible values: `Enabled`, `Disabled`

DHCP, Port-Related Settings:

Port

Display the port number in <slot/port> notation.

Mode

Display the DCHP server interface information.
Possible values: `enable`, `disable`

DHCP, Pools:

Display the DCHP server pool related information.

5.8.3 show dhcp-server operation

Display DHCP Server global information.

Format

```
show dhcp-server operation
```

Mode

Privileged EXEC and User EXEC

DHCP Server

Display the DCHP server operation setting.
Possible values: `Enabled`, `Disabled`

DHCP Address Probe

Display the DCHP server address probe setting.
Possible values: `Enabled`, `Disabled`

5.8.4 show dhcp-server port

Display the DCHP port-related settings for all ports or specific port only.

Format

```
show dhcp-server port {all | <slot/port>}
```

Mode

Privileged EXEC and User EXEC

show dhcp-server port all

Display the DCHP port-related settings for all ports.

show dhcp-server port <slot/port>

Display the DCHP port-related settings for the specified port only.

5.8.5 show dhcp-server pool

Display DHCP server pool information for all pool or detailed information for a specific pool.

Format

```
show dhcp-server pool {all | <id>}
```

Mode

Privileged EXEC and User EXEC

show dhcp-server pool all

Display the DCHP server pool information for all IDs.

show dhcp-server pool <id>

Display the DCHP server pool information for the specified ID only.

5.8.6 dhcp-server addr-probe

Use this command tio enable or disable the probing of allocated addresses with an ICMP Echo request.

Format

```
dhcp-server addr-probe {disable|enable}
```

Mode

```
Global Config
```

dhcp-server addr-probe enable

Enable the DHCP server address probe. This is the default.
The DHCP server will send ICMP echo request before offering an IP.

dhcp-server addr-probe disable

Disable the DHCP server address probe.
The DHCP server will offer an IP without checking if already in use.

5.8.7 dhcp-server operation

Enable or disable the DHCP server globally. Default: disable.

Format

```
dhcp-server operation {disable|enable}
```

Mode

```
Interface Config
```

dhcp-server operation disable

Disable the DHCP server. This is the default.

dhcp-server operation enable

Enable the DHCP server.

5.8.8 dhcp-server pool add <id>

Add a pool with a single IP address (static) or with an IP range (dynamic)

Format

```
dhcp-server pool {add <id> {static <ipaddr>
                |dynamic <start ipaddr> <end ipaddr>}
```

Mode

```
Global Config
```

dhcp-server pool add <id> {static <ipaddr>}

Add a pool with a single IP address (static).

dhcp-server pool add <id> {dynamic <start ipaddr> <end ipaddr>}

Add a pool with an IP range (dynamic).

5.8.9 dhcp-server pool modify <id> mode

Add or delete one or more pool modes.

Format

```
dhcp-server pool modify <id> mode
            {interface {all | <slot/port>} 1)
            |mac {none | <macaddr>} 1)
            |clientid {none | <clientid>} 1)
            |relay {none | <ipaddr>}
            |remoteid {none | <remoteid>} 1)
            |circuitid {none | < circuitid >} 1)}
```

Mode

Global Config

dhcp-server pool modify <id> mode interface all 1)

Set pool to all interfaces.

dhcp-server pool modify <id> mode interface <slot/port> 1)

Set pool to a specific interface.

dhcp-server pool modify <id> mode mac none 1)

Use none to remove the mode.

dhcp-server pool modify <id> mode mac <macaddr> 1)

Enter macaddr in xx:xx:xx:xx:xx:xx format.

dhcp-server pool modify <id> mode clientid none 1)

Use none to remove the mode.

dhcp-server pool modify <id> mode clientid <clientid> 1)

Enter clientid in xx:xx:...:xx format.

dhcp-server pool modify <id> mode relay none

Use none to remove the mode.

dhcp-server pool modify <id> mode relay <ipaddr>

Enter IP address of the relay.

dhcp-server pool modify <id> mode remoteid none 1)

Use none to remove the mode.

dhcp-server pool modify <id> mode remoteid <remoteid> [1)]

Enter remoteid in xx:xx:...:xx format.

dhcp-server pool modify <id> mode circuitid none [1)]

Use none to remove the mode.

dhcp-server pool modify <id> mode circuitid <circuitid> [1)]

Enter circuitid in xx:xx:...:xx format.

[1)] Available for pools with single IP address only.

5.8.10 dhcp-server pool modify <id> option

Modify pool options.

Format

```
dhcp-server pool modify <id> option
       {configpath <url> |
        gateway <ipaddr> |
        netmask <netmask> |
        wins <ipaddr> |
        dns <ipaddr> |
        hostname <name>}
        vendor-specific <string>}
```

Mode

Global Config

dhcp-server pool modify <id> option configpath <url>

Option configpath. Enter the configpath URL in 'tftp://<servername-or-ip>/<file>' format.

dhcp-server pool modify <id> option gateway <ipaddr>

Option default gateway. Enter the gateway IP address.

dhcp-server pool modify <id> option netmask <netmask>

Option netmask. Enter the netmask.

dhcp-server pool modify <id> option wins <ipaddr>

Option wins. Enter WINS IP address.

dhcp-server pool modify <id> option dns <ipaddr>

Option DNS. Enter the DNS IP address.

dhcp-server pool modify <id> option hostname <name>

Option hostname. Enter the host name.

dhcp-server pool modify <id> option vendor-specific <string>

Option vendor-specific information. Enter vendor specific information as hex in `xx:xx:...:xx` format..

5.8.11 dhcp-server pool modify leasetime

Modify pool leasetime. Enter the leasetime in seconds.

Format

```
dhcp-server pool modify leasetime <seconds>
```

Mode

```
Global Config
```

5.8.12 dhcp-server pool modify <id> hirschmann-device

Set this pool to Hirschmann devices only or to all devices.

Format

```
dhcp-server pool modify <id> hirschmann-device
{enable|disable}
```

Mode

```
Global Config
```

dhcp-server pool modify <id> hirschmann-device disable

Use pool for all devices.

dhcp-server pool modify <id> hirschmann-device enable

Use pool for Hirschmann devices only.

5.8.13 dhcp-server pool enable

Enable a specific pool.

Format

```
dhcp-server pool enable <id>
```

Mode

```
Global Config
```

5.8.14 dhcp-server pool disable

Disable a specific pool.

Format

```
dhcp-server pool disable <id>
```

Mode

```
Global Config
```

5.8.15 dhcp-server pool delete

Delete a specific pool.

Format

```
dhcp-server pool delete <id>
```

Mode

```
Global Config
```

5.9 Sub-Ring Commands

These commands configure the sub-ring parameters.
The commands are divided by functionality into these different groups:

- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display switch settings, statistics and other information.

5.9.1 show sub-ring

Display sub-ring information for all sub-rings or detailed information for a specific sub-ring.

Format

```
show sub-ring {all-ids | <id>}
  {id | info | mode | operation | protocol | port |
  summary | ring-name | vlan | mrp-domainID |
  partner-mac}
```

Mode

Privileged EXEC and User EXEC

show sub-ring

Display the sub-ring information.

show sub-ring all-ids

Display the sub-ring information for all existing Sub-Ring IDs.

show sub-ring <id>

Display the sub-ring information for the specified ID.

id

Display the given Sub-Ring's ID.

info

Display status information for the given Sub-Ring ID.

mode

Display the switch's mode for the given Sub-Ring ID.

operation

Display the switch's operative setting for the given Sub-Ring ID.
Note: In case of configuration problems, this value may differ from the administrative setting (may become 'Disabled').

protocol

Display the switch's protocol setting for the given Sub-Ring ID.

port

Display the ports for the given Sub-Ring ID.

summary

Display a summary for the given Sub-Ring ID.

ring-name

Display ring name for the given Sub-Ring ID.

vlan

Display the VLAN ID for the given Sub-Ring ID.

mrp-domainID

Display the MRP domain ID for the given Sub-Ring ID.

partner-mac

Display the partner MAC for the given Sub-Ring ID.

5.9.2 sub-ring <id> mode

Configure the switch's Sub-Ring mode for the given ID (manager or redundant-manager).

Format

```
sub-ring <id> mode {manager |
                    redundant-manager |
                    single-manager}
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

manager

Switch is manager for the given Sub-Ring ID.

redundant-manager

Switch is redundant-manager for the given Sub-Ring ID.

single-manager

Switch is single-manager for the given Sub-Ring ID.

5.9.3 sub-ring <id> operation

Enable or disable the switch for the given Sub-Ring ID.

Format

```
sub-ring <id> operation {enable|disable}
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

enable

Enable the switch for the given Sub-Ring ID.

disable

Disable the switch for the given Sub-Ring ID.

5.9.4 sub-ring <id> protocol

Set MRP or FHR as sub-ring protocol for the given Sub-Ring ID.

Format

```
sub-ring <id> protocol standard_mrp
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

standard_mrp

Set MRP as sub-ring protocol for the given Sub-Ring ID.

5.9.5 sub-ring <id> port

Specify the switch's ports for the given Sub-Ring ID.

Format

```
sub-ring <id> port <slot/port>
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

<slot/port>

Specify the port (in slot/port notation).

5.9.6 sub-ring <id> ring-name

Set a ring name for the given Sub-Ring ID.

Format

```
sub-ring <id> ring-name <ring-name>
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

<ring-name>

Enter a name for the given Sub-Ring ID. The name may be up to 254 characters long and contain only printable characters. If you do not give a name, the current name will be set to an empty string ("").

5.9.7 sub-ring <id> vlan

Specify the VLAN for the given Sub-Ring ID.

Format

```
sub-ring <id> vlan <0-4042>
```

Mode

```
Global Config
```

<id>

Specify the Sub-Ring ID whose settings you want to configure.

<0-4042>

Enter the VLAN for the given Sub-Ring ID
(min.: 0, max.: 4042, default: 0).

5.9.8 sub-ring <id> mrp-domainID

Set an MRP domain ID for the given Sub-Ring ID.

Format

```
sub-ring <id> mrp-domainID {<id> |
                            default-domainID}
```

Mode

```
Global Config
```

<id>

sub-ring <id>: Specify the Sub-Ring ID whose settings you want to configure.

<id>

Enter an MRP domainID for the given Sub-Ring ID.
The ID has to be 16 bytes long and contain only printable characters.

default-domainID

Enter the default MRP domainID for the given Sub-Ring ID.
The MRP domainID will be set to 255.255.255.255.255.255 255.255.255.255.255.255.255.255.255.255

5.9.9 sub-ring delete-ring

Delete all existing Sub-Rings IDs or a specific Sub-Ring ID.

Format

```
sub-ring delete-ring {all-ids | <id>}
```

Mode

```
Global Config
```

all-ids

Delete all existing Sub-Ring IDs.

<id>

Delete the given Sub-Ring ID. Format: a number in the range 1-2147483647 (2^{31} - 1). An ID of 0 is invalid.

5.9.10 sub-ring new-ring

Create a new Sub-Ring ID. The configuration will consist of default parameters and its operation will be disabled.

Format

```
sub-ring new-ring <id>
```

Mode

```
Global Config
```

<id>

Enter a new Sub-Ring ID. Format: a number in the range 1-2147483647 (2^{31} - 1). An ID of 0 is invalid.

6 CLI Commands: Security

This chapter provides a detailed explanation of the Security commands. The following Security CLI commands are available in the software Switching Package. Use the security commands to configure security settings for login users and port users.

The commands are divided into these different groups:

- Show commands are used to display device settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

6.1 Security Commands

6.1.1 authentication login

This command creates an authentication login list. The `<listname>` is up to 15 alphanumeric characters and is not case sensitive. Up to 10 authentication login lists can be configured on the switch. When a list is created, the authentication method “local” is set as the first method.
When the optional parameters “Option1”, “Option2” and/or “Option3” are used, an ordered list of methods are set in the authentication login list. If the authentication login list does not exist, a new authentication login list is first created and then the authentication methods are set in the authentication login list. The maximum number of authentication login methods is three. The possible method values are `local, radius` and `reject`.
The value of `local` indicates that the user’s locally stored ID and password are used for authentication. The value of `radius` indicates that the user’s ID and password will be authenticated using the RADIUS server. The value of `reject` indicates the user is never authenticated.
To authenticate a user, the authentication methods in the user’s login will be attempted in order until an authentication attempt succeeds or fails.

Note: The default login list included with the default configuration can not be changed.

Note: When assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable.

Format

```
authentication login <listname> [method1 [method2
[method3]]]
```

Mode

```
Global Config
```

no authentication login

This command deletes the specified authentication login list.
You will be unable to delete if any of the following conditions are true:

- The login list name is invalid or does not match an existing authentication login list
- The specified authentication login list is assigned to any user or to the non configured user for any component
- The login list is the default login list included with the default configuration and was not created using ‘authentication login’. The default login list cannot be deleted.

Format

```
no authentication login <listname>
```

Mode

```
Global Config
```

6.1.2 authorization network radius

Use this command to enable the switch to accept VLAN assignment by the RADIUS server.

Format

```
authorization network radius
```

Mode

```
Privileged EXEC
```

no authorization network radius

Use this command to disable the switch to accept VLAN assignment by the RADIUS server.

Format

```
no authorization network radius
```

Mode

```
Global Config
```

6.1.3 clear dot1x statistics

This command resets the 802.1X statistics for the specified port or for all ports.

Format

```
clear dot1x statistics {<slot/port> | all}
```

Mode

```
Privileged EXEC
```

6.1.4 clear radius statistics

This command is used to clear all RADIUS statistics.

Format

```
clear radius statistics
```

Mode

```
Privileged EXEC
```

6.1.5 dot1x defaultlogin

This command assigns the authentication login list to use for non-configured users for 802.1X port security. This setting is over-ridden by the authentication login list assigned to a specific user if the user is configured locally. If this value is not configured, users will be authenticated using local authentication only.

Format

```
dot1x defaultlogin <listname>
```

Mode

```
Global Config
```

6.1.6 dot1x dynamic-vlan enable

Use this command to enable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default

```
disabled
```

Format

```
dot1x dynamic-vlan enable
```

Mode

```
Global Config
```

no dot1x dynamic-vlan enable

Use this command to disable the switch to create VLANs dynamically when a RADIUS-assigned VLAN does not exist in the switch.

Default

```
disabled
```

Format

```
no dot1x dynamic-vlan enable
```

Mode

```
Global Config
```

6.1.7 dot1x guest-vlan

This command configures VLAN as guest vlan on an interface. The command specifies an active VLAN as an IEEE 802.1x guest VLAN. The range is 1 to the maximum VLAN ID supported by the platform.

Format

```
dot1x guest-vlan <vlan-id>
```

Mode

```
Interface Config
```

<vlan-id>

Enter an existing VLAN ID.

no dot1x guest-vlan

This command is used to disable Guest VLAN for the port.

Format

```
no dot1x guest-vlan
```

Mode

```
Global Config
```

6.1.8 dot1x initialize

This command begins the initialization sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format

```
dot1x initialize <slot/port>
```

Mode

```
Privileged EXEC
```

6.1.9 dot1x login

This command assigns the specified authentication login list to the specified user for 802.1X port security. The <user> parameter must be a configured user and the <list-name> parameter must be a configured authentication login list.

Format

```
dot1x login <user> <listname>
```

Mode

```
Global Config
```

6.1.10 dot1x mac-auth-bypass

This command enables the MAC-authorized-bypass on that interface.

Default

```
disabled
```

Format

```
dot1x mac-auth-bypass
```

Mode

```
Interface Config
```

no dot1x mac-auth-bypass

This command disables the MAC-authorized-bypass on that interface.

Default

```
disabled
```

Format

```
no dot1x mac-auth-bypass
```

Mode

```
Interface Config
```

6.1.11 dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant. The <count> value must be in the range 1 - 10.

Default

```
2
```

Format

```
dot1x max-req <count>
```

Mode

```
Interface Config
```

no dot1x max-req

This command sets the maximum number of times the authenticator state machine on this port will transmit an EAPOL EAP Request/Identity frame before timing out the supplicant.

Format

```
no dot1x max-req
```

Mode

```
Interface Config
```

6.1.12 dot1x max-users

Use this command to set the maximum number of clients supported on an interface when MAC-based 802.1X authentication is enabled on the port. The count value is in the range 1-16 and the default value is 16.

Default

```
16
```

Format

```
dot1x max-users <count>
```

Mode

```
Interface Config
```

no dot1x max-users

The ‘no’ form of this command resets the maximum number of clients allowed to its default value of 16.

Format

```
no dot1x max-users
```

Mode

```
Interface Config
```

6.1.13 dot1x port-control

This command sets the authentication mode to be used on the specified port. The control mode may be one of the following.

- `force-unauthorized`: The authenticator PAE unconditionally sets the controlled port to unauthorized. Thus the port is always blocked.
- `force-authorized`: The authenticator PAE unconditionally sets the controlled port to authorized. Thus the port is always opened.
- `auto`: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. The port mode is controlled by the protocol.
- `mac-based`: Enable MAC-based 802.1X authentication on the port.

Default

```
force-authorized
```

Format

```
dot1x port-control {force-unauthorized | force-
authorized | auto | mac-based}
```

Mode

```
Interface Config
```

no dot1x port-control
This command sets the port-control mode for the specified port to the default mode (force-authorized).

Format

```
no dot1x port-control
```

Mode

```
Interface Config
```

6.1.14 dot1x port-control all

This command sets the authentication mode to be used on all ports. The control mode may be one of the following.

- `force-unauthorized`: The authenticator PAE unconditionally sets the controlled port to unauthorized. Thus the ports are always blocked.
- `force-authorized`: The authenticator PAE unconditionally sets the controlled port to authorized. Thus the ports are always opened.
- `auto`: The authenticator PAE sets the controlled port mode to reflect the outcome of the authentication exchanges between the supplicant, authenticator and the authentication server. The port mode is controlled by the protocol.
- `mac-based`: Enable the MAC-based 802.1X authentication on the port.

Default

```
force-authorized
```

Format

```
dot1x port-control all {force-unauthorized | force-
authorized | auto |mac-based}
```

Mode

```
Global Config
```

no dot1x port-control all
This command sets the port-control mode for all the ports to the default mode (force-authorized).

Format

```
no dot1x port-control all
```

Mode

```
Global Config
```

6.1.15 dot1x re-authenticate

This command begins the re-authentication sequence on the specified port. This command is only valid if the control mode for the specified port is 'auto'. If the control mode is not 'auto' an error will be returned.

Format

```
dot1x re-authenticate <slot/port>
```

Mode

```
Privileged EXEC
```

6.1.16 dot1x re-authentication

This command enables re-authentication of the supplicant for the specified port.

Default

```
disabled
```

Format

```
dot1x re-authentication
```

Mode

```
Interface Config
```

no dot1x re-authentication
This command disables re-authentication of the supplicant for the specified port.

Format

```
no dot1x re-authentication
```

Mode

```
Interface Config
```

6.1.17 dot1x safe-vlan

Use this command to enable the safe-vlan assignment on the switch.

Note: This command is available for the RS20/RS30/RS40, RSB20, MS20/MS30, RSR20/RSR30, MACH100, MACH1000, PowerMICE, MACH4000, OCTOPUS devices.

Default

```
disabled
```

Format

```
dot1x safe-vlan
```

Mode

```
Global Config
```

no dot1x safe-vlan

Use this command to disable the safe-vlan assignment on the switch.

Default

```
disabled
```

Format

```
no dot1x safe-vlan
```

Mode

```
Global Config
```

6.1.18 dot1x system-auth-control

This command is used to enable the dot1x authentication support on the switch. By default, the authentication support is disabled. While disabled, the dot1x configuration is retained and can be changed, but is not activated.

Default

```
disabled
```

Format

```
dot1x system-auth-control
```

Mode

```
Global Config
```

no dot1x system-auth-control

This command is used to disable the dot1x authentication support on the switch.

Format

```
no dot1x system-auth-control
```

Mode

```
Global Config
```

6.1.19 dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port. Depending on the token used and the value (in seconds) passed, various timeout configurable parameters are set. The following tokens are supported.

- reauth-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when re-authentication of the supplicant takes place. The reauth-period must be a value in the range 1 - 65535.

- quiet-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The quiet-period must be a value in the range 0 - 65535.
- tx-period: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The quiet-period must be a value in the range 1 - 65535.
- supp-timeout: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the supplicant. The supp-timeout must be a value in the range 1 - 65535.
- server-timeout: Sets the value, in seconds, of the timer used by the authenticator state machine on this port to timeout the authentication server. The supp-timeout must be a value in the range 1 - 65535.

Defaults

```
reauth-period: 3600 seconds
quiet-period: 60 seconds
tx-period: 30 seconds
supp-timeout: 30 seconds
server-timeout: 30 seconds
```

Format

```
dot1x timeout {{reauth-period <seconds>} | {quiet-
period <seconds>} | {tx-period <seconds>} | {supp-
timeout <seconds>} | {server-timeout <seconds>}}
```

Mode

```
Interface Config
```

no dot1x timeout

This command sets the value, in seconds, of the timer used by the authenticator state machine on this port to the default values. Depending on the token used, the corresponding default values are set.

Format

```
no dot1x timeout {reauth-period | quiet-period |
tx-period | supp-timeout | server-timeout}
```

Mode

```
Interface Config
```

6.1.20 dot1x timeout guest-vlan-period

Use this command to configure the timeout value for the guest-vlan-period. The time, in seconds, for which the authenticator waits to see if any EAPOL packets are received on a port before authorizing the port and placing the port in the guest vlan (if configured). The guest vlan timer is only relevant when guest vlan has been configured on that specific port.
Default guest-vlan-period: 90 seconds.

Default

```
90
```

Format

```
dot1x timeout guest-vlan-period <seconds>
```

Mode

```
Interface Config
```

<seconds>

Enter an integer in the range of 1-300.

no dot1x timeout guest-vlan-period

The ‘no’ form of this command resets the timeout value for the guest-vlan-period to its default value (90 seconds).

Format

```
no dot1x timeout guest-vlan-period
```

Mode

```
Interface Config
```

6.1.21 dot1x unauthenticated-vlan

Use this command to configure the unauthenticated VLAN associated with the specified interface. The unauthenticated VLAN ID can be a valid VLAN ID from 0 to maximum supported VLAN ID. The unauthenticated VLAN must be statically configured in the VLAN database to be operational. By default, the unauthenticated VLAN is 0, i.e. invalid and not operational.

Default

```
0
```

Format

```
dot1x unauthenticated-vlan <vlan-id>
```

Mode

```
Interface Config
```

<vlan-id>

Enter an existing VLAN ID.

no dot1x unauthenticated-vlan

The ‘no’ form of this command resets the value for the unauthenticated VLAN to its default value.

Format

```
no dot1x unauthenticated-vlan
```

Mode

```
Interface Config
```

6.1.22 dot1x user

This command adds the specified user to the list of users with access to the specified port or all ports. The <user> parameter must be a configured user.

Format

```
dot1x user <user> {<slot/port> | all}
```

Mode

```
Global Config
```

no dot1x user
This command removes the user from the list of users with access to the specified port or all ports.

Format

```
no dot1x user <user> {<slot/port> | all}
```

Mode

```
Global Config
```

6.1.23 ip ssh protocol

Use this command to configure the IP secure shell (SSH) parameters, the first and the optional second SSH protocol level).
Possible settings: v1, v2 or v1 & v2.

Format

```
ip ssh [protocol <protocollevel1>
                 [<protocollevel2>]]
```

Default

```
2 1
```

Mode

```
Privileged Exec
```

<protocollevel1>

Enter the first SSH Protocol Level (Version).
Possible values: `1`, `2`

<protocollevel2>

Optionally enter the second SSH Protocol Level (Version).
Possible values: `1`, `2`

no ip ssh
This command sets IP secure shell (SSH) parameters to default value.

Format

```
no ip ssh
```

Mode

```
Privileged Exec
```

6.1.24 radius accounting mode

This command is used to enable the RADIUS accounting function.

Default

```
disabled
```

Format

```
radius accounting mode
```

Mode

```
Global Config
```

no radius accounting mode
This command is used to set the RADIUS accounting function to the default value - i.e. the RADIUS accounting function is disabled.

Format

```
no radius accounting mode
```

Mode

```
Global Config
```

6.1.25 radius server host

This command is used to configure the RADIUS authentication and accounting server.

If the 'auth' token is used, the command configures the IP address to use to connect to a RADIUS authentication server. Up to 3 servers can be configured per RADIUS client. If the maximum number of configured servers is reached, the command will fail until one of the servers is removed by executing the no form of the command. If the optional <port> parameter is

used, the command will configure the UDP port number to use to connect to the configured RADIUS server. In order to configure the UDP port number, the IP address must match that of a previously configured RADIUS authentication server. The port number must lie between 1 - 65535, with 1812 being the default value.
If the 'acct' token is used, the command configures the IP address to use for the RADIUS accounting server. Only a single accounting server can be configured. If an accounting server is currently configured, it must be removed from the configuration using the no form of the command before this command succeeds. If the optional <port> parameter is used, the command will configure the UDP port to use to connect to the RADIUS accounting server. The IP address specified must match that of a previously configured accounting server. If a port is already configured for the accounting server then the new port will replace the previously configured value. The port must be a value in the range 1 - 65535, with 1813 being the default value.

Format

```
radius server host {auth | acct} <ipaddr> [<port>]
```

Mode

```
Global Config
```

no radius server host

This command is used to remove the configured RADIUS authentication server or the RADIUS accounting server. If the 'auth' token is used, the previously configured RADIUS authentication server is removed from the configuration. Similarly, if the 'acct' token is used, the previously configured RADIUS accounting server is removed from the configuration. The <ipaddr> parameter must match the IP address of the previously configured RADIUS authentication / accounting server.

Format

```
no radius server host {auth | acct} <ipaddress>
```

Mode

```
Global Config
```

6.1.26 radius server key

This command is used to configure the shared secret between the RADIUS client and the RADIUS accounting / authentication server. Depending on whether the 'auth' or 'acct' token is used, the shared secret will be configured for the RADIUS authentication or RADIUS accounting server. The IP address provided must match a previously configured server. When this command is executed, the secret will be prompted. The secret must be an alphanumeric value not exceeding 20 characters.

Format

```
radius server key {auth | acct} <ipaddr>
```

Mode

```
Global Config
```

6.1.27 radius server msgauth

This command enables the message authenticator attribute for a specified server.

Default

```
radius server msgauth <ipaddr>
```

Mode

```
Global Config
```

6.1.28 radius server primary

This command is used to configure the primary RADIUS authentication server for this RADIUS client. The primary server is the one that is used by default for handling RADIUS requests. The remaining configured servers are only used if the primary server cannot be reached. A maximum of three servers can be configured on each client. Only one of these servers can be configured as the primary. If a primary server is already configured prior to this command being executed, the server specified by the IP address used in this command will become the new primary server. The IP address must match that of a previously configured RADIUS authentication server.

Format

```
radius server primary <ipaddr>
```

Mode

```
Global Config
```

6.1.29 radius server retransmit

This command sets the maximum number of times a request packet is retransmitted when no response is received from the RADIUS server. The retries value is an integer in the range of 1 to 15.

Default

```
4
```

Format

```
radius server retransmit <retries>
```

Mode

```
Global Config
```

no radius server retransmit
This command sets the maximum number of times a request packet is re-transmitted, when no response is received from the RADIUS server, to the default value, i.e. 10.

Format

```
no radius server retransmit
```

Mode

```
Global Config
```

6.1.30 radius server timeout

This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received. The timeout value is an integer in the range of 1 to 30.

Default

```
6
```

Format

```
radius server timeout <seconds>
```

Mode

```
Global Config
```

no radius server timeout
This command sets the timeout value (in seconds) after which a request must be retransmitted to the RADIUS server if no response is received, to the default value, i.e. 6.

Format

```
no radius server timeout
```

Mode

```
Global Config
```

6.1.31 show radius accounting

This command is used to display the configured RADIUS accounting mode, accounting server and the statistics for the configured accounting server.

Format

```
show radius accounting [statistics <ipaddr>]
```

Mode

```
Privileged EXEC and User EXEC
```

If the optional token 'statistics <ipaddr>' is not included, then only the accounting mode and the RADIUS accounting server details are displayed.

Mode

Enabled or disabled

IP Address

The configured IP address of the RADIUS accounting server

Port

The port in use by the RADIUS accounting server

Secret Configured

Yes or No

If the optional token 'statistics <ipaddr>' is included, the statistics for the configured RADIUS accounting server are displayed. The IP address parameter must match that of a previously configured RADIUS accounting server. The following information regarding the statistics of the RADIUS accounting server is displayed.

Accounting Server IP Address

IP Address of the configured RADIUS accounting server

Round Trip Time

The time interval, in hundredths of a second, between the most recent Accounting-Response and the Accounting-Request that matched it from the RADIUS accounting server.

Requests

The number of RADIUS Accounting-Request packets sent to this accounting server. This number does not include retransmissions.

Retransmission

The number of RADIUS Accounting-Request packets retransmitted to this RADIUS accounting server.

Responses

The number of RADIUS packets received on the accounting port from this server.

Malformed Responses

The number of malformed RADIUS Accounting-Response packets received from this server. Malformed packets include packets with an

invalid length. Bad authenticators and unknown types are not included as malformed accounting responses.

Bad Authenticators

The number of RADIUS Accounting-Response packets containing invalid authenticators received from this accounting server.

Pending Requests

The number of RADIUS Accounting-Request packets sent to this server that have not yet timed out or received a response.

Timeouts

The number of accounting timeouts to this server.

Unknown Types

The number of RADIUS packets of unknown types, which were received from this server on the accounting port.

Packets Dropped

The number of RADIUS packets received from this server on the accounting port and dropped for some other reason.

6.1.32 show authentication

This command displays the ordered authentication methods for all authentication login lists.

Format

```
show authentication
```

Mode

```
Privileged EXEC and User EXEC
```

Authentication Login List

This displays the authentication login listname.

Method 1

This displays the first method in the specified authentication login list, if any.

Method 2

This displays the second method in the specified authentication login list, if any.

Method 3

This displays the third method in the specified authentication login list, if any.

6.1.33 show authentication users

This command displays information about the users assigned to the specified authentication login list. If the login is assigned to non-configured users, the user “default” will appear in the user column.

Format

```
show authentication users <listname>
```

Mode

```
Privileged EXEC and User EXEC
```

User

This field displays the user assigned to the specified authentication login list.

Component

This field displays the component (User or 802.1X) for which the authentication login list is assigned.

6.1.34 show dot1x

This command is used to show a summary of the global dot1x configuration, summary information of the dot1x configuration for a specified port or all ports, the detailed dot1x configuration for a specified port and the dot1x statistics for a specified port - depending on the tokens used.

Format

```
show dot1x [{summary {<slot/port> | all} | {detail
<slot/port>} | {statistics <slot/port>}]
```

Mode

```
Privileged EXEC and User EXEC
```

If none of the optional parameters are used, the global dot1x configuration summary is displayed.

Administrative mode

Indicates whether authentication control on the switch is enabled or disabled.

VLAN Assignment Mode

Indicates whether the VLAN Assignment Mode is enabled or disabled.

Dynamic VLAN Creation Mode

Indicates whether the Dynamic VLAN Creation Mode is enabled or disabled.

Safe VLAN Mode

Indicates whether the Safe VLAN Mode is enabled or disabled.

If the optional parameter 'summary {<slot/port> | all}' is used, the dot1x configuration for the specified port or all ports are displayed.

Port

The interface whose configuration is displayed.

Control Mode

The configured control mode for this port. Possible values are `force-unauthorized | force-authorized | auto | mac-based`

Operating Control Mode

The control mode under which this port is operating. Possible values are `authorized | unauthorized`

Reauthentication Enabled

Indicates whether re-authentication is enabled on this port

Key Transmission Enabled

Indicates if the key is transmitted to the supplicant for the specified port

If the optional parameter 'detail <slot/port>' is used, the detailed dot1x configuration for the specified port are displayed.

Port

The interface whose configuration is displayed

Protocol Version

The protocol version associated with this port. The only possible value is 1, corresponding to the first version of the dot1x specification.

PAE Capabilities

The port access entity (PAE) functionality of this port.
Possible values: `Authenticator, Supplicant`.

Control Mode

Display the state of the Control Mode.
Possible values: `auto, forceauthorized`, ...

Authenticator PAE State

Current state of the authenticator PAE state machine.
Possible values: `Initialize, Disconnected, Connecting, Authenticating, Authenticated, Aborting, Held, ForceAuthorized, and ForceUnauthorized`.

Backend Authentication State

Current state of the backend authentication state machine.
Possible values: `Request, Response, Success, Fail, Time-out, Idle, Initialize`.

Quiet Period

The timer used by the authenticator state machine on this port to define periods of time in which it will not attempt to acquire a supplicant. The value is expressed in seconds and will be in the range `0..65535`.

Transmit Period

The timer used by the authenticator state machine on the specified port to determine when to send an EAPOL EAP Request/Identity frame to the supplicant. The value is expressed in seconds and will be in the range of `1..65535`.

Guest VLAN ID

Display the Guest VLAN ID.
Default value: `0`.

Guest VLAN Period (secs)

Display the Guest VLAN Period.
Default value: `90` seconds.

Supplicant Timeout

The timer used by the authenticator state machine on this port to timeout the supplicant. The value is expressed in seconds and will be in the range of `1..65535`.

Server Timeout

The timer used by the authenticator on this port to timeout the authentication server. The value is expressed in seconds and will be in the range of `1..65535`.

Maximum Requests

The maximum number of times the authenticator state machine on this port will retransmit an EAPOL EAP Request/Identity before timing out the supplicant. The value will be in the range of `1..10`.

VLAN Id

Display the VLAN Id.

VLAN Assigned Reason

Display the state of the VLAN Assigned Reason parameter.
Possible values: `RADIUS, Not Assigned`.

Reauthentication Period

The timer used by the authenticator state machine on this port to determine when reauthentication of the supplicant takes place. The value is expressed in seconds and will be in the range of `1..65535`.

Reauthentication Enabled

Indicates if reauthentication is enabled on this port.
Possible values: `True, False`

Key Transmission Enabled

Indicates if the key is transmitted to the supplicant for the specified port.
Possible values: `True, False`.

Control Direction

Indicates the control direction for the specified port or ports.
Possible values: `both, in`.

Maximum Users

Display the value of Maximum Users.

Unauthenticated VLAN ID

Display the value of Unauthenticated VLAN ID

Session Timeout

Display the value of Session Timeout

Session Termination Action

Display the value of Session Termination Action

MAC-Authorized-Bypass

Display the value of MAC-Authorized-Bypass

If the optional parameter 'statistics **<**slot/port**>**' is used, the dot1x statistics for the specified port are displayed.

Port

The interface whose statistics are displayed.

EAPOL Frames Received

The number of valid EAPOL frames of any type that have been received by this authenticator.

EAPOL Frames Transmitted

The number of EAPOL frames of any type that have been transmitted by this authenticator.

EAPOL Start Frames Received

The number of EAPOL start frames that have been received by this authenticator.

EAPOL Logoff Frames Received

The number of EAPOL logoff frames that have been received by this authenticator.

Last EAPOL Frame Version

The protocol version number carried in the most recently received EAPOL frame.

Last EAPOL Frame Source

The source MAC address carried in the most recently received EAPOL frame.

EAP Response/Id Frames Received

The number of EAP response/identity frames that have been received by this authenticator.

EAP Response Frames Received

The number of valid EAP response frames (other than resp/id frames) that have been received by this authenticator.

EAP Request/Id Frames Transmitted

The number of EAP request/identity frames that have been transmitted by this authenticator.

EAP Request Frames Transmitted

The number of EAP request frames (other than request/identity frames) that have been transmitted by this authenticator.

Invalid EAPOL Frames Received

The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

EAP Length Error Frames Received

The number of EAPOL frames that have been received by this authenticator in which the frame type is not recognized.

6.1.35 show dot1x users

This command displays 802.1X port security user information for locally configured users.

Format

```
show dot1x users <slot/port>
```

Mode

```
Privileged EXEC and User EXEC
```

User

Users configured locally to have access to the specified port.

6.1.36 show dot1x clients

This command displays 802.1X port security client information for locally configured clients.

Format

```
show dot1x clients <slot/port>
```

Mode

```
Privileged EXEC
```

Logical Interface

Display the Logical Interface.

Interface

Display the Interface.

User Name

Display the User Name.

Supp MAC Address

Display the Supp MAC Address.

Session Time

Display the Session Time.

Vlan Id

Display the Vlan Id.

Vlan Assigned Reason

Display the Vlan Assigned Reason.
Possible values: RADIUS, ...

Session Timeout

Display the Session Timeout.

Session Termination Action

Display the Session Termination Action.
Possible values: Reauthenticate, ...

6.1.37 show ip ssh

This command displays the IP secure shell (SSH) information.

Format

`show ip ssh`

Mode

`Privileged EXEC`

Administrative Mode

Display the SSH administrative mode setting.
Possible values: `Disabled`, `Enabled`.

Protocol Levels

Display the SSH protocol levels setting.
Possible values: `Versions 1 and 2`, `Version 1`, `Version 2`
(default setting: `Versions 1 and 2`).

SSH Sessions Currently Active

Display the number of SSH sessions being currently set up.
Possible values: `1..5`.

Max SSH Sessions Allowed

Display the max. number of SSH sessions that can be set up simultaneously.
Possible values: `1..5` (default setting: `5`).

SSH Timeout

Display the SSH timeout in minutes.
Possible values: `1..160` (default setting: `5`).

6.1.38 show radius

This command is used to display the various RADIUS configuration items for the switch as well as the configured RADIUS servers. If the optional token 'servers' is not included, the following RADIUS configuration items will be displayed.

Format

`show radius [servers]`

Mode

`Privileged EXEC and User EXEC`

Primary Server IP Address

Indicates the configured server currently in use for authentication

Number of configured servers

The configured IP address of the authentication server

Max number of retransmits

The configured value of the maximum number of times a request packet is retransmitted

Timeout Duration

The configured timeout value, in seconds, for request re-transmissions

Accounting Mode

Yes or No

If the optional token 'servers' is included, the following information regarding the configured RADIUS servers is displayed.

IP Address

IP Address of the configured RADIUS server

Port

The port in use by this server

Type

Primary or secondary

Secret Configured

Yes / No

6.1.39 show radius statistics

This command is used to display the statistics for RADIUS or configured server . To show the configured RADIUS server statistic, the IP Address specified must match that of a previously configured RADIUS server. On execution, the following fields are displayed.

Format

```
show radius statistics [ipaddr]
```

Mode

```
Privileged EXEC and User EXEC
```

If ip address is not specified than only Invalid Server Address field is displayed. Otherwise other listed fields are displayed.

Invalid Server Addresses

The number of RADIUS Access-Response packets received from unknown addresses.

Server IP Address

Round Trip Time

The time interval, in hundredths of a second, between the most recent Access-Reply | Access-Challenge and the Access-Request that matched it from the RADIUS authentication server.

Access Requests

The number of RADIUS Access-Request packets sent to this server. This number does not include retransmissions.

Access Retransmission

The number of RADIUS Access-Request packets retransmitted to this RADIUS authentication server.

Access Accepts

The number of RADIUS Access-Accept packets, including both valid and invalid packets, which were received from this server.

Access Rejects

The number of RADIUS Access-Reject packets, including both valid and invalid packets, which were received from this server.

Access Challenges

The number of RADIUS Access-Challenge packets, including both valid and invalid packets, which were received from this server.

Malformed Access Responses

The number of malformed RADIUS Access-Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or signature attributes or unknown types are not included as malformed access responses.

Bad Authenticators

The number of RADIUS Access-Response packets containing invalid authenticators or signature attributes received from this server.

Pending Requests

The number of RADIUS Access-Request packets destined for this server that have not yet timed out or received a response.

Timeouts

The number of authentication timeouts to this server.

Unknown Types

The number of RADIUS packets of unknown types, which were received from this server on the authentication port.

Packets Dropped

The number of RADIUS packets received from this server on the authentication port and dropped for some other reason.

6.1.40 show users authentication

This command displays all user and all authentication login information. It also displays the authentication login list assigned to the default user.

Format

```
show users authentication
```

Mode

```
Privileged EXEC
```

User

This field lists every user that has an authentication login list assigned.

System Login

This field displays the authentication login list assigned to the user for system login.

802.1x Port Security

This field displays the authentication login list assigned to the user for 802.1X port security.

6.1.41 users login

This command assigns the specified authentication login list to the specified user for system login. The <user> must be a configured <user> and the <listname> must be a configured login list.
If the user is assigned a login list that requires remote authentication, all access to the interface from all CLI, web, and telnet sessions will be blocked until the authentication is complete.

Note: Note that the login list associated with the ‘admin’ user can not be changed to prevent accidental lockout from the switch.

Format

`users login <user> <listname>`

Mode

`Global Config`

user

Enter user name.

listname

Enter an alphanumeric string of not more than 15 characters.
Note: When assigning a list to the 'admin' account, include an authentication method that allows administrative access even when remote authentication is unavailable (use 'authentication login <listname> [method1 [method2 [method3]]]').

6.2 HTTP Commands

6.2.1 ip http server

This command enables access to the switch‘s graphical user interface (web-based interface) via a web browser. When access is enabled, the user can login to the switch from the web-based interface. When access is disabled, the user cannot login to the switch's web server.

Disabling the web-based interface takes effect immediately. All interfaces are effected.

Default

```
enabled
```

Format

```
ip http server
```

Mode

```
Privileged EXEC
```

no ip http server

This command disables access to the switch‘s graphical user interface (web-based interface) via a web browser. When access is disabled, the user cannot login to the switch's web server.

Format

```
no ip http server
```

Mode

```
Privileged EXEC
```

6.2.2 show ip http

This command displays the http settings for the switch.

Format

```
show ip http
```

Mode

```
Privileged EXEC and User EXEC
```

HTTP Mode (Unsecure)

THis field indicates whether the HTTP mode is enabled or disabled.

6.2.3 ip https server

This command is used to turn on the HTTPS server 3.
This command enables access to the switch‘s graphical user interface (web-based interface) via a web browser. When access is enabled, the user can login to the switch from the web interface. When access is disabled, the user cannot login to the switch's web server.

Default

```
disabled
```

Format

```
ip https server
```

Mode

```
Privileged EXEC
```

no ip https server

This command is used to turn off the HTTPS server 3.
This command disables access to the switch‘s graphical user interface (web-based interface) via a web browser. When access is disabled, the user cannot login to the switch's web server.

Format

```
no ip https server
```

Mode

```
Privileged EXEC
```

6.2.4 ip https port

This command is used to set the HTTPS listening port.
The acceptable range is 1-65535. The default is 443

Note: After this setting, re-enable the HTTPS server.
See “ip http server” on page 575.

Default

```
443
```

Format

```
ip https port <port_no>
```

Mode

```
Privileged EXEC
```

no ip https port
This command is used to reset the https port to the default value.

Format

```
no ip https port
```

Mode

```
Privileged EXEC
```

6.2.5 ip https certgen

Use this command to generate an X509/PEM certificate in-place.

Format

```
ip https certgen
```

Mode

```
Privileged EXEC
```

6.2.6 show ip https

This command displays the status of the HTTPS server (status of the server and port number).

Format

```
show ip https
```

Mode

```
Privileged EXEC and User EXEC
```

HTTPS Mode

Displays the status of the HTTPS server (enabled, disabled).

HTTPS Port

Displays the port number of the HTTPS server (default: 443).

7 Appendix- VLAN Example

LAN switches can segment networks into logically defined virtual work-groups.This logical segmentation is commonly referred as a virtual LAN (VLAN). This logical segmentation of devices provides better LAN administration, security, and management of broadcast activity over the network. Virtual LANs have become an integral feature of switched LAN solutions.

The VLAN example below demonstrates a simple VLAN configuration.

If a single port is a member of VLANs 2, 3 and 4, the port expects to see traffic tagged with either VLAN 2,3 or 4.

The PVID (Port Virtual Identification) could be something entirely different, for example '12' and things would still work fine, just so incoming traffic was tagged.

Example:
Project A = (VLAN2, ports 1,2)
Project B = (VLAN3, ports 3,4)
Project C = (VLAN4, ports 5,6)
Project P = (VLAN 9, port 7)

7.1 SOLUTION 1

All traffic entering the ports is tagged traffic. Since the traffic is tagged, the PVID configuration for each port is not a concern.

- The network card configuration for devices on Project A must be set to tag all traffic with 'VLAN 2'
- The network card configuration for devices on Project B must be set to tag all traffic with 'VLAN 3'
- The network card configuration for devices on Project C must be set to tag all traffic with 'VLAN 4'
- The network card configuration for devices on Project P must be set to tag all traffic with 'VLAN 9'

7.2 SOLUTION 2

The network card configuration for devices on Project A, B and C should be set to NOT tag traffic.

To take care of these untagged frames configure the following:

- vlan pvid 2 (in interface 0/1)
- vlan pvid 2 (in interface 0/2)
- vlan pvid 3 (in interface 0/3)
- vlan pvid 3 (in interface 0/4)
- vlan pvid 4 (in interface 0/5)
- vlan pvid 4 (in interface 0/6)

8 Routing Commands

This chapter provides a detailed explanation of the Routing commands.

8.1 ARP Commands

This chapter provides a detailed explanation of the Address Resolution Protocol (ARP) commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Copy commands are used to transfer configuration and informational files to and from the switch.

8.1.1 arp

This command creates an ARP entry. The value for <*ipaddress*> is the IP address of a device on a subnet attached to an existing routing interface. <*macaddr*> is a unicast MAC address for that device.

The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 00:06:29:32:81:40.

Format

```
arp <ipaddress> <macaddr>
```

Mode

```
Global Config
```

no arp

This command deletes an ARP entry. The value for <*arpentry*> is the IP address of the interface. The value for <*ipaddress*> is the IP address of a device on a subnet attached to an existing routing interface. <*macaddr*> is a unicast MAC address for that device.

Format

```
no arp <ipaddress> <macaddr>
```

Mode

```
Global Config
```

8.1.2 ip proxy-arp

This command enables proxy ARP on a router interface.
Without proxy ARP, a device only responds to an ARP request if the target IP address is an address configured on the interface where the ARP request arrived. With proxy ARP, the device may also respond if the target IP address is reachable. The device only responds if all next hops in its route to the destination are through interfaces other than the interface that received the ARP request.

Default

```
enabled
```

Format

```
ip proxy-arp
```

Mode

```
Interface Config
```

no ip proxy-arp

This command disables proxy ARP on a router interface.

Format

```
no ip proxy-arp
```

Mode

```
Interface Config
```

8.1.3 arp cachesize

This command configures the ARP cache size.

Format

```
arp cachesize <288-2048>
```

Mode

```
Global Config
```

no arp cachesize

This command configures the default ARP cache size which is 2048.

Format

```
no arp cachesize
```

Mode

```
Global Config
```

8.1.4 arp dynamicrenew

This command enables ARP component to automatically renew ARP entries of type dynamic when they age out.

Format

```
arp dynamicrenew
```

Mode

```
Global Config
```

no arp dynamicrenew

This command disables ARP component from automatically renewing ARP entries of type dynamic when they age out.

Format

```
no arp dynamicrenew
```

Mode

```
Global Config
```

8.1.5 arp purge

This command causes the specified IP address to be removed from the ARP cache. Only entries of type dynamic or gateway are affected by this command.

Format

```
arp purge <ipaddr>
```

Mode

```
Privileged EXEC
```

8.1.6 arp resptime

This command configures the ARP request response timeout.

The value for <*seconds*> is a valid positive integer, which represents the IP ARP entry response timeout time in seconds.
The range for <*seconds*> is 1..10 seconds.

Default

1

Format

arp resptime <*1-10*>

Mode

Global Config

no arp resptime

This command configures the default ARP request response timeout.

Format

no arp resptime

Mode

Global Config

8.1.7 arp retries

This command configures the ARP count of maximum requests for retries.

The value for *<retries>* is an integer, which represents the maximum number of requests for retries.
The range for *<retries>* is an integer between 0..10 retries.

Default

4

Format

arp retries *<0-10>*

Mode

Global Config

no arp retries

This command configures the default ARP count of maximum requests for retries.

Format

no arp retries

Mode

Global Config

8.1.8 arp selective-learning

This command enables selective learning of ARPs. Normally, the router learns ARP entries from every ARP request it sees. With this feature enabled it will learn only from ARP requests that ask for one of its own interfaces.

Default

```
Disabled
```

Format

```
arp selective-learning
```

Mode

```
Global Config
```

no arp selective-learning

This command disables selective learning of ARPs

Format

```
no arp selective-learning
```

Mode

```
Global Config
```

8.1.9 arp timeout

This command configures the ARP entry ageout time.

The value for <*seconds*> is a valid positive integer, which represents the IP ARP entry ageout time in seconds.
The range for <*seconds*> is between 15..21600 seconds.

Default

1200

Format

arp timeout <*15-21600*>

Mode

Global Config

no arp timeout

This command configures the default ARP entry ageout time.

Format

no arp timeout

Mode

Global Config

8.1.10 clear arp-cache

This command causes all ARP entries of type dynamic to be removed from the ARP cache. If the *gateway* parameter is specified, the dynamic entries of type gateway are purged as well.

Format

clear arp-cache *[gateway]*

Mode

Privileged EXEC

8.1.11 show arp

This command displays the Address Resolution Protocol (ARP) cache. The displayed results are not the total ARP entries. To view the total ARP entries, the operator should view the `show arp` results in conjunction with the `show arp switch` results.

Format

`show arp`

Mode

`Privileged EXEC`

Age Time (seconds)

`Is the time it takes for an ARP entry to age out. This value was configured into the unit. Age time is measured in seconds.`

Response Time (seconds)

`Is the time it takes for an ARP request timeout. This value was configured into the unit. Response time is measured in seconds.`

Retries

`Is the maximum number of times an ARP request is retried. This value was configured into the unit.`

Cache Size

`Is the maximum number of entries in the ARP table. This value was configured into the unit.`

Dynamic Renew Mode

`Displays whether the ARP component automatically attempts to renew dynamic ARP entries when they age out.`

Selective Learning Mode

`Shows whether the router learns from all ARP requests (Disabled) or only from those targeted to one of its own interfaces (Enabled).`

Total Entry Count Current / Peak

`Field listing the total entries in the ARP table and the peak entry count in the ARP table.`

Static Entry Count Current / Max

Field listing the static entry count in the ARP table and maximum static entry count in the ARP table.

The following are displayed for each ARP entry.

IP Address

Is the IP address of a device on a subnet attached to an existing routing interface.

MAC Address

Is the hardware MAC address of that device.

Interface

Is the routing slot/port associated with the device ARP entry.

Type

Is the type that was configured into the unit. The possible values are Local, Gateway, Dynamic and Static.

Age

This field displays the current age of the ARP entry since last refresh (in hh:mm:ss format

8.1.12 show arp brief

This command displays the brief Address Resolution Protocol (ARP) table information.

Format

```
show arp brief
```

Mode

```
Privileged EXEC
```

Age Time (seconds)

```
Is the time it takes for an ARP entry to age out.
This value was configured into the unit. Age time
is measured in seconds.
```

Response Time (seconds)

```
Is the time it takes for an ARP request timeout.
This value was configured into the unit. Response
time is measured in seconds.
```

Retries

```
Is the maximum number of times an ARP request is
retried. This value was configured into the unit.
```

Cache Size

```
Is the maximum number of entries in the ARP table.
This value was configured into the unit.
```

Dynamic Renew Mode

```
Displays whether the ARP component automatically
attempts to renew dynamic ARP entries when they age
out.
```

Selective Learning Mode

```
Shows whether the router learns from all ARP
requests (Disabled) or only from those targeted to
one of its own interfaces (Enabled).
```

Total Entry Count Current / Peak

```
Field listing the total entries in the ARP table
and the peak entry count in the ARP table.
```

Static Entry Count Current / Max

Field listing the static entry count in the ARP table and maximum static entry count in the ARP table.

8.1.13 show arp switch

This command displays connectivity between the switch and other devices. The Address Resolution Protocol (ARP) cache identifies the MAC addresses of the IP stations communicating with the switch.

Format

```
show arp switch
```

Mode

Privileged EXEC

MAC Address

A unicast MAC address for which the switch has forwarding and/or filtering information. The format is 6 two-digit hexadecimal numbers that are separated by colons, for example 01:23:45:67:89:AB

IP Address

The IP address assigned to each interface.

Interface

Valid slot and port number separated by forward slashes.

8.2 IP Routing

This chapter provides a detailed explanation of the IP Routing commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

Note: Shared VLAN learning and routing are mutually exclusive. Make sure that shared VLAN learning is disabled before using IP routing (see “bridge vlan-learning” on page 122).

8.2.1 routing

This command enables routing for an interface.

The current value for this function is displayed under "show ip interface" labeled as "Routing Mode".

Default

```
disabled
```

Format

```
routing
```

Mode

```
Interface Config
```

no routing

This command disables routing for an interface.

The current value for this function is displayed under "show ip interface" labeled as "Routing Mode".

Format

```
no routing
```

Mode

```
Interface Config
```

8.2.2 ip routing

This command enables the IP Router Admin Mode for the master switch.

Format

```
ip routing
```

Mode

```
Global Config
```

no ip routing

This command disables the IP Router Admin Mode for the master switch.

Format

```
no ip routing
```

Mode

```
Global Config
```

8.2.3 ip address

This command configures an IP address on an interface. The IP address may be a secondary IP address.

The value for <*ipaddr*> is the IP Address of the interface.

The value for <*subnetmask*> is a 4-digit dotted-decimal number which represents the subnet mask of the interface. This changes the label IP address in `show ip interface`.

Format

`ip address <ipaddr> <subnetmask> [secondary]`

Mode

`Interface Config`

no ip address

This command deletes an IP address from an interface.

The value for <*ipaddr*> is the IP Address of the interface.

The value for <*subnetmask*> is a 4-digit dotted-decimal number which represents the Subnet Mask of the interface.

Format

`no ip address <ipaddr> <subnetmask> [secondary]`

Mode

`Interface Config`

8.2.4 ip mtu

This command configures the MTU size (maximum transfer unit) for IP protocol on the specified interface.

The value for *<68-9000>* is the MTU value for IP protocol.

Default

`1500`

Format

`ip mtu <68-9000>`

Mode

`Interface Config`

no ip mtu

This command sets the MTU size (maximum transfer unit) for IP protocol on the specified interface to the default value (`1500`).

Format

`no ip mtu`

Mode

`Interface Config`

8.2.5 ip netdirbcast

This command enables net directed broadcasts of IP frames.
Use no command to disable.

The current value for this function is displayed under "show ip interface" labeled as "Forward Net Directed Broadcasts".

Default

```
disabled
```

Format

```
ip netdirbcast
```

Mode

```
Interface Config
```

no ip netdirbcast

This command disables net directed broadcasts of IP frames.

The current value for this function is displayed under "show ip interface" labeled as "Forward Net Directed Broadcasts".

Format

```
no ip netdirbcast
```

Mode

```
Interface Config
```

8.2.6 ip route

This command configures a static route. The <*ip_addr*> is a valid ip address. The <*subnet_mask*> is a valid subnet mask. The <*nextHopRtr*> is a valid IP address of the next hop router.
The <*preference*> is an integer value from 1 to 255. The user can specify the preference value (sometimes called "administrative distance") of an individual static route. Among routes to the same destination, the route with the lowest preference value is the route entered into the forwarding database. By specifying the preference of a static route, the user controls whether a static route is more or less preferred than routes from dynamic routing protocols. The preference also controls whether a static route is more or less preferred than other static routes to the same destination.
The value 255 stands for „unreachable“. This means that the appropriate route is never entered into the forwarding database.

If the optional parameter <*track*> and a tracking id are given, the route is removed from the routing table if the tracking instance is down. When the tracking instance comes up, the route is added to the route table again.

Note: The following must be present before the static routes are visible:
- Enable ip routing globally.
- Enable ip routing for the interface.
- The associated link must also be up.

To see all configured static routes use the command
`show ip route static.`

Default

`preference – 1`

Format

`ip route <ip_addr> <subnet_mask> <nextHopRtr> [<preference>] [track<trackid>]`

Mode

`Global Config`

no ip route

This command deletes all next hops to a destination static route. If the optional <nextHopRtr> parameter is designated, the next hop is deleted and if the optional preference value is designated, the preference value of the static route is reset to its default.

If the optional parameter *<track>* is given, tracking is disabled for this nextHop.

Format

```
no ip route <ip_addr> <subnet_mask> [{<nextHopRtr>
[track] | <preference>}]
```

Mode

```
Global Config
```

8.2.7 ip route default

This command configures the default route. The value for *<nextHopRtr>* is a valid IP address of the next hop router. The *<preference>* is an integer value from 1 to 255.

If the optional parameter *<track>* and a tracking id are given, the route is removed from the routing table if the tracking instance is down. When the tracking instance comes up, the route is added to the route table again.

Default

```
preference – 1
```

Format

```
ip route default <nextHopRtr> [<preference>]
[track<trackid>]
```

Mode

```
Global Config
```

no ip route default

This command deletes all configured default routes. If the optional *<nextHopRtr>* parameter is designated, the specific next hop is deleted from the configured default route and if the optional preference value is designated, the preference of the configured default route is reset to its default.

If the optional parameter *<track>* is given, tracking is disabled for this nextHop.

Format

```
no ip route default [{<nextHopRtr> [track]
| <preference>}]
```

Mode

```
Global Config
```

8.2.8 ip route distance

This command sets the default distance for static routes. Lower route preference values are preferred when determining the best route. The `ip route` and `ip route default` commands allow you to optionally set the distance of an individual static route. The default distance is used when no distance is specified in these commands. Changing the default distance does not update the distance of existing static routes, even if they were assigned the original default distance. The new default distance will only be applied to static routes created after invoking the `ip route distance` command.
The value 255 stands for „unreachable“. This means that the appropriate route is never entered into the forwarding database.

Default

`1`

Format

`ip route distance <1-255>`

Mode

`Global Config`

no ip route distance

This command sets the default static route preference value in the router. Lower route preference values are preferred when determining the best route.

Format

`no ip route distance`

Mode

`Global Config`

8.2.9 ip forwarding

This command enables forwarding of IP frames.

Default

`enabled`

Format

`ip forwarding`

Mode

`Global Config`

no ip forwarding

This command disables forwarding of IP frames.

Format

`no ip forwarding`

Mode

`Global Config`

8.2.10 ip vlan-single-mac

PowerMICE and MACH4000 without MACH4002-24G.../MACH4002-48G...: In normal operating mode, packets that routed over VLAN router interfaces, are not sent with the VLAN router interface's MAC address as the source MAC address but with the physical port's MAC Address. This is compliant with the standard. Some terminal devices with incorrect IP implementation may have problems with that situation, resulting in them being unreachable via a VLAN router interface. For that reason, the SW Release 02.0.02 introduces the feature "Single MAC Mode". In this mode, all VLAN interfaces and all physical ports (except the port based router interfaces) use the same MAC address.

Default

```
enabled
```

Format

```
ip vlan-single-mac
```

Mode

```
Global Config
```

no ip vlan-single-mac

This command disables VLAN Single Mac Address Mode.

Format

```
no ip vlan-single-mode
```

Mode

```
Global Config
```

8.2.11 show ip brief

This command displays all the summary information of the IP. This command takes no options.

Format

```
show ip brief
```

Modes

```
Privileged EXEC
User EXEC
```

Default Time to Live

```
The computed TTL (Time to Live) of forwarding a
packet from
the local router to the final destination.
```

Routing Mode

```
Shows whether the routing mode is enabled or dis-
abled.
```

IP Forwarding Mode

```
Shows whether forwarding of IP frames is enabled or
disabled. This is a configured value.
```

Maximum Next Hops

```
The maximum number of next hops which can be used
for a given destination.
```

Vlan Single Mac Address Mode

```
Shows if the Vlan Single Mac Address Mode is
enabled or disabled.
Note: This output is available for the MACH4002-
48+4G and PowerMICE devices.
```

ARP-Entries
Unicast Routes
Multicast Routes

```
Shows the current and configured sizes of the
tables for ARP entries, unicast routes and
multicast routes. The configured values become
active if they are saved locally and the switch is
rebooted.
Note: This output is available for the MACH4002-
24G... and MACH4002-48G... devices.
```

8.2.12 ip table-sizes

Note: This command is available for the MACH4002-24G... and MACH4002-48G... devices.

Sets the size of various routing table sizes. The values can be changed but won't have any effect on the switch until they are saved locally and the switch is rebooted.

Default

```
2228 arp entries (2048 + interfaces)
1860 unicast routes
512 multicast routes
```

Format

```
ip table-sizes <number>
```

Mode

```
Global Config
```

no ip table-sizes

Resets the sizes of the routing tables to their default values.

Default

```
2228 arp entries (2048 + interfaces)
1860 unicast routes
512 multicast routes
```

Format

```
no ip table-sizes
```

Mode

```
Global Config
```

8.2.13 ip table-sizes arp-entries

Note: This command is available for the MACH 4002-24G... and MACH 4002-48G... devices.

This command sets the size of the arp table. Number is a positive integer value describing the maximum number of ARP entries the tables can hold.

Default

```
2228
```

Format

```
ip table-sizes arp-entries <number>
```

Mode

```
Global Config
```

no ip table-sizes arp-entries

This command resets the size of the arp table to its default value.

Default

```
2228
```

Format

```
no ip table-sizes arp-entries
```

Mode

```
Global Config
```

8.2.14 ip table-sizes unicast-routes

Note: This command is available for the MACH 4002-24G... and MACH 4002-48G... devices.

This command sets the size of the unicast routing table. Number is a positive integer value describing the maximum number of unicast routes the tables can hold.

Default

```
1860
```

Format

```
ip table-sizes unicast-routes <number>
```

Mode

```
Global Config
```

no ip table-sizes unicast-routes

This command resets the size of the unicast routing table to its default value.

Default

```
1860
```

Format

```
no ip table-sizes unicast-routes
```

Mode

```
Global Config
```

8.2.15 ip table-sizes multicast-routes

Note: This command is available for the MACH 4002-24G... and MACH 4002-48G... devices.

This command sets the size of the multicast routing table. Number is a positive integer value describing the maximum number of multicast routes the tables can hold.

Default

```
512
```

Format

```
ip table-sizes multicast-routes <number>
```

Mode

```
Global Config
```

no ip table-sizes multicast-routes

This command resets the size of the unicast routing table to its default value.

Default

```
512
```

Format

```
no ip table-sizes multicast-routes
```

Mode

```
Global Config
```

8.2.16 show ip interface

This command displays all pertinent information about the IP interface.

Format

```
show ip interface <slot/port>
```

Modes

```
Privileged EXEC
User EXEC
```

Primary IP Address

Is an IP address representing the subnet configuration of the router interface. This value was configured into the unit.

Subnet Mask

Is a mask of the network and host portion of the IP address for the router interface. This value was configured into the unit.

Secondary IP Address

The secondary ip addresses of the router interface in case of multinetting.

Routing Mode

Is the administrative mode of router interface participation. The possible values are enable or disable. This value was configured into the unit.

Administrative Mode

Is the administrative mode of the specified interface. The possible values of this field are enable or disable. This value was configured into the unit.

Forward Net Directed Broadcasts

Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.

Proxy ARP

Shows if the Proxy ARP is enabled or disabled on this router interface.

Active State

Displays whether the interface is active or inactive. An interface is considered active if its link is up and it is in forwarding state.

Link Speed Data Rate

Is an integer representing the physical link data rate of the specified interface. This is measured in Megabits per second (Mbps).

MAC Address

Is the burned in physical address of the specified interface. The format is 6 two-digit hexadecimal numbers that are separated by colons.

Encapsulation Type

Is the encapsulation type for the specified interface. The types are: Ethernet or SNAP.

IP MTU

The maximum transfer unit for the specified interface.

8.2.17 show ip interface brief

This command displays summary information about IP configuration settings for all ports in the router. This command takes no options.

Format

```
show ip interface brief
```

Modes

```
Privileged EXEC
User EXEC
```

Interface

Valid slot and port number separated by forward slashes.

IP Address

The IP address of the routing interface in 32-bit dotted decimal format.

IP Mask

The IP mask of the routing interface in 32-bit dotted decimal format.

Netdir Bcast

Indicates if IP forwards net-directed broadcasts on this interface. Possible values are Enable or Disable.

MultiCast Fwd

Indicates the multicast forwarding operational mode on the interface. Possible values are Enable or Disable.

8.2.18 show ip route

This command displays the entire route table. This commands takes no options.

Format

`show ip route`

Mode

`Privileged EXEC`

Network Address

`Is an IP address identifying the network on the specified interface.`

Subnet Mask

`Is a mask of the network and host portion of the IP address for the router interface.`

Protocol

`Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.`

Total Number of Routes

`The total number of routes.`

For each Next Hop

Next Hop Intf

`The outgoing router interface to use when forwarding traffic to the next destination.`

Next Hop IP Address

`The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.`

8.2.19 show ip route bestroutes

This command causes the entire route table to be displayed. This commands takes no options.

Format

`show ip route bestroutes`

Mode

`Privileged EXEC`

Network Address

`Is an IP route prefix for the destination.`

Subnet Mask

`Is a mask of the network and host portion of the IP address for the specified interface.`

Protocol

`Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.`

Total Number of Routes

`The total number of routes in the route table.`

For each Next Hop

Next Hop Intf

`The outgoing router interface to use when forwarding traffic to the next destination.`

Next Hop IP Address

`The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination. The next router will always be one of the adjacent neighbors or the IP address of the local interface for a directly attached network.`

8.2.20 show ip route entry

This command displays the entire route table.

Format

`show ip route entry`

Mode

`Privileged EXEC`

Network Address

`Is a valid network address identifying the network on the specified interface.`

Subnet Mask

`Is a mask of the network and host portion of the IP address for the attached network.`

Protocol

`Tells which protocol added the specified route. The possibilities are: local, static, OSPF or RIP.`

For each Next Hop

Next Hop Interface

`The outgoing router interface to use when forwarding traffic to the next destination.`

Next Hop IP Address

`The outgoing router IP address to use when forwarding traffic to the next router (if any) in the path toward the destination.`

Metric

`The cost associated with this route.`

Preference

`The administrative distance associated with this route.`

8.2.21 show ip route preferences

This command displays detailed information about the route preferences. Route preferences are used in determining the best route. Lower router preference values are preferred over higher router preference values.

Format

```
show ip route preferences
```

Modes

```
Privileged EXEC
User EXEC
```

Local

This field displays the local route preference value.

Static

This field displays the static route preference value.

OSPF Intra

This field displays the OSPF Intra route preference value.

OSPF Inter

This field displays the OSPF Inter route preference value.

OSPF Ext T1

This field displays the OSPF Type-1 route preference value.

OSPF Ext T2

This field displays the OSPF Type-2 route preference value.

RIP

This field displays the RIP route preference value.

8.2.22 show ip route static

This command displays the entire static route table.

Format

```
show ip route static
```

Mode

```
Privileged EXEC
```

Network Address

```
Is a valid network address identifying the network
on the specified interface.
```

Subnet Mask

```
Is a mask of the network and host portion of the IP
address for the attached network.
```

For each Next Hop

Pref

```
The administrative distance associated with this
route.
```

Next Hop IP Address

```
The outgoing router IP address to use when forwarding
traffic to the next router in the path toward the desti-
nation.
```

Intf.

```
The outgoing router interface to use when forwarding
traffic to the next destination. This is only shown if
there is a working router interface with a subnet
matching the next hop ip address.
```

Track ID

```
The id of the tracked object (if any).
```

Track State

```
The state of the tracked object (up or down) if the route
uses tracking.
```

8.2.23 show ip stats

This command displays IP statistical information. Refer to RFC 1213 for more information about the fields that are displayed.

Format

```
show ip stats
```

Modes

```
Privileged EXEC
User EXEC
```

Received on routing interfaces:

IpInReceives

Display the total number of input datagrams.

Received by CPU:

IpInHdrErrors

Display the number of input datagrams discarded due to errors in their IP headers.

IpInAddrErrors

Display the number of input datagrams discarded because the IP address in their IP header's destination field was not a valid.

Routed by the device:

IpForwDatagrams

Display number of input datagrams for which this entity was not their final IP destination, as a result of which an attempt was made to find a route to forward them to that final destination. In entities which do not act as IP Gateways, this counter will include only those packets which were Source-Routed via this entity, and the Source-Route option processing was successful.

Received by CPU:

IpInUnknownProtos

Display number of locally-addressed datagrams received successfully but discarded because of an unknown or unsupported protocol.

IpInDiscards

Display the The number of input IP datagrams for which no problems were encountered to prevent their continued processing, but which were discarded (e.g., for lack of buffer space).
Note that this counter does not include any datagrams discarded while awaiting re-assembly.

IpInDelivers

Display the total number of input datagrams successfully delivered to IP user-protocols (including ICMP).

IpOutRequests

Display the total number of IP datagrams which local IP user-protocols (including ICMP) supplied to IP in requests for transmission.
Note that this counter does not include any datagrams counted in ipForwDatagrams.

IpOutDiscards

Display the number of output IP datagrams for which no problem was encountered to prevent their transmission to their destination, but which were discarded (e.g., for lack of buffer space).
Note that this counter would include datagrams counted in ipForwDatagrams if any such packets met this (discretionary) discard criterion.

IpOutNoRoutes

Display the number of IP datagrams discarded because no route could be found to transmit them to their destination.
Note that this counter includes any packets counted in ipForwDatagrams which meet this `no-route' criterion.
Note that this includes any datagarms which a host cannot route because all of its default gateways are down.

Reassembly/fragmentation (not supported):

IpReasmTimeout

Display the maximum number of seconds which received fragments are held while they are awaiting reassembly at this entity.

IpReasmReqds

Display the number of IP fragments received which needed to be reassembled at this entity.

IpReasmOKs

Display the number of IP datagrams successfully re-assembled.

IpReasmFails

Display the number of failures detected by the IP re-assembly algorithm (for whatever reason: timed out, errors, etc).
Note that this is not necessarily a count of discarded IP fragments since some algorithms (notably the algorithm in RFC 815) can lose track of the number of fragments by combining them as they are received.

IpFragOKs

Display the number of IP datagrams that have been successfully fragmented at this entity.

Received by CPU:

IpFragFails

Display the number of IP datagrams that have been discarded because they needed to be fragmented at this entity but could not be, e.g., because their Don't Fragment flag was set.

IpFragCreates

Display the number of IP datagram fragments that have been generated as a result of fragmentation at this entity.

Faulty packets:

IpRoutingDiscards

Display the number of routing entries which were chosen to be discarded even though they are valid. One possible reason for discard-

ing such an entry could be to free-up buffer space for other routing entries.

Received / sent by CPU:

IcmpInMsgs

Display the total number of ICMP messages which the entity received.
Note that this counter includes all those counted by icmpInErrors.

IcmpInErrors

Display the number of ICMP messages which the entity received but determined as having ICMP-specific errors (bad ICMP checksums, bad length, etc.).

IcmpInDestUnreachs

Display the number of ICMP Destination Unreachable messages received.

IcmpInTimeExcds

Display the number of ICMP Time Exceeded messages received.

IcmpInParmProbs

Display the number of ICMP Parameter Problem messages received.

IcmpInSrcQuenchs

Display the number of ICMP Source Quench messages received.

IcmpInRedirects

Display the number of ICMP Redirect messages received.

IcmpInEchos

Display the number of ICMP Echo (request) messages received.

IcmpInEchoReps

Display the number of ICMP Echo (request) messages received.

IcmpInTimestamps

Display the number of ICMP Timestamp (request) messages received.

IcmpInTimestampReps

Display the number of ICMP Timestamp Reply messages received.

IcmpInAddrMasks

Display the number of ICMP Address Mask Request messages received.

IcmpInAddrMaskReps

Display the number of ICMP Address Mask Reply messages received.

IcmpOutMsgs

Display the total number of ICMP messages which this entity attempted to send.
Note that this counter includes all those counted by icmpOutErrors.

IcmpOutErrors

Display the number of ICMP messages which this entity did not send due to problems discovered within ICMP such as a lack of buffers. This value should not include errors discovered outside the ICMP layer such as the inability of IP to route the resultant datagram. In some implementations there may be no types of error which contribute to this counter's value.

IcmpOutDestUnreachs

Display the number of ICMP Destination Unreachable messages sent.

IcmpOutTimeExcds

Display the number of ICMP Time Exceeded messages sent.

IcmpOutParmProbs

Display the number of ICMP Parameter Problem messages sent.

IcmpOutSrcQuenchs

Display the number of ICMP Source Quench messages sent.

IcmpOutRedirects

Display the number of ICMP Redirect messages sent. For a host, this object will always be zero, since hosts do not send redirects.

IcmpOutEchoReps

Display the number of ICMP Echo Reply messages sent.

IcmpOutTimestamps

Display the number of ICMP Timestamp (request) messages sent.

IcmpOutTimestampReps

Display the number of ICMP Timestamp Reply messages sent.

IcmpOutAddrMasks

Display the number of ICMP Address Mask Request messages sent.

IcmpOutAddrMaskReps

Display the number of ICMP Address Mask Reply messages sent.

Outgoing ICMP packets dropped by limiter

Display the number of outgoing ICMP packets dropped by limiter.

8.3 Router Discovery Protocol Commands

This chapter provides a detailed explanation of the Router Discovery commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Copy commands are used to transfer configuration and informational files to and from the switch.

8.3.1 ip irdp

This command enables Router Discovery on an interface.

Default

```
disabled
```

Format

```
ip irdp
```

Mode

```
Interface Config
```

no ip irdp

This command disables Router Discovery on an interface.

Format

```
no ip irdp
```

Mode

```
Interface Config
```

8.3.2 ip irdp address

This command configures the address to be used to advertise the router for the interface. The valid values for ipaddr are 224.0.0.1 and 255.255.255.255.

Default

```
224.0.0.1
```

Format

```
ip irdp address <ipaddr>
```

Mode

```
Interface Config
```

no ip irdp address

This command configures the default address to be used to advertise the router for the interface.

Format

```
no ip irdp address
```

Mode

```
Interface Config
```

8.3.3 ip irdp holdtime

This command configures the value, in seconds, of the holdtime field of the router advertisement sent from this interface.
The range is the `maxadvertinterval` to `9000` seconds.

Default

`3 * maxinterval`

Format

`ip irdp holdtime <maxadvertinterval-9000>`

Mode

`Interface Config`

no ip irdp holdtime

This command configures the default value, in seconds, of the holdtime field of the router advertisement sent from this interface.

Format

`no ip irdp holdtime`

Mode

`Interface Config`

8.3.4 ip irdp maxadvertinterval

This command configures the maximum time, in seconds, allowed between sending router advertisements from the interface.
The range for maxadvertinterval is `4` to `1800` seconds.

Default

`600`

Format

`ip irdp maxadvertinterval <4-1800>`

Mode

`Interface Config`

no ip irdp maxadvertinterval

This command configures the default maximum time, in seconds.

Format

`no ip irdp maxadvertinterval`

Mode

`Interface Config`

8.3.5 ip irdp minadvertinterval

This command configures the minimum time, in seconds, allowed between sending router advertisements from the interface.
The range for minadvertinterval is `3` to the value of `maxadvertinterval`.

Default

`0.75 * maxadvertinterval`

Format

`ip irdp minadvertinterval <3-maxadvertinterval>`

Mode

`Interface Config`

no ip irdp minadvertinterval

This command sets the default minimum time to the default.

Format

`no ip irdp minadvertinterval`

Mode

`Interface Config`

8.3.6 ip irdp preference

This command configures the preferability of the address as a default router address, relative to other router addresses on the same subnet.
The range is −2147483648 to −1 to 0 to 1 to 2147483647.

Default

0

Format

ip irdp preference <*-2147483648-2147483647*>

Mode

Interface Config

no ip irdp preference

This command configures the default preferability of the address as a default router address, relative to other router addresses on the same subnet.

Format

no ip irdp preference

Mode

Interface Config

8.3.7 show ip irdp

This command displays the router discovery information for all interfaces, or a specified interface.

Format

show ip irdp *{*<slot/port> | *all}*

Modes

Privileged EXEC

User EXEC

Ad Mode

Displays the advertise mode which indicates whether router discovery is enabled or disabled on this interface.

Advertise Address

Displays the address which is used to advertise the router on this interface.

Max Int

Displays the maximum advertise interval which is the maximum time allowed between sending router advertisements from the interface in seconds.

Min Int

Displays the minimum advertise interval which is the minimum time allowed between sending router advertisements from the interface in seconds.

Hold Time

Displays advertise lifetime which is the value of the lifetime field of the router advertisement sent from the interface in seconds.

Preferences

Displays the preference of the address as a default router address, relative to other router addresses on the same subnet.

8.4 Virtual LAN Routing Commands

This chapter provides a detailed explanation of the Virtual LAN Routing commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Copy commands are used to transfer configuration and informational files to and from the switch.

8.4.1 vlan routing

This command creates routing on a VLAN. The <*vlanid*> value has a range from 1 to 4042. Submitting this command creates a new logical interface 9/x.

Format

```
vlan routing <vlanid>
```

Mode

```
VLAN Database
```

no vlan routing

This command deletes routing on a VLAN. The <*vlanid*> value has a range from 1 to 4042. Submitting this command deletes the logical interface 9/x.

Format

```
no vlan routing <vlanid>
```

Mode

```
VLAN Database
```

8.4.2 show ip vlan

This command displays the VLAN routing information for all VLANs with routing enabled in the system.

Format

```
show ip vlan
```

Modes

```
Privileged EXEC
User EXEC
```

VLAN ID

```
Is the identifier of the VLAN.
```

Logical Interface

```
Indicates the logical slot/port associated with the
VLAN routing interface.
```

IP Address

```
Displays the IP Address associated with this VLAN.
```

Subnet Mask

```
Indicates the subnet mask that is associated with
this VLAN.
```

MAC Address

```
Displays the MAC Address associated with this VLAN.
```

8.5 Tracking Commands

This chapter provides a detailed explanation of the Tracking commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display tracking information.
- Configuration Commands are used to configure the tracking function.

8.5.1 track interface

Connects a trackid to an interface to monitor. The trackid is an integer value from 1 to 128 (L3P: 256). Link-up-delay and link-down-delay can be configured from 0 to 255 seconds. If a delay parameter is omitted, the default delay is 0.

Format

```
track <trackid> interface <slot/port>
[link-up-delay <0-255>] [link-down-delay <0-255>]
```

Mode

```
Global Config
```

no track

Frees a `<trackid>` and track object and end tracking for this object.
The `<trackid>` is an integer value from 1 to 128 (L3P: 256) and the id of an existing track object.

Format

```
no track <trackid>
```

Mode

```
Global Config
```

8.5.2 track logical

Combines up to eight tracking instances into one single instance using a logical operation (AND or OR). The trackids are integer values from 1 to 128 (L3P: 256).

Format

```
track <trackid> logical {and|or} <trackid1>
[<trackid2> [ … [<trackid8]…]]
```

Mode

```
Global Config
```

8.5.3 track mode

Enables a track object. The trackid is an integer value from 1 to 128 (L3P:256) and the id of an existing track object.

Format

```
track <trackid> mode
```

Mode

```
Global Config
```

no track mode

Disables a track object. The trackid is an integer value from 1 to 128 (L3P:256) and the id of an existing track object. A disabled track object is defined to be up regardless of the state of the monitored object.

Format

```
no track <trackid> mode
```

Mode

```
Global Config
```

8.5.4 track ping

Enables tracking of a remote ip host or router by sending ICMP echo requests (ping). The trackid is an integer value from 1 to 128 (L3P: 256). The timeout is given in milliseconds. If <miss> consecutive answers are not received, the object switches to down, if <success> consecutive answers are received, the object switches to up. If interface is set to auto, the best route is used automatically.

The parameters can be omitted, but those given must be in the order shown below.

Note: To enable the ping to be sent via the interface, make sure that it concerns a routing interface.

Format

```
track <trackid> ping <remote-ip>
<interface {<slot/port> | auto}>
[interval  <1-10>] [miss <1-10>]
[success <1-10>] [timeout <10-10000>]
```

Defaults

```
Interface: auto
Interval: 1 second
Miss: 3
Success: 2
Timeout: 100 milliseconds
```

Mode

```
Global Config
```

8.5.5 track trap

Enables sending of a state change trap for a track object. The <trackid> is an integer value from 1 to 128 (L3P:256) and the id of an existing track object.

Format

```
track <trackid> trap
```

Mode

```
Global Config
```

no track trap

Disables sending of the state change trap for a track object. The <trackid> is an integer value from 1 to 128 (L3P:256) and the id of an existing track object.

Format

```
no track <trackid> trap
```

Mode

```
Global Config
```

8.5.6 show track

Displays information about all configured track objects.
Depending on the configuration, up to five tables are shown. There are separate tables for each tracking type (interface, logical, ping) and one for instances that do not yet have a valid type.
Additionally, a list of unconfigured track objects with registered applications (e.g. VRRP) is displayed.

Format

```
show track
```

Modes

```
Privileged EXEC
User EXEC
```

General Information

ID

The id of the track object.

Type

The type of the track object.

Status

Shows whether the monitored tracking object is up or down.

Mode

Shows whether the track object is activated.

No. Of Changes

Shows how often the State of the object changed since the track object was enabled.

Time since last change

Shows the time elapsed between the last change in state or mode.

Additional Information for Interface Objects

Intf

The Interface that is tracked by this object.

Link Delay Down

The time before a down event is signalled to the applications.

Link Delay Up

The time before an up event is signalled to the applications.

Additional Information for Logical Objects

Instances

A comma separated list of tracking instances combined into this object. If the list is incomplete (ends with "…") see show track <id> for the complete list.

Additional Information for Ping Objects

IP Address

The target IP address to monitor.

Intvl

The time interval between sending ping packets.

8.5.7 show track <id>

Displays detailed information about the given track object. The <trackid> is an integer value from 1 to 128 (L3P:256) and the id of an existing track object.

Format

show track <trackid>

Modes

Privileged EXEC

User EXEC

General Information

ID

The id of the track object.

Type

The type of the track object.

Status

Shows whether the monitored object is up or down.

Send State Change Traps

Shows whether the track trap is activated.

Mode

Shows whether the track object is activated.

No. Of Changes

Shows how often the State of the object changed since the track object was enabled.

Time since last change

Shows the time elapsed between the last change in State or mode.

Applications

The list of applications registered to this track object.

Additional Information for Interface Objects

Interface

The slot and port of the tracked interface.

Link-down-delay

Time in seconds before a link-down event is announced to the applications.

Link-up-delay

Time in seconds before a link-up event is announced to the applications.

Additional Information for Logical Objects

Operator

The logical operator used to combine the states of the members (AND or OR).

Instances included

A comma separated list of tracking instances combined into this entry.

Additional Information for Ping Objects

Target IP Address

The IP address of the remote host that is monitored.

Interface

The slot and port of the interface used to reach the remote host. If none is configured, the interface of the current best route is shown.

Ping Interval

The time between sending ping packets for this object.

Lost pings until down

Number of consecutive ping answers that must be lost (not received before the timeout) to change the state to Down.

Replies until up

Number of consecutive ping answers that must be received (before the timeout) to change the state to up.

Timeout for each Ping

The ping replies must arrive within this timeout in milliseconds to be counted as received.

8.5.8 show track applications

Displays a List of all applications registered to a track object. An application is shown for each track object it is registered to. If the track object is not yet configured, the last two columns are empty.

Format

show track applications

Modes

Privileged EXEC

User EXEC

TrackId

The id of the track object.

Application

The identifier string of the application.

Changes

Shows how often the State of the object changed since the track object was enabled.

Time since last change

Shows the time elapsed between the last change in state or mode.

8.6 VRRP Commands

This chapter provides a detailed explanation of the Virtual Router Redundancy Protocol (VRRP) commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Copy commands are used to transfer configuration and informational files to and from the switch.

8.6.1 ip vrrp

This command enables the global administrative mode of VRRP in the router.

Default

```
disabled
```

Format

```
ip vrrp
```

Mode

```
Global Config
```

no ip vrrp

This command disables the global administrative mode of VRRP in the router.

Format

```
no ip vrrp
```

Mode

```
Global Config
```

8.6.2 ip vrrp domain send-member-advertisements

This command controls whether the members of a VRRP domain send advertisements themselves as a fallback if the supervisor is still up but can't get advertisements from the master because of a single vlan failure.

Default

```
disabled
```

Format

```
ip vrrp domain <domain-id> send-member-advertise-
ments
```

Mode

```
Global Config
```

no ip vrrp domain send-member-advertisements

This command disables the sending of advertisements for the members of the domain.

Format

```
no ip vrrp domain <domain-id> send-member-adver-
tisements
```

Mode

```
Global Config
```

8.6.3 ip vrrp trap

This command enables vrrp traps.

Default

disabled

Format

ip vrrp trap {authentication-failure|new-master}

Mode

Global Config

authentication-failure

Enable or disable the sending of a trap if this router detects an authentication failure on any of its VRRP interfaces.

new-master

Enable or disable the sending of a trap if this router becomes new master for any of its VRRP interfaces.

no ip vrrp trap

This command disables vrrp traps.

Format

no ip vrrp trap {authentication-failure|new-master}

Mode

Global Config

8.6.4 ip vrrp

This command enables the VRRP protocol on an interface.
The parameter <*vrID*> is the virtual router ID which has an integer value ranging from 1 to 255.

Default

none

Format

ip vrrp <*vrID*>

Mode

Interface Config

no ip vrrp

This command disables the VRRP protocol on an interface.
The parameter <*vrID*> is the virtual router ID which has an integer value ranging from 1 to 255.
Note: If you intend to disable the protocol instance, first deactivate it using the no ip vrrp <*vrID*> mode command.

Format

no ip vrrp <*vrID*>

Mode

Interface Config

8.6.5 ip vrrp mode

This command enables the virtual router configured on the specified interface. Enabling the status field starts a virtual router. The parameter <vrID> is the virtual router ID which has an integer value ranging from 1 to 255.

Default

```
disabled
```

Format

```
ip vrrp <vrID> mode
```

Mode

```
Interface Config
```

no ip vrrp mode

This command disables the virtual router configured on the specified interface. Disabling the status field stops a virtual router.

Format

```
no ip vrrp <vrID> mode
```

Mode

```
Interface Config
```

8.6.6 ip vrrp ip

This command sets the virtual router ipaddress value for an interface. The value for <*ipaddr*> is the IP Address which is to be configured on that interface for VRRP. This may be a secondary virtual IP address. The parameter <*vrID*> is the virtual router ID which has an integer value ranging from 1 to 255.

Default

none

Format

ip vrrp <*vrID*> ip <*ipaddr*> *[secondary]*

Mode

Interface Config

8.6.7 ip vrrp authentication

This command sets the authorization details value for the virtual router configured on a specified interface. The parameter *{none | simple}* specifies the authorization type for virtual router configured on the specified interface. The parameter *[key]* is optional, it is only required when authorization type is simple text password. The parameter *<vrID>* is the virtual router ID which has an integer value ranging from 1 to 255.

Default

```
no authorization
```

Format

```
ip vrrp <vrID> authentication {none | simple <key>}
```

Mode

```
Interface Config
```

no ip vrrp authentication

This command sets the default authorization details value for the virtual router configured on a specified interface.

Format

```
no ip vrrp <vrID> authentication
```

Mode

```
Interface Config
```

8.6.8 ip vrrp preempt

This command sets the preemption mode value for the virtual router configured on a specified interface. The parameter <*vrID*> is the virtual router ID which has an integer value ranging from 1 to 255.

Default

enabled

Format

ip vrrp <*vrID*> preempt

Mode

Interface Config

no ip vrrp preempt

This command sets the default preemption mode value for the virtual router configured on a specified interface.

Format

no ip vrrp <*vrID*> preempt

Mode

Interface Config

8.6.9 ip vrrp delay-preemption

This command enables a delay before a virtual router preempts a master with a lower priority. This way dynamic routing protocols have some time to set up the routing tables before the router actually becomes Master. The delay time is given in seconds, the parameter <vrID> is the virtual router ID which is an integer value ranging from 1 to 255.

Default

```
Disabled (0 seconds)
```

Format

```
ip vrrp <vrID> delay-preemption <seconds>
```

Mode

```
Interface Config
```

no ip vrrp delay-preemption

This command disables the delay before a virtual router preempts a master with a lower priority.

Format

```
no ip vrrp <vrID> delay-preemption
```

Mode

```
Interface Config
```

8.6.10 ip vrrp priority

This command sets the priority value for the virtual router configured on a specified interface. The priority of the interface is a priority integer from 1 to 254. The parameter <*vrID*> is the virtual router ID which has an integer value ranging from 1 to 255.
The priority of a virtual router cannot be set to a value lower than the sum of the decrement values of all tracking entries for that virtual router.

Default

100

Format

ip vrrp <*vrID*> priority <*1-254*>

Mode

Interface Config

no ip vrrp priority

This command sets the default priority value for the virtual router configured on a specified interface.

Format

no ip vrrp <*vrID*> priority

Mode

Interface Config

8.6.11 ip vrrp timers advertise

This command sets the virtual router's advertisement packet interval. The parameter is an integer representing the advertisement interval from 1 to 255 seconds. The parameter <vrID> is the virtual router ID which is an interger value ranging from 1 to 255.

Default

```
1
```

Format

```
ip vrrp <vrID> timers advertise <1-255>
```

Mode

```
Interface Config
```

ip vrrp timers advertise milliseconds

This command sets the virtual router's advertisement packet interval. Use this command, if you want to set an interval below 1 second. Use the above command to set intervals greater than one second. The parameter is an integer representing the advertisement interval in milliseconds. The parameter <vrID> is the virtual router ID which is an interger value ranging from 1 to 255.

Default

```
1000 milliseconds (1 second)
```

Format

```
ip vrrp <vrID> timers advertise milliseconds <100-
1000>
```

Mode

```
Interface Config
```

no ip vrrp timers advertise

This command sets the default advertisement interval for a virtual router.

Format

```
no ip vrrp <vrID> timers advertise
```

Mode

```
Interface Config
```

8.6.12 ip vrrp advertisement-address

This command sets the destination address for the VRRP advertisement packets. This can either be the multicast group address for all vrrp routers (224.0.0.18) or the unicast address of a backup router for this virtual interface. A Unicast address must be within the same subnet as the interface's ip address but must not be equal to it. The parameter <vrID> is the virtual router ID which is an integer value ranging from 1 to 255.

Default

```
224.0.0.18
```

Format

ip vrrp <vrID> advertisement-address <ipaddress>

Mode

```
Interface Config
```

no ip vrrp advertisement-address

This command resets the destination address for the VRRP advertisement packets to its default value 224.0.0.18

Format

```
no ip vrrp <vrID> advertisement-address
```

Mode

```
Interface Config
```

8.6.13 ip vrrp link-down-notification

This command enables a notification to a backup router when the virtual router looses its link. The parameter <vrID> is the virtual router ID which is an integer value ranging from 1 to 255. Give a unicast IP address of a backup router as the last parameter.

Default

```
Disabled (0.0.0.0)
```

Format

```
ip vrrp <vrID> link-down-notification <ipAddress>
```

Mode

```
Interface Config
```

no ip vrrp link-down-notification

This command disables the link down notification.

Format

```
no ip vrrp <vrID> link-down-notification
```

Mode

```
Interface Config
```

8.6.14 ip vrrp track

With this command the virtual router is configured to observe a tracked object. The trackid and the object to track are configured with the command „track“. The Parameter trackid is an integer value, the range is determined by the tracking module. The decrement value is an integer from 1 to 253. The sum of all decrement values for a given virtual router must not exceed the priority configured for that virtual router.

Default

`20`

Format

ip vrrp <vrID> track <trackid> [decrement <1-253>]

Mode

`Interface Config`

no ip vrrp track

This command configures the virtual router to stop observing a tracked object.

Format

`no ip vrrp <vrID> track <trackid>`

Mode

`Interface Config`

8.6.15 ip vrrp domain

This command configures a virtual router into a VRRP domain and can make it the supervisor of that domain.

Default

```
0 (no domain)
```

Format

```
ip vrrp <vrID> domain <1-8> [supervisor]
```

Mode

```
Interface Config
```

no ip vrrp domain supervisor

This command configures the virtual router not to be the supervisor of the domain. It will still be a member of the domain.

Format

```
no ip vrrp <vrID> domain <1-8> supervisor
```

Mode

```
Interface Config
```

no ip vrrp domain

This command removes the virtual router from any domain it is in. If the domain-id is given, the virtual router will only be removed from that domain.

Format

```
no ip vrrp <vrID> domain [<1-8>]
```

Mode

```
Interface Config
```

8.6.16 show ip vrrp interface stats

This command displays the statistical information about each virtual router configured on the switch.

Format

show ip vrrp interface stats <slot/port> <*vrID*>

Modes

Privileged EXEC

User EXEC

Uptime

The time that the virtual router has been up, in days, hours, minutes and seconds.

Protocol

Represents the protocol configured on the interface.

State Transitioned to Master

Represents the total number of times the virtual router state has changed to MASTER.

Advertisement Received

Represents the total number of VRRP advertisements received by this virtual router.

Advertisement Interval Errors

Represents the total number of VRRP advertisements received for which advertisement interval is different than the configured value for this virtual router.

Authentication Failure

Represents the total number of VRRP packets received that don't pass the authentication check.

IP TTL errors

Represents the total number of VRRP packets received by the virtual router with IP TTL (time to live) not equal to 255.

Zero Priority Packets Received

Represents the total number of VRRP packets receivedbyvirtualrouterwithapriorityof'0'.

Zero Priority Packets Sent

Represents the total number of VRRP packets sent by the virtual router with a priority of '0'.

Invalid Type Packets Received

Represents the total number of VRRP packets received by the virtual router with invalid 'type' field.

Address List Errors

Represents the total number of VRRP packets received for which address list does not match the locally configured list for the virtual router.

Invalid Authentication Type

Represents the total number of VRRP packets received with unknown authentication type.

Authentication Type Mismatch

Represents the total number of VRRP advertisements received for which 'auth type' not equal to locally configured one for this virtual router.

Packet Length Errors

Represents the total number of VRRP packets received with packet length less than length of VRRP header.

8.6.17 show ip vrrp

This command displays whether VRRP functionality is enabled or disabled on the switch. It also displays some global parameters which are required for monitoring This command takes no options.

Format

show ip vrrp

Modes

Privileged EXEC

User EXEC

Admin Mode

Displays the administrative mode for VRRP functionality on the switch.

Authentication Failure Trap

Represents the administrative mode for VRRP authentication failure trap function.

New Master Trap

Represents the administrative mode of the New Master Trap function.

Fast instances configured

Shows the number of virtual routers with an advertisement intervall of less than one second. 16 of these fast instances can be configured at a time.

Router Checksum Errors

Represents the total number of VRRP packets received with an invalid VRRP checksum value.

Router Version Errors

Represents the total number of VRRP packets received with Unknown or unsupported version number.

Router VRID Errors

Represents the total number of VRRP packets received with invalid VRID for this virtual router.

8.6.18 show ip vrrp domain

This command displays information about a VRRP domain.

Format

`show ip vrrp domain <1-8>`

Modes

`Privileged EXEC`

`User EXEC`

Interface

`Valid slot and port number separated by forward slashes.`

VRID

`Represents the router ID of the virtual router.`

State

`Represents the state (Master/backup) of the virtual router.`

Role

`Represents the role of the virtual router in this domain (Member or Supervisor).`

Members Send Advertisements

`Displays whether the members of the domain send advertisements themselves.`

Supervisor Priority

`Displays the current priority of the supervisor of the domain. This priority is used by all members.`

Supervisor Advertisement Address

`The IP address the supervisor sends its advertisement packets to.`

8.6.19 show ip vrrp interface

This command displays all configuration information and VRRP router statistics of a virtual router configured on a specific interface.

Format

`show ip vrrp interface <slot/port> <vrID>`

Modes

`Privileged EXEC`

`User EXEC`

Primary IP Address

`This field represents the configured primary IP Address for the Virtual router.`

Secondary IP Addresses

`This field represents the configured secondary IP Address for the Virtual router.`

VMAC address

`Represents the VMAC address of the specified router.`

Authentication type

`Represents the authentication type for the specific virtual router.`

Priority

`Represents the priority value for the specific virtual router.`

Advertisement interval

`Represents the advertisement interval for the specific virtual router.`

Pre-Empt Mode

`Is the preemption mode configured on the specified virtual router.`

Administrative Mode

`Represents the status (Enable or Disable) of the specific router.`

State

`Represents the state (Master/backup) of the virtual router.`

Current Priority

Displays the current priority used by this virtual router. This can be different from the configured priority if tracking or domains are used.

Preemption Delay

Shows the time preemption of a master with lower priority is delayed.

Link Down Notification

Shows the IP address link down notifications are sent to.

VRRP Domain

Displays the domain this virtual router is in.

VRRP Domain Role

Shows the role that this virtual router has in its domain (Member or Supervisor)

VRRP Domain State

Shows if the domain is completely configured or if the supervisor is missing or down.

Advertisement Address

Shows the IP address the virtual router sends its advertisement packets to.

Tracking

Shows the trackids this virtual router is observing.

Decrement

The value by which the priority of the virtual router is decremented when the tracked object goes down.

State

Shows if the tracked object is up or down. If the trackid is not a configured tracking object, it is always shown as up.

8.6.20 show ip vrrp interface brief

This command displays information about each virtual router configured on the switch. This command takes no options. It displays information about each virtual router.

Format

```
show ip vrrp interface brief
```

Modes

```
Privileged EXEC
User EXEC
```

Interface

```
Valid slot and port number separated by forward
slashes.
```

VRID

```
Represents the router ID of the virtual router.
```

IP Address

```
The primary virtual router IP address.
```

Mode

```
Represents whether the virtual router is enabled or
disabled.
```

State

```
Represents the state (Master/backup) of the virtual
router.
```

Domain

```
Displays the domain this virtual router is in. (S)
shows that the virtual router is the supervisor of
that domain.
```

8.7 OSPF Commands

This chapter provides a detailed explanation of the Open Shortest Path First (OSPF) commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Copy commands are used to transfer configuration and informational files to and from the switch.

8.7.1 enable (OSPF)

This command sets the administrative mode of OSPF in the router to active.

Default

`enabled`

Format

`enable`

Mode

`Router OSPF Config`

no enable (OSPF)

This command sets the administrative mode of OSPF in the router to inactive.

Format

`no enable`

Mode

`Router OSPF Config`

8.7.2 ip ospf

This command enables OSPF on a router interface.

Default

```
disabled
```

Format

```
ip ospf
```

Mode

```
Interface Config
```

no ip ospf

This command disables OSPF on a router interface.

Format

```
no ip ospf
```

Mode

```
Interface Config
```

8.7.3 1583compatibility

This command enables OSPF 1583 compatibility.

Note: 1583 compatibility mode is enabled by default. If all OSPF routers in the routing domain are capable of operating according to RFC 2328, OSPF 1583 compatibility mode should be disabled.

Default

`enabled`

Format

`1583compatibility`

Mode

`Router OSPF Config`

no 1583compatibility

This command disables OSPF 1583 compatibility.

Format

`no 1583compatibility`

Mode

`Router OSPF Config`

8.7.4 area default-cost

This command configures the monetary default cost for the stub area. This is the cost for the default route injected into the atttached stub area. The operator must specify the area id and an integer value between 1-16777215.

Format

`area <areaid> default-cost <1-16777215>`

Mode

`Router OSPF Config`

8.7.5 area nssa

This command configures the specified areaid to function as an NSSA.

Format

```
area <areaid> nssa
```

Mode

```
Router OSPF Config
```

no area nssa

This command disables nssa from the specified area id.

Format

```
no area <areaid> nssa
```

Mode

```
Router OSPF Config
```

8.7.6 area nssa default-info-originate

This command configures the metric value and type for the default route advertised into the NSSA. The optional metric parameter specifies the metric of the default route and is to be in a range of 1-16777215. If no metric is specified, the default value is `1`. The metric type can be comparable (nssa-external 1) or non-comparable (nssa-external 2).

Format

```
area <areaid> nssa default-info-originate [<metric>]
[{comparable | non-comparable}]
```

Mode

```
Router OSPF Config
```

8.7.7 area nssa no-redistribute (OSPF)

This command configures the NSSA ABR so that learned external routes will not be redistributed to the NSSA.

Format

`area <areaid> nssa no-redistribute`

Mode

`Router OSPF Config`

8.7.8 area nssa no-summary (OSPF)

This command configures the NSSA so that summary LSAs are not advertised from the Backbone into the NSSA.

Format

`area <areaid> nssa no-summary`

Mode

`Router OSPF Config`

8.7.9 area nssa translator-role (OSPF)

This command configures the translator role of the NSSA. A value of `always` causes the router to assume the role of the translator the instant it becomes a border router and a value of `candidate` causes the router to participate in the translator election process when it attains border router status.

Format

`area <areaid> nssa translator-role {always | candidate}`

Mode

`Router OSPF Config`

8.7.10 area nssa translator-stab-intv

This command configures the translator <*stabilityinterval*> of the NSSA. The <*stabilityinterval*> is the period of time that an elected translator continues to perform its duties after it determines that its translator status has been deposed by another router.

Format

area <*areaid*> nssa translator-stab-intv <*stabilityinterval*>

Modes

Router OSPF Config

8.7.11 area range

This command creates a specified area range for a specified area. The <*ipaddr*> is a valid IP address. The <*subnetmask*> is a valid subnet mask. The LSDB type must be specified by either summarylink or nssaexternallink, and the advertising of the area range can be allowed or suppressed.

Format

area <*areaid*> range <*ipaddr*> <*subnetmask*> *{summarylink | nssaexternallink} [advertise | not-advertise]*

Mode

Router OSPF Config

no area range

This command deletes a specified area range. The <ipaddr> is a valid IP address. The <subnetmask> is a valid subnet mask.

Format

no area <*areaid*> range <*ipaddr*> <*subnetmask*>

Mode

Router OSPF Config

8.7.12 area stub

This command creates a stub area for the specified area ID. A stub area is characterized by the fact that AS External LSAs are not propagated into the area. Removing AS External LSAs and Summary LSAs can significantly reduce the link state database of routers within the stub area.

Format

```
area <areaid> stub
```

Mode

```
Router OSPF Config
```

no area stub

This command deletes a stub area for the specified area ID.

Format

```
no area <areaid> stub
```

Mode

```
Router OSPF Config
```

8.7.13 area stub summarylsa

This command configures the Summary LSA mode for the stub area identified by **<***areaid***>**. The Summary LSA mode is configured as enabled.

Default

`disabled`

Format

`area <areaid> stub summarylsa`

Mode

`Router OSPF Config`

no area stub summarylsa

This command configures the default Summary LSA mode for the stub area identified by **<***areaid***>**.

Format

`no area <areaid> stub summarylsa`

Mode

`Router OSPF Config`

8.7.14 area virtual-link

This command creates the OSPF virtual interface for the specified **<***areaid***>** and **<***neighbor***>**. The **<***neighbor***>** parameter is the Router ID of the neighbor.

Format

```
area <areaid> virtual-link <neighbor>
```

Mode

```
Router OSPF Config
```

no area virtual-link

This command deletes the OSPF virtual interface from the given interface, identified by **<***areaid***>** and **<***neighbor***>**. The **<***neighbor***>** parameter is the Router ID of the neighbor.

Format

```
no area <areaid> virtual-link <neighbor>
```

Mode

```
Router OSPF Config
```

8.7.15 area virtual-link authentication

This command configures the authentication type and key for the OSPF virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor. The value for <*type*> is either none, simple, or encrypt. The *[key]* is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 256 bytes. Unauthenticated interfaces do not need an authentication key. If the type is encrypt, a key id in the range of 0 and 255 must be specified.The default value for authentication type is none. Neither the default password key nor the default key id are configured.

Default

none

Format

area <*areaid*> virtual-link <*neighbor*> authentication *{none | {simple <key>} | {encrypt <key> <keyid>}}*

Mode

Router OSPF Config

no area virtual-link authentication

This command configures the default authentication type for the OSPF virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format

no area <*areaid*> virtual-link <*neighbor*> authentication

Mode

Router OSPF Config

8.7.16 area virtual-link dead-interval

This command configures the dead interval for the OSPF virtual interface on the virtual interface identified by **<***areaid***>** and **<***neighbor***>**. The **<***neighbor***>** parameter is the Router ID of the neighbor.
The range for **<***seconds***>** is `1..65535`.

Default

`40`

Format

`area <areaid> virtual-link <neighbor> dead-interval <1-65535>`

Mode

`Router OSPF Config`

no area virtual-link dead-interval

This command configures the default dead interval for the OSPF virtual interface on the virtual interface identified by **<***areaid***>** and **<***neighbor***>**. The **<***neighbor***>** parameter is the Router ID of the neighbor.

Format

`no area <areaid> virtual-link <neighbor> dead-interval`

Mode

`Router OSPF Config`

8.7.17 area virtual-link hello-interval

This command configures the hello interval for the OSPF virtual interface on the virtual interface identified by **<***areaid***>** and **<***neighbor***>**. The **<***neighbor***>** parameter is the Router ID of the neighbor.
The range for **<***seconds***>** is `1..65535`.

Default

`10`

Format

`area <areaid> virtual-link <neighbor> hello-interval <1-65535>`

Mode

`Router OSPF Config`

no area virtual-link hello-interval

This command configures the default hello interval for the OSPF virtual interface on the virtual interface identified by `<areaid>` and `<neighbor>`. The `<neighbor>` parameter is the Router ID of the neighbor.

Format

`no area <areaid> virtual-link <neighbor> hello-interval`

Mode

`Router OSPF Config`

8.7.18 area virtual-link retransmit-interval

This command configures the retransmit interval for the OSPF virtual interface on the virtual interface identified by <areaid> and <neighbor>. The <neighbor> parameter is the Router ID of the neighbor.
The range for <*seconds*> is `0..3600`.

Default

`5`

Format

`area <areaid> virtual-link <neighbor> retransmit-interval <0-3600>`

Mode

`Router OSPF Config`

no area virtual-link retransmit-interval

This command configures the default retransmit interval for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format

`no area <areaid> virtual-link <neighbor> retransmit-interval`

Mode

`Router OSPF Config`

8.7.19 area virtual-link transmit-delay

This command configures the transmit delay for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.
The range for <*seconds*> is `0..3600` (1 hour).

Default

`1`

Format

`area <areaid> virtual-link <neighbor> transmit-delay <0-3600>`

Mode

`Router OSPF Config`

no area virtual-link transmit-delay

This command configures the default transmit delay for the OSPF virtual interface on the virtual interface identified by <*areaid*> and <*neighbor*>. The <*neighbor*> parameter is the Router ID of the neighbor.

Format

`no area <areaid> virtual-link <neighbor> transmit-delay`

Mode

`Router OSPF Config`

8.7.20 default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Default

```
metric -- unspecified;
type -- 2
```

Format

```
default-information originate [always] [metric <0-
16777215>] [metric-type {1 | 2}]
```

Mode

```
Router OSPF Config
```

no default-information originate (OSPF)

This command is used to control the advertisement of default routes.

Format

```
no default-information originate {always | metric |
metric-type}
```

Mode

```
Router OSPF Config
```

8.7.21 default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format

```
default-metric <1-16777215>
```

Mode

```
Router OSPF Config
```

no default-metric (OSPF)

This command is used to set a default for the metric of distributed routes.

Format

```
no default-metric
```

Mode

```
Router OSPF Config
```

8.7.22 distance ospf

This command sets the route preference value of OSPF in the router. Lower route preference values are preferred when determining the best route. The type of OSPF can be intra, inter, type-1, or type-2. The OSPF specification (RFC 2328) requires that preferences must be given to the routes learned via OSPF in the following order: intra < inter < type-1 < type-2. The <*preference*> range is

- 1 to 255 for intra
- 2 to 253 for inter
- 3 to 253 for type-1
- 4 to 255 for type-2.

Default

```
intra -- 8;
inter -- 10;
type-1 -- 13;
type-2 -- 150.
```

Format

```
distance ospf {intra | inter | type1 | type2}
<preference>
```

Mode

```
Router OSPF Config
```

no distance ospf

This command sets the default route preference value of OSPF in the router. The type of OSPF can be intra, inter, type-1, or type-2.

Format

```
no distance ospf {intra | inter | type1 | type2}
```

Mode

```
Router OSPF Config
```

8.7.23 distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format

`distribute-list <1-199> out {rip | bgp | static | connected}`

Mode

`Router OSPF Config`

no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format

`no distribute-list <1-199> out {rip | bgp | static | connected}`

Mode

`Router OSPF Config`

8.7.24 exit-overflow-interval

This command configures the exit overflow interval for OSPF. It describes the number of seconds after entering Overflow state that a router will wait before attempting to leave the Overflow State. This allows the router to again originate non-default AS-external-LSAs. When set to 0, the router will not leave Overflow State until restarted.
The range for <*seconds*> is 0..2147483647 seconds.

Default

0

Format

exit-overflow-interval <*0-2147483647*>

Mode

Router OSPF Config

no exit-overflow-interval

This command configures the default exit overflow interval for OSPF.

Format

no exit-overflow-interval

Mode

Router OSPF Config

8.7.25 external-lsdb-limit

This command configures the external LSDB limit for OSPF. If the value is -1, then there is no limit. When the number of non-default AS-external-LSAs in a router's link-state database reaches the external LSDB limit, the router enters overflow state. The router never holds more than the external LSDB limit non-default AS-external-LSAs in it database. The external LSDB limit MUST be set identically in all routers attached to the OSPF backbone and/or any regular OSPF area.
The range for <*limit*> is `-1..2147483647`.

Default

`-1`

Format

`external-lsdb-limit <-1-2147483647>`

Mode

`Router OSPF Config`

no external-lsdb-limit

This command configures the default external LSDB limit for OSPF.

Format

`no external-lsdb-limit`

Mode

`Router OSPF Config`

8.7.26 ip ospf areaid

This command sets the OSPF area to which the specified router interface belongs. The value for <*areaid*> is an IP address, formatted as a 4-digit dotted-decimal number that uniquely identifies the area to which the interface connects. Assigning an area id, which does not exist on an interface, causes the area to be created with default values.

Format

```
ip ospf areaid <areaid>
```

Mode

```
Interface Config
```

8.7.27 ip ospf authentication

This command sets the OSPF Authentication Type and Key for the specified interface. The value of <*type*> is either none, simple or encrypt. The [*key*] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. The authentication key must be 8 bytes or less if the authentication type is simple. If the type is encrypt, the key may be up to 256 bytes. If the type is encrypt a <*keyid*> in the range of 0 and 255 must be specified.

Default

The default authentication type is none.

Default

The default password key is not configured. Unauthenticated interfaces do not need an authentication key.

Default

The default keyid is not configured. Unauthenticated interfaces do not need an authentication key id.

Format

ip ospf authentication *{none | {simple <key>} | {encrypt <key> <keyid>}}*

Mode

Interface Config

no ip ospf authentication

This command sets the default OSPF Authentication Type for the specified interface.

Format

no ip ospf authentication

Mode

Interface Config

8.7.28 ip ospf cost

This command configures the cost on an OSPF interface. The <*cost*> parameter has a range of 1 to 65535.

Default

`10`

Format

`ip ospf cost <1-65535>`

Mode

`Interface Config`

no ip ospf cost

This command configures the default cost on an OSPF interface.

Format

`no ip ospf cost`

Mode

`Interface Config`

8.7.29 ip ospf dead-interval

This command sets the OSPF dead interval for the specified interface. The value for <*seconds*> is a valid positive integer, which represents the length of time in seconds that a router's Hello packets have not been seen before its neighbor routers declare that the router is down. The value for the length of time must be the same for all routers attached to a common network. This value should be some multiple of the Hello Interval (i.e. 4). Valid values range for <*seconds*> is `1..2147483647`.

Default

`40`

Format

`ip ospf dead-interval <1-2147483647>`

Mode

`Interface Config`

no ip ospf dead-interval

This command sets the default OSPF dead interval for the specified interface.

Format

`no ip ospf dead-interval`

Mode

`Interface Config`

8.7.30 ip ospf hello-interval

This command sets the OSPF hello interval for the specified interface. The value for <*seconds*> is a valid positive integer, which represents the length of time in seconds. The value for the length of time must be the same for all routers attached to a network.

Valid values range from `1..65535`.

Default

`10`

Format

`ip ospf hello-interval <1-65535>`

Mode

`Interface Config`

no ip ospf hello-interval

This command sets the default OSPF hello interval for the specified interface.

Format

`no ip ospf hello-interval`

Mode

`Interface Config`

8.7.31 ip ospf priority

This command sets the OSPF priority for the specified router interface. The priority of the interface is a priority integer from 0 to 255. A value of 0 indicates that the router is not eligible to become the designated router on this network.

Default

`1, which is the highest router priority.`

Format

`ip ospf priority <0-255>`

Mode

`Interface Config`

no ip ospf priority

This command sets the default OSPF priority for the specified router interface.

Format

`no ip ospf priority`

Mode

`Interface Config`

8.7.32 ip ospf retransmit-interval

This command sets the OSPF retransmit Interval for the specified interface. The retransmit interval is specified in seconds. The value for <*seconds*> is the number of seconds between link-state advertisement retransmissions for adjacencies belonging to this router interface. This value is also used when retransmitting database description and link-state request packets. Valid values range from `0..3600` (1 hour).

Default

`5`

Format

`ip ospf retransmit-interval <0-3600>`

Mode

`Interface Config`

no ip ospf retransmit-interval

This command sets the default OSPF retransmit Interval for the specified interface.

Format

`no ip ospf retransmit-interval`

Mode

`Interface Config`

8.7.33 ip ospf transmit-delay

This command sets the OSPF Transit Delay for the specified interface. The transmit delay is specified in seconds. In addition, it sets the estimated number of seconds it takes to transmit a link state update packet over this interface. Valid values for <*seconds*> range from 1 to 3600 (1 hour).

Default

```
1
```

Format

```
ip ospf transmit-delay <1-3600>
```

Mode

```
Interface Config
```

no ip ospf transmit-delay

This command sets the default OSPF Transit Delay for the specified interface.

Format

```
no ip ospf transmit-delay
```

Mode

```
Interface Config
```

8.7.34 ip ospf mtu-ignore

This command disables OSPF maximum transmission unit (MTU) mismatch detection. OSPF Database Description packets specify the size of the largest IP packet that can be sent without fragmentation on the interface. When a router receives a Database Description packet, it examines the MTU advertised by the neighbor. By default, if the MTU is larger than the router can accept, the Database Description packet is rejected and the OSPF adjacency is not established.

Default

`enabled`

Format

`ip ospf mtu-ignore`

Mode

`Interface Config`

no ip ospf mtu-ignore

This command enables the OSPF MTU mismatch detection.

Format

`no ip ospf mtu-ignore`

Mode

`Interface Config`

8.7.35 router-id

This command sets a 4-digit dotted-decimal number uniquely identifying the router ospf id. The <*ipaddress*> is a configured value.

Format

`router-id <ipaddress>`

Mode

`Router OSPF Config`

8.7.36 redistribute

This command configures OSPF protocol to allow redistribution of routes from the specified source protocol/routers.

Default

```
metric -- unspecified;
type -- 2;
tag -- 0
```

Format

```
redistribute {rip | bgp | static | connected} [metric
<0-16777215>] [metric-type {1 | 2}] [tag <0-4294967295>]
[subnets]
```

Mode

```
Router OSPF Config
```

no redistribute

This command configures OSPF protocol to prohibit redistribution of routes from the specified source protocol/routers.

Format

```
no redistribute {rip | bgp | static | connected} [met-
ric] [metric-type] [tag] [subnets]
```

Mode

```
Router OSPF Config
```

8.7.37 maximum-paths

This command sets the number of paths that OSPF can report for a given destination where maxpaths is platform dependent.

Default

```
4
```

Format

```
maximum-paths <maxpaths>
```

Mode

```
OSPF Router Config
```

no maximum-paths

This command resets the number of paths that OSPF can report for a given destination back to its default value.

Format

```
no maximum-paths
```

Mode

```
OSPF Router Config
```

8.7.38 trapflags

This command enables OSPF traps.

Default

enabled

Format

trapflags

Mode

Router OSPF Config

no trapflags

This command disables OSPF traps.

Format

no trapflags

Mode

Router OSPF Config

8.7.39 show ip ospf

This command displays information relevant to the OSPF router.

Format

show ip ospf

Mode

Privileged EXEC

Router ID

Is a 32 bit integer in dotted decimal format identifying the router, about which information is displayed. This is a configured value.

OSPF Admin Mode

The administrative mode of OSPF in the router. This is a configured value.

ASBR Mode

Reflects whether the ASBR mode is enabled or disabled. Enable implies that the router is an autonomous system border router. Router automatically becomes an ASBR when it is configured to redistribute routes learnt from other protocol. The possible values for the ASBR status is enabled (if the router is configured to re-distribute routes learnt by other protocols) or disabled (if the router is not configured for the same).

RFC 1583 Compatibility

Reflects whether 1583 compatibility is enabled or disabled. This is a configured value.

Default-metric

Default value for redistributed routes.

Source

Source protocol/routes that are being redistributed.

Metric-value

Metric of the routes being redistributed.

Type-value

External Type 1 or External Type 2 routes.

Tag-value

Decimal value attached to each external route.

Subnets

For redistributing routes into OSPF, the scope of redistribution for the specified protocol.

Distribute-list

TAccess list used to filter redistributed routes.

Default-info originate

Indicates whether the default routes received from other source protocols are advertised or not

The information below will only be displayed if OSPF is enabled.

ABR Status

Reflects the whether or not the router is an OSPF Area Border Router.

Exit Overflow Interval

The number of seconds that, after entering OverflowState, a router will attempt to leave OverflowState.

External LSA count

The number of external (LS type 5) link-state advertisements in the link-state database.

External LSA Checksum

A number which represents the sum of the LS checksums of external link-state advertisements contained in the link-state database.

New LSAs Originated

The number of new link-state advertisements that have been originated.

LSAs Received

The number of link-state advertisements received determined to be new instantiations.

External LSDB Limit

The maximum number of non-default AS-external-LSAs entries that can be stored in the link-state database.

Max Paths

Maximum number of paths that OSPF can report for a given destination.

8.7.40 show ip ospf area

This command displays information about the area. The <*areaid*> identifies the OSPF area that is being displayed.

Format

`show ip ospf area <areaid>`

Modes

`Privileged EXEC`

`User EXEC`

AreaID

`Is the area id of the requested OSPF area.`

Aging Interval

`Is a number representing the aging interval for this area.`

External Routing

`Is a number representing the external routing capabilities for this area.`

Authentication Type

Is the configured authentication type to use for this area.

Spf Runs

`Is the number of times that the intra-area route table has been calculated using this area's link-state database.`

Area Border Router Count

`The total number of area border routers reachable within this area.`

Area LSA Count

`Total number of link-state advertisements in this area's link-state database, excluding AS External LSA's.`

Area LSA Checksum

`A number representing the Area LSA Checksum for the specified AreaID excluding the external (LS type 5) link-state advertisements.`

Stub Mode

Represents whether the specified Area is a stub area or not. The possible values are enabled and disabled. This is a configured value.

Import Summary LSAs

Metric Value

Is a number representing the Metric Value for the specified area.

Metric Type

Is the Default Metric Type for the specified Area.

8.7.41 show ip ospf database

This command displays the link state database.

Note: The information below is only displayed if OSPF is enabled.

Note: The OSPF database information is grouped into sections by link-type and area. The groups are as follows:

- Router Link States
- Network Link States
- Network Summary States
- Summary ASBR States

The AS-Externals are not grouped by area.

Format

```
show ip ospf database
```

Modes

Privileged EXEC

User EXEC

For each link-type and area, the following information is displayed.

Link Id

Is a number that "uniquely identifies an LSA that a router originates from all other self originated LSA's of the same LS type.

Adv Router

The Advertising Router. Is a 32 bit dotted decimal number representing the LSDB interface.

Age

Is a number representing the age of the link state advertisement in seconds.

Sequence

Is a number that represents which LSA is more recent.

Checksum

Is the total number LSA checksum.

Options

This is an integer. It indicates that the LSA receives special handling during routing calculations.

Rtr Opt

Router Options are valid for router links only.

8.7.42 show ip ospf interface

This command displays the information for the IFO object or virtual interface tables.

Format

```
show ip ospf interface <slot/port>
```

Modes

```
Privileged EXEC
User EXEC
```

IP Address

Represents the IP address for the specified interface.

Subnet Mask

A mask of the network and host portion of the IP address for the OSPF interface.

OSPF Admin Mode

States whether OSPF is enabled or disabled on a router interface.

OSPF Area ID

Represents the OSPF Area Id for the specified interface.

Router Priority

A number representing the OSPF Priority for the specified interface.

Retransmit Interval

A number representing the OSPF Retransmit Interval for the specified interface.

Hello Interval

A number representing the OSPF Hello Interval for the specified interface.

Dead Interval

A number representing the OSPF Dead Interval for the specified interface.

LSA Ack Interval

A number representing the OSPF LSA Acknowledgement Interval for the specified interface.

Transit Delay Interval

A number representing the OSPF Transit Delay for the specified interface.

Authentication Type

The OSPF Authentication Type for the specified interface are: none, simple, and encrypt.

The information below will only be displayed if OSPF is enabled.

OSPF Interface Type

Broadcast LANs, such as Ethernet and IEEE 802.5, take the value broadcast. The OSPF Interface Type will be 'broadcast'.

State

The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router.

Designated Router

The router ID representing the designated router.

Backup Designated Router

The router ID representing the backup designated router.

Number of Link Events

The number of link events.

Metric Cost

The cost of the OSPF interface.

8.7.43 show ip ospf interface brief

This command displays brief information for the IFO object or virtual interface tables.

Format

```
show ip ospf interface brief
```

Modes

```
Privileged EXEC
User EXEC
```

Interface

Valid slot and port number separated by forward slashes.

OSPF Admin Mode

States whether OSPF is enabled or disabled on a router interface.

OSPF Area ID

Represents the OSPF Area Id for the specified interface.

Router Priority

A number representing the OSPF Priority for the specified interface.

Hello Interval

A number representing the OSPF Hello Interval for the specified interface.

Dead Interval

A number representing the OSPF Dead Interval for the specified interface.

Retransmit Interval

A number representing the OSPF Retransmit Interval for the specified interface.

Transit Delay Interval

A number representing the OSPF Transit Delay for the specified interface.

LSA Ack Interval

A number representing the OSPF LSA Acknowledgement Interval for the specified interface.

8.7.44 show ip ospf interface stats

This command displays the statistics for a specific interface. The information below will only be displayed if OSPF is enabled.

Format

```
show ip ospf interface stats <slot/port>
```

Modes

```
Privileged EXEC
User EXEC
```

OSPF Area ID

```
The area id of this OSPF interface.
```

Spf Runs

```
The number of times that the intra-area route table
has been calculated using this area's link-state
database.
```

Area Border Router Count

```
The total number of area border routers reachable
within this area. This is initially zero, and is
calculated in each SPF pass.
```

AS Border Router Count

```
The total number of Autonomous System border rout-
ers reachable within this area.
```

Area LSA Count

```
The total number of link-state advertisements in
this area's link-state database, excluding AS
External LSAs.
```

IP Address

```
The IP address associated with this OSPF interface.
```

OSPF Interface Events

```
The number of times the specified OSPF interface
has changed its state, or an error has occurred.
```

Virtual Events

```
The number of state changes or errors that occurred
on this virtual link.
```

Neighbor Events

The number of times this neighbor relationship has changed state, or an error has occurred.

External LSA Count

The number of external (LS type 5) link-state advertisements in the link-state database.

LSAs Received

The number of LSAs received.

Originate New LSAs

The number of LSAs originated.

8.7.45 show ip ospf neighbor

This command displays the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below will only be displayed if OSPF is enabled and the interface has a neighbor. The IP address is the IP address of the neighbor.

Format

show ip ospf neighbor <*ipaddr*> <slot/port>

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes..

Router Id

Is a 4-digit dotted-decimal number identifying neighbor router.

Options

An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neigh-

bor's optional OSPF capabilities are also listed in its Hello packets. This enables received Hello Packets to be rejected (i.e., neighbor relationships will not even start to form) if there is a mismatch in certain crucial OSPF capabilities.

Router Priority

Displays the OSPF priority for the specified interface. The priority of an interface is a priority integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network.

State

The types are:

Down- initial state of the neighbor conversation - no recent information has been received from the neighbor.

Attempt - no recent information has been received from the neighbor but a more concerted effort should be made to contact the neighbor.

Init - an Hello packet has recently been seen from the neighbor, but bi-directional communication has not yet been established.

2 way - communication between the two routers is bi-directional.

Exchange start - the first step in creating an adjacency between the two neighboring routers, the goal is to decide which router is the master and to decide upon the initial DD sequence number.

Exchange - the router is describing its entire link state database by sending Database Description packets to the neighbor.

Loading - Link State Request packets are sent to the neighbor asking for the more recent LSAs that have been discovered (but not yet received) in the Exchange state.

Full - the neighboring routers are fully adjacent and they will now appear in router-LSAs and network-LSAs.

Events

The number of times this neighbor relationship has changed state, or an error has occurred.

Permanence

This variable displays the status of the entry, either dynamic or permanent. This refers to how the neighbor became known.

Hellos Suppressed

This indicates whether Hellos are being suppressed to the neighbor. The types are enabled and disabled.

Retransmission Queue Length

Is an integer representing the current length of the retransmission queue of the specified neighbor router Id of the specified interface.

8.7.46 show ip ospf neighbor brief

This command displays the OSPF neighbor table list. When a particular neighbor ID is specified, detailed information about a neighbor is given. The information below will only be displayed if OSPF is enabled.

Format

```
show ip ospf neighbor brief {<slot/port> | all}
```

Modes

```
Privileged EXEC
User EXEC
```

Router ID

```
A 4 digit dotted decimal number representing the
neighbor interface.
```

IP Address

```
An IP address representing the neighbor interface.
```

Neighbor Interface Index

```
Is a slot/port identifying the neighbor interface
index.
```

8.7.47 show ip ospf range

This command displays information about the area ranges for the specified <*areaid*>. The <*areaid*> identifies the OSPF area whose ranges are being displayed.

Format

`show ip ospf range <areaid>`

Modes

`Privileged EXEC`

`User EXEC`

Area ID

`The area id of the requested OSPF area.`

IP Address

`An IP Address which represents this area range.`

Subnet Mask

`A valid subnet mask for this area range.`

Lsdb Type

`The type of link advertisement associated with this area range.`

Advertisement

`The status of the advertisement. Advertisement has two possible settings: enabled or disabled.`

8.7.48 show ip ospf stub table

This command displays the OSPF stub table. The information below will only be displayed if OSPF is initialized on the switch.

Format

```
show ip ospf stub table
```

Modes

```
Privileged EXEC
User EXEC
```

Area ID

```
Is a 32-bit identifier for the created stub area.
```

Type of Service

```
Is the type of service associated with the stub
metric. The switch only supports Normal TOS.
```

Metric Val

```
The metric value is applied based on the TOS. It
defaults to the least metric of the type of service
among the interfaces to other areas. The OSPF cost
for a route is a function of the metric value.
```

Metric Type

```
Is the type of metric advertised as the default
route.
```

Import Summary LSA

```
Controls the import of summary LSAs into stub
areas.
```

8.7.49 show ip ospf virtual-link

This command displays the OSPF Virtual Interface information for a specific area and neighbor. The <*areaid*> parameter identifies the area and the <*neighbor*> parameter identifies the neighbor's Router ID.

Format

`show ip ospf virtual-link <areaid> <neighbor>`

Modes

`Privileged EXEC`

`User EXEC`

Area ID

`The area id of the requested OSPF area.`

Neighbor Router ID

`The input neighbor Router ID.`

Hello Interval

`The configured hello interval for the OSPF virtual interface.`

Dead Interval

`The configured dead interval for the OSPF virtual interface.`

Iftransit Delay Interval

`The configured transit delay for the OSPF virtual interface.`

Retransmit Interval

`The configured retransmit interval for the OSPF virtual interface.`

Authentication Type

`The configured authentication type of the OSPF virtual interface.`

State

`The OSPF Interface States are: down, loopback, waiting, point-to-point, designated router, and backup designated router. This is the state of the OSPF interface.`

Neighbor State

`The neighbor state.`

8.7.50 show ip ospf virtual-link brief

This command displays the OSPF Virtual Interface information for all areas in the system.

Format

```
show ip ospf virtual-link brief
```

Modes

```
Privileged EXEC
User EXEC
```

Area Id

```
The area id of the requested OSPF area.
```

Neighbor

```
The neighbor interface of the OSPF virtual inter-
face.
```

Hello Interval

```
The configured hello interval for the OSPF virtual
interface.
```

Dead Interval

```
The configured dead interval for the OSPF virtual
interface.
```

Retransmit Interval

```
The configured retransmit interval for the OSPF
virtual interface.
```

Transit Delay

```
The configured transit delay for the OSPF virtual
interface.
```

8.8 RIP Commands

This chapter provides a detailed explanation of the Routing Information Protocol (RIP) commands. The commands are divided by functionality into the following different groups:

- Show commands are used to display switch settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Copy commands are used to transfer configuration and informational files to and from the switch.

8.8.1 enable (RIP)

This command sets the administrative mode of RIP in the router to active.

Default

```
enabled
```

Format

```
enable
```

Mode

```
Router RIP Config
```

no enable (RIP)

This command sets the administrative mode of RIP in the router to inactive.

Format

```
no enable
```

Mode

```
Router RIP Config
```

8.8.2 ip rip

This command enables RIP on a router interface.

Default

```
disabled
```

Format

```
ip rip
```

Mode

```
Interface Config
```

no ip rip

This command disables RIP on a router interface.

Format

```
no ip rip
```

Mode

```
Interface Config
```

8.8.3 auto-summary

This command enables the RIP auto-summarization mode.

Default

```
disabled
```

Format

```
auto-summary
```

Mode

```
Router RIP Config
```

no auto-summary

This command disables the RIP auto-summarization mode.

Format

```
no auto-summary
```

Mode

```
Router RIP Config
```

8.8.4 default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format

```
default-information originate
```

Mode

```
Router RIP Config
```

no default-information originate (RIP)

This command is used to control the advertisement of default routes.

Format

```
no default-information originate
```

Mode

```
Router RIP Config
```

8.8.5 default-metric (RIP)

This command is used to set a default for the metric of distributed routes.

Format

```
default-metric <0-15>
```

Mode

```
Router RIP Config
```

no default-metric (RIP)

This command is used to reset the default metric of distributed routes to its default value.

Format

```
no default-metric
```

Mode

```
Router RIP Config
```

8.8.6 distance rip

This command sets the route preference value of RIP in the router. Lower route preference values are preferred when determining the best route.

Default

15

Format

distance rip <*1-255*>

Mode

Router RIP Config

no distance rip

This command sets the default route preference value of RIP in the router.

Format

no distance rip

Mode

Router RIP Config

8.8.7 distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Default

0

Format

distribute-list <*1-199*> out *{ospf | bgp | static | connected}*

Mode

Router RIP Config

no distribute-list out

This command is used to specify the access list to filter routes received from the source protocol.

Format

no distribute-list <*1-199*> out *{ospf | bgp | static | connected}*

Mode

Router RIP Config

no default-information originate

This command is used to control the advertisement of default routes.

Format

no default-information originate

Mode

Router RIP Config

8.8.8 ip rip authentication

This command sets the RIP Version 2 Authentication Type and Key for the specified interface. The value of <*type*> is either `none`, `simple`, or `encrypt`.

The value for authentication key [*key*] must be 16 bytes or less. The [*key*] is composed of standard displayable, non-control keystrokes from a Standard 101/102-key keyboard. If the value of <*type*> is `encrypt`, a keyid in the range of 0 and 255 must be specified.

Default

`The default authentication type is none.`

Default

`The default password key is an empty string. Unauthenticated interfaces do not need an authentication key.`

Default

`The default key id is not defined. Unauthenticated interfaces do not need an authentication key id.`

Format

`ip rip authentication` *{none | {simple <key>} | {encrypt <key> <keyid>}}*

Mode

`Interface Config`

no ip rip authentication

This command sets the default RIP Version 2 Authentication Type for an interface.

Format

`no ip rip authentication`

Mode

`Interface Config`

8.8.9 ip rip receive version

This command configures the interface to allow RIP control packets of the specified version(s) to be received.

The value for <*mode*> is one of: `rip1` to receive only RIP version 1 formatted packets, `rip2` for RIP version 2, `both` to receive packets from either format, or `none` to not allow any RIP control packets to be received.

Default

`both`

Format

`ip rip receive version` *{rip1 | rip2 | both | none}*

Mode

`Interface Config`

no ip rip receive version

This command configures the interface to allow RIP control packets of the default version(s) to be received.

Format

`no ip rip receive version`

Mode

`Interface Config`

8.8.10 ip rip send version

This command configures the interface to allow RIP control packets of the specified version to be sent.

The value for <*mode*> is one of: `rip1` to broadcast RIP version 1 formatted packets, `rip1c` (RIP version 1 compatibility mode) which sends RIP version 2 formatted packets via broadcast, `rip2` for sending RIP version 2 using multicast, or `none` to not allow any RIP control packets to be sent.

Default

`rip2`

Format

`ip rip send version {rip1 | rip1c | rip2 | none}`

Mode

`Interface Config`

no ip rip send version

This command configures the interface to allow RIP control packets of the default version to be sent.

Format

`no ip rip send version`

Mode

`Interface Config`

8.8.11 hostroutesaccept

This command enables the RIP hostroutesaccept mode.

Default

```
enabled
```

Format

```
hostroutesaccept
```

Mode

```
Router RIP Config
```

no hostroutesaccept

This command disables the RIP hostroutesaccept mode.

Format

```
no hostroutesaccept
```

Mode

```
Router RIP Config
```

8.8.12 redistribute

This command configures RIP protocol to redistribute routes from the specified source protocol/routers. There are five possible match options. When you submit the command redistribute ospf match <match-type> the match-type or types specified are added to any match types presently being redistributed. Internal routes are redistributed by default.

Default

`metric -- not-configured; match -- internal`

Format for OSPF as source protocol

`redistribute ospf` *`[metric <0-15>] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`*

Format for other source protocol

`redistribute` *`{bgp | static | connected} [metric <0-15>]`*

Mode

`Router RIP Config`

no redistribute

This command de-configures RIP protocol to redistribute routes from the specified source protocol/routers.

Format

`no redistribute` *`{ospf | bgp | static | connected} [metric] [match [internal] [external 1] [external 2] [nssa-external 1] [nssa-external-2]]`*

Mode

`Router RIP Config`

8.8.13 split-horizon

This command sets the RIP split horizon mode.

Default

```
simple
```

Format

```
split-horizon {none | simple | poison}
```

Mode

```
Router RIP Config
```

no split-horizon

This command sets the default RIP split horizon mode.

Format

```
no split-horizon
```

Mode

```
Router RIP Config
```

8.8.14 update-timer

This command configures the RIP update interval in seconds. Shorter update intervals can improve the RIP convergence time significally. However, update intervals shorter than 10 seconds should be used only for small networks. The other RIP timers are set by the switch accordingly:
Timeout: 6 times the update interval.
Gabage Collection : 10 times the update interval.

Default

```
30
```

Format

```
update-timer <1-1000>
```

Mode

```
Router RIP Config
```

no update-timer

This command sets the default RIP update interval.

Format

```
no update-timer
```

Mode

```
Router RIP Config
```

8.8.15 show ip rip

This command displays information relevant to the RIP router.

Format

```
show ip rip
```

Modes

```
Privileged EXEC
User EXEC
```

RIP Admin Mode

Enable or disable.

Split Horizon Mode

None, simple or poison reverse. Split horizon is a technique for avoiding problems caused by including routes in updates sent to the router from which the route was originally learned. The options are: None – no special processing for this case. Simple – a route will not be included in updates sent to the router from which it was learned. Poisoned reverse – a route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity. The default is simple

Auto Summary Mode

Enable or disable. If enabled, groups of adjacent routes are summarized into single entries, in order to reduce the total number of entries The default is enable.

Host Routes Accept Mode

Enable or disable. If enabled the router accepts host routes. The default is enable.

Update Timer Interval

Current RIP update interval in seconds.

Global Route Changes

The number of route changes made to the IP Route Database by RIP. This does not include the refresh of a route's age.

Global queries -

The number of responses sent to RIP queries from other systems.

Default Metric

Sets a default for the metric of redistributed routes.This field displays the default metric if one has already been set or blank if not configured earlier. The valid values are (1 to 15)

Default Route Advertise

The default route.

8.8.16 show ip rip interface brief

This command displays general information for each RIP interface. For this command to display successful results routing must be enabled per interface (i.e. ip rip).

Format

`show ip rip interface brief`

Modes

`Privileged EXEC`

`User EXEC`

Interface

`Valid slot and port number separated by forward slashes.`

IP Address

`The IP source address used by the specified RIP interface.`

Send Version

`The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2.`

Receive Version

`The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both`

RIP Mode

`RIP administrative mode of router RIP operation; enable activates, disable de-activates it.`

Link State

`The mode of the interface (up or down).`

8.8.17 show ip rip interface

This command displays information related to a particular RIP interface.

Format

```
show ip rip interface <slot/port>
```

Modes

```
Privileged EXEC
User EXEC
```

Interface

Valid slot and port number separated by forward slashes. This is a configured value.

IP Address

The IP source address used by the specified RIP interface. This is a configured value.

Send version

The RIP version(s) used when sending updates on the specified interface. The types are none, RIP-1, RIP-1c, RIP-2. This is a configured value.

Receive version

The RIP version(s) allowed when receiving updates from the specified interface. The types are none, RIP-1, RIP-2, Both. This is a configured value.

RIP Admin Mode

RIP administrative mode of router RIP operation; enable activates, disable de-activates it. This is a configured value.

Link State

Indicates whether the RIP interface is up or down. This is a configured value.

Authentication Type

The RIP Authentication Type for the specified interface. The types are none, simple, and encrypt. This is a configured value.

Default Metric

A number which represents the metric used for default routes in RIP updates originated on the specified interface. This is a configured value.

The following information will be invalid if the link state is down.

Bad Packets Received

The number of RIP response packets received by the RIP process which were subsequently discarded for any reason.

Bad Routes Received

The number of routes contained in valid RIP packets that were ignored for any reason.

Updates Sent

The number of triggered RIP updates actually sent on this interface.

9 IP Multicast Commands

This chapter provides a detailed explanation of the IP Multicast Routing commands.

9.1 Multicast Commands

The following commands are used to configure IP Multicast.

9.1.1 ip mcast boundary

This command adds an administrative scope multicast boundary specified by <groupipaddr> and <mask> for which this multicast administrative boundary is applicable. <groupipaddr> is a group IP address and <mask> is a group IP mask.

Format

```
ip mcast boundary <groupipaddr> <mask>
```

Mode

```
Interface Config
```

no ip mcast boundary

This command deletes an administrative scope multicast boundary specified by <groupipaddr> and <mask> for which this multicast administrative boundary is applicable. <groupipaddr> is a group IP address and <mask> is a group IP mask.

Format

```
no ip mcast boundary <groupipaddr> <mask>
```

Mode

```
Interface Config
```

9.1.2 ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to active. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Default

```
disabled
```

Format

```
ip multicast
```

Mode

```
Global Config
```

no ip multicast

This command sets the administrative mode of the IP multicast forwarder in the router to inactive. For multicast routing to become operational, IGMP must be currently enabled. An error message will be displayed on the CLI if multicast routing is enabled while IGMP is disabled. However, the IP multicast mode configuration is stored in the multicast configuration file and is automatically enabled once IGMP is enabled.

Format

```
no ip multicast
```

Mode

```
Global Config
```

9.1.3 ip multicast staticroute

This command creates a static route which is used to perform RPF checking in multicast packet forwarding. The combination of the <*sourceipaddr*> and the <*mask*> fields specify the network IP address of the multicast packet source. The <*groupipaddr*> is the IP address of the next hop toward the source. The <*metric*> is the cost of the route entry for comparison with other routes to the source network and is a value in the range of 0 and 255. The *current* incoming interface is used for RPF checking for multicast packets matching this multicast static route entry.

Default

```
none
```

Format

```
ip multicast staticroute <sourceipaddr> <mask>
<rpfipaddr> <metric> <slot/port>
```

Mode

```
Global Config
```

no ip multicast staticroute

This command add deletes a static route in the static mcast table. The <*sourceipaddr*> is the IP address of the multicast packet source.

Format

```
no ip multicast staticroute <sourceipaddr>
```

Mode

```
Global Config
```

9.1.4 ip multicast ttl-threshold

This command applies the given <*ttlthreshold*> to a routing interface. The <*ttlthreshold*> is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface. The value for <*ttlthreshold*> has range from 0 to 255.

Default

```
1
```

Format

```
ip multicast ttl-threshold <ttlvalue>
```

Mode

```
Interface Config
```

no ip multicast ttl-threshold

This command applies the default <*ttlthreshold*> to a routing interface. The <*ttlthreshold*> is the TTL threshold which is to be applied to the multicast Data packets which are to be forwarded from the interface.

Format

```
no ip multicast ttl-threshold
```

Mode

```
Interface Config
```

9.1.5 disable ip multicast mdebug mtrace

This command is used to disable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Default

```
none
```

Format

```
disable ip multicast mdebug mtrace
```

Mode

```
Global Config
```

no disable ip multicast mdebug mtrace

This command is used to enable the processing capability of mtrace query on this router. If the mode is enable, the mtrace queries received by the router are processed and forwarded appropriately by the router. If the mode is disable, this router does not respond to the mtrace queries it receives from other router devices.

Format

```
no disable ip multicast mdebug mtrace
```

Mode

```
Global Config
```

9.1.6 mrinfo

This command is used to query the neighbor information of a multicast-capable router specified by [ipaddr]. The default value is the IP address of the system at which the command is issued. The mrinfo command can take up to 2 minutes to complete. Only one mrinfo command may be in process at a time. The results of this command will be available in the results bufferpool which can be displayed by using "show mrinfo".

Default

```
none
```

Format

```
mrinfo [<ipaddr>]
```

Mode

```
Privileged EXEC
```

9.1.7 mstat

This command is used to find the IP Multicast packet rate and loss information path from a source to a receiver (unicast router id of the host running mstat). The results of this command will be available in the results bufferpool which can be displayed by using the command “show mstat” on page 760. If a debug command is already in progress, a message is displayed and the new request fails.
The <source> is the IP address of the remote multicast-capable source. The [receiver] is the IP address of the receiver. The default value is the IP address of the system at which the command is issued. The [group] is a multicast address of the group to be displayed. The default value is `224.2.0.1`(the group used for the multicast backbone).

Note: The group and receiver IP addresses can be entered in any order.

Default

```
none
```

Format

```
mstat <source> [<group/receiver>] [<group/
receiver>]
```

Mode

```
Privileged EXEC
```

9.1.8 mtrace

This command is used to find the IP Multicast path from a source to a receiver (unicast router ID of the host running mtrace). A trace query is passed hop-by-hop along the reverse path from the receiver to the source, collecting hop addresses, packet counts, and routing error conditions along the path, and then the response is returned to the requestor. The results of this command are available in the results buffer pool which can be displayed by using the command “show mtrace” on page 761.
The <source> is the IP address of the remote multicast-capable source. The [receiver] is the IP address of the receiver. The default value is the IP address of system at which the command is issued. The [group] is the multicast address of the group to be displayed. The default value is `224.2.0.1`(the group used for the multicast backbone).
If a debug command is already in execution, a message is displayed and the new request fails.

Note: The group and destination IP addresses can be entered in any order.

Default

`none`

Format

```
mtrace <sourceipaddr> [<group/destination>]
[<group/destination >]
```

Mode

`Privileged EXEC`

9.1.9 no ip mcast mroute

This command is used to clear entries in the mroute table. The all parameters is used to clear all entries.
The source parameter is used to clear the routes in the mroute table entries containing the specified <*sourceipaddr*> or <*sourceipaddr*> *[groupipaddr]* pair. The source address is the source IP address of the multicast packet. The group address is the Group Destination IP address of the multicast packet.
The group parameter is used to clear the routes in the mroute table entries containing the specified <*groupipaddr*>. The group address is the Group Destination IP address of the multicast packet.

Default

```
none
```

Format

```
no ip mcast mroute {group <groupipaddr> | source
<sourceipaddr> [<groupipaddr>] | all}
```

Mode

```
Global Config
```

9.1.10 show ip mcast

This command displays the system-wide multicast information.

Format

```
show ip mcast
```

Modes

```
Privileged EXEC
User EXEC
```

Admin Mode

The administrative status of multicast.

Protocol State

The current state of the multicast protocol. Possible values are Operational or Non-Operational.

Table Max Size

The maximum number of entries allowed in the multicast table.

Number Of Packets For Which Source Not Found

The number of packets for which the source is not found.

Number Of Packets For Which Group Not Found

The number of packets for which the group is not found.

Protocol

The multicast protocol running on the router. Possible values are PIMDM, PIMSM or DVMRP.

Entry Count

The number of entries in the multicast table.

Highest Entry Count

The highest entry count in the multicast table.

9.1.11 show ip mcast boundary

This command displays all the configured administrative scoped multicast boundaries.

Format

```
show ip mcast boundary {<slot/port> | all}
```

Modes

```
Privileged EXEC
User EXEC
```

Interface

```
Valid slot and port number separated by forward
slashes.
```

Group Ip

```
The group IP address
```

Mask

```
The group IP mask
```

9.1.12 show ip mcast interface

This command displays the multicast information for the specified interface.

Format

```
show ip mcast interface <slot/port>
```

Modes

```
Privileged EXEC
User EXEC
```

Interface

```
Valid slot and port number separated by forward
slashes.
```

TTL

```
The time-to-live value for this interface.
```

9.1.13 show ip mcast mroute

This command displays a summary or all the details of the multicast table.

Format

```
show ip mcast mroute {detail | summary}
```

Modes

```
Privileged EXEC
User EXEC
```

If the “detail” parameter is specified, the following fields are displayed:

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Expiry Time

The time of expiry of this entry in seconds.

Up Time

The time elapsed since the entry was created in seconds.

RPF Neighbor

The IP address of the RPF neighbor.

Flags

The flags associated with this entry.

If the “summary” parameter is specified, the following fields are displayed:

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Protocol

The multicast routing protocol by which the entry was created.

Incoming Interface

The interface on which the packet for the source/group arrives.

Outgoing Interface List

The list of outgoing interfaces on which the packet is forwarded.

9.1.14 show ip mcast mroute group

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given <*groupipaddr*>.

Format

```
show ip mcast mroute group <groupipaddr> {detail
|summary}
```

Modes

Privileged EXEC

User EXEC

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Protocol

The multicast routing protocol by which this entry was created.

Incoming Interface

The interface on which the packet for this group arrives.

Outgoing Interface List

The list of outgoing interfaces on which this packet is forwarded.

9.1.15 show ip mcast mroute source

This command displays the multicast configuration settings such as flags, timer settings, incoming and outgoing interfaces, RPF neighboring routers, and expiration times of all the entries in the multicast mroute table containing the given <*sourceipaddr*> or <*sourceipaddr> [<groupipaddr>]* pair.

Format

```
show ip mcast mroute source <sourceipaddr> {summary
| <groupipaddr>}
```

Modes

```
Privileged EXEC
User EXEC
```

If the detail parameter is specified the follow fields are displayed:

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Expiry Time

The time of expiry of this entry in seconds.

Up Time

The time elapsed since the entry was created in seconds.

RPF Neighbor

The IP address of the RPF neighbor.

Flags

The flags associated with this entry.

If the summary parameter is specified the follow fields are displayed:

Source IP Addr

The IP address of the multicast data source.

Group IP Addr

The IP address of the destination of the multicast packet.

Protocol

The multicast routing protocol by which this entry was created.

Incoming Interface

The interface on which the packet for this source arrives.

Outgoing Interface List

The list of outgoing interfaces on which this packet is forwarded.

9.1.16 show ip mcast mroute static

This command displays all the static routes configured in the static mcast table if is specified or displays the static route associated with the particular <*sourceipaddr*>.

Format

show ip mcast mroute static [<sourceipaddr>]

Modes

Privileged EXEC

User EXEC

Source Address

The IP address of the multicast packet source.

Source Mask

The mask applied to the IP address of the multicast packet source.

RPF Address

The IP address to be used as RPF for the given source and mask.

Metric

The metric value corresponding to the source address.

Interface

Valid slot and port number separated by forward slashes.

9.1.17 show mrinfo

This command is used to display the neighbor information of a multicast-capable router from the results buffer pool of the router subsequent to the execution/completion of a "mrinfo [ipaddr]" command. The results subsequent to the completion of the latest "mrinfo" will be available in the buffer pool after a maximum duration of two minutes after the completion of the ‘show mrinfo’ command. A subsequent issue ‘mrinfo’ will overwrite the contents of the buffer pool with fresh results.

Default

none

Format

show mrinfo

Mode

Privileged EXEC

Router Interface

The IP address of this neighbor

Neighbor

The neighbor associated with the router interface

Metric

The metric value associated with this neighbor

TTL

The TTL threshold associated with this neighbor

Flags

Status of the neighbor

9.1.18 show mstat

This command is used to display the results of packet rate and loss information from the results buffer pool of the router, subsequent to the execution/ completion of a ‘mstat <source> [group] [receiver]’ command. Within two minutes of the completion of the ‘mstat’ command, the results will be available in the buffer pool. The next issuing of "mstat" would overwrite the buffer pool with fresh results.

Default

```
none
```

Format

```
show mstat
```

Mode

```
Privileged EXEC
```

9.1.19 show mtrace

This command is used to display results of multicast trace path from the results buffer pool of the router, subsequent to the execution/completion of a "mtrace <source> [group] [receiver]" command. The results subsequent to the completion of the "mtrace" will be available in the buffer pool within two minutes and thereafter. A subsequent "mtrace" command would overwrite the results in the buffer pool.

Default

none

Format

show mtrace

Modes

Privileged EXEC

User EXEC

Hops Away From Destination

The ordering of intermediate routers between the source and the destination

Intermediate Router Address

The address of the intermediate router at the specified hop distance

Mcast Protocol In Use

The multicast routing protocol used for the out interface of the specified intermediate router.

TTL Threshold

The Time-To-Live threshold of the out interface on the specified intermediate router.

Time Elapsed Between Hops (msecs)

The time between arrival at one intermediate router to the arrival at the next.

9.2 DVMRP Commands

This section provides a detailed explanation of the Distance Vector Multicast Routing Protocol (DVMRP) commands.

DVMRP is a dense mode multicast protocol and is most appropriate for use in networks where bandwidth is relatively plentiful and there is at least one multicast group member in each subnet. DVMRP assumes that all hosts are part of a multicast group until it is informed of multicast group changes. When the dense-mode multicast router is informed of a group membership change, the multicast delivery tree is pruned. DVMRP uses a distributed routing algorithm to build per-source-group multicast trees. It is also called Broadcast and Prune Multicasting protocol. It dynamically generates per-source-group multicast trees using Reverse Path Multicasting. Trees are calculated and updated dynamically to track membership of individual groups.

The commands are divided into the following different groups:

- Show commands are used to display device settings, statistics and other information.
- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

9.2.1 ip dvmrp

This command sets administrative mode of DVMRP in the router to active. IGMP must be enabled before DVMRP can be enabled.

Default

```
disabled
```

Format

```
ip dvmrp
```

Mode

```
Global Config
```

no ip dvmrp

This command sets administrative mode of DVMRP in the router to inactive.

Format

```
no ip dvmrp
```

Mode

```
Global Config
```

9.2.2 ip dvmrp metric

This command configures the metric for an interface. This value is used in the DVMRP messages as the cost to reach this network. This field has a range of 1 to 31.

Default

```
1
```

Format

```
ip dvmrp metric <metric>
```

Mode

```
Interface Config
```

no ip dvmrp metric

This command resets the metric for an interface to the default value. This value is used in the DVMRP messages as the cost to reach this network.

Format

```
no ip dvmrp metric
```

Mode

```
Interface Config
```

9.2.3 ip dvmrp trapflags

This command enables the DVMRP trap mode.

Default

```
disabled
```

Format

```
ip dvmrp trapflags
```

Mode

```
Global Config
```

no ip dvmrp trapflags

This command disables the DVMRP trap mode.

Format

```
no ip dvmrp trapflags
```

Mode

```
Global Config
```

9.2.4 ip dvmrp

This command sets the administrative mode of DVMRP on an interface to active.

Default

```
disabled
```

Format

```
ip dvmrp
```

Mode

```
Interface Config
```

no ip dvmrp

This command sets the administrative mode of DVMRP on an interface to inactive.

Format

```
no ip dvmrp
```

Mode

```
Interface Config
```

9.2.5 show ip dvmrp

This command displays the system-wide information for DVMRP.

Format

```
show ip dvmrp
```

Modes

```
Privileged EXEC
User EXEC
```

Admin Mode

This field indicates whether DVMRP is enabled or disabled.

Version String

The version of DVMRP being used.

Number of Routes

The number of routes in the DVMRP routing table.

Reachable Routes

The number of entries in the routing table with non-infinite metrics.

The following fields are displayed for each interface.

Interface

Valid slot and port number separated by forward slashes.

Interface Mode

The mode of this interface. Possible values are Enabled and Disabled.

State

The current state of DVMRP on this interface. Possible values are Operational or Non-Operational.

9.2.6 show ip dvmrp interface

This command displays the interface information for DVMRP on the specified interface.

Format

```
show ip dvmrp interface <slot/port>
```

Modes

```
Privileged EXEC
User EXEC
```

Interface Mode

This field indicates whether DVMRP is enabled or disabled on the specified interface.

Metric

The metric of this interface. This is a configured value.

Local Address

The IP Address of the interface.

This Field is displayed only when DVMRP is operational on the interface.

Generation ID

The Generation ID value for the interface. This is used by the neighboring routers to detect that the DVMRP table should be resent.

The following fields are displayed only if DVMRP is enabled on this interface.

Received Bad Packets

The number of invalid packets received.

Received Bad Routes

The number of invalid routes received.

Sent Routes

The number of routes that have been sent on this interface.

9.2.7 show ip dvmrp neighbor

This command displays the neighbor information for DVMRP.

Format

show ip dvmrp neighbor

Modes

Privileged EXEC

User EXEC

IfIndex

The value of the interface used to reach the neighbor.

Nbr IP Addr

The IP Address of the DVMRP neighbor for which this entry contains information.

State

The state of the neighboring router. The possible value for this field are ACTIVE or DOWN.

Up Time

The time since this neighboring router was learned.

Expiry Time

The time remaining for the neighbor to age out. This field is not applicable if the State is DOWN.

Generation ID

The Generation ID value for the neighbor.

Major Version

The major version of DVMRP protocol of neighbor.

Minor Version

The minor version of DVMRP protocol of neighbor.

Capabilities

The capabilities of neighbor.

Received Routes

The number of routes received from the neighbor.

Rcvd Bad Pkts

The number of invalid packets received from this neighbor.

Rcvd Bad Routes

The number of correct packets received with invalid routes.

9.2.8 show ip dvmrp nexthop

This command displays the next hop information on outgoing interfaces for routing multicast datagrams.

Format

```
show ip dvmrp nexthop
```

Modes

```
Privileged EXEC
User EXEC
```

Source IP

The sources for which this entry specifies a next hop on an outgoing interface.

Source Mask

The IP Mask for the sources for which this entry specifies a next hop on an outgoing interface.

Next Hop Interface

The interface in slot/port format for the outgoing interface for this next hop.

Type

The network is a LEAF or a BRANCH.

9.2.9 show ip dvmrp prune

This command displays the table listing the router's upstream prune information.

Format

```
show ip dvmrp prune
```

Modes

```
Privileged EXEC
User EXEC
```

Group IP

This field identifies the multicast Address that is pruned.

Source IP

This field displays the IP Address of the source that has pruned.

Source Mask

This field displays the network Mask for the prune source. It should be all 1s or both the prune source and prune mask must match.

Expiry Time (secs)

This field indicates the expiry time in seconds. This is the time remaining for this prune to age out.

9.2.10 show ip dvmrp route

This command displays the multicast routing information for DVMRP.

Format

```
show ip dvmrp route
```

Modes

```
Privileged EXEC
User EXEC
```

Source Address

This field displays the multicast address of the source group.

Source Mask

This field displays the IP Mask for the source group.

Upstream Neighbor

This field indicates the IP Address of the neighbor which is the source for the packets for a specified multicast address.

Interface

This field displays the interface used to receive the packets sent by the sources.

Metric

This field displays the distance in hops to the source subnet. This field has a different meaning than the Interface Metric field.

Expiry Time (secs)

This field indicates the expiry time in seconds. This is the time remaining for this route to age out.

Up Time (secs)

This field indicates the time when a specified route was learnt, in seconds.

9.3 IGMP Commands

This section provides a detailed explanation of the Internet Group Management Protocol (IGMP) commands. The commands are divided into the following different groups:

- Show commands are used to display device settings, statistics and other information.
- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

9.3.1 ip igmp

This command enables Multicast Routing.
This command also enables IGMP and IGMP snooping (MACH4000).

Default

```
disabled
```

Format

```
ip igmp
```

Mode

```
Global Config
```

no ip igmp

This command sets the administrative mode of IGMP in the router to inactive.

Format

```
no ip igmp
```

Mode

```
Global Config
```

9.3.2 ip igmp version

This command configures the version of IGMP for an interface.
The value for <version> is either `1`, `2` or `3`.

Default

`2`

Format

`ip igmp version <version>`

Mode

`Interface Config`

no ip igmp version

This command resets the version of IGMP to the default value.

Format

`no ip igmp version`

Mode

`Interface Config`

9.3.3 ip igmp last-member-query-count

This command sets the number of Group-Specific Queries sent before the router assumes that there are no local members on the interface.
The range for `<count>` is `1..20`.

Format

```
ip igmp last-member-query-count <count>
```

Mode

```
Interface Config
```

no ip igmp last-member-query-count

This command resets the number of Group-Specific Queries to the default value.

Format

```
no ip igmp last-member-query-count
```

Mode

```
Interface Config
```

9.3.4 ip igmp last-member-query-interval

This command configures the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface.
The range for `<tenth_seconds>` is `0..255` tenths of a second.

Default

```
10 tenths of a second (1 second)
```

Format

```
ip igmp last-member-query-interval <tenth_seconds>
```

Mode

```
Interface Config
```

<tenth_seconds>

Enter last member query interval in tenths of a second.
Valid range: 0 to 255.

no ip igmp last-member-query-interval

This command resets the Maximum Response Time being inserted into Group-Specific Queries sent in response to Leave Group messages on the interface to the default value.

Format

```
no ip igmp last-member-query-interval
```

Mode

```
Interface Config
```

9.3.5 ip igmp query-interval

This command configures the query interval for the specified interface. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.
The range for `<seconds>` is `1..3600` seconds.

Default

`125 seconds`

Format

`ip igmp query-interval <seconds>`

Mode

`Interface Config`

no ip igmp query-interval

This command resets the query interval for the specified interface to the default value. This is the frequency at which IGMP Host-Query packets are transmitted on this interface.

Format

`no ip igmp query-interval`

Mode

`Interface Config`

9.3.6 ip igmp query-max-response-time

This command configures the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface.The time interval is specified in tenths of a second.
The range for `<seconds>` is `0..255` tenths of a second.

Default

`100`

Format

`ip igmp query-max-response-time <seconds>`

Mode

`Interface Config`

no ip igmp query-max-response-time

This command resets the maximum response time interval for the specified interface, which is the maximum query response time advertised in IGMPv2 queries on this interface to the default value. The maximum response time interval is reset to the default time.

Format

`no ip igmp query-max-response-time`

Mode

`Interface Config`

9.3.7 ip igmp robustness

This command configures the robustness that allows tuning of the interface. The robustness is the tuning for the expected packet loss on a subnet. If a subnet is expected to have a lot of loss, the Robustness variable may be increased for the interface.
The range for `<robustness>` is `1..255`.

Default

`2`

Format

`ip igmp robustness <robustness>`

Mode

`Interface Config`

no ip igmp robustness

This command sets the robustness value to default.

Format

`no ip igmp robustness`

Mode

`Interface Config`

9.3.8 ip igmp startup-query-count

This command sets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface.
The range for `<count>` is `1..20`.

Default

`2`

Format

`ip igmp startup-query-count <count>`

Mode

`Interface Config`

no ip igmp startup-query-count

This command resets the number of Queries sent out on startup, separated by the Startup Query Interval on the interface to the default value.

Format

`no ip igmp startup-query-count`

Mode

`Interface Config`

9.3.9 ip igmp startup-query-interval

This command sets the interval between General Queries sent on startup on the interface. The time interval value is in seconds.
The range for `<interval>` is `1..300` seconds.

Default

`1`

Format

`ip igmp startup-query-interval <interval>`

Mode

`Interface Config`

no ip igmp startup-query-interval

This command resets the interval between General Queries sent on startup on the interface to the default value.

Format

`no ip igmp startup-query-interval`

Mode

`Interface Config`

9.3.10 show ip igmp

This command displays the system-wide IGMP information.

Format

```
show ip igmp
```

Modes

```
Privileged EXEC
User EXEC
```

IGMP Admin Mode

```
This field displays the administrative status of
IGMP. This is a configured value.
```

Interface

```
Valid slot and port number separated by forward
slashes.
```

Interface Mode

```
This field indicates whether IGMP is enabled or
disabled on the interface. This is a configured
value.
```

Protocol State

```
This field indicates the current state of IGMP on
this interface. Possible values are Operational or
Non-Operational.
```

9.3.11 show ip igmp groups

This command displays the registered multicast groups on the interface. If `[detail]` is specified this command displays the registered multicast groups on the interface in detail.

Format

```
show ip igmp groups <slot/port> [detail]
```

Mode

Privileged EXEC
User EXEC

If detail is not specified, the following fields are displayed:

IP Address

This displays the IP address of the interface participating in the multicast group.

Subnet Mask

This displays the subnet mask of the interface participating in the multicast group.

Interface Mode

This displays whether IGMP is enabled or disabled on this interface.

The following fields are not displayed if the interface is not enabled:

Querier Status

This displays whether the interface has IGMP in Querier mode or Non-Querier mode.

Groups

This displays the list of multicast groups that are registered on this interface.

If detail is specified, the following fields are displayed:

Multicast IP Address

This displays the IP Address of the registered multicast group on this interface.

Last Reporter

This displays the IP Address of the source of the last membership report received for the specified multicast group address on this interface.

Up Time

This displays the time elapsed since the entry was created for the specified multicast group address on this interface.

Expiry Time

This displays the amount of time remaining to remove this entry before it is aged out.

Version1 Host Timer

This displays the time remaining until the local router will assume that there are no longer any IGMP version 1 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 1 host present.

Version2 Host Timer

This displays the time remaining until the local router will assume that there are no longer any IGMP version 2 multicast members on the IP subnet attached to this interface. This could be an integer value or "-----" if there is no Version 2 host present.

Group Compatibility Mode

The group compatibility mode (v1, v2 or v3) for this group on the specified interface.

9.3.12 show ip igmp interface

This command displays the IGMP information for the interface.

Format

```
show ip igmp interface <slot/port>
```

Modes

Privileged EXEC

User EXEC

Interface

Valid slot and port number separated by forward slashes.

IGMP Admin Mode

The administrative status of IGMP.

Interface Mode

This field indicates whether IGMP is enabled or disabled on the interface.

IGMP Version

The version of IGMP running on the interface. This value can be configured to create a router capable of running either IGMP version 1 or 2.

Query Interval

The frequency at which IGMP Host-Query packets are transmitted on this interface.

Query Max Response Time

The maximum query response time advertised in IGMPv2 queries on this interface.

Robustness

The tuning for the expected packet loss on a subnet. If a subnet is expected to be have a lot of loss, the Robustness variable may be increased for that interface.

Startup Query Interval

The interval between General Queries sent by a Querier on startup.

Startup Query Count

The number of Queries sent out on startup, separated by the Startup Query Interval.

Last Member Query Interval

The Maximum Response Time inserted into Group-Specific Queries sent in response to Leave Group messages.

Last Member Query Count

The number of Group-Specific Queries sent before the router assumes that there are no local members.

9.3.13 show ip igmp interface membership

This command displays the list of interfaces that have registered in the multicast group.

Format

```
show ip igmp interface membership <multiipaddr>
[detail]
```

Mode

```
Privileged EXEC
```

Interface

```
Valid unit, slot and port number separated by for-
ward slashes.
```

Interface IP

```
The IP address of the interface participating in
the multicast group.
```

State

```
The interface that has IGMP in Querier mode or Non-
Querier mode.
```

Group Compatibility Mode

```
The group compatibility mode (v1, v2 or v3) for the
specified group on this interface.
```

Source Filter Mode

```
The source filter mode (Include/Exclude) for the
specified group on this interface. This is "-----"
for IGMPv1 and IGMPv2 Membership Reports.
```

If detail is specified, the following fields are displayed:

Interface

```
Valid unit, slot and port number separated by for-
ward slashes.
```

Group Compatibility Mode

```
The group compatibility mode (v1, v2 or v3) for the
specified group on this interface.
```

Source Filter Mode

The source filter mode (Include/Exclude) for the specified group on this interface. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

Source Hosts

The list of unicast source IP Addresses in the group record of the IGMPv3 Membership Report with the specified multicast group IP Address. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

Expiry Time

The amount of time remaining to remove this entry before it is aged out. This is "-----" for IGMPv1 and IGMPv2 Membership Reports.

9.3.14 show ip igmp interface stats

This command displays the IGMP statistical information for the interface. The statistics are only displayed when the interface is enabled for IGMP.

Format

```
show ip igmp interface stats <slot/port>
```

Modes

```
Privileged EXEC
User EXEC
```

Querier Status

The status of the IGMP router, whether it is running in Querier mode or Non-Querier mode.

Querier IP Address

The IP Address of the IGMP Querier on the IP subnet to which this interface is attached.

Querier Up Time

The time since the interface Querier was last changed.

Querier Expiry Time

The amount of time remaining before the Other Querier Present Timer expires. If the local system is the querier, the value of this object is zero.

Wrong Version Queries

The number of queries received whose IGMP version does not match the IGMP version of the interface.

Number of Joins

The number of times a group membership has been added on this interface.

Number of Groups

The current number of membership entries for this interface

9.4 PIM-DM Commands

This section provides a detailed explanation of the Protocol Independent Multicast - Dense Mode (PIM-DM) commands.
PIM-DM is most appropriate for networks with relatively plentiful bandwidth and with at least one multicast member in each subnet. PIM-DM assumes that all hosts are part of a multicast group and forwards packets to hosts until informed that group membership has changed. A group membership change results in the multicast delivery tree being pruned.

The commands are divided into the following different groups:

- Show commands are used to display device settings, statistics and other information.
- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

9.4.1 ip pimdm

This command enables the administrative mode of PIM-DM in the router.

Default

`disabled`

Format

`ip pimdm`

Mode

`Global Config`

no ip pimdm

This command disables the administrative mode of PIM-DM in the router. IGMP must be enabled before PIM-DM can be enabled.

Format

`no ip pimdm`

Mode

`Global Config`

9.4.2 ip pimdm holdtimes

This command configures the holdtimes for prunes and asserts. This field has a range of 30 to 64800 seconds (= 18 hours)

Default

```
210
```

Format

```
ip pimdm holdtimes <seconds>
```

Mode

```
Global Config
```

no ip pimdm holdtimes

This command resets the holdtimes to the default value.

Format

```
no ip pimdm holdtimes
```

Mode

```
Global Config
```

9.4.3 ip pimdm mode

This command sets administrative mode of PIM-DM on an interface in the router to enabled.

Default

```
disabled
```

Format

```
ip pimdm mode <slot/port>
```

Mode

```
Interface Config
```

no ip pimdm mode

This command sets administrative mode of PIM-DM on an interface in the router to disabled.

Format

```
no ip pimdm mode <slot/port>
```

Mode

```
Interface Config
```

9.4.4 ip pimdm hello-interval

This command configures the transmission frequency of hello messages between PIM enabled neighbors. This field has a range of 1 to 3600 seconds.

Default

```
30
```

Format

```
ip pimdm query-interval <seconds>
```

Mode

```
Interface Config
```

no ip pimdm hello-interval

This command resets the transmission frequency of hello messages between PIM enabled neighbors to the default value.

Format

```
no ip pimdm query-interval
```

Mode

```
Interface Config
```

9.4.5 show ip pimdm

This command displays the system-wide information for PIM-DM.

Format

```
show ip pimdm
```

Modes

```
Privileged EXEC
User EXEC
```

PIM-DM Admin Mode

This field indicates whether PIM-DM is enabled or disabled.

Holdtimes

This field displays the congifured holdtimes for prunes and asserts.

Interface

Valid slot and port number separated by forward slashes.

Interface Mode

This field indicates whether PIM-DM is enabled or disabled on this interface.

State

The current state of PIM-DM on this interface. Possible values are Operational or Non-Operational.

9.4.6 show ip pimdm interface

This command displays the interface information for PIM-DM on the specified interface.

Format

```
show ip pimdm interface <slot/port>
```

Modes

```
Privileged EXEC
User EXEC
```

Interface Mode

This field indicates whether PIM-DM is enabled or disabled on the specified interface.

PIM-DM Interface Hello Interval

The frequency at which PIM hello messages are transmitted on this interface. By default, the value is 30 seconds.

9.4.7 show ip pimdm interface stats

This command displays the statistical information for PIM-DM on the specified interface.

Format

```
show ip pimdm interface stats {<slot/port> | all}
```

Modes

```
Privileged EXEC
User EXEC
```

Interface

```
Valid slot and port number separated by forward
slashes.
```

IP Address

```
The IP Address that represents the PIM-DM inter-
face.
```

Nbr Count

```
The neighbor count for the PIM-DM interface.
```

Hello Interval

```
The time interval between two hello messages sent
from the router on the given interface.
```

Designated Router

```
The IP Address of the Designated Router for this
interface.
```

9.4.8 show ip pimdm neighbor

This command displays the neighbor information for PIM-DM on the specified interface.

Format

```
show ip pimdm neighbor {<slot/port> | all}
```

Modes

```
Privileged EXEC
User EXEC
```

Neighbor Address

```
The IP Address of the neighbor on an interface.
```

Interface

```
Valid slot and port number separated by forward
slashes.
```

Up Time

```
The time since this neighbor has become active on
this interface.
```

Expiry Time

```
The expiry time of the neighbor on this interface.
```

9.4.9 ip pim-trapflags

This command enables the PIM trap mode for both Sparse Mode (SM) and Dense Mode. (DM).

Default

```
disabled
```

Format

```
ip pim-trapflags
```

Mode

```
Global Config
```

no ip pim-trapflags

This command sets the PIM trap mode to the default.

Format

```
no ip pim-trapflags
```

Mode

```
Global Config
```

9.5 PIM-SM Commands

This section provides a detailed explanation of the Protocol Independent Multicast - Sparse Mode (PIM-SM) commands.
PIM-SM routes multicast packets to multicast groups, and is designed to efficiently establish distribution trees across wide area networks (WANs).

The Sparse Mode (SM) version of PIM is most appropriate for networks with relatively limited bandwidth and where group membership is widely distributed across regions. Sparse mode protocols begin with the assumption that few routers in the network will be involved in any given multicast path. Sparse mode routers minimize network traffic by adding branches to the tree only when explicitly requested to do so. Therefore, sparse mode protocols such as PIM-SM are better suited to WANs than the dense mode protocols.

PIM-SM uses the following concepts:

- Rendezvous Point (RP): The root of a shared distribution tree down which all multicast traffic flows.
- Designated Router (DR): Responsible for sending join messages to the RP for group members and for sending register messages to the RP for sources.
- Bootstrap Router (BSR): mechanism which provides a way in which viable group-to-RP mappings can be created and distributed to all the PIM-SM routers in a domain. This component implements the functionality for handling C-RP Advertisement and Bootstrap messages, for RP-Set creation and distribution in the PIM domain, as well as the procedures for BSR election.

The commands are divided into the following different groups:

- Show commands are used to display device settings, statistics and other information.
- Configuration commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

9.5.1 ip pimsm mode

This command is used to administratively enable PIM-SM multicast routing mode on a particular router interface.

Default

`disabled`

Format

`ip pimsm mode`

Mode

`Interface Config`

no ip pimsm mode

This command is used to administratively disable PIM-SM multicast routing mode on a particular router interface.

Format

`no ip pimsm mode`

Mode

`Interface Config`

9.5.2 ip pimsm bsr-border

Use this command to prevent bootstrap router (BSR) messages from being sent or received through an interface.

Default

```
disabled
```

Format

```
ip pimsm bsr-border
```

Mode

```
Interface Config
```

no ip pimsm bsr-border

Use this command to disable the interface from being the BSR border.

Format

```
no ip pimsm bsr-border
```

Mode

```
Interface Config
```

9.5.3 ip pimsm dr-priority

Use this command to set the priority value for which a router is elected as the designated router (DR).

Default

1

Format

```
ip pimsm dr-priority <0-2147483647>
```

Mode

```
Interface Config
```

<0-2147483647>

Enter the Designated Router priority <0 - 2147483647>.

no ip pimsm dr-priority

Use this command to set the DR priority for the interface to the default value.

Format

```
no ip pimsm dr-priority
```

Mode

```
Interface Config
```

9.5.4 ip pimsm join-prune-interval

This command is used to configure the interface join/prune interval for the PIM-SM router. The join/prune interval is specified in seconds. This parameter can be configured to a value from 1 to 18,000.

Default

```
60
```

Format

```
ip pimsm join-prune-interval <1-18000>
```

Mode

```
Interface Config
```

no ip pimsm join-prune-interval

Use this command to set the join/prune interval to the default value.

Format

```
no ip pimsm join-prune-interval
```

Mode

```
Interface Config
```

9.5.5 ip pimsm hello-interval

This command is used to configure the PIM-SM hello interval for the specified interface. The hello interval is specified in seconds. This parameter can be configured to a value from 1 to 18,000.

Default

```
30
```

Format

```
ip pimsm hello-interval <1-18000>
```

Mode

```
Interface Config
```

no ip pimsm hello-interval

Use this command to set the hello-interval to the default value.

Format

```
no ip pimsm hello-interval
```

Mode

```
Interface Config
```

9.5.6 ip pimsm bsr-candidate

This command is used to configure the router to announce its candidacy as a bootstrap router (BSR).

Format

```
ip pimsm bsr-candidate interface <slot/port>
                       [hash-mask-length] [priority]
```

Mode

```
Global Config
```

no ip pimsm bsr-candidate

This command is used to disable the router to announce its candidacy as a bootstrap router (BSR).

Format

```
no ip pimsm bsr-candidate interface <slot/port>
[hash-mask-length] [priority]
```

Mode

```
Global Config
```

9.5.7 ip pimsm register-threshold

This command configures the Register Threshold rate for the Rendezvous Point router to switch to a source-specific shortest path. The valid values are 0 to 2,000 kilobits/sec.

Default

```
0
```

Format

```
ip pimsm register-threshold <0-2000>
```

Mode

```
Global Config
```

<0-2000>

Enter the rate in kilobits per seconds <0-2000>.

no ip pimsm register-threshold

This command resets the register threshold rate for the Rendezvous Pointer router to the default value.

Format

```
no ip pimsm register-threshold
```

Mode

```
Global Config
```

9.5.8 ip pimsm rp-address

This command is used to statically configure the Rendezvous Point (RP) address for one or more multicast groups.

Default

0

Format

```
ip pimsm rp-address <rp-address> <group-address>
                                  <group-mask> [override]
```

Mode

Global Config

<rp-address>

Enter the IP Address of the RP.

<group-address>

Enter the Group Address supported by the RP.

<group-mask>

Enter the Group Mask for the Group Address.

[override]

The optional keyword override indicates that if there is a conflict, the RP configured with this command prevails over the RP learned by BSR.

no ip pimsm rp-address

This command is used to statically remove the RP address for one or more multicast groups.

Format

```
no ip pimsm rp-address <rpaddress> <group-address>
                                                <group-mask>
```

Mode

Global Config

9.5.9 ip pimsm rp-candidate

This command is used to configure the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format

```
ip pimsm rp-candidate interface <slot/port>
                        <group-address> <group-mask>
```

Mode

```
Global Config
```

<group-address>

Enter the Group Address supported by the RP.

<group-mask>

Enter the Group Mask for the Group Address.

no ip pimsm rp-candidate

This command is used to disable the router to advertise itself as a PIM candidate rendezvous point (RP) to the bootstrap router (BSR).

Format

```
no ip pimsm rp-candidate interface <slot/port>
                       <group-address> <group-mask>
```

Mode

```
Global Config
```

9.5.10 ip pimsm ssm default

This command is used to define the SSM range access list to 232/8.

Format

```
ip pimsm ssm default
```

Mode

```
Global Config
```

9.5.11 ip pimsm ssm

This command is used to define the SSM range.

Format

```
ip pimsm ssm <group-address> [group-mask]
```

Mode

```
Global Config
```

<group-address>

Enter the Group Address supported by the RP.

<group-mask>

Enter the Group Mask for the Group Address.

no ip pimsm

This command is used to disable the SSM range

Format

```
no ip pimsm ssm <group-address> [group-mask]
```

Mode

```
Global Config
```

9.5.12 show ip pimsm

This command is used to display the PIM-SM parameters.

Format

```
ip pimsm ssm
```

Mode

```
Privileged EXEC
User EXEC
```

Admin Mode

Enable/Disable

Data Threshold Rate (Kbps)

Display the Data Threshold Rate in Kbps.
Default: 0

Register Threshold Rate (Kbps)

Display the Register Threshold Rate in Kbps.
Default: 0

SSM RANGE TABLE

Display the SSM RANGE TABLE information (Group Address/Prefix Length).

Group Address/Prefix Length

Display the Group Address/Prefix Length.

PIM-SM INTERFACE STATUS

Display the PIM-SM INTERFACE STATUS table information (Interface, Interface-Mode, Operational-Status).

Interface

Display the Interface information.

Interface-Mode

Display the Interface-Mode information.

Operational-Status

Display the Operational-Status information.

9.5.13 show ip pimsm bsr

This command is used to display PIM-SM BSR table information.

Format

```
ip pimsm ssm bsr
```

Mode

```
Privileged EXEC
User EXEC
```

9.5.14 show ip pimsm interface

This command is used to display PIM-SM status of the router.

Format

```
ip pimsm ssm interface
```

Mode

```
Privileged EXEC
User EXEC
```

9.5.15 show ip pimsm neighbor

This command is used to display router's PIM neighbors on the interface.

Format

```
ip pimsm ssm neighbor
```

Mode

```
Privileged EXEC
User EXEC
```

9.5.16 show ip pimsm rp mapping

Use this command to display all group-to-RP mappings of which the router is a aware (either configured or learned from the bootstrap router (BSR)). If no RP is specified, all active RPs are displayed.

Format

```
ip pimsm ssm rp mapping [rp-address]
```

Mode

```
Privileged EXEC
User EXEC
```

9.5.17 show ip pimsm rphash

This command is used to display the PIM-SM RP information for a specific group.

Format

```
ip pimsm ssm rphash <group-address>
```

Mode

```
Privileged EXEC
User EXEC
```

9.5.18 show ip pimsm candidate

This command is used to display PIM-SM candidate-RP table information.

Format

```
ip pimsm ssm candidate
```

Mode

```
Privileged EXEC
User EXEC
```

10 Quality of Service (QoS) Commands

This chapter provides a detailed explanation of the Quality of Service (QOS) commands.
The commands are divided into these different groups:

- Show commands are used to display device settings, statistics and other information.
- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.

10.1 MAC ACL Commands

MAC Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

Note:

- The maximum number of ACLs of any type that can be created is 100.
- ACLs are supported in the inbound direction only.
- Only Ethernet II frame types are supported.
- The maximum number of rules per MAC ACL is 10.
- The maximum number of rules per interface is 20 (100 for Software Version L3P).
- ACLs are configured separately for Layer 2 and Layer 3 / Layer 4 and cannot be applied to the same interface (PowerMICE, MACH104, MACH1040 and MACH4000 without MACH4002-24G.../MACH4002-48G...).
- ACLs are configured separately for Layer 2 and Layer 3/Layer 4 and can be applied to the same interface (MACH4002-24G.../MACH4002-48G...).
- Wildcard masking for MAC ACLs (srcmacmask, dstmacmask) operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0’s) in a bit position that must be checked. A ‘1’ in a bit position of the ACL mask indicates the corresponding bit can be ignored.

10.1.1 mac access-list extended

Note: This command is available for the devices of the MACH104, MACH1040 and MACH4000 families and for the PowerMICE devices.

This command creates a MAC Access Control List (ACL) identified by <name>, consisting of classification fields defined for the Layer 2 header of an Ethernet frame. The <name> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
If a MAC ACL by this name already exists, this command enters Mac-Access-List config mode to allow updating the existing MAC ACL.

Note: The CLI mode is changed to Mac-Access-List Config when this command is successfully executed.

Format

```
mac access-list extended <name>
```

Mode

```
Interface Config
Global Config
```

name

```
Enter access-list name up to 31 characters in
length.
```

no mac access-list extended

This command deletes a MAC ACL identified by <name> from the system.

Format

```
no mac access-list extended <name>
```

Mode

```
Global Config
```

name

```
Enter access-list name up to 31 characters in
length.
```

10.1.2 mac access-list extended rename

Note: This command is available for the devices of the MACH104, MACH1040 and MACH4000 families and for the PowerMICE devices.

This command changes the name of a MAC Access Control List (ACL). The <*oldname*> parameter is the name of an existing MAC ACL. The <*newname*> parameter is a case-sensitive alphanumeric string from 1 to 31 characters uniquely identifying the MAC access list.
This command fails if a MAC ACL by the name <*newname*> already exists.

Format

```
mac access-list extended rename <oldname> <newname>
```

Mode

```
Global Config
```

10.1.3 {deny|permit}

This command creates a new rule for the current MAC access list. Each rule is appended to the list of configured rules for the list.

Note: The 'no' form of this command is not supported, since the rules within a MAC ACL cannot be deleted individually. Rather, the entire MAC ACL must be deleted and re-specified.

Note: An implicit 'deny all' MAC rule always terminates the access list.

A rule may either deny or permit traffic according to the specified classification fields. At a minimum, the source and destination MAC value and mask pairs must be specified, each of which may be substituted using the keyword any to indicate a match on any value in that field. The bpdu keyword may be specified for the destination MAC value/mask pair indicating a well-known BPDU MAC value of 01-80-c2-xx-xx-xx (hex), where 'xx' indicates a don't care. The remaining command parameters are all optional, but the most frequently used parameters appear in the same relative order as shown in the command format.
The Ethertype may be specified as either a keyword or a four-digit hexadecimal value from 0x0600-0xFFFF. The currently supported <*ethertypekey*> values are: appletalk, arp, ibmsna, ipv4, ipv6, ipx, mplsmcast, mplsucast, netbios, novell, pppoe, rarp. Each of these translates into its equivalent Ethertype value(s).

Ethertype Keyword	Corresponding Value
appletalk	0x809B
arp	0x0806
ibmsna	0x80D5
ipv4	0x0800
ipv6	0x86DD
ipx	0x8037
mplsmcast	0x8848
mplsucast	0x8847
netbios	0x8191
novell	0x8137, 0x8138

Table 17: Ethertype Keyword and 4-digit Hexadecimal Value

Ethertype Keyword	Corresponding Value
pppoe	0x8863, 0x8864
rarp	0x8035

Table 17: Ethertype Keyword and 4-digit Hexadecimal Value

The vlan and cos parameters refer to the VLAN identifier and 802.1p user priority fields, respectively, of the VLAN tag. For packets containing a double VLAN tag, this is the first (or outer) tag.
The assign-queue parameter allows specification of a particular 802.1p user priority for traffic that matches this rule. The allowed *<queue-id>* value is 0-7. The matching traffic is transmitted with the modified 802.1p user priority and also with modified IP-DSCP value for IP frames.
The redirect parameter allows the traffic matching this rule to be forwarded to the specified *<slot/port>*. The assign-queue and redirect parameters are only valid for a 'permit' rule.

Format

```
{deny|permit} {{<srcmac> <srcmacmask>} | any} {{<dstmac>
<dstmacmask>} | any| bpdu} [<ethertypekey> | <0x0600-
0xFFFF>] [vlan eq <0-4095> | cos <0-7>] [secondary-vlan
eq <0-4095>] [secondary-cos <0-7>] [assign-queue <queue-
id>] [redirect <slot/port>]
```

Note: The special command form *{deny|permit}* any is used to match all Ethernet layer 2 packets, and is the equivalent of the IP access list "match every" rule.

Mode

```
Mac-Access-List Config
```

10.1.4 mac access-group

This command attaches a specific MAC Access Control List (ACL) identified by <*name*> to an interface in the inbound direction. The <*name*> parameter must be the name of an existing MAC ACL.
An optional sequence number may be specified to indicate the order of this MAC access list relative to other MAC access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface, the specified MAC access list replaces the currently attached MAC access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.
This command specified in Interface Config mode only affects a single interface, whereas the Global Config mode setting is applied to all interfaces.

Format

`mac access-group <name> in [sequence <1-4294967295>]`

Modes

`Global Config`

`Interface Config`

name

`Enter name of MAC Access Control List.`

<1-4294967295>

`Enter the sequence number (greater than 0) to rank precedence for this interface and direction. A lower sequence number has higher precedence.`

no mac access-group

This command removes a MAC ACL identified by <*name*> from the interface in a given direction.

Format

```
no mac access-group <name> [in]
```

Modes

```
Global Config
Interface Config
```

name

```
Enter name of MAC Access Control List.
```

10.1.5 show mac access-lists

Note: This command is available for the devices of the MACH104, MACH1040 and MACH4000 families and for the PowerMICE devices.

This command displays a MAC access list and all of the rules that are defined for the MAC ACL. The *[name]* parameter is used to identify a specific MAC ACL to display.

Format

```
show mac access-lists [name]
```

name

```
Enter name of MAC Access Control List.
```

Mode

```
Privileged EXEC
```

Rule Number

```
The ordered rule number identifier defined within
the MAC ACL.
```

Action

```
Displays the action associated with each rule. The
possible values are permit or deny.
```

Source MAC Address

Displays the source MAC address for this rule.

Source MAC Mask

Displays the source MAC mask for this rule.

Destination MAC Address

Displays the destination MAC address for this rule.

Destination MAC Mask

Displays the destination MAC mask for this rule.

Ethertype

Displays the Ethertype keyword or custom value for this rule.

VLAN ID

Displays the VLAN identifier value or range for this rule.

COS

Displays the COS (802.1p) value for this rule.

Secondary VLAN

Displays the Secondary VLAN identifier value or range for this rule.This field is contained in the inner tag of a double VLAN-tagged packet.

Secondary COS

Displays the Secondary COS (802.1p) value for this rule. This field is contained in the inner tag of a double VLAN-tagged packet.

Assign Queue

Displays the 802.1p user priority to which packets matching this rule are assigned.

Redirect Interface

Displays the slot/port to which packets matching this rule are forwarded.

10.2 IP ACL Commands

IP Access Control Lists (ACLs) ensure that only authorized users have access to specific resources while blocking off any unwarranted attempts to reach network resources.

Note:

- IP ACL configuration for IP packet fragments is not supported.
- ACLs are supported in the inbound direction only.
- The maximum number of ACLs of any type that can be created is 100.
- The maximum number of rules per IP ACL is 10.
- The maximum number of rules per interface is 20 (100 for Software Version L3P).
- ACLs are configured separately for Layer 2 and Layer 3/Layer 4 and cannot be applied to the same interface. (PowerMICE and MACH4000 without MACH4002-24G.../MACH4002-48G...)
- ACLs are configured separately for Layer 2 and Layer 3/Layer 4 and can be applied to the same interface. (MACH4002-24G.../MACH4002-48G...)
- Wildcard masking for IP ACLs (srcmask, dstmask) operates differently from a subnet mask. A wildcard mask is in essence the inverse of a subnet mask. With a subnet mask, the mask has ones (1's) in the bit positions that are used for the network address, and has zeros (0's) for the bit positions that are not used. In contrast, a wildcard mask has (0’s) in a bit position that must be checked. A ‘1’ in a bit position of the ACL mask indicates the corresponding bit can be ignored. The mask for the TOS value (tosmask) uses the common notation, i.e. the mask has ones (1's) in the bit positions that must be checked.

10.2.1 access-list

Note: This command is available for the devices of the MACH4000 family, for the PowerMICE devices and for the MACH1040 devices.

This command creates an IP Access Control List (ACL) that is identified by the parameter <*accesslistnumber*>.
The IP ACL number (<*accesslistnumber*>) is an integer from 1 to 199. The <*accesslistnumber*> range 1 to 99 is for an IP standard ACL and the <*accesslistnumber*> range 100 to 199 is for an IP extended ACL.
The IP ACL rule is specified with either a *permit or deny* action.
The protocol to filter for an IP ACL rule is specified by giving the protocol to be used like i*cmp, igmp, ip, tcp, udp.*
The command specifies a source ipaddress and source mask for match condition of the IP ACL rule specified by the *srcip* and *srcmask* parameters.
The source layer 4 port match condition for the IP ACL rule is specified by the *port value* parameter. The range of values is from 0 to 65535. The <*startport*> and <*endport*> parameters identify the first and last ports that are part of the port range. They have values from 0 to 65535. The ending port must have a value equal or greater than the starting port. The starting port, ending port, and all ports in between will be part of the destination port range.
The <*portvalue*> parameter uses a single keyword notation and currently has the values of *domain, echo, ftp, ftpdata, http, smtp, snmp, telnet, tftp*, and *www*. Each of these values translates into its equivalent port number, which is used as both the start and end of a port range.
The command specifies a destination ipaddress and destination mask for match condition of the IP ACL rule specified by the *dstip* and *dstmask* parameters.
The command specifies the TOS for an IP ACL rule depending on a match of precedence or DSCP values using the parameters *dscp, precedence*, *tos/tosmask*.
The assign-queue parameter allows specification of a particular 802.1p user priority for traffic that matches this rule. The allowed <*queue-id*> value is 0-7. The matching traffic is transmitted with the modified 802.1p user priority and also with modified IP-DSCP value for IP frames.
The command specifies the redirect interface which is the slot/port to which packets matching this rule are forwarded.

Default

none

(IP Standard ACL)

Format

```
access-list <1-99>
  {deny | permit}
  {every | <srcip> <srcmask>}
  [assign-queue <queue-id>] |
                            [redirect <slot/port>]
```

Mode

```
Global Config
```

(IP Extended ACL)

Format

```
access-list <100-199>
  {deny | permit}
  {every | icmp | igmp | ip | tcp | udp | <number>}
  {<srcip> <srcmask> | any}
  [{eq {<portkey> | <portvalue>}]]
  {<dstip> <dstmask> | any}
  [{eq {<portkey>|  <portvalue>}] |
  [precedence <precedence> | tos <tos> <tosmask> |
   dscp <dscp>] | [assign-queue <queue-id>] |
  [redirect <slot/port>]}}
```

Mode

```
Global Config
```

no access-list

This command deletes an IP ACL that is identified by the parameter <*accesslistnumber*> from the system.

Format

```
no access-list <accesslistnumber>
```

Mode

```
Global Config
```

accesslistnumber

```
Vaild range: 1-99, 100-199
```

10.2.2 access-list fragments

Note: This command is available for the devices of the MACH104 and MACH1040 family and for the MACH4002-24G... and MACH4002-48G... devices.

This command enables IP fragments processing.

Default

```
none
```

Format

```
access-list fragments
```

Modes

```
Global Config
```

no access-list fragments

This command disables IP fragments processing.

Default

```
none
```

Format

```
no access-list fragments
```

Mode

```
Global Config
```

10.2.3 ip access-group

Note: This command is available for the devices of the MACH4000 family and for the PowerMICE devices.

This command attaches a specified IP ACL to one interface or to all interfaces.
An optional sequence number may be specified to indicate the order of this IP access list relative to other IP access lists already assigned to this interface. A lower number indicates higher precedence order. If a sequence number is already in use for this interface, the specified access list replaces the currently attached IP access list using that sequence number. If the sequence number is not specified for this command, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used.

Default

none

Format

ip access-group *<accesslistnumber> in> [<1-4294967295>]*

Modes

Interface Config

Global Config

accesslistnumber

Enter the ACL ID in the range of 1 to 199.

<1-4294967295>

Enter the sequence number (greater than 0) to rank precedence for this interface and direction. A lower sequence number has higher precedence.

no ip access-group

This command removes a specified IP ACL from an interface.

Default

none

Format

no ip access-group <*accesslistnumber*> <in>

Mode

Interface Config
Global Config

accesslistnumber

Enter the ACL ID in the range of 1 to 199.

10.2.4 show ip access-lists

Note: This command is available for the devices of the MACH4000 family and for the PowerMICE devices.

This command displays an IP ACL.
<*accesslistnumber*> is the number used to identify the IP ACL.

Format

show ip access-lists <*accesslistnumber*>

Modes

Privileged EXEC

accesslistnumber

Enter the ACL ID in the range of 1 to 199.

Rule Number

This displays the number identifier for each rule that is defined for the IP ACL.

Action

This displays the action associated with each rule. The possible values are permit or deny.

Protocol

This displays the protocol to filter for this rule.

Source IP Address

This displays the source IP address for this rule.

Source IP Mask

This field displays the source IP Mask for this rule.

Source L4 Port

This field displays the source port for this rule.

Destination IP Address

This displays the destination IP address for this rule.

Destination IP Mask

This field displays the destination IP Mask for this rule.

Destination L4 Port

This field displays the destination port for this rule.

Service Type Field Match

This field indicates whether an IP DSCP, IP Precedence, or IP TOS match condition is specified for this rule.

Service Type Field Value

This field indicates the value specified for the Service Type Field Match (IP DSCP, IP Precedence, or IP TOS).

10.2.5 show access-lists global

Note: This command is available for the devices of the MACH104 and MACH1040 family and for the MACH4002-24G... and MACH4002-48G... devices.

This command displays global access list information.

Format

```
show access-lists global
```

Modes

```
Privileged EXEC
```

L4 Fragment Processing

```
This field displays the status of IP fragments
processing.
Possible values: Enabled, Disabled.
```

10.2.6 show access-lists

Note: This command is available for the devices of the MACH4000 family and for the PowerMICE devices.

This command displays IP ACLs and MAC access control lists information for a designated interface and direction.

Format

`show access-lists interface <slot/port> <in>`

Modes

`Privileged EXEC`

ACL Type

`Type of access list (IP or MAC).`

ACL ID

`Access List name for a MAC access list or the numeric identifier for an IP access list.`

Sequence Number

`An optional sequence number may be specified to indicate the order of this access list relative to other access lists already assigned to this interface and direction. A lower number indicates higher precedence order. If a sequence number is already in use for this interface and direction, the specified access list replaces the currently attached access list using that sequence number. If the sequence number is not specified by the user, a sequence number that is one greater than the highest sequence number currently in use for this interface and direction is used. Valid range is (1 to 4294967295).`

10.3 CoS Commands

This chapter provides a detailed explanation of the QoS Class of Service (CoS) commands. The following commands are available.
The commands are divided into these different groups:

- Configuration Commands are used to configure features and options of the switch. For every configuration command there is a show command that will display the configuration setting.
- Show commands are used to display device settings, statistics and other information.

Note: The 'Interface Config' mode only affects a single interface, whereas the 'Global Config' mode is applied to all interfaces.

10.3.1 cos-queue max-bandwidth

This command specifies the maximum transmission bandwidth limit for each interface queue. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmitted traffic rate is bounded. The switch supports 8 queues per interface. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no maximum bandwidth is in effect.

Format

```
cos-queue max-bandwidth <bw-0> <bw-1> ... <bw-n>
```

Modes

```
Global Config
Interface Config (not MACH 4002 24G/48G)
```

<bw-n>

```
Enter the minimum bandwidth percentage for Queue n.
Valid range: n = 0 ...7.
```

no cos-queue max-bandwidth

This command restores the default for each queue's maximum bandwidth value.

Format

```
no cos-queue max-bandwidth
```

Mode

```
Global Config
Interface Config (not MACH 4002 24G/48G)
```

10.3.2 cos-queue min-bandwidth

This command specifies the minimum transmission bandwidth guarantee for each interface queue. The switch supports 8 queues per interface. A value from 0-100 (percentage of link rate) must be specified for each supported queue, with 0 indicating no guaranteed minimum bandwidth. The sum of all values entered must not exceed 100.

Format

```
cos-queue min-bandwidth <bw-0> <bw-1> ... <bw-n>
```

Modes

```
Global Config
Interface Config (not MACH 4002 24G/48G)
```

<bw-n>

```
Enter the minimum bandwidth percentage for Queue n.
Valid range: n = 0 ...7.
```

no cos-queue min-bandwidth

This command restores the default for each queue's minimum bandwidth value.

Format

```
no cos-queue min-bandwidth
```

Modes

```
Global Config
Interface Config (not MACH 4002 24G/48G)
```

10.3.3 cos-queue strict

This command activates the strict priority scheduler mode for each specified queue. A queue cannot be a member of a queuing algorithm higher than its next higher priority queue. That is, any strict priority queue must start at class 7 and be consecutive.

Format

```
cos-queue strict <queue-id-1> [<queue-id-2> ...
<queue-id-n>]
```

Modes

```
Global Config
Interface Config (not MACH 4002 24G/48G)
```

<queue-id-n>

```
Enter a Queue Id from 0 to 7.
```

no cos-queue strict

This command activates the weighted round robin (WRR) scheduler mode for each specified queue. A queue cannot be a member of a queuing algorithm lower than its next lowe priority queue. That is, any WRR queue must start at class 0 and be consecutive.

Format

```
no cos-queue strict <queue-id-1> [<queue-id-2> ...
<queue-id-n>]
```

Modes

```
Global Config
Interface Config (not MACH 4002 24G/48G)
```

<queue-id-n>

```
Enter a Queue Id from 0 to 7.
```

10.3.4 traffic-shape

This command specifies the maximum transmission bandwith limit for the interface as a whole. Also known as rate shaping, this has the effect of smoothing temporary traffic bursts over time so that the transmission traffic rate is bounded. A value from 0-100 (percentage of link rate) must be specified, with 0 indicating no traffic shaping is in effect. When interface shaping is enabled on a port which has some queues in WRR group, then the minimum bandwith configuration of the weighted queues is not honored.

Format

```
traffic-shape <bw>
```

Modes

```
Global Config
Interface Config
```

<bw>

```
Enter the shaping bandwidth percentage from 0 to
100 in increments of 5.
```

no traffic-shape

This command disables the traffic shaping.

Format

```
no traffic-shape
```

Modes

```
Global Config
Interface Config
```

10.3.5 show interfaces cos-queue

This command displays the class-of-service queue configuration for the specified interface. The slot/port parameter is optional. If specified, the class-

of-service queue configuration of the interface is displayed. If omitted, the most recent global configuration settings are displayed.

Format

```
show interfaces cos-queue [slot/port]
```

Mode

```
Privileged EXEC
```

Interface

```
This displays the slot/port of the interface. If
displaying the global configuration, this line is
replaced by a Global Configuration indication.
```

Intf Shaping Rate

```
The maximum transmission bandwidth limit for the
interface as a whole. It is independent of any per-
queue maximum bandwidth value(s) in effect for the
interface. This is a configured value.
```

The following information is repeated for each queue on the interface.

Queue Id

```
An interface supports 8 queues numbered 0 to 7.
```

Minimum Bandwidth

```
The minimum transmission bandwidth guarantee for
the queue, expressed as a percentage. A value of 0
means bandwidth is not guaranteed and the queue
operates using best-effort. This is a configured
value.
```

Maximum Bandwidth

```
The maximum transmission bandwidth limit for the
queue, expressed as a percentage. A value of 0
means no upper limit is enforced, so the queue may
use any or all of the available bandwidth of the
interface. This is a configured value.
```

Scheduler Type

```
Indicates whether this queue is scheduled for
transmission using a strict priority or a weighted
scheme. This is a configured value.
```

11 Protocol-based VLAN Commands

This chapter provides a detailed explanation of the protocol-based VLAN commands.

11.1 Show Commands

11.1.1 show port protocol

This command displays the Protocol-Based VLAN information for either the entire system, or for the indicated Group.

Format

```
show port protocol {<groupid> | all}
```

Mode

```
Privileged EXEC
```

Group Name

```
This field displays the group name of an entry in
the Protocol-based VLAN table.
```

Group ID

```
This field displays the group identifier of the
protocol group.
```

Protocol(s)

```
This field indicates the type of protocol(s) for
this group.
```

VLAN

```
This field indicates the VLAN associated with this
Protocol Group.
```

Interface(s)

```
This field lists the slot/port interface(s) that
are associated with this Protocol Group.
```

11.2 Configuration Commands

11.2.1 vlan protocol group

This command adds protocol-based VLAN group to the system. The <*groupName*> is a character string of 1 to 16 characters. When it is created, the protocol group will be assigned a unique number that will be used to identify the group in subsequent commands.

Format

```
vlan protocol group <groupname>
```

Mode

```
Global Config
```

11.2.2 vlan protocol group add protocol

This command adds the <protocol> to the protocol-based VLAN identified by <groupid>. A group may have more than one protocol associated with it. Each interface and protocol combination can only be associated with one group. If adding a protocol to a group causes any conflicts with interfaces currently associated with the group, this command will fail and the protocol will not be added to the group. The possible values for protocol are *ip*, *arp*, and *ipx*.

Default

none

Format

vlan protocol group add protocol <groupid> <protocol>

Mode

Global Config

no vlan protocol group add protocol

This command removes the <*protocol*> from this protocol-based VLAN group that is identified by this <*groupid*>. The possible values for protocol are *ip*, *arp*, and *ipx*.

Format

no vlan protocol group add protocol <groupid> <protocol>

Mode

Global Config

11.2.3 vlan protocol group remove

This command removes the protocol-based VLAN group that is identified by this <groupid>.

Format

```
vlan protocol group remove <groupid>
```

Mode

```
Global Config
```

11.2.4 protocol group

This command attaches a <vlanid> to the protocol-based VLAN identified by <groupid>. A group may only be associated with one VLAN at a time, however the VLAN association can be changed.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

Default

```
none
```

Format

```
protocol group <groupid> <vlanid>
```

Mode

```
VLAN database
```

no protocol group

This command removes the <vlanid> from this protocol-based VLAN group that is identified by this <*groupid*>.

Format

```
no protocol group <groupid> <vlanid>
```

Mode

```
VLAN database
```

11.2.5 protocol vlan group

This command adds the physical <slot/port> interface to the protocol-based VLAN identified by <groupid>. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

Default

```
none
```

Format

```
protocol vlan group <groupid>
```

Mode

```
Interface Config
```

no protocol vlan group

This command removes the <interface> from this protocol-based VLAN group that is identified by this <groupid>. If <all> is selected, all ports will be removed from this protocol group.

Format

```
no protocol vlan group <groupid>
```

Mode

```
Interface Config
```

11.2.6 protocol vlan group all

This command adds all physical interfaces to the protocol-based VLAN identified by <groupid>. A group may have more than one interface associated with it. Each interface and protocol combination can only be associated with one group. If adding an interface to a group causes any conflicts with protocols currently associated with the group, this command will fail and the interface(s) will not be added to the group.

The referenced VLAN should be created prior to the creation of the protocol-based VLAN except when GVRP is expected to create the VLAN.

Default

```
none
```

Format

```
protocol vlan group all <groupid>
```

Mode

```
Global Config
```

no protocol vlan group all

This command removes all interfaces from this protocol-based VLAN group that is identified by this <groupid>.

Format

```
no protocol vlan group all <groupid>
```

Mode

```
Global Config
```

12 Index

Symbols

{deny|permit} 819

Numerics

1583compatibility 678

A

access-list 825
access-list fragments 827
addport 191
address-conflict 309
adminmode 192
arc 479
area default-cost 678
area nssa 679
area nssa default-info-originate 679
area nssa no-redistribute (OSPF) 680
area nssa no-summary (OSPF) 680
area nssa translator-role (OSPF) 680
area nssa translator-stab-intv 681
area range 681
area stub 682
area stub summarylsa 683
area virtual-link 684
area virtual-link authentication 685
area virtual-link dead-interval 686
area virtual-link hello-interval 687
area virtual-link retransmit-interval 688
area virtual-link transmit-delay 689
areaid 36
ARP
- aging 597
- cache, displaying 598, 600
- response time 594
- retries 595

arp 590
arp cachesize 590, 592
arp dynamicrenew 593
arp purge 593
arp resptime 594
arp retries 595
arp selective-learning 596
arp timeout 597
authentication login 533
authorization network radius 535
auto-disable reason 193
auto-disable reset 195
auto-disable timer 195
auto-negotiate 196
auto-negotiate all 197
auto-summary 727

B

boot skip-aca-on-boot 310, 310
bridge address-learning 118
bridge address-relearn detect operation 119
bridge address-relearn detect threshold 119
bridge aging-time 120
bridge duplex-mismatch-detect operation 121
bridge fast-link-detection 121
bridge framesize 70
bridge vlan-learning 122
broadcasts
- broadcast storm recovery mode 274, 275, 277
- broadcast storm trap 765, 798

C

cable-crossing 198
cablestatus 311
classofservice dot1pmapping 102
classofservice ip-dscp-mapping 103
classofservice trus 104
clear arp-cache 597
clear arp-table-switch 312
clear commands
- clear arp-table-switch 312
- clear config 313
- clear pass 315
- clear traplog 316, 317
- clear vlan 317

clear config 313
clear config factory 313
clear counters 313
clear dot1x statistics 535
clear eventlog 311
clear hiper-ring 314
clear igmpsnooping 314
clear inlinepower 419
clear link-aggregation 316
clear lldp config all 357
clear mac-addr-table 315
clear pass 315
clear port-sec 506
clear radius statistics 536
clear ring-coupling 317
clear sfp-white-list 326
clear signal-contact 316

clear traplog 317
clear vlan 317
Competence Center 877
config commands
config arp agetime 597
config arp resptime 594
config arp retries 595
config lags adminmode 212
config lags linktrap 213
config lags name 214
config loginsession 298
config port admin-mode 267, 268
config port linktrap 269, 270, 271
config port physical-mode 273
config switchconfig broadcast 274, 275, 277
config switchconfig flowcontrol 278, 279
config trapflags bcaststorm 765, 798
config users add 303, 304
config users delete 302, 303, 304
config users passwd 305
config vlan add 280
config vlan delete 280
config vlan garp jointime 214, 215, 216, 217, 218, 219, 220
config vlan garp leavealltime 222
config vlan garp leavetime 221
config vlan interface acceptframe 282, 283, 288
config vlan name 285
config vlan participation 286, 287
config vlan ports ingressfilter 284, 289
config vlan ports pvid 290, 292
config vlan ports tagging 291, 293
config port autoneg 214
Config router ospf adminmode 676
Config router ospf area externrouting 678
Config router rip adminmode 727, 730, 735, 737, 738
Config router rip interface defaultmetric 726, 732, 733
Config router rip interface version receive 726
Config router rip interface version send 734
config switchconfig flowcontrol 278, 279
config users delete 302, 303, 304, 305
config users passwd 302, 303, 304, 305
config vlan delete 280
config vlan ports acceptframe 292
config vlan ports ingressfilter 283, 288, 289, 290, 842
configuration reset 313
config-watchdog 318
copy 318
copy nvram clibanner 324
copy nvram startup-config 326
copy system bootcode 326
copy system image 326
copy system running-config 326
copy nvram capture 321
copy nvram capture aca capture 321
copy nvram clibanner 321
copy nvram errorlog 322
copy nvram script 322
copy nvram traplog 323
copy system running-config 323
copy tftp/// nvram httpscert 321
cos-queue max-bandwidth 834
cos-queue min-bandwidth 835
cos-queue strict 836

D

debug tcpdump filter delete 99
debug tcpdump filter list 98
debug tcpdump filter show 98
debug tcpdump help 96
debug tcpdump start cpu 96
debug tcpdump start cpu filter 97
debug tcpdump stop 97
default-information originate (OSPF) 690, 728
default-metric (OSPF) 691
default-metric (RIP) 729
deleteport 200
deleteport all 200
device configuration commands 201
device-status connection-error 327
device-status monitor 328
DHCP server configuration example 512
dhcp-relay 508, 509
dhcp-server addr-probe 516
dhcp-server operation 517
dhcp-server pool add 517
dhcp-server pool delete 522
dhcp-server pool disable 522
dhcp-server pool enable 522
dhcp-server pool modify hirschmann-device 521
dhcp-server pool modify mode 518
dhcp-server pool modify option 520
dhcp-server pool modify leasetime 521
digital-input 122
digital-output 124
dip-switch operation 201
disable ip multicast mdebug mtrace 748

disconnect 298
distance ospf 692
distance rip 730
distribute-list out 693, 731
dot1x defaultlogin 536
dot1x dynamic-vlan enable 537
dot1x guest-vlan 538
dot1x initialize 539
dot1x login 539
dot1x mac-auth-bypass 540
dot1x max-req 541
dot1x max-users 542
dot1x port-control 543
dot1x port-control all 544
dot1x re-authenticate 545
dot1x re-authentication 545
dot1x safe-vlan 546
dot1x system-auth-control 547
dot1x timeout 547
dot1x user 551
duplex settings 273
dvlan-tunnel ethertype 108

E

enable (OSPF) 676
enable (RIP) 725
ethernet-ip 135
exit-overflow-interval 694
external-lsdb-limit 695

F

fast-hiper-ring 490
flow control 278, 279
frame acceptance mode 282, 283, 288

G

Global Config Mode 58
GVRP
join time 214, 215, 216, 217, 218, 219, 220
leave time 221

H

hiper-ring 484
hiper-ring mode 484
hiper-ring port primary 485
hiper-ring port secondary 485
hiper-ring recovery-delay 486
hostroutesaccept 735

I

IEEE 802.1Q 282, 283, 288
ingress filtering 284, 289
inlinepower (Global Config) 417
inlinepower (Interface Config) 418
inlinepower budget slot 421
inlinepower threshold slot 422
inlinepower trap slot 422
Interface Config Mode 59
inventory 244, 245, 246, 248, 249, 250, 252, 253, 533, 745, 746, 747, 748, 749, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 763, 764, 766, 767, 768, 769, 770, 771, 772, 773, 775, 776, 777, 778, 779, 780, 781, 782, 784, 788, 790, 791, 792, 793, 794, 795, 796, 797, 829, 831, 832, 840
ip access-group 828
ip address 605
ip dvmrp 763, 766
ip dvmrp metric 764
ip dvmrp trapflags 765
ip forwarding 612
ip http secure-port 575
ip http secure-protocol 575
ip http server 575
ip https certgen 578
ip https port 578
ip https server 577
ip igmp 773
ip igmp last-member-query-count 775
ip igmp last-member-query-interval 776
ip igmp query-interval 777
ip igmp query-max-response-time 778
ip igmp robustness 779
ip igmp startup-query-count 780
ip igmp startup-query-interval 781
ip igmp version 774
ip irdp 634
ip irdp address 635
ip irdp holdtime 636
ip irdp maxadvertinterval 637
ip irdp minadvertinterval 638
ip irdp preference 639
ip mcast boundary 744
ip mtu 606
ip multicast 745
ip multicast staticroute 746
ip multicast ttl-threshold 747
ip netdirbcast 607
ip ospf 677
ip ospf areaid 696
ip ospf authentication 697
ip ospf cost 698
ip ospf dead-interval 699
ip ospf hello-interval 700
ip ospf mtu-ignore 704
ip ospf priority 701
ip ospf retransmit-interval 702

ip ospf transmit-delay 703
ip pimdm 790
ip pimdm hello-interval 793
ip pimdm holdtimes 791
ip pimdm mode 792
ip pim-trapflags 798
ip proxy-arp 591
ip rip 726
ip rip authentication 732
ip rip receive version 733
ip rip send version 734
ip route default 610
ip route distance 611
ip routing 604
ip ssh protocol 552
ip table-sizes 615
ip table-sizes arp-entries 616
ip table-sizes multicast-routes 618
ip table-sizes unicast-routes 617
ip vlan-single-mac 613
ip vrrp 653, 656
ip vrrp advertisement-address 664
ip vrrp authentication 659
ip vrrp delay-preemption 661
ip vrrp domain 667
ip vrrp domain send-member-advertisements 654
ip vrrp ip 658
ip vrrp link-down-notification 665
ip vrrp mode 657
ip vrrp preempt 660
ip vrrp priority 662
ip vrrp tap 655
ip vrrp timers advertise 663
ip vrrp timers advertise milliseconds 663
ip vrrp track 666
ipaddr 36

J

join time 214, 215, 216, 217, 218, 219, 220

L

LAGs
- enabling or disabling 212
- link traps 213
- name 214
- summary information 257

leave time 221, 222
Line Config Mode 59
Link Aggregation(802.3ad) Commands 112
link aggregations. See LAGs
link traps
- interface 269, 270, 271
- LAG 213

link-aggregation 211
link-aggregation adminmode 212
link-aggregation linktrap 213
link-aggregation name 214
link-aggregation staticcapability 112
lldp 353
LLDP - Link Layer Discovery Protocol 341
lldp admin-state 357
lldp chassis tx-interval 356
lldp config chassis admin-state 354
lldp config chassis notification-interval 354
lldp config chassis re-init-delay 355
lldp config chassis tx-delay 355
lldp config chassis tx-hold-mult 356
lldp fdb-mode 358
lldp hm-mode 358
lldp max-neighbors 359
lldp med 360
lldp med al 361
lldp med confignotification 361
lldp med confignotification all 362
lldp med faststartrepeatcount 363
lldp med transmit-tlv 364
lldp med transmit-tlv all 365
lldp notification 366
lldp tlv gmrp 369
lldp tlv igmp 369
lldp tlv link-aggregation 366
lldp tlv mac-phy-config-state 366
lldp tlv max-frame-size 367
lldp tlv mgmt-addr 367
lldp tlv pnio 367
lldp tlv pnio-alias 368
lldp tlv pnio-mrp 368
lldp tlv port-desc 368
lldp tlv portsec 370
lldp tlv port-vlan 369
lldp tlv protocol 370
lldp tlv ptp 370
lldp tlv sys-cap 371
lldp tlv sys-desc 371
lldp tlv sys-name 371
lldp tlv vlan-name 372
logging buffered 178
logging buffered wrap 179
logging cli-command 180
logging console 181
logging host 182
logging host reconfigure 183
logging host remove 183
logging snmp-requests get operation 183
logging snmp-requests get severity 184
logging snmp-requests set operation 184
logging snmp-requests set severity 185

logging syslog 186
logging syslog port 186
logout 329
logout command 329

M

mac access-group 821
mac access-list extended 817
mac access-list extended rename 818
mac notification (Global Config) 205
mac notification (Interface Config) 206
macaddr 36
mac-address conflict 329
macfilter 202
macfilter adddest 203
macfilter adddest all 204
maximum-paths 706
media-module 199
media-module remove 199
mode dvlan-tunnel 110
monitor session 207
monitor session mode 209
monitor session source/destination 210
mrinfo 749
mrp current-domain 476
mrp delete-domain 478
mrp new-domain 478
mstat 750
mtrace 751

N

name 372
network javascriptmode 136
network mgmt_vlan 100
network mgmt-access add 136
network mgmt-access delete 136
network mgmt-access modify 137
network mgmt-access operation 138
network mgmt-access status 139
network parms 139
network priority 141
network protocol 140
no dhcp-relay 508
no ip access-group 827, 829
no ip mcast mroute 752
no ip vrrp advertisement-address 664
no ip vrrp mode 657
no ip vrrp tap 655
no ip vrrp track 666
no lldp 353
no sntp 378
no sntp anycast address 379, 380, 386
no sntp client server 382
no sntp client server primary 383, 384, 385
no storm-control broadcast 274
no track mode 644, 645

P

passwords
changing user 305
resetting all 315
PDUs 214, 215, 216, 217, 218, 219, 220, 222
ping 330
ping command 327, 328, 330
PoE - Power over Ethernet 413
Port monitor 423
port-monitor (Global Config) 430
port-monitor (Interface Config) 430
port-monitor action 431
port-monitor condition crc-fragment (Global Config) 433
port-monitor condition crc-fragment (Interface Config) 434
port-monitor condition link-flap (Global Config) 432
port-monitor condition link-flap (Interface Config) 432
port-monitor condition speed-duplex-monitor (Interface Config) 434
port-monitor condition speed-duplex-monitor clear (Interface Config) 435
port-monitor condition speed-duplex-monitor speed (Interface Config) 435
ports
administrative mode 267, 268
frame acceptance mode 282, 283, 288
information 256
ingress filtering 284, 289
link traps 269, 270, 271
physical mode 273
tagging 291, 293
VLAN IDs 290, 292
VLAN information 264
port-sec action 502
port-sec allowed-ip 503
port-sec allowed-ip add 503
port-sec allowed-ip remove 504
port-sec allowed-mac 504
port-sec allowed-mac add 505
port-sec allowed-mac remove 505
port-sec dynamic 506
port-sec mode 501
Privileged Exec Mode 58
profinetio 142
Protocol Data Units. See PDUs
protocol group 843
protocol vlan group 844

protocol vlan group all 845
PTP - Precision Time Protocol 388
ptp clock-mode 394
ptp operation 395
ptp sync-lower-bound 395
ptp sync-upper-bound 396
ptp v1 burst 402
ptp v1 operation 402
ptp v1 preferred-master 396
ptp v1 re-initialize 397
ptp v1 subdomain-name 397
ptp v1 sync-interval 398
ptp v2bc announce-interval 403
ptp v2bc announce-timeout 404
ptp v2bc asymmetry 406
ptp v2bc delay-mechanism 404
ptp v2bc domain 400
ptp v2bc network-protocol 405
ptp v2bc operation 403
ptp v2bc pdelay-interval 405
ptp v2bc priority1 399
ptp v2bc priority2 399
ptp v2bc sync-interval 404
ptp v2bc utc-offset 400
ptp v2bc utc-offset-valid 400
ptp v2bc v1-compatibility-mode 405
ptp v2bc vlan 401
ptp v2bc vlan-priority 401
ptp v2tc asymmetry 406
ptp v2tc delay-mechanism 406
ptp v2tc management 407
ptp v2tc multi-domain-mode 407
ptp v2tc network-protocol 408
ptp v2tc operation 408
ptp v2tc pdelay-interval 409
ptp v2tc power-tlv-check 411
ptp v2tc primary-domain 409
ptp v2tc profile 410
ptp v2tc sync-local-clock 412
ptp v2tc syntonization 410
ptp v2tc vlan 411
ptp v2tc vlan-priority 412

R

radius accounting mode 553
radius server host 553
radius server key 555
radius server msgauth 555
radius server primary 556
radius server retransmit 557
radius server timeout 558
reboot 333
redistribute 736
redistribute (RIP) 705
reload 335
reset system command 333, 335
response time 594
retries 595
ring-coupling 495
ring-coupling config 496
ring-coupling net-coupling 497
ring-coupling operation 497
ring-coupling port 498
ring-coupling redundancy-mode 498
rmon-alarm add 214
rmon-alarm delete 215
rmon-alarm disable 216
rmon-alarm enable 215
rmon-alarm modify falling-event 219
rmon-alarm modify interval 217
rmon-alarm modify mib-variable 216
rmon-alarm modify rising-event 219
rmon-alarm modify sample-type 218
rmon-alarm modify startup-alarm 218
rmon-alarm modify thresholds 217
Router Config RIP Mode 59
router-id 704
routing 603

S

Schulungsangebot 877
script apply 187
script delete 188
script list 188
script show 189
script validate 189
selftest ramtest 239
selftest reboot-on-error 240
serial timeout 143
serviceshell 241
session-limit 117
sessions
  closing 298, 329
  displaying 299
session-timeout 118
set cli banner 337
set garp timer join 220
set garp timer leave 221
set garp timer leaveall 222
set gmrp adminmode 223
set gmrp forward-all-groups 226
set gmrp forward-unknown 227
set gmrp interfacemode 224, 225
set igmp 228, 229
set igmp aging-time-unknown 229
set igmp automatic-mode 230
set igmp forward-all 231

set igmp forward-unknown 232
set igmp groupmembershipinterval 233
set igmp interfacemode 234
set igmp lookup-interval-unknown 235
set igmp lookup-resp-time-unknown 235
set igmp maxresponse 236
set igmp querier max-response-time 237
set igmp querier protocol-version 237
set igmp querier status 238
set igmp querier tx-interval 238
set igmp query-ports-to-filter 239
set igmp static-query-port 232
set pre-login-banner text 239
set pro-login-banner banner 339
set prompt 143
show 66
show access-lists 832
show access-lists global 831
show address-conflict 66
show arc 480
show arp 598
show arp brief 600
show arp switch 67, 73, 601
show authentication 72, 561
show authentication users 562
show auto-disable brief 242
show auto-disable reasons 243
show boot skip-aca-on-boot 310, 310
show bridge address-learning 67
show bridge address-relearn-detect 68
show bridge aging-time 68
show bridge duplex-mismatch-detect 69
show bridge fast-link-detection 69
show bridge framesize 69
show bridge vlan-learning 70
show classofservice dot1pmapping 105
show classofservice ip-dscp-mapping 106
show classofservice trust 107
show commands
show arp table 598, 600
show inventory 244, 245, 246, 248, 249, 250, 252, 253, 533, 745, 746, 747, 748, 749, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 763, 764, 766, 767, 768, 769, 770, 771, 772, 773, 775, 776, 777, 778, 779, 780, 781, 782, 784, 788, 790, 791, 792, 793, 794, 795, 796, 797, 829, 831, 832, 840
show lags summary 257
show loginsession 299
show port 256
show stats switch detailed 74, 76, 82
show switchconfig 258, 259, 260
show users 300
show vlan detailed 261
show vlan interface 264
show vlan summary 263
show config-watchdog 71
show device-status 71
show dhcp-relay 508, 510
show dhcp-server 514
show dhcp-server operation 515
show dhcp-server pool 516
show dhcp-server port 515
show digital-input 127, 130
show digital-input all 129
show digital-input config 128
show digital-output 131, 134
show digital-output all 133
show digital-output config 132
show dip-switch 244
show dot1x 562
show dot1x clients 568
show dot1x users 567
show dvlan-tunnel 111
show ethernet-ip 144, 147
show eventlog 73
show fast-hiper-ring 488
show garp 245
show gmrp configuration 245
show hiper-ring 483
show hiper-ring info 484
show igmpsnooping 246
show inlinepower 413
show inlinepower port 414
show inlinepower slot 420
show interface 74
show interface ethernet 76
show interface switchport 83
show interface utilization 84
show interfaces cos-queue 837
show inventory 284
show ip access-lists 829
show ip brief 614
show ip dvmrp 767
show ip dvmrp interface 768
show ip dvmrp neighbor 769
show ip dvmrp nexthop 770
show ip dvmrp prune 771
show ip dvmrp route 772
show ip http 576
show ip https 579
show ip igmp 782
show ip igmp groups 782
show ip igmp interface 784
show ip igmp interface stats 788

show ip interface 619
show ip interface brief 621
show ip irdp 639
show ip mcast 753
show ip mcast boundary 754
show ip mcast interface 754
show ip mcast mroute 755
show ip mcast mroute group 756
show ip mcast mroute source 757
show ip mcast mroute static 758
show ip ospf 707
show ip ospf area 710
show ip ospf database 711
show ip ospf interface 713
show ip ospf interface brief 715
show ip ospf interface stats 716
show ip ospf neighbor 717
show ip ospf neighbor brief 720
show ip ospf range 721
show ip ospf stub table 722
show ip ospf virtual-link 723
show ip ospf virtual-link brief 724
show ip pimdm 794
show ip pimdm interface 795
show ip pimdm interface stats 796
show ip pimdm neighbor 797
show ip rip 738
show ip rip interface brief 740
show ip route 622
show ip route bestroutes 623
show ip route entry 624
show ip route preferences 625
show ip route static 626
show ip ssh 569
show ip stats 627
show ip vlan 643
show ip vrrp 670
show ip vrrp domain 671
show ip vrrp interface 672
show ip vrrp interface brief 674
show ip vrrp interface stats 668
show link-aggregation 257
show link-aggregation brief 113
show lldp 341
show lldp chassis tx-interval 344
show lldp config 341
show lldp config chassis 342
show lldp config chassis admin-state 342
show lldp config chassis notification-interval 342
show lldp config chassis re-init-delay 343
show lldp config chassis tx-delay 343
show lldp config chassis tx-hold-mult 343
show lldp config port 345
show lldp config port tlv 346
show lldp med 347
show lldp med interface 348
show lldp med local-device detail 349
show lldp med remote-device 350
show lldp med remote-device detail 351
show lldp remote-data 351
show logging 85
show loginsession 299, 306
show mac access-lists 822
show mac notification 253
show mac-address-conflict 86
show mac-addr-table 87
show mac-filter-table gmrp 248
show mac-filter-table igmpsnooping 249
show mac-filter-table multicast 250
show mac-filter-table static 251
show mac-filter-table staticfiltering 252
show mac-filter-table stats 253
show monitor session 255
show mrinfo 759
show mrp 474
show mrp current domain 475
show mstat 760
show mtrace 761
show network 120, 144
show network mgmt-access 146
show port 256, 278, 279
show port protocol 840
show port-monitor 424, 424
show port-monitor brief 426
show port-monitor crc-fragment 427
show port-monitor link-flap 427
show port-monitor speed-duplex 429
show port-sec dynamic 499
show port-sec mode 500
show port-sec port 501
show ptp 388
show ptp configuration 391
show ptp operation 391
show ptp port 392
show ptp status 393
show radius 570
show radius accounting 558
show radius statistics 571
show reboot 334
show reload 336
show ring-coupling 493
show rmon-alarm 258
show router rip interface 741
show running-config 91
show selftest 259
show serial 147
show serviceshell 259

show signal-contact 88
show slot 90
show snmp sync 150
show snmp-access 148
show snmpcommunity 149
show snmptrap 151
show sntp 373
show sntp anycast 375
show sntp client 375
show sntp operation 376
show sntp server 377
show sntp status 377
show sntp time 378
show spanning-tree 439
show spanning-tree brief 440
show spanning-tree interface 442
show spanning-tree mst detailed 443
show spanning-tree mst port detailed 444
show spanning-tree mst port summary 447
show spanning-tree mst summary 448
show spanning-tree summary 449
show spanning-tree vlan 450
show storm-control 260
show storm-control limiters port 260
show sub-ring 523
show switchconfig 120
show sysinfo 92, 107, 108
show telnet 152
show telnetcon 153
show temperature 95
show track 647, 649
show track applications 651
show trapflags 154
show users 300
show users authentication 573
show vlan 261
show vlan brief 263
show vlan port 264
show voice vlan 265
show voice vlan interface 266
shutdown 267
shutdown all 268
signal-contact 331
signal-contact connection-error 330
slot/port 36
snmp sync community-to-v3 269
snmp trap link-status 270
snmp trap link-status all 271
snmp-access global 155, 156
snmp-access version v3-encryption 156
snmp-server 96, 158
snmp-server community 159
snmp-server community ipaddr 161
snmp-server community ipmask 162
snmp-server community mode 163
snmp-server community ro 164
snmp-server community rw 164
snmp-server contact 160
snmp-server enable traps 165
snmp-server enable traps linkmode 168
snmp-server enable traps multiusers 169
snmp-server enable traps port-sec 170
snmp-server enable traps stpmode 171
snmp-server location 164
snmp-server sysname 165
snmptrap 172
snmptrap ipaddr 173
snmptrap mode 174
snmptrap snmpversion 175
SNTP - Simple Network Time Protocol 373
sntp anycast address 379
sntp anycast transmit-interval 379
sntp anycast vlan 380
sntp client accept-broadcast 380
sntp client disable-after-sync 381
sntp client offset 381
sntp client request-interval 382
sntp client server primary 383
sntp client server secondary 384
sntp client threshold 385
sntp operation 386
sntp server disable-if-local 387
sntp time system 387
spanning-tree 451
spanning-tree auto-edgeport 452
spanning-tree bpduguard 453
spanning-tree bpdumigrationcheck 272
spanning-tree configuration name 454
spanning-tree configuration revision 455
spanning-tree edgeport 456
spanning-tree forceversion 457
spanning-tree forward-time 458, 460
spanning-tree guard loop 459
spanning-tree guard none 460
spanning-tree guard root 461
spanning-tree hello-time 462
spanning-tree hold-count 462
spanning-tree max-age 463
spanning-tree max-hops 464
spanning-tree mst 465
spanning-tree mst instance 469
spanning-tree mst priority 467
spanning-tree mst vlan 468
spanning-tree port mode 470
spanning-tree port mode all 471
spanning-tree stp-mrp-mode 472
spanning-tree tcnguard 473
speed 273

speeds 273
split-horizon 737
statistics
switch, related commands 74, 76, 82
storm-control broadcast 274
storm-control broadcast (port-related) 276
storm-control egress-limit 276
storm-control egress-limiting 274
storm-control flowcontrol 278
storm-control flowcontrol per port 279
storm-control ingress-limit 277
storm-control ingress-limiting 275
storm-control ingress-mode 275, 277
sub-ring mode 525
sub-ring mrp-domainID 529
sub-ring operation 526
sub-ring port 527
sub-ring protocol 526
sub-ring ring-name 527
sub-ring vlan 528
Sub-Ring Commands 523
sub-ring delete-ring 530
sub-ring new-ring 530
switch
information, related commands 258, 259, 260
inventory 244, 245, 246, 248, 249, 250, 252, 253, 533, 745, 746, 747, 748, 749, 752, 753, 754, 755, 756, 757, 758, 759, 760, 761, 763, 764, 766, 767, 768, 769, 770, 771, 772, 773, 775, 776, 777, 778, 779, 780, 781, 782, 784, 788, 790, 791, 792, 793, 794, 795, 796, 797, 829, 831, 832, 840
resetting 333, 335
statistics, related commands 74, 76, 82
System Information and Statistics Commands 100
System Utilities 309, 533
system utilities 309–330

T

tagging 291, 293
telnet 114
sessions, closing 298, 329
sessions, displaying 299
telnetcon maxsessions 176
telnetcon timeout 177
temperature 332
timeouts
ARP 597
traceroute 312
track interface 644
track logical 645
track mode 645
track ping 646
track trap 647
traffic-shape 837
transport input telnet 115
transport output telnet 116
trap flags
broadcast storm 765, 798
trap log
clearing 316, 317
trapflags 707
trunks. See LAGs

U

update module-configuration 241
update-timer 738
User Account Management Commands 298
user account management commands 298
User Exec Mode 58
users
adding 303, 304
deleting 302, 303, 304
displaying 300
passwords 305, 315
users access 303
users defaultlogin 301
users login 302, 574
users name 304
users passwd 305
users snmpv3 accessmode 306
users snmpv3 authentication 307
users snmpv3 encryption 308
utilization alarm-threshold 95

V

vlan 280
vlan acceptframe 282, 283
vlan ingressfilter 284
VLAN Mode 58
vlan name 285
vlan participation 286
vlan participation all 287
vlan port acceptframe all 288
vlan port ingressfilter all 289
vlan port priority all 107
vlan port pvid all 290
vlan port tagging all 291
vlan priority 108
vlan protocol group 841
vlan protocol group add protocol 842
vlan protocol group remove 843

vlan pvid 292
vlan routing 642
vlan tagging 293
vlan0-transparent-mode 281
VLANs
adding 280
changing the name of 285
deleting 280
details 261
frame acceptance mode 282, 283, 288
IDs 290, 292
ingress filtering 284, 289
jointime 214, 215, 216, 217, 218, 219, 220
leave all time 222
leave time 221
participation in 286, 287
port information 264
resetting parameters 317
summary information 263
tagging 291, 293
voice vlan (Global Config Mode) 294
voice vlan (Interface Config Mode) 295
voice vlan auth 297

W

Web connections, displaying 299

13 Glossary

Numerics

802.1D. The IEEE designator for Spanning Tree Protocol (STP). STP, a link management protocol, is part of the 802.1D standard for media access control bridges. Using the spanning tree algorithm, STP provides path redundancy while preventing endless loops in a network. An endless loop is created by multiple active paths between stations where there are alternate routes between hosts. To establish path redundancy, STP creates a logical tree that spans all of the switches in an extended network, forcing redundant paths into a standby, or blocked, state. STP allows only one active path at a time between any two network devices (this prevents the loops) but establishes the redundant links as a backup if the initial link should fail. If STP costs change, or if one network segment in the STP becomes unreachable, the spanning tree algorithm reconfigures the spanning tree topology and reestablishes the link by activating the standby path. Without spanning tree in place, it is possible that both connections may be simultaneously live, which could result in an endless loop of traffic on the LAN.

802.1P. The IEEE protocol designator for Local Area Network (LAN). This Layer 2 network standard improves support of time critical traffic, and limits the extent of high bandwidth multicast traffic within a bridged LAN. To do this, 802.1P defines a methodology for introducing traffic class priorities. The 802.1P standard allows priority to be defined in all 802 MAC protocols (Ethernet, Token Bus, Token Ring), as well as in FDDI. For protocols (such as Ethernet) that do not contain a priority field, 802.1P specifies a method for indicating frame priority based on the new fields defined in the 802.1Q (VLAN) standard.

802.1Q VLAN. The IEEE protocol designator for Virtual Local Area Network (VLAN). This standard provides VLAN identification and quality of service (QoS) levels. Four bytes are added to an Ethernet frame to allow eight priority levels (QoS) and to identify up to 4096 VLANs. See “VLAN” on page 875 for more information.

A

ABR. See “Area Border Router” on page 860.

Access Control List. An ACL is a database that an Operating System uses to track each user’s access

rights to system objects (such as file directories and/or files).

ACL. See “Access Control List” on page 859.

Address Resolution Protocol. An Internet Protocol that dynamically maps Internet addresses to physical (hardware) addresses on a LAN.

Advanced Network Device Layer/ Software. Hirschmann term for the Device Driver level.

Aging. When an entry for a node is added to the lookup table of a switch, it is given a timestamp. Each time a packet is received from a node, the timestamp is updated. The switch has a user-configurable timer that erases the entry after a certain length of time with no activity from that node.

API. See “Application Programming Interface” on page 860.

Application Programming Interface. An API is an interface used by an programmer to interface with functions provided by an application.

Area Border Router. A router located on the border of one or more OSPF areas that connects those areas to the backbone network. ABRs are considered members of both the OSPF backbone and the attached areas. They therefore maintain routing tables describing both the backbone topology and the topology of the other areas. (Cisco Systems Inc.)

ARP. See “Address Resolution Protocol” on page 860.

ASAM. See “ATM Subscriber Access Multiplexer” on page 860.

ASBR. See “Autonomous System Boundary Router” on page 860.

ATM Subscriber Access Multiplexer. A telephone central office multiplexer that supports SDL ports over a wide range of network interfaces. An ASAM sends and receives subscriber data (often Internet services) over existing copper telephone lines, concentrating all traffic onto a single high-speed trunk for transport to the Internet or the enterprise intranet. This device is similar to a DSLAM (different manufacturers use different terms for similar devices). (Cisco Systems Inc.)

Autonomous System Boundary Router. ABR located between an OSPF autonomous system and a non-OSPF network. ASBRs run both OSPF and another routing protocol, such as RIP. ASBRs must reside in a non-stub OSPF area. See also ABR, non-stub area, and OSPF. (Cisco Systems Inc.)

AVL tree. Binary tree having the property that for any node in the tree, the difference in height between the left and right subtrees of that node is no more than 1.

B

BPDU. See “Bridge Protocol Data Unit” on page 861.

BGP. See “Border Gateway Protocol” on page 861.

BootP. See “Bootstrap Protocol.” on page 861.

Bootstrap Protocol. An Internet protocol that enables a diskless workstation to discover its own IP address, the IP address of a BootP server on the network, and a file to be loaded into memory to boot the machine. This enables the workstation to boot without requiring a hard or floppy disk drive.

Border Gateway Protocol. BGP is a protocol for exchanging routing information between gateway host (each with its own router) in a network of autonomous systems. BGP is often the protocol used between gateway hosts on the Internet. The routing table contains a list of known routers, the addresses they can reach, and a cost metric associated with the path to each router so that the best available route is chosen. Hosts using BGP communicate using the Transmission Control Protocol (TCP) and send updated router table information only when one host has detected a change. Only the affected part of the routing table is sent. BGP-4, the latest version, lets administrators configure cost metrics based on policy statements. (BGP-4 is sometimes called BGP4, without the hyphen.) BGP communicates with autonomous (local) networks using Internal BGP (IBGP) since it doesn't work well with IGP. The routers inside the autonomous network thus maintain two routing tables: one for the interior gateway protocol and one for IBGP. BGP-4 makes it easy to use Classless Inter-Domain Routing (Classless Inter-Domain Routing), which is a way to have more addresses within the network than with the current IP address assignment scheme.

Bridge Protocol Data Unit. BPDU is the IEEE 802.1D MAC Bridge Management protocol that is the standard implementation of STP (Spanning Tree Protocol). It uses the STP algorithm to insure that physical loops in the network topology do not result in logical looping of network traffic. Using one bridge configured as root for reference, the BPDU switches one of two bridges forming a network loop into standby mode, so that only one side of a potential loop passes traffic. By examing frequent 802.1d configuration updates, a bridge in the standby mode can switch automatically into the forward mode if the other bridge forming the loop fails.

C

cards.h. A file that instructs the base code driver how to construct the driver.

card_db. A database that contains everything from port maps to module information.

Checksum. A simple error-detection scheme in which each transmitted message is identified with a numerical value based on the number of set bits in the message. The receiving station then applies a formula to the message and checks to make sure the accompanying numerical value is the same. If not, the receiver can assume that the message has been corrupted.

CLI. See “Command Line Interface” on page 862.

Command Line Interface. CLI is a line-item interface for configuring systems.

Common Open Policy Service Protocol. A proposed standard protocol for exchanging network policy information between a Policy Decision Point (PDP) in a network and Policy Enforcement Points (PEPs) as part of overall Quality of Service (QoS) - the allocation of network traffic resources according to desired priorities of service. The policy decision point might be a network server controlled directly by the network administrator who enters policy statements about which kinds of traffic (voice, bulk data, video, teleconferencing, and so forth) should get the highest priority. The policy enforcement points might be router or layer 3 switches that implement the policy choices as traffic moves through the network. Currently, COPS is designed for use with the Resource Reservation Protocol (RSVP), which lets you allocate traffic priorities in advance for temporary high-bandwidth requirements (for example, video broadcasts or multicasts). It is possible that COPS will be extended to be a general policy communications protocol.

Complex Programmable Logic Device. CPLD is a programmable circuit on which a logic network can be programmed after its construction.

COPS. See “Common Open Policy Service Protocol.” on page 862.

CPLD. See “Complex Programmable Logic Device.” on page 862.

D

DAPI. See “Device Application Programming Interface” on page 862.

Device Application Programming Interface. DAPI is the software interface that facilitates communication of both data and

control information between the Application Layer and HAPI, with support from System Support.

DHCP. See “Dynamic Host Configuration Protocol.” on page 863.

Differentiated Services. Diffserv is a protocol for specifying and controlling network traffic by class so that certain types of traffic get precedence - for example, voice traffic, which requires a relatively uninterrupted flow of data, might get precedence over other kinds of traffic. Differentiated Services is the most advanced method for managing traffic in terms of what is called Class of Service (CoS). Unlike the earlier mechanisms of 802.1P tagging and Type of Service (ToS), Differentiated Services avoids simple priority tagging and depends on more complex policy or rule statements to determine how to forward a given network packet. An analogy is made to travel services, in which a person can choose among different modes of travel - train, bus, airplane - degree of comfort, the number of stops on the route, standby status, the time of day or period of year for the trip, and so forth. For a given set of packet travel rules, a packet is given one of 64 possible forwarding behaviors - known as per hop behaviors (PHBs). A six-bit field, known as the Differentiated Services Code Point (DSCP), in the Internet Protocol (Internet Protocol) header specifies the per hop behavior for a given flow of packets. Differentiated Services and the Class of Service approach provide a way to control traffic that is both more flexible and more scalability than the Quality of Service approach.

Diffserv. See “Differentiated Services.” on page 863..

Distance-Vector Multicast Routing Protocol. DVMRP is a distance vector routing protocol used between routers in an intranet. This hop-based protocol describes a method of building multicast trees from the multicast source to all the receivers (or leaves) of the tree.

DVMRP. See “Distance-Vector Multicast Routing Protocol.” on page 863.

Dynamic Host Configuration Protocol. DHCP is a protocol for assigning dynamic IP addresses to devices on a network. With dynamic addressing, a device can have a different IP address every time it connects to the network. In some systems, the device's IP address can even change while it is still connected. DHCP also supports a mix of static and dynamic IP addresses. Dynamic addressing simplifies network administration because the software tracks IP addresses rather than requiring an administrator to manage the task. A new computer can be added to a network without the hassle of

manually assigning it a unique IP address.

E

EEPROM. See “Electronically Erasable Programmable Read Only Memory” on page 864.

Electronically Erasable Programmable Read Only Memory. EEPROM is also known as Flash memory. This is re-programmable memory.

F

Fast STP. A high-performance Spanning Tree Protocol. See “STP” on page 874 for more information.

FIFO. First In First Out.

Flash Memory. See “EEPROM” on page 864.

Flow Control. The process of adjusting the flow of data from one network device to another to ensure that the receiving device can handle all of the incoming data. This is particularly important where the sending device is capable of sending data much faster than the receiving device can receive it. There are many flow control mechanisms. One of the most common flow control protocols for asynchronous communication is called xon-xoff. In this case, the receiving device sends a an “xoff” message to the sending device when its buffer is full. The sending device then stops sending data. When the receiving device is ready to receive more data, it sends an “xon” signal.

Forwarding. When a frame is received on an input port on a switch, the address is checked against the lookup table. If the lookup table has recorded the destination address, the frame is automatically forwarded on an output port.

Frame Check Sequence. The extra characters added to a frame for error detection and correction. FCS is used in X.25, HDLC, Frame Relay, and other data link layer protocols.

G

GARP. See “Generic Attribute Registration Protocol.” on page 865.

GARP Information Propagation.

GIP is the propagation of information between GARP participants for the same application in a bridge is carried out by a GIP component.

GARP Multicast Registration Protocol. GMRP provides a mechanism that allows Bridges and end stations to dynamically register (and subsequently, de-register) Group membership information with the MAC Bridges attached to the same LAN segment, and for that information to be disseminated

across all Bridges in the Bridged LAN that support Extended Filtering Services. The operation of GMRP relies upon the services provided by the GARP.

GARP VLAN Registration Protocol. GVRP allows workstations to request admission to a particular VLAN for multicast purposes.

GE. See “Gigabit Ethernet” on page 865.

General Purpose Chip-select Machine. GPCM provides interfacing for simpler, lower-performance memory resources and memory mapped-devices. The GPCM does not support bursting and is used primarily for boot-loading.

Generic Attribute Registration Protocol. GARP provides a generic attribute dissemination capability that is used by participants in GARP Applications (called GARP Participants) to register and de-register attribute values with other GARP Participants within a Bridged LAN. The definition of the attribute types, the values that they can carry, and the semantics that are associated with those values when registered are specific to the operation of the GARP Application concerned.

Gigabit Ethernet. A high-speed Ethernet connection.

GIP. See “GARP Information Propagation” on page 864.

GMRP. See “GARP Multicast Registration Protocol” on page 864.

GPCM. See “General Purpose Chip-select Machine” on page 865.

GVD. GARP VLAN Database.

GVRP. See “GARP VLAN Registration Protocol.” on page 865.

H

.h file. Header file in C code. Contains function and coding definitions.

HAPI. See “Hardware Abstraction Programming Interface” on page 865.

Hardware Abstraction Programming Interface. HAPI is the module that contains the NP specific software that interacts with the hardware.

hop count. The number of routers that a data packet passes through on its way to its destination.

I

ICMP. See “Internet Control Message Protocol” on page 866.

IGMP. See “Internet Group Management Protocol” on page 866.

IGMP Snooping. A series of operations performed by

intermediate systems to add logic to the network to optimize the flow of multicast traffic; these intermediate systems (such as Layer 2 switches) listen for IGMP messages and build mapping tables and associated forwarding filters, in addition to reducing the IGMP protocol traffic. See “Internet Group Management Protocol” on page 866 for more information.

Internet Control Message Protocol. ICMP is an extension to the Internet Protocol (IP) that supports packets containing error, control, and informational messages. The PING command, for example, uses ICMP to test an Internet connection.

Internet Group Management Protocol. IGMP is the standard for IP Multicasting on the Internet. IGMP is used to establish host memberships in particular multicast groups on a single network. The mechanisms of the protocol allow a host to inform its local router, using Host Membership Reports, that it wants to receive messages addressed to a specific multicast group. All hosts conforming to Level 2 of the IP Multicasting specification require IGMP.

IP. See “Internet Protocol” on page 866.

IP Multicasting. Sending out data to distributed servers on the MBone (Multicast Backbone). For large amounts of data, IP Multicast is more efficient than normal Internet transmissions because the server can broadcast a message to many recipients simultaneously. Unlike traditional Internet traffic that requires separate connections for each source-destination pair, IP Multicasting allows many recipients to share the same source. This means that just one set of packets is transmitted for all the destinations.

Internet Protocol. The method or protocol by which data is sent from one computer to another on the Internet. Each computer (known as a host) on the Internet has at least one IP address that uniquely identifies it among all other computers on the Internet. When you send or receive data (for example, an e-mail note or a Web page), the message gets divided into little chunks called packets. Each of these packets contains both the sender's Internet address and the receiver's address. Any packet is sent first to a gateway computer that understands a small part of the Internet. The gateway computer reads the destination address and forwards the packet to an adjacent gateway that in turn reads the destination address and so forth across the Internet until one gateway recognizes the packet as belonging to a computer within its immediate neighborhood or domain. That gateway then forwards the

packet directly to the computer whose address is specified.

Because a message is divided into a number of packets, each packet can, if necessary, be sent by a different route across the Internet. Packets can arrive in a different order than they were sent. The Internet Protocol just delivers them. It's up to another protocol, the Transmission Control Protocol (TCP) to put them back in the right order. IP is a connectionless protocol, which means that there is no continuing connection between the end points that are communicating. Each packet that travels through the Internet is treated as an independent unit of data without any relation to any other unit of data. (The reason the packets do get put in the right order is because of TCP, the connection-oriented protocol that keeps track of the packet sequence in a message.) In the Open Systems Interconnection (OSI) communication model, IP is in Layer 3, the Networking Layer. The most widely used version of IP today is IP version 4 (IPv4). However, IP version 6 (IPv6) is also beginning to be supported. IPv6 provides for much longer addresses and therefore for the possibility of many more Internet users. IPv6 includes the capabilities of IPv4 and any server that can support IPv6 packets can also support IPv4 packets.

J

Joint Test Action Group. An IEEE group that specifies test framework standards for electronic logic components.

JTAG. See “Joint Test Action Group” on page 867.

L

LAN. See “Local Area Network” on page 868.

LDAP. See “Lightweight Directory Access Protocol” on page 867.

Lightweight Directory Access Protocol. A set of protocols for accessing information directories. LDAP is based on the standards contained within the X.500 standard, but is significantly simpler. Unlike X.500, LDAP supports TCP/IP, which is necessary for any type of Internet access. Although not yet widely implemented, LDAP should eventually make it possible for almost any application running on virtually any computer platform to obtain directory information, such as e-mail addresses and public keys. Because LDAP is an open protocol, applications need not worry about the type of server hosting the directory.

Learning. The bridge examines the Layer 2 source addresses of every frame on the attached networks (called listening) and then maintains

a table, or cache, of which MAC addresses are attached to each of its ports.

Link-State. In routing protocols, the declared information about the available interfaces and available neighbors of a router or network. The protocol's topological database is formed from the collected link-state declarations.

LLDP. The IEEE 802.1AB standard for link layer discovery in Ethernet networks provides a method for switches, routers and access points to advertise their identification, configuration and capabilities to neighboring devices that store the data in a MIB (management information base). Link layer discovery allows a network management system to model the topology of the network by interrogating the MIB databases in the devices.

Local Area Network. A group of computers that are located in one area and are connected by less than 1,000 feet of cable. A typical LAN might interconnect computers and peripherals on a single floor or in a single building. LANs can be connected together, but if modems and telephones connect two or more LANs, the larger network constitutes what is called a WAN or Wide Area Network.

M

MAC. (1) Medium Access Control. In LANs, the sublayer of the data link control layer that supports medium-dependent functions and uses the services of the physical layer to provide services to the logical link control (LLC) sublayer. The MAC sublayer includes the method of determing when a device has access to the transmission medium. (2) Message Authentication Code. In computer security, a value that is a part of a message or accompanies a message and is used to determine that the contents, origin, author, or other attributes of all or part of the message are as they appear to be. (*IBM Glossary of Computing Terms*)

Management Information Base.

When SNMP devices send SNMP messages to the management console (the device managing SNMP messages), it stores information in the MIB.

MBONE. See “Multicast Backbone” on page 869.

MDC. Management Data Clock.

MDI. Management Data Interface.

MDIO. Management Data Input/ Output.

MDIX. Management Dependent Interface Crossover.

MIB. See “Management Information Base” on page 868.

MOSPF. See “Multicast OSPF” on page 869.

MPLS. See “Multi-Protocol Label Switching” on page 869.

Multicast Backbone. The MBONE is a virtual network. It is layered on top of portions of the physical Internet to support routing of IP multicast packets since that function has not yet been integrated into many production routers. The network is composed of islands that can directly support IP multicast, such as multicast LANs like Ethernet, linked by virtual point-to-point links called "tunnels". The tunnel endpoints are typically workstation-class machines having operating system support for IP multicast and running the "mrouted" multicast routing daemon.

Multicasting. To transmit a message to specific recipients across a network. A simple example of multicasting is sending an e-mail message to a mailing list. Teleconferencing and videoconferencing also use multicasting, but require more robust protocols and networks. Standards are being developed to support multicasting over a TCP/IP network such as the Internet. These standards, IP Multicast and Mbone, will allow users to easily join multicast groups. Note that multicasting refers to sending a message to a select group whereas broadcasting refers to sending a message to everyone connected to a network. The terms multicast and narrowcast are often used interchangeably, although narrowcast usually refers to the business model whereas multicast refers to the actual technology used to transmit the data.

Multicast OSPF. With a MOSPF specification, an IP Multicast packet is routed based both on the packet's source and its multicast destination (commonly referred to as source/destination routing). As it is routed, the multicast packet follows a shortest path to each multicast destination. During packet forwarding, any commonality of paths is exploited; when multiple hosts belong to a single multicast group, a multicast packet will be replicated only when the paths to the separate hosts diverge. See “OSPF” on page 871 for more information.

Multiplexing. A function within a layer that interleaves the information from multiple connections into one connection.

Multi-Protocol Label Switching.

An initiative that integrates Layer 2 information about network links (bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system—or ISP—in order to simplify and improve IP-

packet exchange. MPLS gives network operators a great deal of flexibility to divert and route traffic around link failures, congestion, and bottlenecks. From a QoS standpoint, ISPs will better be able to manage different kinds of data streams based on priority and service plan. For instance, those who subscribe to a premium service plan, or those who receive a lot of streaming media or high-bandwidth content can see minimal latency and packet loss. When packets enter into a MPLS-based network, Label Edge Routers (LERs) give them a label (identifier). These labels not only contain information based on the routing table entry (i.e., destination, bandwidth, delay, and other metrics), but also refer to the IP header field (source IP address), Layer 4 socket number information, and differentiated service. Once this classification is complete and mapped, different packets are assigned to corresponding Labeled Switch Paths (LSPs), where Label Switch Routers (LSRs) place outgoing labels on the packets. With these LSPs, network operators can divert and route traffic based on data-stream type and Internet-access customer.

MT-RJ connector. A type of fiber-optic cable jack that is similar in shape and concept to a standard telephone jack, enabling duplex fiber-optic cables to be plugged into compatible devices as easily as plugging in a telephone cable.

MUX. See “Multiplexing” on page 869.

N

NAT. See “Network Address Translation” on page 870.

Network Address Translation.

Sometimes referred to as Transparent Proxying, IP Address Overloading, or IP Masquerading. Involves use of a device called a Network Address Translator, which assigns a contrived, or logical, IP address and port number to each node on an organization's internal network and passes packets using these assigned addresses.

NM. Network Module.

nm. Nanometer (1 x $10e^9$) meters.

non-stub area. Resource-intensive OSPF area that carries a default route, static routes, intra-area routes, interarea routes, and external routes. Non-stub areas are the only OSPF areas that can have virtual links configured across them, and are the only areas that can contain an ASBR. Compare with stub area. See also ASAM and OSPF. (Cisco Systems Inc.)

NP. Network Processor.

O

Open Shortest Path First. A link-state (algorithm used by the router to determine the current topology of a network), Interior Gateway (distributes routing information between routers belonging to a single Autonomous System) routing protocol. This protocol's algorithm determines the shortest path from its router to all the other routers in the network. This protocol is rapidly replacing RIP on the Internet.

Open Systems Interconnection.

OSI is a seven (7) layer architecture model for communications systems developed by the ISO for the interconnection of data communications systems. Each layer uses and builds on the services provided by those below it.

Operating System Application Programming Interface. OSAPI is a module within the System Support software that provides a set of interfaces to OS support functions.

OS. Operating System.

OSAPI. See “Operating System Application Programming Interface” on page 871.

OSI. See “Open Systems Interconnection” on page 871.

OSPF. See “Open Shortest Path First” on page 871.

P

PDU. See “Protocol Data Unit” on page 872.

PHY. The OSI Physical Layer: The physical layer provides for transmission of cells over a physical medium connecting two ATM devices. This physical layer is comprised of two sublayers: the Physical Medium Dependent (PMD) sublayer, and the Transmission Convergence (TC) sublayer.

PIM-DM. See “Protocol Independent Multicast – Dense Mode” on page 872.

PMC. Packet Mode Channel.

Port Mirroring. Also known as a roving analysis port. This is a method of monitoring network traffic that forwards a copy of each incoming and outgoing packet from one port of a network switch to another port where the packet can be studied. A network administrator uses port mirroring as a diagnostic tool or debugging feature, especially when fending off an attack. It enables the administrator to keep close track of switch performance and alter it if necessary. Port mirroring can be managed locally or remotely. An administrator configures port mirroring by assigning a port from which to copy all packets and another port where those packets will be sent. A packet bound for or heading away from the

first port will be forwarded onto the second port as well. The administrator places a protocol analyzer on the port receiving the mirrored data to monitor each segment separately. The analyzer captures and evaluates the data without affecting the client on the original port. The monitor port may be a port on the same SwitchModule with an attached RMON probe, a port on a different SwitchModule in the same hub, or the SwitchModule processor. Port mirroring can consume significant CPU resources while active. Better choices for long-term monitoring may include a passive tap like an optical probe or an Ethernet repeater.

Protocol Data Unit. PDU is a packet of data passed across a network. The term implies a specific layer of the OSI model and a specific protocol.

Protocol Independent Multicast – Dense Mode. Like DVMRP, PIM-DM uses a flood and prune protocol for building multicast trees. However, unlike DVMRP, PIM-DM uses existing unicast protocols for determing the route to the source.

Q

QoS. See “Quality of Service” on page 872.

Quality of Service. QoS is a networking term that specifies a guaranteed level of throughput. Throughput is the amount of data transferred from one device to another or processed in a specified amount of time - typically, throughputs are measured in bytes per second (Bps).

R

Real-Time Operating System.

RTOS is a component of the OSAPI module that abstracts operating systems with which other systems can interface.

Resource Reservation Setup Protocol. RSVP is a new Internet protocol being developed to enable the Internet to support specified Qualities-of-Service (QoS). Using RSVP, an application will be able to reserve resources along a route from source to destination. RSVP-enabled routers will then schedule and prioritize packets to meet the prioritization assigned by QoS. RSVP is a chief component of a new type of Internet being developed, known broadly as an integrated services Internet. The general idea is to enhance the Internet to support transmission of real-time data.

RFC. Request For Comment.

RIP. See “Routing Information Protocol” on page 872.

Routing Information Protocol.

RIP is the routing protocol used by the routed process on Berkeley-

derived UNIX systems. Many networks use RIP; it works well for small, isolated, and topologically simple networks.

RIPng. Routing Information Protocol, new generation.

RMON. Short for remote monitoring, a network management protocol that allows network information to be gathered at a single workstation. Whereas SNMP gathers network data from a single type of Management Information Base (MIB), RMON 1 defines nine additional MIBs that provide a much richer set of data about network usage. For RMON to work, network devices, such as hubs and switches, must be designed to support it. The newest version of RMON, RMON 2, provides data about traffic at the network layer in addition to the physical layer. This allows administrators to analyze traffic by protocol.

RP. Rendezvous Point. Used with IP Multicast.

RPU. Remote Power Unit.

RSVP. See “Resource Reservation Setup Protocol” on page 872.

RTOS. See “Real-Time Operating System” on page 872.

S

SDL. Synchronous Data Link.

Simple Network Management Protocol. SNMP is the protocol governing network management and the monitoring of network devices and their functions. It is not necessarily limited to TCP/IP networks. The versions have the following differences:

SNMPv1 (full): Security is based on community strings.

SNMPsec (historic): Security is based on parties. Few, if any, vendors implemented this version of the protocol, which is now largely forgotten.

SNMPv2p (historic): For this version, much work was done to update the SNMPv1 protocol and the SMIv1, and not just security. The result was updated protocol operations, new protocol operations and data types, and party-based security from SNMPsec.

SNMPv2c (experimental): This version of the protocol is called community string-based SNMPv2. It is an update of the protocol operations and data types of SNMPv2p, and uses community-based security from SNMPv1.

SNMPv2u (experimental): This version of the protocol uses the protocol operations and data types of SNMPv2c and security based on users.

*SNMPv2** (experimental): This version combined the best features

of SNMPv2p and SNMPv2u. (It is also called SNMPv2star.) The documents defing this version were never published as RFCs.

SNMPv3 (proposed): This version of the protocol is a combination of user-based security and the protocol operations and data types from SNMPv2p and support for proxies. The security is based on that found in SNMPv2u and SNMPv2*, and updated after much review. The documents defing this protocol will soon be published as RFCs.

SimpleX signaling. SX is one of IEEE 802.3's designations for media. For example, 1000SX indicates 1000 Gigabit Ethernet over "short haul" or "short wavelength" optical fiber.

SMC1. A model of Serial Management Controller from Motorola.

SMII. Serial Media Independent Interface.

SNMP. See “Simple Network Management Protocol” on page 873.

SODIMM. Small Outline Dual Inline Memory Module.

SRAM. Static Random Access Memory.

STP. Spanning Tree Protocol. See “802.1D” on page 859 for more information.

stub area. OSPF area that carries a default route, intra-area routes, and interarea routes, but does not carry external routes. Virtual links cannot be configured across a stub area, and they cannot contain an ASBR. Compare with non-stub area. See also ASAM and OSPF. (Cisco Systems Inc.)

SX. See “SimpleX signaling” on page 874.

SYSAPI. See “Systems Application Programming Interface” on page 874.

Systems Application Programming Interface. SYSAPI is a module within the System Support software that provides system-wide routines for network and mbuf support and provides the interface into the system registry.

T

TBI. Ten Bit Interface.

Telnet. A character-based UNIX application that enables users with a Telnet server account to log on to a UNIX computer and utilize its resources.

TFTP. See “Trivial File Transfer Protocol” on page 874.

Trivial File Transfer Protocol.

TFTP is a simple form of the File Transfer Protocol (FTP). TFTP uses the User Datagram Protocol (UDP, a

direct protocol used to communicate datagrams over a network with little error recovery) and provides no security features. It is often used by servers to boot diskless workstations, X-terminals, and routers.

Trunking. The process of combing a set of trunks that are traffic-engineered as a unit for the establishment of connections between switching systems in which all of the communications paths are interchangeable.

U

UPM. User Programmable Machine.

UPMA. The first of two UPMs in Motorola's MPC855T processor.

UPMB. The second of two UPMs in Motorola's MPC855T processor.

USP. An abbreviation that represents Unit, Slot, Port.

V

Virtual Local Area Network.

Operating at the Data Link Layer (Layer 2 of the OSI model), the VLAN is a means of parsing a single network into logical user groups or organizations, as if they physically resided on a dedicated LAN segment of their own. In reality, this virtually defined community may have individual members peppered across a large, extended LAN. The VLAN identifier is part of the 802.1Q tag, which is added to an Ethernet frame by an 802.1Q-compliant switch or router. Devices recognizing 802.1Q-tagged frames maintain appropriate tables to track VLANs. The first three bits of the 802.1Q tag are used by 802.1P to establish priority for the packet.

Virtual Router Redundancy Protocol. VRRP specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. The VRRP router controlling the IP address(es) associated with a virtual router is called the Master, and forwards packets sent to these IP addresses. The election process provides dynamic fail-over in the forwarding responsibility should the Master become unavailable. This allows any of the virtual router IP addresses on the LAN to be used as the default first hop router by end-hosts. The advantage gained from using VRRP is a higher availability default path without requiring configuration of dynamic routing or router discovery protocols on every end-host.

VLAN. See “Virtual Local Area Network” on page 875.

vMAN. Virtual Metropolitan Area Network.

VRRP. See “Virtual Router Redundancy Protocol” on page 875.

W

WAN. See “Wide Area Network” on page 876.

Web. Also known as World-Wide Web (WWW) or W3. An Internet client-server system to distribute information, based upon the hypertext transfer protocol (HTTP).

Wide Area Network. A WAN is a computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs).

X

X.500. A directory standard that enables applications like e-mail to access information that can either be central or distributed. The benefit of a directory is the ability to minimize the impact on the user of changes to a network. The standard is broken down under subsequent standards, as follows:

X.501 Models

X.509 Authentication framework

X.511 Abstract service definition

X.518 Procedures for distributed operation

X.519 Protocol specifications

X.520 Selected attribute types

X.521 Selected object types

XModem. One of the most popular file transfer protocols (FTPs). Xmodem is fairly effective at detecting errors. It sends blocks of data together with a checksum and then waits for acknowledgment of the block's receipt. The waiting slows down the rate of data transmission considerably, but it ensures accurate transmission. Xmodem can be implemented either in software or in hardware. Many modems, and almost all communications software packages, support Xmodem. However, it is useful only at relatively slow data transmission speeds (less than 4,800 bps). Enhanced versions of Xmodem that work at higher transmission speeds are known as Ymodem and Zmodem.

Further support

Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at http://www.hirschmann.com

Contact our support at
https://hirschmann-support.belden.eu.com

You can contact us

in the EMEA region at:
- Tel.: +49 (0)1805 14-1538
- E-mail: hac.support@belden.com

in the America region at:
- Tel.: +1 (717) 217-2270
- E-mail: inet-support.us@belden.com

in the Asia-Pacific region at:
- Tel.: +65 6854 9860
- E-mail: inet-ap@belden.com

Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- 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.
  The current technology and product training courses can be found at http://www.hicomcenter.com
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Hirschmann Competence Center, you have 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

HIRSCHMANN
A BELDEN BRAND

Anwender-Handbuch

Grundkonfiguration
Industrial ETHERNET (Gigabit-)Switch
PowerMICE, MACH 104, MACH 1040, MACH 4000

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

© 2015 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken. Bei Geräten mit eingebetteter Software gilt die Endnutzer-Lizenzvereinbarung auf der mitgelieferten CD/DVD.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die jeweils neueste Version dieses Handbuches finden Sie im Internet auf den Hirschmann-Produktseiten (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Rel. 9.0 - 02/2015 – 22.01.2015

Inhalt

Sicherheitshinweise 9

Über dieses Handbuch 11

Legende 13

Einleitung 15

1 Zugang zu den Benutzeroberflächen 17

1.1 System-Monitor 18

1.2 Command Line Interface 21

1.3 Grafische Benutzeroberfläche 24

2 IP-Parameter eingeben 27

2.1 Grundlagen IP-Parameter 29
2.1.1 IP-Adresse (Version 4) 29
2.1.2 Netzmaske 30
2.1.3 Classless Inter-Domain Routing 33

2.2 IP-Parameter via CLI eingeben 35

2.3 IP-Parameter per HiDiscovery eingeben 38

2.4 System-Konfiguration vom ACA laden 40

2.5 System-Konfiguration via BOOTP 42

2.6 System-Konfiguration via DHCP 47

2.7 System-Konfiguration via DHCP-Option 82 50

2.8 IP-Konfiguration via grafische Benutzeroberfläche 51

2.9 Defekte Geräte ersetzen 54

3 Einstellungen laden/speichern 55

3.1 Einstellungen laden 56
3.1.1 Laden aus lokalem nicht-flüchtigen Speicher 57
3.1.2 Laden aus einer Datei 58
3.1.3 Die aktuelle Konfiguration in den Lieferzustand zurückzusetzen. 60

3.1.4 Laden vom AutoConfiguration Adapter 61
3.1.5 Den Offline-Konfigurator verwenden 63

3.2 Einstellungen speichern 65
3.2.1 Lokal (und auf den ACA) speichern 65
3.2.2 Speichern in eine Binär- oder Skript-Datei auf einem URL 67
3.2.3 Speichern in eine Binär-Datei auf den PC 68
3.2.4 Speichern als Skript auf den PC 68
3.2.5 Speichern als Offline-Konfigurations-Datei auf den PC 69

3.3 Konfigurations-Signatur 70

4 Neueste Software laden 71

4.1 Software manuell vom ACA laden 73
4.1.1 Auswahl der zu ladenden Software 74
4.1.2 Starten der Software 75
4.1.3 Kaltstart durchführen 76

4.2 Automatischer Software-Update vom ACA 77

4.3 Software vom TFTP-Server laden 79

4.4 Software über Datei-Auswahl laden 81

4.5 Bootcode-Update via TFTP 82
4.5.1 Aktualisieren der Bootcode-Datei 82

5 Ports konfigurieren 85

6 Unterstützung beim Schutz vor unberechtigtem Zugriff 91

6.1 Das Gerät schützen 92

6.2 Passwort für SNMP-Zugriff 93
6.2.1 Beschreibung Passwort für SNMP-Zugriff 93
6.2.2 Passwort für SNMP-Zugriff eingeben 94

6.3 Telnet-/Web-/SSH-Zugriff 98
6.3.1 Beschreibung Telnet-Zugriff 98
6.3.2 Beschreibung Web-Zugriff (http) 98
6.3.3 Beschreibung SSH-Zugriff 99
6.3.4 Telnet-/Web-/SSH-Zugriff aus-/einschalten 100
6.3.5 Web-Zugriff über HTTPS 101

6.4 Restricted Management Access 104

6.5 HiDiscovery-Zugriff aus-/einschalten 107

6.5.1 Beschreibung HiDiscovery-Protokoll 107
6.5.2 HiDiscovery-Funktion aus-/einschalten 107

6.6 Portzugangskontrolle 109
6.6.1 Beschreibung der Portzugangskontrolle 109
6.6.2 Anwendungsbeispiel für Portzugangskontolle 110

6.7 Port-Authentifizierung nach IEEE 802.1X 112
6.7.1 Beschreibung Port-Authentifizierung nach IEEE 802.1X 112
6.7.2 Authentifizierungsablauf nach IEEE 802.1X 113
6.7.3 Vorbereitung des Gerätes für die IEEE 802.1X-Port-Authentifizierung 113
6.7.4 IEEE 802.1X-Einstellungen 114

6.8 Zugriffs-Kontroll-Listen (ACL) 116
6.8.1 Beschreibung Priorisierung mit ACLs 117
6.8.2 Beschreibung IP-basierte ACLs 118
6.8.3 Beschreibung MAC-basierte ACLs 119
6.8.4 IP-ACLs konfigurieren 121
6.8.5 MAC-ACLs konfigurieren 123
6.8.6 Priorisierung mit IP-ACLs konfigurieren 124
6.8.7 Reihenfolge der Regeln festlegen 126
6.8.8 ACLs für Layer-4-Fragmente 127

6.9 Login-Banner 128

6.10 CLI-Banner 129

7 Die Systemzeit im Netz synchronisieren 131

7.1 Uhrzeit einstellen 132

7.2 SNTP 134
7.2.1 Beschreibung SNTP 134
7.2.2 Vorbereitung der SNTP-Konfiguration 135
7.2.3 Konfiguration SNTP 136

7.3 Precison Time Protocol 139
7.3.1 Funktionsbeschreibung PTP 139
7.3.2 PTP-Konfiguration vorbereiten 145
7.3.3 Anwendungsbeispiel 147

7.4 Interaktion von PTP und SNTP 152

8 Netzlaststeuerung 155

8.1 Gezielte Paketvermittlung 156
8.1.1 Store and Forward 156
8.1.2 Multiadress-Fähigkeit 156
8.1.3 Aging gelernter MAC-Adressen 157

8.1.4 Statische Adresseinträge eingeben 158
8.1.5 Gezielte Paketvermittlung ausschalten 160

8.2 Multicast-Anwendung 161
8.2.1 Beschreibung Multicast-Anwendung 161
8.2.2 Beispiel für eine Multicast-Anwendung 162
8.2.3 Beschreibung IGMP-Snooping 163
8.2.4 IGMP-Snooping einstellen 164
8.2.5 Beschreibung von GMRP 169
8.2.6 GMRP einstellen 171

8.3 Lastbegrenzer 173
8.3.1 Beschreibung Lastbegrenzer 173
8.3.2 Lastbegrenzer-Einstellungen 174

8.4 QoS/Priorität 175
8.4.1 Beschreibung Priorisierung 175
8.4.2 VLAN-Tagging 176
8.4.3 IP ToS / DiffServ 179
8.4.4 Management-Priorisierung 182
8.4.5 Behandlung empfangener Prioritätsinformationen 183
8.4.6 Handhabung der Verkehrsklassen 183
8.4.7 Priorisierung einstellen 186

8.5 Flusskontrolle 193
8.5.1 Beschreibung Flusskontrolle 193
8.5.2 Flusskontrolle einstellen 195

8.6 VLANs 196
8.6.1 Beschreibung VLAN 196
8.6.2 Beispiele für ein VLAN 197
8.6.3 Double-VLAN-Tagging 210

9 Funktionsdiagnose 217

9.1 Alarmmeldungen versenden 218
9.1.1 Auflistung der SNMP-Traps 219
9.1.2 SNMP-Traps beim Booten 220
9.1.3 Trapeinstellung 221

9.2 Gerätestatus überwachen 223
9.2.1 Gerätestatus konfigurieren 224
9.2.2 Gerätestatus anzeigen 225

9.3 Out-of-band-Signalisierung 226
9.3.1 Meldekontakt steuern 227
9.3.2 Gerätestatus mit Meldekontakt überwachen 228
9.3.3 Gerätefunktionen mit Meldekontakt überwachen 228
9.3.4 Lüfter überwachen 230

9.4 Port-Zustandsanzeige 232

9.5 Ereigniszähler auf Portebene 234
9.5.1 Erkennen der Nichtübereinstimmung der Duplex-Modi 235
9.5.2 TP-Kabeldiagnose 237
9.5.3 Port-Monitor 239
9.5.4 Auto-Disable 242
9.6 SFP-Zustandsanzeige 244
9.7 Topologie-Erkennung 245
9.7.1 Beschreibung Topologie-Erkennung 245
9.7.2 Anzeige der Topologie-Erkennung 246
9.8 IP-Adresskonflikte erkennen 248
9.8.1 Beschreibung von IP-Adresskonflikten 248
9.8.2 ACD konfigurieren 249
9.8.3 ACD anzeigen 249
9.9 Erkennen von Loops (Schleifen) 250
9.10 Berichte 252
9.11 Datenverkehr von Ports beobachten (Port-Mirroring) 254
9.12 Syslog 258
9.13 Trap-Log 261
9.14 MAC-Benachrichtigung 262

A Konfigurationsumgebung einrichten 265

A.1 DHCP/BOOTP-Server einrichten 266
A.2 DHCP-Server Option 82 einrichten 272
A.3 TFTP-Server für SW-Updates 276
A.3.1 tftp-Prozess einrichten 277
A.3.2 Software-Zugriffsrechte 280
A.4 SSH-Zugriff vorbereiten 281
A.4.1 Schlüssel erzeugen 281
A.4.2 Schlüssel auf das Gerät laden 283
A.4.3 Zugriff mittels SSH 283
A.5 HTTPS-Zertifikat 286
A.6 Service-Shell 287

B Allgemeine Informationen 289

B.1 Management Information BASE (MIB) 290

B.2 Verwendete Abkürzungen 293

B.3 Technische Daten 294

B.4 Leserkritik 295

C Stichwortverzeichnis 297

D Weitere Unterstützung 301

Sicherheitshinweise

⚠ WARNUNG
UNKONTROLLIERTE MASCHINENBEWEGUNGEN Um unkontrollierte Maschinenbewegungen aufgrund von Datenverlust zu vermeiden, konfigurieren Sie alle Geräte zur Datenübertragung individuell. Nehmen Sie eine Maschine, die mittels Datenübertragung gesteuert wird, erst in Betrieb, wenn Sie alle Geräte zur Datenübertragung vollständig konfiguriert haben. **Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.**

Über dieses Handbuch

Das Dokument „Anwender-Handbuch Grundkonfiguration“ enthält die Informationen, die Sie zur Inbetriebnahme des Gerätes benötigen. Es leitet Sie Schritt für Schritt von der ersten Inbetriebnahme bis zu den grundlegenden Einstellungen für einen Ihrer Umgebung angepassten Betrieb.

In der Praxis hat sich folgende thematische Reihenfolge bewährt:

- Gerätezugang zur Bedienung herstellen durch Eingabe der IP-Parameter
- Stand der Software prüfen, gegebenenfalls die Software aktualisieren
- Eine ggf. bereits existierende Konfiguration laden/speichern
- Ports konfigurieren
- Schutz vor unberechtigtem Zugriff konfigurieren
- Datenübertragung optimieren durch Netzlaststeuerung
- Systemzeit im Netz synchronisieren
- Funktionsdiagnose
- Die neu erstellte Konfiguration nichtflüchtig speichern

Das Dokument „Anwender-Handbuch Installation“ enthält eine Gerätebeschreibung, Sicherheitshinweise, Anzeigebeschreibung und weitere Informationen, die Sie zur Installation des Gerätes benötigen, bevor Sie mit der Konfiguration des Gerätes beginnen.

Das Dokument „Anwender-Handbuch Redundanzkonfiguration“ enthält die Informationen, die Sie zur Auswahl des geeigneten Redundanzverfahrens und dessen Konfiguration benötigen.

Das Dokument „Anwender-Handbuch Industrie-Protokolle“ beschreibt die Anbindung des Gerätes über ein in der Industrie übliches Kommunikationsprotokoll wie z.B. EtherNet/IP und PROFINET IO.

Das Dokument „Anwender-Handbuch Routing-Konfiguration“ enthält Informationen, die Sie zur Inbetriebnahme der Routing-Funktion benötigen. Es leitet Sie Schritt für Schritt von einer kleinen Router-Anwendung bis hin zur Router-Konfiguration eines komplexen Netzes.
Das Handbuch versetzt Sie in die Lage, durch Ableitung aus den Beispielen Ihre Router zu konfigurieren.

Das Dokument „Referenz-Handbuch GUI“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über die grafische Oberfläche.

Das Dokument „Referenz-Handbuch Command Line Interface“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über das Command Line Interface.

Die Netzmanagement-Software Industrial HiVision bietet Ihnen weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:

- ActiveX-Control für SCADA-Integration
- Autotopologie-Erkennung
- Browser-Interface
- Client/Server-Struktur
- Ereignisbehandlung
- Ereignislogbuch
- Gleichzeitige Konfiguration mehrerer Geräte
- Grafische Benutzeroberfläche mit Netz-Layout
- SNMP/OPC-Gateway

Wartung

Hirschmann arbeitet ständig an der Verbesserung und Weiterentwicklung der Software. Prüfen Sie regelmäßig, ob ein neuerer Stand der Software Ihnen weitere Vorteile bietet. Informationen und Software-Downloads finden Sie auf den Hirschmann-Produktseiten im Internet (www.hirschmann.com).

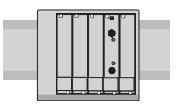
Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
☐	Arbeitsschritt
■	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	ASCII-Darstellung in der grafischen Benutzeroberfläche
	Ausführung in der grafischen Benutzeroberfläche
	Ausführung im Command Line Interface

Verwendete Symbole:

	WLAN-Access-Point
	Router mit Firewall
	Switch mit Firewall
	Router
	Switch

	Bridge
	Hub
	Beliebiger Computer
	Konfigurations-Computer
	Server
	SPS - Speicherprogrammier-bare Steuerung
	I/O - Roboter

Einleitung

Das Gerät ist für die Praxis in der rauen Industrieumgebung entwickelt. Dementsprechend einfach ist die Installation. Mit wenigen Einstellungen können Sie dank der gewählten Voreinstellungen das Gerät sofort in Betrieb nehmen.

Anmerkung: Änderungen, die Sie an den Dialogen vornehmen, übernimmt das Gerät flüchtig, wenn Sie auf „Schreiben“ klicken.
Um die Änderungen im Gerät nicht-flüchtig zu speichern, wählen Sie im Dialog `Grundeinstellungen:Laden/Speichern` den permanenten Speicherort und klicken Sie auf „Speichern“.

1 Zugang zu den Benutzeroberflächen

Das Gerät bietet Ihnen 3 Benutzeroberflächen, die Sie über unterschiedliche Schnittstellen erreichen:

- System-Monitor über die V.24-Schnittstelle (out-of-band),
- Command Line Interface (CLI) über den V.24-Anschluss (out-of-band) sowie über Telnet und SSH (in-band)
- Grafische Benutzeroberfläche über Ethernet (in-band)

1.1 System-Monitor

Der System-Monitor ermöglicht

- die Auswahl der zu ladenden Software,
- die Durchführung eines Updates der Software,
- Starten der ausgewählten Software,
- Beenden des System-Monitors,
- Löschen der gespeicherten Konfiguration und
- Anzeige der Bootcode-Information.

System-Monitor starten

Voraussetzungen

- Terminal-Kabel für die Verbindung vom Gerät zu Ihren PC (als optionales Zubehör erhältlich).
- PC mit einer VT100-Terminalemulation (z. B. PuTTY) oder serielles Terminal

Führen Sie die folgenden Arbeitsschritte aus:

☐ Verbinden Sie mit Hilfe des Terminal-Kabels den V.24-Anschluss des Gerätes mit dem „COM“-Port des PCs.
☐ Starten Sie die VT100-Terminalemulation auf dem PC.
☐ Legen Sie folgende Übertragungsparameter fest:
  – Geschwindigkeit: 9.600 Baud
  – Daten: 8 bit
  – Parität: Keine
  – Stopbit: 1 bit
  – Flusskontrolle: Keine

Speed	9600 Baud
Data	8 bit
Parity	none
Stoppbit	1 bit
Handshake	off

Tab. 1: Übertragungsparameter

☐ Starten Sie das Terminalprogramm auf dem PC und stellen Sie eine Verbindung mit dem Gerät her.

Beim Booten des Gerätes erscheint auf dem Terminal die Meldung „Press <1> to enter System Monitor 1“.

```
< Device Name  (Boot) Release: 1.00 Build: 2005-09-17 15:36 >

Press <1> to enter System Monitor 1 ...
 1
```

Abb. 1: Bildschirmansicht beim Bootvorgang

☐ Drücken Sie innerhalb von einer Sekunde die „1“-Taste, um den System-Monitor 1 zu starten.

```
System Monitor

(Selected OS: L3P-06.0.00 (2010-09-09 09:09))

1  Select Boot Operating System
2  Update Operating System
3  Start Selected Operating System
4  End (reset and reboot)
5  Erase main configuration file




sysMon1>
```

Abb. 2: Bildschirmansicht des System-Monitor 1

☐ Wählen Sie durch Eingabe der Zahl den gewünschten Menüpunkt aus.
☐ Um ein Untermenü zu verlassen und zum Hauptmenü des System-Monitor 1 zurückzukehren, drücken Sie <ESC>.

1.2 Command Line Interface

Das Command Line Interface bietet Ihnen die Möglichkeit, die Funktionen des Gerätes über eine lokale oder eine Fernverbindung zu bedienen. IT-Spezialisten finden im Command Line Interface die gewohnte Umgebung zur Konfiguration von IT-Geräten.
Die Skriptfähigkeit des Command Line Interfaces versetzt Sie u.a. in die Lage, mehrere Geräte mit gleichen Konfigurationsdaten zu speisen, partielle Konfigurationen zu erzeugen und anzuwenden oder 2 Konfigurationen mit Hilfe von 2 Skriptdateien zu vergleichen.

Eine detaillierte Beschreibung des Command Line Interface finden Sie im Referenz-Handbuch „Command Line Interface“.

Zugang zum Command Line Interface haben Sie über:

- den V.24-Port (out-of-band)
- Telnet (in-band)
- SSH (in-band)

Anmerkung: Zur Erleichterung der Eingabe bietet Ihnen das CLI die Möglichkeit, Schlüsselwörter abzukürzen. Tippen Sie den Beginn eines Schlüsselwortes ein. Mit dem Betätigen der Tabulatortaste ergänzt das CLI das Schlüsselwort.

Öffnen des Command Line Interfaces

☐ Verbinden Sie das Gerät über V.24 mit einem Terminal oder einem „COM“-Port eines PCs mit Terminalemulation nach VT100 und drücken Sie eine Taste (siehe auf Seite 18 „System-Monitor“) oder rufen Sie das Command Line Interface über Telnet auf.
Auf dem Bildschirm erscheint ein Fenster für die Eingabe des Benutzernamens.
Bis zu 5 Benutzer können auf das Command Line Interface zugreifen.

```
        Copyright (c) 2004-2010 Hirschmann Automation and Control GmbH

                          All rights reserved

                       PowerMICE Release L3P-06.0.00

                       (Build date 2010-09-09 12:13)



                     System Name:  PowerMICE
                     Mgmt-IP    :  10.0.1.105
                     1.Router-IP:  0.0.0.0
                     Base-MAC   :  00:80:63:51:74:00
                     System Time:  2010-09-09 13:14:15


User:
```

Abb. 3: Einloggen in das Command Line Interface Programm

☐ Geben Sie einen Benutzernamen ein. Im Lieferzustand ist der Benutzername **admin** eingetragen. Drücken Sie die Eingabetaste.

☐ Geben Sie das Passwort ein. Im Lieferzustand ist das Passwort **private** eingetragen. Drücken Sie die Eingabetaste.
Sie können den Benutzernamen und das Passwort später im Command Line Interface ändern.
Beachten Sie die Schreibweise in Groß-/Kleinbuchstaben.

Der Start-Bildschirm erscheint.

```
NOTE: Enter '?' for Command Help. Command help displays all options
      that are valid for the 'normal' and 'no' command forms.  For
      the syntax of a particular command form, please consult the
      documentation.


(Hirschmann Product) >
```

Abb. 4: CLI-Bildschirm nach dem Einloggen

1.3 Grafische Benutzeroberfläche

Die grafische Benutzeroberfläche (GUI) bietet Ihnen die Möglichkeit, die Einstellungen des Gerätes von einem Computer im Netz aus komfortabel festzulegen und zu überwachen.

Sie erreichen die grafische Benutzeroberfläche (GUI) mit folgenden Programmen:

- HiView
- Web-Browser

Systemvoraussetzungen

Verwenden Sie zum Öffnen der grafischen Benutzeroberfläche HiView. Diese Applikation bietet Ihnen die Möglichkeit, frei von weiteren Anwendungen wie einem Web-Browser oder einer installierten Java-Laufzeitumgebung (JRE), die grafische Benutzeroberfläche zu bedienen.

Alternativ haben Sie die Möglichkeit, die grafische Benutzeroberfläche im Web-Browser zu öffnen, z. B. im Mozilla Firefox ab Version 3.5 oder im Microsoft Internet Explorer ab Version 6. Installieren Sie hierzu auch die Java-Laufzeitumgebung (JRE) in der zuletzt freigegebenen Version. Installationspakete für Ihr Betriebssystem finden Sie unter http://java.com.

Grafische Benutzeroberfläche starten

Voraussetzung für das Starten der grafischen Benutzeroberfläche ist, dass die IP-Parameter im Gerät konfiguriert sind.

Grafische Benutzeroberfläche in HiView starten:

☐ Starten Sie HiView.

☐ Geben Sie in das URL-Feld des Startfensters die IP-Adresse Ihres Gerätes ein.

☐ Klicken Sie „Öffnen“.

HiView stellt die Verbindung zum Gerät her und zeigt das Login-Fenster.

Grafische Benutzeroberfläche im Web-Browser starten:

– Voraussetzung ist, dass Java in den Sicherheitseinstellungen Ihres Web-Browsers aktiviert ist.

☐ Starten Sie Ihren Web-Browser.

☐ Schreiben Sie die IP-Adresse des Gerätes in das Adressfeld des Web-Browsers. Verwenden Sie die folgende Form:
`https://xxx.xxx.xxx.xxx`

Der Web-Browser stellt die Verbindung zum Gerät her und zeigt das Login-Fenster.

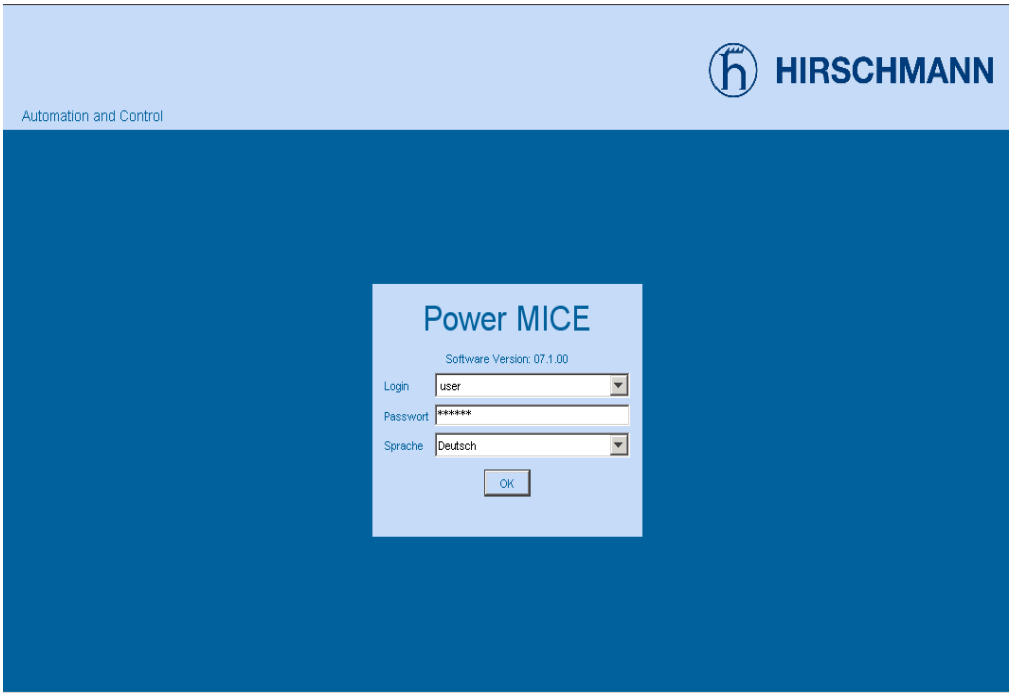


Abb. 5: Login-Fenster

☐ Wählen Sie den Benutzernamen und geben Sie das Passwort ein.
  – Wählen Sie den Benutzernamen `user`, um mit Leserechten auf das Gerät zuzugreifen.
  – Wählen Sie den Benutzernamen `admin`, um mit Schreib- und Leserechten auf das Gerät zuzugreifen.

☐ Wählen Sie die Sprache, in der Sie die grafische Benutzeroberfläche verwenden möchten.

☐ Klicken Sie „Ok“.

Der Web-Browser zeigt die grafische Benutzeroberfläche.

2 IP-Parameter eingeben

Bei der Erstinstallation des Gerätes benötigen Sie die IP-Parameter.

Das Gerät bietet bei der Erstinstallation die folgenden Möglichkeiten zur Eingabe der IP-Parameter:

- Eingabe mit Hilfe des Command Line Interfaces (CLI).
  Diese sogenannte „out-of-band“-Methode wählen Sie, wenn
  - Sie Ihr Gerät außerhalb seiner Betriebsumgebung vorkonfigurieren, oder
  - Sie den Netzzugang („in-band“) zum Gerät wiederherstellen möchten
- Eingabe über das Protokoll HiDiscovery.
  Wählen Sie diese „Inband“-Methode für ein bereits installiertes Netzgerät, oder wenn eine weitere Ethernet-Verbindung zwischen Ihrem PC und dem Gerät besteht.
- Konfiguration mit Hilfe des AutoConfiguration Adapter (ACA).
  Diese Methode wählen Sie, wenn Sie ein Gerät durch ein Gerät des gleichen Typs austauschen und zuvor die Konfiguration auf einem ACA gespeichert haben.
- Verwendung von BOOTP.
  Wählen Sie diese „Inband“-Methode, um die Konfiguration des installierten Gerätes über BOOTP vorzunehmen. Hierzu benötigen Sie einen BOOTP-Server. Der BOOTP-Server weist dem Gerät anhand seiner MAC-Adresse die Konfigurationsdaten zu. Der DHCP-Modus ist der Standardmodus für den Bezug der Konfigurationsdaten. Setzen Sie für diese Methode den Parameter auf den BOOTP-Modus.
- Konfiguration über DHCP.
  Wählen Sie diese „Inband“-Methode, um die Konfiguration des installierten Gerätes über DHCP vorzunehmen. Hierzu benötigen Sie einen DHCP-Server. Der DHCP-Server weist dem Gerät anhand seiner MAC-Adresse oder seines Systemnamens die Konfigurationsdaten zu.

- Konfiguration über DHCP Option 82.
  Diese sogenannte „in-band“-Methode wählen Sie, wenn Sie das bereits installierte Gerät mittels DHCP Option 82 konfigurieren wollen. Hierzu benötigen Sie einen DHCP-Server mit der Option 82. Der DHCP-Server ordnet dem Gerät anhand seiner physikalischen Anbindung die Konfigurationsdaten zu (siehe auf Seite 50 „System-Konfiguration via DHCP-Option 82“).
- Konfiguration über die grafische Benutzeroberfläche.
  Verfügt das Gerät bereits über eine IP-Adresse und ist über das Netz erreichbar, dann bietet Ihnen die grafische Benutzeroberfläche eine weitere Möglichkeit, die IP-Parameter zu konfigurieren.

2.1 Grundlagen IP-Parameter

2.1.1 IP-Adresse (Version 4)

Die IP-Adressen bestehen aus vier Bytes. Die vier Bytes werden durch einen Punkt getrennt, dezimal dargestellt.

Seit 1992 sind im RFC 1340 fünf Klassen von IP-Adressen definiert.

Klasse	Netzadresse	Hostadresse	Adressbereich
A	1 Byte	3 Bytes	0.0.0.0 bis 127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 bis 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 bis 223.255.255.255
D			224.0.0.0 bis 239.255.255.255
E			240.0.0.0 bis 255.255.255.255

Tab. 2: Klassen der IP-Adressen

Die Netzadresse stellt den festen Teil der IP-Adresse dar. Das weltweit oberste Organ für die Vergabe von Netzadressen ist die IANA (Internet Assigned Numbers Authority). Wenn Sie einen IP-Adressblock benötigen, dann kontaktieren Sie Ihren Internet-Service-Provider. Internet-Service-Provider wenden sich an ihre lokale übergeordnete Organisation:

- APNIC (Asia Pacific Network Information Centre) - Asien/Pazifik-Region
- ARIN (American Registry for Internet Numbers) - Amerika und sub-saharisches Afrika
- LACNIC (Regional Latin-American and Caribbean IP Address Registry) – Lateinamerika und Teile der karibischen Inseln
- RIPE NCC (Réseaux IP Européens) - Europa und angrenzende Regionen

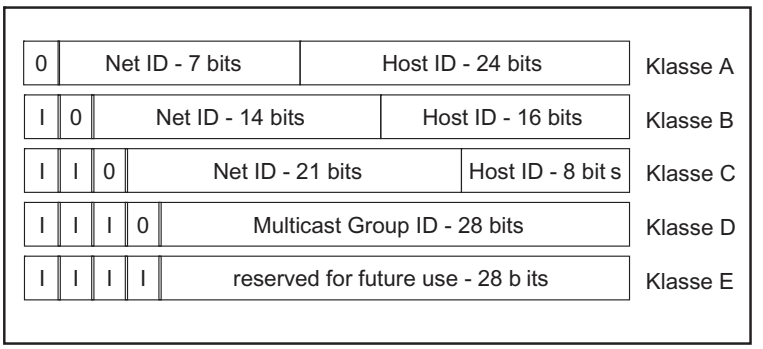


Abb. 6: Bitdarstellung der IP-Adresse

IP-Adressen, deren erstes Bit eine Null ist, das heißt die erste Dezimalzahl kleiner als 128 ist, gehören der Klasse A an.
Ist das erste Bit einer IP-Adresse eine Eins und das zweite Bit eine Null, das heißt die erste Dezimalzahl liegt im Bereich von 128 bis 191, dann gehört die IP-Adresse der Klasse B an.
Sind die ersten beiden Bits einer IP-Adresse eine Eins, das heißt die erste Dezimalzahl ist größer als 191, dann handelt es sich um eine IP-Adresse der Klasse C.

Die Vergabe der Hostadresse (host ID) obliegt dem Netzbetreiber. Er allein ist für die Einmaligkeit der IP-Adressen, die er vergibt, verantwortlich.

2.1.2 Netzmaske

Router und Gateways unterteilen große Netze in Subnetze. Die Netzmaske ordnet die IP-Adressen der einzelnen Geräte einem bestimmten Subnetz zu.

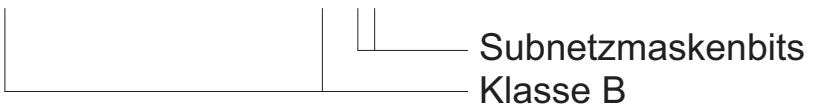
Die Einteilung in Subnetze mit Hilfe der Netzmaske geschieht analog zu der Einteilung in die Klassen A bis C der Netzadresse (net id).

Die Bits der Hostadresse (host id), die die Maske darstellen sollen, werden auf Eins gesetzt. Die restlichen Bits der Hostadresse in der Netzmaske werden auf Null gesetzt (vgl. folgende Beispiele).

Beispiel für eine Netzmaske:

Dezimale Darstellung
255.255.192.0

Binäre Darstellung
11111111.11111111.11000000.00000000



Beispiel für IP-Adressen mit Subnetzzuordnung nach der Netzmaske aus dem obigen Beispiel:

Dezimale Darstellung
129.218.65.17

128 < 129 191 › Klasse B

Binäre Darstellung
10000001.11011010.01000001.00010001

Dezimale Darstellung
129.218.129.17

128 < 129 191 › Klasse B

Binäre Darstellung
10000001.11011010.10000001.00010001

Beispiel für die Anwendung der Netzmaske

In einem großen Netz ist es möglich, dass Gateways oder Router den Management-Agenten von ihrer Managementstation trennen. Wie erfolgt in einem solchen Fall die Adressierung?

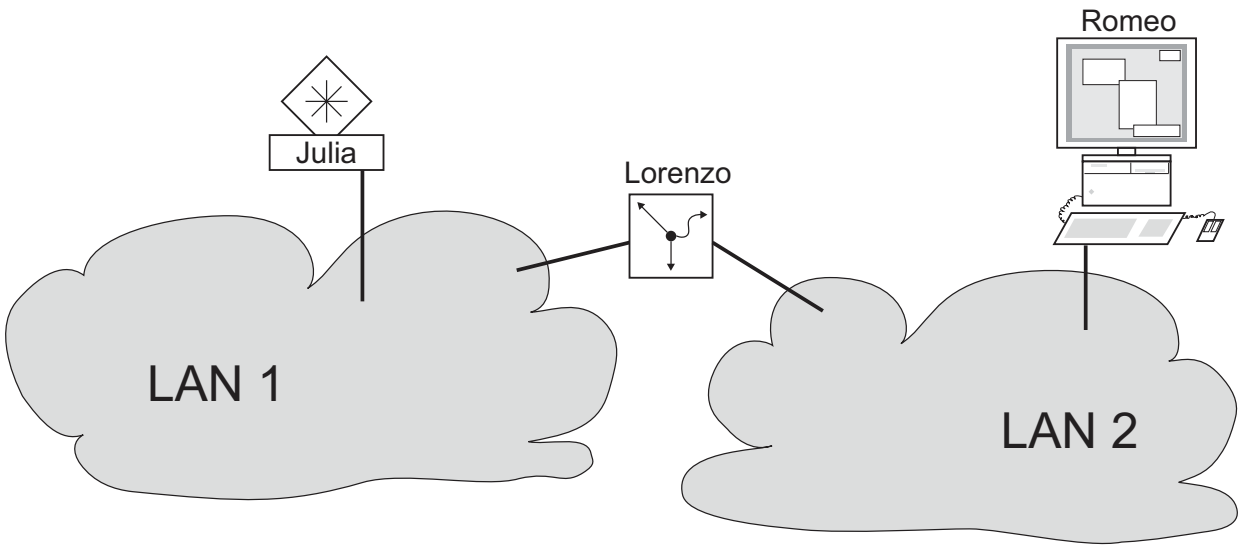


Abb. 7: Management-Agent durch Router von der Managementstation getrennt

Die Managementstation „Romeo” möchte Daten an den Management-Agenten „Julia” schicken. Romeo kennt die IP-Adresse von Julia und weiß, dass der Router „Lorenzo” den Weg zu Julia kennt.

Also packt Romeo seine Botschaft in einen Umschlag und schreibt als Zieladresse die IP-Adresse von Julia und als Quelladresse seine eigene IP-Adresse darauf.

Diesen Umschlag steckt Romeo in einen weiteren Umschlag mit der MAC-Adresse von Lorenzo als Zieladresse und seiner eigenen MAC-Adresse als Quelladresse. Dieser Vorgang ist vergleichbar mit dem Übergang von der Ebene 3 zur Ebene 2 des ISO/OSI-Basis-Referenzmodells.

Nun steckt Romeo das gesamte Datenpaket in den Briefkasten, vergleichbar mit dem Übergang von der Ebene 2 zur Ebene 1, dem Senden des Datenpaketes in das Ethernet.

Lorenzo erhält den Brief, entfernt den äußeren Umschlag und erkennt auf dem inneren Umschlag, dass der Brief für Julia bestimmt ist. Er steckt den inneren Umschlag in einen neuen äußeren Umschlag, schaut in seiner Adressliste, der ARP-Tabelle, nach der MAC-Adresse von Julia und schreibt diese auf den äußeren Umschlag als Zieladresse und seine eigene MAC-Adresse als Quelladresse. Das gesamte Datenpaket steckt er anschließend in den Briefkasten.

Julia empfängt den Brief, entfernt den äußeren Umschlag. Übrig bleibt der innere Umschlag mit Romeos IP-Adresse. Das Öffnen des inneren Umschlages und lesen der Botschaft entspricht einer Übergabe an höhere Protokollschichten des ISO/OSI-Schichtenmodells.

Julia möchte eine Antwort an Romeo zurücksenden. Sie steckt ihre Antwort in einen Umschlag mit der IP-Adresse von Romeo als Zieladresse und ihrer eigenen IP-Adresse als Quelladresse. Doch wohin soll Sie die Antwort schicken? Die MAC-Adresse von Romeo hat sie ja nicht erhalten.
Die MAC-Adresse von Romeo blieb beim Wechseln des äußeren Umschlags bei Lorenzo zurück.

Julia findet in der MIB unter der Variablen hmNetGatewayIPAddr Lorenzo als Vermittler zu Romeo. So steckt sie den Umschlag mit den IP-Adressen in einen weiteren Umschlag mit der MAC-Zieladresse von Lorenzo.

Nun findet der Brief den gleichen Weg über Lorenzo zu Romeo, so wie der Brief von Romeo zu Julia fand.

2.1.3 Classless Inter-Domain Routing

Die Klasse C mit maximal 254 Adressen war zu klein und die Klasse B mit maximal 65.534 Adressen war für die meisten Anwender zu groß. Hieraus resultierte eine nicht effektive Nutzung der zur Verfügung stehenden Klasse B-Adressen.

Die Klasse D enthält reservierte Multicast-Adressen. Die Klasse E ist für experimentelle Zwecke reserviert. Ein Gateway, das nicht an diesen Experimenten teilnimmt, ignoriert Datagramme mit diesen Zieladressen. Seit 1993 bietet die RFC 1519 mit Classless Inter-Domain Routing (CIDR) eine Lösung. Das CIDR überwindet diese Klassenschranken und unterstützt klassenlose IP-Adressbereiche.

Mit CIDR geben Sie die Anzahl der Bits an, die den IP-Adressbereich kennzeichnen. Hierzu stellen Sie den IP-Adressbereich in binärer Form dar und zählen die Maskenbits zur Bezeichnung der Netzmaske. Die Netzmaske gibt die Anzahl der Bits an, welche für die IP-Adressen in einem gegebenen Adressbreich, dem Netz-Teil identisch sind. Beispiel:

IP-Adresse dezimal	Netzmaske dezimal	IP-Adresse binär
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111

25 Maskenbits

CIDR-Schreibweise: 149.218.112.0/25

Maskenbits

Die Zusammenfassung mehrerer Klasse C-Adressbereiche heißt „Supernetting“. Auf diese Weise lassen sich Klasse-B-Adressbereiche sehr fein untergliedern.

2.2 IP-Parameter via CLI eingeben

Sollten Sie weder über BOOTP/DHCP, DHCP Option 82, HiDiscovery Protokoll noch über den AutoConfiguration Adapter ACA das System konfigurieren, dann nehmen Sie die Konfiguration über die V.24-Schnittstelle mit Hilfe des CLI vor.

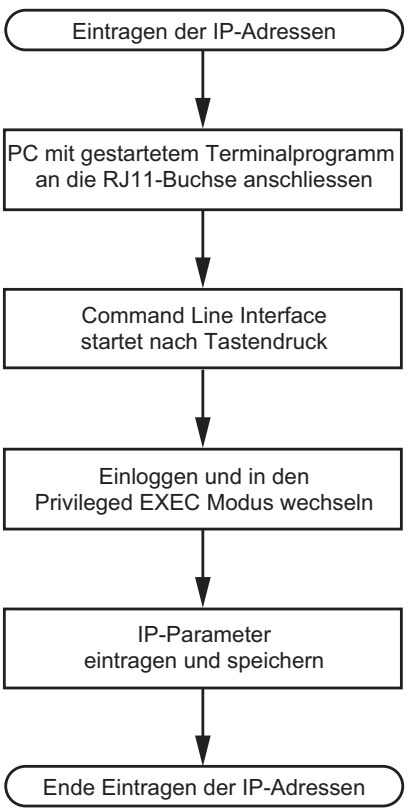


Abb. 8: Ablaufdiagramm Eintragen der IP-Adressen

Anmerkung: Sollten Sie in der Nähe des Installationsortes kein Terminal oder keinen PC mit Terminalemulation zur Verfügung haben, können Sie das Gerät an ihrem Arbeitsplatz konfigurieren und danach an seinen endgültigen Installationsort bringen.

☐ Stellen Sie eine Verbindung mit dem Gerät her (siehe auf Seite 18 „System-Monitor starten“).

Der Start-Bildschirm erscheint.

```
NOTE: Enter '?' for Command Help. Command help displays all options
      that are valid for the 'normal' and 'no' command forms.  For
      the syntax of a particular command form, please consult the
      documentation.


(Hirschmann PowerMICE) >
```

☐ Schalten Sie DHCP aus.

☐ Geben Sie die IP-Parameter ein.

- Lokale IP-Adresse
  Im Lieferzustand besitzt das Gerät die lokale IP-Adresse `0.0.0.0`.
- Netzmaske
  Wenn Sie Ihr Netz in Subnetze aufgeteilt haben und diese mit einer Netzmaske identifizieren, geben Sie an dieser Stelle die Netzmaske ein.

Im Lieferzustand ist die Netzmaske `0.0.0.0` eingetragen.

- IP-Adresse des Gateways.
  Diese Eingabe ist ausschließlich dann notwendig, wenn sich das Gerät und die Managementstation bzw. der TFTP-Server in unterschiedlichen Subnetzen befinden (siehe auf Seite 32 „Beispiel für die Anwendung der Netzmaske“).
  Tragen Sie die IP-Adresse des Gateways ein, welches das Subnetz mit dem Gerät vom Pfad zur Managementstation trennt.
  Im Lieferzustand ist die IP-Adresse `0.0.0.0` eingetragen.

☐ Speichern Sie die eingegebene Konfiguration mit `copy system:running-config nvram:startup-config`.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network protocol none`	DHCP ausschalten.
`network parms 10.0.1.23 255.255.255.0`	Dem Gerät die IP-Adresse 10.0.1.23 und die Netzmaske 255.255.255.0 zuweisen. Optional können Sie zusätzlich eine Gateway-Adresse zuweisen.
`copy system:running-config nvram:startup-config`	Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

Nach Eingabe der IP-Parameter können Sie das Gerät über die grafische Benutzeroberfläche (siehe Referenz-Handbuch „GUI“) komfortabel konfigurieren.

2.3 IP-Parameter per HiDiscovery eingeben

Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät über das Ethernet IP-Parameter zuzuweisen.
Weitere Parameter können Sie mit der grafischen Benutzeroberfläche (siehe Referenz-Handbuch „GUI“ (Graphical User Interface / Web-based Interface)) komfortabel konfigurieren.

Installieren Sie die HiDiscovery-Software auf Ihrem PC. Sie finden die Software auf der CD, die Sie mit dem Gerät erhalten haben.

☐ Zur Installation starten Sie das Installationsprogramm auf der CD.
☐ Starten Sie das Programm HiDiscovery.
Beim Start von HiDiscovery untersucht HiDiscovery automatisch das Netz nach Geräten, die das HiDiscovery-Protokoll unterstützen.
HiDiscovery benutzt das erste gefundene Netz-Interface des PCs. Sollte Ihr Rechner über mehrere Netzwerkkarten verfügen, können Sie das gewünschte in der Werkzeugleiste von HiDiscovery auswählen.

HiDiscovery zeigt für jedes Gerät, das auf das HiDiscovery-Protokoll reagiert, eine Zeile an.

HiDiscovery ermöglicht das Identifizieren der angezeigten Geräte.
☐ Wählen Sie eine Gerätezeile aus.
☐ Klicken Sie auf das Signal-Symbol in der Werkzeugleiste, um das Blinken der LEDs des ausgewählten Gerätes einzuschalten. Ein weiteres Klicken auf das Symbol schaltet das Blinken aus.
☐ Mit einem Doppelklick auf eine Zeile öffnen Sie ein Fenster, in dem Sie den Gerätename und die IP-Parameter eintragen können.

Anmerkung: Mit dem Eintragen der IP-Adresse übernimmt das Gerät die lokalen Konfigurationseinstellungen (siehe auf Seite 55 „Einstellungen laden/speichern“).

Anmerkung: Schalten Sie aus Sicherheitsgründen in der grafischen Benutzeroberfläche die HiDiscovery-Funktion des Gerätes aus, nachdem Sie dem Gerät die IP-Parameter zugewiesen haben (siehe auf Seite 51 „IP-Konfiguration via grafische Benutzeroberfläche“).

Anmerkung: Speichern Sie die Einstellungen, damit Sie die Eingaben nach einem Neustart noch verfügbar haben (siehe auf Seite 55 „Einstellungen laden/speichern“).

2.4 System-Konfiguration vom ACA laden

Der AutoConfiguration Adapter (ACA) ist ein Gerät

- zum Speichern der Konfigurationsdaten eines Gerätes und
- zum Speichern der Geräte-Software.

Sofern ein Gerät nicht betriebsfähig ist, bietet Ihnen der ACA die Möglichkeit, die Konfigurationsdaten auf ein Austauschgerät des selben Typs zu übertragen.

Beim Start prüft das Gerät, ob ein ACA verfügbar ist. Ist ein ACA mit gültigem Passwort und gültiger Software vorhanden, lädt das Gerät die Konfigurationsdaten aus dem ACA.

Das Passwort ist gültig, wenn

- das Passwort im Gerät mit dem Passwort im ACA übereinstimmt oder
- das voreingestellte Passwort im Gerät eingegeben ist.

Um die Konfigurationsdaten im ACA zu speichern, Siehe 65 „Lokal (und auf den ACA) speichern“.

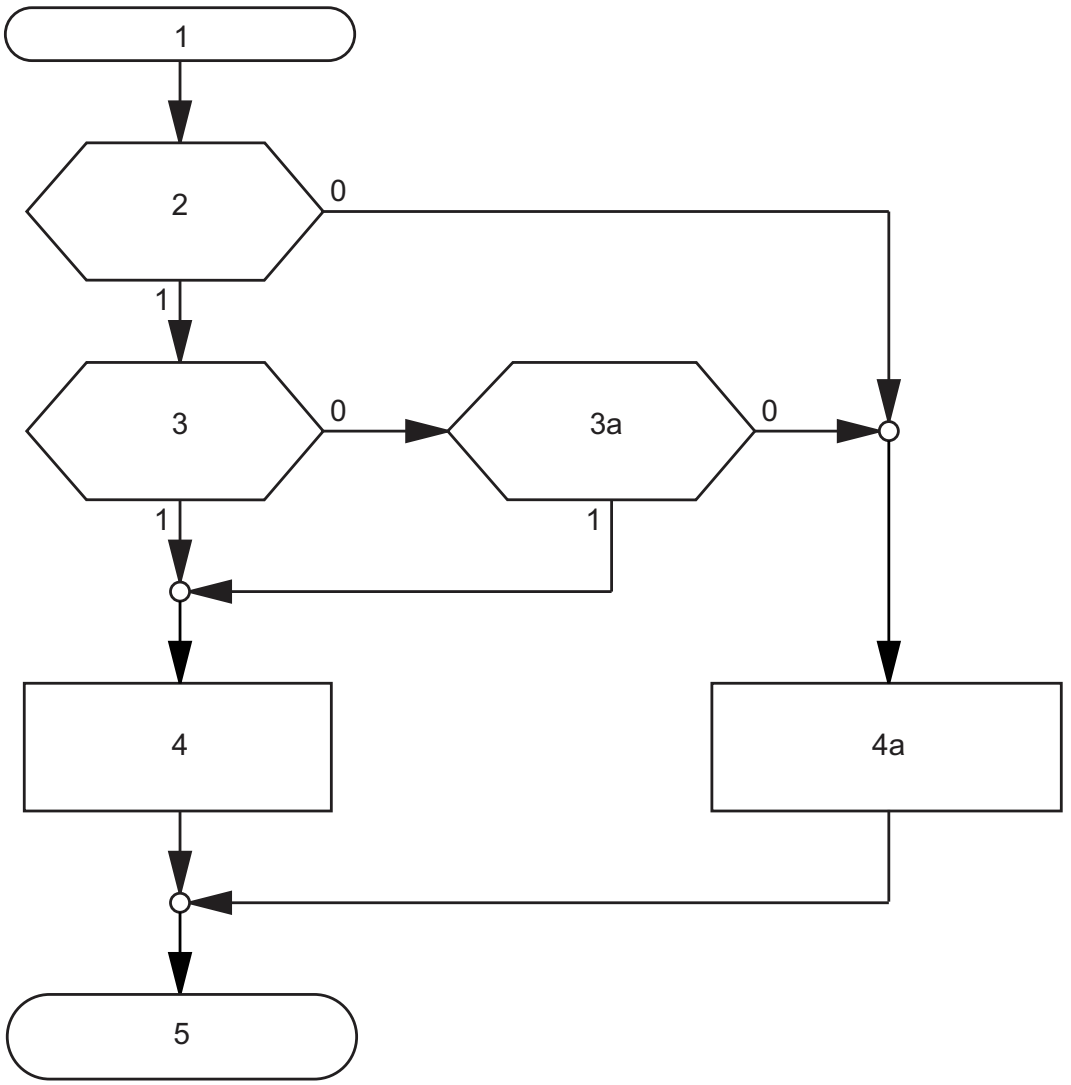


Abb. 9: Ablaufdiagramm Konfigurationsdaten vom ACA laden
1 – Gerät starten
2 – ACA vorhanden?
3 – Passwort im Gerät und ACA identisch?
3a – Voreingestelltes Passwort im Gerät?
4 – Konfiguration vom ACA laden,
ACA-LEDs blinken synchron
4a –Konfiguration aus lokalem Speicher laden,
ACA-LEDs blinken alternierend
5 – Konfigurationsdaten geladen

2.5 System-Konfiguration via BOOTP

Bei der Inbetriebnahme mit Hilfe von BOOTP (Bootstrap Protocol) erhält ein Gerät gemäß dem Ablaufdiagramm "BOOTP-Prozess" (siehe Abbildung 10) seine Konfigurationsdaten.

Anmerkung: Im Lieferzustand bezieht das Gerät seine Konfigurationsdaten vom DHCP-Server.

☐ Aktivieren Sie BOOTP für den Bezug der Konfigurationsdaten (siehe auf Seite 51 „IP-Konfiguration via grafische Benutzeroberfläche“) oder siehe im CLI:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network protocol bootp`	BOOTP aktivieren.
`copy system:running-config nvram:startup-config`	BOOTP aktivieren.
`y`	Speicherwunsch bestätigen..

☐ Stellen Sie dem BOOTP-Server folgende Daten für ein Gerät bereit:

```
# /etc/bootptab for BOOTP-daemon bootpd
#
# gw -- gateway
# ha -- hardware address
# ht -- hardware type
# ip -- IP address
# sm -- subnet mask
# tc -- template

.global:\
:gw=0.0.0.0:\
:sm=255.255.240.0:
```

```
switch_01:ht=ethernet:ha=008063086501:ip=10.1.112.83:tc=.global:
switch_02:ht=ethernet:ha=008063086502:ip=10.1.112.84:tc=.global:
.
.
```

Zeilen mit vorangestelltem #-Zeichen sind Kommentarzeilen.

Die Zeilen unter ".global:" dienen der Arbeitserleichterung bei der Konfiguration mehrerer Geräte. Jedem Gerät weisen Sie mit dem Template (tc) die globalen Konfigurationsdaten (tc=.global:) zu.
In den Gerätezeilen (switch-0...) erfolgt die direkte Zuordnung von Hardware- und IP-Adresse.

☐ Geben Sie für jedes Gerät eine Zeile ein.
☐ Geben Sie nach ha= die Hardware-Adresse des Gerätes ein.
☐ Geben Sie nach ip= die IP-Adresse des Gerätes ein.

Im Anhang finden Sie ein Beispiel zur Konfiguration eines BOOTP/DHCP-Servers.
Siehe „DHCP/BOOTP-Server einrichten” auf Seite 266.

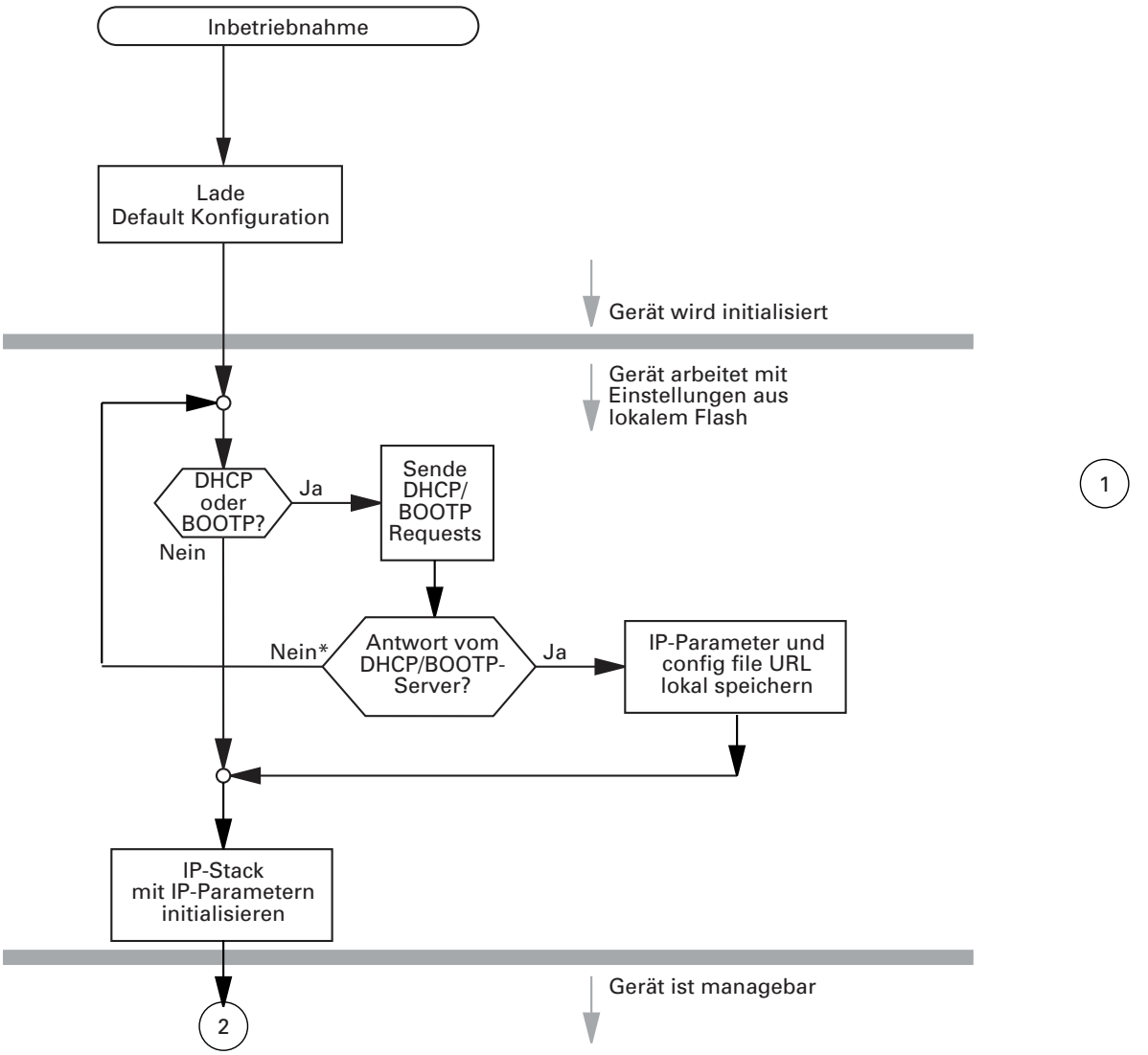


Abb. 10: Ablaufdiagramm BOOTP/DHCP-Prozess, Teil 1
** siehe Hinweis Abbildung 11*

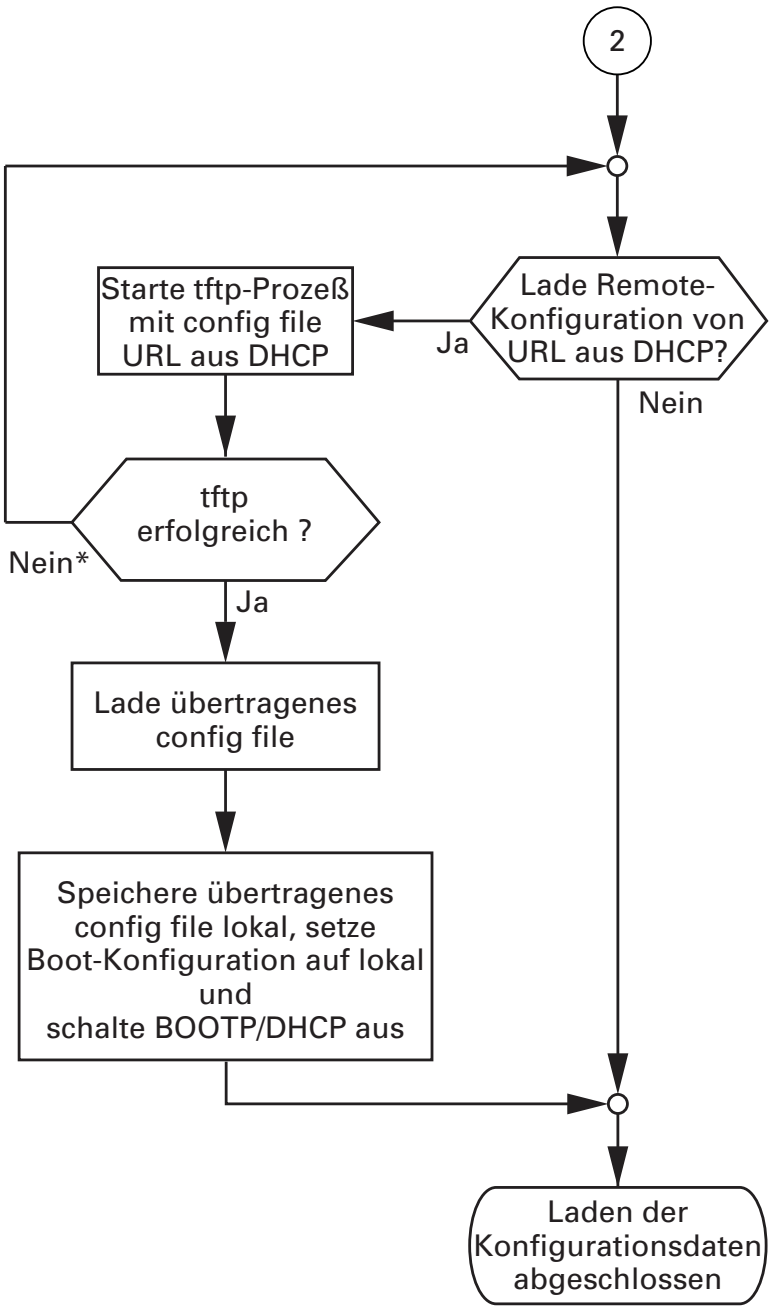


Abb. 11: Ablaufdiagramm BOOTP/DHCP-Prozess, Teil 2

Anmerkung: Den von DHCP/BOOTP (siehe auf Seite 42 „System-Konfiguration via BOOTP“) gestarteten Ladevorgang zeigt die Selektion von „vom URL & lokal speichern“ im Rahmen „Laden“ an. Sollten Sie beim Speichern einer Konfiguration eine Fehlermeldung erhalten, dann kann eine Ursache ein aktiver Ladevorgang sein. DHCP/BOOTP beendet einen Ladevorgang erst, wenn eine gültige Konfiguration geladen ist. Findet DHCP/BOOTP keine gültige Konfiguration, dann beenden Sie den Ladevorgang durch Laden der lokalen Konfiguration im Rahmen „Laden“.

2.6 System-Konfiguration via DHCP

Das DHCP (Dynamic Host Configuration Protocol) ist eine Weiterentwicklung von BOOTP und hat dieses abgelöst. DHCP bietet zusätzlich die Konfiguration eines DHCP-Clients über einen Namen anstatt über die MAC-Adresse an.
Dieser Name heißt bei DHCP nach RFC 2131 "Client Identifier".
Das Gerät verwendet den in der System-Gruppe der MIB II unter sysName eingetragenen Namen als Client Identifier. Die Eingabe dieses Systemnamens können Sie direkt vornehmen über SNMP, das Web-based Management (siehe System-Dialog) oder das Command Line Interface.

Bei der Inbetriebnahme erhält ein Gerät gemäß dem Ablaufdiagramm "DHCP-Prozess" (siehe Abbildung 10) seine Konfigurationsdaten.

Das Gerät übermittelt seinen Systemnamen dem DHCP-Server. Der DHCP-Server kann dann alternativ zur MAC-Adresse anhand des Systemnamens eine IP-Adresse vergeben.

Neben der IP-Adresse überträgt der DHCP-Server

- die Netzmaske
- das Default-Gateway (falls vorhanden)
- die TFTP-URL der Konfigurationsdatei (falls vorhanden)

Das Gerät übernimmt diese Daten als Konfigurationsparameter (siehe auf Seite 51 „IP-Konfiguration via grafische Benutzeroberfläche“). Wurde eine IP-Adresse von einem DHCP-Server zugeteilt, wird diese permanent lokal gespeichert.

Option	Bedeutung
1	Subnet Mask
2	Time Offset
3	Router

Tab. 3: DHCP-Optionen, die das Gerät anfordert

Option	Bedeutung
4	Time server
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Tab. 3: DHCP-Optionen, die das Gerät anfordert

Der Vorteil beim Einsatz von DHCP gegenüber BOOTP ist, dass der DHCP-Server die Gültigkeit der Konfigurationsparameter (“Lease”) auf eine bestimmte Zeitspanne einschränken kann (sogenannte dynamische Adress-Vergabe) Rechtzeitig vor Ablauf dieser Zeitspanne (“Lease Duration”), kann der DHCP-Client versuchen, dieses Lease zu erneuern. Alternativ kann er ein neues Lease aushandeln. Der DHCP-Server weist dann eine beliebige freie Adresse zu.
Um dies zu umgehen, bieten DHCP-Server die explizite Konfigurationsmöglichkeit, einem bestimmten Client anhand einer eindeutigen Hardware-ID dieselbe IP-Adresse zuzuordnen (sogenannte statische Adressvergabe).

Im Lieferzustand ist DHCP aktiviert. Solange DHCP aktiviert ist, versucht das Gerät, eine IP-Adresse zu bekommen. Findet das Gerät nach einem Neustart keinen DHCP-Server, hat es keine IP-Adresse. Der Dialog `Grund-einstellungen:Netz:Global` bietet Ihnen die Möglichkeit, DHCP zu aktivieren oder zu deaktivieren.

Anmerkung: Achten Sie bei der Anwendung des Netzmanagements Industrial HiVision darauf, dass DHCP jedem Gerät die original IP-Adresse zuweist.

Im Anhang finden Sie ein Beispiel zur Konfiguration eines BOOTP/DHCP-Servers (siehe auf Seite 266 „DHCP/BOOTP-Server einrichten“).

Beispiel für eine DHCP-Konfigurationsdatei:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Zeilen mit vorangestelltem #-Zeichen sind Kommentarzeilen.
Die Zeilen vor den einzeln aufgeführten Geräten bezeichnen Einstellungen, welche für die folgenden Geräte gelten.
Die Zeile fixed-address weist dem Gerät eine feste IP-Adresse zu.
Weitere Informationen entnehmen Sie Ihren DHCP-Server-Handbuch.

2.7 System-Konfiguration via DHCP-Option 82

Wie beim klassischen DHCP erhält bei der Inbetriebnahme ein Agent gemäß dem Ablaufdiagramm „BOOTP/DHCP-Prozess“ (siehe Abbildung 10) seine Konfigurationsdaten.

Während sich die System-Konfiguration über das klassische DHCP-Protokoll (siehe auf Seite 47 „System-Konfiguration via DHCP“) am zu konfigurierenden Gerät orientiert, orientiert sich die Option 82 an der Netztopologie. Dieses Verfahren bietet somit die Möglichkeit, einem beliebigen Gerät, das an einem bestimmten Ort (Port eines Gerätes) am LAN angeschlossen wird, immer die selbe IP-Adresse zuzuordnen.
Die Installation eines DHCP-Servers beschreibt das Kapitel „DHCP-Server Option 82 einrichten” auf Seite 272.

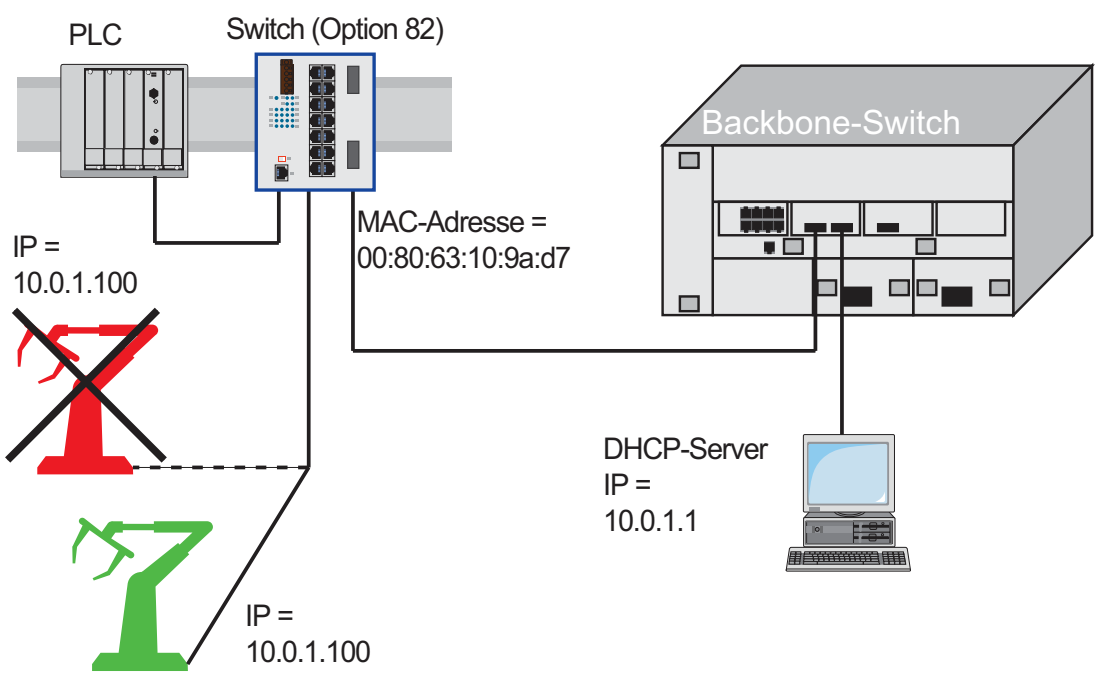


Abb. 12: Anwendungsbeispiel für den Einsatz von Option 82

2.8 IP-Konfiguration via grafische Benutzeroberfläche

Mit dem Dialog `Grundeinstellungen:Netz` legen Sie fest, aus welcher Quelle das Gerät seine IP-Parameter nach dem Start erhält, weisen IP-Parameter und VLAN-ID zu und konfigurieren den HiDiscovery-Zugriff.

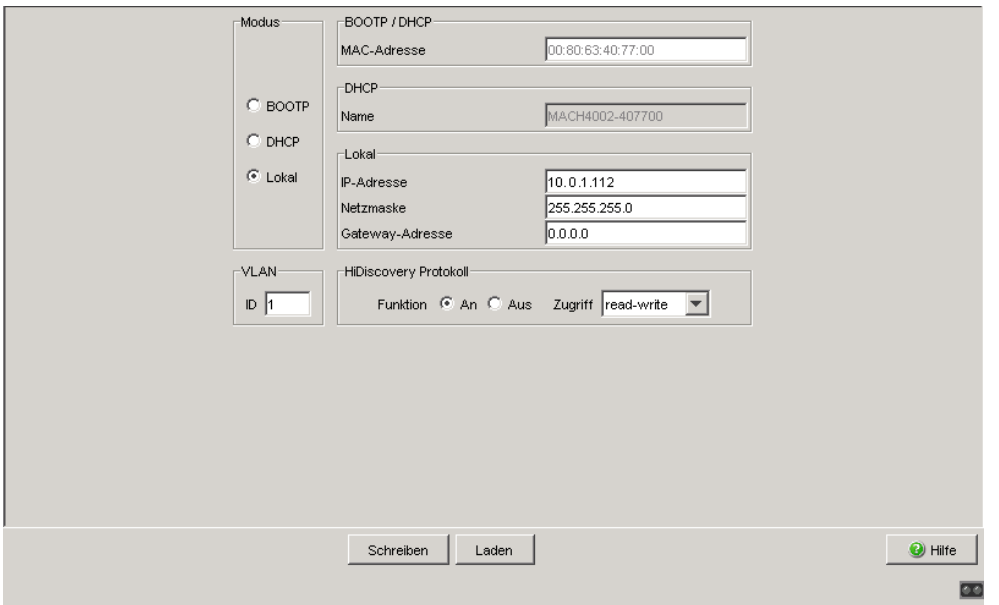


Abb. 13: Dialog Netzparameter

☐ Geben Sie unter „Modus“ ein, woher das Gerät seine IP-Parameter bezieht:

- Im Modus BOOTP erfolgt die Konfiguration durch einen BOOTP- oder DHCP-Server auf der Basis der MAC-Adresse des Gerätes.
  Siehe „DHCP/BOOTP-Server einrichten” auf Seite 266.
- Im Modus DHCP erfolgt die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes.
  Siehe „DHCP-Server Option 82 einrichten” auf Seite 272.
- Im Modus „lokal“ werden die Netzparameter aus dem Speicher des Gerätes verwendet.

☐ Geben Sie entsprechend des gewählten Modus rechts die Parameter ein.

☐ Den für das DHCP-Protokoll relevanten Namen geben Sie in der grafischen Benutzeroberfläche in der Zeile „Name“ des Dialogs `Grundeinstellungen:System` ein.

☐ Der Rahmen „VLAN“ bietet Ihnen die Möglichkeit, der Management-CPU des Geräts ein VLAN zuzuweisen. Wenn Sie hier als VLAN-ID 0 eingeben (im VLAN-Standard nicht enthalten), dann ist die Management-CPU von allen VLANs erreichbar.

☐ Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät eine IP-Adresse zuzuweisen. Aktivieren Sie das HiDiscovery-Protokoll, wenn Sie von Ihrem PC aus mit der mitgelieferten HiDiscovery-Software dem Gerät eine IP-Adresse zuweisen wollen (Lieferzustand: „Funktion“ `An`, „Zugriff“ `read-write`).

Anmerkung: Speichern Sie die Einstellungen, damit Sie die Eingaben nach einem Neustart noch verfügbar haben (siehe auf Seite 55 „Einstellungen laden/speichern“).

2.9 Defekte Geräte ersetzen

Das Gerät bietet 2 Plug-and-Play-Lösungen zum Austauschen eines defekten Gerätes durch ein Gerät des gleichen Typs (Faulty Device Replacement):

- Konfiguration des neuen Gerätes mit Hilfe eines AutoConfiguration Adapters (siehe auf Seite 40 „System-Konfiguration vom ACA laden“) oder
- Konfiguration mit Hilfe des DHCP Option 82 (siehe auf Seite 272 „DHCP-Server Option 82 einrichten“).

In beiden Fällen erhält das neue Gerät beim Starten die gleichen Konfigurationsdaten, die das ersetzte Gerät hatte.

Anmerkung: Wenn Sie ein Gerät mit DIP-Schaltern ersetzen, prüfen Sie die DIP-Schalterstellungen, um sicherzustellen, dass sie dieselben sind.

Anmerkung: Wenn Sie per SSH auf das Gerät zugreifen wollen, benötigen Sie zusätzlich einen SSH-Schlüssel. Um den SSH-Schlüssel des alten Geräts auf das neue zu bringen, haben Sie folgende Möglichkeiten:

- Wenn Sie den Schlüssel bereits erzeugt und außerhalb des Geräts gespeichert haben (z.B. auf Ihrer Administrations-Workstation), laden Sie den gespeicherten Schlüssel auf das neue Gerät (siehe auf Seite 283 „Schlüssel auf das Gerät laden“).

- Andernfalls erzeugen Sie einen neuen SSH-Schlüssel und laden ihn auf das neue Gerät (siehe auf Seite 281 „SSH-Zugriff vorbereiten“). Beachten Sie, dass sich das neue Gerät nun durch einen anderen Schlüssel identifiziert.

3 Einstellungen laden/speichern

Einstellungen wie z.B. IP-Parameter und Portkonfiguration speichert das Gerät im flüchtigen Arbeitsspeicher. Diese gehen beim Ausschalten oder einem Neustart verloren.
Das Gerät bietet Ihnen die Möglichkeit,

- Einstellungen von einem nicht-flüchtigen Speicher in den flüchtigen Arbeitsspeicher zu laden,
- Einstellungen aus dem flüchtigen Arbeitsspeicher in einen nichtflüchtigen Speicher zu speichern.

Wenn Sie die laufende Konfiguration verändern (z. B. einen Port ausschalten), ändert die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol im Navigationsbaum von einem Diskettensymbol in ein gelbes Dreieck. Nach dem Speichern der Konfiguration zeigt die grafische Benutzeroberfläche das „Laden/Speichern“-Symbol wieder als Diskette an.

3.1 Einstellungen laden

Bei einem Neustart lädt das Gerät seine Konfigurationsdaten vom lokalen nichtflüchtigen Speicher. Die Voraussetzungen dafür sind:

- Sie haben keinen AutoConfiguration Adapter (ACA) angeschlossen und
- die IP-Konfiguration ist „lokal“.

Bei einem Neustart bietet Ihnen das Gerät außerdem die Möglichkeit, Einstellungen aus folgenden Quellen zu laden:

- aus einer Binärdatei vom AutoConfiguration Adapter. Ist ein ACA am Gerät angeschlossen, dann lädt das Gerät seine Konfiguration während des Boot-Vorgangs automatisch vom ACA.
- aus einer Skriptdatei vom AutoConfiguration Adapter. Ist ein ACA am Gerät angeschlossen, dann lädt das Gerät seine Konfiguration während des Boot-Vorgangs automatisch aus der Skriptdatei auf dem ACA (siehe auf Seite 61 „Laden eines Skripts vom ACA“).

Anmerkung: Details zur Dauer eines Neustarts:

- Die Zeit für einen Kaltstart ist die Zeit, die das Gerät vom Einschalten der Stromversorgung braucht, bis es voll vermittelt und seine Management-CPU voll erreichbar ist.
- Ein Kaltstart dauert abhängig vom Gerätetyp und dem Umfang der Konfigurationseinstellungen minimal ca. 10 Sekunden.
- Eine umfangreiche Konfiguration verlängert die Dauer eines Neustarts, vor allem, wenn sie viele VLANs enthält. Der Neustart kann im Extremfall bis zu ca. 200 Sekunden dauern.
- Ein Warmstart ist kürzer, weil das Gerät in diesem Fall das Laden der Software aus dem NVRAM überspringt.

Während des Betriebs bietet Ihnen das Gerät die Möglichkeit, Einstellungen aus folgenden Quellen zu laden:

- vom lokalen nicht-flüchtigen Speicher,
- aus einer Datei im angeschlossenen Netz (Einstellung im Lieferzustand)
- aus einer Binärdatei oder einem editier- und lesbaren Skript vom PC und
- aus der Firmware (Wiederherstellung der Konfiguration des Lieferzustands).

Anmerkung: Wenn Sie eine Konfiguration laden, dann warten Sie mit einem Zugriff auf das Gerät, bis dieses die Konfigurationsdatei geladen und die neuen Konfigurationseinstellungen vorgenommen hat.
Abhängig vom Gerätetyp und dem Umfang der Konfigurationseinstellungen kann dieser Vorgang 10-200 Sekunden dauern.

3.1.1 Laden aus lokalem nicht-flüchtigen Speicher

Beim lokalen Laden der Konfigurationsdaten lädt das Gerät die Konfigurationsdaten aus dem lokalen nicht-flüchtigen Speicher, sofern kein ACA am Gerät angeschlossen ist.

☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
☐ Klicken Sie im Rahmen „Laden“ auf „vom Gerät“.
☐ Klicken Sie auf „Wiederherstellen“.

```
enable
copy nvram:startup-config
  system:running-config
```

Wechsel in den Privileged-EXEC-Modus.
Das Gerät lädt die Konfigurationsdaten aus dem lokalen nicht-flüchtigen Speicher.

3.1.2 Laden aus einer Datei

Das Gerät bietet Ihnen die Möglichkeit, die Konfigurationsdaten aus einer Datei im angeschlossenen Netz zu laden, sofern kein AutoConfiguration Adapter am Gerät angeschlossen ist.

- ☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie im Rahmen „Laden“ auf
  - ▶ „vom URL“, wenn das Gerät die Konfigurationsdaten aus einer Datei laden soll und die lokal gespeicherte Konfiguration erhalten bleiben soll.
  - ▶ „vom URL & auf dem Gerät speichern“, wenn das Gerät die Konfigurationsdaten aus einer Datei laden soll und diese Konfiguration auch lokal speichern soll.
  - ▶ „via PC“, wenn das Gerät die Konfigurationsdaten aus einer Datei vom PC laden soll und die lokal gespeicherte Konfiguration erhalten bleiben soll.
- ☐ Geben Sie im Rahmen „URL“ den Pfad an, unter welchem das Gerät die Konfigurationsdatei findet, falls Sie vom URL laden möchten.
- ☐ Klicken Sie auf „Wiederherstellen“.

Anmerkung: Beachten Sie beim Wiederherstellen einer Konfiguration durch eine der Optionen im Rahmen „Laden“ folgende Besonderheiten:

- ▶ Das Gerät kann die Konfiguration aus einer Binär- oder einer Skript-Datei wiederherstellen:
  - – Die Option „vom Gerät“ stellt die Konfiguration ausschließlich aus der Geräte-internen Binärdatei wieder her.
  - – Die 3 Optionen „vom URL“, „vom URL & auf dem Gerät speichern“ oder „via PC“ können die Konfiguration sowohl aus einer Binärdatei als auch aus einer Skript-datei wiederherstellen. Die Skriptdatei kann eine Offline-Konfigurations-Datei (*.ocf) oder eine CLI-Skriptdatei (*.cli) sein. Das Gerät ermittelt den Dateityp auto-matisch.
- ▶ Wenn Sie die Konfiguration aus einer Skriptdatei wiederherstellen, löschen Sie zuerst die Gerätekonfiguration, so dass die Voreinstel-lungen richtig überschrieben werden. Für weitere Informationen (siehe auf Seite 60 „Die aktuelle Konfiguration in den Lieferzustand zurückzusetzen.“)

Der URL kennzeichnet den Pfad zum tftp-Server von dem das Gerät die Konfigurationsdatei lädt. Der URL hat die Form tftp://IP-Adresse des tftp-Servers/Pfadname/Dateiname (z.B. `tftp://10.1.112.5/switch/config.dat`).

Beispiel zum Laden von einem tftp-Server

☐ Bevor Sie eine Datei vom tftp-Server herunterladen können, speichern Sie die Konfigurationsdatei in den entsprechenden Pfad des tftp-Servers mit dem Dateinamen, z.B. `switch/switch_01.cfg`(siehe auf Seite 67 „Speichern in eine Binär- oder Skript-Datei auf einem URL“).

☐ Geben Sie in der Zeile „URL“ den Pfad des tftp-Servers ein, z.B. `tftp://10.1.112.214/switch/switch_01.cfg`.

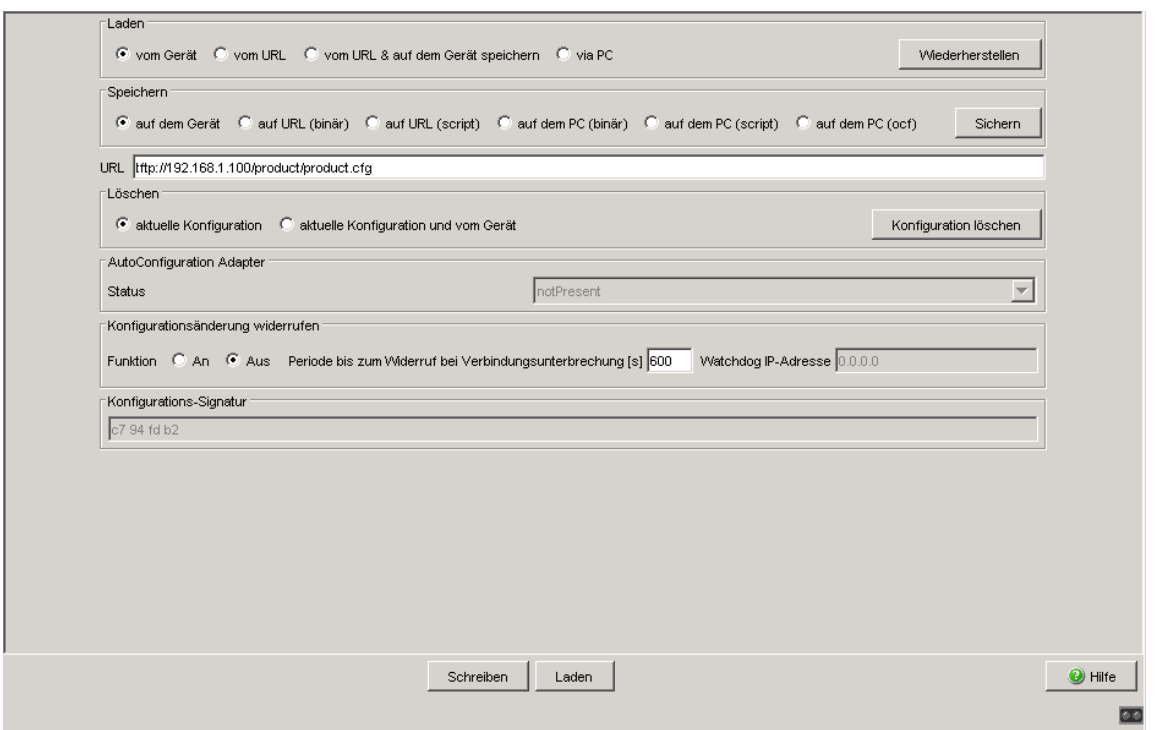


Abb. 14: Dialog Laden/Speichern

```
enable
copy
tftp://10.1.112.159/switch/c
onfig.dat
  nvram:startup-config
```

Wechsel in den Privileged-EXEC-Modus.
Das Gerät lädt die Konfigurationsdaten von einem tftp-Server im angeschlossenen Netz.

Anmerkung: Den von DHCP/BOOTP (siehe auf Seite 42 „System-Konfiguration via BOOTP“) gestarteten Ladevorgang zeigt die Selektion von „vom URL & lokal speichern“ im Rahmen „Laden“ an. Sollten Sie beim Speichern einer Konfiguration eine Fehlermeldung erhalten, dann kann eine Ursache ein aktiver Ladevorgang sein. DHCP/BOOTP beendet einen Ladevorgang erst, wenn eine gültige Konfiguration geladen ist. Findet DHCP/BOOTP keine gültige Konfiguration, dann beenden Sie den Ladevorgang durch Laden der lokalen Konfiguration im Rahmen „Laden“.

3.1.3 Die aktuelle Konfiguration in den Lieferzustand zurückzusetzen.

Das Gerät ermöglicht Ihnen,

- die aktuelle Konfiguration in den Lieferzustand zurückzusetzen. Die lokal gespeicherte Konfiguration bleibt erhalten.
- das Gerät in den Lieferzustand zurückzusetzen. Nach dem nächsten Neustart ist auch die IP-Adresse im Lieferzustand.

☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
☐ Treffen Sie Ihre Wahl im Rahmen „Löschen“.
☐ Klicken Sie auf „Konfiguration löschen“. Das Gerät löscht seine Konfiguration sofort.

Zurücksetzen des Gerätes über den System-Monitor

☐ Wählen Sie 5 „Erase main configuration file“
Dieser Menüpunkt bietet Ihnen die Möglichkeit, die aktuelle Konfiguration in den Lieferzustand zurückzusetzen. Die Konfiguration selbst liegt im nicht-flüchtigen Speicher. Ebenso speichert das Gerät eine Sicherungskopie der Konfiguration sowie eine mit der Firmware assoziierte Konfiguration im Flash-Speicher.
☐ Drücken sie die Eingabetaste, um die Konfigurationsdatei zu löschen.

3.1.4 Laden vom AutoConfiguration Adapter

Laden einer Konfiguration während des Boot-Vorgangs

Wenn Sie einen ACA an das Gerät anschließen, während sich die Passwörter auf dem Gerät noch im Lieferzustand befinden, fehlen oder mit denen des ACA identisch sind, lädt das Gerät seine Konfiguration während des Boot-Vorgangs automatisch vom ACA. Nach dem Boot-Vorgang aktualisiert das Gerät seine Konfiguration im lokalen nicht-flüchtigen Speicher mit der Konfiguration aus dem ACA.

Anmerkung: Während des Boot-Vorgangs hat die Konfiguration auf dem ACA Vorrang vor der Konfiguration im lokalen nicht-flüchtigen Speicher.

Das Kapitel „Lokal (und auf den ACA) speichern” auf Seite 65 beschreibt, wie Sie eine Konfigurationsdatei auf einen ACA speichern.

Laden eines Skripts vom ACA

Enthält der ACA eine Skriptdatei, dann lädt das Gerät seine Konfiguration während des Boot-Vorgangs automatisch aus der Skiptdatei auf dem ACA. Die Voraussetzungen dafür sind:

- Der ACA ist während des Bootvorgangs angeschlossen.
- Im Hauptverzeichnis des ACA befindet sich keine Binärkonfiguration.

- Im Hauptverzeichnis des ACA befindet sich eine Datei mit dem Namen „autoupdate.txt“.
- Die Datei „autoupdate.txt“ ist eine Textdatei und enthält eine Zeile mit einem Inhalt nach dem Muster `script=<file_name>`. Dabei steht `<file_name>` für den Namen der zu ladenden Skriptdatei, z.B. `custom.cli`.
- Die mittels `script=<file_name>` angegebene Datei, z.B. `custom.cli` befindet sich im Hauptverzeichnis des ACA und ist eine gültige Skriptdatei.

Ist im lokalen nicht-flüchtigen Speicher des Gerätes eine Konfiguration vorhanden, ignoriert das Gerät diese.
Das Gerät aktualisiert nach dem Anwenden des Skripts die Konfiguration im lokalen nicht-flüchtigen Speicher mit der aus dem Skript.
Dabei schreibt es außerdem die aktuelle Binärkonfiguration auf den ACA.

Anmerkung: Beim Boot-Vorgang hat eine Binärkonfiguration auf dem ACA Vorrang vor einem Skript auf dem ACA.

Das Kapitel „Lokal (und auf den ACA) speichern“ beschreibt, wie Sie eine Skriptdatei auf einen ACA speichern können.

Melden von Konfigurationsunterschieden

Das Gerät bietet Ihnen die Möglichkeit, folgende Ereignisse auszulösen, wenn die auf dem ACA gespeicherte Konfiguration nicht mit der im Gerät übereinstimmt:

- einen Trap zu senden (siehe auf Seite 221 „Trapeinstellung“),
- den Gerätestatus zu aktualisieren (siehe auf Seite 224 „Gerätestatus konfigurieren“),
- den Zustand der Meldekontakte zu aktualisieren (siehe auf Seite 227 „Meldekontakt steuern“).

3.1.5 Den Offline-Konfigurator verwenden

Der Offline-Konfigurator bietet Ihnen die Möglichkeit, Konfigurationen für Geräte im Voraus zu erstellen. Sie erstellen die Konfiguration virtuell auf Ihrem PC und laden sie in einem 2. Schritt auf Ihr Gerät..

Auf diese Weise können Sie die Geräte-Konfiguration effizient vorbereiten und verwalten, und sparen Zeit und Aufwand sowohl beim Erstellen der Konfiguration als auch beim Laden auf die Geräte.

Die Details zur Bedienung des Offline-Konfigurators finden Sie im Dokument „Referenz-Handbuch GUI“ (Graphical User Interface / Web-based Interface) im Kapitel „Konfiguration von Offline-Konfigurator laden“.

Beispiel für den Einsatz des Offline-Konfigurators

Ein IT-Mitarbeiter erstellt die Konfigurationsdateien für die Geräte einer Fertigungszelle bereits in der Planungsphase. Dabei greift er auf bereits vorhandene Konfigurationsdateien für eine gleichartige Fertigungszelle zurück und passt diese an.
Er stellt die Offline-Konfigurationsdateien dem Außendienst-Mitarbeiter zur Verfügung, der die Geräte vor Ort montiert und die Konfiguration anschließend auf die Geräte lädt. Dazu ist lediglich erforderlich, dass die Geräte erreichbar sind und eine IP-Adresse z.B. über HiDiscovery erhalten haben.

Datenformat

Der Offline-Konfigurator liest und schreibt Konfigurations-Dateien in einem XML-basierten Format. Die Dateinamen-Erweiterung dieser Dateien ist „.ocf“ (Offline Configurator Format).

Über die grafische Benutzeroberfläche sind Sie dazu in der Lage, diese Dateien zu laden und Ihre Geräte innerhalb kürzester Zeit zu konfigurieren.

Das XML-Format bietet Ihnen zudem die Möglichkeit, andere Werkzeuge zum Erzeugen, Bearbeiten und Verwalten der Offline-Konfigurationsdateien einzusetzen und so Ihre Administrations-Prozesse zu optimieren.

Installations- und Betriebs-Voraussetzungen

Voraussetzung für die Installation ist ein PC mit einem Betriebssystem Windows™ XP (mit Service Pack 3) oder neuer.
Installieren Sie den Offline-Konfigurator von der Produkt-CD, die dem Gerät beiliegt. Starten Sie dazu die Installationsdatei „Setup.exe“ aus dem Ordner „ocf_setup“.

Der Offline-Konfigurator verwendet – genau wie die grafische Benutzeroberfläche – die Java-Software 6 („Java™ Runtime Environment (JRE) Version 1.6.x“).
Installieren Sie die Software von www.java.com.

Bedienung des Offline-Konfigurators

Starten Sie den Offline-Konfigurator durch Doppelklick auf das Desktop-Symbol „Offline Management“.

Die Details zur Bedienung des Offline-Konfigurators finden Sie im Dokument „Referenz-Handbuch GUI“ (Graphical User Interface / Web-based Interface) im Kapitel „Konfiguration von Offline-Konfigurator laden“.

3.2 Einstellungen speichern

Im Rahmen „Speichern“ haben Sie die Möglichkeit,

- die aktuelle Konfiguration auf dem Gerät speichern,
- die aktuelle Konfiguration in einer Datei unter dem angegebenen URL im Binärformat oder als editier- und lesbares Skript zu speichern,
- die aktuelle Konfiguration im Binärformat oder als editier- und lesbares CLI-Skript auf dem PC zu speichern,
- die aktuelle Konfiguration für den Offline-Konfigurator im XML-Format auf dem PC zu speichern.

3.2.1 Lokal (und auf den ACA) speichern

Das Gerät bietet Ihnen die Möglichkeit, die aktuellen Konfigurationsdaten in den lokalen nicht-flüchtigen Speicher und den ACA zu speichern.

☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
☐ Klicken Sie im Rahmen „Speichern“ auf „auf dem Gerät“.
☐ Klicken Sie auf „Sichern“.
Das Gerät speichert die aktuellen Konfigurationsdaten in den lokalen nicht-flüchtigen Speicher und, sofern ein ACA angeschlossen ist, auch in den ACA.

```
enable
copy system:running-config
  nvram:startup-config
```

Wechsel in den Privileged-EXEC-Modus.
Das Gerät speichert die aktuellen Konfigurationsdaten in den lokalen nicht-flüchtigen Speicher und, sofern ein ACA angeschlossen ist, auch in den ACA

Anmerkung: Nachdem Sie die Konfiguration erfolgreich auf dem Gerät gespeichert haben, sendet das Gerät einen Trap `hmConfigurationSavedTrap`, zusammen mit der Information über einen ggf. angeschlossenen AutoConfiguration Adapter (ACA). Wenn Sie die Konfiguration nach dem Speichern zum ersten Mal verändern, sendet das Gerät einen Trap `hmConfigurationChangedTrap`.

Anmerkung: Das Gerät bietet Ihnen die Möglichkeit, folgende Ereignisse auszulösen, wenn die auf dem ACA gespeicherte Konfiguration nicht mit der im Gerät übereinstimmt:

- einen Trap zu senden (siehe auf Seite 221 „Trapeinstellung“),
- den Gerätestatus zu aktualisieren (siehe auf Seite 224 „Gerätestatus konfigurieren“),
- den Zustand der Meldekontakte zu aktualisieren (siehe auf Seite 227 „Meldekontakt steuern“).

ACA21 in der Bootphase überspringen

Das Gerät bietet Ihnen die Möglichkeit, einen gesteckten AutoConfiguration Adapter ACA21 in der Bootphase zu überspringen. In diesem Fall ignoriert das Gerät den ACA21 in der Bootphase. Sie verkürzen damit die Dauer der Bootphase des Gerätes um 1 bis 4 Sekunden. Wenn Sie diese Funktion eingeschaltet haben, steht Ihnen die ACA21-Funktionalität nach der Bootphase wie gewohnt zur Verfügung. Das Gerät überspringt lediglich die ACA21-Ladevorgänge in der Bootphase.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Global-Configure-Modus.
`#boot skip-aca-on-boot enable`	Den ACA21 in der Bootphase überspringen. (Lieferzustand: ausgeschaltet).
`#boot skip-aca-on-boot disable`	Den ACA21 in der Bootphase berücksichtigen.
`#show boot skip-aca-on-boot`	Anzeigen, ob die Funktion „Den ACA21 in der Bootphase überspringen“ eingeschaltet ist.

3.2.2 Speichern in eine Binär- oder Skript-Datei auf einem URL

Das Gerät bietet Ihnen die Möglichkeit, die aktuellen Konfigurationsdaten in eine Datei im angeschlossenen Netz zu speichern.

Anmerkung: Die Konfigurationsdatei enthält alle Konfigurationsdaten, auch das Passwort. Achten Sie deshalb auf die Zugriffsrechte auf dem tftp-Server.

- ☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Wählen Sie im Rahmen „Speichern“
  „auf URL (binär)“, um eine Binär-Datei zu erzeugen, oder
  „auf URL (script)“, um eine editier- und lesbares Skript-Datei zu erzeugen.
- ☐ Geben Sie im Rahmen „URL“ den Pfad an, unter welchem das Gerät die Konfigurationsdatei speichern soll.

Der URL kennzeichnet den Pfad zum tftp-Server, auf den das Gerät die Konfigurationsdatei speichert. Der URL hat die Form tftp://IP-Adresse des tftp-Servers/Pfadname/Dateiname (z.B. `tftp://10.1.112.5/switch/config.dat`).

- ☐ Klicken Sie auf „Sichern“.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy nvram:startup-config tftp://10.1.112.159/switch/config.dat`	Das Gerät speichert die Konfigurationsdaten in eine Binärdatei auf einen tftp-Server im angeschlossenen Netz
`copy nvram:script tftp://10.0.1.159/switch/config.txt`	Das Gerät speichert die Konfigurationsdaten in eine Script-Datei auf einen tftp-Server im angeschlossenen Netz.

Anmerkung: Wenn Sie die Konfiguration in eine Binärdatei speichern, speichert das Gerät alle Konfigurationseinstellungen in der Binärdatei.
Im Gegensatz dazu speichert das Gerät beim Speichern in eine Skriptdatei nur diejenigen Konfigurationseinstellungen, die von der Voreinstellung abweichen.

Beim Laden von Skript-Dateien sind diese ausschließlich dazu gedacht, die Voreinstellung der Konfiguration zu überschreiben.

3.2.3 Speichern in eine Binär-Datei auf den PC

Das Gerät bietet Ihnen die Möglichkeit, die aktuellen Konfigurationsdaten in eine Binär-Datei Ihres PCs zu speichern.

- ☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Klicken Sie im Rahmen „Speichern“ auf „auf dem PC (binär)“.
- ☐ Geben Sie im Speichern-Fenster den Dateinamen an, unter welchem das Gerät die Konfigurationsdatei speichern soll.
- ☐ Klicken Sie auf „Sichern“.

3.2.4 Speichern als Skript auf den PC

Das Gerät bietet Ihnen die Möglichkeit, die aktuellen Konfigurationsdaten in eine editer- und lesbare Datei Ihres PCs zu speichern.

☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
☐ Klicken Sie im Rahmen „Speichern“ auf „auf dem PC (script)“.
☐ Geben Sie im Speichern-Fenster den Dateinamen an, unter welchem das Gerät die Konfigurationsdatei speichern soll.
☐ Klicken Sie auf „Sichern“.

3.2.5 Speichern als Offline-Konfigurations-Datei auf den PC

Das Gerät bietet Ihnen die Möglichkeit, die aktuellen Konfigurationsdaten für den Offline-Konfigurator im XML-Format in eine Datei Ihres PCs zu speichern.

☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
☐ Klicken Sie im Rahmen „Speichern“ auf „auf dem PC (ocf)“.
☐ Geben Sie im Speichern-Fenster den Dateinamen an, unter welchem das Gerät die Konfigurationsdatei speichern soll.
☐ Klicken Sie auf „Sichern“.

3.3 Konfigurations-Signatur

Das Gerät weist einer Konfiguration zur eindeutigen Identifikation eine Prüfsumme oder Signatur zu, die Änderungen an der Konfiguration sichtbar macht. Jedes Mal, wenn Sie eine Konfiguration auf dem Gerät speichern, generiert das Gerät eine zufällige Zeichenfolge aus Nummern und/oder Buchstaben als Signatur für die Konfiguration. Diese Signatur ändert sich jedes Mal, wenn Sie die Konfiguration auf dem Gerät ändern. Jede Konfiguration besitzt eine eindeutige Kennung.

Das Gerät speichert die zufällig generierte Signatur zusammen mit der Konfiguration, um sicherzustellen, dass das Gerät bei einem Neustart die betreffende Konfiguration lädt.

Die Signatur besteht aus einer Prüfsumme für die Konfigurationsdatei und einer zufälligen Nummer. Das Gerät prüft die Signatur um sicherzustellen, dass sie sich von den zuvor generierten Nummern unterscheidet.

4 Neueste Software laden

Hirschmann arbeitet ständig an der Leistungssteigerung der Produkte. Deshalb besteht die Möglichkeit, dass Sie auf der Internetseite von Hirschmann (www.hirschmann.com) eine neuere Release der Geräte-Software finden, als die Release, die auf Ihrem Gerät gespeichert ist.

Prüfen der installierten Software-Release

- ☐ Wählen Sie den Dialog `Grundeinstellungen:Software`.
- ☐ Dieser Dialog zeigt Ihnen die Release-Nr. der im Gerät gespeicherten Software an.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`show sysinfo`	Anzeigen der Systeminformation.

```
Alarm..................................... None

System Description........................ Hirschmann Railswitch
System Name............................... RS-1F1054
System Location........................... Hirschmann Railswitch
System Contact............................ Hirschmann Automation
  and Control GmbH
System Up Time............................ 0 days 0 hrs 45 mins
  57 secs
System Date and Time (local time zone)..... 2009-11-12 14:15:16
System IP Address......................... 10.0.1.13
Boot Software Release..................... L2B-05.2.00
Boot Software Build Date.................. 2009-11-12 13:14
OS Software Release....................... L2B-03.1.00
OS Software Build Date.................... 2009-11-12 13:14
Hardware Revision......................... 1.22 / 4 / 0103
Hardware Description...................... RS20-1600T1T1SDAEHH
Serial Number............................. 943434023000001191
Base MAC Address.......................... 00:80:63:1F:10:54
Number of MAC Addresses................... 32 (0x20)
```

Software laden

Das Gerät bietet 4 Möglichkeiten, die Software zu laden:

- manuell vom AutoConfiguration Adapter (out-of-band),
- automatisch vom AutoConfiguration Adapter (out-of-band),
- über TFTP von einem tftp-Server (in-band) und
- über ein Datei-Auswahl-Fenster von Ihrem PC.

Anmerkung: Die Konfiguration des Gerätes bleibt nach der Installation der neuen Software erhalten.

4.1 Software manuell vom ACA laden

Den AutoConfiguration Adapter (ACA) können Sie wie einen gewöhnlichen USB-Stick an einen USB-Port Ihres PCs anschließen und die Geräte-Software in das Hauptverzeichnis des ACA kopieren.

☐ Kopieren Sie die Geräte-Software von Ihrem Computer auf den ACA.

☐ Verbinden Sie den ACA nun mit dem USB-Port des Gerätes.

☐ Öffnen Sie den System-Monitor (siehe auf Seite 18 „System-Monitor starten“).

☐ Wählen Sie 2 und drücken Sie die Eingabetaste, um die Software vom ACA in den lokalen Speicher des Gerätes zu kopieren.
Am Ende des Updates fordert Sie der System-Monitor auf, eine beliebige Taste zu drücken, um fortzufahren.

☐ Wählen Sie 3, um die neue Software auf dem Geräte zu starten.

Der System-Monitor bietet Ihnen weitere Möglichkeiten, die im Zusammenhang mit der Software auf Ihrem Gerät stehen:

- Auswahl der zu ladenden Software,
- Starten der Software,
- Kaltstart durchführen

4.1.1 Auswahl der zu ladenden Software

Mit diesem Menüpunkt des System-Monitors wählen Sie eine von 2 möglichen Software-Releases aus, die geladen werden soll.
Am Bildschirm erscheint folgendes Fenster:

```
Select Operating System Image

(Available OS: Selected: 05.0.00 (2009-08-07 06:05), Backup: 04.2.00
 (2009-07-06 06:05 (Locally selected: 05.0.00 (2009-08-07 06:05))

 1  Swap OS images
 2  Copy image to backup
 3  Test stored images in Flash mem.
 4  Test stored images in USB mem.
 5  Apply and store selection
 6  Cancel selection
```

Abb. 15: Bildschirmansicht Update Betriebssystem

Swap OS images

Der Speicher des Gerätes bietet Platz für 2 Abbildungen der Software. So haben Sie z.B. die Möglichkeit, eine neue Version der Software zu laden, ohne dabei das bestehende zu löschen.

☐ Wählen Sie 1, um beim nächsten Booten die andere Software zu laden.

Copy image to backup

☐ Wählen Sie 2, um eine Kopie der aktiven Software zu speichern.

Test stored images in flash memory

☐ Wählen Sie 3, um zu prüfen, ob die gespeicherten Abbilder der Software im Flash-Speicher gültige Codes enthalten.

Test stored images in USB memory

☐ Wählen Sie 4, um zu prüfen, ob die gespeicherten Abbilder der Software im ACA gültige Codes enthalten.

Apply and store selection

☐ Wählen Sie 5, um die Auswahl der Software zu bestätigen und zu speichern.

Cancel selection

☐ Wählen Sie 6, um diesen Dialog ohne Änderungen zu verlassen.

4.1.2 Starten der Software

Dieser Menüpunkt (Start Selected Operating System) des System-Monitors bietet Ihnen die Möglichkeit, die ausgewählte Software zu starten.

4.1.3 Kaltstart durchführen

Dieser Menüpunkt (End (reset and reboot)) des System-Monitors bietet Ihnen die Möglichkeit, die Hardware des Gerätes zurückzusetzen und einen Neustart durchzuführen.

4.2 Automatischer Software-Update vom ACA

☐ Für ein Software-Update über den ACA kopieren Sie zunächst die neue Geräte-Software in das Hauptverzeichnis des AutoConfiguration Adapters. Ist die Version der Software auf dem ACA neuer oder älter als die auf dem Gerät, dann führt das Gerät ein Software-Update durch.

Anmerkung: Software-Versionen ab der Release 06.0.00 und höher im nichtflüchtigen Speicher des Geräts unterstützen den Software-Update über den ACA. Ist die Gerätesoftware älter, haben Sie die Möglichkeit, die Software manuell vom ACA zu laden. Siehe „Software manuell vom ACA laden” auf Seite 73.

☐ Geben Sie der Datei den Namen, der zum Gerätetyp und der Software-Variante passt, z.B. rsL2P.bin für den Gerätetyp RS2 mit der Software-Variante L2P. Beachten Sie dabei die Groß- und Kleinschreibung. Wenn Sie die Software von einer Produkt-CD oder von einem Web-Server des Herstellers kopiert haben, hat die Software schon den richtigen Dateinamen.

☐ Erzeugen Sie zusätzlich eine leere Datei mit dem Namen „autoupdate.txt“ im Hauptverzeichnis des ACA. Beachten Sie dabei die Groß- und Kleinschreibung.

☐ Schließen Sie den AutoConfiguration Adapter an das Gerät an und starten Sie das Gerät neu.

☐ Das Gerät führt automatisch folgende Schritte aus:
- Es prüft während des Bootvorgangs, ob ein ACA angeschlossen ist.
- Es prüft, ob der ACA eine Datei mit dem Namen „autoupdate.txt“ im Hauptverzeichnis enthält.
- Es prüft, ob der ACA eine Software-Datei mit dem zum Gerätetyp passsenden Namen im Hauptverzeichnis enthält.
- Es vergleicht die auf dem ACA gespeicherte Software-Version mit der auf dem Gerät gespeicherten.
- Sind diese Bedingungen erfüllt, lädt das Gerät die Software vom ACA als Haupt-Software in seinen nichtflüchtigen Speicher.

– Das Gerät bewahrt von der bisherigen Software ein Backup im nichtflüchtigen Speicher auf.
– Danach führt das Gerät einen Kaltstart durch und lädt dabei die neue Software aus dem nichtflüchtigen Speicher.

Eine der folgenden Meldungen in der Log-Datei zeigt das Ergebnis des Update-Vorgangs an:

- S_watson_AUTOMATIC_SWUPDATE_SUCCESSFUL: Update erfolgreich beendet.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_WRONG_FILE: Update fehlgeschlagen, Ursache: Falsche Datei.
- S_watson_AUTOMATIC_SWUPDATE_FAILED_SAVING_FILE: Update fehlgeschlagen, Ursache: Fehler beim Abspeichern.

☐ Klicken Sie in Ihrem Browser auf „Neu laden“, um nach dem Booten des Gerätes über die grafische Benutzeroberfläche wieder auf das Gerät zuzugreifen.

4.3 Software vom TFTP-Server laden

Für ein Software-Update per TFTP benötigen Sie einen TFTP-Server, auf dem die zu ladende Software abgelegt ist (siehe auf Seite 276 „TFTP-Server für SW-Updates“).

☐ Wählen Sie den Dialog `Grundeinstellungen:Software`.

Der URL kennzeichnet den Pfad zu der auf dem tftp-Server gespeicherten Software. Der URL hat die Form
tftp://IP-Adresse des tftp-Servers/Pfadname/Dateiname
(z.B. `tftp://192.168.1.1/device/device.bin`).

☐ Geben Sie den Pfad zur Geräte-Software ein.

☐ Klicken Sie auf "tftp-Update" um die Software vom tftp-Server auf das Gerät zu laden.

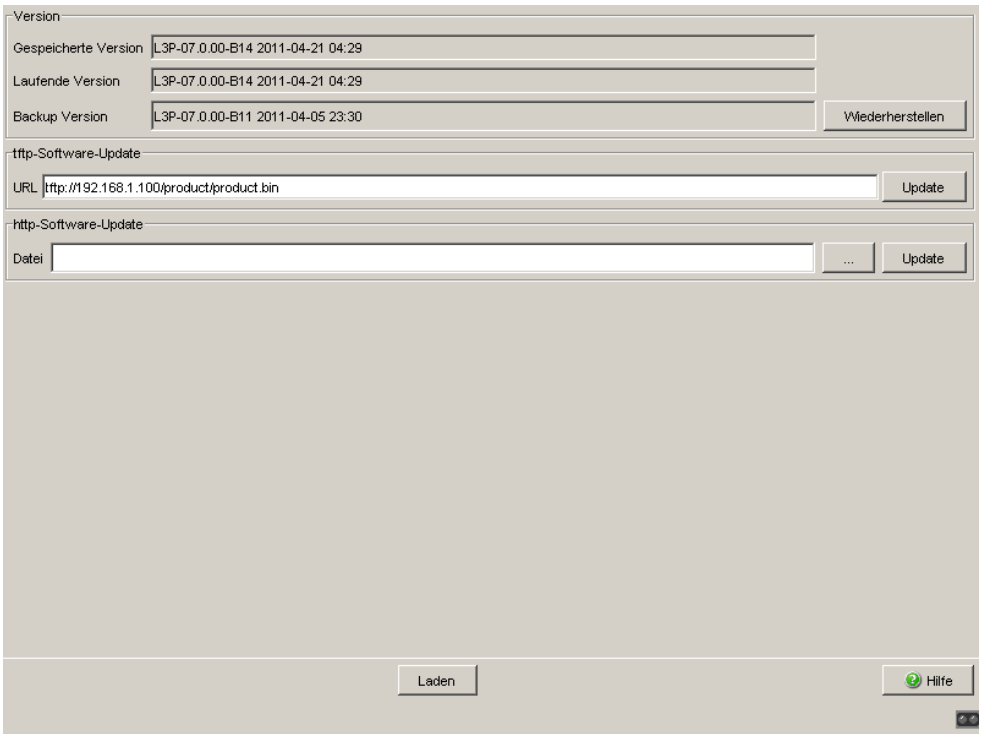


Abb. 16: Dialog Software-Update

☐ Nach erfolgreichem Laden aktivieren Sie die neue Software:
Wählen Sie den Dialog `Grundeinstellungen:Neustart` und führen Sie einen Kaltstart durch.
Beim Kaltstart lädt das Gerät die Software erneut aus dem permanenten Speicher, führt einen Neustart und einen Selbsttest durch.

☐ Klicken Sie nach dem Booten des Gerätes in Ihrem Browser auf „Neu laden“, um wieder auf das Gerät zugreifen zu können.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy tftp://10.0.1.159/product.bin system:image`	Übertragen der Software-Datei „product.bin” vom tftp-Server mit der IP-Adresse 10.0.1.159 auf das Gerät.

4.4 Software über Datei-Auswahl laden

Für ein Software-Update über das Datei-Auswahl-Fenster kopieren Sie die Geräte-Software auf einem Datenträger, den Sie von Ihrem PC aus erreichen.

☐ Wählen Sie den Dialog `Grundeinstellungen:Software`.
☐ Klicken Sie im Datei-Auswahl-Rahmen auf „...“.
☐ Wählen Sie im Datei-Auswahl-Fenster die Geräte-Software aus (Namensmuster: *.bin, z.B. device.bin) und klicken Sie auf „Öffnen“.
☐ Klicken Sie auf „Update“, um die Software auf das Gerät zu übertragen.

Eine der folgenden Meldungen zeigt das Ende der Update-Aktion an:
- Update erfolgreich beendet.
- Update fehlgeschlagen, Ursache: Falsche Datei.
- Update fehlgeschlagen, Ursache: Fehler beim Abspeichern.
- Datei nicht gefunden (Ursache: Dateiname nicht gefunden oder nicht vorhanden).
- Verbindungsfehler (Ursache: Pfad ohne Dateiname).

☐ Nach erfolgreichem Update aktivieren Sie die neue Software: Wählen Sie den Dialog `Grundeinstellungen: Neustart` und führen Sie einen Kaltstart durch.
Bei einem Kaltstart lädt das Gerät die Software neu aus dem nichtflüchtigen Speicher, startet neu und führt einen Selbsttest durch.
☐ Klicken Sie in Ihrem Browser auf „Neu laden“, um nach dem Booten des Gerätes wieder auf das Gerät zugreifen zu können.

4.5 Bootcode-Update via TFTP

In sehr seltenen Fällen ist für ein Software-Update ein erweiterter Funktionsumfang des Bootcodes erforderlich. In einem solchen Fall fordert Sie unser Service-Desk auf, vor dem Software-Update den Bootcode zu aktualisieren.

4.5.1 Aktualisieren der Bootcode-Datei

Für ein TFTP-Update benötigen Sie einen TFTP-Server, auf dem Sie den Bootcode hinterlegen.
Der URL kennzeichnet den Pfad zum auf dem TFTP-Server gespeicherten Bootcode. Der URL hat das Format
tftp://IP-Adresse des tftp-Servers/Pfadname/Dateiname
(z. B.: `tftp://192.168.1.1/device/device_bootrom.img`)

- ☐ Öffnen Sie den Dialog `Grundeinstellungen:Software`.
- ☐ Klicken Sie im Rahmen „tftp-Software-Update“ auf das Optionsfeld „Bootcode“.
- ☐ Geben Sie den Pfad zur Bootcode-Datei mit der Endung *.bin in das Eingabefeld „URL“ ein.
- ☐ Um mit dem Update zu beginnen, klicken Sie „Update“.
- ☐ Um nach dem Laden mit dem neuen Bootcode zu starten, öffnen Sie den Dialog `Grundeinstellungen:Neustart` und klicken „Kaltstart…“.

Anmerkung: Für diesen Dialog benötigen Sie Schreibrechte.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`copy <url> system:bootcode`	Kopieren Sie die Bootcode-Datei vom TFTP-Server auf das Gerät an.

5 Ports konfigurieren

Die Portkonfiguration umfasst:

- Port ein-/ausschalten,
- Betriebsart wählen,
- Meldung von Verbindungsfehlern aktivieren,
- Power over ETHERNET konfigurieren.

Port ein-/ausschalten

Im Lieferzustand ist jeder Port eingeschaltet. Um einen höheren Zugangsschutz zu erzielen, schalten Sie die Ports aus, an denen Sie keine Verbindung anschließen.

☐ Wählen Sie den Dialog `Grundeinstellungen:Portkonfiguration`.
☐ Wählen Sie in der Spalte „Port an“ die Ports aus, die mit einem anderen Gerät verbunden sind.

Betriebsart wählen

Im Lieferzustand befinden sich die Ports im Betriebsmodus „Automatische Konfiguration“.

Anmerkung: Die aktive automatische Konfiguration hat Vorrang vor der manuellen Konfiguration.

☐ Wählen Sie den Dialog `Grundeinstellungen:Portkonfiguration`.
☐ Falls das an diesem Port angeschlossene Gerät eine feste Einstellung voraussetzt
  – wählen Sie in der Spalte „Manuelle Konfiguration“ die Betriebsart (Übertragungsgeschwindigkeit, Duplexbetrieb) und
  – deaktivieren Sie in der Spalte „Automatische Konfiguration“ den Port.

Unbenutzte Modul-Steckplätze deaktivieren

Diese Funktion ist auf den Geräten MS, PowerMICE, MACH102 und MACH4000 verfügbar.

Wenn Sie an modularen Geräten ein Modul in einen leeren Steckplatz stecken, weist das Gerät dem Modul automatisch die Voreinstellungen zu. Die Voreinstellungen erlauben den Zugriff auf das Netzwerk. Um den Netzwerkzugang zu unterbinden, bietet die Funktion Ihnen die Möglichkeit, einen unbenutzten Slot zu deaktivieren.

- ☐ Öffnen Sie den Dialog `Grundeinstellungen:Module`.
- ☐ Deactivate the unused slots in the „Enabled“ column.

Erkannte Kommunikationsunterbrechung melden

Im Lieferzustand zeigt das Gerät einen ermittelten Verbindungsfehler über den Meldekontakt und die LED-Anzeige an. Das Gerät erlaubt Ihnen, diese Anzeige zu unterdrücken. Auf diese Weise vermeiden Sie z. B., ein ausgeschaltetes Gerät fälschlicherweise als unterbrochene Verbindung zu interpretieren.

- ☐ Wählen Sie den Dialog `Grundeinstellungen:Portkonfiguration`.
- ☐ Selektieren Sie in der Spalte „Verbindungsfehler weitermelden“ die Ports aus, bei denen Sie eine Verbindungsüberwachung wünschen.

Power over Ethernet konfigurieren

Ist das Gerät mit PoE-Medienmodulen ausgestattet, dann bietet es Ihnen die Möglichkeit, Endgeräte wie z.B. IP-Telefone über das Twisted-Pair-Kabel mit Strom zu versorgen. PoE-Medienmodule unterstützen Power over ETHERNET nach IEEE 802.3af.
Im Lieferzustand ist die Funktion Power over ETHERNET global und an allen PoE-fähigen Ports eingeschaltet.

Nominale Leistung für MS20/30, MACH 1000 und PowerMICE:
Das Gerät bietet die nominale Leistung für die Summe aller PoE-Ports zuzüglich einer Reserve. Da das PoE-Medienmodul seine PoE-Spannung von extern bezieht, kennt das Gerät die mögliche nominale Leistung nicht.
Deshalb nimmt das Gerät an dieser Stelle als „Nominale Leistung“ den Wert 60 Watt pro PoE-Medienmodul an.

Nominale Leistung für MACH 4000:
Das Gerät bietet die nominale Leistung für die Summe aller PoE-Ports zuzüglich einer Reserve. Benötigen die angeschlossenen Geräte mehr PoE-Leistung, als die angebotene PoE-Leistung, dann schaltet das Gerät PoE an Ports aus. Zunächst schaltet das Gerät PoE an den Ports mit der niedrigsten PoE-Priorität ab. Haben mehrere Ports die gleiche Priorität, dann schaltet das Gerät zuerst PoE an den Ports mit der höheren Portnummer ab.

☐ **Globale Einstellungen**
- Für Geräte mit **PoE** wählen Sie den Dialog `Grundeinstellungen:Power over Ethernet`.
- Für Geräte mit **PoE+** wählen Sie den Dialog `Grundeinstellungen:Power over Ethernet Plus:Global`.

Rahmen „Funktion“:

☐ Mit „Funktion An/Aus" schalten Sie PoE ein/aus.

Rahmen „Konfiguration“:

☐ „Verschicke Trap“ bietet Ihnen die Möglichkeit, das Gerät zu veranlassen, in folgenden Fällen einen Trap zu senden:
- Beim Überschreiten/Unterschreiten der Leistungsschwelle.
- Beim Ein-/Ausschalten der PoE-Versorgungsspannung an mindestens einem Port.

☐ Geben Sie eine Leistungsschwelle unter „Threshold“ an. Ist die Funktion „Verschicke Trap“ aktiviert, sendet das Gerät einen Trap, sobald das Gerät diesen Wert über- oder unterschreitet. Die Leistungsschwelle geben Sie in Prozent der abgegebenen Leistung zur nominalen Leistung ein.

☐ „Budget [W]“ zeigt die Leistung an, die das Gerät den PoE-Ports nominal zur Verfügung stellt.

☐ „Reserviert [W]“ zeigt an, wieviel Leistung das Gerät den angeschlossenen PoE-Geräten aufgrund ihrer Klassifizierung maximal zur Verfügung stellt.

☐ „Abgegeben [W]" zeigt an, wie groß der momentane Leistungsbedarf der PoE-Ports ist.

Die Differenz von „Nominale“ und „Reservierte“ Leistung gibt an, wieviel Leistung an den freien PoE+-Ports noch zur Verfügung steht.

☐ **Port-Einstellungen**

– Für Geräte mit **PoE** wählen Sie den Dialog `Grundeinstellungen:Power over Ethernet`.
– Für Geräte mit **PoE+** wählen Sie den Dialog `Grundeinstellungen:Power over Ethernet Plus:Port`.

Die Tabelle zeigt ausschließlich Ports an, die PoE unterstützen.

☐ In der Spalte „POE an" haben Sie die Möglichkeit, PoE an diesem Port ein-/auszuschalten.
☐ Die Spalte „Status" zeigt den PoE-Status des Ports an.
☐ In der Spalte „Priorität" (MACH 4000) legen Sie die PoE-Priorität „niedrig“, „hoch“ oder „kritisch" des Ports fest.
☐ Die Spalte "Class" zeigt die Klasse des angeschlossenen Gerätes an:
Class: Maximal abgegebene Leistung
0: 15,4 W = Lieferzustand
1: 4,0 W
2: 7,0 W
3: 15,4 W
4: reserviert, wie Klasse 0 behandeln
☐ Die Spalte „Verbrauch [W]“ zeigt die aktuelle Leistungsabgabe an dem jeweiligen Port an.
☐ Die Spalte „Name“ zeigt den Namen des Ports an, siehe `Grundeinstellungen:Portkonfiguration`.

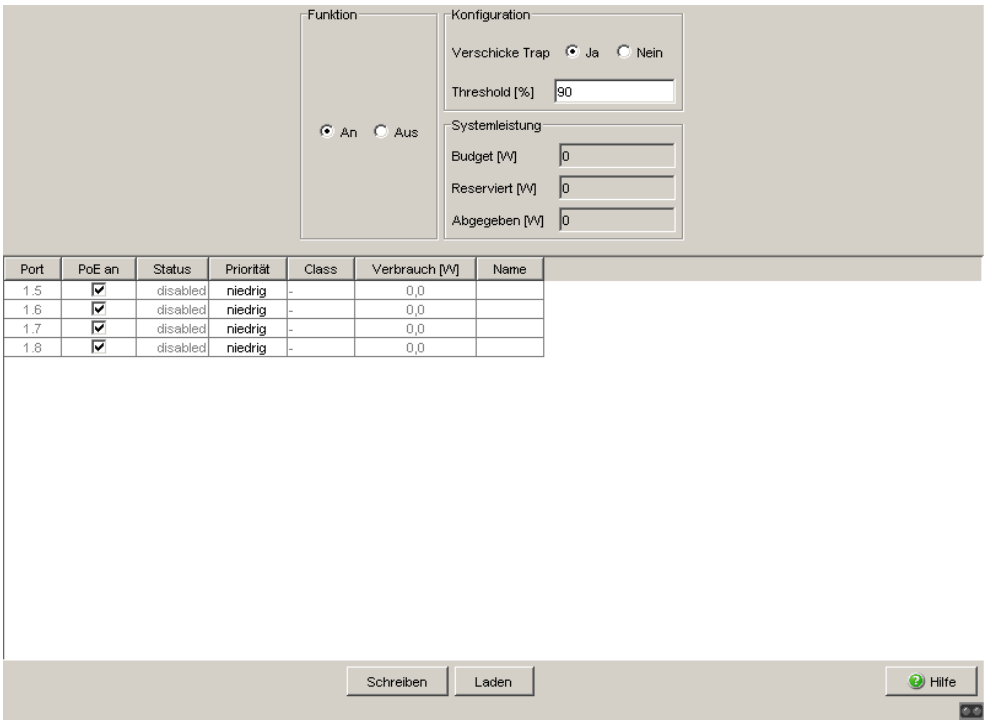


Abb. 17: Dialog Power over Ethernet

PoE-Spannungsversorgung bereitstellen

OCTOPUS PoE-Geräte bieten Ihnen die Möglichkeit, die PoE-Spannungsversorgung bereits vor dem Laden und Starten der Software einzuschalten. Damit versorgen Sie die angeschlossenen PoE-Geräte (powered devices) schneller mit der PoE-Spannung und verkürzen die Startphase des gesamten Netzes.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Global-Configure-Modus.
`#inlinepower fast-startup enable`	Inline Power Fast Startup einschalten (Lieferzustand: ausgeschaltet).
`#inlinepower fast-startup disable`	Inline Power Fast Startup ausschalten.
`#show inlinepower`	Power over Ethernet System Informationen anzeigen (Fast Startup und weitere Informationen).

Kaltstart bei erkannten Fehlern

Die Funktion bietet Ihnen die Möglichkeit, das Gerät in folgenden Fällen mit einem Kaltstart automatisch zurückzusetzen:

- bei einem erkannten Fehler
  (selftest reboot-on-error enable)
  oder
- ausschließlich bei einem erkannten schwerwiegenden Fehler
  (selftest reboot-on-error seriousOnly)

Bei aktivierter Funktion `selftest reboot-on-error seriousOnly` verhält sich das Gerät wie folgt:

- Bei einem erkannten Fehler in einem Subsystem (zum Beispiel bei einer erkannten HDX/FDX-Fehlanpassung an einem Port) entfällt der Kaltstart des Gerätes.
- Bei einem erkannten Fehler, der die Funktion des gesamten Gerätes beeinträchtigt, führt das Gerät dennoch einen Kaltstart durch.
- Das Gerät sendet einen Trap (siehe auf Seite 218 „Alarmmeldungen versenden“).

Anmerkung: Wenn das Gerät bei aktivierter Funktion `selftest reboot-on-error seriousOnly` eine HDX/FDX-Fehlanpassung erkennt, entfällt der automatische Kaltstart des Gerätes. Um den/die betroffenen Port(s) in diesem Fall wieder in einen verwendbaren Zustand zu versetzen, führen Sie über `Grundeinstellungen:Neustart` einen Kaltstart des Gerätes durch.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Global-Configure-Modus.
`#selftest reboot-on-error enable`	Die Funktion „Kaltstart bei erkanntem Fehler“ einschalten.
`#selftest reboot-on-error seriousOnly`	Die Funktion „Kaltstart ausschließlich bei erkanntem schwerwiegenden Fehler“ einschalten.
`#selftest reboot-on-error disable`	Die Funktion „Kaltstart bei erkanntem Fehler“ ausschalten (Lieferzustand: eingeschaltet).
`#show selftest`	Status der Funktion „Kaltstart bei erkanntem Fehler“ (Enabled/Disabled/seriousOnly) anzeigen.

6 Unterstützung beim Schutz vor unberechtigtem Zugriff

Das Gerät bietet Ihnen folgende Funktionen zur Hilfe beim Schutz gegen unberechtigte Zugriffe.

- Passwort für SNMP-Zugriff
- Telnet-/Web/SSH-Zugriff abschaltbar
- Eingeschränkter Management-Zugriff
- HiDiscovery-Funktion abschaltbar
- Portzugangskontrolle über IP- oder MAC-Adresse
- Portauthentifizierung nach IEEE 802.1X
- Zugriffs-Kontroll-Listen (Access Control Lists, ACL)
- Login-Banner

6.1 Das Gerät schützen

Wenn Sie den Schutz vor unberechtigtem Zugriff auf das Gerät mit wenigen Schritten maximieren möchten, können Sie nach der Konfiguration des Geräts einige oder alle der folgenden Schritte ausführen:

- ☐ Schalten Sie SNMPv1 und SNMPv2 ab und stellen Sie für den SNMPv3-Zugriff ein anderes als das Standard-Passwort ein (siehe auf Seite 94 „Passwort für SNMP-Zugriff eingeben“).
- ☐ Schalten Sie den Web-Zugriff ab, nachdem Sie das Applet der grafischen Benutzeroberfläche auf Ihre Management-Station heruntergeladen haben. Sie können das Applet als eigenständiges Programm starten und haben damit SNMPv3-Zugriff auf das Gerät.
  Schalten Sie den Telnet-Zugriff ab.
  Schalten Sie ggf. auch den SSH-Zugriff ab.
  Siehe „Telnet-/Web-/SSH-Zugriff aus-/einschalten” auf Seite 100.
- ☐ Schalten Sie den HiDiscovery-Zugriff ab.

Anmerkung: Behalten Sie mindestens eine Zugriffsmöglichkeit auf das Gerät. Der V.24-Zugriff ist immer möglich, da er nicht abschaltbar ist.

6.2 Passwort für SNMP-Zugriff

6.2.1 Beschreibung Passwort für SNMP-Zugriff

Eine Netzmanagement-Station kommuniziert über das Simple Network Management Protocol (SNMP) mit dem Gerät.
Jedes SNMP-Paket enthält die IP-Adresse des sendenden Rechners und das Passwort, mit welchem der Absender des Pakets auf die MIB des Gerätes zugreifen will.

Das Gerät empfängt das SNMP-Paket und vergleicht die IP-Adresse des sendenden Rechners und das Passwort mit den Einträgen in der MIB des Gerätes.
Liegt das Passwort mit dem entsprechenden Zugriffsrecht vor und ist die IP-Adresse des sendenden Rechners eingetragen, dann gewährt das Gerät den Zugriff.

Im Lieferzustand ist das Gerät über das Passwort „public“ (nur lesen) und „private“ (lesen und schreiben) von jedem Rechner aus zugänglich.

Zur Unterstützung beim Schutz Ihres Gerät vor unerwünschten Eingriffen:

☐ Definieren Sie zuerst ein neues Passwort, unter welchem Sie mit allen Rechten von Ihrem Rechner aus zugreifen können.

☐ Behandeln Sie dieses Passwort vertraulich, denn jeder, der das Passwort kennt, kann mit der IP-Adresse ihres Rechners auf die MIB des Gerätes zugreifen.

☐ Beschneiden Sie die Zugriffsrechte der bekannten Passwörter oder löschen Sie deren Einträge.

6.2.2 Passwort für SNMP-Zugriff eingeben

☐ Wählen Sie den Dialog `Sicherheit:Passwort / SNMP-Zugriff`.

Dieser Dialog bietet Ihnen die Möglichkeit, das Lese- und das Schreib/Lese-Passwort für den Zugriff über die grafische Benutzeroberfläche, über das CLI und per SNMPv3 (SNMP-Version 3) auf dem Gerät zu ändern.
Stellen Sie für das Lesepasswort und das Schreib-/Lesepasswort unterschiedliche Passwörter ein, damit ein Benutzer, der nur Lesezugriff hat (Benutzername „user“), das Passwort für den Schreib-/Lesezugriff (Benutzername „admin“) nicht kennen oder erraten kann.
Wenn Sie identische Passwörter setzen, meldet das Gerät beim Versuch, diese Daten zu schreiben, einen allgemeinen Fehler.

Die grafische Benutzeroberfläche und das Command-Line-Interface (CLI) verwenden für die Benutzer „admin“ und „user“ die selben Passwörter wie SNMPv3.

Anmerkung: Passwörter unterscheiden Groß- und Kleinschreibung.

☐ Wählen Sie „Lesepasswort ändern (user)“, um das Lesepasswort einzugeben.
☐ Geben Sie das neue Lesepasswort in der Zeile „Neues Passwort“ ein und wiederholen Sie die Eingabe in der Zeile „Bitte nochmals eingeben“.
☐ Wählen Sie „Schreib-/Lesepasswort ändern (admin)“, um das Schreib-/Lesepasswort einzugeben.
☐ Geben Sie das Schreib-/Lesepasswort ein und wiederholen Sie die Eingabe.
☐ Die Funktion „Nur verschlüsselte Anfragen akzeptieren“ sorgt für die Verschlüsselung der Daten des Web-based Managements, die zwischen Ihrem PC und dem Gerät mit SNMPv3 übertragen werden. Sie können die Funktion für den Zugriff mit Lese- und Schreib/Lesepasswort unterschiedlich einstellen.

☐ Wenn Sie die Funktion „Passwort als v1/v2-Community übernehmen“ aktivieren, synchronisiert das Gerät beim Ändern des Passworts den korrespondierenden Community-Namen.
  – Wenn Sie das Passwort für den Schreib-/Lesezugriff ändern, aktualisiert das Gerät die readWrite-Community für den SNMPv1/v2-Zugriff auf denselben Wert.
  – Wenn Sie das Passwort für den Lesezugriff ändern, aktualisiert das Gerät die readOnly-Community für den SNMPv1/v2-Zugriff auf denselben Wert.

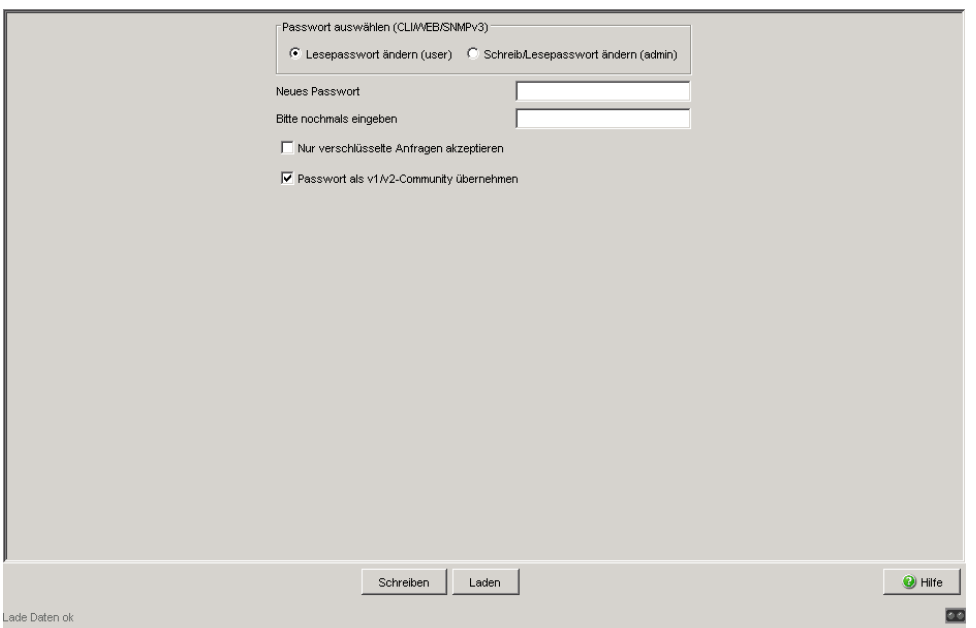


Abb. 18: Dialog Passwort/SNMP-Zugriff

Anmerkung: Wenn Sie kein Passwort mit der Berechtigung „schreiben/lesen“ kennen, haben Sie keine Möglichkeit, auf das Gerät schreibend zuzugreifen.

Anmerkung: Aus Sicherheitsgründen zeigt das Gerät die Passwörter nicht an. Notieren Sie sich jede Änderung. Ohne gültiges Passwort können Sie nicht auf das Gerät zugreifen.

Anmerkung: Aus Sicherheitsgründen verschlüsselt SNMPv3 das Passwort. Mit der Einstellung „SNMPv1“ oder „SNMPv2“ im Dialog `Sicherheit: SNMPv1/v2-Zugriff` überträgt das Gerät das Passwort unverschlüsselt, dieses kann dann mitgelesen werden.

Anmerkung: Verwenden Sie bei SNMPv3 für das Passwort 5-32 Zeichen, da viele Anwendungen keine kürzeren Passwörter akzeptieren.

☐ Wählen Sie den Dialog Sicherheit:SNMPv1/v2-Zugriff.
Dieser Dialog bietet Ihnen die Möglichkeit, den Zugriff über SNMPv1 oder SNMPv2 auszuwählen. Im Lieferzustand sind beide Protokolle aktiviert. Damit können Sie das Gerät mit HiVision verwalten und mit früheren Versionen von SNMP kommunizieren.

Wenn Sie SNMPv1 oder SNMPv2 auswählen, dann können Sie in der Tabelle festlegen, über welche IP-Adressen auf das Gerät zugegriffen werden darf und welche Art von Paßwörtern dabei zu benutzen sind.
Die Tabelle lässt bis zu 8 Einträge zu.
Aus Sicherheitsgründen können Lesepasswort und Schreib-/Lesepasswort nicht identisch sein.
Beachten Sie die Groß/Kleinschreibung.

Index Laufende Nummer für diesen Tabelleneintrag

Community-Name	Passwort, mit welchem dieser Rechner auf das Gerät zugreifen darf. Dieses Passwort ist unabhängig vom SNMPv3-Passwort. Wenn Sie die Funktion „Community als v3-Passwort übernehmen“ im Rahmen „Konfiguration“ aktivieren, synchronisiert das Gerät beim Ändern des Community-Namens das korrespondierende SNMPv3-Passwort.
IP-Adresse	IP-Adresse des Rechners, der auf das Gerät zugreifen darf.
IP-Maske	IP-Maske zur IP-Adresse
Zugriffsrecht	Zugriffsrecht legt fest, ob der Rechner mit Lese- oder Schreib-/Leserecht zugreifen darf.
Aktiv	Aktivieren/Deaktivieren dieses Tabelleneintrags.

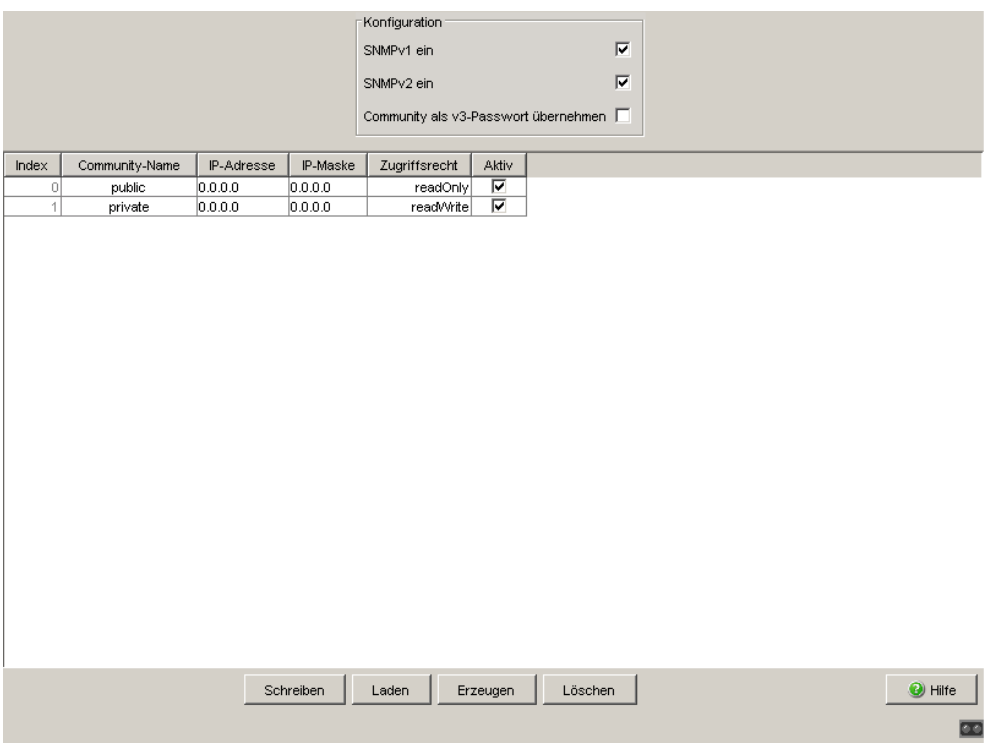


Abb. 19: Dialog SNMPv1/v2-Zugriff

- ☐ Um eine neue Zeile in der Tabelle zu erzeugen, klicken Sie auf „Eintrag erzeugen“.
- ☐ Um einen Eintrag aus der Tabelle zu löschen, wählen Sie die Zeile aus und klicken Sie auf „Eintrag löschen“ .

6.3 Telnet-/Web-/SSH-Zugriff

6.3.1 Beschreibung Telnet-Zugriff

Der Telnet-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe des Command Line Interfaces (in-band) zu konfigurieren. Sie können den Telnet-Server deaktivieren, um einen Telnet-Zugriff auf das Gerät abzuschalten.
Im Lieferzustand ist der Server eingeschaltet.
Nach dem Abschalten des Telnet-Servers ist ein erneuter Zugriff auf das Gerät über eine neue Telnet-Verbindung nicht mehr möglich. Eine bestehende Telnet-Verbindung bleibt erhalten.

Anmerkung: Das Command-Line-Interface (out-of-band) und der Dialog `Sicherheit:Telnet/Web-/SSH-Zugriff` in der grafischen Benutzeroberfläche bieten Ihnen die Möglichkeit, den Telnet-Server wieder zu aktivieren.

6.3.2 Beschreibung Web-Zugriff (http)

Der Web-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe der grafische Benutzeroberfläche zu konfigurieren. Sie können den Web-Server ausschalten, um einen Web-Zugriff auf das Gerät zu verhindern.
Im Lieferzustand ist der Server eingeschaltet.

Nach dem Abschalten des HTTP-Web-Servers ist ein erneutes Anmelden über einen HTTP-Web-Browser nicht mehr möglich. Die HTTP-Session im offenen Browserfenster bleibt aktiv.

6.3.3 Beschreibung SSH-Zugriff

Der SSH-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe des Command Line Interfaces (in-band) zu konfigurieren. Sie können den SSH-Server ausschalten, um einen SSH-Zugriff auf das Gerät zu verhindern. Im Lieferzustand ist der Server ausgeschaltet.
Nach dem Abschalten des SSH-Servers ist ein erneuter Zugriff auf das Gerät über eine neue SSH-Verbindung nicht mehr möglich. Eine bestehende SSH-Verbindung bleibt erhalten.

Anmerkung: Das Command Line Interface (out-of-band) und der Dialog `Sicherheit:Telnet/Web-Zugriff` in grafische Benutzeroberfläche bieten Ihnen die Möglichkeit, den SSH-Server wieder zu aktivieren.

Anmerkung: Um über SSH auf das Gerät zugreifen zu können, benötigen Sie einen Schlüssel, der auf dem Gerät installiert werden muss. Siehe „SSH-Zugriff vorbereiten” auf Seite 281.

Das Gerät unterstützt SSH Version 1 und Version 2. Sie haben die Möglichkeit, das anzuwendende Protokoll festzulegen.

- ☐ Öffnen Sie den Dialog `Sicherheit:Telnet-/Web-/SSH-Zugriff`.
- ☐ Wählen Sie im Rahmen „Konfiguration“, Feld „SSH-Version“ das anzuwendende Protokoll.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`no ip ssh`	SSH-Server ausschalten.
ip ssh protocol 2	SSH-Server wendet SSH Version 2 an.
ip ssh protocol 1	SSH-Server wendet SSH Version 1 an.
ip ssh protocol 1 2	SSH-Server wendet SSH Version 1 und 2 an.
`ip ssh`	SSH-Server einschalten.

6.3.4 Telnet-/Web-/SSH-Zugriff aus-/einschalten

Der Web-Server kopiert ein Java-Applet für die grafische Benutzeroberfläche auf Ihren Rechner. Dieses Applet kommuniziert anschließend per SNMPv3 (Simple Network Management Protocol) mit dem Gerät. Der Web-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe der grafischen Benutzeroberfläche zu konfigurieren. Sie können den Web-Server ausschalten, um das Kopieren des Applets zu verhindern.

☐ Wählen Sie den Dialog `Sicherheit:Telnet/Web-/SSH-Zugriff`.

☐ Schalten Sie den Server aus, zu welchem Sie den Zugang verwehren wollen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`lineconfig`	Wechsel in den Konfigurationsmodus für das CLI.
`transport input telnet`	Telnet-Server einschalten.
`no transport input telnet`	Telnet-Server ausschalten.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`ip http server`	Web-Server einschalten.
`no ip http server`	Web-Server ausschalten.
`ip ssh`	SSH-Funktion am Switch einschalten
`no ip ssh`	SSH-Funktion am Switch ausschalten

6.3.5 Web-Zugriff über HTTPS

Das Kommunikationsprotokoll HTTPS (HyperText Transfer Protocol Secure, d.h. sicheres Hypertext-Übertragungsprotokoll) hilft, Daten abhörsicher zu übertragen. Das Gerät verwendet das HTTPS-Protokoll zur Verschlüsselung und Authentifizierung der Kommunikation zwischen Web-Server und Browser.
Der Web-Server läd über HTTP ein Java-Applet für die grafische Benutzeroberfläche auf Ihren Rechner. Dieses Applet kommuniziert anschließend per SNMP (Simple Network Management Protocol) mit dem Gerät. Wenn Sie die Funktion `Web Server (HTTPS)` aktiviert haben, startet das Java-Applet den Verbindungsaufbau zum Gerät über HTTPS. Das Gerät tunnelt SNMP über HTTPS. Es verwendet DES-Codierung mit 56 Bit. Das Gerät bietet Ihnen die Möglichkeit, HTTPS-Zertifikate auf das Gerät hochzuladen.

Zertifikat

Für die Verschlüsselung ist ein Zertifikat nach dem Standard X.509/PEM (Public-Key-Infrastruktur) erforderlich. Im Lieferzustand befindet sich ein selbst generiertes Zertifikat auf dem Gerät.

- ☐ Ein X509/PEM-Zertifikat erzeugen Sie mit dem folgenden CLI-Kommando: `# ip https certgen`
- ☐ Ein neues Zertifikat laden Sie mit dem folgenden CLI-Kommando hoch: `copy tftp://<server_ip>/<path_to_pem> nvram:httpscert`
- ☐ Den HTTPS-Server schalten Sie mit der folgenden CLI-Kommandosequenz aus und wieder ein:

```
# no ip https server
# ip https server
```

Anmerkung: Wenn Sie ein Zertifikat neu hoch laden, starten Sie anschließend das Gerät oder den HTTPS-Server neu, damit das Zertifikat aktiv wird.

HTTPS-Verbindung

Anmerkung: Der Standard-Port für HTTPS-Verbindungen ist 443. Wenn Sie die Nummer des HTTPS-Port ändern, starten Sie anschließend das Gerät oder den HTTPS-Server neu, damit die Änderung wirksam wird.

☐ Die Nummer des HTTPS-Ports ändern Sie mit dem folgenden CLI-Kommando (<port_no> ist die Nummer des HTTPS-Ports):
`#ip https port <port_no>`

Anmerkung: Schalten Sie sowohl HTTPS als auch HTTP ein, wenn Sie HTTPS verwenden möchten. Dies ist Voraussetzung für das Laden des Applets. Im Lieferzustand des Gerätes ist HTTPS ausgeschaltet.

☐ Wählen Sie den Dialog `Sicherheit:Telnet/Web-/SSH-Zugriff`.

☐ Markieren Sie die Felder `Telnet-Server aktiv`, `Web-Server(http)` und `Web-Server(https)`. Tragen Sie in das Feld `HTTPS Port Nummer` den Wert `443` ein.

☐ Um über HTTPS auf das Gerät zuzugreifen, geben Sie in Ihrem Browser HTTPS statt HTTP und die IP-Adresse des Gerätes ein.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`# ip https server`	HTTPS-Server einschalten.
`# ip https port <port_no>`	Die HTTPS-Portnummer für eine gesicherte HTTP-Verbindung setzen. - Lieferzustand: 443. - Wertebereich: 1-65535
`# no ip https server` `# ip https server`	Nach dem Ändern HTTPS-Portnummer den HTTPS-Server aus- und wieder einschalten, damit die Änderung wirksam wird.
`# show ip https`	Optional: Den Status des HTTPS-Servers und die HTTPS-Portnummer anzeigen lassen.
`# ip https certgen`	X509/PEM-Zertifikat erzeugen.
`# copy tftp://<server_ip>/<path_to_pem> nvram:httpscert`	Ein X509/PEM-Zertifikat für HTTPS über TFTP hoch laden.
`# no ip https server` `# ip https server`	Nach dem Hochladen des Zertifikates den HTTPS-Server aus- und wieder einschalten, damit das Zertifikat aktiv wird.

Das Gerät verwendet das HTTPS-Protocol und baut eine neue Verbindung auf. Am Ende der Sitzung, nach dem Logout des Users, beendet das Gerät die Verbindung.

Anmerkung: Das Gerät bietet Ihnen die Möglichkeit, gleichzeitig HTTPS- und HTTP-Verbindungen zu öffnen. Die maximale Anzahl an gleichzeitig geöffneten HTTP(S)-Verbindungen beträgt 16.

6.4 Restricted Management Access

Das Gerät bietet Ihnen die Möglichkeit, den Management-Zugang zu dem Gerät nach IP-Adressbereichen und diese wiederum nach Management-Diensten (http, snmp, telnet, ssh) zu differenzieren. So haben Sie die Möglichkeit, Management-Zugriffsrechte fein einzustellen.

Wenn Sie das Gerät, das sich beispielsweise in einer Fertigungshalle befindet, nur aus dem Netz der IT-Abteilung per Web-Interface managen lassen möchten, dem Administrator aber auch den Fernzugriff per SSH ermöglichen wollen, können Sie dies mit der Funktion „Eingeschränkter Management-Zugriff“ erreichen.

Sie haben die Möglichkeit, diese Funktion mit der grafischen Benutzeroberfläche oder mit dem CLI zu konfigurieren. Die grafische Benutzeroberfläche bietet Ihnen eine komfortable Möglichkeit der Konfiguration. Achten Sie dabei darauf, dass Sie sich den Zugang zum Gerät nicht ungewollt versperren. Das CLI per V.24 bietet Ihnen die Möglichkeit, stets auf das Gerät zuzugreifen, ist von der Funktion ausgenommen und lässt sich nicht einschränken.

Das IT-Netz hat im folgenden Beispiel den Adressbereich 192.168.1.0/24 und der Remote-Zugriff erfolgt aus einem Mobilfunknetz mit dem IP-Adress-Bereich 109.237.176.0 - 109.237.176.255.

Das Gerät sei bereits auf den SSH-Zugriff vorbereitet (siehe auf Seite 281 „SSH-Zugriff vorbereiten“) und die SSH-Client-Applikation kennt bereits den Fingerprint des Host-Keys auf dem Gerät.

Parameter	IT-Netz	Mobilfunk-Netz
Netzadresse	192.168.1.0	109.237.176.0
Netzmaske	255.255.255.0	255.255.255.0
Gewünschter Management-Zugriff	http, snmp	ssh

Tab. 4: Beispiel-Parameter für den eingeschränkten Management-Zugriff

☐ Wählen Sie den Dialog `Sicherheit:Eingeschränkter Management-Zugriff`.

- ☐ Lassen Sie den bestehenden Eintrag unverändert und erzeugen Sie mit der Taste „Erzeugen“ einen neuen Eintrag für das IT-Netz.
- ☐ Tragen Sie als IP-Adresse 192.168.1.0 ein.
- ☐ Tragen Sie als Netzmaske 255.255.255.0 ein.
- ☐ Lassen Sie die Management-Dienste HTTP und SNMP eingeschaltet und schalten Sie die Dienste Telnet und SSH ab, indem Sie das Häkchen aus dem jeweiligen Kästchen entfernen.
- ☐ Erzeugen Sie mit der Taste „Erzeugen“ einen neuen Eintrag für das Mobilfunk-Netz.
- ☐ Tragen Sie als IP-Adresse 109.237.176.0 ein.
- ☐ Tragen Sie als Netzmaske 255.255.255.0 ein.
- ☐ Schalten Sie die Dienste HTTP, SNMP und Telnet ab und lassen Sie SSH eingeschaltet.
- ☐ Vergewissern Sie sich, dass Sie CLI-Zugang zum Gerät per V.24 haben.
- ☐ Deaktivieren Sie den voreingestellten Eintrag, da dieser alles erlaubt und Ihre nachfolgenden Einträge dadurch unwirksam wären.
- ☐ Schalten Sie die Funktion ein.
- ☐ Klicken Sie auf „Schreiben“, um die Daten flüchtig zu speichern.
- ☐ Wenn sich Ihre momentane Management-Station ebenfalls im IT-Netz befindet, haben Sie weiterhin Zugang zur grafischer Benutzeroberfläche. Andernfalls ignoriert das Gerät Bedienungen über die grafische Benutzeroberfläche, und lehnt auch einen Neustart der grafischen Benutzeroberfläche ab.
- ☐ Prüfen Sie, ob Sie vom IT-Netz das Gerät per http und snmp erreichen können: Öffnen Sie dazu die grafische Benutzeroberfläche des Geräts in einem Browser, loggen Sie sich im Startbildschirm ein und prüfen Sie, ob Sie Daten lesen können (als Benutzer „user“) oder lesen und schreiben können (als Benutzer „admin“). Prüfen Sie, ob das Gerät Verbindungen per telnet und ssh ablehnt.
- ☐ Prüfen Sie, ob Sie vom Mobilfunknetz das Gerät per ssh erreichen können: Öffnen Sie einen SSH-Client, verbinden Sie sich mit dem Gerät, loggen Sie sich ein und prüfen Sie, ob Sie Daten lesen bzw. lesen und schreiben können.
  Prüfen Sie, ob das Gerät Verbindungen per http, snmp und telnet ablehnt.
- ☐ Haben Sie beide Überprüfungen erfolgreich abgeschlossen, speichern Sie die Einstellungen nichtflüchtig. Andernfalls prüfen Sie Ihre Konfiguration. Das Gerät den Zugriff mit der grafischen Benutzeroberfläche ablehnt, verwenden Sie das CLI des Geräts per V.24, um die Funktion erst zu deaktivieren.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`show network mgmt-access`	Zeigt die momentane Konfiguration an.
`network mgmt-access add`	Legt einen Eintrag für das IT-Netz an. Dieser bekommt die kleinste freie ID, im Beispiel 2.
`network mgmt-access modify 2 ip 192.168.1.0`	Setzt die IP-Adresse des Eintrags für das IT-Netz.
`network mgmt-access modify 2 netmask 255.255.255.0`	Setzt die Netzmaske des Eintrags für das IT-Netz.
`network mgmt-access modify 2 telnet disable`	Schaltet Telnet für den Eintrag des IT-Netzes ab.
`network mgmt-access modify 2 ssh disable`	Schaltet SSH für den Eintrag des IT-Netzes ab.
`network mgmt-access add`	Legt einen Eintrag für das Mobilfunk-Netz an. Dieser bekommt im Beispiel die ID 3.
`network mgmt-access modify 3 ip 109.237.176.0`	Setzt die IP-Adresse des Eintrags für das Mobilfunk-Netz.
`network mgmt-access modify 3 netmask 255.255.255.0`	Setzt die Netzmaske des Eintrags für das Mobilfunk-Netz.
`network mgmt-access modify 3 http disable`	Schaltet http für den Eintrag des Mobilfunk-Netzes ab.
`network mgmt-access modify 3 snmp disable`	Schaltet snmp für den Eintrag des Mobilfunk-Netzes ab.
`network mgmt-access modify 3 telnet disable`	Schaltet Telnet für den Eintrag des Mobilfunk-Netzes ab.
`network mgmt-access status 1 disable`	Schaltet den **voreingestellten** Eintrag ab.
`network mgmt-access operation enable`	Schaltet die Funktion **sofort** ein.
`show network mgmt-access`	Zeigt die momentane Konfiguration der Funktion an.
`copy system:running-config nvram:startup-config`	Speichert die gesamte Konfiguration nichtflüchtig.

6.5 HiDiscovery-Zugriff aus-/einschalten

6.5.1 Beschreibung HiDiscovery-Protokoll

Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät eine IP-Adresse zuzuweisen (siehe auf Seite 38 „IP-Parameter per HiDiscovery eingeben“). HiDiscovery v1 ist ein Layer 2-Protokoll. HiDiscovery v2 ist ein Layer 3-Protokoll.

Anmerkung: Schränken Sie aus Sicherheitsgründen die HiDiscovery-Funktion des Gerätes ein oder schalten Sie sie aus, nachdem Sie dem Gerät die IP-Parameter zugewiesen haben.

6.5.2 HiDiscovery-Funktion aus-/einschalten

☐ Wählen Sie den Dialog `Grundeinstellungen:Netz`.

☐ Im Rahmen „HiDiscovery Protokoll v1/v2“ schalten Sie die HiDiscovery-Funktion aus oder beschränken Sie den Zugriff auf `read-only`.

`enable`	Wechsel in den Privileged-EXEC-Modus.

`network protocol hidiscovery off`	HiDiscovery-Funktion ausschalten.
`network protocol hidiscovery read-only`	HiDiscovery-Funktion mit dem Zugriffsrecht „lesen“ einschalten
`network protocol hidiscovery read-write`	HiDiscovery-Funktion mit dem Zugriffsrecht „lesen und schreiben“ einschalten

6.6 Portzugangskontrolle

6.6.1 Beschreibung der Portzugangskontrolle

Sie haben die Möglichkeit, das Gerät so zu konfigurieren, dass es Sie unterstützt, jeden Port vor unberechtigtem Zugriff zu schützen. Abhängig von Ihrer Auswahl prüft das Gerät die MAC-Adresse oder die IP-Adresse des angeschlossenen Gerätes.
Zur Sicherheitsüberwachung jedes einzelnen Ports stehen folgende Funktionen zur Verfügung:

- Das Gerät kann zwischen berechtigtem und unberechtigtem Zugang unterscheiden und unterstützt 2 Klassen der Zugangskontrolle:
  - Zugang für jeden:
    – keine Zugangsbeschränkung.
    – MAC-Adresse 00:00:00:00:00:00 oder
    – IP-Adresse 0.0.0.0.
  - Zugang ausschließlich für definierte MAC- oder IP-Adressen:
    – ausschließlich Geräte mit definierten MAC- oder IP-Adressen haben Zugang.
    – Sie können bis zu 10 IP-Adressen, bis zu 50 MAC-Adressen oder maskierbare MAC-Addressen definieren.
- Das Gerät reagiert auf einen unberechtigten Zugriff mit den folgenden auswählbaren Aktionen:
  - none: keine Reaktion.
  - trapOnly: Meldung durch Verschicken eines Traps.
  - portDisable: Meldung durch Verschicken eines Traps und Abschaltung des Ports.
  - autoDisable: Abschaltung des Ports durch die AutoDisable-Funktion mit der Möglichkeit, den Port nach Ablauf einer festlegbaren Zeit wieder einzuschalten.

6.6.2 Anwendungsbeispiel für Portzugangskontolle

Sie haben einen LAN-Anschluss in einem Raum, der für jeden zugänglich ist. Um einzustellen, dass ausschließlich definierte Benutzer diesen LAN-Anschluss nutzen können, aktivieren Sie die Portzugangskontrolle an diesem Port. Bei einem unberechtigten Zugriff soll das Gerät den Port ausschalten und Sie mit einer Alarmmeldung informieren.
Bekannt sind:

Parameter	Wert	Erläuterung
Erlaubte IP-Adressen	10.0.1.228 10.0.1.229	Definierte Benutzer sind das Gerät mit der IP-Adresse 10.0.1.228 und das Gerät mit der IP-Adresse 10.0.1.229
Aktion	portDisable	Den Port durch den entsprechenden Eintrag in der Port-Konfigurationstabelle (siehe auf Seite 85 „Ports konfigurieren“) abschalten und einen Alarm verschicken

Voraussetzungen für die weitere Konfiguration:
- Der Port für den LAN-Anschluss ist eingeschaltet und richtig konfiguriert (siehe auf Seite 85 „Ports konfigurieren“)
- Voraussetzungen damit das Gerät einen Alarm (Trap) senden kann (siehe auf Seite 221 „Trapeinstellung“):
  - Sie haben mindestens einen Empfänger eingetragen,
  - Sie haben für mindestens einen Empfänger in der Spalte „Aktiv“ ein Kreuz gesetz,
  - Sie haben im Rahmen „Auswahl“ die „Portsicherheit“ angekreuzt.

☐ Konfigurieren Sie die Portsicherheit.

☐ Wählen Sie den Dialog `Sicherheit:Portsicherheit`.

☐ Wählen Sie im Rahmen „Konfiguration“ die „IP-basierte Portsicherheit“.

☐ Klicken Sie in der Tabelle in der Zeile des zu schützenden Ports in die Zelle „Erlaubte IP-Adressen“.
☐ Geben Sie der Reihe nach ein:
– die IP-Subnetz-Gruppe: 10.0.1.228
– ein Leerzeichen als Trennelement
– die IP-Adresse: 10.0.1.229
Eingabe: `10.0.1.228 10.0.1.229`
☐ Klicken Sie in der Tabelle in der Zeile des zu schützenden Ports in die Zelle „Aktion“ und wählen Sie `portDisable`.

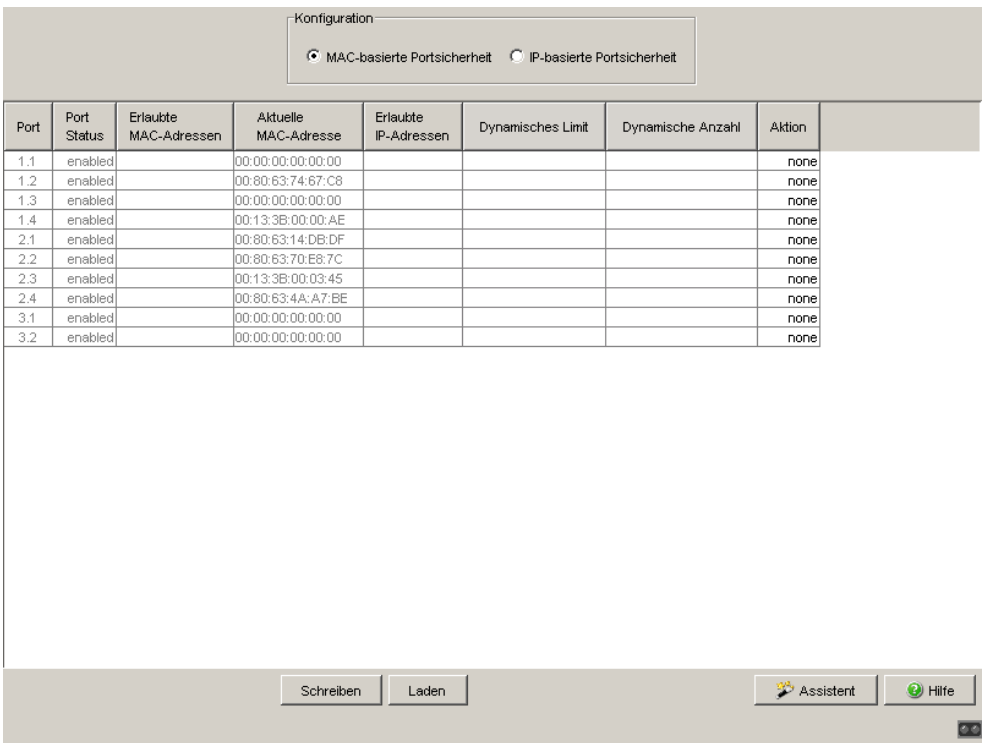


Abb. 20: Dialog Portsicherheit

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
☐ Wählen Sie im Rahmen „Speichern“ den Speicherort „auf dem Gerät“ und klicken Sie auf „Sichern“, um die Konfiguration nicht-flüchtig in der aktiven Konfiguration zu speichern.

6.7 Port-Authentifizierung nach IEEE 802.1X

6.7.1 Beschreibung Port-Authentifizierung nach IEEE 802.1X

Die portbasierte Netzzugriffskontrolle ist eine im Standard IEEE 802.1X beschriebene Methode zur Unterstützung beim Schutz von IEEE 802-Netzen vor unberechtigtem Zugriff. Durch die Authentifizierung und Autorisierung eines Endgeräts, das an einem Port des Gerätes angeschlossen ist, kontrolliert das Protokoll den Zugang an diesem Port.
Die Authentifizierung und Autorisierung erfolgt durch den Authentikator, in diesem Fall das Gerät. Dieser authentifiziert den Supplikanten (das anfragende Gerät, z. B. ein PC, etc.), d.h. er lässt den Zugriff auf die von ihm angebotenen Dienste (z. B. Zugang zum Netzwerk, an das das Gerät angeschlossen ist) zu oder weist ihn ab. Hierzu greift das Gerät auf einen externen Authentifizierungsserver (RADIUS-Server) zu, der die Authentifizierungsdaten des Supplikanten überprüft. Das Gerät tauscht die Authentifizierungsdaten mit dem Supplikanten über das Extensible Authentication Protocol over LANs (EAPOL), mit dem RADIUS-Server über das RADIUS-Protokoll aus.

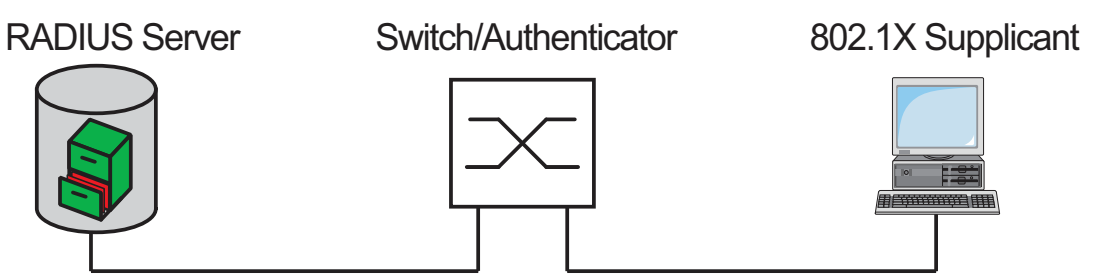


Abb. 21: Radius-Server-Anbindung

6.7.2 Authentifizierungsablauf nach IEEE 802.1X

Ein Supplikant versucht über einen Geräteport zu kommunizieren.

- Das Gerät fordert den Supplikanten auf, sich zu authentifizieren. Zu diesem Zeitpunkt ist ausschließlich EAPOL Verkehr zwischen Supplikant und Gerät erlaubt.
- Der Supplikant antwortet mit seinen Identitätsdaten.
- Das Gerät leitet die Identitätsdaten an den Authentifizierungsserver weiter.
- Der Authentifizierungsserver beantwortet die Anfrage entsprechend der Berechtigung.
- DasGerät wertet diese Antwort aus und gewährt dem Supplikant den Zugriff an diesem Port (oder lässt den Port im gesperrten Zustand).

6.7.3 Vorbereitung des Gerätes für die IEEE 802.1X-Port-Authentifizierung

- ☐ Eigene IP-Parameter (des Gerätes) konfigurieren.
- ☐ Die Funktion der 802.1X-Portauthentifizierung global einschalten.
- ☐ Die 802.1X-Portkontrolle auf „auto" setzen. Voreingestellt ist „force-authorized".
- ☐ Das „Shared Secret" zwischen Authenticator und RADIUS-Server eintragen. Das Shared Secret ist ein Textstring, den der RADIUS-Server-Administrator vergibt.
- ☐ Die IP-Adresse und den Port des RADIUS-Servers eingeben. Der vorgegebene UDP-Port des RADIUS-Servers ist der Port 1812.

6.7.4 IEEE 802.1X-Einstellungen

Konfiguration des RADIUS-Servers

☐ Wählen Sie den Dialog `Sicherheit:802.1X Port-Authentifizierung:RADIUS-Server`.

Dieser Dialog bietet Ihnen die Möglichkeit, die Daten für bis zu 3 RADIUS-Server einzugeben.

☐ Klicken Sie auf „Eintrag erzeugen“, um das Dialogfenster zur Eingabe der IP-Adresse eines RADIUS-Servers zu öffnen.
☐ Bestätigen Sie die Eingabe der IP-Adresse mit „OK“. Damit erzeugen Sie eine neue Zeile in der Tabelle für diesen RADIUS-Server.
☐ Tragen Sie in der Spalte „Shared Secret“ die Zeichenfolge ein, die Sie vom Administrator Ihres RADIUS-Servers als Schlüssel erhalten.
☐ Mit „Primary Server“ ernennen Sie diesen Server zum ersten Server, den das Gerät bei Portauthentifizierungsanfragen kontaktieren soll. Ist dieser Server nicht erreichbar, dann richtet sich das Gerät an den nächsten Server in der Tabelle.
☐ „Ausgewählter Server“ zeigt Ihnen an, an welchen Server das Gerät seine Anfragen tatsächlich richtet.
☐ Mit „Eintrag löschen“ löschen Sie die ausgewählte Zeile in der Tabelle.

Ports auswählen

☐ Wählen Sie den Dialog `Sicherheit:802.1X Port-Authentifizierung:Port Konfiguration`.
☐ In der Spalte „Portkontrolle“ wählen Sie „auto“ für die Ports, für die die portbezogene Netzzugriffskontrolle aktiv sein soll.

Zugriffskontrolle aktivieren

- ☐ Wählen Sie den Dialog `Sicherheit:802.1X Port-Authentifizierung:Global`.
- ☐ Mit „Funktion" schalten Sie die Funktion an.

6.8 Zugriffs-Kontroll-Listen (ACL)

Mit Zugriffs-Kontroll-Listen (Access Control Lists, ACL) haben Sie die Möglichkeit, Datenpakete beim Empfangen auszufiltern, weiterzuleiten, umzuleiten oder zu priorisieren. Das Gerät bietet

- MAC-basierte ACLs und
- IP-basierte ACLs.

Das Gerät berücksichtigt die ACLs beim Paketempfang. Deshalb heißen die Listen Ingress-ACLs.

Access Control Lists konfigurieren Sie über das Command Line Interface. Details hierzu finden Sie im Dokument „Referenz-Handbuch Command Line Interface“.

Das Gerät bietet folgende ACL-Fähigkeiten:

- bis zu 100 ACLs,
- 10 Regeln pro ACL,
- bis zu 100 Regeln pro Interface,
- bis zu 1000 Regeln auf allen Interfaces zusammen
- mögliche Aktionen:
  - erlauben (permit) und verweigern (deny),
  - in Kombination mit erlauben: priorisieren (assign-queue) und umleiten (redirect), d.h. wenn eine Regel zutrifft, erfolgt die Weiterleitung an das spezifizierte Interface.
- „alles verweigern“ ist stets die (unsichtbare) letzte Regel. Sie tritt dann in Kraft, wenn keine anderen Regeln dieses Interfaces zutreffen.

Die Konfiguration von ACLs umfasst folgende Schritte:

☐ ACL zuerst definieren und danach
☐ ACL an ein oder alle Interfaces binden.
Sie können ACLs an alle physikalischen Ports und an alle Link-Aggregation-Interfaces binden.

Die Reihenfolge bei der Definition der Regeln einer Liste und die Reihenfolge der Anbindung dieser Listen an ein Interface entscheidet über die Reihenfolge der Anwendung der Regeln und Listen (siehe auf Seite 126 „Reihenfolge der Regeln festlegen“).

Anmerkung: Access Control Lists konfigurieren Sie über das Command Line Interface. Details hierzu finden Sie im Dokument „Referenz-Handbuch Command Line Interface“.

Anmerkung: Beim PowerMICE und MACH 4000 können Sie je Interface entweder MAC-basierte oder IP-basierte ACLs anwenden.
Beim MACH 4002-24G/48G können Sie je Interface sowohl MAC-basierte als auch IP-basierte ACLs anwenden.

6.8.1 Beschreibung Priorisierung mit ACLs

Die Priorisierung mit ACLs bietet Ihnen eine Erweiterung der Priorisierungsfunktion. Mit Hilfe der ACL-Aktion „assign queue” können Sie eine erweiterte Priorisierung an Hand von Protokollen, Quell- und Zieladressen, VLAN-ID, u.v.m. (siehe auf Seite 118 „Beschreibung IP-basierte ACLs“), (siehe auf Seite 119 „Beschreibung MAC-basierte ACLs“) vornehmen.

Trifft beim Paketempfang eine ACL-Regel zu, die mit einer Assign-Queue-Aktion versehen ist, dann modifiziert das Gerät die Prioritätsinformation im Datenpaket (siehe auf Seite 175 „QoS/Priorität“) entsprechend des spezifizierten (siehe Tabelle 5) Assign-Queue-Parameters. Dieser Vorgang heißt ACL-Remarking. Das Gerät sendet die Datenpakete mit der modifizierten Prioritätsinformation.

Assign-Queue-Paramter	VLAN-Priorität	DSCP
0	0	CS0 (0)
1	1	CS1 (8)
2	2	CS2 (16)
3	3	CS3 (24)
4	4	CS4 (32)
5	5	CS5 (40)
6	6	CS6 (48)
7	7	CS7 (56)

Tab. 5: Zuordnung der Assign-Queue-Parameter zur modifizierten VLAN-Priorität und zum modifizierten DSCP-Wert

6.8.2 Beschreibung IP-basierte ACLs

Das Gerät unterscheidet zwischen Standard- und erweiterten IP-basierten ACLs. ACLs mit einer Identifikationsnummer (ACL-ID)

- von 1 bis 99 sind Standard-IP-basierte ACLs und
- von 100 bis 199 sind erweiterte (extended) IP-basierte ACLs.

Standard-IP-basierte ACLs bieten folgende Kriterien zur Filterung:

- IP-Quelladresse mit Netzmaske
- Alle Datenpakete (match any)

Erweiterte IP-basierte ACLs bieten folgende Kriterien zur Filterung:

- Alle Datenpakete (every)
- Protokollnummer bzw. Protokoll (IP, ICMP, IGMP, TCP, UDP)
- IP-Quelladresse mit Netzmaske oder alle IP-Quelladressen (any)
- Schicht 4-Protokollportnummer der Quelle (UDP-Port, TCP-Port)
- IP-Zieladresse mit Netzmaske oder alle IP-Zieladressen (any)
- Schicht 4-Protokollportnummer des Ziels (UDP-Port, TCP-Port)
- ToS-Feld mit Maske

- DSCP-Feld
- IP-Precedence-Feld

Anmerkung: Wenn Sie IP-ACLs an Ports anwenden, die sich im HIPER-Ring befinden oder an der Ring-/Netzkopplung beteiligt sind, dann fügen Sie den ACLs die folgende Regel hinzu:

- PERMIT
- Protocol: UDP
- Source IP: ANY
- Destination IP: 0.0.0.0/32
- Source-Port: 0
- Destination-Port: 0
- CLI-Kommando (1xx steht für 100..199):

```
access-list 1xx permit udp any eq 0
0.0.0.0 0.0.0.0 eq 0
```

Anmerkung: IP-Adressmasken in den Regeln von ACLs sind invers. Das bedeutet, wenn Sie eine einzelne IP-Adresse maskieren wollen, dann wählen Sie die Netzmaske 0.0.0.0.

6.8.3 Beschreibung MAC-basierte ACLs

Während Sie IP-basierte ACLs über eine Identifikationsnummer identifizieren, identifizieren Sie MAC-basierte ACLs über einen beliebigen eindeutigen Namen.

MAC-basierte ACLs bieten folgende Kriterien zur Filterung:

- Quell-MAC-Adresse mit Masken oder alle Quellen (any)
- Ziel-MAC-Adresse oder alle Ziele (any)

- Ethernet Type
- VLAN-ID
- VLAN-Priorität (COS)
- Secondary VLAN-ID
- Secondary VLAN-Priorität

Anmerkung: Wenn Sie MAC-ACLs an Ports anwenden, die sich im HIPER-Ring befinden oder an der Ring-/Netzkopplung beteiligt sind, dann fügen Sie den ACLs die folgende Regel hinzu:

- PERMIT
- Source MAC: ANY
- Destination MAC: 00:80:63:00:00:00
- Destination MAC-Maske: 01:00:00:ff:ff:ff
- CLI-Komando im Config-mac-access-Modus:
  `permit any 00:80:63:00:00:00 01:00:00:ff:ff:ff`

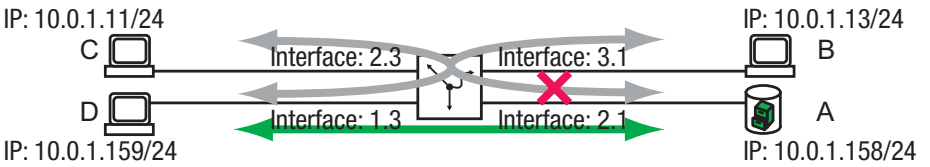
Anmerkung: Wenn Sie MAC-ACLs an Ports anwenden, die sich im MRP-Ring befinden, dann fügen Sie den ACLs die folgende Regel hinzu:

- PERMIT
- Source MAC: ANY
- Destination MAC: 01:15:4E:00:00:00
- Destination MAC-Maske: 00:00:00:00:00:03
- CLI-Komando im Config-mac-access-Modus:
  `permit any 01:15:4E:00:00:00 00:00:00:00:00:03`

Anmerkung: MAC-Adressmasken in den Regeln von ACLs sind invers. Das bedeutet, wenn Sie eine einzelne MAC-Adresse maskieren wollen, dann wählen Sie die Netzmaske 00:00:00:00:00:00.
Wenn Sie MAC-Adressen im Bereich von 00:80:63:00:00:00 bis 00:80:63:FF:FF:FF maskieren wollen, dann wählen Sie die Netzmaske 00:00:00:FF:FF:FF.

6.8.4 IP-ACLs konfigurieren

Beispiel: Erweiterte ACL



B und C dürfen nicht mit A kommunizieren.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`access-list 100 deny ip 10.0.1.11 0.0.0.0 10.0.1.158 0.0.0.0`	Erzeugt die erweiterte ACL 100 mit der 1. Regel. Diese verweigert den Datenverkehr von der IP-Quelladresse 10.0.1.11 zur IP-Zieladresse 10.0.1.158.
`access-list 100 permit ip any any`	Fügt der ACL 100 eine weitere Regel hinzu. Diese erlaubt den Datenverkehr von jeder IP-Quelladresse zu jeder IP-Zieladresse.
`access-list 110 deny ip 10.0.1.13 0.0.0.0 10.0.1.158 0.0.0.0`	Erzeugt die erweiterte ACL 110 mit der 1. Regel. Diese verweigert den Datenverkehr von der IP-Quelladresse 10.0.1.13 zur IP-Zieladresse 10.0.1.158.
`access-list 110 permit ip any any`	Fügt der ACL 110 eine weitere Regel hinzu. Diese erlaubt den Datenverkehr von jeder IP-Quelladresse zu jeder IP-Zieladresse.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show ip access-lists 100`	Zeigt die Regeln von ACL 100 an.

```
ACL ID: 100


Rule Number: 1
Action..................................... deny
Match All.................................. FALSE
Protocol................................... 255(ip)
Source IP Address.......................... 10.0.1.11
Source IP Mask............................. 0.0.0.0
Destination IP Address..................... 10.0.1.158
Destination IP Mask........................ 0.0.0.0

Rule Number: 2
Action..................................... permit
Match All.................................. TRUE
```

`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/3`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/3.
`ip access-group 100 in`	Bindet die ACL 100 für empfangene Daten an das Interface 2.3.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 3/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 3.1.
`ip access-group 110 in`	Bindet die ACL 110 für empfangene Daten an das Interface 3.1.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.

```
show access-lists interface 2/3 in

ACL Type             ACL ID                Sequence Number
-------- ------------------------------ ---------------
IP       100                            1
```

6.8.5 MAC-ACLs konfigurieren

Beispiel: MAC-ACL
AppleTalk und IPX aus dem gesamten Netz ausfiltern.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mac access-list extended ipx-apple`	Erzeugt die erweiterte ACL „ipx-apple“
`deny any any ipx`	Fügt der Liste die Regel „IPX verweigern“ hinzu.
`deny any any appletalk`	Fügt der Liste die Regel „AppleTalk verweigern“ hinzu.
`permit any any`	Fügt der Liste die Regel „alle anderen Daten zulassen“ hinzu.
`exit`	Wechsel in den Konfigurationsmodus.
`mac access-group ipx-apple in`	Bindet die ACL „ipx-apple“ an alle Interfaces.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show mac access-lists`	Zeigt die ACLs an.

```
     MAC ACL Name                Rules Direction      Interface(s)
------------------------------- ----- --------- ------------------
ipx-apple                        3     inbound   1/1,1/2,1/3,1/4,2/
                                                   1,2/2,2/3,2/4,3/1,3/2
```

`show access-lists interface 1/1 in`	Zeigt die ACLs von Interface 1.1 an.

```
ACL Type             ACL ID                Sequence Number
-------- ------------------------------ ---------------
MAC      ipx-apple                      1
```

6.8.6 Priorisierung mit IP-ACLs konfigurieren

Beispiel: Priorisieren von Multicast-Strömen.

- Den Multicast-Strömen mit den IP-Multicast-Zieladressen 239.1.1.1 bis 239.1.1.255 die Priorität 6 zuordnen und
- Den Multicast-Strömen mit den IP-Multicast-Zieladressen 237.1.1.1 bis 237.1.1.255 die Priorität 5 zuordnen und

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`access-list 102 permit ip any 239.1.1.1 0.0.0.255 assign-queue 6`	Erzeugt die erweiterte ACL 102 mit der 1. Regel. Diese Regel weist den IP-Multicast-Zieladressen 239.1.1.1 mit der Maske 0.0.0.255 die Priorität 6 zu.
`access-list 102 permit ip any 237.1.1.1 0.0.0.255 assign-queue 5`	Fügt der ACL 102 eine weitere Regel hinzu. Diese Regel weist den IP-Multicast-Zieladressen 237.1.1.1 mit der Maske 0.0.0.255 die Priorität 5 zu.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show ip access-lists 102`	Zeigt die Regeln von ACL 102 an.

```
ACL ID: 102

Rule Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 255(ip)
Destination IP Address..................... 239.1.1.1
Destination IP Mask........................ 0.0.0.255
Assign Queue............................... 6

Rule Number: 2
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 255(ip)
Destination IP Address..................... 237.1.1.1
Destination IP Mask........................ 0.0.0.255
Assign Queue............................... 5
```

Beispiel: Erweiterte ACL mit Priorisierung an Hand des Simple Network Management-Protokolls (SNMP, Layer 4)

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`access-list 104 permit udp any any eq snmp assign-queue 5`	Erzeugt die erweiterte ACL 104 mit der 1. Regel. Diese Regel weist allen SNMP-Paketen mit dem UDP-Zielport (=161) die Priorität 5 zu. Diese Regel überschreibt eine eventuell in einem VLAN-Tag enthaltene Priorität mit dem Wert 5 und auch den IP-DSCP-Wert mit cs5.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show ip access-lists 104`	Zeigt die Regeln von ACL 104 an.

```
ACL ID: 104


Rule Number: 1
Action..................................... permit
Match All.................................. FALSE
Protocol................................... 17(udp)
Destination L4 Port Keyword................ 161(snmp)
Assign Queue............................... 5
```

`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/1.
`ip access-group 104 in`	Bindet die ACL 104 an das Interface 2.1.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show access-lists interface 2/1 in`	Zeigt die am Interface 2.1 angebundenen ACLs für empfangene Datenpakete an.

```
ACL Type             ACL ID                 Sequence Number
-------- ------------------------------ ---------------
IP       100                            1
IP       102                            3
IP       104                            4
```

ACL 100 enthält am Ende die Regel „alles erlauben”. Dadurch greifen die ACLs 102 und 104 nie. Die Reihenfolge zur Bearbeitung der ACLs können Sie über die Sequenznummer beeinflussen (siehe auf Seite 126 „Reihenfolge der Regeln festlegen“).

6.8.7 Reihenfolge der Regeln festlegen

Die Anwendung der ACLs hängt von deren Reihenfolge ab. Die erste Liste, die zutrifft kommt zur Anwendung und alle folgenden Regeln werden ignoriert. Durch die Vergabe der „Sequence Number“ können Sie die Reihenfolge beeinflussen. Eine kleine „Sequence Number“ hat Vorrang vor einer höheren.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip access-group 100 in 30`	Weist der ACL 100 die „Sequence Number“ 30 zu.
`ip access-group 102 in 10`	Weist der ACL 102 die „Sequence Number“ 10 zu.
	Weist der ACL 104 die „Sequence Number“ 20 zu.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show access-lists interface 2/1 in`	Zeigt die am Interface 2.1 angebundenen ACLs für empfangen Datenpakete an.

```
ACL Type             ACL ID                 Sequence Number
-------- ------------------------------- ---------------
IP       100                                30
IP       104                                20
IP       102                                10
```

6.8.8 ACLs für Layer-4-Fragmente

Die Aufteilung eines langen Datenpaketes auf mehrere kürzere Datenpakete heißt Fragmentierung. Beispielsweise fragmentieren manche Router ein Layer-4-Datenpaket in mehrere Layer-3-Datenpakete, wenn die Länge des Datenpaketes größer ist als die MTU (Maximum Transmission Unit) der übertragenden Schnittstelle.

Ausschließlich das erste Layer-3-Datenpaket enthält den Layer-4-Header, z.B. TCP oder UDP. Die folgenden Datenpakete mit den Layer-4-Fragmenten enthalten keinen auswertbaren Layer-4-Header. ACLs verwerfen diese Datenpakete deshalb. Die Geräte MACH104, MACH1040 und MACH4002 24G/48G bieten Ihnen durch die Verarbeitung von Layer-4-Fragmenten die Möglichkeit, auch diese Datenpakete weiterzuleiten.

Wenn Sie eine ACL für Layer 4 einrichten, erzeugt das Gerät aus der benutzerdefinierten Regel automatisch eine zweite Regel für die Fragmente:

- Die benutzerdefinierte Regel bearbeitet das Datenpaket mit dem ersten Layer-4-Fragment.
- Die automatisch erzeugte Regel bearbeitet die Datenpakete mit den folgenden Layer-4-Fragmenten.

Bei eingeschalteter Fragment-Verarbeitung reduziert sich deshalb im Gerät die maximal mögliche Anzahl der ACLs.

Die Verarbeitung der Layer-4-Fragmente aktivieren Sie global im Gerät:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`access-list fragments`	Aktiviert im Gerät die Fragment-Verarbeitung.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show access-lists global`	Zeigt die globalen ACL-Einstellungen des Gerätes.

```
L4 Fragment Processing..................... Enabled
```

6.9 Login-Banner

Das Gerät bietet Ihnen die Möglichkeit, Benutzern einen Begrüßungstext anzuzeigen, bevor diese sich auf dem Gerät anmelden. Die Benutzer sehen den Begrüßungstext im Login-Dialog der grafischen Benutzeroberfläche (GUI) und des Command Line Interfaces (CLI).

Benutzer, die sich mit SSH anmelden, sehen den Begrüßungstext – abhängig vom verwendeten Client – vor oder während der Anmeldung.

Führen Sie die folgenden Arbeitsschritte aus:

- ☐ Öffnen Sie den Dialog `Sicherheit:Login-/CLI-Banner`, Registerkarte „Login-Banner“.
- ☐ Geben Sie im Rahmen „Banner-Text“ den Begrüßungstext ein. Max. 255 Zeichen sind zulässig.
- ☐ Um die Funktion einzuschalten, markieren Sie im Rahmen „Funktion“ das Optionsfeld „An“.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`set pre-login-banner text "<string>"`	Weist den Begrüßungstext zu: – Den Text in Anführungszeichen setzen. – Max. 255 Zeichen sind zulässig. – Tabulator durch Zeichenfolge `\\t` einfügen. – Zeilenumbruch durch Zeichenfolge `\\n` einfügen.
`set pre-login-banner operation`	Funktion einschalten.
`logout`	Vom Gerät abmelden. Vor dem erneuten Anmelden ist der Text sichtbar.

6.10 CLI-Banner

In der Voreinstellung zeigt der CLI-Startbildschirm Informationen über das Gerät, z. B. die Software-Version und Geräte-Einstellungen. Die Funktion „CLI-Banner“ bietet Ihnen die Möglichkeit, diese Informationen durch einen individuellen Text zu ersetzen.

Führen Sie die folgenden Arbeitsschritte aus:

- ☐ Öffnen Sie den Dialog `Sicherheit:Login-/CLI-Banner`, Registerkarte „CLI-Banner“.
- ☐ Geben Sie im Rahmen „Banner-Text“ den gewünschten Text ein. Max. 2048 Zeichen sind zulässig.
- ☐ Um die Funktion einzuschalten, markieren Sie im Rahmen „Funktion“ das Optionsfeld „An“.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`set clibanner text "<string>"`	Weist den Text zu: – Den Text in Anführungszeichen setzen. – Max. 2048 Zeichen sind zulässig. – Tabulator durch Zeichenfolge `\\t` einfügen. – Zeilenumbruch durch Zeichenfolge `\\n` einfügen.
`set clibanner operation`	Funktion einschalten.
`logout`	Vom Gerät abmelden. Vor dem erneuten Anmelden ist der Text sichtbar.

7 Die Systemzeit im Netz synchronisieren

Was Echtzeit wirklich bedeutet, hängt von den Zeitanforderungen der Anwendung ab.

Das Gerät bietet 2 Möglichkeiten mit unterschiedlicher Genauigkeit, die Zeit in Ihrem Netz zu synchronisieren.

Das Simple Network Time Protocol (SNTP) ist eine einfache Lösung für geringere Genauigkeitsanforderungen. Unter idealen Bedingungen erzielt SNTP eine Genauigkeit im Millisekunden-Bereich. Die Genauigkeit ist abhängig von der Signallaufzeit.

IEEE 1588 mit dem Precision Time Protocol (PTP) erreicht eine Genauigkeit im Submikrosekunden-Bereich. Diese Methode eignet sich auch für anspruchsvolle Anwendungen bis hin zur Prozesssteuerung.

Anwendungsgebiete sind beispielsweise:
- Logbucheinträge
- Produktionsdaten mit Zeitstempel versehen
- Prozesssteuerung

In Abhängigkeit von Ihren Bedürfnissen wählen Sie die passende Methode (SNMP oder PTP). Unter Beachtung der gegenseitigen Beeinflussung können Sie auch beide Methoden gleichzeitig nutzen.

7.1 Uhrzeit einstellen

Steht Ihnen keine Referenzuhr zur Verfügung, dann haben Sie die Möglichkeit, in einem Gerät die Systemzeit einzugeben, um das Gerät dann wie eine Referenzuhr einzusetzen (siehe auf Seite 136 „Konfiguration SNTP“), (siehe auf Seite 147 „Anwendungsbeispiel“).

Das Gerät ist mit einer gepufferten Hardware-Uhr ausgestattet. Diese führt die aktuelle Uhrzeit weiter,

- wenn die Stromversorgung ausfällt oder
- wenn Sie das Gerät von der Stromversorgung trennen.

Damit steht Ihnen nach dem Start des Gerätes wieder die aktuelle Uhrzeit zur Verfügung, z. B. für Log-Einträge.
Die Hardware-Uhr überbrückt eine Ausfallzeit der Stromversorgung von 1 Stunde. Voraussetzung dafür ist, dass die Stromversorgung das Gerät vorher mindestens 5 Minuten kontinuierlich gespeist hat.

Anmerkung: Passen Sie in Zeitzonen mit Sommer-/Winterzeit den lokalen Offset bei der Zeitumstellung an. Das Gerät kann die SNTP-Server-IP-Adresse und den lokalen Offset auch von einem DHCP-Server beziehen.

☐ Öffnen Sie den Dialog `Zeit:Grundeinstellungen`.

Dieser Dialog bietet Ihnen die Möglichkeit, unabhängig vom gewählten Zeitsynchronisationsprotokoll zeitbezogene Einstellungen vorzunehmen.

- Die „Systemzeit (UTC)“ zeigt die mittels SNTP oder PTP empfangene Uhrzeit an.
  Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.

  Anmerkung: Ist die Zeit-Quelle PTP, beachten Sie, dass die PTP-Zeit die Zeitskala TAI verwendet. Die TAI-Zeit geht gegenüber der UTC-Zeit um 34 s vor (Stand 01.01.2011).
  Ist auf der PTP-Referenzuhr der UTC-Offset richtig konfiguriert, korrigiert das Gerät diesen Unterschied bei der Anzeige von „Systemzeit (UTC) automatisch.
- Die „Systemzeit“ übernimmt die „Systemzeit (UTC)“ unter Berücksichtigung der lokalen Zeitdifferenz zur „Systemzeit (UTC)“.
  „Systemzeit“ = „Systemzeit (UTC)“ + „Lokaler Offset“.
- Quelle der Zeit zeigt den Ursprung der folgenden Zeitangabe an. Das Gerät wählt automatisch die Quelle mit der höchsten Genauigkeit.
  Mögliche Quellen sind: `local`, `ptp` und `sntp`. Die Quelle ist zunächst `local`.
  Ist PTP aktiviert und empfängt das Gerät einen gültigen PTP-Frame, setzt es seine Zeit-Quelle auf `ptp`. Ist SNTP aktiviert und empfängt das Gerät ein gültiges SNTP-Paket, setzt es seine Zeit-Quelle auf `sntp`. Das Gerät gibt der Zeitquelle PTP den Vorrang vor SNTP.
- ☐ Mit „Setze Zeit vom PC“ übernimmt das Gerät die Zeit des PCs als Systemzeit und berechnet mit der lokalen Zeitdifferenz die „Systemzeit (UTC)“.
  „Systemzeit (UTC)“ = „Systemzeit“ - „Lokaler Offset“
- ☐ Lokaler Offset dient zur Anzeige/Eingabe der Zeitdifferenz zwischen der lokalen Zeit und der „Systemzeit (UTC)“.

  Mit „Setze Offset vom PC“ ermittelt das Gerät die Zeitzone auf Ihrem PC und berechnet daraus die lokale Zeitdifferenz.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`sntp time <YYYY-MM-DD HH:MM:SS>`	Einstellen der Systemzeit des Gerätes.
`sntp client offset <-1000 to 1000>`	Eingeben der Zeitdifferenz zwischen der lokalen Zeit und der „Systemzeit (UTC)“.

7.2 SNTP

7.2.1 Beschreibung SNTP

Das Simple Network Time Protocol (SNTP) bietet Ihnen die Möglichkeit, die Systemzeit in Ihrem Netz zu synchronisieren.
Das Gerät unterstützt die SNTP-Client- und die SNTP-Server-Funktion.

Der SNTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die Anzeige ist weltweit gleich. Lokale Zeitverschiebungen bleiben unberücksichtigt.

SNTP verwendet dasselbe Paketformat wie NTP, daher kann ein SNTP-Client seine Zeit sowohl von einem SNTP-Server als auch von einem NTP-Server beziehen.

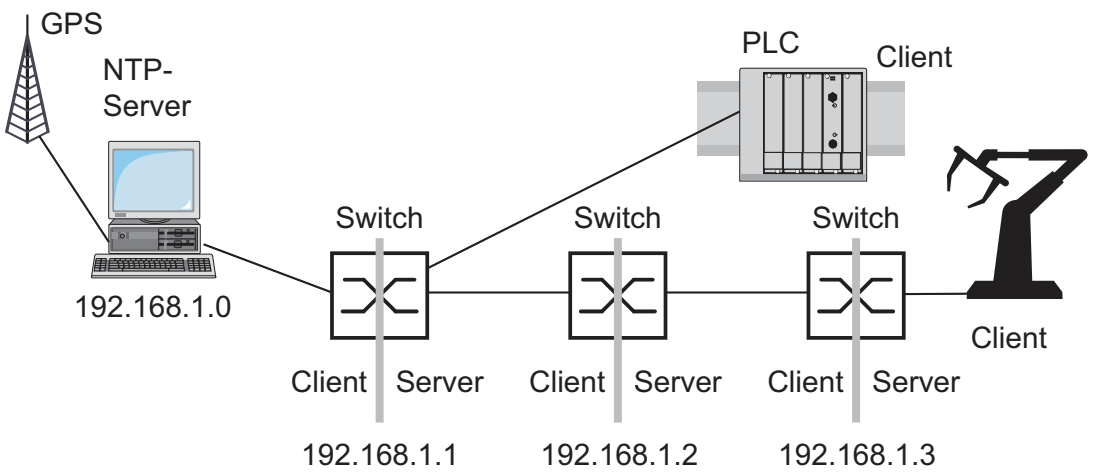


Abb. 22: SNTP-Kaskade

7.2.2 Vorbereitung der SNTP-Konfiguration

☐ Zeichnen Sie einen Netzplan mit den am SNTP beteiligten Geräten, um einen Überblick über die Weitergabe der Uhrzeit zu erhalten. Beachten Sie bei der Planung, dass die Genauigkeit der Uhrzeit von der Signallaufzeit abhängig ist.

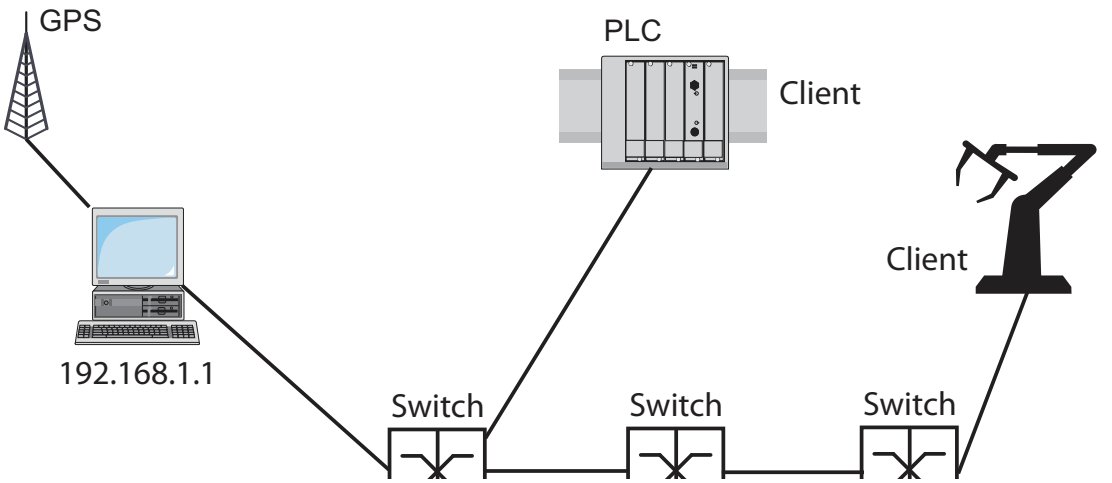


Abb. 23: Beispiel SNTP-Kaskade

☐ Schalten Sie die SNTP-Funktion auf den Geräten ein, deren Zeit Sie mittels SNTP einstellen wollen.
Der SNTP-Server des Geräts antwortet auf Unicast-Anfragen, sobald er eingeschaltet ist.

☐ Wenn Sie keine Referenzuhr zur Verfügung haben, dann bestimmen Sie ein Gerät als Referenzuhr und stellen Sie dessen Systemzeit möglichst genau ein.

Anmerkung: Für eine genaue Systemzeitverteilung mit kaskadierten SNTP-Servern und -Clients verwenden Sie im Signalpfad zwischen SNTP-Servern und SNTP-Clients ausschließlich Netzkomponenten (Router, Switches, Hubs), die SNTP-Pakete mit möglichst kleiner Verzögerung weiterleiten.

7.2.3 Konfiguration SNTP

☐ Wählen Sie den Dialog `Zeit:SNTP`.

▶ Funktion

☐ In diesem Rahmen schalten Sie die SNTP-Funktion global ein/aus.

▶ SNTP-Status

☐ Die „Statusmeldung“ zeigt Zustände des SNTP-Clients als eine oder mehrere Textmeldungen an, z.B. `Server 1 antwortet nicht`.

▶ Konfiguration SNTP-Client

☐ In „Client-Status“ schalten Sie den SNTP-Client des Geräts ein/aus.

☐ In „Externe Server-Adresse“ geben Sie die IP-Adresse des SNTP-Servers ein, von dem das Gerät zyklisch die Systemzeit anfordert.

☐ In „Redundante Server-Adresse“ geben Sie die IP-Adresse des SNTP-Servers ein, von dem das Gerät zyklisch die Systemzeit anfordert, wenn es 1 Sekunde nach einer Anforderung keine Antwort vom „Externen Server-Adresse“ erhält.

Anmerkung: Wenn Sie von einer externen/redundanten Server-Adresse die Systemzeit beziehen, stellen Sie die zugehörigen Server-Adresse(n) ein und deaktivieren Sie die Einstellung `SNTP-Broadcasts akzeptieren` (siehe unten). So stellen Sie sicher, dass das Gerät die Zeit der eingetragenen Server verwendet und sich nicht auf Broadcasts synchronisiert, die möglicherweise nicht vertrauenswürdig sind.

☐ In „Server-Anforderungsintervall“ geben Sie den Zeitabstand ein, in dem das Gerät SNTP-Pakete anfordert (gültige Werte: 1 s bis 3600 s, Lieferzustand: 30 s).

☐ Mit „SNTP-Broadcasts akzeptieren“ übernimmt das Gerät die Systemzeit aus SNTP-Broadcast-/Multicast-Paketen, die es empfängt.

☐ Mit „Client deaktivieren nach erfolgter Synchronisation“ stellt das Gerät nur einmal nach dem Aktivieren des Client-Status seine Systemzeit nach dem SNTP-Server und schaltet den Client danach ab.

Anmerkung: Haben Sie gleichzeitig PTP eingeschaltet, sammelt der SNTP-Client zuerst 60 Zeitstempel, bevor er sich deaktiviert. Dabei ermittelt das Gerät die Driftkompensation für seine PTP-Uhr. Dies dauert beim voreingestellten Server-Anforderungsintervall etwa eine halbe Stunde.

Konfiguration SNTP-Server

- ☐ In „Server-Status“ schalten Sie den SNTP-Server des Geräts ein/aus.
- ☐ In „Anycast-Zieladresse“ geben Sie die IP-Adresse an, an die der SNTP-Server des Gerätes seine SNTP-Pakete schickt (siehe Tabelle 6).
- ☐ In „VLAN-ID“ geben Sie das VLAN an, in das das Gerät zyklisch seine SNTP-Pakete verschicken soll.
- ☐ In „Anycast-Sendeintervall“ geben Sie den Zeitabstand an, in dem das Gerät SNTP-Pakete verschickt (gültige Werte: 1 s bis 3600 s, Lieferzustand: 120 s).
- ☐ Mit „Server deaktivieren bei lokaler Zeitquelle“ schaltet das Gerät die SNTP-Server-Funktion aus, wenn die Quelle der Zeit `local` ist (siehe Dialog `Zeit`).

IP-Zieladresse	SNTP-Paket versenden an
0.0.0.0	Niemand
Unicast-Adresse (0.0.0.1 - 223.255.255.254)	Unicast-Adresse
Multicast-Adresse (224.0.0.0 - 239.255.255.254), insbesondere 224.0.1.1 (NTP-Adresse)	Multicast-Adresse
255.255.255.255	Broadcast-Adresse

Tab. 6: Zieladressklassen für SNTP- und NTP-Pakete

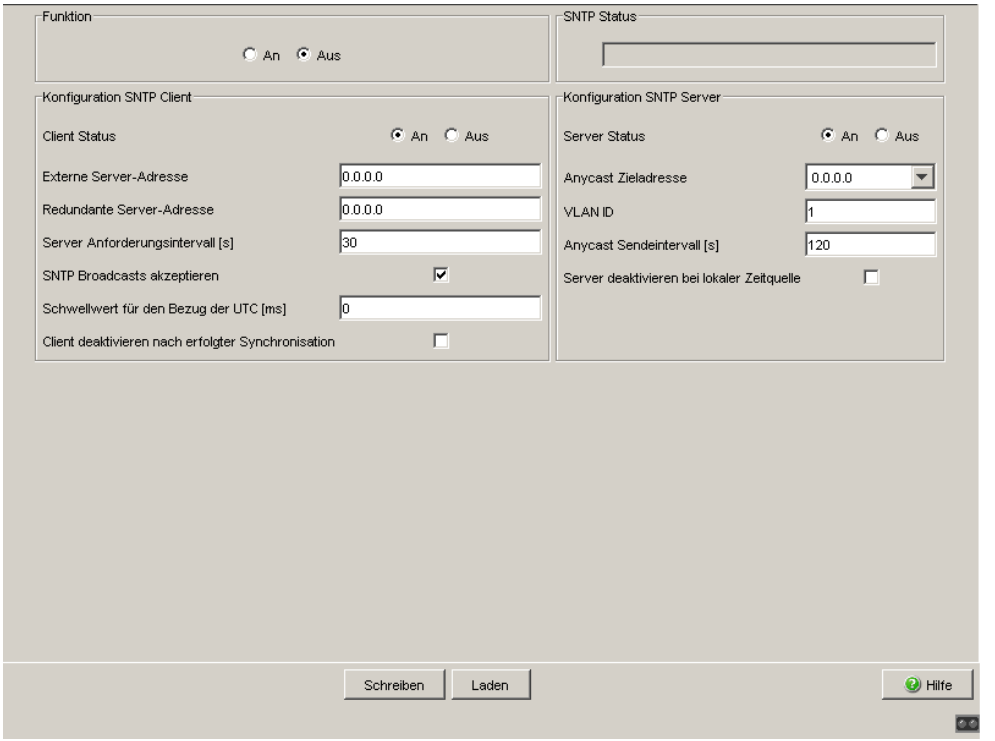


Abb. 24: Dialog SNTP

Gerät	192.168.1.1	192.168.1.2	192.168.1.3
Funktion	an	an	an
Server Zieladresse	0.0.0.0	0.0.0.0	0.0.0.0
Server VLAN-ID	1	1	1
Sendeintervall	120	120	120
Client Externe Server Adresse	192.168.1.0	192.168.1.1	192.168.1.2
Anforderungsintervall	30	30	30
Broadcasts akzeptieren	nein	nein	nein

Tab. 7: Einstellungen für das Beispiel (siehe Abbildung 23)

7.3 Precison Time Protocol

7.3.1 Funktionsbeschreibung PTP

Voraussetzung für zeitkritische, über ein LAN gesteuerte Anwendungen ist ein präzises Zeitmanagement.
Der Standard IEEE 1588 beschreibt mit dem Precision Time Protocol (PTP) ein Verfahren, das die beste Hauptuhr (Best Master Clock) in einem LAN bestimmt und somit die präzise Synchronisation der Uhren in diesem LAN ermöglicht.

Dieses Verfahren erlaubt eine Synchronisation der betroffenen Uhren mit einer Genauigkeit bis zu wenigen 100 ns. Die Belastung des Netzes mit Synchronisationsnachrichten ist dabei verschwindend gering. PTP benutzt die Multicast-Kommunikation.

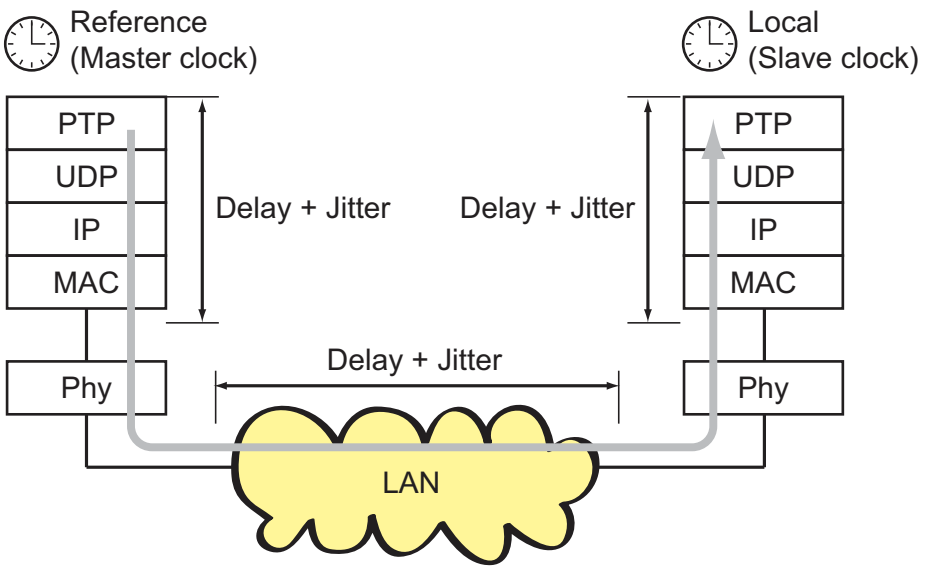
Einfluß auf die Präzision haben:

- Genauigkeit der Referenzuhr
  IEEE 1588 klassifiziert Uhren nach ihrer Genauigkeit. Ein Algorithmus, der die Genauigkeit der verfügbaren Uhren im Netz ermittelt, bestimmt die genaueste Uhr zur „Grandmaster"-Uhr.

PTPv1 Stratum-nummer	PTPv2 Clock Class	Spezifikation
0	– (Priorität 1 = 0)	Für zeitlich begrenzte, spezielle Zwecke, um einer Uhr eine höhere Genauigkeit zuzuordnen als allen anderen Uhren im Netz.
1	6	Bezeichnet die Uhr als Referenzuhr mit höchster Genauigkeit. Die Uhr kann sowohl eine Boundary- als auch eine Ordinary-Uhr sein. Zu Stratum 1-/Clock Class 6-Uhren gehören GPS-Uhren und kalibrierte Atomuhren. Eine Stratum 1-Uhr kann nicht mittels PTP von einer anderen Uhr im PTP-System synchronisiert werden.
2	6	Bezeichnet die Uhr als Referenzuhr zweiter Wahl.
3	187	Bezeichnet die Uhr als Referenzuhr, die über eine externe Leitung synchronisiert werden kann.
4	248	Bezeichnet die Uhr als Referenzuhr, die nicht über eine externe Leitung synchronisiert werden kann. Dies ist die Standardeinstellung für Boundary Clocks.
5–254	–	Reserviert.
255	255	Eine solche Uhr sollte niemals als die sogenannte beste Hauptuhr verwendet werden.

Tab. 8: Stratum – Klassifikation der Uhren

- Kabellaufzeiten; Gerätelaufzeiten (Delay)
  Das von IEEE 1588 vorgegebene Kommunikationsprotokoll ermöglicht die Ermittlung von Laufzeiten. Algorithmen zur Berechnung der aktuellen Uhrzeit gleichen diese Laufzeiten aus.
- Genauigkeit lokaler Uhren
  Das von IEEE 1588 vorgegebene Kommunikationsprotokoll berücksichtigt die Ungenauigkeit lokaler Uhren gegenüber der Referenzuhr. Berechnungsformeln erlauben die Synchronisation der lokalen Zeit unter Berücksichtigung der Ungenauigkeit der lokalen Uhr gegenüber der Referenzuhr.



PTP	Precision Time Protocol (Application Layer)
UDP	User Datagramm Protocol (Transport Layer)
IP	Internet Protocol (Network Layer)
MAC	Media Access Control
Phy	Physical Layer

Abb. 25: Delay- und Jitter beim Uhrenabgleich

Um die Reduktion der Laufzeit und des Jitters im Protokollstapel zu umgehen, empfiehlt IEEE 1588, eine spezielle Hardware-Zeitstempeleinheit (Time Stamp Unit) zwischen MAC und Phy einzusetzen.
Geräte/Module mit der Namensergänzung „-RT“ besitzen diese Zeitstempeleinheit und unterstützen PTP Version 1. Die Medienmodule MM23 und MM33 unterstützen PTP Version 1 und PTP Version 2.

Die Laufzeit und der Jitter im LAN summieren sich in den Medien und Übertragungsgeräten entlang des Übertragungspfades.

Mit der Einführung von PTP Version 2 stehen 2 verschiedene Verfahren der Laufzeitmessung zur Verfügung:

- End-to-End (E2E)
  E2E entspricht dem von PTP Version 1 verwendeten Verfahren. Dabei misst jede Slave-Uhr ausschließlich die Laufzeit zu ihrer Master-Uhr.
- Peer-to-Peer (P2P)
  Bei P2P misst wie bei E2E jede Slave-Uhr die Laufzeit zu ihrer Master-Uhr. Zusätzlich misst bei P2P jede Master-Uhr die Laufzeit zur Slave-Uhr. Z.B. kann bei einer Unterbrechung eines redundanten Ringes die Slave-Uhr zur Master-Uhr und die Master-Uhr zur Slave-Uhr werden. Dieser Wechsel der Synchronisationsrichtung findet ohne Präzisionsverlust statt, da bei P2P die Laufzeit in die andere Richtung schon bekannt ist.

Die Kabellaufzeiten sind relativ konstant. Änderungen treten sehr langsam auf. Diese Tatsache berücksichtigt IEEE 1588 durch regelmäßige Messungen und Neuberechnungen.

Die Ungenauigkeit durch Gerätelaufzeit und Geräte-Jitter umgeht IEEE 1588 durch die Definition von „Boundary Clocks“. Boundary Clocks sind Uhren, die in Geräte integriert sind. Diese Uhren werden auf der einen Seite im Signalpfad synchronisiert und auf der anderen Seite des Signalpfades dienen sie zur Synchronisation der folgenden Uhren (Ordinary Clocks).
PTP Version 2 definiert darüberhinaus sogenannte Transparent Clocks. Eine Transparent Clock kann selbst keine Referenzuhr sein und kann sich auch nicht auf diese synchronisieren. Sie korrigiert jedoch die von ihr vermittelten PTP-Nachrichten um die eigene Durchlaufzeit und entfernt somit den durch die Vermittlung entstandenen Jitter. Besonders bei der Kaskadierung mehrerer Uhren können Sie mit Transparent-Clocks eine höhere Präzision der Zeit für die verbundenen Endgeräte erreichen als mit Boundary-Clocks.

Der Power-Profile-TLV-Check ist auf den Geräten Mice, PowerMICE, MACH1040, MACH104 verfügbar. Im aktivierten Zustand prüft diese Funktion, ob Power-TLVs existieren. Folgen Sie den nachfolgenden Handlungsschritten, um für das Gerät die Prüfung der Datenpakete auf Power-Profile-TLVs zu aktivieren und TLVs für die Syntonisierung zu benutzen:

☐ Öffnen Sie den Dialog `Zeit:PTP:Version 2(TC):Global`.

☐ Aktivieren Sie das Kontrollkästchen für „Power TLV Check“.

☐ Aktivieren Sie das Kontrollkästchen für „Syntonize“.

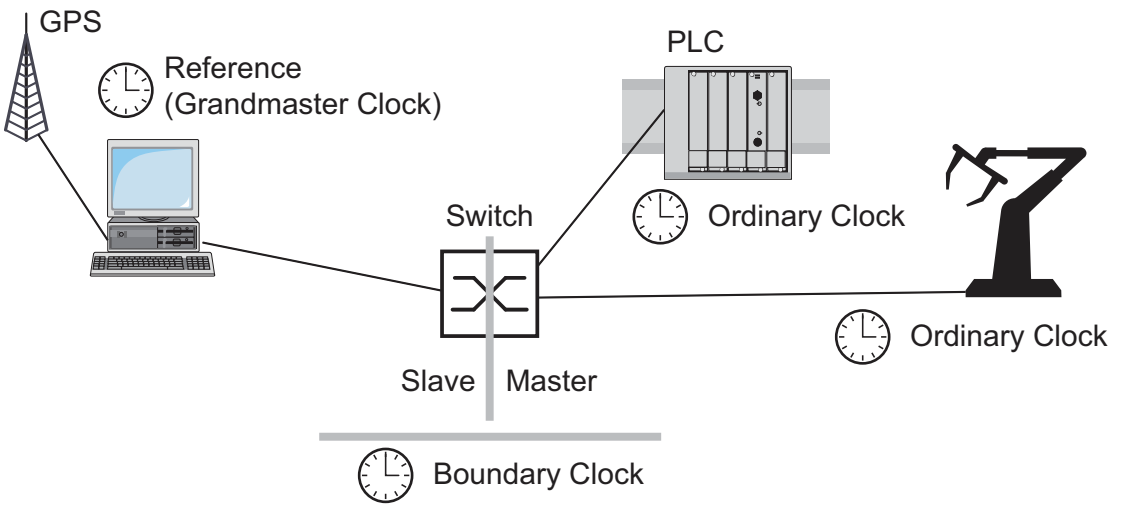


Abb. 26: Position der Boundary-Clock in einem Netz

Unabhängig von physikalischen Kommunikationspfaden sieht das PTP logische Kommunikationspfade vor, die Sie durch das Einrichten von PTP-Subdomänen definieren. Subdomänen haben den Zweck, Gruppen von Uhren, die zeitlich unabhängig vom Rest der Domäne sind, zu bilden. Typischerweise benutzen die Uhren einer Gruppe die gleichen Kommunikationspfade wie andere Uhren auch.

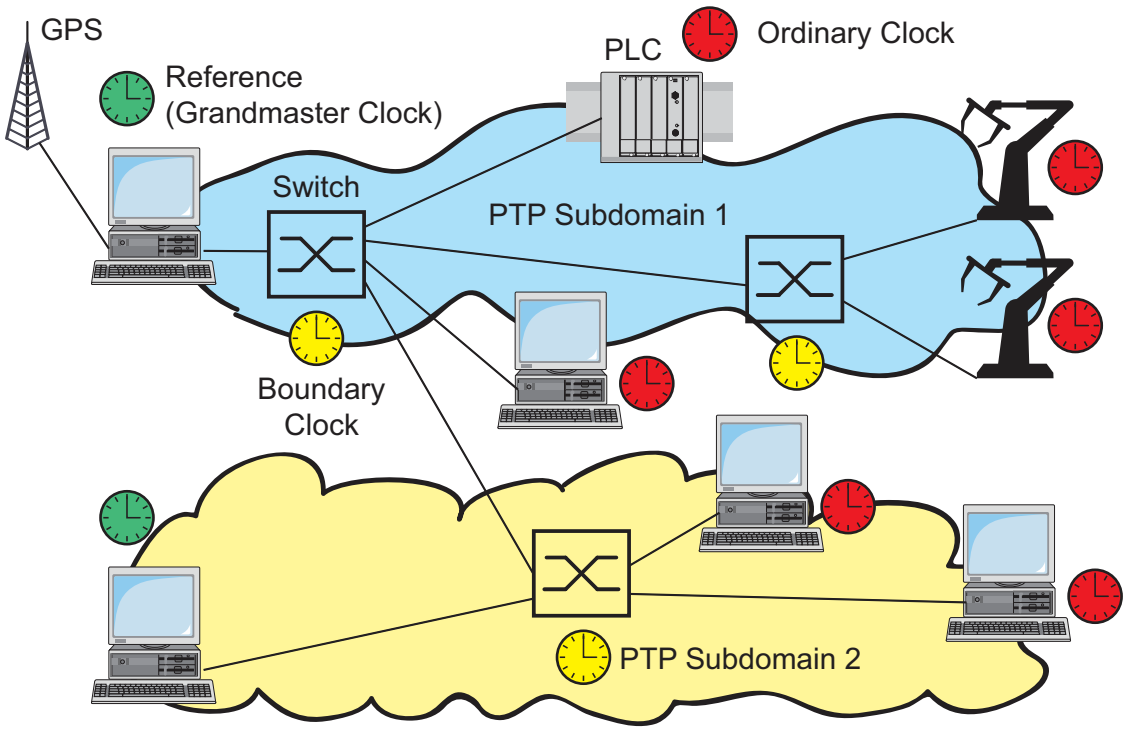


Abb. 27: PTP-Subdomänen

7.3.2 PTP-Konfiguration vorbereiten

Nach dem Aktivieren der Funktion übernimmt das PTP die Konfiguration automatisch.

☐ Um sich einen Überblick über die Uhrenverteilung zu verschaffen, zeichnen Sie einen Netzplan mit den am PTP beteiligten Geräten.

Anmerkung: Schließen Sie alle Verbindungen, die Sie zur Verteilung der PTP-Informationen benutzen an Anschlüsse mit integrierter Zeitstempeleinheit (RT-Module) an.
Geräte ohne Zeitstempeleinheit nehmen die Informationen des PTP auf und stellen ihre Uhr danach. Sie beteiligen sich nicht am Protokoll.

☐ Schalten Sie die PTP-Funktion auf die Geräten ein, deren Zeit Sie mittels PTP synchronisieren wollen.

☐ Wählen Sie die PTP-Version und den PTP-Modus. Wählen Sie für alle Geräte, die Sie synchronisieren wollen die gleiche PTP-Version.

PTP-Modus	Anwendung
v1-simple-mode	Unterstützung für PTPv1 ohne spezielle Hardware. Das Gerät synchronisiert sich auf empfangene PTPv1-Nachrichten. Wählen Sie diesen Modus für Geräte ohne Zeitstempeleinheit (RT-Modul).
v1-boundary-clock	Boundary-Clock-Funktion nach IEEE 1588-2002 (PTPv1)
v2-boundary-clock-onestep	Boundary-Clock-Funktion nach IEEE 1588-2008 (PTPv2) für Geräte mit MM23- und MM33-Medienmodulen. Der One-Step Modus übermittelt die präzise PTP-Zeit mit einer Nachricht.
v2-boundary-clock-twostep	Boundary-Clock-Funktion nach IEEE 1588-2008 (PTPv2) für Geräte mit RT-Modulen. Der Two-Step Modus übermittelt die präzise PTP-Zeit mit 2 Nachrichten.

Tab. 9: Auswahl eines PTP-Modus´

PTP-Modus	Anwendung
v2-simple-mode	Unterstützung für PTPv2 ohne spezielle Hardware. Das Gerät synchronisiert sich auf empfangene PTPv2-Nachrichten. Wählen Sie diesen Modus für Geräte ohne Zeitstempeleinheit (RT-Modul).
v2-transparent-clock	Transparent-Clock-(One-Step)-Funktion nach IEEE 1588-2008 (PTPv2) für Geräte mit MM23- und MM33-Medienmodulen.

Tab. 9: Auswahl eines PTP-Modus´

☐ Wenn Sie keine Referenzuhr zur Verfügung haben, dann bestimmen Sie ein Gerät als Referenzuhr und stellen Sie dessen Systemzeit möglichst genau ein.

7.3.3 Anwendungsbeispiel

Die Synchronisation der Zeit im Netz soll über PTP erfolgen. Das linke Gerät (siehe Abbildung 28) erhält als SNTP-Client über SNTP die Uhrzeit vom NTP-Server. Einer von einem NTP-Server empfangenen Uhrzeit weist das Gerät ein PTP-Clock-Stratum von 2 (PTPv1) bzw. eine Clock Class von 6 (PTPv2) zu. Somit wird das linke Gerät zur Referenzuhr für die PTP-Synchronisation und es ist „Bevorzugter Master“. Der „Bevorzugte Master“ gibt über seine Anschlüsse am RT-Modul das genaue Zeitsignal weiter. Das Gerät mit RT-Modul empfängt das genaue Zeitsignal an einem Anschluss seines RT-Moduls und hat somit den „Clock Modus“ „v1-boundary-clock“. Die Geräte ohne RT-Modul bekommen den „Clock Modus“ „v1-simple-mode“.

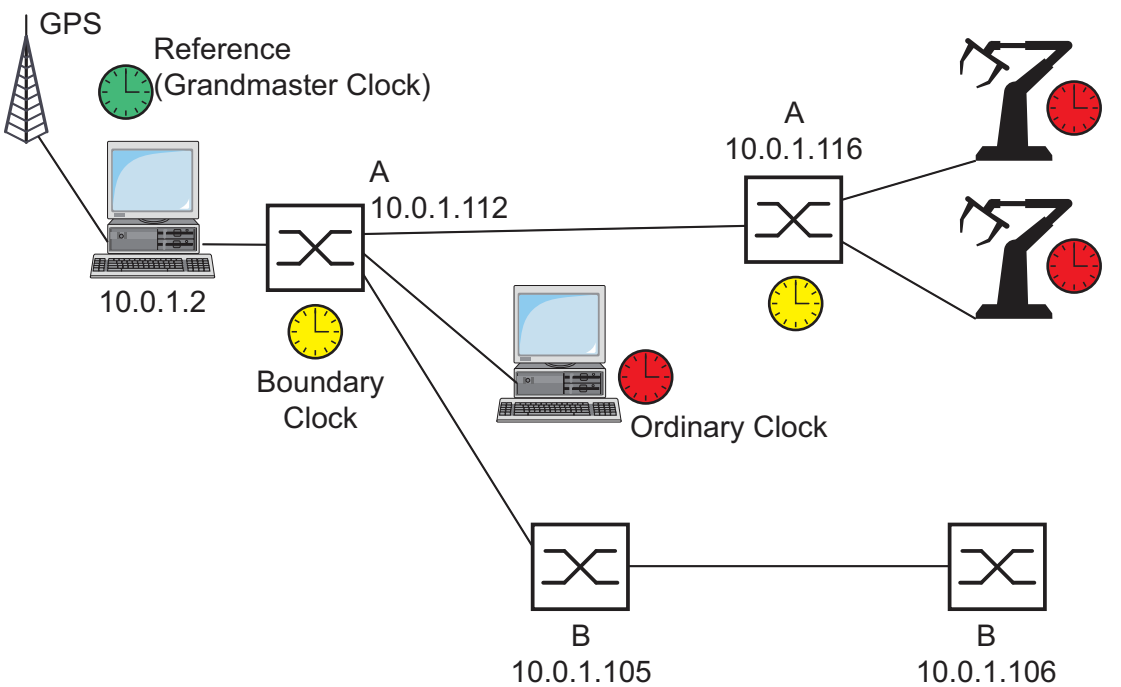


Abb. 28: Beispiel für PTP-Synchronisation .
A: Gerät mit RT-Modul
B: Gerät ohne RT-Modul

Gerät	10.0.1.112	10.0.1.116	10.0.1.105	10.0.1.106
PTP Global				
Funktion	an	an	an	an
Clock Modus	v1-boundary-clock	v1-boundary-clock	v1-simple-mode	v1-simple-mode
Bevorzugter Master	true	false	false	false
SNTP				
Funktion	an	aus	aus	aus
Client-Status	an	aus	aus	aus
Externe Server-Adresse	10.0.1.2	0.0.0.0	0.0.0.0	0.0.0.0
Server-Anforderungsintervall	30	beliebig	beliebig	beliebig
SNTP-Broadcasts akzeptieren	nein	beliebig	beliebig	beliebig
Server-Status	an	aus	aus	aus
Anycast-Zieladresse	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
VLAN-ID	1	1	1	1

Tab. 10: Einstellungen für das Beispiel (siehe Abbildung 28)

Die folgenden Konfigurationsschritte gelten für das Gerät mit der IP-Adresse 10.0.1.112. Konfigurieren Sie die anderen Geräte analog mit den Werten aus der Tabelle oben.

☐ Geben Sie die SNTP-Parameter ein.

☐ Wählen Sie den Dialog `Zeit:SNTP`.
☐ Schalten Sie im Rahmen „Funktion“ SNTP global ein.
☐ Schalten Sie im Rahmen „Konfiguration SNTP-Client“ den SNTP-Client ein (Client-Status).
☐ Geben Sie im Rahmen „Konfiguration SNTP-Client“ ein:
– „Externe Server-Adresse“: 10.0.1.2
– „Anforderungsintervall“: 30
– „SNTP Broadcasts akzeptieren“: nein

☐ Schalten Sie im Rahmen „Konfiguration SNTP-Server“ den SNTP-Server ein (Server-Status).
☐ Geben Sie im Rahmen „Konfiguration SNTP-Server“ ein:
– „Anycast Zieladresse“: 0.0.0.0
– „VLAN-ID“: 1
☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`sntp operation on`	SNTP global einschalten.
`sntp operation client on`	SNTP-Client einschalten.
`sntp client server primary 10.0.1.2`	Die IP-Adresse des externen SNTP-Servers 10.0.1.2 eingeben.
`sntp client request-interval 30`	Den Wert 30 Sekunden für das SNTP-Server-Anforderungsintervall eingeben.
`sntp client accept-broadcast off`	„SNTP-Broadcasts akzeptieren“ ausschalten.
`sntp operation server on`	SNTP-Server einschalten.
`sntp anycast address 0.0.0.0`	Die SNTP-Server-Anycast-Zieladresse 0.0.0.0 eingeben.
`sntp anycast vlan 1`	Die SNTP-Server-VLAN-ID 1 eingeben.

☐ Geben Sie die globalen PTP-Parameter ein.

☐ Wählen Sie den Dialog `Zeit:PTP:Global`.
☐ Schalten Sie im Rahmen „Funktion IEEE 1588 / PTP“ die Funktion ein.
☐ Wählen Sie `v1-boundary-clock` für „PTP-Version-Modus“.
☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

`ptp operation enable`	PTP global einschalten.
`ptp clock-mode v1-boundary-clock`	PTP-Version und Clock-Modus wählen.

☐ In diesem Beispiel haben Sie das Gerät mit der IP-Adresse 10.0.1.112 zur PTP-Referenzuhr bestimmt. Damit definieren Sie dieses Gerät zum „Bevorzugten Master“.

☐ Wählen Sie den Dialog `Zeit:PTP:Version 1:Global`.
☐ Wählen Sie im Rahmen „Funktion IEEE 1588 / PTP“ die Stellung `true` für den „Bevorzugten Master“.
☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

`ptp v1 preferred-master true`	Dieses Gerät als „Bervorzugten Master“ definieren.

☐ Veranlassen Sie PTP, die Parameter zu übernehmen.

☐ Klicken Sie im Dialog `Zeit:PTP:Version 1:Global` auf „Reinitialisieren, damit PTP die eingetragenen Parameter übernimmt.

`ptp v1 re-initialize`	PTP-Parameter übernehmen.

☐ Speichern Sie die Einstellungen in den nicht-flüchtigen Speicher.

☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.

☐ Wählen Sie im Rahmen „Speichern“ den Speicherort „auf dem Gerät“ und klicken Sie auf „Sichern“, um die Konfiguration nicht-flüchtig in der aktiven Konfiguration zu speichern.

`copy system:running-config nvram:startup-config`	Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

7.4 Interaktion von PTP und SNTP

Laut PTP- und SNTP-Standard können beide Protokolle parallel in einem Netz existieren. Da beide Protokolle die Systemzeit des Gerätes beeinflussen, können Situationen auftreten, in denen beide Protokolle konkurrieren.

Anmerkung: Konfigurieren Sie die Geräte so, dass jedes Gerät ausschließlich aus einer Quelle die Uhrzeit bezieht.
Soll das Gerät seine Uhrzeit über PTP beziehen, dann geben Sie bei der SNTP-Client-Konfiguration die „Externe Server Adresse“ 0.0.0.0 ein und akzeptieren Sie keine SNTP-Broadcasts.
Soll das Gerät seine Uhrzeit über SNTP beziehen, dann achten Sie darauf, dass am SNTP-Server die „beste“ Uhr angeschlossen ist. Dann beziehen beide Protokolle die Uhrzeit vom selben Server. Das Beispiel (siehe Abbildung 29) zeigt eine solche Anwendung.

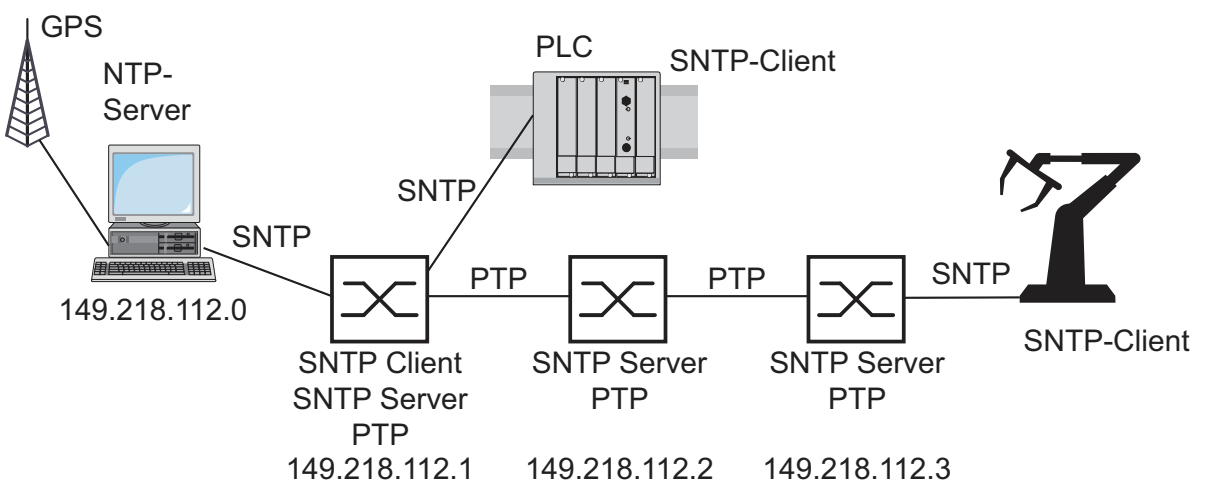


Abb. 29: Beispiel für die Koexistenz von PTP und SNTP

Anwendungsbeispiel

Die Anforderungen an die Genauigkeit der Uhrzeit im Netz sei recht hoch, die Endgeräte unterstützen jedoch ausschließlich SNTP (siehe Abbildung 29).

Gerät	149.218.112.1	149.218.112.2	149.218.112.3
PTP			
Funktion	an	an	an
Clock Modus	v1-boundary-clock	v1-boundary-clock	v1-boundary-clock
Bevorzugter Master	false	false	false
SNTP			
Funktion	an	an	an
Client-Status	an	aus	aus
Externe Server-Adresse	149.218.112.0	0.0.0.0	0.0.0.0
Server-Anforderungsinterval	beliebig	beliebig	beliebig
SNTP-Broadcasts akzeptieren	nein	nein	nein
Server-Status	an	an	an
Anycast-Zieladresse	224.0.1.1	224.0.1.1	224.0.1.1
VLAN-ID	1	1	1
Anycast-Sendeintervall	30	30	30

Tab. 11: Einstellungen für das Beispiel

Im Beispiel erhält das linke Gerät als SNTP-Client über SNTP die Uhrzeit vom NTP-Server. Einer von einem NTP-Server empfangenen Uhrzeit weist das Gerät ein PTP-Clock-Stratum von 2 (PTPv1) bzw. eine Clock Class von 6 (PTPv2) zu. Somit wird das linke Gerät zur Referenzuhr für die PTP-Synchronisation. Bei allen 3 Geräten ist PTP aktiv, was eine präzise Zeitsynchronisation unter ihnen ermöglicht. Da im Beispiel die anschließbaren Engeräte ausschließlich SNTP unterstützen, dienen alle 3 Geräte als SNTP-Server.

8 Netzlaststeuerung

Zur Optimierung der Datenübertragung bietet Ihnen das Gerät folgende Funktionen, um die Netzauslastung zu steuern:

- Einstellungen zur gezielten Paketvermittlung (MAC-Adressfilter)
- Multicast-Einstellungen
- Lastbegrenzung
- Priorisierung - QoS
- Flusskontrolle
- Virtuelle LANs (VLANs)

8.1 Gezielte Paketvermittlung

Durch gezielte Paketvermittlung hilft Ihnen das Gerät, Sie vor unnötiger Netzbelastung zu bewahren. Folgende Funktionen bietet Ihnen das Gerät zur gezielten Paketvermittlung:

- Store and Forward
- Multiadress-Fähigkeit
- Altern gelernter Adressen
- Statische Adresseinträge
- Ausschalten der gezielten Paketvermittlung

8.1.1 Store and Forward

Das Gerät speichert die erhaltenen Daten und prüft ihre Gültigkeit. Ungültige und fehlerhafte Datenpakete (> 1.536 Bytes oder CRC-Fehler) sowie Fragmente (> 64 Byte) verwirft das Gerät. Gültige Datenpakete leitet das Gerät anschließend weiter.

8.1.2 Multiadress-Fähigkeit

Das Gerät lernt alle Quelladressen je Port. Nur Pakete mit

- unbekannten Ziel-Adressen
- diesen Ziel-Adressen oder
- einer Multi-/Broadcast-Ziel-Adresse

im Zieladressfeld werden an diesen Port gesendet. Gelernte Quelladressen trägt das Gerät in seine Filtertabelle ein (siehe auf Seite 158 „Statische Adresseinträge eingeben“).
Das Gerät kann bis zu 8.000 Adressen lernen. Dies wird notwendig, wenn an einem oder mehreren Ports mehr als ein Endgerät angeschlossen ist. So können mehrere eigenständige Subnetze an das Gerät angeschlossen werden.

8.1.3 Aging gelernter MAC-Adressen

Das Gerät überwacht das Alter der gelernten Adressen. Adresseinträge, die ein bestimmtes Alter, die Aging Time, überschreiten, löscht das Gerät aus seiner Adresstabelle.
Datenpakete mit einer unbekannten Zieladresse flutet das Gerät.
Datenpakete mit bekannter Zieladresse vermittelt das Gerät gezielt.

Anmerkung: Ein Neustart löscht die gelernten Adresseinträge.

- ☐ Wählen Sie den Dialog `Switching:Global`.
- ☐ Geben Sie die Aging Time für alle dynamischen Einträge im Bereich von 10 bis 630 Sekunden (Einheit: 1 Sekunde, Voreinstellung: 30). Im Zusammenhang mit der Router-Redundanz wählen Sie die Zeit ≥ 30 Sekunden.

8.1.4 Statische Adresseinträge eingeben

Eine wichtige Funktion des Gerätes ist unter anderem die Filterfunktion. Sie selektiert Datenpakete nach definierten Mustern, den Filtern. Diesen Mustern sind Vermittlungsvorschriften zugeordnet. Das heißt, ein Datenpaket, das ein Gerät an einem Port empfängt, wird mit den Mustern verglichen. Besteht ein Muster, mit dem das Datenpaket übereinstimmt, dann sendet oder blockiert ein Gerät dieses Datenpaket entsprechend den Vermittlungsvorschriften an den betroffenen Ports.

Als Filterkriterium können gelten:

- Zieladresse (Destination Address),
- Broadcast-Adresse,
- Gruppenadresse (Multicast),
- VLAN-Zugehörigkeit.

Zur Speicherung der einzelnen Filter dient die Filtertabelle (Forwarding Database, FDB). Sie enthält 3 Teile: einen statischen und zwei dynamische Teile.

- Der Management-Administrator beschreibt den statischen Teil der Filtertabelle (`dot1qStaticTable`).
- Das Gerät besitzt die Fähigkeit, während des Betriebes zu lernen, an welchem Port es Datenpakete mit welchen Quelladressen empfängt (siehe auf Seite 156 „Multiadress-Fähigkeit“). Diese Information wird in einen dynamischen Teil (`dot1qTpFdbTable`) geschrieben.
- Von Nachbar-Agenten dynamisch gelernte und die per GMRP gelernten Adressen werden in den anderen dynamischen Teil geschrieben.

Adressen, die schon in der statischen Filtertabelle stehen, übernimmt das Gerät automatisch in den dynamischen Teil.
Eine statisch eingetragene Adresse kann nicht durch Lernen überschrieben werden.

Anmerkung: Bei aktivem Ring-Manager sind keine permanenten Unicast-Einträge möglich.

Anmerkung: Die Filtertabelle bietet Ihnen für Multicast-Adressen die Möglichkeit, bis zu 100 Filter-Einträge zu erzeugen.

☐ Wählen Sie den Dialog `Switching:Filter für MAC-Adressen`.

Jede Zeile der Filtertabelle stellt einen Filter dar. Filter legen die Vermittlungsweise von Datenpaketen fest. Sie werden entweder automatisch vom Gerät (Status learned) oder manuell angelegt. Datenpakete, deren Zieladresse in der Tabelle eingetragen ist, werden vom Empfangsport an die in der Tabelle markierten Ports vermittelt. Datenpakete, deren Zieladresse nicht in der Tabelle enthalten ist, werden vom Empfangsport an alle anderen Ports vermittelt. Im Dialog „Filter anlegen“ (siehe Bedientaste unten) haben Sie die Möglichkeit, neue Filter zu erzeugen. Folgende Zustände sind möglich:

- `learned`: Das Filter wurde vom Gerät automatisch angelegt.
- `permanent`: Das Filter wird im Gerät oder auf dem URL dauerhaft gespeichert (siehe auf Seite 65 „Einstellungen speichern“).
- `invalid`: Mit diesem Status löschen Sie ein manuell angelegtes Filter.
- `gmrp`: Das Filter wurde durch GMRP angelegt.
- `gmrp/permanent`: GMRP hat dem Filter, nachdem es durch den Administrator angelegt worden ist, weitere Portmarken hinzugefügt. Die durch das GMRP hinzugefügten Portmarken werden bei einem Neustart gelöscht.
- `igmp`: Das Filter wurde durch IGMP-Snooping angelegt.

Um Einträge mit dem Status „learned“ aus der Filtertabelle zu löschen, wählen Sie den Dialog `Grundeinstellungen:Neustart` und klicken Sie auf „MAC-Adresstabelle zurücksetzen“.

8.1.5 Gezielte Paketvermittlung ausschalten

Um die Daten aller Ports beobachten zu können, bietet Ihnen das Gerät die Möglichkeit, das Lernen der Adressen auszuschalten. Ist das Lernen der Adressen ausgeschaltet, dann überträgt das Gerät alle Daten von allen Ports an alle Ports.

☐ Wählen Sie den Dialog `Switching:Switching Global`.
Heben Sie die Markierung „Adressen lernen“ auf, um die Daten aller Ports beobachten zu können.

8.2 Multicast-Anwendung

8.2.1 Beschreibung Multicast-Anwendung

Die Datenverteilung im LAN unterscheidet 3 Verteilungsklassen bezüglich der adressierten Empfänger:

- Unicast - ein Empfänger,
- Multicast - eine Gruppe von Empfängern,
- Broadcast - jeder erreichbare Empfänger.

Im Falle der Multicast-Adressierung leitet das Gerät alle Datenpakete mit einer Multicast-Adresse an allen Ports weiter. Dies führt zu einem erhöhten Bandbreitenbedarf.
Protokolle wie das GMRP und Verfahren wie IGMP-Snooping ermöglichen dem Gerät einen Informationsaustausch über die gezielte Vermittlung von Multicast-Datenpaketen. Das Vermitteln der Multicast-Datenpakete ausschließlich an den Ports, an denen Empfänger dieser Multicast-Datenpakete angeschlossenen sind, begrenzt den benötigten Bandbreitenbedarf.

IGMP-Multicast-Adressen erkennen Sie an dem Bereich, in dem eine Adresse liegt:

- MAC-Multicast-Adresse
  01:00:5E:00:00:00 - 01:00:5E:FF:FF:FF
  (in Masken-Schreibweise 01:00:5E:00:00:00/24)
- Klasse D IP-Multicast-Adresse
  224.0.0.0 - 239.255.255.255
  (in Masken-Schreibweise 224.0.0.0/4)

8.2.2 Beispiel für eine Multicast-Anwendung

Die Kameras zur Maschinenüberwachung übertragen in der Regel ihre Bilder auf Monitore im Maschinenraum und in einen Überwachungsraum. Bei einer IP-Übertragung sendet eine Kamera ihre Bilddaten mit einer Multicast-Adresse über das Netz.
Damit die vielen Videodaten nicht unnötig das ganze Netz belasten, benutzt das Gerät das GMRP zur Verteilung der Multicast-Adress-Information. Dies hat zur Folge, dass die Bilddaten mit einer Multicast-Adresse nur noch an jenen Ports vermittelt werden, an denen die zugehörigen Monitore zur Überwachung angeschlossen sind.

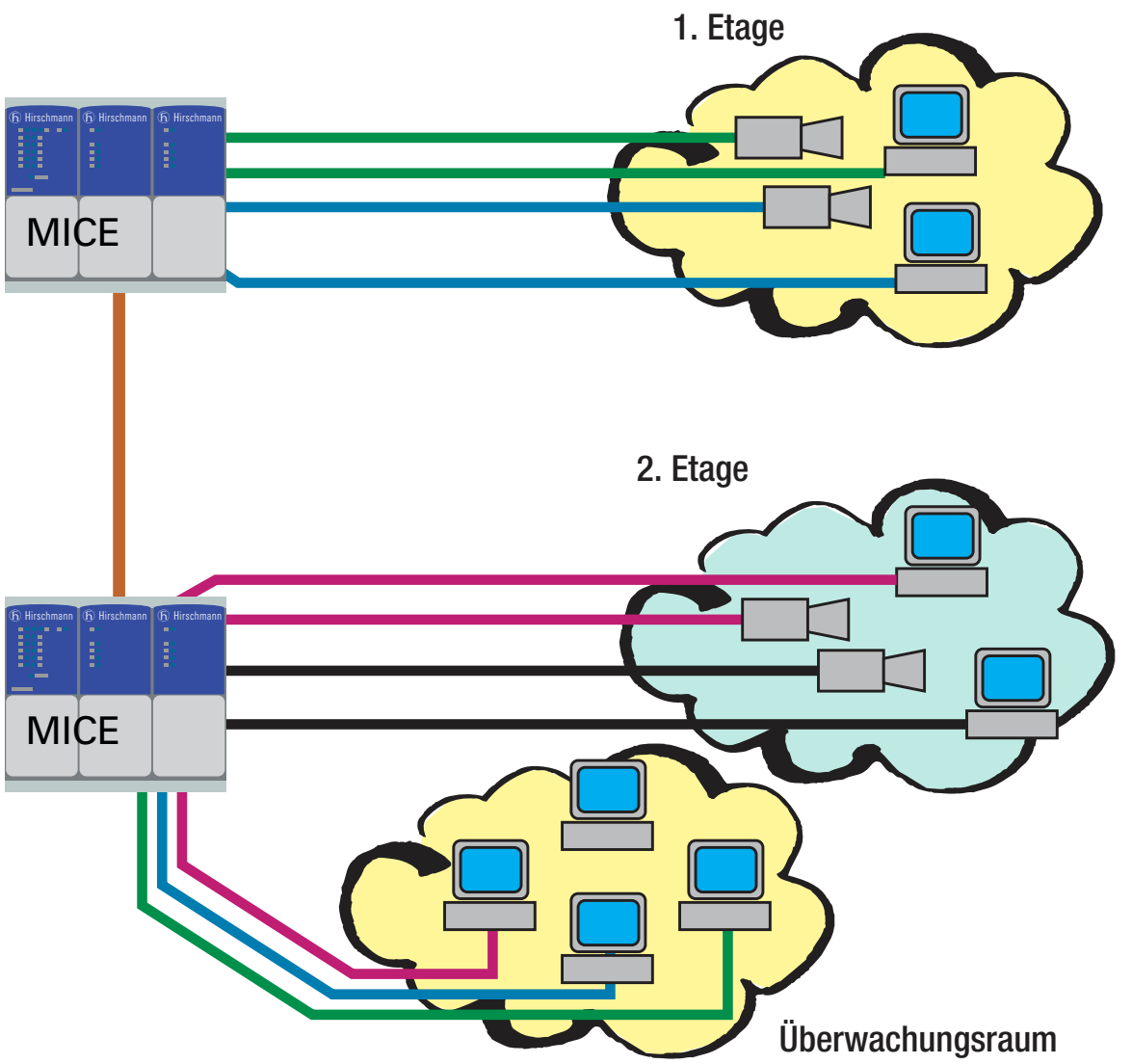


Abb. 30: Beispiel: Video-Überwachung in Maschinenräumen

8.2.3 Beschreibung IGMP-Snooping

Das Internet Group Management Protocol (IGMP) beschreibt die Verteilung von Multicast-Informationen zwischen Routern und Endgeräten auf Layer 3.

Router mit aktiver IGMP-Funktion verschicken periodisch Anfragen (Query), um zu erfahren, welche IP-Multicast-Gruppen-Mitglieder im LAN angeschlossen sind. Multicast-Gruppen-Mitglieder antworten mit einer Report-Nachricht. Diese Report-Nachricht enthält alle für das IGMP notwendigen Parameter. Der Router trägt die IP-Multicast-Group-Adresse aus der Report-Nachricht in seine Routing-Tabelle ein. Dies bewirkt, dass er Frames mit dieser IP-Multicast-Group-Adresse im Zieladressfeld ausschließlich gemäß der Routing-Tabelle vermittelt.

Geräte, die nicht mehr Mitglied einer Multicast-Gruppe sein wollen, melden sich mit einer Leave-Nachricht ab (ab IGMP-Version 2) und versenden keine Report-Nachrichten mehr. Im IGMP-Version 1 und 2 entfernt der Router den Routing-Tabelleneintrag, wenn er innerhalb einer bestimmten Zeit (Aging Time) keine Report-Nachricht empfängt.

Sind mehrere Router mit aktiver IGMP-Funktion im Netz, dann verhandeln diese bei IGMP Version 2 untereinander, welcher Router die Query-Funktion übernimmt. Ist kein Router im Netz, dann kann ein entsprechend ausgestatteter Switch die Query-Funktion übernehmen.

Ein Switch, der einen Multicast-Empfänger mit einem Router verbindet, kann mit Hilfe des IGMP-Snooping-Verfahrens die IGMP-Informationen auswerten.

IGMP-Snooping übersetzt IP-Multicast-Group-Adressen in MAC-Multicast-Adressen, so dass die IGMP-Funktion auch von Layer 2-Switches wahrgenommen werden können. Der Switch trägt die vom IGMP-Snooping aus den IP-Adressen gewonnenen MAC-Adressen der Multicast-Empfänger in die statische Adresstabelle ein. Dadurch vermittelt der Switch diese Multicast-Pakete ausschließlich an Ports, an denen Multicast-Empfänger angeschlossen sind. Die anderen Ports bleiben von diesen Paketen unbelastet.

Als Besonderheit bietet Ihnen das Gerät die Möglichkeit, zu bestimmen, ob es Datenpakete mit nicht registrierten Multicast-Adressen verwirft, an alle Ports vermittelt, oder nur an Ports, an denen das Gerät Query-Pakete empfangen hat. Sie haben außerdem die Möglichkeit, bekannte Multicast-Pakete zusätzlich an Query-Ports zu senden.

Lieferzustand: „Aus“.

8.2.4 IGMP-Snooping einstellen

☐ Wählen Sie den Dialog `Switching:Multicast:IGMP`.

Funktion

Der Rahmen „Funktion“ bietet Ihnen die Möglichkeit, IGMP Snooping für das gesamte Gerät global an-oder auszuschalten.
Ist IGMP Snooping ausgeschaltet, dann:

- wertet das Gerät empfangene Query- und Report-Pakete nicht aus und
- sendet (flutet) empfangene Datenpakete mit einer Multicast-Adresse als Zieladresse an allen Ports.

Einstellungen für IGMP-Querier und IGMP

Diese Rahmen bieten Ihnen die Möglichkeit, globale Einstellungen für die IGMP- und die IGMP-Querier-Funktion vorzunehmen.
Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.

IGMP-Querier

„IGMP Querier aktiv“ bietet Ihnen die Möglichkeit, die Query-Funktion ein-/auszuschalten.

„Protokoll-Version“ bietet Ihnen die Möglichkeit, die IGMP-Version 1, 2 oder 3 auszuwählen.

In „Sende-Intervall [s]“ geben Sie den Zeitabstand an, in welchem der Switch Query-Pakete verschickt (gültige Werte: 2-3.599 s, Lieferzustand: 125 s).

Beachten Sie den Parameter-Zusammenhang zwischen Max. Response-Time, Sende-Intervall und Group-Membership-Intervall (siehe auf Seite 166 „Werte der Parameter“).

IGMP-fähigen Endgeräte antworten auf einen Query mit einer Report-Nachricht und erzeugen damit Netzlast.
Wählen Sie große Sende-Intervalle, wenn Sie Ihr Netz entlasten wollen und die sich daraus ergebenden längeren Umschaltzeiten akzeptieren können.
Wählen Sie kleine Sende-Intervalle, wenn Sie kurze Umschaltzeiten benötigen und die sich daraus ergebende Netzlast akzeptieren können.

IGMP-Einstellungen

„Aktuelle Querier IP-Adresse“ zeigt Ihnen die IP-Adresse des Gerätes an, das die Query-Funktion innehat.

In „Max. Response-Time“ geben Sie die Zeit ein, innerhalb derer die Multicast-Gruppen-Mitglieder auf einen Query antworten (gültige Werte: 1-3.598 s, Lieferzustand: 10 s).

Beachten Sie den Parameter-Zusammenhang zwischen Max. Response-Time, Sende-Intervall und Group-Membership-Intervall (siehe auf Seite 166 „Werte der Parameter“).

Die Multicast-Gruppen-Mitglieder wählen einen zufälligen Wert innerhalb der maximalen Response-Time für ihre Antwort aus, um zu verhindern, dass alle Multicast-Gruppen-Mitglieder gleichzeitig auf den Query antworten.
Wählen Sie einen großen Wert, wenn Sie Ihr Netz entlasten wollen und die sich daraus ergebenden längeren Umschaltzeiten akzeptieren können.
Wählen Sie einen kleinen Wert, wenn Sie kurze Umschaltzeiten benötigen und die sich daraus ergebende Netzlast akzeptieren können.

In „Group-Membership-Intervall“ geben Sie die Zeit ein, für die eine dynamische Multicast-Gruppe im Gerät eingetragen bleibt, wenn es keine Report-Nachrichten empfängt (gültige Werte: 3-3.600 s, Lieferzustand: 260 s).

Beachten Sie den Parameter-Zusammenhang zwischen Max. Response-Time, Sende-Intervall und Group-Membership-Intervall (siehe auf Seite 166 „Werte der Parameter“).

Werte der Parameter

Die Parameter
– Max. Response-Time,
– Sende-Intervall und
– Group-Membership-Intervall
stehen in Beziehung zueinander:

Max. Response-Time < Sende-Intervall < Group-Membership-Intervall.

Wenn Sie Werte eingeben, die dieser Beziehung widersprechen, dann ersetzt das Gerät diese Werte durch eine Voreinstellung oder die zuletzt gültigen Werte.

Parameter	Protokoll Version	Wertebereich	Voreinstellung
Max. Response-Time	1, 2 3	1-25 Sekunden 1-3.598 Sekunden	10 Sekunden
Sende-Intervall	1, 2, 3	2-3.599 Sekunden	125 Sekunden
Group-Membership-Intervall	1, 2, 3	3-3.600 Sekunden	260 Sekunden

Tab. 12: Wertebereich für Max. Response-Time, Sende-Intervall und Group-Membership-Intervall

Multicasts

Diese Rahmen bieten Ihnen die Möglichkeit, globale Einstellungen für die Multicastfunktionen vorzunehmen.
Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.

Unbekannte Multicasts
In diesem Rahmen bestimmen Sie, wie das Gerät im IGMP-Modus Pakete mit bekannten und unbekannten - nicht mit IGMP-Snooping gelernten - MAC/IP-Multicast-Adressen vermittelt.

„Unbekannte Multicasts“ bietet Ihnen die Möglichkeit, zu bestimmen, wie das Gerät unbekannte MC-Pakete vermittelt:

- „An Query Ports senden".
  Das Gerät sendet die Pakete mit unbekannter MAC/IP-Multicast-Adresse an alle Query-Ports.
- „An alle Ports senden".
  Das Gerät sendet die Pakete mit unbekannter MAC/IP-Multicast-Adresse an alle Ports
- „Verwerfen".
  Das Gerät verwirft alle Pakete mit unbekannter MAC/IP-Multicast-Adresse.

Anmerkung: Die Behandlung von ungelernten Multicast-Adressen gilt auch für die reservierten IP-Adressen aus dem „Local Network Control Block" (224.0.0.0 - 224.0.0.255). Dies kann z.B. Auswirkungen auf übergeordnete Routing-Protokolle haben.

Bekannte Multicasts
In diesem Rahmen bestimmen Sie, wie das Gerät im IGMP-Modus Pakete mit bekannten - mit IGMP-Snooping gelernten - MAC/IP-Multicast-Adressen vermittelt.

- „An Query- und registrierte Ports senden".
  Das Gerät sendet die Pakete mit bekannter MAC/IP-Multicast-Adresse an alle Query-Ports und an registrierte Ports.
  Diese standardkonforme Einstellung sendet alle Multicasts an allen Query-Ports und an registrierte Ports. Sie hat den Vorteil, dass sie in den meisten Anwendungen ohne weitere Konfiguration funktioniert.
  Anwendung: „Flood and Prune”-Routing bei PIM-DM.
- „An registrierte Ports senden".
  Das Gerät sendet die Pakete mit bekannter MAC/IP-Multicast-Adresse an registrierte Ports.
  Diese vom Standard abweichende Einstellung hat den Vorteil, die verfügbare Bandbreite durch gezielte Vermittlung optimal zu nutzen. Sie erfordert zusätzliche Porteinstellungen.
  Anwendung: Routing-Protokoll PIM-SM.

Einstellungen pro Port (Tabelle)

- „IGMP an“
  Diese Tabellenspalte bietet Ihnen die Möglichkeit, bei eingeschaltetem globalem IGMP-Snooping das IGMP je Port ein-/auszuschalten. Registrierungen für diesen Port erfolgen nicht, wenn IGMP abgeschaltet ist.

- „IGMP Forward all“
  Diese Tabellenspalte bietet Ihnen die Möglichkeit, bei eingeschaltetem globalem IGMP Snooping die IGMP Snooping-Funktion „Forward All" ein-/auszuschalten. Mit der Einstellung „Forward All" vermittelt das Gerät an diesem Port alle Datenpakete mit einer Multicast-Adresse im Zieladressfeld.

  Anmerkung: Sind mehrere Router an ein Subnetz angeschlossen, dann verwenden Sie IGMP-Version 1, damit alle Router alle IGMP-Reports erhalten.

  Anmerkung: Wenn Sie IGMP-Version 1 in einem Subnetz verwenden, dann verwenden Sie IGMP-Version 1 auch im gesamten Netz.

- „IGMP Automatic Query Port“
  Diese Tabellenspalte zeigt Ihnen, welche Ports das Gerät als Query-Ports gelernt hat, wenn in „Statischer Query Port“ „automatic“ gewählt ist.

- „Statischer Query Port“
  IGMP-Report-Nachrichten vermittelt das Gerät an die Ports, an denen es IGMP-Anfragen empfängt (disable=Lieferzustand).
  Diese Tabellenspalte bietet Ihnen die Möglichkeit, IGMP-Report-Nachrichten auch an:
  anderen ausgewählten Ports (enable) oder
  angeschlossene Hirschmann-Geräte (automatic) zu vermitteln .

- „Gelernter Query Port“
  Diese Tabellenspalte zeigt Ihnen, an welchen Ports das Gerät IGMP-Anfragen empfangen hat, wenn in „Statischer Query Port“ „disable“ gewählt ist.

Anmerkung: Ist das Gerät in einen HIPER-Ring eingebunden, dann erreichen Sie für Datenpakete mit registrierten Multicast-Zieladressen eine schnelle Rekonfiguration des Netzes nach einer Ringumschaltung durch die folgenden Einstellungen:

- Schalten Sie IGMP-Snooping an den Ringports und global ein; und
- schalten Sie „IGMP Forward All“ pro Port an den Ringports ein.

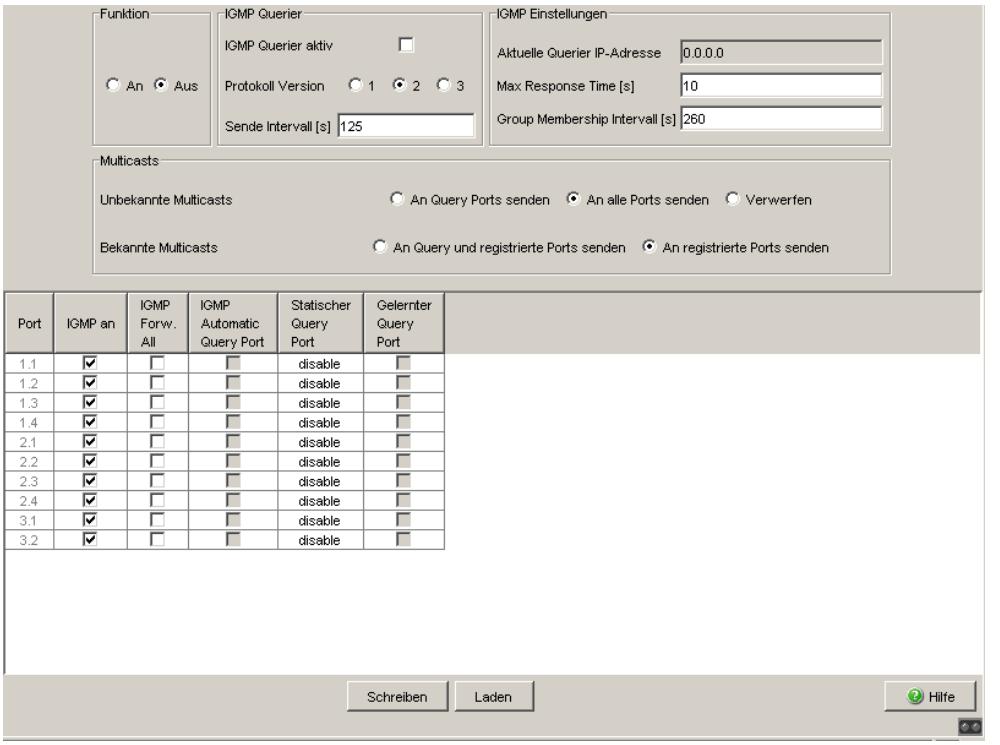


Abb. 31: Dialog IGMP-Snooping

8.2.5 Beschreibung von GMRP

Das GARP Multicast Registration Protocol (GMRP) beschreibt die Verteilung von Datenpaketen mit einer Multicast-Adresse als Zieladresse auf Ebene 2.

Geräte, die Datenpakete mit einer Multicast-Adresse als Zieladresse empfangen wollen, veranlassen mit Hilfe des GMRPs die Registrierung der Multicast-Adresse. Registrieren heißt für einen Switch, die Multicast-Adresse in die Filtertabelle einzutragen. Beim Eintrag einer Multicast-Adresse in die Filtertabelle, sendet der Switch diese Information in einem GMRP-Paket an die Ports. Infolgedessen leiten die angeschlossenen Switches die Multicast-Adresse, die sich in der Filtertabelle befindet, an diesen Switch weiter. Das GMRP vermittelt Pakete mit einer Multicast-Adresse im Zieladressfeld an die eingetragenen Ports.

Diese Funktion ist auf den Geräten MS, RS, MACH102, MACH1020/30, Octopus, RSR und MACH1040, MACH104 verfügbar. In Abhängigkeit von der Konfiguration verwirft der Switch entweder unbekannte Multicast-Addressen oder leitet die Datenpakete mit unbekannten Multicast-Addressen an alle Ports weiter.

Voreinstellung: „Aus“.

8.2.6 GMRP einstellen

☐ Wählen Sie den Dialog `Switching:Multicasts:GMRP`.

Funktion

Der Rahmen „Funktion“ bietet Ihnen die Möglichkeit, GMRP für das gesamte Gerät global einzuschalten.

Ist GMRP ausgeschaltet, dann

- generiert das Gerät keine GMRP-Pakete,
- wertet empfangene GMRP-Pakete nicht aus und
- sendet (flutet) empfangene Datenpakete an allen Ports.

Für empfangene GMRP-Pakete ist das Gerät unabhängig von der GMRP-Einstellung transparent

Multicasts

Der Rahmen „Multicasts“ bietet Ihnen die Möglichkeit, GMRP so zu konfigurieren, dass das Gerät Multicast-Adressen entweder verwirft oder an alle Ports weiterleitet.

Schalten Sie GMRP ein, dann

- Einstellung „Verwerfen“: löscht das Gerät unbekannte Multicasts.
- Einstellung „An alle Ports senden“: wertet das Gerät die empfangenen Datenpakete aus und sendet (flutet) empfangene Datenpakete an alle Ports.

Einstellungen pro Port (Tabelle)

- „GMRP“
  Diese Tabellenspalte bietet Ihnen die Möglichkeit, bei global eingeschaltetem GMRP das GMRP je Port ein-/auszuschalten. Das Ausschalten des GMRPs an einem Port verhindert Registrierungen für diesen Port und das Weiterleiten von GMRP-Paketen an diesem Port.

- „GMRP Service Requirement“
  Geräte, die das GMRP nicht unterstützen, können in die Multicast-Adressierung mit eingebunden werden durch
  - einen statischen Filteradress-Eintrag am Anschluss-Port.
  - Auswählen von „Forward all groups“ in der Tabellenspalte „GMRP Service Requirement“. Ports mit der Auswahl „Forward all groups“ trägt das Gerät in alle Multicast-Filtereinträge ein, die über GMRP gelernt wurden.

Anmerkung: Ist das Gerät in einen HIPER-Ring eingebunden, dann erreichen Sie für Datenpakete mit registrierten Multicast-Zieladressen eine schnelle Rekonfiguration des Netzes nach einer Ringumschaltung durch die folgende Einstellungen:
- Schalten Sie GMRP an den Ringports und global ein; und
- schalten Sie „Forward all groups“ an den Ringports ein.

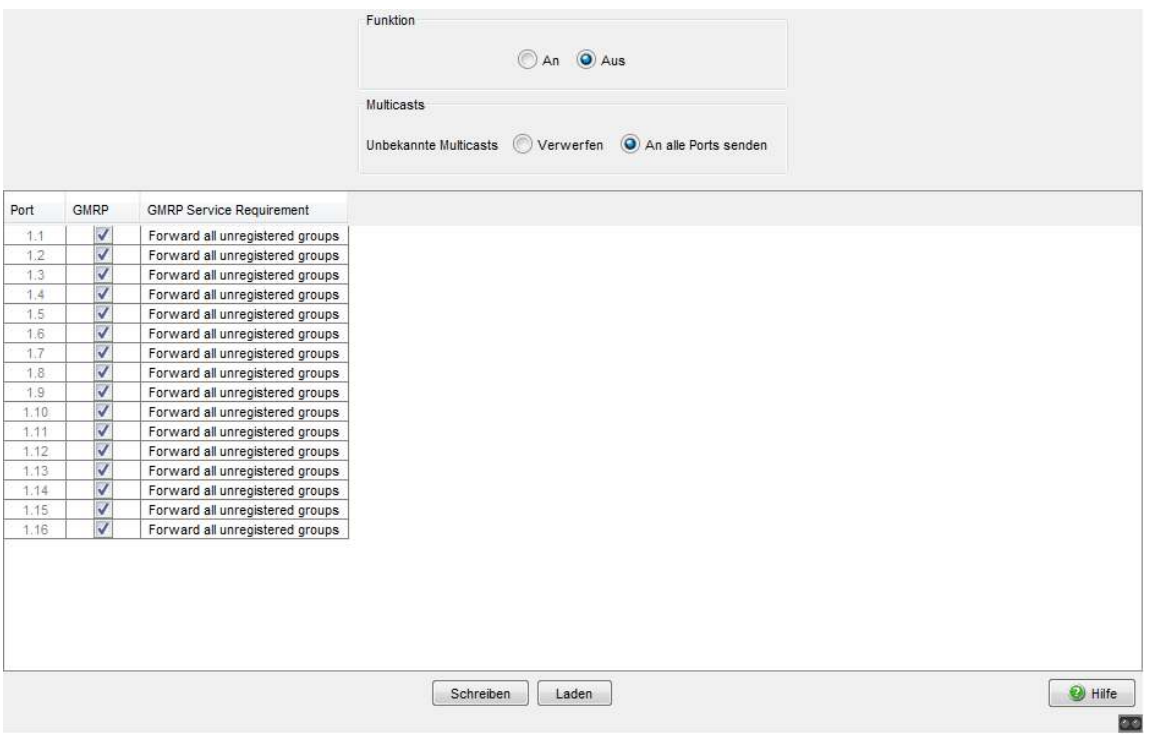


Abb. 32: Dialog GMRP

8.3 Lastbegrenzer

8.3.1 Beschreibung Lastbegrenzer

Um bei hohem Verkehrsaufkommen einen zuverlässigen Betrieb zu gewährleisten, bieten Ihnen das Gerät die Möglichkeit, die Rate des Verkehrs an den Ports zu begrenzen.

Die Eingabe einer Begrenzungsrate je Port legt fest, welchen maximalen Verkehr das Gerät ausgangs- und eingangsseitig vermittelt.

Überschreitet der Verkehr an diesem Port die eingegebene maximale Rate, dann verwirft das Gerät die Überlast an diesem Port.

Eine globale Einstellung aktiviert/deaktiviert die Lastbegrenzer-Funktion an allen Ports.

Anmerkung: Die Begrenzerfunktionen arbeiten ausschließlich auf Layer 2 und dienen dem Zweck, Stürme von Frame-Typen, die der Switch flutet (typischerweise Broadcasts), in ihrer Auswirkung zu begrenzen. Die Begrenzerfunktion übergeht dabei Protokollinformationen höherer Schichten wie IP oder TCP. Dies kann sich z.B. auf TCP-Verkehr auswirken.

Um diese Auswirkungen zu minimieren, nutzen Sie die folgenden Möglichkeiten:

- die Begrenzungsfunktion auf bestimmte Frame-Typen einschränken (z.B. auf Broadcasts, Multicasts und Unicasts mit nicht gelernter Zieladresse) und Unicasts mit bekannter Zieladresse von der Begrenzung ausnehmen,
- die Ausgangsbegrenzerfunktion statt der Eingangsbegrenzerfunktion verwenden, da die erstere durch die Switch-interne Pufferung der Frames etwas besser mit der TCP-Flusssteuerung zusammenarbeitet.
- die Aging-Zeit für gelernte Unicast-Adressen erhöhen.

8.3.2 Lastbegrenzer-Einstellungen

☐ Wählen Sie den Dialog `Switching:Lastbegrenzer`.

- „Eingangsbegrenzer (kbit/s)“ bietet Ihnen die Möglichkeit, die Eingangsbegrenzerfunktion für alle Ports ein-/auszuschalten und die Eingangsbegrenzung für Broadcast-Pakete oder für Broadcast- und Multicast-Pakete an allen Ports zu wählen.
- „Ausgangsbegrenzer (Pkt/s)“ bietet Ihnen die Möglichkeit, die Ausgangs-Broadcastbegrenzung an allen Ports ein/auszuschalten.

Einstellmöglichkeiten pro Port:

- Eingangsbegrenzerrate für den im Eingangsbegrenzerrahmen gewählten Pakettyp:
  - = 0, keine Begrenzung eingangsseitig an diesem Port.
  - > 0, maximale Übertragungsrate in kbit/s, die eingangsseitig an diesem Port empfangen werden darf.
- Ausgangsbegrenzerrate für Broadcast-Pakete:
  - = 0, keine Begrenzung der Broadcasts ausgangsseitig an diesem Port.
  - > 0, maximale Anzahl der Broadcasts, die pro Sekunde ausgangsseitig an diesem Port gesendet werden.

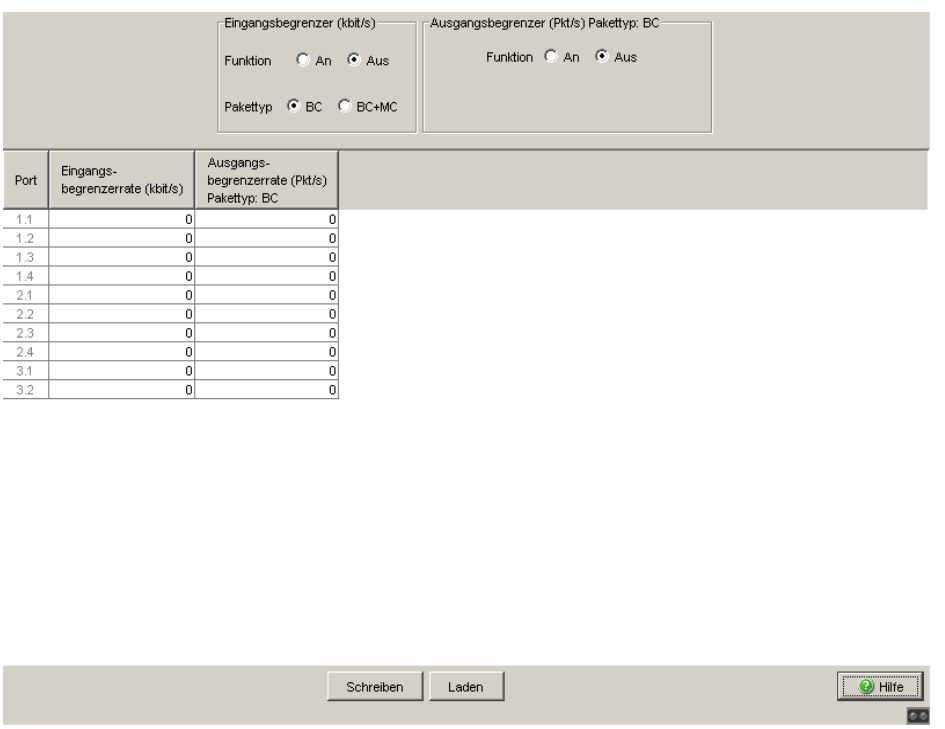


Abb. 33: Dialog Lastbegrenzer

8.4 QoS/Priorität

8.4.1 Beschreibung Priorisierung

Diese Funktion hilft zu verhindern, dass zeitkritischer Datenverkehr wie Sprach-/Video- oder Echtzeitdaten in Zeiten starker Verkehrslast durch weniger zeitkritischen Datenverkehr gestört wird. Die Zuweisung von hohen Verkehrsklassen (Traffic Class) für zeitkritische Daten und niedrigen Verkehrsklassen für weniger zeitkritische Daten bietet einen optimierten Datenfluss für zeitkritische Datenverkehr.

Das Gerät unterstützt 8 Priority Queues (Traffic Classes nach IEEE 802.1D). Die Zuordnung von empfangenen Datenpaketen zu diesen Klassen erfolgt durch

- Access-Control-Listen, MAC- oder IP-basierte ACLs (siehe auf Seite 116 „Zugriffs-Kontroll-Listen (ACL)“).
- die im VLAN-Tag enthaltene Priorität des Datenpaketes, wenn der Empfangsport auf „trust dot1p“ konfiguriert wurde.
- die im IP-Header enthaltene QoS-Information (ToS/DiffServ), wenn der Empfangsport auf „trust ip-dscp“ konfiguriert wurde.
- die Port-Priorität, wenn der Port auf „untrusted" konfiguriert wurde.
- die Port-Priorität beim Empfang von Nicht-IP-Paketen, wenn der Port auf „trust ip-dscp” konfiguriert wurde.
- die Port-Priorität beim Empfang von Datenpaketen, die kein VLAN-Tag enthalten (siehe auf Seite 85 „Ports konfigurieren“) und wenn der Port auf „trust dot1p" konfiguriert wurde.
  Voreinstellung: „trust dot1p“.

Das Gerät berücksichtigt die Klassifizierungsmechanismen in der oben dargestellten Reihenfolge. D.h. Access-Control-Listen haben immer Vorrang vor den folgenden Mechanismen. Access-Control-Listen können die Datenpakete bezüglich Layer 2, Layer 3 und Layer 4 klassifizieren (z.B. MAC-Adressen, IP-Adressen, Protokolle, TCP/UDP-Ports).

Datenpakete können Priorisierungs/QoS-Informationen enthalten:

- VLAN-Priorität nach IEEE 802.1Q/ 802.1D (Layer 2)
- Type-of-Service (ToS) bzw. DiffServ (DSCP) bei IP-Paketen (Layer 3)

8.4.2 VLAN-Tagging

Für die Funktionen VLAN und Priorisierung sieht der Standard IEEE 802.1Q vor, dass in einen MAC-Datenrahmen das VLAN-Tag eingebunden wird. Das VLAN-Tag besteht aus 4 Bytes. Es steht zwischen dem Quelladressfeld und dem Typfeld.

Das Gerät wertet bei Datenpaketen mit VLAN-Tag aus:
- die Prioritäts-Information und
- die VLAN-Information, wenn VLANs eingerichtet sind.

Datenpakete, deren VLAN-Tags eine Prioritäts-Information, aber keine VLAN-Information (VLAN-ID = 0) enthält, heißen „Priority Tagged Frames“.

Eingetragene Priorität	Traffic Class (Voreinstellung)	IEEE 802.1D-Verkehrstyp
0	2	Best Effort (default)
1	0	Background
2	1	Standard
3	3	Excellent Effort (business critical)

Tab. 13: Zuordnung der im Tag eingetragenen Priorität zu den Traffic Classes

Eingetragene Priorität	Traffic Class (Voreinstellung)	IEEE 802.1D-Verkehrstyp
4	4	Controlled Load (Streaming multimedia)
5	5	Video, less than 100 millisconds of latency and jitter
6	6	Voice; less than 10 milliseconds of latency and jitter
7	7	Network Control reserved traffic

Tab. 13: Zuordnung der im Tag eingetragenen Priorität zu den Traffic Classes

Anmerkung: Netzprotokolle und Redundanzmechanismen nutzen die höchste Traffic Class 7. Wählen Sie deshalb andere Traffic Classes für Anwendungsdaten.

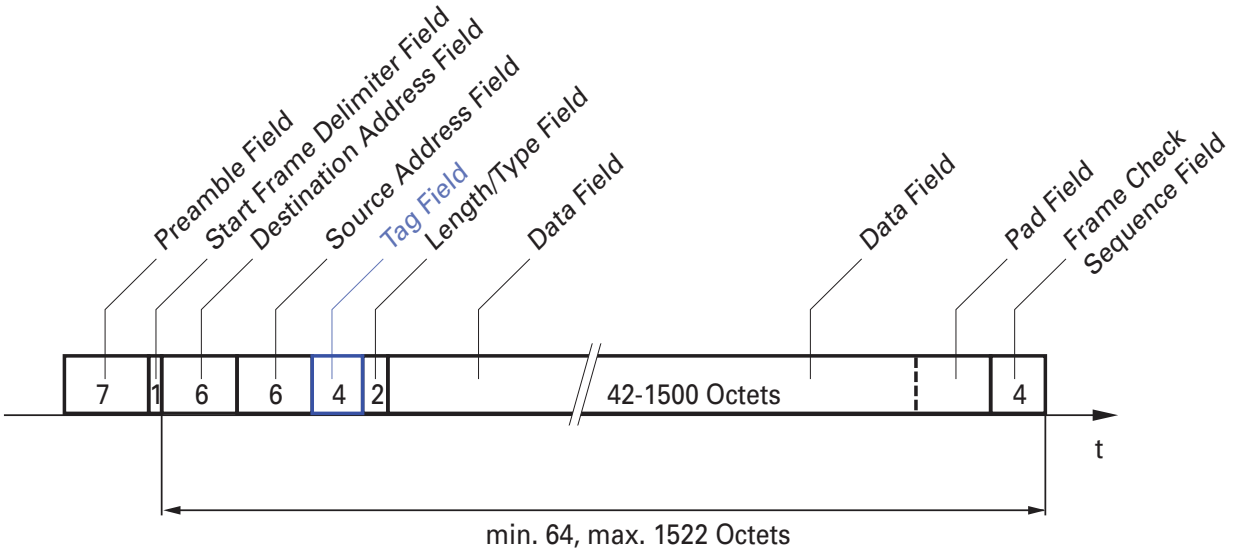


Abb. 34: Ethernet-Datenpaket mit Tag

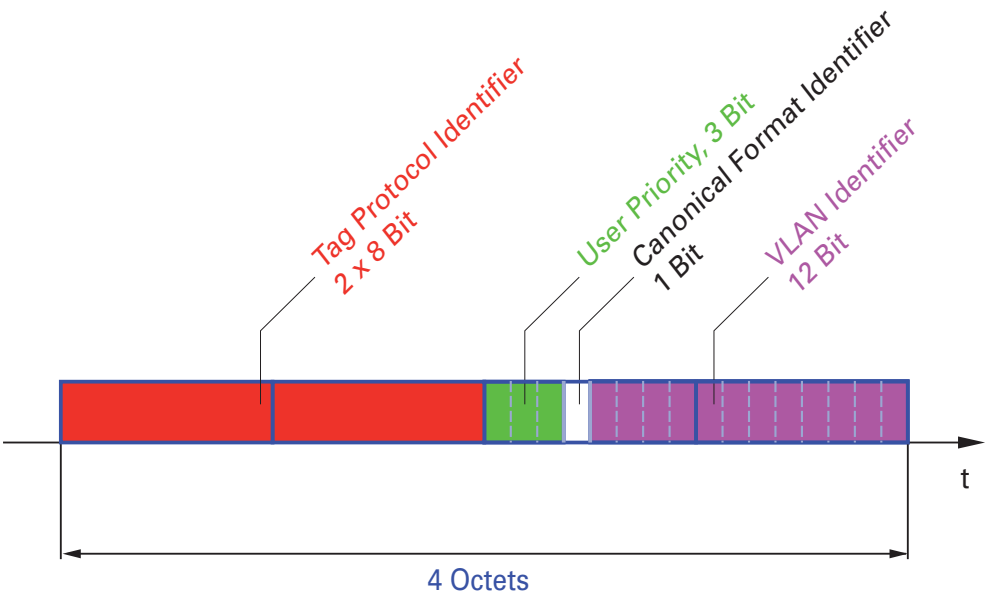


Abb. 35: Tag-Format

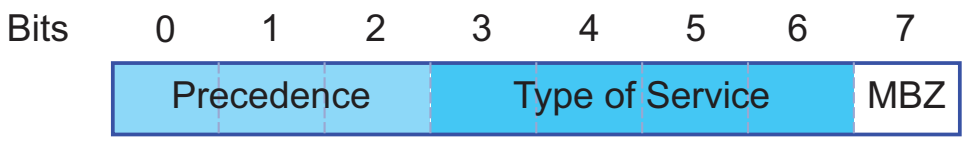
Beim Einsatz der VLAN-Priorisierung beachten Sie folgende Besonderheiten:

- Eine Ende-zu-Ende Priorisierung setzt das Übertragen der VLAN-Tags im gesamten Netz voraus, d.h. alle Netzkomponenten müssen VLAN-fähig sein.
- Router können über portbasierte Router-Interfaces keine Pakete mit VLAN-Tags empfangen bzw. senden.

8.4.3 IP ToS / DiffServ

TYPE of Service

Das Type of Service-Feld (ToS) im IP-Header (siehe Tabelle 14) ist bereits von Beginn an Bestandteil des IP-Protokolls und war zur Unterscheidung unterschiedlicher Dienstgüten in IP-Netzen vorgesehen. Schon damals machte man sich aufgrund der geringen zur Verfügung stehenden Bandbreiten und der unzuverlässigen Verbindungswege Gedanken um eine differenzierte Behandlung von IP-Paketen. Durch die kontinuierliche Steigerung der zur Verfügung stehenden Bandbreiten bestand keine Notwendigkeit, das ToS-Feld zu nutzen. Erst die Echtzeitanforderungen an heutige Netze rücken das ToS-Feld in den Blickpunkt. Eine Markierung im ToS-Byte des IP-Headers ermöglicht eine Unterscheidung unterschiedlicher Dienstgüten. In der Praxis hat sich die Nutzung dieses Feldes jedoch nicht durchgesetzt.



Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Must be zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immidiate		
001 - Priority		
000 - Routine		

Tab. 14: ToS-Feld im IP-Header

Differentiated Services

Das in RFC 2474 neu definierte Differentiated Services Feld im IP-Header (siehe Abbildung 36) - oft auch als DiffServ-Codepoint oder DSCP bezeichnet, löst das ToS-Feld ab und dient zur Markierung der einzelnen Pakete mit einem DSCP. Hier werden die Pakete in unterschiedliche Qualitäts-Klassen eingeteilt. Die ersten 3 Bits des DSCP dienen der Einteilung in Klassen. Die nachfolgenden 3 Bits dienen der weiteren Unterteilung der Klassen nach unterschiedlichen Kriterien. Im Gegensatz zum ToS-Byte nutzt DiffServ 6 Bit zur Klasseneinteilung. Daraus ergeben sich bis zu 64 unterschiedliche Dienstgüteklassen.

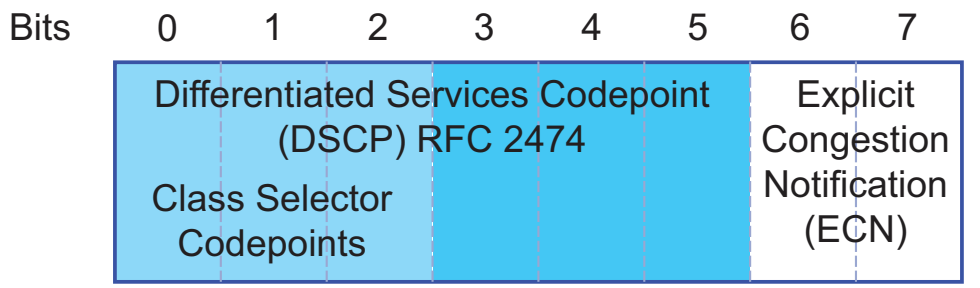


Abb. 36: Differentiated-Services-Feld im IP-Header

Die unterschiedlichen DSCP-Werte bewirken bei dem Gerät ein unterschiedliches Weiterleitungs-Verhalten, das Per-Hop-behavior (PHB). PHB-Klassen:

- Class Selector (CS0-CS7): Aus Kompatibilitätsgründen zu TOS/IP-Precedence
- Expedited Forwarding (EF): Premium-Service.
  Geringe Verzögerung, Jitter + Paketverluste (RFC 2598)
- Assured Forwarding (AF): Bietet ein differenziertes Schema zur Behandlung unterschiedlichen Verkehrs (RFC 2597).
- Default Forwarding/Best Effort: Keine besondere Priorisierung.

Das Class Selector PHB ordnet die 7 möglichen IP-Precedence Werte aus dem alten TOS-Feld bestimmten DSCP-Werten zu, was die Abwärtskompatibilität gewährleistet.

ToS-Bedeutung	Precedence -Wert	Zugeordneter DSCP
Network Control	111	CS7 (111000)
Internetwork Control	110	CS6 (110000)
Critical	101	CS5 (101000)
Flash Override	100	CS4 (100000)
Flash	011	CS3 (011000)
Immidiate	010	CS2 (010000)
Priority	001	CS1 (001000)
Routine	000	CS0 (000000)

Tab. 15: Zuordnung der IP-Precedence Werte zum DSCP-Wert

DSCP-Wert	DSCP-Name	Traffic Class (Voreinstellung)
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

Tab. 16: Abbildung der DSCP-Werte auf die Traffic Classes

8.4.4 Management-Priorisierung

Damit Sie in Situationen großer Netzlast immer vollen Zugriff auf die Verwaltung des Gerätes haben, bietet Ihnen das Gerät die Möglichkeit, Management-Pakete zu priorisieren.
Bei der Priorisierung von Management-Paketen (SNMP, Telnet, usw.) sendet das Gerät die Management-Pakete mit einer Prioritäts-Information.

- Auf Layer 2 modifiziert das Gerät die VLAN-Priorität im VLAN-Tag. Das sinnvolle Nutzen dieser Funktion setzt voraus, dass die Konfiguration der entsprechenden Ports das Versenden von Paketen mit VLAN-Tag erlaubt.

- Auf Layer 3 modifiziert das Gerät den IP-DSCP-Wert.

8.4.5 Behandlung empfangener Prioritätsinformationen

Das Gerät bietet folgende Möglichkeiten, diese Prioritätsinformation auszuwerten:

- trust dot1p
  VLAN-getaggten Paketen ordnet das Gerät entsprechend ihrer VLAN-Priorität den unterschiedlichen Traffic Classes zu. Die Zuordnung erfolgt nach der voreingestellten Tabelle (siehe auf Seite 176 „VLAN-Tagging“). Diese Zuordnung können Sie modifizieren. Paketen, die das Gerät ohne Tag empfängt, ordnet das Gerät die Port-Priorität zu.
- untrusted
  Das Gerät ignoriert die Prioritäts-Informationen im Paket und weist den Paketen immer die Port-Priorität des Empfangsports zu.
- trust ip-dscp
  Das Gerät ordnet IP-Paketen entsprechend des DSCP-Wertes im IP-Header den unterschiedlichen Traffic Classes zu, auch wenn das Paket zusätzlich VLAN-getagged war. Die Zuordnung erfolgt nach den voreingestellten Werten (siehe Tabelle 16). Diese Zuordnung können Sie modifizieren.
  Nicht-IP-Pakete priorisiert das Gerät entsprechend der Port-Priorität.

8.4.6 Handhabung der Verkehrsklassen

Für die Handhabung der Traffic Classes bietet das Gerät:

- Strict Priority
- Weighted Fair Queuing
- Strict Priority kombiniert mit Weighted Fair Queuing

Voreinstellung: Strict Priority.

Beschreibung Strict-Priority

Bei Strict-Priority vermittelt das Gerät zuerst alle Datenpakete mit höherer Verkehrsklasse (höherer Priorität), bevor es ein Datenpaket mit der nächst niedrigeren Verkehrsklasse vermittelt. Ein Datenpaket mit der niedrigsten Verkehrsklasse (niedrigsten Priorität) vermittelt das Gerät demnach erst, wenn keine anderen Datenpakete mehr in der Warteschlange stehen. In ungünstigen Fällen sendet das Gerät Pakete mit niedriger Priorität nie, wenn an diesem Port ein hohes Aufkommen von höherpriorem Verkehr zum Senden ansteht.
Bei zeit- und latenzkritischen Anwendungen, wie z.B. VoIP oder Video, ermöglicht Strict Priority das unmittelbare Senden hochpriorer Daten (siehe auf Seite 185 „Maximale Bandbreite“).

Beschreibung Weighted-Fair-Queuing

Mit Weighted-Fair-Queuing, auch WeightedRoundRobin (WRR) genannt, weist der Anwender jeder Verkehrsklasse eine minimale oder reservierte Bandbreite zu. Dies hat zur Folge, dass das Gerät bei hoher Netzlast auch Datenpakete mit einer niedrigen Priorität vermittelt.

Die Werte für die Gewichtung liegen im Bereich von 0% bis 100% der verfügbaren Bandbreite in Schritten von 5%.

- Die Gewichtung „0“ entspricht der Einstellung „keine Bandbreitenreservierung“.
- Die Summe der Einzelbandbreiten darf bis zu 100% betragen.

Wenn Sie allen Verkehrsklassen das Weighted-Fair-Queuing zuweisen, dann steht diesen die gesamte Bandbreite des entsprechenden Ports zur Verfügung.

Wenn Sie Weighted Fair Queuing mit Strict Priority kombinieren, dann achten Sie darauf, dass die höchste Traffic Class von Weighted Fair Queuing kleiner ist als die niedrigste Traffic Class von Strict Priority.
In diesem Fall kann eine hohe Strict-Priority-Netzlast die für Weighted Fair Queuing verfügbare Bandbreite deutlich reduzieren.

Maximale Bandbreite

Die Eingabe einer maximalen Bandbreite bietet Ihnen die Möglichkeit, die Bandbreite jeder Traffic Class auf einen Maximalwert zu begrenzen, unabhängig davon ob Sie „Weighted Fair Queuing“ oder „Strict Priority“ gewählt haben.

- Weighted Fair Queuing (siehe auf Seite 184 „Beschreibung Weighted-Fair-Queuing“) setzt voraus, dass die maximale Bandbreite mindestens so groß ist wie die minimale Bandbreite.
- Bei „Strict Priority“ werden einzelne hochpriore Pakete mit geringer Latenz bearbeitet (siehe auf Seite 184 „Beschreibung Strict-Priority“). Die Konfiguration der maximalen Bandbreite auf einen Wert kleiner 100% ermöglicht auch bei einer hochprioren Überlast das Vermitteln von Datenpaketen mit niedrigeren Traffic Classes.
  Die Werte für die Gewichtung liegen im Bereich von 0% bis 100% der verfügbaren Bandbreite in Schritten von 5%.

Beschreibung Traffic Shaping

Beim Traffic Shaping haben Sie die Möglichkeit, die maximale Bandbreite eines Interfaces zu beschränken.

Die Werte für die Bandbreitenbegrenzung liegen im Bereich von 0% bis 95% in Schritten von 5%.

- Der Wert „0“ entspricht der Einstellung „keine Bandbreiten-begrenzung“.
- er Wert „95“ entspricht 95% der zur Verfügung stehenden Bandbreite.

Bei kurzzeitigem Überschreiten der eingestellten Bandbreite speichert das Gerät die Daten, um sie nach der Spitzenbelastung zu senden. Auf diese Weise glättet das Traffic Shaping Überlastsituationen.

Ist Traffic Shaping an einem Interface aktiv, dann ignoriert das Gerät die für Weighted Fair Queuing reservierten Bandbreiten.

8.4.7 Priorisierung einstellen

Port-Priorität zuweisen

- ☐ Öffnen Sie den Dialog `QoS/Priorität:Portkonfiguration`.
- ☐ In der Spalte „Port Priorität“ haben Sie die Möglichkeit, die Priorität (0-7) festzulegen, mit welcher das Gerät Datenpakete vermittelt, die er an diesem Port ohne VLAN-Tag empfängt.
- ☐ In der Spalte „Trust Mode“ haben Sie die Möglichkeit, festzulegen, nach welchem Kriterium das Gerät empfangenen Datenpakete einer Traffic Class zuordnet (siehe auf Seite 175 „Beschreibung Priorisierung“).

Anmerkung: Falls Sie VLANs eingerichtet haben, beachten Sie den „VLAN 0-Transparent Modus“ (siehe `Switching:VLAN:Global`).

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1.1.
`vlan priority 3`	Weist dem Interface 1/1 die Port-Priorität 3 zu.
`exit`	Wechsel in den Konfigurationsmodus.

VLAN-Priorität einer Verkehrsklasse zuordnen

- ☐ Wählen Sie den Dialog `QOS/Priorität:802.1D/p-Mapping`.
- ☐ Tragen Sie in der Spalte „Traffic Class“ die gewünschten Werte ein.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`classofservice dot1p-mapping 0 2`	Weist der VLAN-Priorität 0 die Traffic Class 2 zu.
`classofservice dot1p-mapping 1 2`	Weist der VLAN-Priorität 1 auch die Traffic Class 2 zu.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show classofservice dot1p-mapping`	Zeigt die Zuordnung an.

```
User Priority    Traffic Class
-------------    -------------
      0                2
      1                2
      2                0
      3                1
      4                2
      5                2
      6                3
      7                3
```

Empfangenen Datenpaketen immer die Port-Priorität zuweisen (PowerMICE, MACH 104, MACH 1040 und MACH 4000)

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1.1.
`no classofservice trust vlan priority 1`	Weist dem Interface den „no trust“-Modus zu. Setzt die Port-Priorität auf den Wert 1.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show classofservice trust 1/1`	Zeigt den Trust-Modus am Interface 1/1 an.

```
Class of Service Trust Mode: Untrusted

Untrusted Traffic Class: 4
```

Einem DSCP die Traffic Class zuweisen

☐ Wählen Sie den Dialog `QOS/Priorität:IP DSCP Mapping`.
☐ Tragen Sie in der Spalte „Traffic Class“ die gewünschten Werte ein.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`classofservice ip-dscp-mapping cs1 1`	Weist dem DSCP CS1 die Traffic Class 1 zu.

```
show classofservice ip-dscp-mapping

    IP DSCP       Traffic Class
 -------------    -------------
   0(be/cs0)           2
   1                   2
   .
   .
   8(cs1)              1
   .
```

Empfangenen IP-Datenpaketen immer die DSCP-Priorität pro Interface zuweisen (PowerMICE, MACH 104, MACH 1040 und MACH 4000)

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 6/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 6/1.
`classofservice trust ip-dscp`	Weist dem Interface den „trust ip-dscp“-Modus zu.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show classofservice trust 6/1`	Zeigt den Trust-Modus am Interface 6/1 an.

```
Class of Service Trust Mode: IP DSCP

Non-IP Traffic Class: 2
```

Empfangenen IP-Datenpaketen immer die DSCP-Priorität global zuweisen

☐ Öffnen Sie den Dialog `QoS/Priorität:Global`.
☐ Wählen Sie in der Zeile „Trust Mode” `trustIPDSCP` aus.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`classofservice trust ip-dscp`	Weist global den „trust ip-dscp“-Modus zu.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show classofservice trust`	Zeigt den Trust-Modus an.

```
Class of Service Trust Mode: IP DSCP
```

Konfiguration von Weighted Fair Queuing und Traffic Shaping

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`no cos-queue strict 0 1 2 3 4 5`	Schaltet Strict Priority für die Traffic Classes 0 bis 5 aus und somit Weighted Fair Queuing ein. Die Traffic Classes 6 und 7 verbleiben im Strict-Priority-Modus.
`cos-queue min-bandwidth 10 10 15 15 20 30 0 0`	Weist den Weighted-Fair-Queuing-Traffic Classes die Gewichtung zu. Da das Gerät bei Strict Priority zuerst alle Datenpakete mit höherer Priorität vermittelt, können Sie hier für die Strict-Priority-Traffic Classes die Gewichtung 0 eingeben und auf die verbleibenden Traffic Classes 100% verteilen. Das Gerät verteilt die verbleibende Bandbreite entsprechend der prozentualen Gewichtung.
`cos-queue max-bandwidth 20 20 20 20 20 30 30 30`	Weist allen Traffic Classes eine maximale Bandbreite zu (Shaping). Weil die beiden Strict-Priority-Traffic Classes auf maximal 30% begrenzt sind, steht den verbleibenden Queues mindestens 40% der Bandbreite zur Verfügung. Strict-Priority-Daten sendet das Gerät bis zu einer maximalen Bandbreite von 30% unmittelbar.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show interfaces cos-queue`	Zeigt die Konfiguration an.

```
Global Configuration
Interface Shaping Rate..................... 0

Queue Id   Min. Bandwidth   Max. Bandwidth   Scheduler Type
--------   --------------   --------------   --------------
0          10               20               Weighted
1          10               20               Weighted
2          15               20               Weighted
3          15               20               Weighted
4          20               20               Weighted
5          30               30               Weighted
6          0                30               Strict
7          0                30               Strict
```

Traffic Shaping an einem Port konfigurieren

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus des Ports 1.2.

`traffic-shape 50`	Begrenzt die maximale Bandbreite von Interface 1/2 auf 50%.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show interfaces cos-queue 1/2`	Zeigt die Konfiguration von Interface 1/2 an.

```
Interface..................................... 1/2
Interface Shaping Rate........................ 50

Queue Id   Min. Bandwidth   Max. Bandwidth   Scheduler Type
--------   --------------   --------------   --------------
0          10               20               Weighted
1          10               20               Weighted
2          15               20               Weighted
3          15               20               Weighted
4          20               20               Weighted
5          30               30               Weighted
6          0                30               Strict
7          0                30               Strict
```

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus des Ports 1.2.
`traffic-shape 50`	Begrenzt die maximale Bandbreite von Interface 1/2 auf 50%.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show interfaces cos-queue 1/2`	Zeigt die Konfiguration von Interface 1/2 an.

```
Interface..................................... 1/2
Interface Shaping Rate........................ 50

Queue Id   Min. Bandwidth   Max. Bandwidth   Scheduler Type
--------   --------------   --------------   --------------
0          10               20               Weighted
1          10               20               Weighted
2          15               20               Weighted
3          15               20               Weighted
4          20               20               Weighted
5          30               30               Weighted
6          0                30               Strict
7          0                30               Strict
```

Management-Priorität Layer 2 konfigurieren

☐ Konfigurieren Sie die VLAN-Ports, an denen das Gerät Management-Pakete verschickt, als Mitglied im VLAN, das Datenpakete mit Tag versendet (siehe auf Seite 197 „Beispiele für ein VLAN“).

☐ Öffnen Sie den Dialog `QoS/Priorität:Global`.
☐ Im Feld „VLAN-Priorität für Management-Pakete“ geben Sie den Wert der VLAN-Priorität ein.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network priority dot1p-vlan 7`	Der Management-Priorität den Wert 7 zuweisen, damit Management-Pakete mit höchster Priorität gesendet werden.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show network`	Zeigt die Management VLAN-Priorität an.

```
System IP Address.............................. 10.0.1.116
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.0.1.200
Burned In MAC Address.......................... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)...... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
HiDiscovery Version............................ v1, v2
Management VLAN ID............................. 1
Management VLAN Priority....................... 7
Management IP-DSCP Value....................... 0(be/cs0)
Web Mode....................................... Enable
```

Management-Priorität Layer 3 konfigurieren

☐ Öffnen Sie den Dialog `QoS/Priorität:Global`.
☐ Im Feld „IP-DSCP-Wert für Management-Pakete“ geben Sie den IP-DSCP-Wert ein, mit denen das Gerät Management-Pakete sendet.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network priority ip-dscp cs7`	Der Management-Priorität den Wert cs7 zuweisen, damit Management-Pakete mit höchster Priorität behandelt werden.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show network`	Zeigt die Management VLAN-Priorität an.

```
System IP Address.............................. 10.0.1.116
Subnet Mask.................................... 255.255.255.0
Default Gateway................................ 10.0.1.200
Burned In MAC Address.......................... 00:80:63:51:7A:80
Network Configuration Protocol (BootP/DHCP).... None
DHCP Client ID (same as SNMP System Name)...... "PowerMICE-517A80"
Network Configuration Protocol HiDiscovery..... Read-Write
HiDiscovery Version............................ v1, v2
Management VLAN ID............................. 1
Management VLAN Priority....................... 7
Management IP-DSCP Value....................... 56(cs7)
Web Mode....................................... Enable
```

8.5 Flusskontrolle

8.5.1 Beschreibung Flusskontrolle

Flusskontrolle (flow control) ist ein Mechanismus, der als Überlastschutz für das Gerät dient. Während verkehrsstarken Zeiten hält er zusätzlichen Verkehr vom Netz fern.

Im Beispiel (siehe Abbildung 37) ist die Wirkungsweise der Flusskontrolle graphisch dargestellt. Die Workstations 1, 2 und 3 wollen zur gleichen Zeit viele Daten an die Workstation 4 übertragen. Die gemeinsame Bandbreite der Workstations 1, 2 und 3 zum Gerät ist größer, als die Bandbreite von Workstation 4 zum Gerät. So kommt es zum Überlaufen der Sende-Warteschlange von Port 4. Der linke Trichter symbolisiert diesen Zustand.

Wenn nun an den Ports 1, 2 und 3 des Gerätes die Funktion Flusskontrolle eingeschaltet ist, dann reagiert das Gerät bevor der Trichter überläuft. Die Ports 1, 2 und 3 melden den angeschlossenen Geräten, dass im Moment keine Daten empfangen werden können.

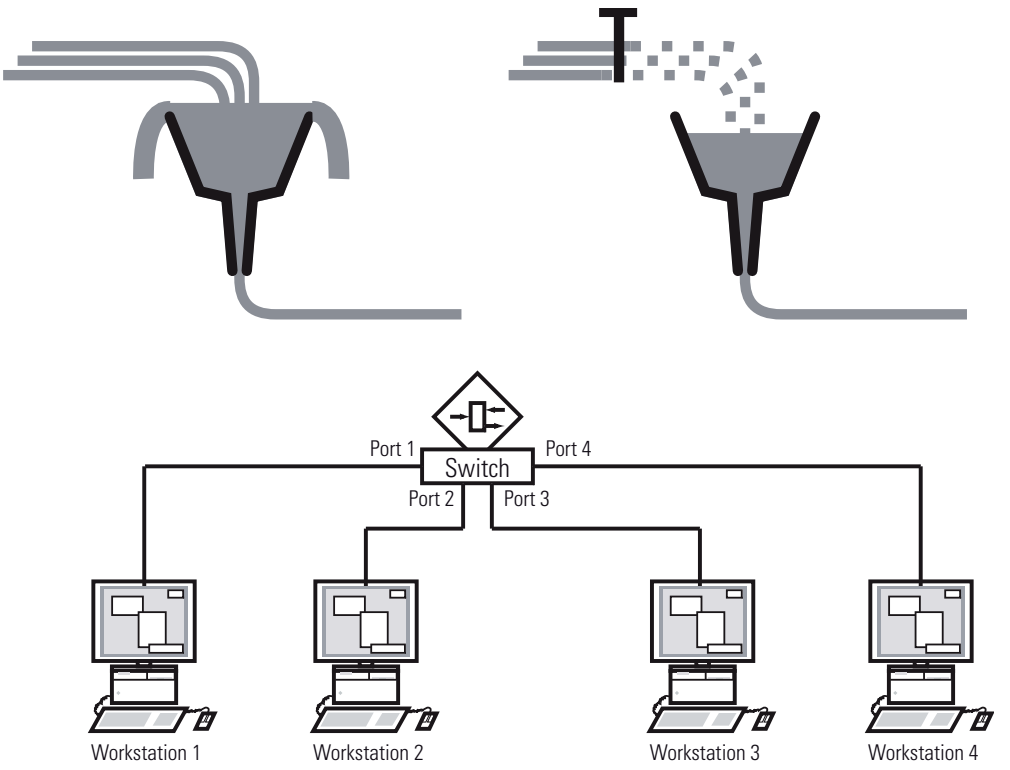


Abb. 37: Beispiel für Flusskontrolle

Flusskontrolle bei Vollduplex-Verbindung

Im Beispiel (siehe Abbildung 37) sei zwischen der Workstation 2 und dem Gerät eine Vollduplex-Verbindung.
Bevor die Sende-Warteschlange von Port 2 überläuft, sendet das Gerät eine Aufforderung an Workstation 2, beim Senden eine kleine Pause einzulegen.

Anmerkung: Die Geräte RS20/30/40, MS20/30, Octopus, MACH 100, RSR und MACH 1000 unterstützen die Flusskontrolle ausschließlich im Vollduplex-Betrieb.

Flusskontrolle bei Halbduplex-Verbindung
Im Beispiel (siehe Abbildung 37) sei zwischen der Workstation 2 und dem Gerät eine Halbduplex-Verbindung.
Bevor die Sende-Warteschlange von Port 2 überläuft, sendet das Gerät Daten zurück, damit die Workstation 2 eine Kollision erkennt und somit den Sendevorgang unterbricht.

Anmerkung: Die Geräte RS20/30/40, MS20/30, Octopus, MACH 100, RSR und MACH 1000 unterstützen im Halbduplex-Betrieb keine Flusskontrolle.

8.5.2 Flusskontrolle einstellen

☐ Wählen Sie den Dialog `Grundeinstellungen:Portkonfiguration`.
In der Spalte „Flusskontolle an“ legen Sie durch Ankreuzen fest, dass an diesem Port Flusskontrolle aktiv ist. Aktivieren Sie hierzu auch den globalen Schalter "Flusskontrolle" im Dialog `Switching:Global`.

☐ Wählen Sie den Dialog `Switching:Global`.
dieser Dialog bietet Ihnen die Möglichkeit,
- die Flusskontrolle an allen Ports auszuschalten oder
- die Flusskontrolle an den Ports einschalten, bei denen die Flusskontrolle in der Portkonfigurationstabelle ausgewählt ist.

Anmerkung: Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Geräte-Ports. Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt.

8.6 VLANs

8.6.1 Beschreibung VLAN

Ein virtuelles LAN (VLAN) besteht im einfachsten Fall aus einer Gruppe von Netzteilnehmern in einem Netzsegment, die so miteinander kommunizieren, als bildeten sie ein eigenständiges LAN.

Komplexere VLANs erstrecken sich über mehrere Netzsegmente und basieren zusätzlich auf logischen (statt ausschließlich physikalischen) Verbindungen zwischen Netzteilnehmern. VLANs werden so zu einem Element der flexiblen Netzgestaltung, da Sie logische Verbindungen einfacher zentral umkonfigurieren können als Kabelverbindungen.

Der Standard IEEE 802.1Q definiert die VLAN-Funktion.

Die wichtigsten Vorteile der VLANs sind:

- Netzlastbegrenzung
  VLANs reduzieren die Netzlast erheblich, da die Geräte Broadcast-, Multicast- und Unicast-Pakete mit unbekannten (nicht gelernten) Zieladressen ausschließlich innerhalb des virtuellen LANs vermitteln. Der Rest des Datennetzes übermittelt den Verkehr wie üblich.

- Flexibilität
  Sie haben die Möglichkeit, flexibel Anwender-Arbeitsgruppen zu bilden, die auf der Funktion der Teilnehmer basieren und nicht auf ihrem physikalischen Standort oder Medium.

- Übersichtlichkeit
  VLANs strukturieren Netze überschaubarer und vereinfachen die Wartung.

8.6.2 Beispiele für ein VLAN

Die folgenden Beispiele aus der Praxis vermitteln einen schnellen Einstieg in den Aufbau eines VLANs.

Beispiel 1

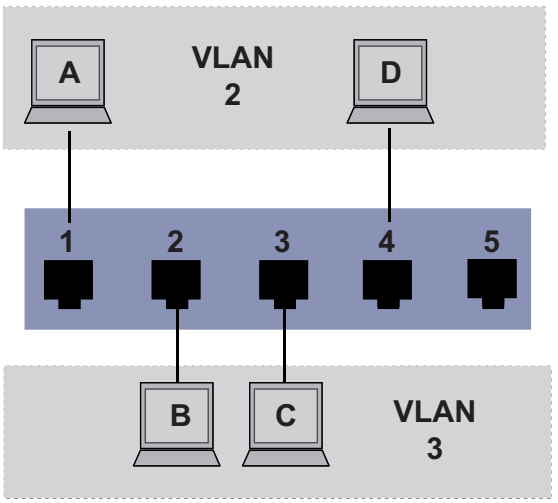


Abb. 38: Beispiel für ein einfaches portbasiertes VLAN

Das Beispiel zeigt eine minimale VLAN-Konfiguration (portbasiertes VLAN). Ein Administrator hat an einem Vermittlungsgerät mehrere Endgeräte angeschlossen und diese 2 VLANs zugeordnet. Dies unterbindet wirksam jeglichen Datenverkehr zwischen verschiedenen VLANs; deren Mitglieder kommunizieren ausschließlich innerhalb ihres eigenen VLANs.
Während der Einrichtung der VLANs erstellen Sie für jeden Port Kommunikationsregeln, die Sie in einer Eingangs- (Ingress-) und einer Ausgangs- (Egress-) Tabelle erfassen.
Die Ingress-Tabelle legt fest, welche VLAN-ID ein Port den eingehenden Datenpaketen zuweist. Hierbei ordnen Sie das Endgerät über seine Portadresse einem VLAN zu.
Die Egress-Tabelle legt fest, an welchen Ports der Switch die Frames aus diesem VLAN senden darf. Mit Ihrem Eintrag definieren Sie zusätzlich, ob der Switch die an diesem Port abgehenden Ethernet-Frames markiert (tagged):

- `T` = mit Tag-Feld (T = Tagged, markiert)
- `U` = ohne Tag-Feld (U = Untagged, nicht markiert)

Für obiges Beispiel hat der Status des TAG-Feldes der Datenpakete keine Relevanz, setzen Sie es generell auf „U“.

Endgerät	Port	Port VLAN Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Tab. 17: Eingangstabelle

VLANID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Tab. 18: Ausgangstabelle

Verfahren Sie wie folgt, um die Beispielkonfiguration durchzuführen:

☐ VLAN konfigurieren

☐ Öffnen Sie den Dialog `Switching:VLAN:Statisch`.

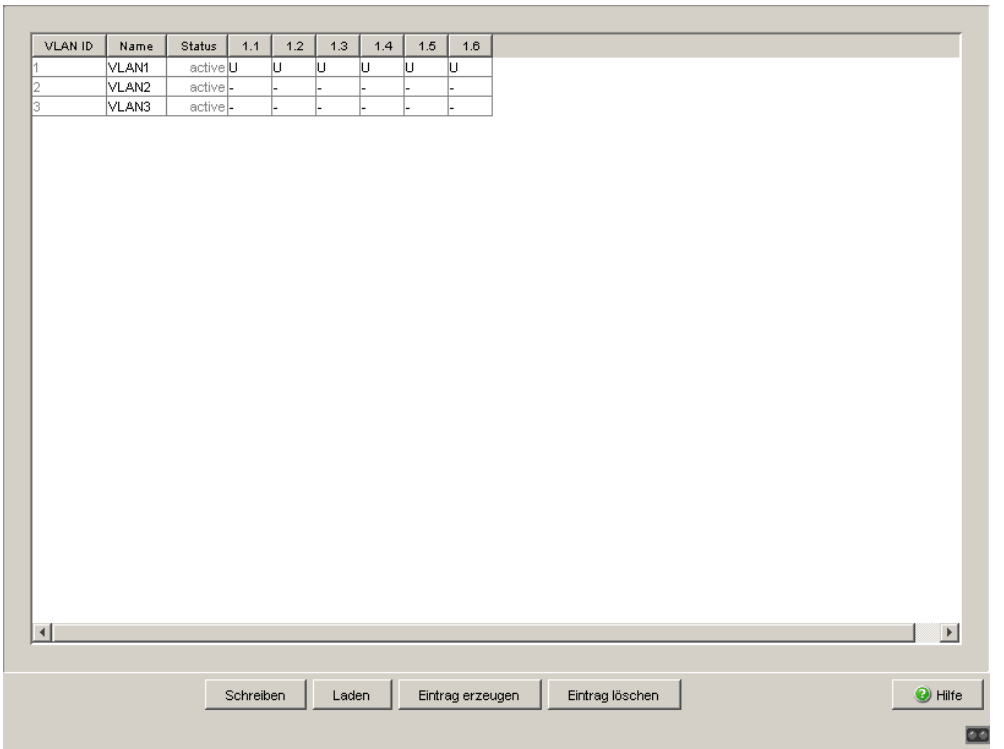


Abb. 39: Neue VLANs erzeugen und benennen

- ☐ Klicken Sie auf „Erzeugen“, um das Eingabefenster für die VLAN-ID zu öffnen.
- ☐ Weisen Sie dem VLAN die VLAN-ID `2` zu.
- ☐ Klicken Sie „OK“.
- ☐ Benennen Sie dieses VLAN mit VLAN2, indem Sie in das Feld klicken und den Namen eintragen. Ändern Sie außerdem die Bezeichnung für VLAN 1 von `Default` in `VLAN1`.
- ☐ Wiederholen Sie die vorherigen Schritte und legen Sie ein weiteres VLAN mit der VLAN-ID `3` und dem Namen `VLAN3` an.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`vlan 2`	Erzeugt ein neues VLAN mit der VLAN-ID 2.
`vlan name 2 VLAN2`	Benennt das VLAN mit der VLAN-ID 2 mit dem Namen VLAN2.
`vlan 3`	Erzeugt ein neues VLAN mit der VLAN-ID 3.
`vlan name 3 VLAN3`	Benennt das VLAN mit der VLAN-ID 3 mit dem Namen VLAN3.
`vlan name 1 VLAN1`	Benennt das VLAN mit der VLAN-ID 1 mit dem Namen VLAN1.
`exit`	Verläßt den VLAN Konfigurationsmodus.

```
show vlan brief                    Zeigt die aktuelle VLAN Konfiguration an.
Max. VLAN ID..................................... 4042
Max. supported VLANs.............................  255
Number of currently configured VLANs...........    3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                      VLAN Type VLAN Creation Time
------- -------------------------------- --------- -------------
1       VLAN1                          Default    0 days, 00:00:05
2       VLAN2                          Static     0 days, 02:44:29
3       VLAN3                          Static     0 days, 02:52:26
```

☐ Ports konfigurieren

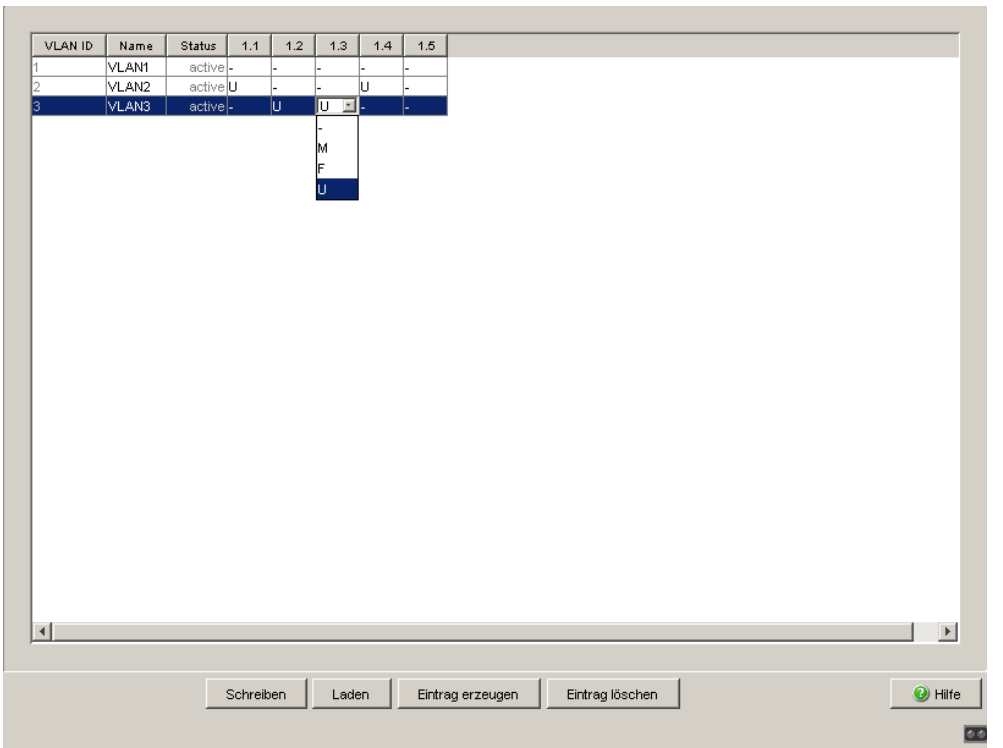


Abb. 40: VLAN-Zugehörigkeit der Ports definieren.

☐ Weisen Sie die Ports des Gerätes den entsprechenden VLANs zu, indem Sie durch einen Klick in die zugehörigen Tabellenzellen das Auswahlmenü öffnen und den Status bestimmen. Entsprechende Wahlmöglichkeiten sind:

- `-` = Momentan kein Mitglied in diesem VLAN (GVRP erlaubt)
- `T` = Mitglied im VLAN, Datenpakete mit Tag versenden
- `U` = Mitglied im VLAN, Datenpakete ohne Tag versenden
- `F` = Kein Mitglied im VLAN (auch für GVRP gesperrt)

Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, wählen Sie hier die Einstellung `U`.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
☐ Öffnen Sie den Dialog `Switching:VLAN:Port`.

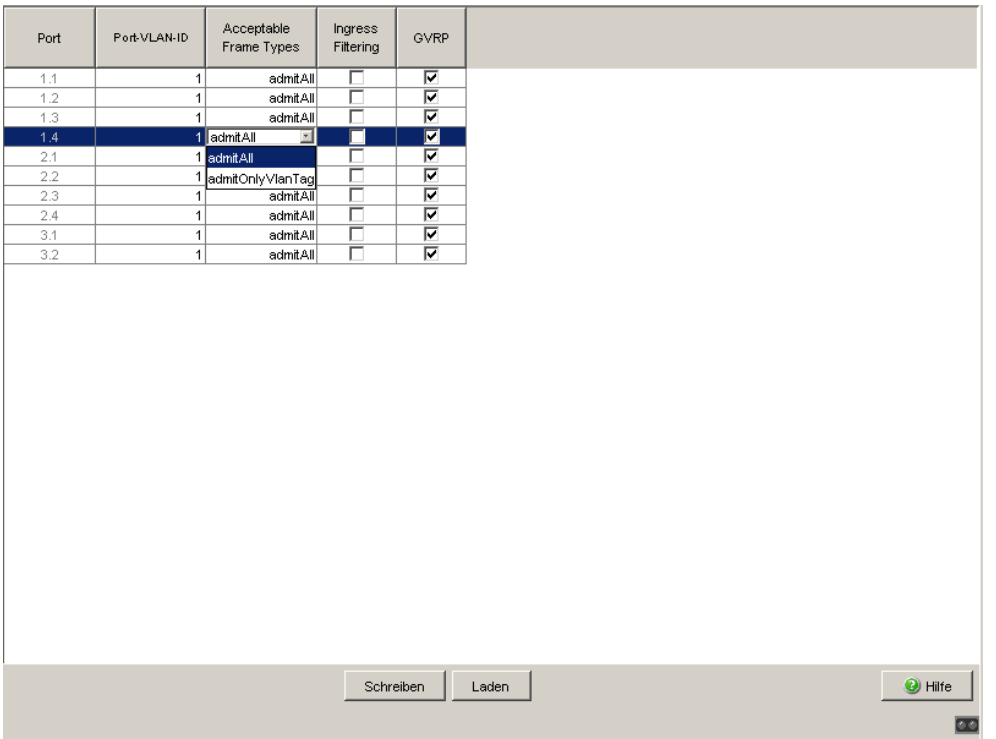


Abb. 41: „Port-VLAN ID“, „Akzeptierte Datenpakete“ und „Ingress-Filtering“ zuweisen und speichern

☐ Weisen Sie den einzelnen Ports die Port-VLAN-ID des zugehörigen VLANs (2 oder 3) zu, siehe Tabelle.
☐ Da Endgeräte Datenpakete in der Regel unmarkiert senden, wählen Sie bei „Akzeptierte Datenpakete“ die Einstellung `admitAll`.
☐ Die Einstellungen von `GVRP` und `Ingress Filter` hat keinen Einfluss auf die Funktion dieses Beispiels.
☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
☐ Wählen Sie im Rahmen „Speichern“ den Speicherort „auf dem Gerät“ und klicken Sie auf „Sichern“, um die Konfiguration nicht-flüchtig in der aktiven Konfiguration zu speichern.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1.1.
`vlan participation include 2`	Port 1/1 wird member untagged in VLAN 2.

```
vlan pvid 2                      Port 1/1 wird die Port-VLAN-ID 2 zugewiesen.
exit                             Wechsel in den Konfigurationsmodus.
interface 1/2                    Wechsel in den Interface-Konfigurationsmodus
                                 des Ports 1.2.
vlan participation include 3     Port 1/2 wird member untagged in  VLAN 3.
vlan pvid 3                      Port 1/2 wird die Port-VLAN-ID 3 zugewiesen.
exit                             Wechsel in den Konfigurationsmodus.
interface 1/3                    Wechsel in den Interface-Konfigurationsmodus
                                 von Interface 1.3.
vlan participation include 3     Port 1/3 wird member untagged in  VLAN 3.
vlan pvid 3                      Port 1/3 wird die Port-VLAN-ID 3 zugewiesen.
exit                             Wechsel in den Konfigurationsmodus.
interface 1/4                    Wechsel in den Interface-Konfigurationsmodus
                                 von Port 1/4.
vlan participation include 2     Port 1/4 wird member untagged in VLAN 2.
vlan pvid 2                      Port 1/4 wird die Port-VLAN-ID 2 zugewiesen.
exit                             Wechsel in den Konfigurationsmodus.
exit                             Wechsel in den Privileged-EXEC-Modus.
show vlan 3                      Zeigt Details zum VLAN 3 an.
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 02:52:26 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Tagged
1/5         Exclude   Autodetect   Tagged
```

Beispiel 2

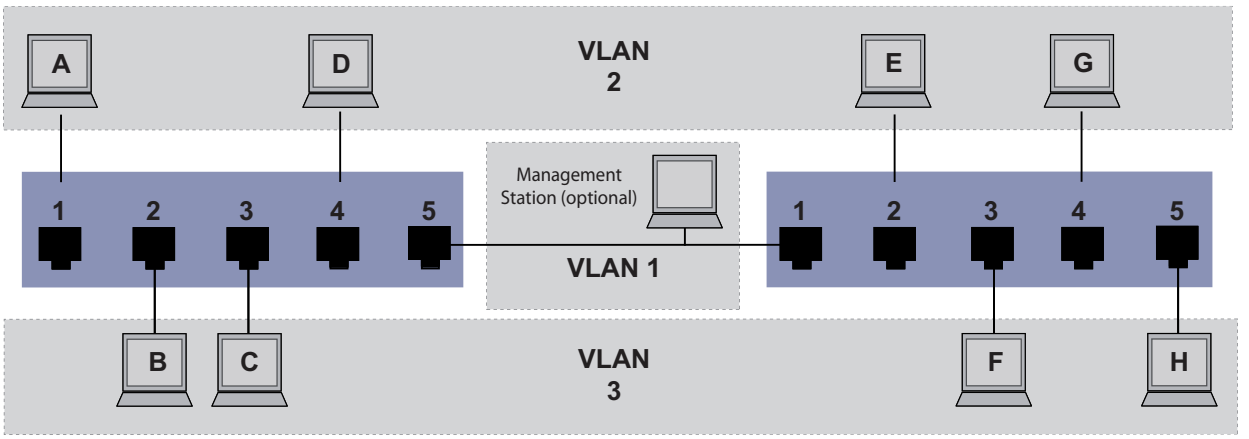


Abb. 42: Beispiel für eine komplexere VLAN-Konfiguration

Das zweite Beispiel zeigt eine komplexere Konfiguration mit 3 VLANs (1 bis 3). Zusätzlich zu dem schon bekannten Switch aus Beispiel 1 setzen Sie einen 2. Switch (im Beispiel rechts gezeichnet) ein.

Die Endgeräte der einzelnen VLANs (A bis H) erstrecken sich über 2 Vermittlungsgeräte (Switch). Derartige VLANs heißen deshalb verteilte VLANs. Zusätzlich ist eine optionale Management Station gezeigt, die bei richtiger VLAN-Konfiguration Zugriff auf alle Netzkomponenten hat.

Anmerkung: Das VLAN 1 hat in diesem Fall keine Bedeutung für die Endgerätekommunikation, ist aber notwendig für die Administration der Vermittlungsgeräte über das sogenannte Management-VLAN.

Ordnen Sie die Ports mit ihren angeschlossenen Endgeräten eindeutig einem VLAN zu (wie im vorherigen Beispiel gezeigt). Bei der direkten Verbindung zwischen den beiden Übertragungsgeräten (Uplink) transportieren die Ports Pakete für beide VLANs. Um diese Uplinks zu unterscheiden, setzen Sie die „VLAN-Markierung" ein, welche für die entsprechende Abwicklung der Frames sorgt. So bleibt die Zuordnung zu den jeweiligen VLANs erhalten.

Verfahren Sie wie folgt, um die Beispielkonfiguration durchzuführen:

Ergänzen Sie die Ingress- und Egress-Tabelle aus Beispiel 1 um den Uplink Port 5. Erfassen Sie für den rechten Switch je eine neue Ingress- und Egress-Tabelle wie im 1. Beispiel beschrieben.

Die Egress-Tabelle legt fest, an welchen Ports der Switch die Frames aus diesem VLAN senden darf. Mit Ihrem Eintrag definieren Sie zusätzlich, ob der Switch die an diesem Port abgehenden Ethernet-Frames markiert (tagged):

- `T` = mit Tag-Feld (T = Tagged, markiert)
- `U` = ohne Tag-Feld (U = Untagged, nicht markiert)

Markierte (Tagged) Frames kommen in diesem Beispiel in der Kommunikation zwischen den Vermittlungsgeräten (Uplink) zum Einsatz, da an diesen Ports Frames für unterschiedliche VLANs unterschieden werden.

Endgerät	Port	Port VLAN Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Tab. 19: Ingress-Tabelle Gerät links

Endgerät	Port	Port VLAN Identifer (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Tab. 20: Ingress-Tabelle Gerät rechts

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tab. 21: Egress Tabelle Gerät links

VLAN-ID	Port				
	1	2	3	4	5
1	U				

Tab. 22: Egress Tabelle Gerät rechts

VLAN-ID	Port					
2	T	U		U		
3	T		U		U	

Tab. 22: Egress Tabelle Gerät rechts

Die Kommunikationsbeziehungen sind hierbei wie folgt:Endgeräte an Port 1 und 4 des linken Gerätes sowie Endgeräte an Port 2 und 4 des rechten Geräts sind Mitglied im VLAN 2 und können somit untereinander kommunizieren. Ebenso verhält es sich mit den Endgeräten an Port 2 und 3 des linken Gerätes sowie Endgeräten an Port 3 und 5 des rechten Gerätes. Diese gehören zu VLAN 3.

Die Endgeräte „sehen“ jeweils ihren Teil des Netzes. Teilnehmer außerhalb dieses VLANs sind unerreichbar. Das Gerät vermittelt auch Broadcast-, Multicast- und Unicast-Pakete mit unbekannter (nicht gelernter) Zieladresse ausschließlich innerhalb der Grenzen eines VLANs.

Dabei kommt innerhalb des VLANs mit der ID 1 (Uplink) das VLAN-Tagging (IEEE 801.1Q) zum Einsatz. Dies erkennen Sie am Buchstaben `T` in der Egress-Tabelle der Ports.

Die Konfiguration des Beispiels erfolgt exemplarisch für das rechte Gerät. Verfahren Sie analog, um das zuvor bereits konfigurierte linke Gerät unter Anwendung der oben erstellten Ingress- und Egress-Tabellen an die neue Umgebung anzupassen.

Verfahren Sie wie folgt, um die Beispielkonfiguration durchzuführen:

☐ VLAN konfigurieren

☐ Öffnen Sie den Dialog `Switching:VLAN:Statisch`.

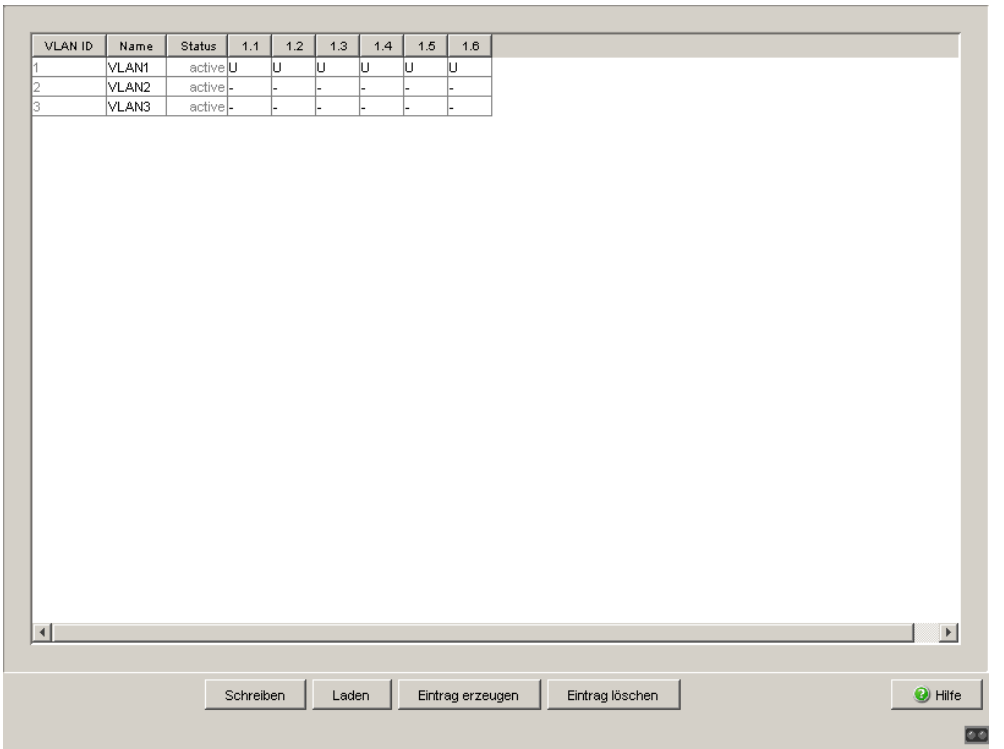


Abb. 43: Neue VLANs erzeugen und benennen

- ☐ Klicken Sie auf „Erzeugen“, um das Eingabefenster für die VLAN-ID zu öffnen.
- ☐ Weisen Sie dem VLAN die VLAN-ID `2` zu.
- ☐ Benennen Sie dieses VLAN mit VLAN2, indem Sie in das Feld klicken und den Namen eintragen. Ändern Sie außerdem die Bezeichnung für VLAN 1 von `Default` in `VLAN1`.
- ☐ Wiederholen Sie die vorherigen Schritte und legen Sie ein weiteres VLAN mit der VLAN-ID 3 und dem Namen `VLAN3` an.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`vlan 2`	Erzeugt ein neues VLAN mit der VLAN-ID 2.
`vlan name 2 VLAN2`	Benennt das VLAN mit der VLAN-ID 2 mit dem Namen VLAN2.
`vlan 3`	Erzeugt ein neues VLAN mit der VLAN-ID 3.
`vlan name 3 VLAN3`	Benennt das VLAN mit der VLAN-ID 3 mit dem Namen VLAN3.
`vlan name 1 VLAN1`	Benennt das VLAN mit der VLAN-ID 1 mit dem Namen VLAN1.
`exit`	Wechsel in den Privileged-EXEC-Modus.

```
show vlan brief                    Zeigt die aktuelle VLAN Konfiguration an.
Max. VLAN ID..................................... 4042
Max. supported VLANs.............................  255
Number of currently configured VLANs...........    3
VLAN 0 Transparent Mode (Prio. Tagged Frames).. Disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
------- -------------------------------- --------- -------------
1       VLAN1                           Default    0 days, 00:00:05
2       VLAN2                           Static     0 days, 02:44:29
3       VLAN3                           Static     0 days, 02:52:26
```

☐ Ports konfigurieren

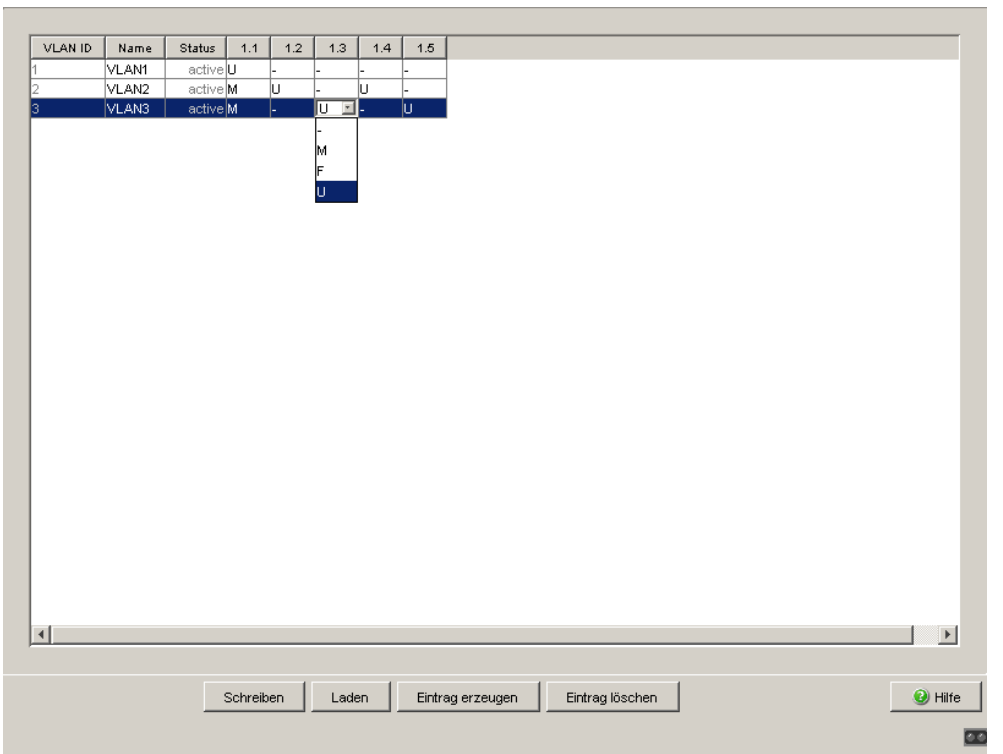


Abb. 44: VLAN-Zugehörigkeit der Ports definieren.

☐ Weisen Sie die Ports des Gerätes den entsprechenden VLANs zu, indem Sie durch einen Klick in die zugehörigen Tabellenzellen das Auswahlmenü öffnen und den Status bestimmen. Entsprechende Wahlmöglichkeiten sind:

- `-` = Momentan kein Mitglied in diesem VLAN (GVRP erlaubt)
- `T` = Mitglied im VLAN, Datenpakete mit Tag versenden
- `U` = Mitglied im VLAN, Datenpakete ohne Tag versenden
- `F` = Kein Mitglied im VLAN (auch für GVRP gesperrt)

Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, wählen Sie die Einstellung `U`. Lediglich am Uplink-Port, an dem die VLANs miteinander kommunizieren, wählen Sie die Einstellung `T`.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Öffnen Sie den Dialog `Switching:VLAN:Port`.

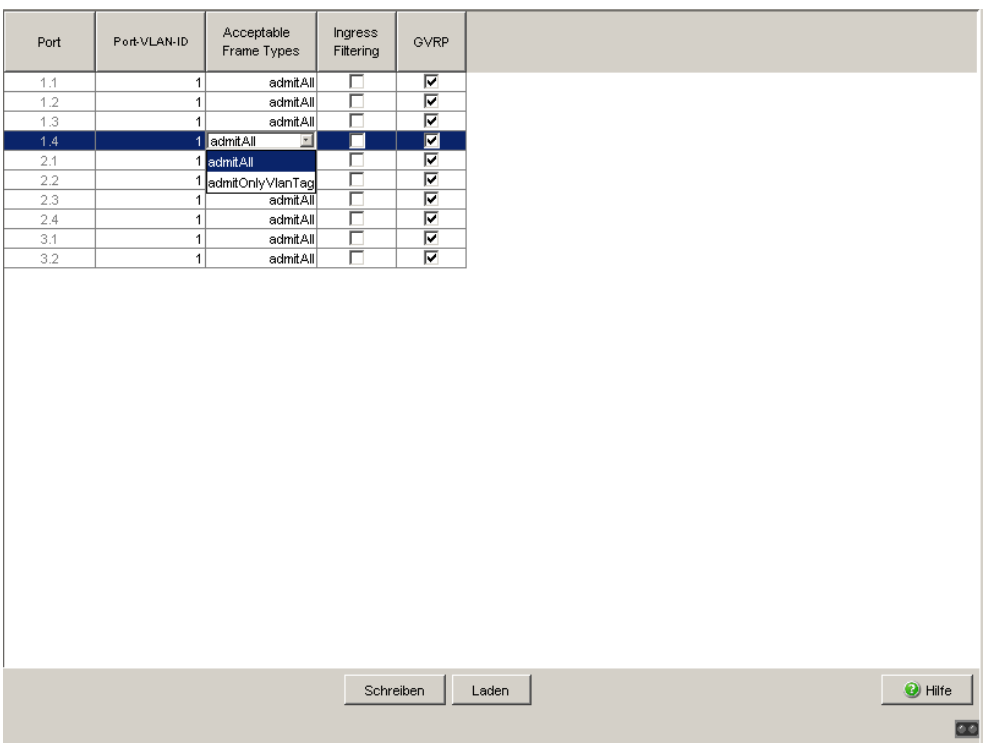


Abb. 45: „Port-VLAN ID“, „Akzeptierte Datenpakete“ und „Ingress-Filtering“ zuweisen und speichern

☐ Weisen Sie den einzelnen Ports die ID des zugehörigen VLANs (1 bis 3) zu.

☐ Da Endgeräte in der Regel keine Datenpakete mit Tag senden, wählen Sie an den Endgeräte-Ports die Einstellung `admitAll`. Konfigurieren Sie den Uplink-Port mit `admit only VLAN tags`.

☐ Um die VLAN-Markierung an diesem Port auszuwerten, aktivieren Sie „Ingress-Filtering“ am Uplink-Port.

- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
- ☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Wählen Sie im Rahmen „Speichern“ den Speicherort „auf dem Gerät“ und klicken Sie auf „Sichern“, um die Konfiguration nicht-flüchtig in der aktiven Konfiguration zu speichern.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1.1.
`vlan participation include 1`	Port 1/1 wird member untagged in VLAN 1.
`vlan participation include 2`	Port 1/1 wird member untagged in VLAN 2.
`vlan tagging 2`	Port 1/1 wird member tagged in VLAN 2.
`vlan participation include 3`	Port 1/1 wird member untagged in VLAN 3.
`vlan tagging 3`	Port 1/1 wird member tagged in VLAN 3.
`vlan pvid 1`	Port 1/1 wird die Port-VLAN-ID 1 zugewiesen.
`vlan ingressfilter`	Port 1/1 Ingress Filtering wird eingeschaltet.
`vlan acceptframe vlanonly`	Port 1/1 überträgt ausschließlich Frames mit VLAN Tag.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus des Ports 1.2.
`vlan participation include 2`	Port 1/2 wird member untagged in VLAN 2.
`vlan pvid 2`	Port 1/2 wird die Port-VLAN-ID 2 zugewiesen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface 1.3.
`vlan participation include 3`	Port 1/3 wird member untagged in VLAN 3.
`vlan pvid 3`	Port 1/3 wird die Port-VLAN-ID 3 zugewiesen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/4`	Wechsel in den Interface-Konfigurationsmodus von Port 1/4.
`vlan participation include 2`	Port 1/4 wird member untagged in VLAN 2.
`vlan pvid 2`	Port 1/4 wird die Port-VLAN-ID 2 zugewiesen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/5`	Wechsel in den Interface-Konfigurationsmodus von Port 1.5.
`vlan participation include 3`	Port 1/5 wird member untagged in VLAN 3.
`vlan pvid 3`	Port 1/5 wird die Port-VLAN-ID 3 zugewiesen.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.

```
#show vlan 3                          Zeigt Details zum VLAN 3 an.
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
VLAN Creation Time: 0 days, 00:07:47 (System Uptime)
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         Exclude   Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         Exclude   Autodetect   Untagged
1/5         Include   Include      Untagged
```

Weitere Informationen zu VLAN finden Sie im Referenzhandbuch und der integrierten Hilfefunktion im Programm.

8.6.3 Double-VLAN-Tagging

Für die Geräte MACH 1040 und MACH 4002-24G/48G.

Double-VLAN-Tagging (VLAN-Tunneling) ermöglicht Ihnen das Vermitteln von Verkehr auf Layer 2. Mit Double-VLAN-Tagging umgehen Sie Konflikte zwischen den VLAN-IDs des eingehenden Verkehrs und bereits eingerichteten VLANs in ihrem Netz. Sie können bestehende VLANs in Ihrem Netz unverändert lassen und minimieren so Ihren Konfigurationsaufwand. Dies gilt für:

- Frames ohne VLAN-Tags,
- Frames mit Prioritäts-Tags und
- Frames mit VLAN-Tags beliebiger VLAN-ID, auch solchen, die Sie in Ihrem Netz bereits für andere Zwecke verwenden.

Anwendungen sind z.B.:

- Tunneln von beliebigem Kundenverkehr auf Layer 2,
- Umgehen von Beschränkungen bei der Anzahl von VLAN-IDs,
- Zusammenfassen von VLANs pro Port.

Sie können mehrere Tunnels mit verschiedenen VLAN-IDs einrichten und dabei den Ethertype des eingefügten Tunnel-Tags für Ihr Netz frei wählen.

Die Ports, die an diesem VLAN-Tunnel beteiligt sind, sind entweder:
- sogenannte Access-Ports, an denen Ihr Netz externen Verkehr empfängt und sendet, oder
- sogenannte Core-Ports, die alle innerhalb Ihres Netzes liegen und mit einem anderen Core-Port verbunden sind.

Zum Aufbau eines VLAN-Tunnels richten Sie frei ein wählbares VLAN auf Ihren Geräten ein und nehmen die Access- und Core-Ports in dieses Tunnel-VLAN auf. Access-Ports sind ungetaggte Mitglieder in ihrem Tunnel-VLAN und haben als Port-VLAN-ID die Tunnel-VLAN-ID. Core-Ports sind getaggte Mitglieder in allen Tunnel-VLANs und benötigen keine Port-VLAN-ID. Erhöhen Sie außerdem auf allen Switches mit Core-Ports die Maximalgröße für Frames auf 1552 Bytes.

Arbeitsweise des VLAN-Tunnels:
- Das Gerät ordnet beim Empfang eines Frames an einem Access-Port dem Frame die Port-VLAN-ID zu. Dies ist die Tunnel-VLAN-ID. Dies gilt auch für bereits getaggte Frames.
- Core-Ports sind getaggte Mitglieder in allen Tunnel-VLANs und senden den Frame mit dem Tunnel-Tag aus.
- Die Core-Ports vermitteln den Verkehr anhand der Tunnel-VLAN-ID.
- Access-Ports sind ungetaggte Mitglieder ausschließlich in ihrem Tunnel-VLAN. An dem sendenden Access-Port entfernt das Gerät das Tunnel-Tag und sendet den ursprünglichen Frame aus.

Lieferzustand: Double-VLAN-Tagging ist an allen Ports ausgeschaltet. Die Voreinstellung für den Ethertype des Tunnel-Tags ist 8100Hex.

Beispiel für Double-VLAN-Tagging

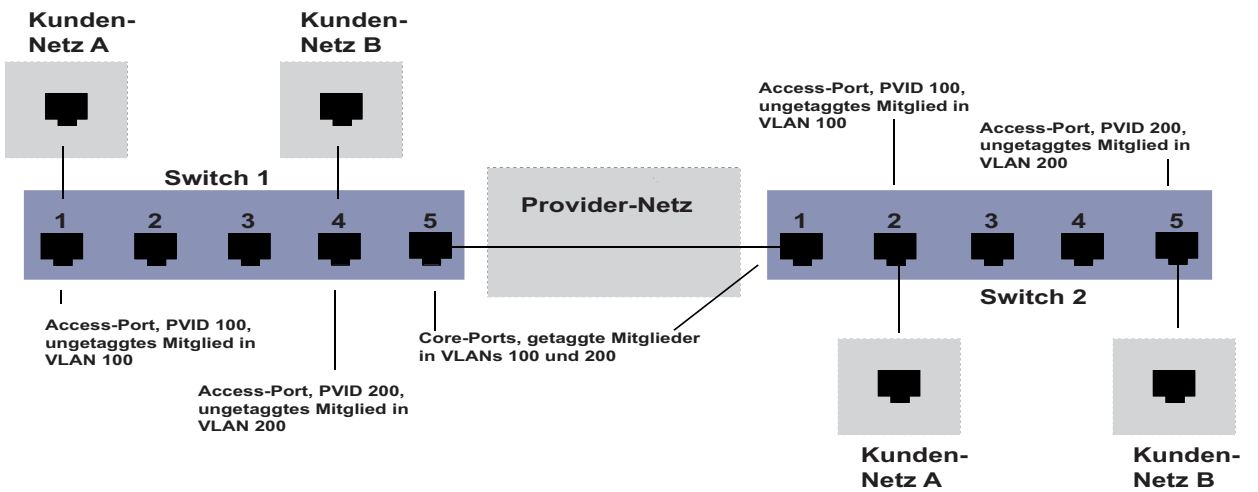


Abb. 46: Beispiel für einen VLAN-Tunnel durch Einsatz von Double-VLAN-Tagging

Das Beispiel zeigt ein Provider-Netz, das Daten aus 2 Kunden-Netzen, A und B, auf Layer 2 durch 2 VLAN-Tunnel transportiert. Der aus den Kunden-Netzen empfangene Verkehr unterliegt keinen Beschränkungen bezüglich der VLAN-IDs. Die empfangenen Frames können ohne VLAN-Tags, mit VLAN-Tags oder nur mit Priorität-Tags versehen sein.

Im Provider-Netz sind die VLAN-IDs 100 und 200 noch nicht verwendet. Sie entscheiden sich, dem Kunden A das neue Service-VLAN 100 zuzuordnen, und dem Kunden B das Service-VLAN 200. Damit liegen die VLANs für die Geräte fest:

Kunde	Service-VLAN-ID
A	100
B	200

Tab. 23: Zuordnung von Kunden-Netzen zu Service-VLANs (VLAN-Tunnels)

Auf dem Switch 1 sind die Ports 1 und 4 Access-Ports (Zugangs-Ports), Port 5 ist ein Core-Port (Port innerhalb des Provider-Netzes). Auf Switch 2 sind die Ports 2 und 5 Access-Ports und Port 1 ist ein Core-Port. Alle Ports befinden sich auf dem Modul 1 des jeweiligen Switch. Damit stehen die Einstellungen für Ports fest:

Switch	Port	Port-Rolle	Mitglied in VLAN (Tagging)	PVID
1	1/1	Access	100 (U)	100
	1/4	Access	200 (U)	200
	1/5	Core	100 (T), 200 (T)	-
2	1/1	Core	100 (T), 200 (T)	-
	1/2	Access	100 (U)	100
	1/5	Access	200 (U)	200

Tab. 24: Port-Einstellungen für VLAN-Tunnel

Stellen Sie die Beispielkonfiguration mit dem CLI ein:

Switch 1:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`vlan 100`	Erzeugt ein neues VLAN mit der VLAN-ID 100.
`vlan name 100 KUNDE_A`	Benennt das VLAN mit der VLAN-ID 100 mit dem Namen KUNDE_A.
`vlan 200`	Erzeugt ein neues VLAN mit der VLAN-ID 200.
`vlan name 200 KUNDE_B`	Benennt das VLAN mit der VLAN-ID 200 mit dem Namen KUNDE_B.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`bridge framesize 1552`	Stellt zulässige Frame-Größe auf 1522 Bytes ein.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1.1.
`vlan pvid 100`	Port 1.1 bekommt die Port-VLAN-ID 100.
`vlan participation include 100`	Port 1.1 wird Mitglied in VLAN 100
`no vlan tagging`	Port 1.1 wird ungetaggtes Mitglied (`no vlan tagging` ist Default)
`mode dvlan-tunnel access`	Port 1.1 wird Access-Port
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/4`	Wechsel in den Interface-Konfigurationsmodus von Port 1/4.
`vlan pvid 200`	Port 1.4bekommt die Port-VLAN-ID 200.
`vlan participation include 200`	Port 1.4 wird Mitglied in VLAN 200
`no vlan tagging`	Port 1.4 wird ungetaggtes Mitglied (`no vlan tagging` ist Default)
`mode dvlan-tunnel access`	Port 1.4 wird Access-Port
`exit`	Wechsel in den Konfigurationsmodus.

`interface 1/5`	Wechsel in den Interface-Konfigurationsmodus von Port 1.5.
`vlan participation include 100`	Port 1.5 wird Mitglied in VLAN 100
`vlan participation include 200`	Port 1.5 wird Mitglied in VLAN 200
`vlan tagging`	Port 1.5 wird getaggtes Mitglied
`mode dvlan-tunnel core`	Port 1.5 wird Core-Port
`exit`	Wechsel in den Konfigurationsmodus.

Switch 2:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`vlan 100`	Erzeugt ein neues VLAN mit der VLAN-ID 100.
`vlan name 100 KUNDE_A`	Benennt das VLAN mit der VLAN-ID 100 mit dem Namen KUNDE_A.
`vlan 200`	Erzeugt ein neues VLAN mit der VLAN-ID 200.
`vlan name 200 KUNDE_B`	Benennt das VLAN mit der VLAN-ID 200 mit dem Namen KUNDE_B.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`bridge framesize 1552`	Stellt zulässige Frame-Größe auf 1522 Bytes ein.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1.1.
`vlan participation include 100`	Port 1.1 wird Mitglied in VLAN 100
`vlan participation include 200`	Port 1.1 wird Mitglied in VLAN 200
`vlan tagging`	Port 1.1 wird getaggtes Mitglied
`mode dvlan-tunnel core`	Port 1.1 wird Core-Port
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus des Ports 1.2.
`vlan pvid 100`	Port 1.2 bekommt die Port-VLAN-ID 100.
`vlan participation include 100`	Port 1.2 wird Mitglied in VLAN 100
`no vlan tagging`	Port 1.2 wird ungetaggtes Mitglied (`no vlan tagging` ist Default)
`mode dvlan-tunnel access`	Port 1.2 wird Access-Port
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/5`	Wechsel in den Interface-Konfigurationsmodus von Port 1.5.

`vlan participation include 200`	Port 1.5 wird Mitglied in VLAN 200
`no vlan tagging`	Port 1.5 wird ungetaggtes Mitglied (`no vlan tagging` ist Default)
`mode dvlan-tunnel access`	Port 1.5 wird Access-Port
`exit`	Wechsel in den Konfigurationsmodus.

9 Funktionsdiagnose

Das Gerät bietet Ihnen folgende Diagnosewerkzeuge:

- Alarmmeldungen versenden
- Gerätestatus überwachen
- Out-of-band-Signalisierung durch Meldekontakt
- Port-Zustandsanzeige
- Ereigniszähler auf Portebene
- Erkennen der Nichtübereinstimmung der Duplex-Modi
- SFP-Zustandsanzeige
- TP-Kabeldiagnose
- Topologie-Erkennung
- IP-Adresskonflikte erkennen
- Erkennen von Loops (Schleifen)
- Berichte
- Datenverkehr eines Ports beobachten (Port Mirroring)
- Syslog
- Ereignis-Log

9.1 Alarmmeldungen versenden

Das Gerät meldet außergewöhnliche Ereignisse, die während des Normalbetriebs auftreten, sofort an die Verwaltungsstation. Dies geschieht über Nachrichten, sogenannte „Traps“, die das Polling-Verfahren umgehen („Polling“: Abfrage der Datenstationen in regelmäßigen Abständen). Traps ermöglichen eine schnelle Reaktion auf außergewöhnliche Ereignisse.

Beispiele für solche Ereignisse sind:

- Hardware-Reset
- Änderungen der Konfiguration
- Segmentierung eines Ports

Das Gerät sendet Traps an verschiedene Hosts,um die Übertragungssicherheit für die Nachrichten zu erhöhen. Die nicht quittierte Trap-Nachricht besteht aus einem Paket mit Informationen zu einem außergewöhnlichen Ereignis.

Das Gerät sendet Traps an jene Hosts, die in der Zieltabelle für Traps eingetragen sind. Das Gerät bietet Ihnen die Möglichkeit, die Trap-Zieltabelle mit der Verwaltungsstation über SNMP zu konfigurieren.

9.1.1 Auflistung der SNMP-Traps

Welche Traps das Gerät verschicken kann, finden Sie in der folgenden Tabelle.

Trapbezeichnung	Bedeutung
authenticationFailure	wird gesendet, falls eine Station versucht, unberechtigt auf den Agenten zuzugreifen.
coldStart	wird sowohl bei Kalt- als auch bei Warmstart während des Bootens nach erfolgreicher Initialisierung des Managements gesendet.
hmAutoconfigAdapterTrap	wird gesendet, wenn der AutoConfiguration Adapter ACA entfernt oder gesteckt wird.
linkDown	wird gesendet, wenn die Verbindung zu einem Port unterbrochen wird.
linkUp	wird gesendet, sobald die Verbindung zu einem Port wieder hergestellt wird.
hmTemperature	wird gesendet, wenn die Temperatur die Grenzen der eingestellten Schwellwerte überschreitet.
hmPowerSupply	wird gesendet, wenn sich der Status der Spannungsversorgung ändert.
hmSigConRelayChange	wird gesendet, wenn sich bei der Funktionsüberwachung der Zustand des Meldekontaktes ändert.
newRoot	wird gesendet, wenn der sendende Agent zur neuen Root des Spanning Trees wird.
topologyChange	wird gesendet, wenn sich der Vermittlungsmodus eines Ports ändert.
risingAlarm	wird gesendet, wenn ein RMON-Alarmeingang seine obere Schwelle überschreitet.
fallingAlarm	wird gesendet, wenn ein RMON-Alarmeingang seine untere Schwelle unterschreitet.
hmPortSecurityTrap	wird gesendet, wenn eine MAC/IP-Adresse an diesem Port erkannt wird, die nicht den aktuellen Einstellungen von – hmPortSecPermission entspricht und – hmPorSecAction entweder auf trapOnly (2) oder portDisable (3) gesetzt ist.
hmModuleMapChange	wird gesendet, wenn sich die Hardware-Konfiguration ändert.
hmBPDUGuardTrap	wird gesendet, wenn an einem Port bei aktivierter BPDU-Guard-Funktion eine BPDU empfangen wird.
hmMrpReconfig	wird gesendet, sobald sich die Konfiguration des MRP-Rings ändert.
hmRingRedReconfig	wird gesendet, sobald sich die Konfiguration des HIPER-Rings ändert.
hmRingRedCplReconfig	wird gesendet, sobald sich die Konfiguration der redundanten Ring-/Netzkopplung ändert.

Tab. 25: Mögliche Traps

Trapbezeichnung	Bedeutung
hmSNTPTrap	wird gesendet, wenn im Zusammenhang mit dem SNTP Fehler auftreten (z.B. Server nicht erreichbar).
hmRelayDuplicateTrap	wird gesendet, wenn im Zusammenhang mit der DHCP-Option 82 eine doppelte IP-Adresse erkannt wird.
lldpRemTablesChange-Trap	wird gesendet, wenn sich ein Eintrag in der Topologie-Remote-Tabelle ändert.
vrrpTrapNewMaster	wird gesendet, wenn ein anderer Router für ein Interface bzw. eine virtuelle Adresse Master geworden ist.
vrrpTrapAuthFailure	wird gesendet, wenn der Router von einem anderen VRRP-Router ein Paket mit ungültiger Authentifizierung empfängt.
hmConfiguration-SavedTrap	wird gesendet, nachdem das Gerät seine Konfiguration erfolgreich lokal gespeichert hat.
hmConfiguration-ChangedTrap	wird gesendet, wenn Sie die Konfiguration des Geräts nach dem Lokalen Speichern zum 1. Mal ändern.
hmAddressRelearnDetec-tTrap	wird gesendet, bei aktivierter Adress Relearn Detection die Schwelle der wiederholt an verschiedenen Ports gelernten MAC-Adressen überschritten wird. Dieser Vorgang weist mit großer Wahrscheinlichkeit auf eine Loop- (Schleifen-) Situation im Netz hin.
hmDuplexMismatchTrap	wird gesandt, wenn das Gerät ein mögliches Problem mit dem Duplex-Modus eines Ports entdeckt.
hmTrapRebootOnError	wird gesendet, wenn das Gerät einen Fehler entdeckt, der mit einem Kaltstart zu beheben ist.

Tab. 25: Mögliche Traps

9.1.2 SNMP-Traps beim Booten

Das Gerät sendet bei jedem Booten die Alarmmeldung „ColdStart“.

9.1.3 Trapeinstellung

☐ Öffnen Sie den Dialog `Diagnose:Alarme (Traps).`

Dieser Dialog bietet Ihnen die Möglichkeit festzulegen, welche Ereignisse einen Alarm (Trap) auslösen und an wen diese Alarme gesendet werden sollen.

☐ Klicken Sie „Erzeugen“.

☐ In der Spalte „IP-Adresse“ geben Sie die IP-Adresse des Empfängers an, an den die Traps geschickt werden sollen.

☐ In der Spalte „Aktiv“ kreuzen Sie die Einträge an, die das Gerät beim Versenden von Traps berücksichtigen sollen. Voreinstellung: inaktiv.

☐ In der Spalte „Passwort“ geben Sie den Community-Namen an, den das Gerät verwendet, um sich als Quelle des Traps zu identifizieren.

☐ Im Rahmen „Konfiguration“ wählen Sie die Trap-Kategorien aus, von denen Sie Traps versenden wollen. Voreinstellung: alle Trap-Kategorien sind aktiv.

Anmerkung: Für diesen Dialog benötigen Sie Schreibrechte.

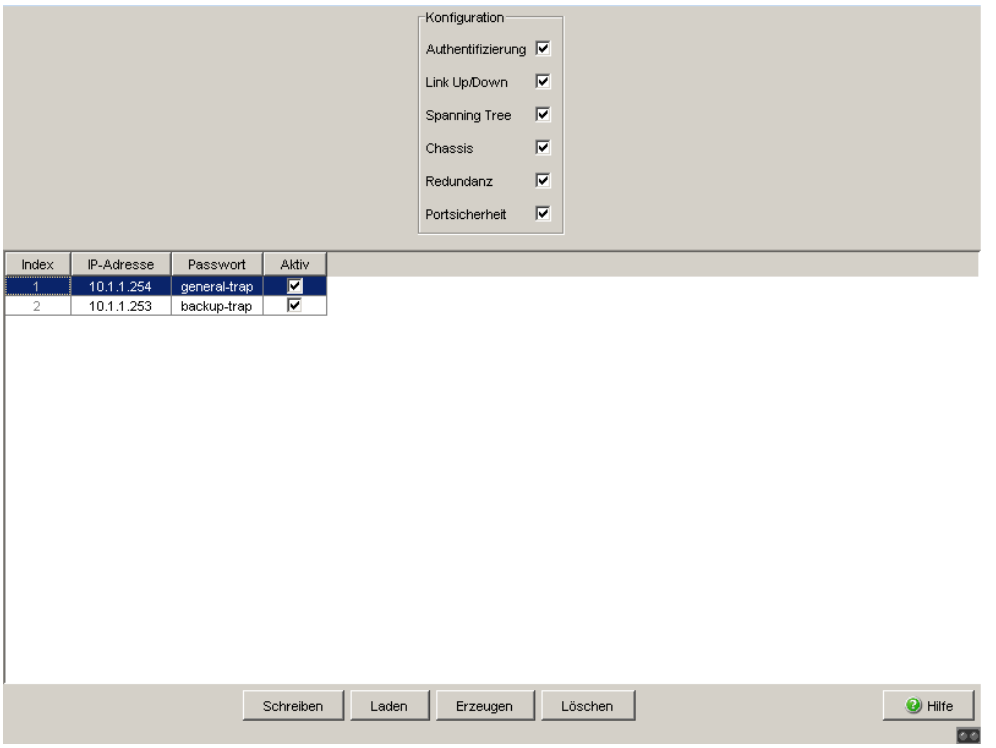


Abb. 47: Dialog Alarme

Die auswählbaren Ereignisse haben folgende Bedeutung:

Name	Bedeutung
Authentifizierung	Das Gerät hat einen unerlaubten Zugriff zurückgewiesen (siehe Dialog `Zugriff für IP-Adressen und Portsicherheit`).
Link Up/Down	An einem Port des Gerätes wurde die Verbindung zu einem anderen Gerät hergestellt/unterbrochen.
Spanning Tree	Die Topologie des Rapid Spanning Tree hat sich geändert
Chassis	Fasst die folgenden Ereignisse zusammen: – Der Status einer Versorgungsspannung hat sich geändert (siehe Dialog `System`). – Der Status des Meldekontakts hat sich geändert. Um dieses Ereignis zu berücksichtigen, aktivieren Sie „Trap bei Statuswechsel erzeugen“ im Dialog `Diagnose:Meldekontakt 1/2`. – Der AutoConfiguration Adapter (ACA) wurde hinzugefügt oder entfernt. – Die Konfiguration auf dem AutoConfiguration Adapter (ACA) unterscheidet sich von der im Gerät. – Die Temperaturschwellen wurden unter- oder überschritten. – Ein Medienmodul wurde hinzugefügt oder entfernt (nur bei modularen Geräten). – Der Empfangsleistungs-Status eines Ports mit SFP-Modul hat sich geändert (siehe Dialog `Diagnose:Ports:SFP-Module`).
	Der Redundanzzustand der Ring-Redundanz (redundante Strecke aktiv/inaktiv) oder (bei Geräten, die redundante Ring-/Netzkopplung unterstützen) der redundanten Ring-/Netzkopplung (Redundanz vorhanden) hat sich geändert.
Portsicherheit	An einem Port wurde ein Datenpaket von einem nicht erlaubten Endgerät empfangen (siehe Dialog `Portsicherheit`).

Tab. 26: Trap-Kategorien

9.2 Gerätestatus überwachen

Der Gerätestatus gibt einen Überblick über den Gesamtzustand des Gerätes. Viele Prozessvisualisierungssysteme erfassen den Gerätestatus eines Gerätes, um seinen Zustand grafisch darzustellen.

Das Gerät zeigt seinen aktuellen Status als „Fehler“ oder „Ok“ im Rahmen „Gerätestatus“ an. Das Gerät bestimmt diesen Status aus den einzelnen Überwachungsergebnissen.
Das Gerät bietet Ihnen die Möglichkeit, den Gerätezustand

- über einen Meldekontakt out-of-band zu signalisieren (siehe auf Seite 228 „Gerätestatus mit Meldekontakt überwachen“)
- durch das Versenden eines Traps bei einer Änderung des Gerätezustandes zu signalisieren.
- in der grafischen Benutzeroberfläche auf der Systemseite zu erkennen und
- im Command Line Interface abzufragen.

Der Dialog `Diagnose:Gerätestatus` umfasst:

- Inkorrekte Versorgungsspannung
  - mindestens eine der 2 Versorgungsspannungen ist außer Betrieb,
  - die interne Versorgungsspannung ist außer Betrieb.
- Über- oder Unterschreiten der eingestellten Temperaturschwelle.
- das Entfernen eines Moduls (bei modularen Geräten).
- das Entfernen des ACA.
- Die Konfiguration auf dem externer Speicher stimmt nicht mit der im Gerät überein.
- die Unterbrechung der Verbindung an mindestens einem Port. Sie definieren im Menü `Grundeinstellung:Portkonfiguration` welche Ports das Gerät bei fehlender Verbindung signalisiert (siehe auf Seite 86 „Erkannte Kommunikationsunterbrechung melden“). Im Lieferzustand erfolgt keine Verbindungsüberwachung.
- Ereignisse der Ring-Redundanz:
  Redundanzverlust (im Ring-Manager-Modus). Im Lieferzustand ist die Ring-Redundanz-Überwachung inaktiv.
  Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in der lokalen Konfiguration.

- Ereignis bei der Ring-/Netzkopplung:
  den Entfall der Redundanz. Im Lieferzustand erfolgt keine Überwachung der Kopplungs-Redundanz.
  Im Stand-by-Modus meldet das Gerät zusätzlich folgende Zustände:
  – fehlerhafter Linkstatus der Steuerleitung
  – Partnergerät ist im Stand-by-Modus
- den Ausfall eines Lüfters (MACH 4000).

Entscheiden Sie durch Markieren der entsprechenden Einträge, welche Ereignisse der Gerätestatus erfasst.

Anmerkung: Bei nicht redundanter Zuführung der Versorgungsspannung meldet das Gerät das Fehlen einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder die Überwachung ausschalten (siehe auf Seite 228 „Gerätefunktionen mit Meldekontakt überwachen“).

9.2.1 Gerätestatus konfigurieren

- ☐ Öffnen Sie den Dialog `Diagnose:Gerätestatus`.
- ☐ Wählen Sie im Feld „Überwachung“ die Ereignisse, die Sie überwachen möchten.
- ☐ Zur Temperaturüberwachung stellen Sie zusätzlich die Temperaturschwellen im Dialog `Grundeinstellungen:System` am Ende der Systemdaten ein .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`device-status monitor all error`	Bezieht alle möglichen Ereignisse zur Gerätestatusermittlung mit ein.
`device-status trap enable`	Aktiviert das Versenden eines Traps, wenn sich der Gerätestatus ändert.

Anmerkung: Die obigen CLI-Kommandos schalten Überwachung und Trapping jeweils für alle unterstützten Komponenten ein. Wenn Sie eine Überwachung nur für einzelne Komponenten ein- bzw. ausschalten möchten, finden Sie die entsprechende Syntax im CLI-Handbuch oder mit der Hilfe der CLI-Konsole (geben Sie ein Fragezeichen „?“ am CLI-Prompt ein).

9.2.2 Gerätestatus anzeigen

☐ Wählen Sie den Dialog `Grundeinstellungen:System`.

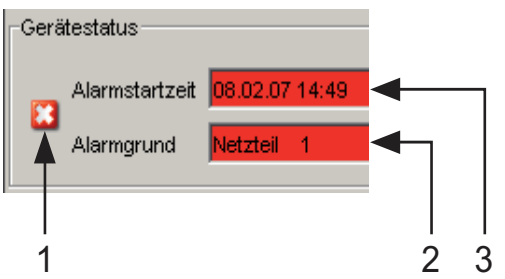


Abb. 48: Gerätestatus- und Alarm-Anzeige
1 - Das Symbol zeigt den Gerätestatus an
2 - Ursache des ältesten, bestehenden Alarms
3 - Beginn des ältesten, bestehenden Alarms

`exit`	Wechsel in den Privileged-EXEC-Modus.
`show device-status`	Zeigt den Gerätestatus und die Einstellung zur Gerätestatusermittlung an.

9.3 Out-of-band-Signalisierung

Die Meldekontakte dienen der Steuerung externer Geräte und der Funktionsüberwachung des Gerätes. Die Funktionsüberwachung bietet Ihnen die Möglichkeit einer Ferndiagnose.
Den Funktionsstatus meldet das Gerät über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) durch Kontaktunterbrechung:

- Inkorrekte Versorgungsspannung
  - mindestens eine der 2 Versorgungsspannungen ist außer Betrieb,
  - die interne Versorgungsspannung ist außer Betrieb.
- Über- oder Unterschreiten der eingestellten Temperaturschwelle.
- das Entfernen eines Moduls (bei modularen Geräten).
- das Entfernen des ACA.
- Die Konfiguration auf dem externer Speicher stimmt nicht mit der im Gerät überein.
- die Unterbrechung der Verbindung an mindestens einem Port. Sie definieren im Menü `Grundeinstellung:Portkonfiguration` welche Ports das Gerät bei fehlender Verbindung signalisiert (siehe auf Seite 86 „Erkannte Kommunikationsunterbrechung melden“). Im Lieferzustand erfolgt keine Verbindungsüberwachung.
- Ereignisse der Ring-Redundanz:
  Redundanzverlust (im Ring-Manager-Modus). Im Lieferzustand ist die Ring-Redundanz-Überwachung inaktiv.
  Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in der lokalen Konfiguration.
- Ereignis bei der Ring-/Netzkopplung:
  den Entfall der Redundanz. Im Lieferzustand erfolgt keine Überwachung der Kopplungs-Redundanz.
  Im Stand-by-Modus meldet das Gerät zusätzlich folgende Zustände:
  – fehlerhafter Linkstatus der Steuerleitung
  – Partnergerät ist im Stand-by-Modus
- den Ausfall eines Lüfters (MACH 4000).

Entscheiden Sie durch Markieren der entsprechenden Einträge, welche Ereignisse der Gerätestatus erfasst.

Anmerkung: Bei nicht redundanter Zuführung der Versorgungsspannung meldet das Gerät das Fehlen einer Versorgungsspannung. Sie können diese Meldung verhindern, indem Sie die Versorgungsspannung über beide Eingänge zuführen oder die Überwachung ausschalten (siehe auf Seite 228 „Gerätefunktionen mit Meldekontakt überwachen“).

9.3.1 Meldekontakt steuern

Dieser Modus dient der Fernsteuerung des Signalkontaktes.

Anwendungsmöglichkeiten:

- Simulation eines bei einer SPS-Fehlerüberwachung ermittelten Fehlers.
- Fernbedienen eines Gerätes über SNMP, z. B. Einschalten einer Kamera.

☐ Wählen Sie den Dialog `Diagnose:Meldekontakt 1/2`.

☐ Wählen Sie „Manuelle Einstellung“ im Feld „Modus Meldekontakt“, um den Meldekontakt manuell zu schalten.

☐ Wählen Sie „Offen“ im Feld „Manuelle Einstellung“, um den Kontakt zu öffnen.

☐ Wählen Sie „Geschlossen“ im Feld „Manuelle Einstellung“, um den Kontakt zu schließen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`signal-contact 1 mode manual`	Wählt die Betriebsart manuelle Einstellung für den Meldekontakt 1.

`signal-contact 1 state open`	Öffnet den Meldekontakt 1.
`signal-contact 1 state close`	Schließt den Meldekontakt 1.

9.3.2 Gerätestatus mit Meldekontakt überwachen

Die Auswahl „Gerätestatus“ bietet Ihnen die Möglichkeit, ähnlich wie bei der Funktionsüberwachung den Gerätestatus (siehe auf Seite 223 „Gerätestatus überwachen“) über den Meldekontakt zu überwachen.

9.3.3 Gerätefunktionen mit Meldekontakt überwachen

Funktionsüberwachung konfigurieren

- ☐ Wählen Sie den Dialog `Diagnose:Meldekontakt`.
- ☐ Wählen Sie „Funktionsüberwachung“ im Feld „Modus Meldekontakt“, um den Kontakt zur Funktionsüberwachung zu nutzen.
- ☐ Wählen Sie im Feld „Funktionsüberwachung“ die Ereignisse, die Sie überwachen möchten.
- ☐ Zur Temperaturüberwachung stellen Sie im Dialog `Grund-einstellungen:System` am Ende der Systemdaten die Temperaturschwellen ein.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.

`signal-contact 1 monitor all`	Bezieht alle möglichen Ereignisse zur Funktionsüberwachung mit ein.
`signal-contact 1 trap enable`	Aktiviert das Versenden eines Traps, wenn sich der Zustand der Funktionsüberwachung ändert.

Meldekontakt-Anzeige

Das Gerät bietet 3 weitere Möglichkeiten, den Zustand des Meldekontaktes darzustellen:

- LED-Anzeige am Gerät,
- Anzeige in der grafischen Benutzeroberfläche,
- Abfrage im Command Line Interface.

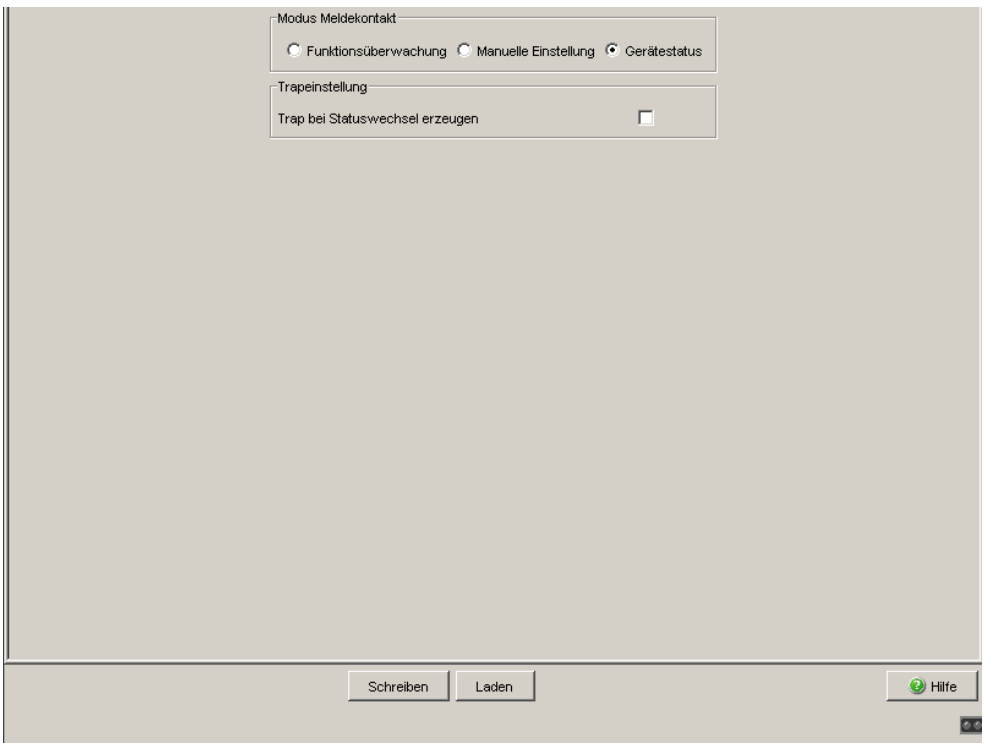


Abb. 49: Dialog Meldekontakt

`exit`	Wechsel in den Privileged-EXEC-Modus.
`show signal-contact 1`	Zeigt den Zustand der Funktionsüberwachung und die Einstellung zur Statusermittlung an.

9.3.4 Lüfter überwachen

Geräte der Mach 4000-Familie verfügen über einen auswechselbaren Lüftereinschub. Dieser Lüftereinschub trägt wesentlich zur Senkung der Innentemperatur des Gerätes bei.
Lüfter unterliegen einem natürlichen Verschleiß. Der Ausfall eines oder mehrerer Einzellüfter des Lüftereinschubs kann die Funktion und die Lebensdauer des Gerätes negativ beeinflussen oder zum Totalausfall des Gerätes führen.
Das Gerät bietet Ihnen die Möglichkeit, Statusänderungen des Lüftereinschubs

- über einen Meldekontakt out-of-band (außerhalb des Datenstroms) zu signalisieren. (siehe auf Seite 228 „Gerätestatus mit Meldekontakt überwachen“)
- durch das Versenden eines Traps bei einer Änderung des Gerätezustandes zu signalisieren.
- im Web-based Interface auf der Systemseite zu erkennen und
- im Command Line Interface abzufragen.

Verfahren Sie wie folgt, um Änderungen am Lüfterstatus über einen Meldekontakt und mit einer Alarmmeldung zu signalisieren:

- ☐ Wählen Sie den Dialog `Diagnose:Meldekontakt`.
- ☐ Wählen Sie über die entsprechende Karteikarte „Meldekontakt 1“ oder „Meldekontakt 2“ den Meldekontakt aus, den Sie zur Signalisisierung benutzen wollen (im Beispiel Meldekontakt 1).
- ☐ Im Rahmen „Modus Meldekontakt“ wählen Sie „Funktionsüberwachung“.
- ☐ Markieren Sie im Rahmen „Funktionsüberwachung“ das Überwachen des Lüfters.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
- ☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Wählen Sie im Rahmen „Speichern“ den Speicherort „auf dem Gerät“ und klicken Sie auf „Sichern“, um die Konfiguration nichtflüchtig in der aktiven Konfiguration zu speichern.

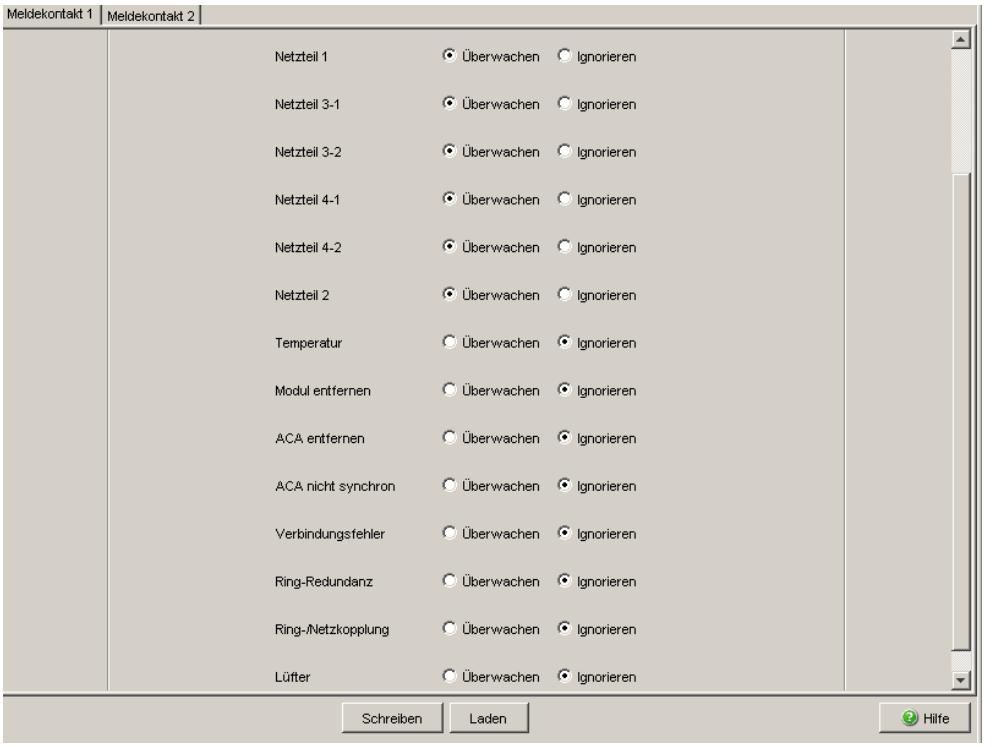


Abb. 50: Lüfter mit Meldekontakt und Trap überwachen

9.4 Port-Zustandsanzeige

☐ Wählen Sie den Dialog `Grundeinstellungen:System`.

Die Gerätedarstellung zeigt das Gerät mit der aktuellen Bestückung. Der Zustand der einzelnen Ports wird durch eines der nachfolgenden Symbole dargestellt. Sie erhalten eine vollständige Beschreibung des Portzustandes, indem Sie den Mauszeiger über das Portsymbol stellen.

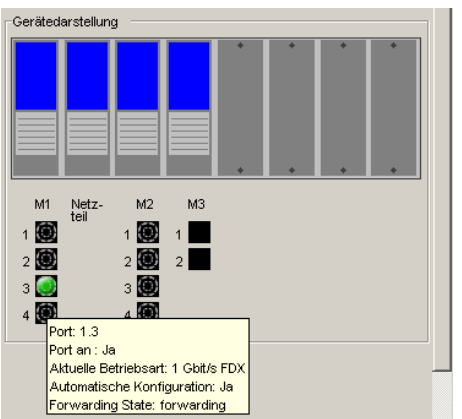


Abb. 51: Gerätedarstellung

Bedeutung der Symbole:

Der Port (10, 100 MBit/s, 1, 10 GBit/s) ist freigegeben und die Verbindung ist in Ordnung.

Der Port ist vom Management gesperrt und hat eine Verbindung.

Der Port ist vom Management gesperrt und hat keine Verbindung.

Der Port ist im Autonegotiation-Modus.

Der Port ist im HDX-Modus.

Der Port (100 MBit/s) ist im Discarding-Modus eines Redundanzprotokolls wie z.B. Spanning Tree oder HIPER-Ring.

Der Port ist im Routing-Modus (100 MBit/s).

9.5 Ereigniszähler auf Portebene

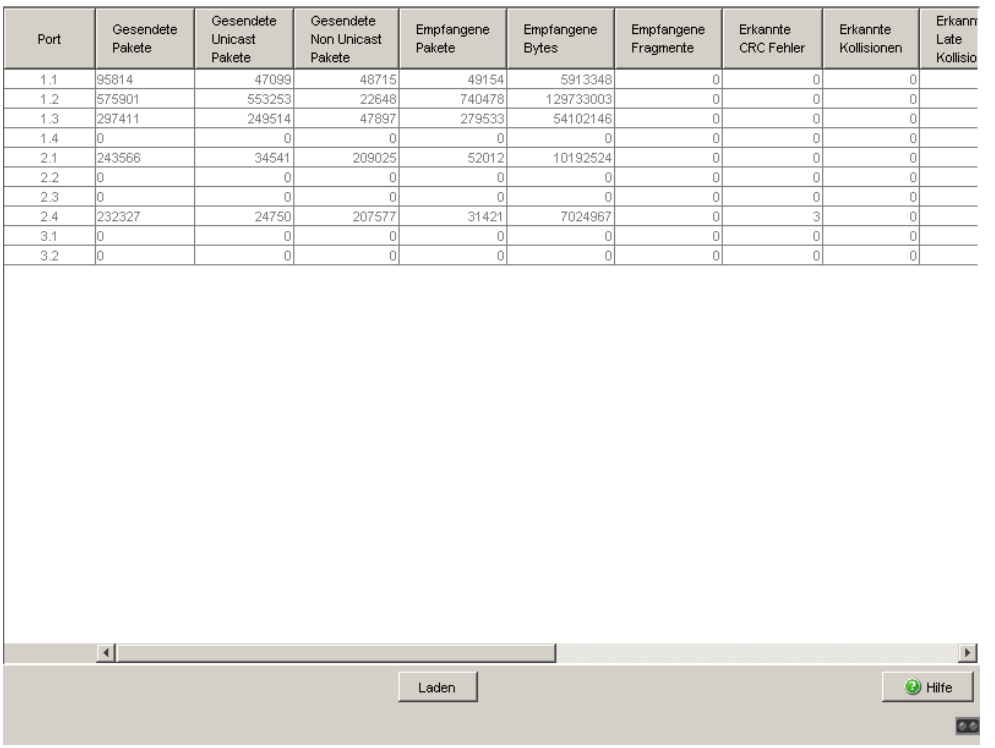
Die Port-Statistiktabelle versetzt den erfahrenen Netzbetreuer in die Lage, erkannte eventuelle Schwachpunkte im Netz zu identifizieren.
Diese Tabelle zeigt Ihnen die Inhalte verschiedener Ereigniszähler an. Im Menüpunkt Neustart können Sie mit „Warmstart“, „Kaltstart“ oder „Portzähler zurücksetzen“ die Ereigniszähler auf 0 zurücksetzen.
Die Paketzähler summieren die Ereignisse aus Sende- und Empfangsrichtung.

Zähler	Angabe bekannter möglicher Schwächen
Empfangene Fragmente	– Nicht funktionierender Controller des verbundenen Gerätes – Elektromagnetische Einkoppelung im Übertragungsmedium
CRC-Fehler	– Nicht funktionierender Controller des verbundenen Gerätes – Elektromagnetische Einkoppelung im Übertragungsmedium – Nicht betriebsbereite Komponente im Netz
Kollisionen	– Nicht funktionierender Controller des verbundenen Gerätes – Netzausdehnung zu groß/Zeilen zu lang – Kollision oder Fehler beim Datenpaket ermittelt

Tab. 27: Beispiele für die Angabe bekannter Schwächen

☐ Wählen Sie den Dialog `Diagnose:Ports:Statistiken`.

☐ Um die Zähler zurückzusetzen, klicken Sie im Dialog Grundeinstellungen:Neustart auf „Portzähler zurücksetzen“.



Port	Gesendete Pakete	Gesendete Unicast Pakete	Gesendete Non Unicast Pakete	Empfangene Pakete	Empfangene Bytes	Empfangene Fragmente	Erkannte CRC Fehler	Erkannte Kollisionen	Erkannt Late Kollisio
1.1	95814	47099	48715	49154	5913348	0	0	0	
1.2	575901	553253	22648	740478	129733003	0	0	0	
1.3	297411	249514	47897	279533	54102146	0	0	0	
1.4	0	0	0	0	0	0	0	0	
2.1	243566	34541	209025	52012	10192524	0	0	0	
2.2	0	0	0	0	0	0	0	0	
2.3	0	0	0	0	0	0	0	0	
2.4	232327	24750	207577	31421	7024967	0	3	0	
3.1	0	0	0	0	0	0	0	0	
3.2	0	0	0	0	0	0	0	0	

Abb. 52: Dialog Portstatistiken

9.5.1 Erkennen der Nichtübereinstimmung der Duplex-Modi

Stimmen die Duplex-Modi von 2 direkt miteinander verbundenen Ports nicht überein, kann dies schwer aufzuspürende Probleme verursachen. Die automatische Detektion und Meldung dieser Situation hat den Vorteil, dies bereits zu erkennen, bevor Probleme auftreten.

Diese Situation kann durch eine Fehlkonfiguration entstehen, z.B. dann, wenn Sie die automatische Konfiguration am entfernten Port abschalten.

Ein typischer Effekt dieser Nichtübereinstimmung ist, dass die Verbindung bei niedriger Datenrate zu funktionieren scheint, das lokale Gerät bei höherem bidirektionalem Verkehrsaufkommen jedoch viele CRC-Fehler zählt und die Verbindung deutlich unter dem Nenndurchsatz bleibt.

Das Gerät bietet Ihnen die Möglichkeit, diese Situation zu erkennen und sie an die Netz-Management-Station zu melden. Das Gerät bewertet dazu die Fehlerzähler des Ports in Abhängigkeit von den Port-Einstellungen.

Möglichen Ursachen für Port-Fehlerereignisse

Die folgende Tabelle nennt die Duplex-Betriebsarten für TX-Ports zusammen mit den möglichen Fehlerereignissen. Die Begriffe in der Tabelle bedeuten:

- Kollisionen: Diese bedeuten im Halbduplexmodus Normalbetrieb.
- Duplex-Problem: Nicht übereinstimmende Duplex-Modi.
- EMI: Elektromagnetische Interferenz.
- Netzausdehnung: Die Netzausdehnung ist zu groß bzw. sind zu viele Kaskadenhubs vorhanden.
- Kollisionen, Spätkollisionen: Im Vollduplex-Modus keine Erhöhung der Port-Zähler für Kollisionen oder Spätkollisionen.
- CRC-Fehler: Das Gerät bewertet diese Fehler als nicht übereinstimmende Duplex-Modi im manuellen Vollduplex-Modus.

Nr.	Automatische Konfiguration	Aktueller Duplex-Modus	Erkannte Fehlerereignisse (≥ 10 nach Link-Up)	Duplex-Modi	Mögliche Ursachen
1	An	Halbduplex	Keine	OK	
2	An	Halbduplex	Kollisionen	OK	
3	An	Halbduplex	Späte Kollisionen (Late Collisions)	Duplex-Problem erkannt	Duplex-Problem, EMI, Netzausdehnung
4	An	Halbduplex	CRC-Fehler	OK	EMI
5	An	Vollduplex	Keine	OK	
6	An	Vollduplex	Kollisionen	OK	EMI
7	An	Vollduplex	Late Collisions	OK	EMI
8	An	Vollduplex	CRC-Fehler	OK	EMI
9	Aus	Halbduplex	Keine	OK	
10	Aus	Halbduplex	Kollisionen	OK	
11	Aus	Halbduplex	Late Collisions	Duplex-Problem erkannt	Duplex-Problem, EMI, Netzausdehnung
12	Aus	Halbduplex	CRC-Fehler	OK	EMI
13	Aus	Vollduplex	Keine	OK	
14	Aus	Vollduplex	Kollisionen	OK	EMI

Tab. 28: Bewertung des nicht übereinstimmenden Duplex-Modus

Nr.	Automatische Konfiguration	Aktueller Duplex-Modus	Erkannte Fehlerereignisse (≥ 10 nach Link-Up)	Duplex-Modi	Mögliche Ursachen
15	Aus	Vollduplex	Late Collisions	OK	EMI
16	Aus	Vollduplex	CRC-Fehler	Duplex-Problem erkannt	Duplex-Problem, EMI

Tab. 28: Bewertung des nicht übereinstimmenden Duplex-Modus (Forts.)

Aktivieren der Erkennung

☐ Wählen Sie den Dialog `Switching:Switching Global`.
☐ Markieren Sie „Duplex Mismatch Detection aktivieren“. Das Gerät prüft dann, ob der Duplex-Modus eines Ports möglicherweise nicht mit dem entfernten Ports übereinstimmt.
Entdeckt das Gerät eine mögliche Nichtübereinstimmung, erzeugt es einen Eintrag im Ereignis-Log und sendet einen Alarm (Trap).

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`bridge duplex-mismatch-detect operation enable`	Schaltet die Erkennung und Meldung der Nichtübereinstimmung der Duplex-Modi ein.
`bridge duplex-mismatch-detect operation disable`	Schaltet die Erkennung und Meldung der Nichtübereinstimmung der Duplex-Modi aus.

9.5.2 TP-Kabeldiagnose

Die TP-Kabeldiagnose ermöglicht Ihnen, das angeschlossene Kabel auf Kurzschluss oder Unterbrechung zu prüfen.

Anmerkung: Während der Überprüfung ruht der Datenverkehr an diesem Port.

Die Prüfung dauert wenige Sekunden. Nach der Prüfung finden Sie in der Zeile „Ergebnis“ das Prüfergebnis der Kabeldiagnose. Ergibt das Prüfergebnis einen Kabelfehler, dann finden Sie in der Zeile „Distanz“ die Entfernung vom Port zum Kabelfehler.

Ergebnis	Bedeutung
normal	Das Kabel ist in Ordnung.
offen	Das Kabel ist unterbrochen.
Kurzschluss	Das Kabel weist einen Kurzschluss auf.
Unbekannt	Sie haben noch keine Kabelprüfung durchgeführt oder diese läuft gerade.

Tab. 29: Bedeutung der möglichen Ergebnisse

Voraussetzungen für eine korrekte TP-Kabeldiagnose:
- 1000BASE-T-Port, über 8-adriges Kabel mit 1000BASE-T-Port verbunden oder
- 10BASE-T/100BASE-TX-Port, mit 10BASE-T/100BASE-TX-Port verbunden.

9.5.3 Port-Monitor

Wenn aktiviert, überwacht das Gerät den Status des Ports. Das Gerät bietet Ihnen die Möglichkeit, bei Auftreten von benutzerdefinierten Situationen einzelne Ports zu deaktivieren oder einen Trap zu senden.

Zu den definierbaren Situationen an Ports gehören:
- Linkänderungen
- CRC-/Fragmentfehler
- Überlasterkennung
- Geschwindigkeits- und Duplex-Kombination

Über den Dialog „Global“ aktivieren Sie die Konfigurationen, die Sie in den Registerkarten „Linkänderungen“, „CRC-/Fragmentfehler“ und „Überlasterkennung“ definiert haben. Wenn Sie die Funktionen aktivieren, erkennt das Gerät automatisch die dazugehörigen Zustände. Erkennt das Gerät an einem Port einen benutzerdefinierten Zustand, erfolgt die Aktion, die Sie für diesen Port definiert haben.

Linkänderungen treten auf, wenn eine Verbindung den Verbindungsstatus abwechselnd als aktiv oder inaktiv meldet. Konfigurieren Sie das Gerät so, dass es diesen Zustand ermittelt und legen Sie anschließend fest, ob das Gerät einen Trap versenden oder den Port abschalten soll.

Wenn Sie die CRC-/Fragmentfehler-Erkennung verwenden, erkennt das Gerät anhand der Prüfsumme Datenpakete, die während der Übertragung verändert worden sind. Das Gerät erkennt die Gesamtzahl der empfangenen Pakete, die weniger als 64 Bytes lang sind und entweder einen FCS-Fehler oder einen Alignment Error haben (ohne Framing Bits, aber einschließlich FCS Octets) .
- Ein FCS-Fehler ist eine ungültige Frame Check Sequence (FCS) mit einer ganzzahligen Anzahl von Oktetten.
- Ein Alignment Error ist eine ungültige Frame Check Sequence (FCS) mit einer nicht ganzzahligen Anzahl von Oktetten.

Das Gerät überwacht beide Kriterien, wenn Sie die Funktion in der Registerkarte „Global“ einschalten. Wenn die Anzahl der CRC-/Fragmentfehler den Schwellwert übersteigt, führt das Gerät die benutzerdefinierte Aktion aus.

Die Überlasterkennung verhindert, dass ein Broadcast-, Multicast- oder Unicast-Storm den Datenverkehr über einen Port lahm legt. Um zu erkennen, ob ein Datenpaket zu einem Unicast, Multicast oder Broadcast gehört, überwacht die Überlasterkennung die Datenpakete, die über einen Port auf den Switching-Bus gelangen. Der Switch zählt die Anzahl der benutzerdefinierten Pakete, die er innerhalb des „Abtastintervall“s erhalten hat,

und vergleicht die Messung mit einem benutzerdefinierten Grenzwert. Erreicht die Messung den Wert für „Oberer Grenzwert“, blockt der Port den Datenverkehr. Wenn Sie die Wiederherstellungsfunktion für die Überlasterkennung aktivieren, bleibt der Port geblockt, bis die Datenverkehrsrate unter den Wert für „Unterer Grenzwert“ sinkt. Danach leitet der Port den Datenverkehr wie gewohnt weiter.

Das Gerät bietet die Möglichkeit festzulegen, welcher Duplex-Modus bei welcher Geschwindigkeit auf einem bestimmten Port erlaubt ist. Die Überwachung der Kombination von Geschwindigkeit und Duplex-Modus verhindert gegebenenfalls unerwünschte Verbindungen.

- ☐ Öffnen Sie den Dialog `Diagnose:Ports:Port-Monitor`.

- ☐ Öffnen Sie die Registerkarte „Linkänderungen“.
- ☐ Geben Sie in das Eingabefeld „Anzahl Linkänderungen“ im Rahmen „Parameter“ die Anzahl der Zyklen an, wie oft ein Port zwischen link-up und link-down alterniert, bevor die Funktion den Port deaktiviert.
- ☐ Definieren Sie im Eingabefeld „Abtastintervall [s]“ im Rahmen „Parameter“ die zu verstreichende Zeit.

- ☐ Öffnen Sie die Registerkarte „CRC-/Fragmentfehler“.
- ☐ Geben Sie in das Eingabefeld „CRC-/Fragmentfehlerrate [ppm]“ im Rahmen „Parameter“ die Zahl der empfangenen Datenpakete an, die aus geänderten Raw-Daten oder Fragmenten bestehen, bevor die Funktion den Port deaktiviert.
- ☐ Definieren Sie im Eingabefeld „Abtastintervall [s]“ im Rahmen „Parameter“ die zu verstreichende Zeit.

- ☐ Öffnen Sie die Registerkarte „Überlasterkennung“.
- ☐ Definieren Sie im Eingabefeld „Abtastintervall [s]“ im Rahmen „Parameter“ die zu verstreichende Zeit.
- ☐ Definieren Sie für jeden Port den Verkehrstyp über die Spalte „Traffic-Typ“.
- ☐ Definieren Sie für jeden Port den zu berücksichtigenden Grenzwert über die Spalte „Grenzwert-Typ“.
- ☐ Definieren Sie für jeden Port den Grenzwert, ab dem das Gerät den Port aktiviert, über die Spalte „Unterer Grenzwert“.

☐ Definieren Sie für jeden Port den Grenzwert, ab dem das Gerät den Port deaktiviert, über die Spalte „Oberer Grenzwert“.

☐ Öffnen Sie die Registerkarte „Speed Duplex“.

☐ Legen Sie für jeden Port individuell fest, welcher Duplex-Modus bei welcher Geschwindigkeit erlaubt ist.

- „hdx“ = Halbduplex
- „fdx“ = Vollduplex
- „10“ = 10 Mbit/s
- „100“ = 100 Mbit/s

usw.

☐ Öffnen Sie die Registerkarte „Global“.

☐ Über die Spalte „Port Monitor an“ auf der Registerkarte „Global“ wählen Sie die zu überwachenden Ports an.

☐ Um die Port-Monitor-Funktion zu aktivieren, wählen Sie `An` im Rahmen „Funktion“.

9.5.4 Auto-Disable

Wenn die Konfiguration einen Port als aktiviert anzeigt, das Gerät jedoch einen Fehler ermittelt, schaltet die Software den betreffenden Port ab. Anders gesagt: Die Geräte-Software deaktiviert den Port aufgrund eines ermittelten Fehlerzustands.

Bei der Auto-Deaktivierung eines Ports schaltet das Gerät den betreffenden Port ab; der Port blockiert den Datenverkehr. Die Port-LED blinkt pro Phase dreimal grün und identifiziert den Grund für das Abschalten. Darüber hinaus erzeugt das Gerät einen Protokolleintrag, der den Grund für die Selbstabschaltung aufführt. Wenn Sie den Port nach einem Time-out der Auto-Disable-Funktion aktivieren, erstellt das Gerät einen Protokolleintrag.

Dieses Produktmerkmal stellt eine Wiederherstellungsfunktion bereit, die einen per Selbstabschaltung deaktivierten Port nach einem benutzerdefinierten Zeitraum automatisch wieder aktiviert. Wenn diese Funktion einen Port aktiviert, sendet das Gerät einen Trap mit der Port-Nummer, jedoch ohne einen Wert für den Parameter „Grund“.

Die Auto-Disable-Funktion hat die folgenden Aufgaben:
- Sie unterstützt den Netzwerk-Administrator bei der Port-Analyse.
- Sie schließt die Möglichkeit aus, dass der betreffende Port ein Abschalten der anderen Ports des Moduls (bzw. des gesamten Moduls) bewirkt.

Anmerkung: Die Schaltfläche „Zurücksetzen“ ermöglicht Ihnen, den Port zu aktivieren, bevor der „Reset-Timer [s]“ abgelaufen ist.

Damit das Gerät die aufgrund eines ermittelten Fehlerzustands ausgeschalteten Ports wieder einschaltet, führen Sie die folgenden Arbeitsschritte aus:

- ☐ Öffnen Sie den Dialog `Diagnose:Ports:Auto-Disable`.
- ☐ Um Ports wieder einzuschalten, die das Gerät aufgrund von Linkänderungen ausgeschaltet hat, markieren Sie im Rahmen „Konfiguration“ das Kontrollkästchen „Linkänderungen“.
  Die Parameter, die zum Ausschalten der Ports bei Linkänderungen führen, legen Sie fest im Dialog `Diagnose:Ports:Port-Monitor`, Registerkarte „Linkänderungen“.

- ☐ Um Ports wieder einzuschalten, die das Gerät aufgrund von CRC- oder Fragmentfehlern ausgeschaltet hat, markieren Sie im Rahmen „Konfiguration“ das Kontrollkästchen „CRC-/Fragmentfehler“.
  Die Parameter, die zum Ausschalten der Ports bei CRC- oder Fragmentfehlern führen, legen Sie fest im Dialog `Diagnose:Ports:Port-Monitor`, Registerkarte „CRC-/Fragmentfehler“.
- ☐ Um Ports wieder einzuschalten, die das Gerät aufgrund von Überlast ausgeschaltet hat, markieren Sie im Rahmen „Konfiguration“ das Kontrollkästchen „Überlasterkennung“.
  Die Parameter, die zum Ausschalten der Ports bei Überlast führen, legen Sie fest im Dialog `Diagnose:Ports:Port-Monitor`, Registerkarte „Überlasterkennung“.
- ☐ Um Ports wieder einzuschalten, die das Gerät aufgrund falscher Geschwindigkeits- und Duplex-Kombination ausgeschaltet hat, markieren Sie im Rahmen „Konfiguration“ das Kontrollkästchen „Speed Duplex“.
  Die Parameter, die zum Ausschalten der Ports bei falscher Geschwindigkeits- und Duplex-Kombination führen, legen Sie fest im Dialog `Diagnose:Ports:Port-Monitor`, Registerkarte „Speed Duplex“.
- ☐ Um Ports wieder einzuschalten, die das Gerät aufgrund eines unberechtigten Zugriffs auf den Port ausgeschaltet hat, markieren Sie im Rahmen „Konfiguration“ das Kontrollkästchen „Port-Sicherheit“.
  Die Parameter, die zum Ausschalten der Ports bei unberechtigten Zugriffen führen, legen Sie fest im Dialog `Sicherheit:Portsicherheit`.
- ☐ Legen Sie die Zeit bis zum automatischen Wiedereinschalten in der Tabelle, Spalte „Reset-Timer [s]“ für jeden Port individuell fest.

9.6 SFP-Zustandsanzeige

Die SFP-Zustandsanzeige bietet Ihnen die Möglichkeit, die aktuelle Bestückung der SFP-Module und deren Eigenschaften einzusehen. Zu den Eigenschaften zählen:

- Modultyp,
- Unterstützung im Medienmodul gewährt,
- Temperatur in ° C,
- Sendeleistung in mW,
- Empfangsleistung in mW.

☐ Wählen Sie den Dialog `Diagnose:Ports:SFP-Module`.

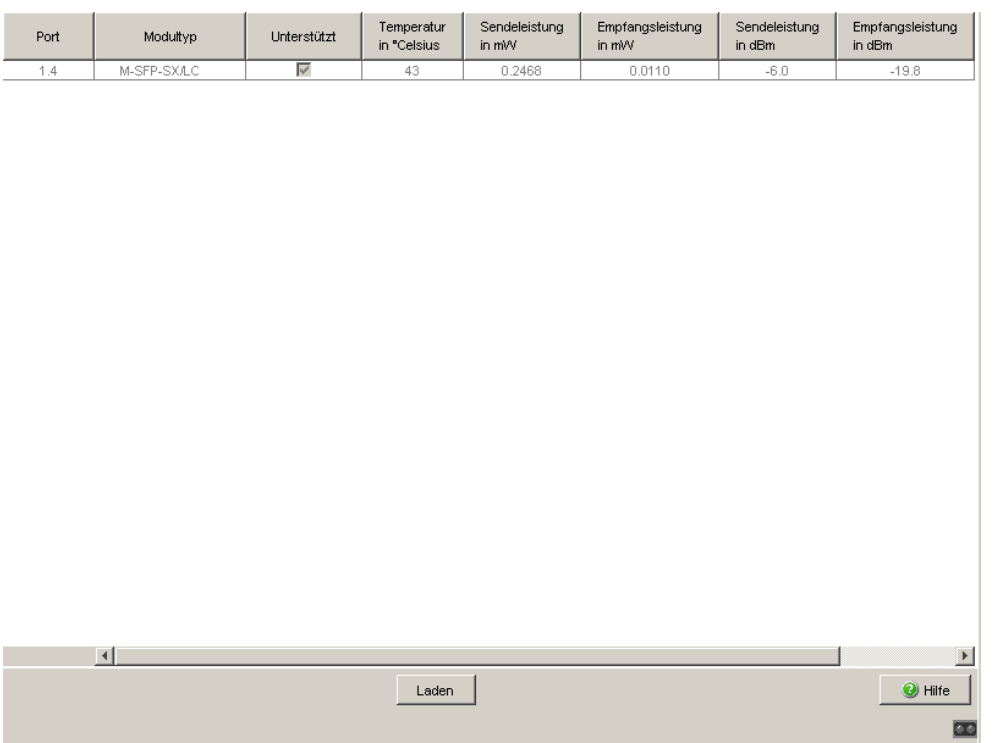


Abb. 53: Dialog SFP-Module

9.7 Topologie-Erkennung

9.7.1 Beschreibung Topologie-Erkennung

IEEE 802.1AB beschreibt das Link Layer Discovery Protocol (LLDP). Das LLDP ermöglicht dem Anwender eine automatische Topologie-Erkennung seines LANs.

Ein Gerät mit aktivem LLDP

- verbreitet eigene Verbindungs- und Management-Informationen an die angrenzenden Geräte des gemeinsamen LANs. Diese können dort ausgewertet werden, sofern diese Geräte auch das LLDP aktiviert haben.
- empfängt Verbindungs- und Management-Informationen von angrenzenden Geräten des gemeinsamen LANs, sofern diese auch das LLDP aktiviert haben.
- errichtet ein Management-Informationsschema und Objektdefinitionen zum Speichern von Informationen benachbarter Geräte mit aktiviertem LLDP.

Als zentrales Element enthält die Verbindungsinformation die genaue, eindeutige Kennzeichnung eines Verbindungsendpunktes: MSAP (MAC Service Access Point). Diese setzt sich zusammen aus einer netzweit eindeutigen Kennung des Gerätes und einer für dieses Gerät eindeutigen Portkennung.
Inhalt der Verbindungs- und Management-Informationen:

- Chassis-Kennung (dessen MAC-Adresse)
- Port-Kennung (dessen Port-MAC-Adresse)
- Beschreibung des Ports
- Systemname
- Systembeschreibung
- Unterstützte "System Capabilities"
- Momentan aktivierte "System Capabilities"
- Interface-ID der Management-Adresse
- Port-VLAN-ID des Ports

- Zustand der Autonegotiation am Port
- Medium, Halb-/Vollduplexeinstellung und Geschwindigkeits-Einstellung des Ports
- Information, ob und welches Redundanzprotokoll an dem Port eingeschaltet ist (z.B. RSTP, HIPER-Ring, Fast-HIPER-Ring, MRP, Ringkopplung).
- Information über die VLANs, die im Gerät eingerichtet sind (VLAN-ID und VLAN-Namen, unabhängig davon, ob der Port VLAN-Mitglied ist).

Diese Informationen kann eine Netzmanagementstation von einem Gerät mit aktivem LLDP abrufen. Mit diesen Informationen ist die Netzmanagement-station in der Lage, die Topologie des Netzes darzustellen.

Zum Informationsaustausch benutzt LLDP eine IEEE-MAC-Adresse, die Geräte normalerweise nicht vermitteln. Deshalb verwerfen Geräte ohne LLDP-Unterstützung LLDP-Pakete. Wird ein nicht LLDP-fähiges Gerät zwischen 2 LLDP-fähigen Geräten platziert, verhindert es den LLDP-Infor-mationsaustausch zwischen diesen beiden Geräten. Um dies zu umgehen, versenden und empfangen Hirschmann-Geräte zusätzliche LLDP-Pakete mit der Hirschmann-Multicast-MAC-Adresse 01:80:63:2F:FF:0B. Hirsch-mann-Geräte mit LLDP-Funktion sind somit in der Lage, LLDP-Informationen auch über nicht LLDP-fähige Geräte hinweg untereinander auszutauschen.

Die Management Information Base (MIB) eines LLDP-fähigen Hirschmann-Gerätes hält die LLDP-Informationen in der lldp-MIB und in der privaten hmLLDP vor.

9.7.2 Anzeige der Topologie-Erkennung

☐ Wählen Sie den Dialog `Diagnose:Topologie-Erkennung`.

Die Tabelle des Karteikartenreiters „LLDP“ zeigt Ihnen die gesammelten LLDP-Informationen zu Nachbargeräten an. Mit diesen Informationen ist eine Netzmanagement-Station in der Lage, die Struktur Ihres Netzes darzustellen.

Das Aktivieren der Einstellung „FDB-Einträge anzeigen“ unterhalb der Tabelle bietet Ihnen die Möglichkeit, die Tabelleneinträge um Einträge von Geräten ohne aktive LLDP-Unterstützung zu erweitern. Das Gerät nimmt in diesem Fall auch Informationen aus seiner FDB (Forwarding Database) auf.

Sind an einem Port, z.B. über einen Hub, mehrere Geräte angeschlossen, dann zeigt die Tabelle pro angeschlossenem Gerät eine Zeile an.

Wenn

- Geräte mit aktiver Topologie-Erkennungs-Funktion und
- Geräte ohne aktive Topologie-Erkennungs-Funktion an einem Port angeschlossen sind

dann

- blendet die Topologie-Tabelle die Geräte ohne aktive Topologie-Erkennung aus.

Wenn

- nur Geräte ohne aktive Topologie-Erkennung an einem Port angeschlossen sind

dann

- enthält die Tabelle stellvertretend für alle Geräte eine Zeile für diesen Port. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.
  MAC-Adressen von Geräten, die die Topologie-Tabelle übersichtshalber ausblendet, finden Sie in der Adress-Tabelle (FDB), (siehe auf Seite 158 „Statische Adresseinträge eingeben“).

9.8 IP-Adresskonflikte erkennen

9.8.1 Beschreibung von IP-Adresskonflikten

Per Definition darf jede IP-Adresse innerhalb eines Subnetzes nur einmal vergeben sein. Existieren innerhalb eines Subnetzes irrtümlicherweise 2 oder mehr Geräte mit der gleichen IP-Adresse, dann kommt es unweigerlich zur Unterbrechung der Kommunikation mit Geräten dieser IP-Adresse. Stuart Cheshire beschreibt in seinem Internet Draft einen Mechanismus, den industrielle Ethernet-Geräte benutzen können, um Adresskonflikte zu erkennen und zu beheben (Address Conflict Detection, ACD).

Modus	Bedeutung
enable	Aktive und passive Erkennung einschalten.
disable	Funktion ausschalten
activeDetectionOnly	Ausschließlich aktive Detektion einschalten. Das Gerät überprüft unmittelbar nach dem Anschluss an ein Netz oder nach einer Änderung der IP-Konfiguration, ob seine eigene IP-Adresse schon im Netz vorhanden ist. Ist die IP-Adresse bereits vorhanden, dann wechselt es, falls möglich, wieder zurück zur vorhergehenden Konfiguration und startet nach 15 Sekunden einen erneuten Versuch. Das Gerät vermeidet so, am Netzverkehr mit einer doppelten IP-Adresse teilzunehmen.
passiveOnly	Ausschließlich passive Detektion einschalten. Das Gerät lauscht passiv am Netz, ob seine IP-Adresse noch einmal vorhanden ist. Erkennt es eine doppelte IP-Adresse, dann verteidigt es mit Hilfe des ACD-Mechanismus´ zuerst seine Adresse durch Aussenden von Gratituous ARPs. Geht die Gegenstelle daraufhin nicht vom Netz, dann geht das Management-Interface des lokalen Gerätes vom Netz. Zyklisch nach 15 Sekunden startet es erneut eine Erkennung, ob der Adresskonflikt noch vorliegt. Falls nicht, geht es wieder ans Netz.

Tab. 30: Mögliche Adresskonflikt-Betriebsmodi

9.8.2 ACD konfigurieren

☐ Wählen Sie den Dialog Diagnose:IP-Adressen Konflikterkennung.
☐ Mit „Status“ schalten Sie die IP-Adressen Konflikterkennung ein/aus bzw. wählen Sie die Betriebsart (siehe Tabelle 30).

9.8.3 ACD anzeigen

☐ Wählen Sie den Dialog `Diagnose:IP-Adressen Konflikterkennung`.

▶ In der Tabelle protokolliert das Gerät IP-Adresskonflikte mit seiner IP-Adresse. Zu jedem Konflikt protokolliert das Gerät folgende Informationen:
  - ▶ die Uhrzeit (Spalte „Timestamp“),
  - ▶ die IP-Adresse, mit der der Konflikt bestand (Spalte „IP-Adresse“),
  - ▶ die MAC-Adresse des Gerätes, mit dem der IP-Adresskonflikt bestand (Spalte „Mac-Adresse“).

  Je IP-Adresse protokolliert das Gerät eine Zeile, und zwar die mit dem letzten Konflikt.

☐ Bei einem Neustart löscht das Gerät die Tabelle.

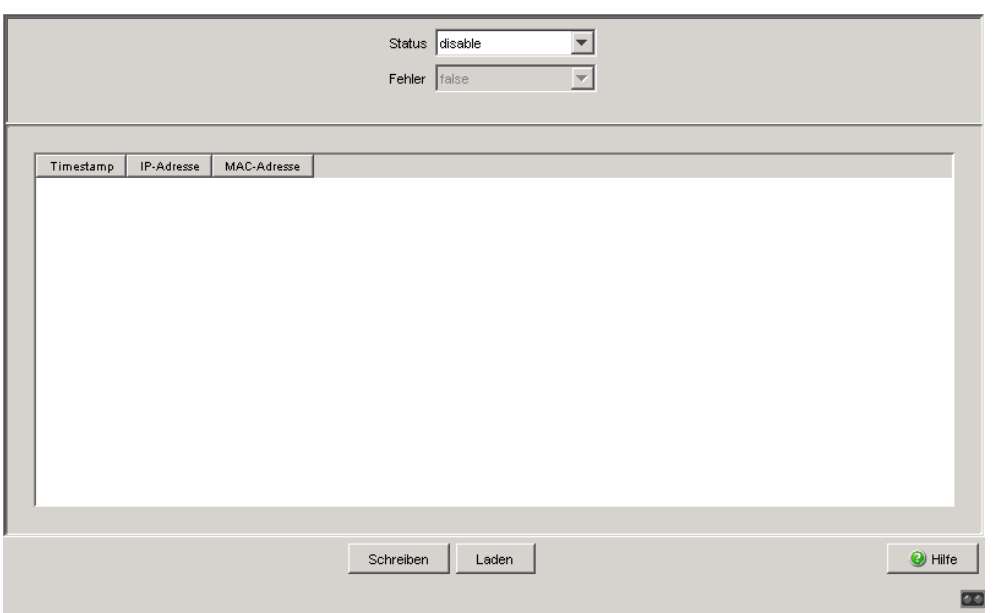


Abb. 54: Dialog IP-Adressen Konflikterkennung

9.9 Erkennen von Loops (Schleifen)

Loops (Schleifen) im Netz, auch vorübergehende, können Verbindungsunterbrechungen oder Datenverlust verursachen, die zu unbeabsichtigten Gerätevorgängen führen können. Die automatische Detektion und Meldung dieser Situation bietet Ihnen die Möglichkeit, diese rascher zu entdecken und leichter zu diagnostizieren.

Eine Fehlkonfiguration kann einen Loop verursachen, z.B., wenn Sie Spanning Tree abschalten.

Das Gerät bietet Ihnen die Möglichkeit, die Effekte zu erkennen, die Loops typischerweise bewirken, und diese Situation automatisch an die Netz-Management-Station zu melden. Dabei haben Sie die Möglichkeit, einzustellen, ab welchem Ausmaß der Loop-Effekte das Gerät eine Meldung verschickt.

Als typischer Effekt eines Loops können Frames von mehreren verschiedenen MAC-Quelladressen innerhalb kurzer Zeit an verschiedenen Ports des Gerätes eintreffen. Das Gerät wertet aus, wie viele derselben MAC-Quelladressen es innerhalb eines Zeitintervalls an verschiedenen Ports gelernt hat. Dieser Prozess erkennt Loops am Eintreffen der selben MAC-Adresse an verschiedenen Ports.
Umgekehrt kann das Eintreffen der selben MAC-Adresse an verschiedenen Ports auch andere Ursachen als einen Loop haben.

☐ Wählen Sie den Dialog `Switching:Switching Global`.

☐ Markieren Sie „Address Relearn Detection aktivieren“. Geben Sie im Feld „Address Relearn Threshold“ den gewünschten Schwellwert ein.

Bei aktivierter Address Relearn Detection prüft das Gerät, ob es wiederholt die selben MAC-Quell-Adressen an verschiedenen Ports gelernt hat. Dieser Vorgang weist mit großer Wahrscheinlichkeit auf eine Loop- (Schleifen-) Situation hin.
Erkennt das Gerät, dass an seinen Ports der eingestellte Schwellwert für die MAC-Adressen während des Auswertungs-Intervalls (wenige Sekunden) überschritten wurde, erzeugt das Gerät einen Eintrag in der Log-Datei und sendet einen Alarm (Trap). Der voreingestellte Schwellwert ist 1.

9.10 Berichte

Folgende Berichte und Bedientasten stehen zur Diagnose zur Verfügung:

- Logdatei.
  Die Logdatei ist eine HTML-Datei, in die das Gerät alle wichtigen geräteinternen Ereignisse schreibt.
- Systeminformation.
  Die Systeminformation ist eine HTML-Datei, die alle systemrelevanten Daten enthält.
- Download Support Informationen.
  Diese Bedientaste bietet Ihnen die Möglichkeit, Systeminformationen als Dateien in einem ZIP-Archiv herunterzuladen.

Diese Berichte geben im Service-Fall dem Techniker die notwendigen Informationen.

Die folgende Bedientaste steht zur alternativen Bedienung des Web-based Interface zur Verfügung:

- Download JAR-Datei.
  Diese Bedientaste bietet Ihnen die Möglichkeit, das Applet des Web-based Interface als JAR-Datei herunterzuladen. Sie haben danach die Möglichkeit, das Applet außerhalb eines Browsers zu starten.
  Dies ermöglicht Ihnen die Administration des Gerätes auch dann, wenn Sie dessen Web-Server aus Sicherheitsgründen abgeschaltet haben.

☐ Um die HTML-Datei mit systemrelevanten Daten anzuzeigen, wählen Sie den Dialog `Diagnose:Bericht:System Information`.
☐ Um die Logdatei mit wichtigen geräteinternen Ereignissen anzuzeigen, wählen Sie den Dialog `Diagnose:Bericht:Event Log`.

☐ Wählen Sie den Dialog `Diagnose:Bericht`.

☐ Klicken Sie auf „Download Switch-Dump“.

☐ Wählen Sie das Verzeichnis aus, in dem Sie den Switch-Dump speichern möchten.

☐ Klicken Sie auf „Speichern“.

Das Gerät erzeugt den Dateinamen des Switch-Dumps automatisch nach dem Muster <IP-Adresse>_<Systemname>.zip, für ein Gerät vom Typ PowerMICE z.B. „10.0.1.112_PowerMICE-517A80.zip“.

☐ Klicken Sie auf „Download JAR-File“.

☐ Wählen Sie das Verzeichnis aus, in dem Sie das Applet speichern möchten.

☐ Klicken Sie auf „Speichern“.

Das Gerät erzeugt den Dateinamen des Applets automatisch nach dem Muster <Gerätetyp><Software-Variante><Software-Version)>_<Software-Revision des Applets>.jar, für ein Gerät von Typ PowerMICE mit der Software-Variante L3P z.B. „pmL3P06000_00.jar“.

9.11 Datenverkehr von Ports beobachten (Port-Mirroring)

Die Geräte MACH4002 24/48 + 4G und Power MICE unterstützen bis zu 8 Ports.

Die Funktion Port-Mirroring bietet Ihnen die Möglichkeit, den Datenverkehr einer Gruppe von Ports des Gerätes zu Diagnosezwecken zu untersuchen (N:1). Dabei leitet das Gerät die Daten dieser Ports an einen anderen Port weiter; es spiegelt sie. Dieses Verfahren heißt Port-Mirroring.
Die Ports, deren Daten das Gerät kopiert, sind die Quellports. Der Port, an dem die Daten eingehen, ist der Zielport. Physikalische Ports sind als Quell- oder Zielports verwendbar.

Beim Port-Mirroring kopiert das Gerät gültige Datenpakete vom Quellport auf den Zielport. Der Datenverkehr an den Quellports bleibt dadurch unbeeinflusst.
Ein am Zielport angeschlossenes Management-Werkzeug, wie z.B. eine RMON-Probe, kann so den Datenverkehr der Quellports in Sende- und Empfangsrichtung beobachten.

Wenn Sie für einen Quell-Port „RX“ als Überwachungsrichtung festlegen, kopiert/spiegelt das Gerät ausschließlich am Quellport empfangene Frames an den Zielport (Eingangsüberwachung).
Wenn Sie für einen Quell-Port „TX“ als Überwachungsrichtung festlegen, kopiert/spiegelt das Gerät ausschließlich am Quellport gesendete Frames an den Zielport (Ausgangsüberwachung).

Ein aktiviertes Port-Mirroring veranlasst das Gerät, den Datenverkehr, der über einen Quell-Port empfangen und/oder weitergeleitet wurde, an den Ziel-Port zu kopieren.

Die Geräte PowerMICE und MACH4000 nutzen ausschließlich den Ziel-Port für das Port-Mirroring. Der Quell-Port empfängt und leitet den Datenverkehr ganz normal weiter.

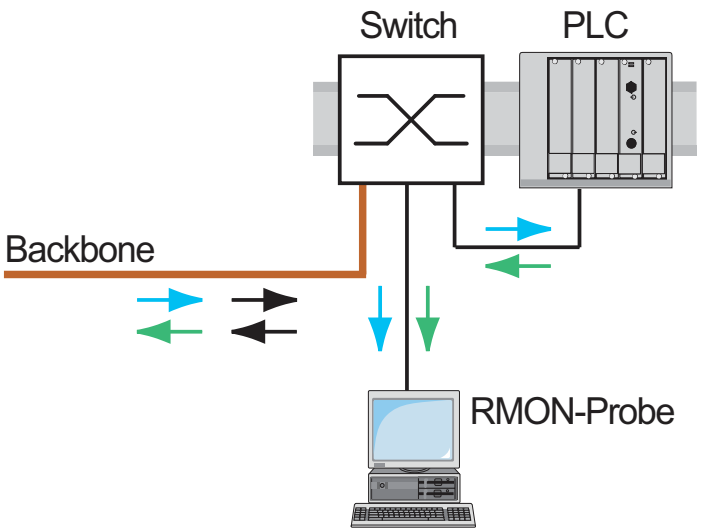


Abb. 55: Port-Mirroring

☐ Wählen Sie den `Dialog Diagnose:Portmirroring`.

Dieser Dialog bietet Ihnen die Möglichkeit, die Port-Mirroring-Funktion des Gerätes zu konfigurieren und zu aktivieren.

- ☐ Wählen Sie die Quell-Ports, deren Datenverkehr sie beobachten möchten, aus der Liste der physikalischen Ports aus, indem Sie die entsprechenden Kästchen markieren.
  Das Gerät stellt den „Quell-Port“ in der Tabelle ausgegraut dar, der sich momentan als „Ziel-Port“ in Verwendung befindet. Voreinstellung: keine Quellports.
- ☐ Wählen Sie den Ziel-Port, an dem Sie Ihr Management-Werkzeug angeschlossen haben, im Ausklappmenü im Rahmen „Ziel-Port“ aus. Die Auswahl eines Ziel-Ports ist für eine gültige Port-Mirroring-Konfiguration unerlässlich. Das Ausklappmenü zeigt ausschließlich die verfügbaren Ports an; Ports, die momentan als Quell-Ports in Benutzung sind, schließt die Liste z. B. aus. Voreinstellung: Port – (kein Ziel-Port).
- ☐ Um die zu überwachende Richtung des Datenverkehrs festzulegen, aktivieren Sie die relevanten Kästchen „RX“ und „TX“ für die eingehenden und die ausgehenden Überwachungsrichtungen.
- ☐ Um die Funktion einzuschalten, wählen Sie `An` im Rahmen `Funktion`. Voreinstellung: `Aus`.

Die Bedientaste „Konfiguration zurücksetzen“ im Dialog bietet Ihnen die Möglichkeit, alle Port-Mirroring-Einstellungen des Gerätes in den Lieferzustand zurückzuversetzen.

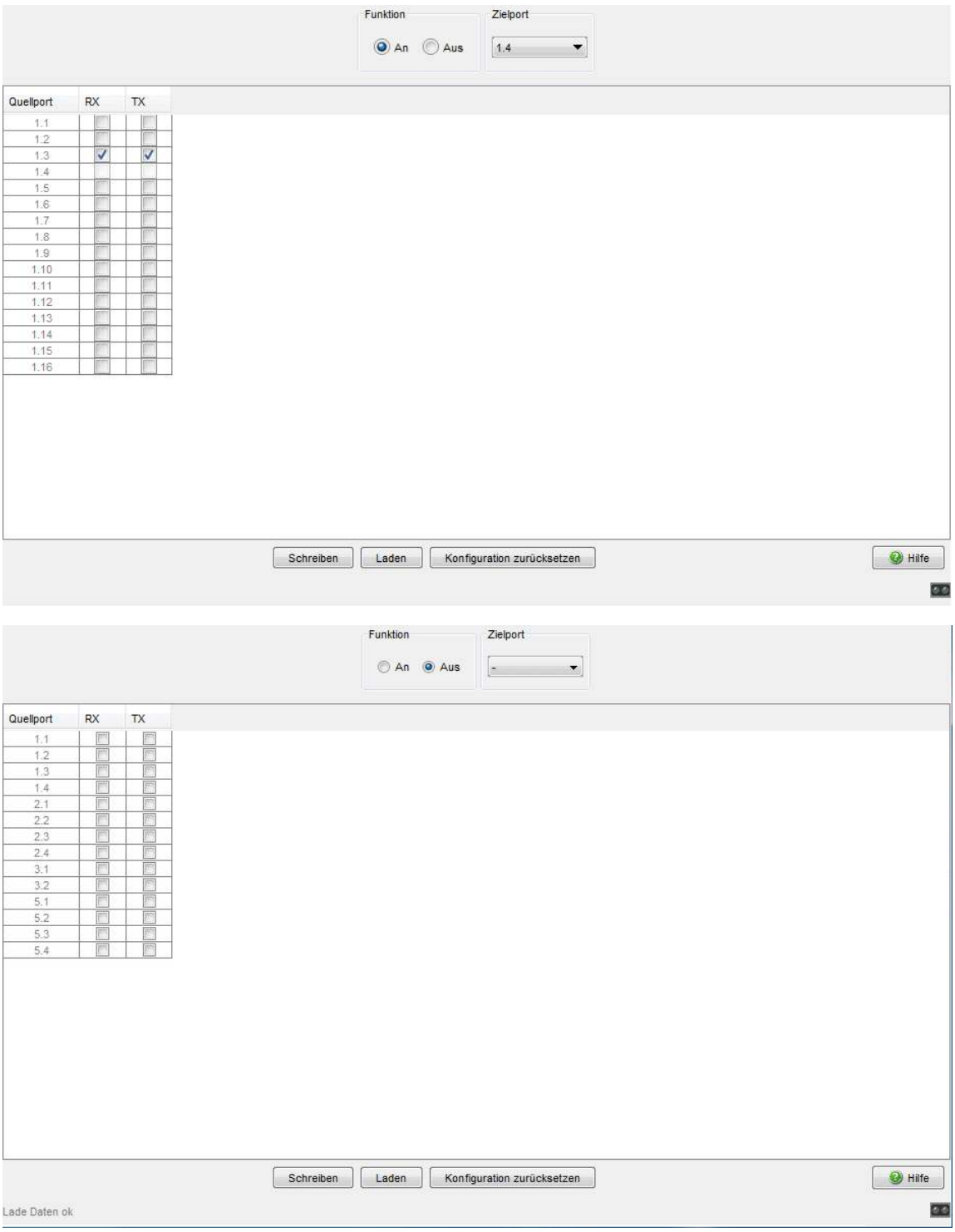


Abb. 56: Dialog Port-Mirroring

9.12 Syslog

Das Gerät bietet Ihnen die Möglichkeit, Meldungen über wichtige Geräte-interne Ereignisse an einen oder mehrere Syslog-Server zu schicken (bis zu 8). Außerdem können Sie SNMP-Anfragen an das Gerät ebenfalls als Ereignisse in den Syslog aufnehmen.

Anmerkung: Die Ereignisse selbst, die das Gerät geloggt hat, finden Sie im Dialog „Ereignis-Log“ (siehe auf Seite 261 „Trap-Log“) und in der Log-Datei (siehe auf Seite 252 „Berichte“), einer HTML-Seite mit dem Titel „Event-Log“.

- ☐ Wählen Sie den Dialog `Diagnose:Syslog`.

- ☐ Schalten Sie im Rahmen „Funktion“ die Syslog-Funktion an.
- ☐ Klicken Sie auf „Erzeugen“.
- ☐ In der Spalte „IP-Adresse“ geben Sie die IP-Adresse des Syslog-Servers an, an den die Log-Einträge geschickt werden sollen.
- ☐ In der Spalte „Port“ geben Sie den UDP-Port des Syslog-Servers an, auf dem dieser Log-Einträge annimmt. Die Voreinstellung ist 514.
- ☐ In der Spalte „Mindest-Schweregrad“ geben Sie den Mindest-Schweregrad an, den ein Ereignis haben muss, damit das Gerät einen Log-Eintrag an diesen Syslog-Server versendet.
- ☐ In der Spalte „Aktiv“ kreuzen Sie die Syslog-Server an, die das Gerät beim Versenden von Logs berücksichtigt.

Rahmen „SNMP-Logging“:

- ☐ Aktivieren Sie „Log SNMP-Get-Request“, wenn Sie lesende SNMP-Anfragen an das Gerät als Ereignisse an den Syslog-Server senden möchten.
- ☐ Wählen Sie den Schweregrad aus, mit dem das Gerät die Ereignisse aus lesenden SNMP-Abfragen erzeugt.
- ☐ Aktivieren Sie „Log SNMP-Set-Request“, wenn Sie schreibende SNMP-Anfragen an das Gerät als Ereignisse an den Syslog-Server senden möchten.
- ☐ Wählen Sie den Schweregrad aus, mit dem das Gerät die Ereignisse aus schreibenden SNMP-Abfragen erzeugt.

Anmerkung: Weitere Details zur Einstellung des SNMP-Loggings finden Sie im Dokument „Referenz-Handbuch GUI“ (Graphical User Interface / Web-based Interface), im Kapitel „Syslog“.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging host 10.0.1.159 514 3`	Wählt den Empfänger der Log-Meldungen und dessen Port 514 aus. Die „3“ gibt den Schweregrad der Meldung an, die das Gerät schickt. „3“ bedeutet „Fehler“.
`logging syslog`	Schaltet die Syslog-Funktion ein.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show logging hosts`	Zeigt die Syslog-Host-Einstellungen.

```
Index     IP Address       Severity   Port     Status
-----  ----------------  ----------  ----  -------------
1      10.0.1.159         error       514   Active
```

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging snmp-requests get operation enable`	Erzeugt aus lesenden SNMP-Anfragen Log-Ereignisse.
`logging snmp-requests get severity 5`	Die „5“ gibt den Schweregrad der Meldung an, die das Gerät Meldungen aus lesenden SNMP-Anfragen zuordnet. „5“ bedeutet „Hinweis“.
`logging snmp-requests set operation enable`	Erzeugt aus schreibenden SNMP-Anfragen Log-Ereignisse.
`logging snmp-requests set severity 5`	Die „5“ gibt den Schweregrad der Meldung an, die das Gerät Meldungen aus schreibenden SNMP-Anfragen zuordnet. „5“ bedeutet „Hinweis“.

```
exit
show logging snmp-requests
Log SNMP SET requests                : enabled
Log SNMP SET severity                : notice
Log SNMP GET requests                : enabled
Log SNMP GET severity                : notice
```

Wechsel in den Privileged-EXEC-Modus.
Zeigt die SNMP-Logging-Einstellungen an.

9.13 Trap-Log

Das Gerät bietet Ihnen die Möglichkeit, einen Log der Systemereignisse abzurufen. Die Tabelle des Dialogs „Trap-Log“ listet die geloggten Ereignisse mit Zeitstempel auf.

- ☐ Klicken Sie auf „Laden“, um den Inhalt des Trap-Logs zu aktualisieren.
- ☐ Klicken Sie auf „Löschen“, um den Inhalt des Trap-Logs zu löschen.

Anmerkung: Sie haben die Möglichkeit, die geloggten Ereignisse zusätzlich an einen oder mehrere Syslog-Server zu senden (siehe auf Seite 258 „Syslog“).

9.14 MAC-Benachrichtigung

Die MAC-Benachrichtigung, auch als MAC-Adressänderungsbenachrichtigung bekannt, überwacht die Nutzer eines Netzes dadurch, dass sie Änderungen von MAC-Adressen speichert. Wenn der Switch eine MAC-Adresse lernt oder entfernt, sendet das Gerät einen SNMP-Trap an eine konfigurierte Trap-Zieladresse. Das Gerät erzeugt MAC-Adressänderungsbenachrichtigungen für dynamische Unicast-MAC-Adressen.

Der Gerätepuffer enthält bis zu 20 Adressen. Wenn der Puffer vor Ablauf der benutzerdefinierten Zeitspanne voll ist, sendet das Gerät einen Trap an die Managementstation.

Diese Funktion ist ausschließlich für Ports gedacht, an denen Endgeräte angeschlossen sind und sich demzufolge die MAC-Adresse selten ändert.

- ☐ Öffnen Sie den Dialog `Diagnose:MAC-Benachrichtigung`.
- ☐ Legen Sie über die Spalte „Modus“ fest, für welche Aktion das Gerät einen Trap sendet.
- ☐ Um die Ports auszuwählen, für die das Gerät einen Trap sendet, aktivieren Sie das Kontrollkästchen in der Spalte „Aktiv“ column.
- ☐ Geben Sie im Eingabefeld „Intervall [s]“ ist Zahl der Sekunden an, die zwischen der Übertragung zweier Traps verstreicht.
- ☐ Klicken Sie zum Aktivieren der Funktion `An` im Rahmen „Funktion“.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mac notification interval 20`	Setzen Sie das Intervall für die MAC-Benachrichtigung auf 20 Sekunden.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1/1.
`mac notification mode`	Setzten Sie den Modus, für den das Gerät eine MAC-Benachrichtigung versendet.
`mac notification operation`	Aktivieren Sie das Versenden von MAC-Benachrichtigungs-Alarmen für diesen Port.

`exit`	Wechsel in den Konfigurationsmodus.
`mac notification operation`	Aktivieren Sie die MAC-Benachrichtigungs-Funktion global.

A Konfigurationsumgebung einrichten

A.1 DHCP/BOOTP-Server einrichten

Auf der Produkt-CD, die dem Gerät bei der Lieferung beiliegt, finden Sie die Software für einen DHCP-Server der Firma Softwareentwicklung, IT-Consulting Dr. Herbert Hanewinkel. Sie können die Software bis zu 30 Kalendertage nach dem Datum der ersten Installation testen, um zu entscheiden, ob Sie eine Lizenz erwerben wollen.

☐ Zur Installation des DHCP-Servers auf Ihrem PC legen Sie die Produkt-CD in das CD-Laufwerk Ihres PCs und wählen Sie unter Zusatzsoftware "haneWIN DHCP-Server". Führen Sie die Installation gemäß des Installationsassistenten durch.

☐ Starten Sie das Programm `DHCP Server`.

Abb. 57: Startfenster des DHCP-Servers

Anmerkung: Die Installation beinhaltet einen Dienst, der in der Grundkonfiguration automatisch beim Einschalten von Windows gestartet wird.
Dieser Dienst ist auch aktiv, wenn das Programm selbst nicht gestartet ist.
Der gestartete Dienst beantwortet DHCP-Anfragen.

☐ Öffnen Sie das Fenster für die Programmeinstellungen in der Menüleiste: `Optionen:Einstellungen` und wählen Sie die Karteikarte `DHCP`.
☐ Nehmen Sie die im Bild dargestellten Einstellungen vor und klicken Sie auf `OK`.

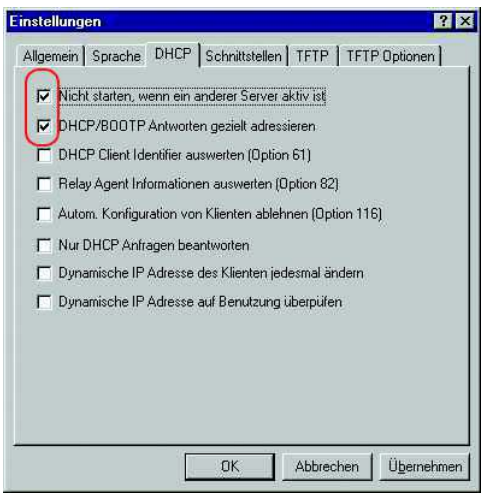


Abb. 58: DHCP-Einstellung

☐ Zur Eingabe der Konfigurationsprofile wählen Sie in der Menüleiste `Optionen:Konfigurationsprofile verwalten`.
☐ Geben Sie den Namen für das neue Konfigurationsprofil ein und klicken Sie auf `Hinzufügen`.

Abb. 59: Konfigurationsprofile hinzufügen

☐ Geben Sie die Netzmaske ein und klicken Sie auf `Übernehmen`.

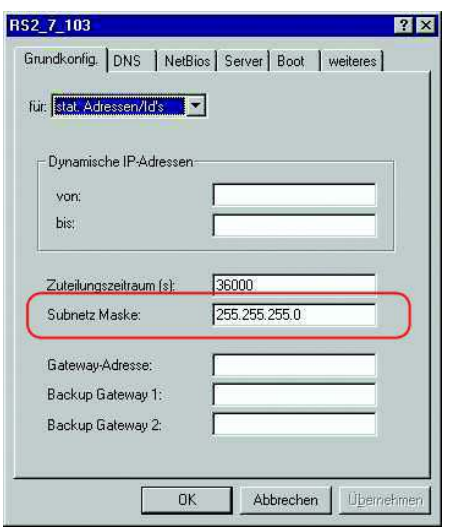


Abb. 60: Netzmaske im Konfigurationsprofil

☐ Wählen Sie die Karteikarte `Boot`.
☐ Geben Sie die IP-Adresse Ihres tftp-Servers.
☐ Geben Sie den Pfad und den Dateinamen für die Konfigurationsdatei ein.
☐ Klicken Sie auf `Übernehmen` und danach auf `OK`.

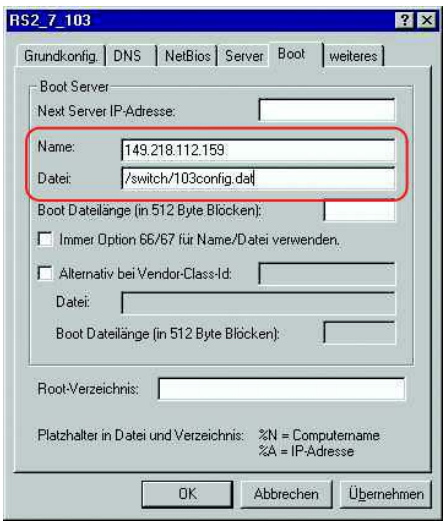


Abb. 61: Konfigurationsdatei auf dem tftp-Server

☐ Fügen Sie für jeden Gerätetyp ein Profil hinzu.
Haben Geräte des gleichen Typs unterschiedliche Konfigurationen, dann fügen Sie für jede Konfiguration ein Profil hinzu.
Zum Beenden des Hinzufügens der Konfigurationsprofile klicken Sie auf `OK`.

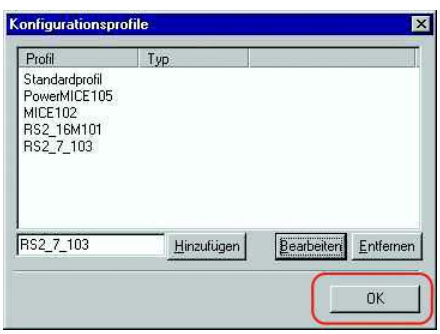


Abb. 62: Konfigurationsprofile verwalten

☐ Zur Eingabe der statischen Adressen klicken Sie im Hauptfenster auf `Statisch`.

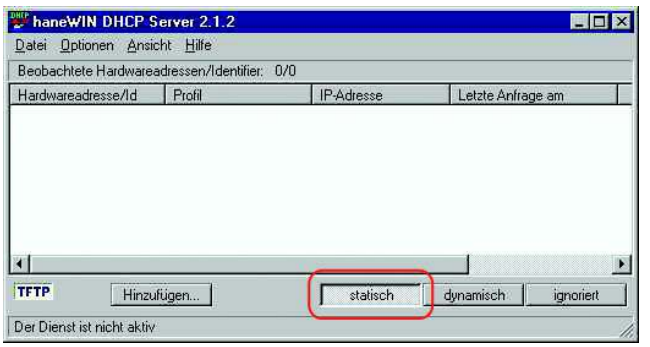


Abb. 63: Statische Adresseingabe

☐ Klicken Sie auf `Hinzufügen`.

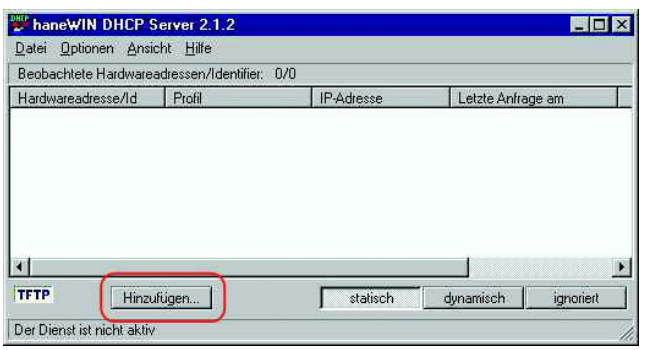


Abb. 64: Statische Adressen hinzufügen

☐ Geben Sie die MAC-Adresse des Gerätes ein.
☐ Geben Sie die IP-Adresse des Gerätes ein.
☐ Wählen Sie das Konfigurationsprofil des Gerätes.
☐ Klicken Sie auf `Übernehmen` und danach auf `OK`.

Abb. 65: Einträge für statische Adressen

☐ Fügen Sie für jedes Gerät, das vom DHCP-Server seine Parameter erhalten soll, einen Eintrag hinzu.

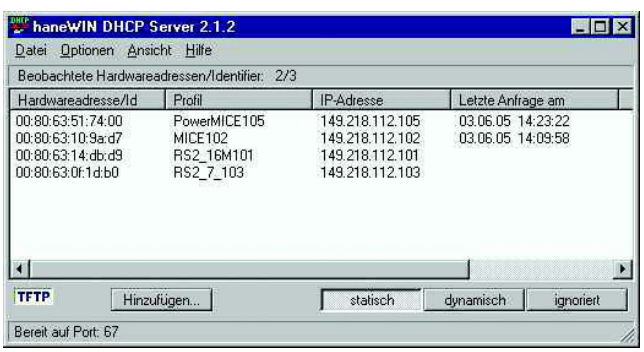


Abb. 66: DHCP-Server mit Einträgen

A.2 DHCP-Server Option 82 einrichten

Auf der Produkt-CD, die dem Gerät bei der Lieferung beiliegt, finden Sie die Software für einen DHCP-Server der Firma Softwareentwicklung, IT-Consulting Dr. Herbert Hanewinkel. Sie können die Software bis zu 30 Kalendertage nach dem Datum der ersten Installation testen, um zu entscheiden, ob Sie eine Lizenz erwerben wollen.

☐ Zur Installation des DHCP-Servers auf Ihrem PC legen Sie die Produkt-CD in das CD-Laufwerk Ihres PCs und wählen Sie unter Zusatzsoftware "haneWIN DHCP-Server". Führen Sie die Installation gemäß des Installationsassistenten durch.

☐ Starten Sie das Programm `DHCP Server`.

Abb. 67: Startfenster des DHCP-Servers

Anmerkung: Die Installation beinhaltet einen Dienst, der in der Grundkonfiguration automatisch beim Einschalten von Windows gestartet wird. Dieser Dienst ist auch aktiv, wenn das Programm selbst nicht gestartet ist. Der gestartete Dienst beantwortet DHCP-Anfragen.

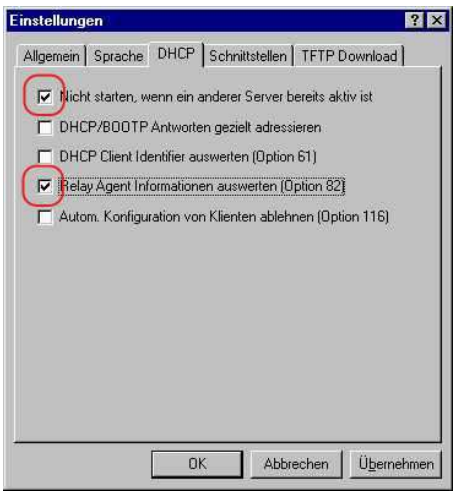


Abb. 68: DHCP-Einstellung

☐ Zur Eingabe der statischen Adressen klicken Sie auf `Hinzufügen`.

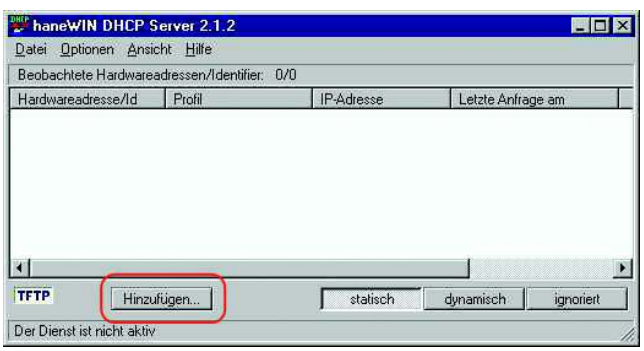


Abb. 69: Statische Adressen hinzufügen

☐ Wählen Sie `Circuit Identifier` und `Remote Identifier`.

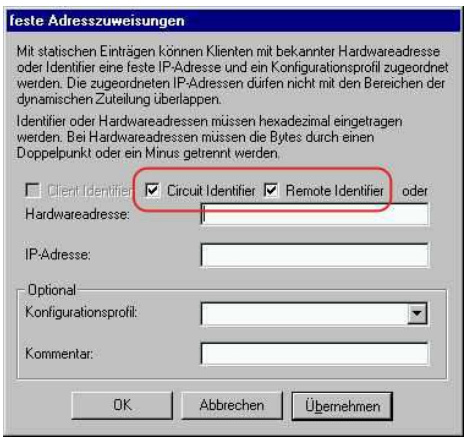


Abb. 70: Voreinstellung für die feste Adresszuweisung

☐ Tragen Sie in das Feld `Hardwareadresse` den `Circuit Identifier` und den `Remote Identifier` ein, siehe “DHCP Relay Agent” im Referenz-Handbuch "Web-based Interface").
Mit `Hardwareadresse` kennzeichnen Sie das Gerät und den Port, an welchen ein Gerät angeschlossen wird, dem Sie die `IP-Adresse` in der Zeile darunter zuweisen wollen.

Die Hardwareadresse hat folgende Form:

ciclhhvvvvssmmpprirlxxxxxxxxxxxx

- ci: Subidentifier für Typ des Circuit-ID
- cl: Länge des Circuit-ID
- hh: Hirschmann-Identifier: 01, wenn an dem Port ein Hirschmann-Gerät angeschlossen wird, sonst 00.
- vvvv: VLAN ID der DHCP-Anfrage (Voreinstellung: 0001 = VLAN 1)
- ss: Steckplatz im Gerät, auf dem sich das Modul mit dem Port befindet, an dem das Gerät angeschlossen wird. Geben Sie den Wert 00 an.
- mm: Modul mit dem Port, an dem das Gerät angeschlossen wird.
- pp: Port an dem das Gerät angeschlossen wird.
- ri: Subidentifier für Typ des Remote-ID
- rl: Länge des Remote-ID
- xxxxxxxxxxxx: Remote-ID des Gerätes (z.B. MAC-Adresse), an dem ein Gerät angeschlossen wird.

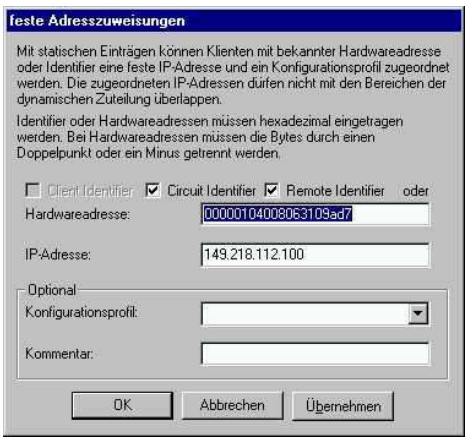


Abb. 71: Eintragen der Adressen

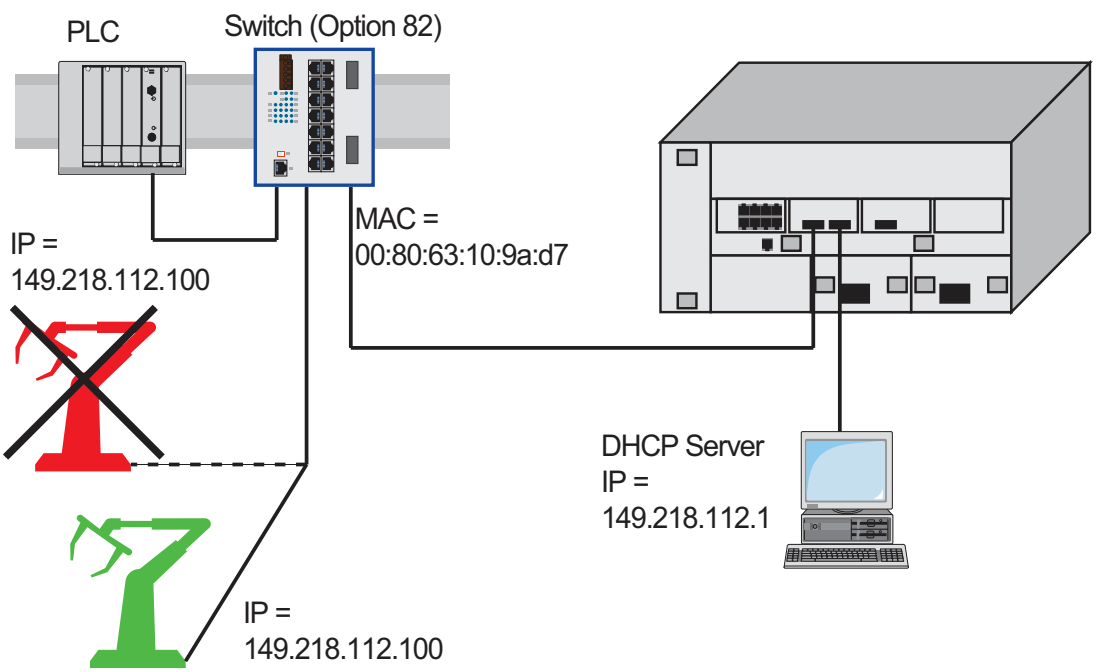


Abb. 72: Anwendungsbeispiel für den Einsatz von Option 82

A.3 TFTP-Server für SW-Updates

Im Lieferzustand steht die Geräte-Software im lokalen Flash-Speicher. Das Gerät bootet die Software vom Flash-Speicher.
Über einen tftp-Server können Software-Updates durchgeführt werden. Dies setzt voraus, daß im angeschlossenen Netz ein tftp-Server installiert und aktiv ist.

Anmerkung: Eine Alternative zum tftp-Update bildet das http-Update. Das http-Update erspart die Konfiguration des tftp-Servers.

Um vom tftp-Server einen Software-Update durchführen zu können benötigt das Gerät folgende Informationen:
- eigene IP-Adresse (fest eingetragen),
- IP-Adresse des tftp-Servers, bzw. des Gateways zum tftp-Server,
- Pfad, der den Speicherort der neuen Geräte-Software auf dem tftp-Server bezeichnet.

Der File-Transfer zwischen Gerät und tftp-Server wird über das Trivial File Transfer Protocol (tftp) abgewickelt.

Managementstation und tftp-Server können sowohl aus einem als auch aus verschiedenen Rechnern bestehen.

Das Vorbereiten des tftp-Servers für die Geräte-Software beinhaltet die Schritte:
- Einrichten des Geräte-Verzeichnisses und Kopieren der Geräte-Software
- Einrichten des tftp-Prozesses

A.3.1 tftp-Prozess einrichten

Allgemeine Voraussetzungen:

- Die lokale IP-Adresse des Gerätes und die IP-Adresse des tftp-Servers bzw. des Gateways sind dem Gerät bekannt.
- Der TCP/IP-Stack mit tftp ist auf dem tftp-Server installiert.

Die folgenden Abschnitte enthalten Hinweise zum Einrichten des tftp-Prozesses gegliedert nach Betriebssystemen und Anwendungen.

SunOS und HP

☐ Überprüfen Sie zunächst, ob der tftp-Dämon (Hintergrundprozess) läuft, d.h. ob in der Datei /etc/inetd.conf folgende Zeile enthalten ist (siehe Abbildung 73) und dessen Prozessstatus „IW“ ist:

SunOS

```
tftp dgram udp wait root /usr/etc/in.tftpd in.tftpd -
s /tftpboot
```

HP

```
tftp dgram udp wait root /usr/etc/in.tftpd tftpd
```

Falls dieser Prozess nicht oder nur als Kommentarzeile (#) eingetragen ist, ändern Sie /etc/inetd.conf entsprechend und führen danach eine Neuinitialisierung des INET-Dämon durch. Dies geschieht mit dem Befehl „kill -1 PID“, wobei PID die Prozessnummer von inetd ist.
Durch Eingabe der folgenden UNIX-Befehlszeile wird diese Neuinitialisierung automatisch durchgeführt:

SunOS

```
ps -ax | grep inetd | head -1 | awk -e {print $1} |
kill -1
```

HP

```
/etc/inetd -c
```

Eine zusätzliche Information zum tftp-Dämon tftpd können Sie mit dem UNIX-Kommando „man tftpd“ abrufen.

Anmerkung: Der tftp-Dämon wird nicht immer mit dem Befehl „`ps`“ angezeigt, obwohl er läuft.

Besonderheit bei HP-Workstations:

☐ Tragen Sie bei der Installation auf einer HP-Workstation in die Datei /etc/passwd den Benutzer tftp ein.

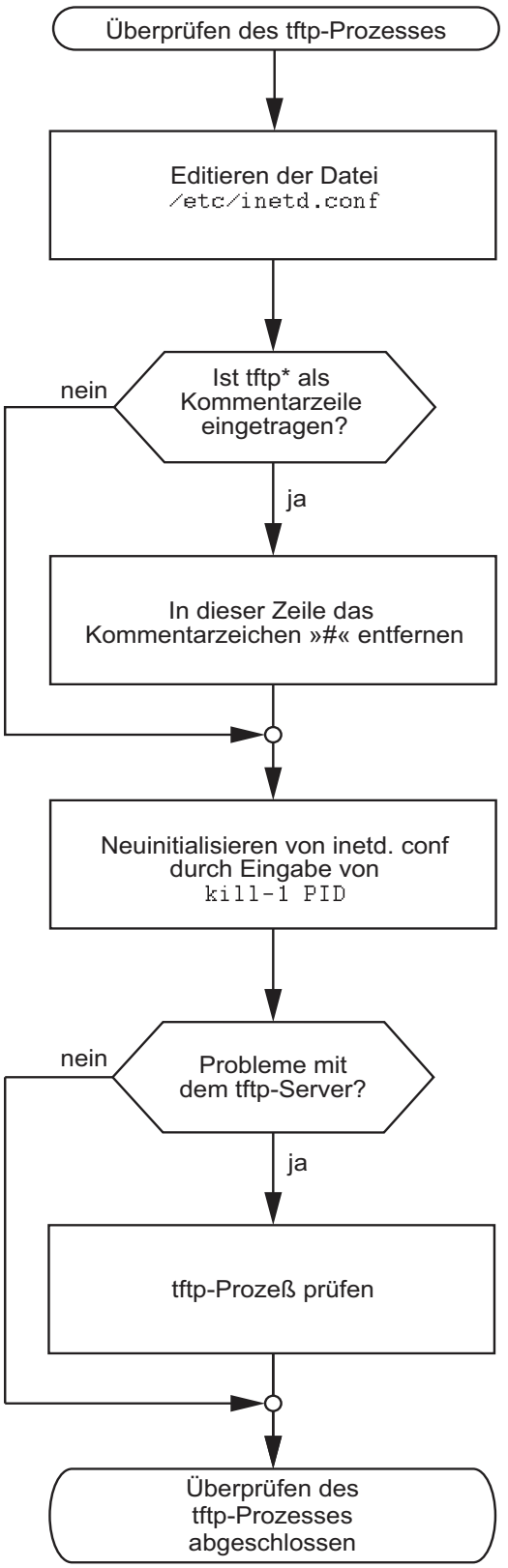
Zum Beispiel:

```
tftp:*:510:20:tftp server:/usr/tftpdir:/bin/false
```

`tftp`Benutzerkennung,
`*` steht im Passwortfeld,
`510` Beispiel für die user-Nr.,
`20` Beispiel für die group-Nr.,
`tftp server` frei wählbare sinnvolle Bezeichnung,
`/bin/false` obligatorischer Eintrag (login shell)

☐ Testen Sie den tftp-Prozeß mit z. B.: `cd /tftpboot/device`

```
tftp <tftp-Servername>
get device/device.bin
rm device.bin
```



z. B:

```
cd /tftpboot/device
tftp <tftp-Servername>
get device/device.bin
```

Antwort, wenn der Prozeß läuft: `Received ...`

```
rm device.bin
```

* `tftp dgram udp wait root/usr/etc/in.tftpd in.tftpd /tftpboot`

Abb. 73: Ablaufdiagramm tftp-Server einrichten bei SunOS und HP

A.3.2 Software-Zugriffsrechte

Der Agent benötigt Leserecht auf dem tftp-Verzeichnis, in das die Geräte-Software abgelegt ist.

Beispiel für einen tftp-Server unter UNIX

Nach der Installation der Geräte-Software sollte sich folgende Verzeichnis-Struktur mit den angegebenen Zugriffsrechten auf dem tftp-Server befinden:.

Dateiname	Rechte
device.bin	-rw-r--r--

Tab. 31: Verzeichnisstruktur der Software

l = Link; d = Verzeichnis; r = lesen; w = schreiben; x = durchführen
1. Stelle bezeichnet den Dateityp (- = normale Datei),
2. bis 4. Stelle bezeichnen die Zugriffsrechte des Benutzers,
5. bis 7. Stelle bezeichnen die Zugriffsrechte von Benutzern anderer Gruppen,
8. bis 10. Stelle bezeichnen die Zugriffsrechte aller anderen Benutzer.

A.4 SSH-Zugriff vorbereiten

Um über SSH auf das Gerät zuzugreifen, führen Sie die folgenden Schritte aus:

- Erzeugen Sie einen Schlüssel (SSH-Host-Key).
- Installieren Sie den Schlüssel auf dem Gerät.
- Geben Sie auf dem Gerät den Zugriff über SSH frei.
- Installieren Sie ein Programm zum Ausführen des SSH-Protokolls (SSH-Client) auf Ihrem Rechner.

A.4.1 Schlüssel erzeugen

Das Gerät bietet Ihnen die Möglichkeit, für den SSH-Server eigene, selbst-generierte Schlüssel zu verwenden. Wenn auf dem Gerät kein SSH-Schlüssel vorhanden ist, erzeugt das Gerät die erforderlichen Schlüssel automatisch beim ersten Einschalten des SSH-Servers.

Eine Möglichkeit den Schlüssel zu erzeugen, bietet das Programm PuTTYgen. Dieses Programm finden Sie auf der Produkt-CD.

☐ Starten Sie das Programm mit einem Doppelklick.
☐ Wählen Sie im Rahmen „Parameter" den Typ des zu generierenden Schlüssels.
  ☐ Um einen Schlüssel für SSH-Version 2 zu generieren, wählen Sie „SSH-2 (RSA)“ oder „SSH-2 (DSA)“.
  ☐ Um einen Schlüssel für SSH-Version 1 zu generieren, wählen Sie „SSH-1 (RSA)“.
☐ Vergewissern Sie sich, dass das Feld „Number of bits in a generated key“ im Rahmen „Parameters“ den Wert `1024` zeigt.
☐ Klicken Sie im Rahmen „Actions" auf „Generate". Bewegen Sie die Maus über dem PuTTYgen-Fenster, damit PuTTYgen mit Zufallszahlen den Schlüssel berechnen kann.
☐ Lassen Sie die Eingabefelder „Key passphrase" und „Confirm passphrase" leer.

- ☐ Speichern Sie den Schlüssel:
  - ☐ Um einen Schlüssel für SSH-Version 2 zu speichern, klicken Sie im Menü `Conversions:Export OpenSSH key`.
  - ☐ Um einen Schlüssel für SSH-Version 1 zu speichern, klicken Sie im Rahmen „Actions“ die Schaltfläche „Save private key“.
- ☐ Beantworten Sie die Frage, ob Sie den Schlüssel ohne „passphrase“ speichern wollen mit „Ja“ .
- ☐ Geben Sie den Speicherort und den Dateinamen der Schlüsseldatei ein.
- ☐ Notieren Sie sich den Fingerabdruck des Schlüssels, damit Sie ihn beim Verbindungsaufbau überprüfen können.
- ☐ Bewahren Sie den Schlüssel zusätzlich getrennt vom Gerät auf, damit Sie ihn beim Austausch des Geräts auf das Ersatzgerät übertragen können.

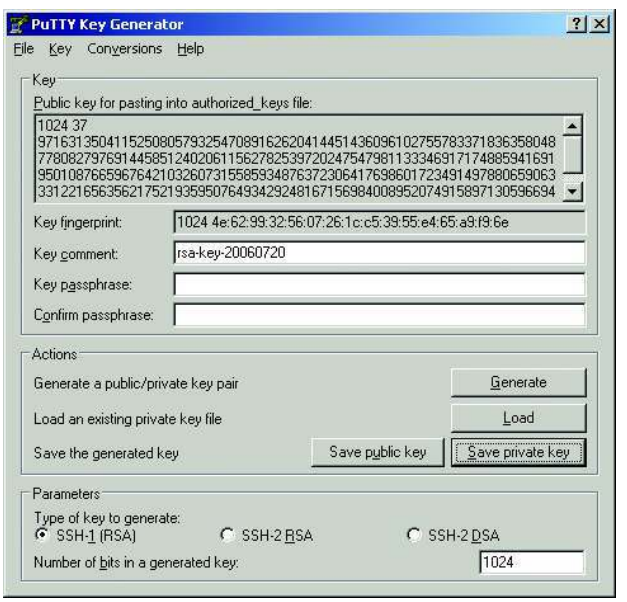


Abb. 74: PuTTY Schlüsselgenerator

Erfahrenen Netzadministratoren bietet die OpenSSH-Suite eine weitere Möglichkeit, den Schlüssel zu erzeugen. Zur Erzeugung des Schlüssels geben Sie folgenden Befehl ein:

```
ssh-keygen(.exe) -q -t rsa1 -f rsa1.key -C '' -N ''
```

A.4.2 Schlüssel auf das Gerät laden

Die SSH-Schlüssel laden Sie mit dem Command Line Interface per TFTP auf das Gerät.

SSH-Version 1 arbeitet mit einem RSA-Schlüssel. SSH-Version 2 dagegen arbeitet mit einem RSA- und einem DSA-Schlüssel. Laden Sie für SSH-Version 2 immer beide Schlüssel auf das Gerät.

☐ Legen Sie die Schlüssel auf Ihren tftp-Server.

☐ Laden Sie die Schlüssel vom tftp-Server auf das Gerät.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`no ip ssh`	SSH-Server ausschalten.
`copy tftp://ip/filepath/key nvram:sshkey-rsa2`	Lädt den Schlüssel in den nicht-flüchtigen Speicher des Gerätes. ▶ `nvram:sshkey-rsa2` ist der Speicherort des RSA-Schlüssels für SSH-Version 2.
`copy tftp://ip/filepath/key nvram:sshkey-dsa`	▶ `nvram:sshkey-dsa` ist der Speicherort des DSA-Schlüssels für SSH-Version 2.
`copy tftp://ip/filepath/key nvram:sshkey-rsa1`	▶ `nvram:sshkey-rsa1` ist der Speicherort des RSA-Schlüssels für SSH-Version 1.
`ip ssh`	SSH-Server einschalten.

A.4.3 Zugriff mittels SSH

Eine Möglichkeit mittels SSH auf Ihr Gerät zuzugreifen, bietet das Programm PuTTY. Dieses Programm finden Sie auf der Produkt-CD.

☐ Starten Sie das Programm mit einem Doppelklick.
☐ Geben Sie die IP-Adresse Ihres Gerätes ein.
☐ Wählen Sie „SSH“.

☐ Klicken Sie auf „Open“, um die Verbindung zu Ihrem Gerät aufzubauen.

Abhängig vom Gerät und vom Zeitpunkt der Konfiguration von SSH kann der Verbindungsaufbau bis zu einer Minute dauern.

Gegen Ende des Verbindungsaufbaus zeigt PuTTY eine Sicherheitsalarmmeldung an und bietet Ihnen die Möglichkeit, den Fingerabdruck des Schlüssels zu überprüfen.

Abb. 75: Sicherheitsabfrage für den Fingerabdruck

- ☐ Überprüfen Sie den Fingerabdruck des Schlüssels, um sicherzustellen, dass Sie sich tatsächlich mit dem gewünschten Gerät verbunden haben. Den Fingerabdruck Ihres Schlüssels finden Sie im Feld „Key fingerprint“ des PuTTY Schlüsselgenerators.
- ☐ Stimmt der Fingerabdruck mit dem Ihres Schlüssels überein, dann klicken Sie auf „Ja“.

PuTTY zeigt eine weitere Sicherheitsalarmmeldung zur eingestellten Warnschwelle an.

Abb. 76: Sicherheitsabfrage zur eingestellten Warnschwelle

☐ Klicken Sie auf „Ja“ dieser Sicherheitsalarmmeldung.

Um für zukünftige Verbindungssaufbauten diese Meldung zu unterdrücken, wählen Sie vor dem Verbindungsaufbau in PuTTY im „Category“-Rahmen „SSH“. Im Rahmen „Encryption options“ wählen Sie „DES“ und klicken Sie auf „Up“ bis „DES“ über der Linie „-- warn below here --“ angekommen ist. Wechseln Sie im „Category“-Rahmen zurück zu Session und bauen Sie die Verbindung wie gewohnt auf.

Erfahrenen Netzadministratoren bietet die OpenSSH-Suite eine weitere Möglichkeit, mittels SSH auf Ihr Gerät zuzugreifen. Zum Aufbau der Verbindung geben Sie folgenden Befehl ein:

```
ssh admin@10.0.112.53 -cdes
```

- `admin` stellt den Benutzernamen dar.
- `10.0.112.53` stellt die IP-Adresse Ihres Gerätes dar.
- `-cdes` legt die Verschlüsselung für SSHv1 fest.

A.5 HTTPS-Zertifikat

Die Verschlüsselung von HTTPS-Verbindungen erfordert ein X.509-Zertifikat. Das Gerät bietet Ihnen die Möglichkeit, ein eigenes X.509-Zertifikat zu verwenden. Wenn auf dem Gerät kein X.509-Zertifikat vorhanden ist, erzeugt das Gerät dieses automatisch beim ersten Einschalten des HTTPS-Servers.

Ein eigenes X.509-Zertifikat laden Sie mit dem Command Line Interface per TFTP auf das Gerät.

☐ Legen Sie das Zertifikat auf Ihren tftp-Server.

☐ Laden Sie das Zertifikat vom tftp-Server auf das Gerät.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`no ip https`	Vor dem Übertragen des Zertifikats auf das Gerät die HTTPS-Funktion ausschalten.
`copy tftp://ip/filepath/cert nvram:httpscert`	Lädt das Zertifikat in den nicht-flüchtigen Speicher des Gerätes. `nvram:httpscert` ist der Speicherort des X.509-Zertifikats.
`ip https`	Nach dem Übertragen des Zertifikats auf das Gerät die HTTPS-Funktion einschalten.

A.6 Service-Shell

Wenn Sie beim Zugriff auf Ihr Gerät Unterstützung benötigen, verwendet das Service-Personal die Service-Shell-Funktion, um interne Bedingungen wie z. B. Schieberegister und CPU-Register zu überwachen.

Das CLI-Referenz-Handbuch enthält eine Beschreibung zum Deaktivieren der Service-Shell.

Anmerkung: Wenn Sie die Shell-Funktion deaktivieren, haben Sie weiterhin die Möglichkeit das Gerät zu konfigurieren, beschränken jedoch die Möglichkeiten des Service-Personals auf System-Diagnosen. Um die Service-Shell-Funktion zu reaktivieren ist das Öffnen des Gerätes seitens des Herstellers erforderlich.

B Allgemeine Informationen

B.1 Management Information BASE (MIB)

Die Management Information Base (MIB) ist als abstrakte Baumstruktur angelegt.
Die Verzweigungspunkte sind die Objektklassen. Die „Blätter“ der MIB tragen die Bezeichnung generische Objektklassen.
Die Instanzierung der generischen Objektklassen, das heißt, die abstrakte Struktur auf die Realität abzubilden, erfolgt z.B. durch die Angabe des Ports oder der Quelladresse (Source Address), soweit dies zur eindeutigen Identifizierung nötig ist.
Diesen Instanzen sind Werte (Integer, TimeTicks, Counter oder Octet String) zugeordnet, die gelesen und teilweise auch verändert werden können. Die Object Description oder der Object-ID (OID) bezeichnet die Objektklasse. Mit dem Subidentifier (SID) werden sie instanziert.

Beispiel:
Die generische Objektklasse
`hmPSState (OID = 1.3.6.1.4.1.248.14.1.2.1.3)`
ist die Beschreibung der abstrakten Information „Netzteilstatus“. Es lässt sich daraus noch kein Wert auslesen, es ist ja auch noch nicht bekannt, welches Netzteil gemeint ist.
Durch die Angabe des Subidentifiers (2) wird diese abstrakte Information auf die Wirklichkeit abgebildet, instanziert, und bezeichnet so den Betriebszustand des Netzteils 2. Diese Instanz bekommt einen Wert zugewiesen, der gelesen werden kann. Damit liefert die Instanz „`get 1.3.6.1.4.1.248.14.1.2.1.3.2`“ als Antwort „1“, das heißt, das Netzteil ist betriebsbereit.

Einige verwendete Abkürzungen in der MIB:	
Comm	Gruppen-Zugriffsrecht
con	Konfiguration
Descr	Beschreibung
Fan	Lüfter
ID	Identifizierer
Lwr	unterer (z. B. Grenzwert)
PS	Spannungsversorgung

Einige verwendete Abkürzungen in der MIB:	
Pwr	Stromversorgung
sys	System
UI	Benutzer-Schnittstelle (User Interface)
Upr	oberer (z. B. Grenzwert)
ven	vendor = Hersteller (Hirschmann)

Definition der verwendeten Syntaxbegriffe:	
Integer	Ganze Zahl im Bereich von -2^{31} - $2^{31}-1$
IP-Adresse	xxx.xxx.xxx.xxx (xxx = ganze Zahl im Bereich von 0-255)
MAC-Adresse	12-stellige Hexzahl nach ISO/IEC 8802-3
Object Identifier	x.x.x.x… (z. B. 1.3.6.1.1.4.1.248...)
Octet String	ASCII-Zeichen-Kette
PSID	Spannungsversorgungsidentifikation (Nummer des Netzteils)
TimeTicks	Stop-Uhr, verronnene Zeit = Zahlenwert/100 in Sekunden Zahlenwert = ganze Zahl im Bereich von $0-2^{32}-1$
Timeout	Zeitwert in hundertstel Sekunden Zeitwert = ganze Zahl im Bereich von $0-2^{32}-1$
Typfeld	4-stellige Hexzahl nach ISO/IEC 8802-3
Zähler	Ganze Zahl ($0-2^{32-1}$), deren Wert beim Auftreten bestimmter Ereignisse um 1 erhöht wird.

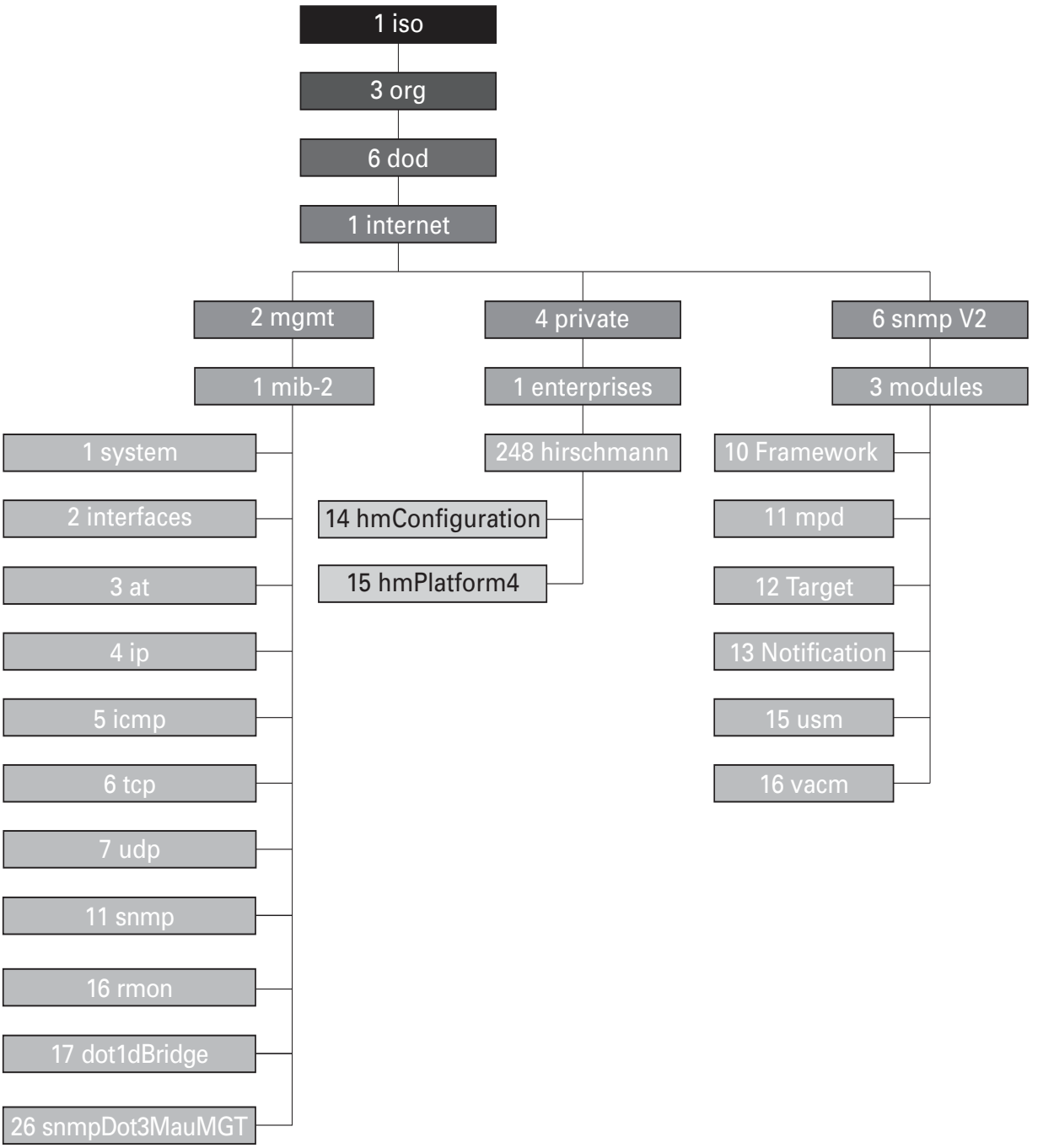


Abb. 77: Baumstruktur der Hirschmann-MIB

Die vollständige Beschreibung der MIB finden Sie auf der Produkt-CD, die zum Lieferumfang des Geräts gehört.

B.2 Verwendete Abkürzungen

ACA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
HTTP	Hypertext Transfer Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
LWL	Lichtwellenleiter
MAC	Media Access Control
MSTP	Multiple Spanning Tree Protocol
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

B.3 Technische Daten

Die technischen Daten finden Sie im Dokument „Referenz-Handbuch GUI“.

B.4 Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, um Sie beim Einsatz dieses Produkts zu unterstützen. Ihre Kommentare und Anregungen helfen uns dabei, die Qualität und den Informationsgrad dieser Dokumentation weiter zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	**gut**	**befriedigend**	**mäßig**	**schlecht**
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer +49 (0)7127 14-1600 oder
- per Post an

Hirschmann Automation and Control GmbH
Abteilung 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

C Stichwortverzeichnis

A

ACA 40, 56, 56, 73, 75, 222
ACD 248
ACL 175
Access-Control-Listen 175
Address Conflict Detection 248
Adresstabelle 157
AF 180
Aging Time 157, 163, 163
Alarm 221
Alarmnachrichten 218
Anforderungsintervall (SNTP) 136
APNIC 29
ARIN 29
ARP 33
Assured Forwarding 180
Authentifizierung 222
AutoConfiguration Adapter 40, 222
Automatische Konfiguration 85

B

Bandbreite 161, 193
Bandbreitenbegrenzung 185
Benutzernamen 22
Bericht 252
BOOTP 27
Booten 19
Boundary Clock 142
Broadcast 156, 158, 161

C

CDROM 266, 272
CIDR 33
CLI-Banner 129
Classless Inter Domain Routing 33
Class Selector 180
Command Line Interface 21

D

Destination Address 158
DHCP 27, 47, 50
DHCP Option 82 50
DHCP-Client 47
DHCP-Server 132, 266, 272
Differentiated Services 180
Differenzierter Management-Zugriff 104
DiffServ 175
DiffServ-Codepoint 180
Double-VLAN-Tagging 210
DSCP 176, 180, 183, 188, 188
DVLAN-Tagging 210
Dynamisch 158

E

E2E 142
Echtzeit 131, 175
EF 180
Empfangsleistungs-Status (Quelle für Alarme) 222
Empfangsport 159
End-to-End 142
Ereignis-Log 261
Erstinstallation 27
Expedited Forwarding 180

F

FAQ 301
Faulty Device Replacement 54
FDB 158
Ferndiagnose 226
Filter 158
Filtertabelle 158, 170
Flash-Speicher 61, 75
Flow control 193
Forwarding Database 158
Funktionsüberwachung 226

G

Gateway 30, 37
Generische Objektklassen 290
Gerätestatus 223
GMRP 161, 169
GMRP pro Port 172
Grafische Benutzeroberfläche 24
Grafische Benutzeroberfläche starten 25
Grandmaster 140

H

HaneWin 266, 272
Hardware-Adresse 43
Hardware-Reset 218
Hardware-Uhr (gepuffert) 132
HIPER-Ring (Quelle für Alarme) 222
HiDiscovery 38, 107
HiView 25
Host-Addresse 30

I

IANA 29
IEEE 1588-Zeit 133
IEEE 802.1 Q 176
IGMP 163
IGMP Querier 165
IGMP-Snooping 161, 163
Industrial HiVision 12, 48
Industrieprotokolle 11
Instanzierung 290
Internet Assigned Numbers Authority 29
Internet-Service-Provider 29
In-band 21
IP-Adresse 29, 36, 43, 47, 248
IP-Header 175, 179, 180
IP-Parameter 27
ISO/OSI-Schichtenmodell 33

J

Java Runtime Environment 64
JRE 64

K

Kaltstart 76
Konfiguration 61
Konfigurationsänderungen 218
Konfigurationsdatei 47, 61, 62
Konfigurationsdaten 42, 50, 58, 65

L

LACNIC 29
Lastbegrenzer Einstellungen 174
Leave 163
Lieferzustand 60, 61, 93
Login-Banner 128
Login-Fenster 26
Lokale Uhr 140
Lüfter 230

M

MAC 141
MAC-Adresse 246
MAC-Zieladresse 33
Maximale Bandbreite 185
Medienmodul für modulare Geräte (Quelle für Alarme) 222
Meldekontakt 86, 226
Meldekontakt (Quelle für Alarm) 222
Modus 85
Multicast 136, 158, 161, 163
Multicast-Adresse 170

N

Nachricht 218
Netzadresse 29
Netzmanagement 48
Netzmanagementstation 247
Netzmaske 30, 37
Netztopologie 50
Neustart 76

O

Object Description 290
Object-ID 290
Objektklassen 290
Offline-Konfiguration 63
Option 82 28, 50, 272
Ordinary Clock 142
Out-of-band 21

P

P2P 142
Passwort 22, 67, 94, 96
Peer-to-Peer 142
PHB 180
Phy 141
Polling 218
Portauthentifizierung 112
Portkonfiguration 85
Port-Mirroring 254
Port-Priorität 183, 187
PROFINET IO 11
Precedence 180
Precision Time Protocol 139
Priorität 176, 183
Prioritätsklasse 187
Priority Queues 175
Priority Tagged Frames 176
Protokollstapel 141
PTP 131, 133, 139
PTP-Subdomäne 143

Q

QoS 176
Quelladresse 156
Query 163
Query-Funktion 165

R

Reboot 76
Redundanz 11
Redundanz Manager 158
Referenzuhr 132, 135, 140, 146
Relaiskontakt 226
Release 71

Report 163
Reset 76
RIPE NCC 29
Ring-/Netzkopplung (Quelle für Alarme) 222
RMON-Probe 254
Router 12, 30
Ruhestromschaltung 226

S

Schulungsangebote 301
Segmentierung 218
Service 252
Service-Provider 29
Service-Shell-Funktion reaktivieren 287
SFP-Modul 244
SFP-Modul (Quelle für Alarme) 222
SFP-Zustandsanzeige 244
Signallaufzeit 135
Skriptdatei vom ACA laden 61
SNMP 24, 93, 218
SNMP-Paket 125
SNTP 131, 136
SNTP-Client 136
SNTP-Server 152
Software 280
Software-Release 71
Sommerzeit 132
SSH 21
Statisch 158
Strict-Priority 184
Subdomäne 143
Subidentifier 290
Subnetz 37, 157
Symbol 13
Systemname 47
Systemvoraussetzungen (GUI) 25
Systemzeit 135, 136
System-Monitor 18

T

TAI 133
TCP/IP-Stack 277
Technische Fragen 301
Telnet 21
TFTP 276
TFTP-Update 79
Time Stamp Unit 141
Topologie 50
ToS 175, 176, 179, 180
TP-Kabeldiagnose 237
Traffic Classes 175, 183
Traffic Shaping 185, 189, 189
Transparent Clock 142
Trap 218, 221
Trap-Zieltabelle 218
Trivial File Transfer Protocol 276
Trust dot1p 183
Trust ip-dscp 183
Type of Service 179
Typfeld 176

U

UDP 125
Uhr 139
Uhrenabgleich 141
Unicast 161
Untrusted 183
Update 18
USB-Stick 73
UTC 133
Überlastschutz 193
Übertragungsparameter 18
Übertragungssicherheit 218

V

Verbindungsfehler 86
Verbindungsüberwachung 223, 226
Versorgungsspannung 222
Video 184
VLAN 176, 183, 196
VLAN-ID (Netzparameter) 51
VLAN-Priorität 186
VLAN-Tag 176, 196
VLAN-Tunnel 210
VoIP 184
V.24 21

W

Warteschlange 184
Weighted Fair Queuing 184, 185, 189
Weighted Round Robin 184
Winterzeit 132

X

XML (Offline Configurator Format) 63

Z

Zeitmanagement 139
Zeitstempeleinheit 141, 145
Zeitverschiebung 133
Zeitzone 132
Zieladresse 157, 158, 159, 170
Zieltabelle 218
Zugangsschutz 85
Zugriff 222
Zugriffsrecht 67, 93

D Weitere Unterstützung

Technische Fragen

Bei technischen Fragen wenden Sie sich bitte an den Hirschmann-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann.

Die Adressen unserer Vertragspartner finden Sie im Internet unter http://www.hirschmann.com

Unser Support steht Ihnen zur Verfügung unter https://hirschmann-support.belden.eu.com

Sie erreichen uns

in der Region EMEA unter
- Tel.: +49 (0)1805 14-1538
- E-Mail: hac.support@belden.com

in der Region Amerika unter
- Tel.: +1 (717) 217-2270
- E-Mail: inet-support.us@belden.com

in der Region Asien-Pazifik unter
- Tel.: +65 6854 9860
- E-Mail: inet-ap@belden.com

Hirschmann Competence Center

Das Hirschmann Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen hat vor den Wettbewerbern gleich dreifach die Nase vorn:

- Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
  Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter http://www.hicomcenter.com
- Der Support reicht von der Inbetriebnahme über den Bereitschafts-service bis zu Wartungskonzepten.

Mit dem Hirschmann Competence Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

Anwender-Handbuch

Industrie-Protokolle
Industrial ETHERNET (Gigabit-)Switch
MACH 100, MACH 1000, MACH 4000, MS20/MS30, OCTOPUS, PowerMICE, RS20/RS30/RS40, RSR20/RSR30

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

© 2015 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken. Bei Geräten mit eingebetteter Software gilt die Endnutzer-Lizenzvereinbarung auf der mitgelieferten CD/DVD.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die jeweils neueste Version dieses Handbuches finden Sie im Internet auf den Hirschmann-Produktseiten (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Rel. 9.0 - 02/2015 – 27.02.2015

Inhalt

Sicherheitshinweise 5

Über dieses Handbuch 7

Legende 9

1 Industrie-Protokolle 11

2 EtherNet/IP 15

2.1 Integration in ein Steuerungssystem 17

2.2 EtherNet/IP-Parameter 21
2.2.1 Identity-Objekt 21
2.2.2 TCP/IP Interface-Objekt 22
2.2.3 Ethernet Link-Objekt 24
2.2.4 Ethernet Switch Agent-Objekt 27
2.2.5 I/O-Daten 30
2.2.6 Zuordnung der Ethernet Link Object-Instanzen 31
2.2.7 Unterstützte Dienste 32

3 PROFINET IO 33

3.1 Integration in ein Steuerungssystem 36
3.1.1 Vorbereitung des Switch 36
3.1.2 Konfiguration der SPS 38
3.1.3 Konfiguration des Gerätes 49
3.1.4 Tauschen von Geräten 50
3.1.5 Tauschen von Modulen 51
3.1.6 Netz überwachen 52

3.2 PROFINET IO-Parameter 56
3.2.1 Alarme 56
3.2.2 Record-Parameter 56
3.2.3 I/O-Daten 60

4 IEC 61850/MMS (RSR20/RSR30/MACH1000) 63

4.1 Switch-Modell für IEC 61850 64

4.2 Integration in ein Steuerungssystem 66
4.2.1 Vorbereitung des Switch 66
4.2.2 Offline-Konfiguration 67
4.2.3 Gerät überwachen 68

A GSD-Datei-Generator 69

B Leserkritik 70

C Stichwortverzeichnis 73

D Weitere Unterstützung 75

Sicherheitshinweise

⚠ WARNUNG
UNKONTROLLIERTE MASCHINENBEWEGUNGEN Um unkontrollierte Maschinenbewegungen aufgrund von Datenverlust zu vermeiden, konfigurieren Sie alle Geräte zur Datenübertragung individuell. Nehmen Sie eine Maschine, die mittels Datenübertragung gesteuert wird, erst in Betrieb, wenn Sie alle Geräte zur Datenübertragung vollständig konfiguriert haben. **Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.**

Über dieses Handbuch

Das Dokument „Anwender-Handbuch Industrie-Protokolle“ beschreibt die Anbindung des Gerätes über ein in der Industrie übliches Kommunikationsprotokoll wie z.B. EtherNet/IP und PROFINET IO.

In der Praxis hat sich folgende thematische Reihenfolge bewährt:

- Gerätekonfiguration gemäß Anwender-Handbuch Grundkonfiguration,
- Prüfen der Verbindung Switch <–> SPS,
- SPS programmieren.

Das Dokument „Anwender-Handbuch Installation“ enthält eine Gerätebeschreibung, Sicherheitshinweise, Anzeigebeschreibung und weitere Informationen, die Sie zur Installation des Gerätes benötigen, bevor Sie mit der Konfiguration des Gerätes beginnen.

Das Dokument „Anwender-Handbuch Redundanzkonfiguration“ enthält die Informationen, die Sie zur Auswahl des geeigneten Redundanzverfahrens und dessen Konfiguration benötigen.

Detaillierte Beschreibungen zur Bedienung der einzelnen Funktionen finden Sie in den Referenz-Handbüchern „Web-based Interface“ und „Command Line Interface“.

Die Netzmanagement-Software Industrial HiVision bietet Ihnen weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:

- Gleichzeitige Konfiguration mehrerer Geräte
- Grafische Benutzeroberfläche mit Netz-Layout
- Autotopologie-Erkennung
- Ereignislogbuch
- Ereignisbehandlung
- Client/Server-Struktur
- Browser-Interface
- ActiveX-Control für SCADA-Integration
- SNMP/OPC-Gateway.

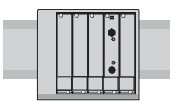
Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
☐	Arbeitsschritt
■	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Anmerkung:	Ein Hinweis betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	ASCII-Darstellung in Bedienoberfläche

Verwendete Symbole:

	WLAN-Access-Point
	Router mit Firewall
	Switch mit Firewall
	Router
	Switch
	Bridge

	Hub
	Beliebiger Computer
	Konfigurations-Computer
	Server
	SPS - Speicherprogrammier-bare Steuerung
	I/O - Roboter

1 Industrie-Protokolle

Lange Zeit gingen die Automatisierungs-Kommunikation und die Büro-Kommunikation getrennte Wege. Die Anforderungen an die Kommunikations-Eigenschaften waren zu unterschiedlich.

Die Büro-Kommunikation bewegt große Datenmengen mit geringen Anforderungen an die Übertragungszeit.
Die Automatisierungs-Kommunikation bewegt kleine Datenmengen mit hohen Anforderungen an die Übertragungszeit und Verfügbarkeit.

Während die Vermittlungsgeräte im Büro meist in temperierten, relativ sauberen Räumen stehen, sind die Vermittlungsgeräte in der Automatisierung einem größeren Temperaturbereich ausgesetzt. Verschmutze, staubige und feuchte Umgebungsbedingungen stellen weitere Anforderungen an die Beschaffenheit der Vermittlungsgeräte.

Mit der Weiterentwicklung der Kommunikations-Technologie näherten sich auch die Anforderungen an die Kommunikations-Eigenschaften an. Mit den heute zur Verfügung stehenden hohen Bandbreiten in der Ethernet-Technologie und den darauf aufsetzenden Protokollen lassen sich große Datenmengen übertragen und genaue Übertragungszeiten definieren.

Mit dem weltweit ersten, aktiven optischen LAN der Welt an der Universität Stuttgart 1984 legte Hirschmann den Grundstein für industriegerechte Büro-Kommunikationsgeräte. Dank der Initiative mit dem weltweit ersten Rail-Hub von Hirschmann in den neunziger Jahren stehen heute Ethernet-Vermittlungsgeräte wie Switches, Router und Firewalls für härteste Automatisierungsbedingungen zur Verfügung.

Der Wunsch nach einheitlichen, durchgängigen Kommunikationsstrukturen veranlasste viele Hersteller von Automatisierungsgeräten, sich zusammenzuschließen, um durch Standards den Fortschritt der Kommunikations-Technologie in der Automatisierung voranzutreiben. So stehen uns heute Protokolle zur Verfügung, die es uns erlauben, vom Büro aus bis in die Feldebene über Ethernet zu kommunizieren.

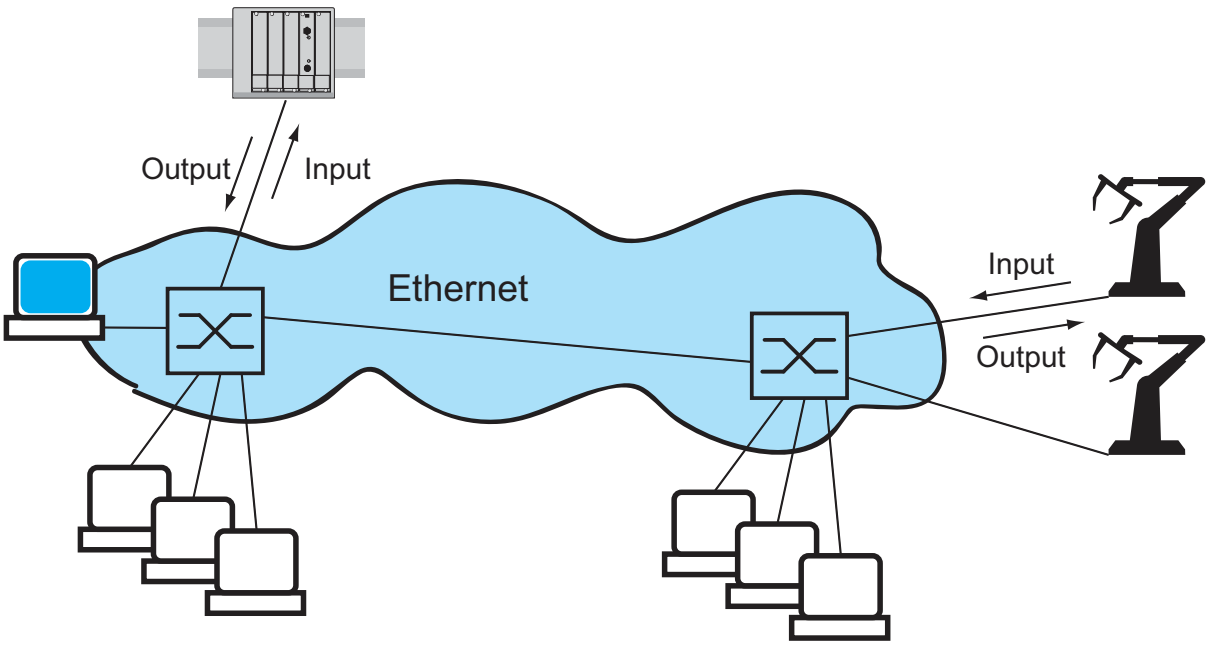


Abb. 1: Beispiel für die Kommunikation.

Hirschmann Switche unterstützen die Industrie-Protokolle bzw. -Systeme

- EtherNet/IP,
- und PROFINET IO

Abhängig von der bestellten Industrie-Protokoll-Variante enthält der Switch die passenden Voreinstellungen:

Einstellungen / Variante	Standard	EtherNet/IP	PROFINET IO
Order code	H	E	P
EtherNet/IP	0	1	0
IGMP Snooping	0	1	0
IGMP Querier	0	1	0
Unbekannte Multicast	An alle Ports senden	Verwerfen	Verwerfen
Address Conflict Detection	0	1	0
RSTP	1	0	1
DIP-Schalter	SW-Konfig	SW-Konfig	SW-Konfig
100 Mbit/s TP-Ringports	Autoneg	Autoneg	Autoneg

Einstellungen / Variante	Standard	EtherNet/IP	PROFINET IO
Statische Queryports	Disable	Automatic	Automatic
PROFINET IO	0	0	1
Boot-Modus	DHCP	DHCP	Lokal
VLAN 0 Transparent Modus	0	0	1
HiDiscovery	Read/Write	Read/Write	ReadOnly
sysName	Product name + 3 Byte MAC	Product name + 3 Byte MAC	empty

Wenn Sie ein Gerät mit der Standardkonfiguration für PROFINET IO konfigurieren wollen, dann finden Sie in der folgenden Tabelle die entsprechenden Dialoge des Web-based Interfaces.

Parameter	Dialog	Aktion
PROFINET IO	`Erweitert:Industrie-Protokolle:PROFINET`	PROFINET IO einschalten.
Boot-Modus	`Grundeinstellungen:Netz/Modus`	„Lokal“ wählen.
IP-Adresse	`Grundeinstellungen:Netz/Lokal`	Die „IP-Adresse“ `0.0.0.0` eingeben
Netzmaske	`Grundeinstellungen:Netz/Lokal`	Die „Netzmaske“ `0.0.0.0` eingeben.
Gateway-Adresse	`Grundeinstellungen:Netz/Lokal`	Die „Gateway-Adresse“ `0.0.0.0` eingeben.
VLAN 0-Transparent-Modus	`Switching:VLAN:Global`	Den „VLAN 0-Transparent-Modus“ einschalten.
HiDiscovery	`Grundeinstellungen:Netz/HiDiscovery Protocol`	Die Funktion einschalten und den Zugriff „Read-only“ wählen.
Systemname	`Grundeinstellungen:System/Systemdaten`	Den Feldinhalt löschen.

Tab. 1: Web-based Interface-Dialoge zur Einstellung der PROFINET IO-Parameter

2 EtherNet/IP

EtherNet/IP ist ein weltweit akzeptiertes, von der Open DeviceNet Vendor Association, (ODVA) standardisiertes industrielles Kommunikationsprotokoll auf Basis von Ethernet. Es baut auf den weit verbreiteten Transportprotokollen TCP/IP und UDP/IP (Standard) auf. EtherNet/IP bildet damit eine breite, von führenden Herstellern unterstützte Basis für effektive Datenkommunikation in der Industrie.

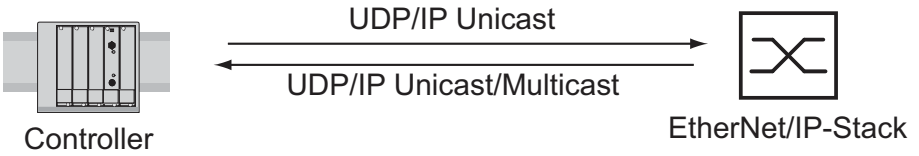


Abb. 2: Kommunikation zwischen Controller (SPS) und Switch

EtherNet/IP erweitert Ethernet um das Industrie-Protokoll CIP (Common Industrial Protocol) als Applikationsschicht für Automatisierungsanwendungen. Damit ist Ethernet für den Bereich der industriellen Steuerungstechnik bestens qualifiziert.

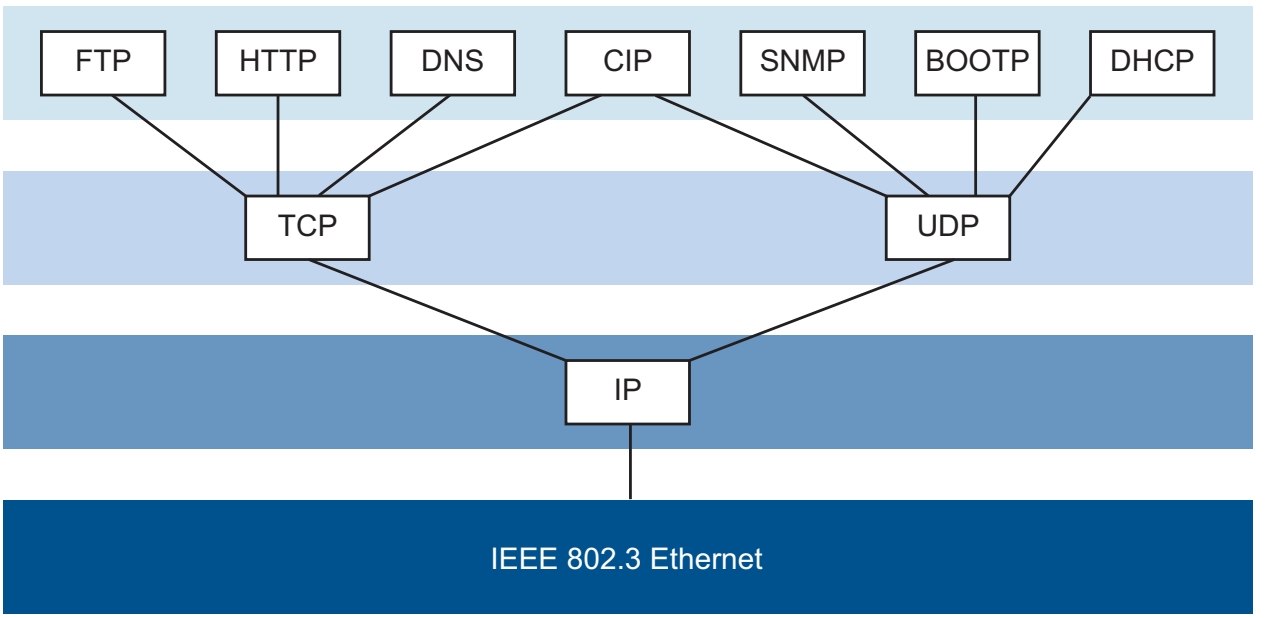


Abb. 3: EtherNet/IP (CIP) im ISO/OSI-Referenzmodell

EtherNet/IP treffen Sie insbesondere in den USA und im Umfeld von Rockwell-Steuerungen an.

Ausführliche Informationen zu EtherNet/IP finden Sie auf der Internetseite der ODVA unter www.ethernetip.de.

2.1 Integration in ein Steuerungssystem

Nach der Installation und dem Anschließen des Switch konfigurieren Sie ihn nach dem Anwender-Handbuch Grundkonfiguration. Danach:

☐ Prüfen Sie mit Hilfe des Web-based Interfaces im Dialog `Switching:Multicasts:IGMP`, ob IGMP-Snooping eingeschaltet ist.

☐ Prüfen Sie mit Hilfe des Web-based Interfaces im Dialog `Erweitert:Industrie-Protokolle`, ob EtherNet/IP eingeschaltet ist.

☐ Laden Sie mit Hilfe des Web-based Interfaces im Dialog `Erweitert:Industrie-Protokolle`, die EDS (EtherNet/IP-Konfigurationsdatei) zusammen mit dem Icon auf Ihren lokalen Rechner herunter.

Anmerkung: Wenn EtherNet/IP und die Router-Funktion gleichzeitig eingeschaltet sind, können Funktionsstörungen bei EtherNet/IP auftreten, z.B. im Zusammenhang mit „RS Who“. Schalten Sie daher die Router-Funktion des Geräts ab.

- Router-Funktion ausschalten im Web-based Interface:
  Dialog `Routing:Global`.
- Router-Funktion ausschalten im Command Line Interface:
  im Konfigurationsmodus (Prompt „`..(Config)#`“) mit dem Befehl `no ip routing`.

Konfiguration einer SPS am Beispiel der Rockwell-Software

- ☐ Öffnen Sie das „EDS Hardware Installation Tool“ von RSLinx.
- ☐ Fügen Sie mit dem „EDS Hardware Installation Tool“ die EDS-Datei hinzu.
- ☐ Starten Sie den Dienst „RSLinx“ neu, damit RSLinx die EDS-Datei des Switch übernimmt.
- ☐ Prüfen Sie mit RSLinx, ob RSLinx den Switch erkannt hat.
- ☐ Öffnen Sie Ihr Logix 5000-Projekt.
- ☐ Binden Sie den Switch als neues Modul (Generic Ethernet Module) am Ethernet-Port des Controllers ein.

Einstellung	I/O-Verbindung	Input-only	Listen-only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP-Address	IP-Adresse des Switch	IP-Adresse des Switch	IP-Adresse des Switch
Input Assembly Instance	2	2	2
Input Size	7 (MACH 4000: 11)	7 (MACH 4000: 11)	7 (MACH 4000: 11)
Output Assembly Instance	1	254	255
Output Size	1 (MACH 4000: 2)	0	0
Configuration Assembly Instance	3	3	3
Configuration Size	0	0	0

Tab. 2: Einstellungen zum Einbinden eines Generic Ethernet Module

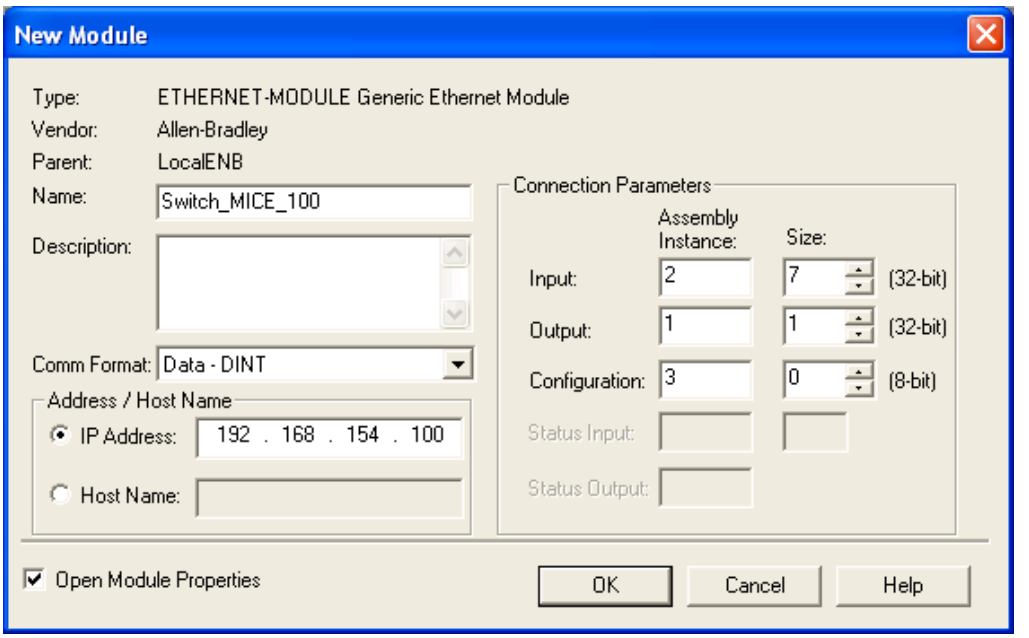


Abb. 4: Neues Modul in Logix 5000 einbinden

☐ Geben Sie in den Moduleigenschaften für das Request Packet Intervall (RPI) einen Wert von mindestens 100 ms ein.

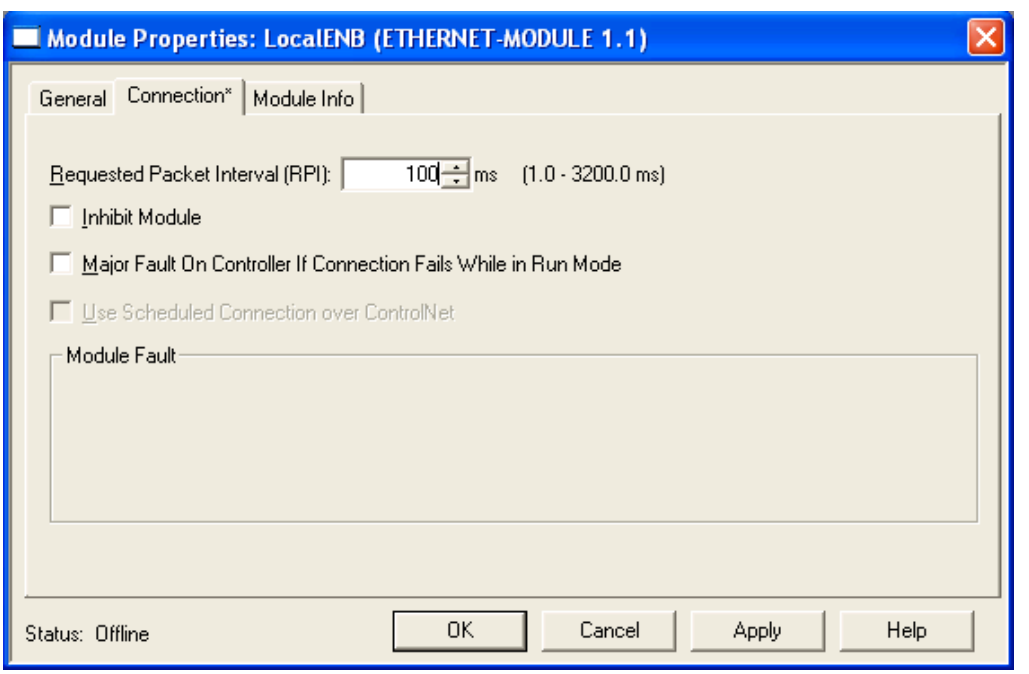


Abb. 5: Moduleigenschaften für das Request Packet Intervall (RPI)

Anmerkung: Wenn z.B. ein Management-Programm die Switch-CPU durch SNMP-Anfragen belastet, kann die I/O-Verbindung zwischen speicherprogrammierbarer Steuerung (SPS) und Switch zeitweise unterbrochen sein. Da der Switch in diesem Fall weiterhin Datenpakete vermitteln kann, kann auch die Anlage weiterhin betriebsbereit sein.
Die Überwachung der I/O-Verbindung zur Switch-CPU als Ausfallkriterium kann zum Anlagenausfall führen und ist deshalb weniger als Ausfallkriterium geeignet.

Beispiel zur Integration aus der Sample Code Library

Die Sample Code Library ist eine Web-Seite von Rockwell. Sie hat das Ziel, den Anwendern einen Platz zu bieten, an welchem sie ihre besten Architekturintegrations-Anwendungen austauschen können.
Suchen Sie in der Web-Seite http://samplecode.rockwellautomation.com nach der „Catalog Number“ 9701. Das ist die Katalognummer für ein Beispiel zur Integration von Hirschmann Switches in RS Logix 5000 Rel. 16, SPS-Firmware Release 16.

2.2 EtherNet/IP-Parameter

2.2.1 Identity-Objekt

Der Switch unterstützt das Identity Object (Class Code 01) von EtherNet/IP. Die Hirschmann-Hersteller-ID ist 634. Hirschmann verwendet die herstellerspezifische ID 149 (95_H) zur Kennzeichnung des Produkttyps „Managed Ethernet Switch“.

Id	Attribute	Access Rule	Data type	Description
1	Vendor ID	Get	UINT	Hirschmann 634
2	Device Type	Get	UINT	Vendor-specific Definition 149 (95H) "Managed Ethernet Switch".
3	Product Code	Get	UINT	Product Code: mapping is defined for every device type, e.g. RS20-0400T1T1SDAPHH is 16650.
4	Revision	Get	STRUCT USINT Major USINT Minor	Revision of the Ethernet/IP implementation, currently 1.1, Major Revision and Minor Revision
5	Status	Get	WORD	Not used
6	Serial Number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
7	Product Name	Get	Short String (max. 32 Byte)	Displayed as "Hirschmann" + order code, e.g. Hirschmann RSxxxxx.

Tab. 3: Identity-Objekt

2.2.2 TCP/IP Interface-Objekt

Der Switch unterstützt eine Instanz (Instance 1) des TCP/IP Interface Object (Class Code $F5_H$, 245) von EtherNet/IP.
Bei einem Schreibzugriff speichert der Switch die komplette Konfiguration in seinen Flash-Speicher. Das Speichern kann 10 Sekunden dauern. Das Unterbrechen des Speichervorgangs, z.B. durch Unterbrechung der Stromversorgung, kann möglicherweise zum Ausfall des Switch führen.

Anmerkung: Der Switch beantwortet den „Set Request" für eine Konfigurationsänderung mit einem „Response", noch bevor die Konfigurationsspeicherung beendet ist.

Id	Attribute	Access rule	Data type	Description
1	Status	Get	DWORD	Interface Status (0: Interface not configured, 1: Interface contains valid config).
2	Interface Capability flags	Get	DWORD	Bit 0: BOOTP Client, Bit 1: DNS Client, Bit 2: DHCP Client, Bit 3: DHCP-DNS Update, Bit 4: Configuration settable (within CIP). Other bits reserved (0).
3	Config Control	Set/Get	DWORD	Bits 0 through 3: Value 0: using stored config, Value 1: using BOOTP, Value 2: using DHCP. Bit 4: 1 device uses DNS for name lookup (always 0 because not supported) Other bits reserved (0).
4	Physical Link Object	Get	Structure: UINT Path size EPATH Path	Path to the Physical Link Objekt, always {20H, F6H, 24H, 01H} describing instance 1 of the Ethernet Link Object.

Tab. 4: TCP/IP Interface-Objekt

Id	Attribute	Access rule	Data type	Description
5	Interface Configuration	Set/Get	Structure: UDINT IP address UDINT Netmask UDINT Gateway address UDINT Name server 1 UDINT Name server 2 STRING Domain name	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Nameservers (DNS, not supported) and the domain name).
6	Host name	Set/Get	STRING	Host name (for DHCP DNS Update).
8	TTL Value	Set/Get	USINT	TTL value for EtherNet/IP multicast packets
9	Mcast Config	Set/Get	STRUCT of:	IP multicast address configuration
	Alloc Control		USINT	Multicast address allocation control word. Determines how addresses are allocated.
	Reserved		USINT	Reserved for future use
	Num Mcast		UINT	Number of IP multicast addresses to allocate for EtherNet/IP
	Mcast Start Addr		UDINT	Starting multicast address from which to begin allocation.
100	Quick Connect	Set/Get	DWORD	Bitmask of 1 bit per port to enable/disable Quick Connect.

Tab. 4: TCP/IP Interface-Objekt

2.2.3 Ethernet Link-Objekt

Der Switch unterstützt mindestens eine Instanz (Instance 1; die Instanz des CPU-Ethernet-Interface) des Ethernet Link Object (Class Code $F6_H$, 246) von EtherNet/IP.

Id	Attribute	Access rule	Data type	Description
1	Interface Speed	Get	UDINT	Used interface speed in MBits/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected problems.
2	Interface Flags	Get	DWORD	Interface Status Flags: Bit 0: Link State (1: Link up), Bit 1: 0: Half-Duplex, 1: FullDuplex1, Bits 2 through 4: Autoneg Status (0: Autoneg in Progress, 1: Autoneg unsuccessful, 2: unsuccessful but Speed detected, 3: Autoneg success, 4: No Autoneg), Bit 5: manual configuration requires reset (always 0 because not needed), Bit 6: detected hardware error.
3	Physical Address	Get	ARRAY of 6 USINTs	MAC address of physical interface.
4	Interface Counters	Get	Struct MIB II Counters Jeweils UDINT	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors.
5	Media Counters	Get	Struct Ethernet MIB Counters Jeweils UDINT	Alignment Errors, FCS Errors, Single Collision, Multiple Collision, SQE Test Errors, Deferred Transmissions, Late Collisions, Excessive Collisions, MAC TX Errors, Carrier Sense Errors, Frame Too Long, MAC RX Errors.
6	Interface Control	Get/Set	Struct Control Bits WORD Forced Iface Speed UINT	Control Bits: Bit 0: Autoneg enable/disable (1: enable), Bit 1: Duplex mode (1: full duplex, if Autoneg is disabled). Interface speed in MBits/s: 10, 100,…, if Autoneg is disabled.
7	Interface Type	Get	USINT	Value 0: Unknown interface type, Value 1: The interface is internal, Value 2: Twisted-pair, Value 3: Optical fiber.

Tab. 5: Ethernet Link-Objekt

Id	Attribute	Access rule	Data type	Description
8	Interface State	Get	USINT	Value 0: Unknown interface state, Value 1: The interface is enabled, Value 2: The interface is disabled, Value 3: The interface is testing,
9	Admin State	Set	USINT	Value 1: Enable the interface, Value 2: Disable the interface.
10	Interface Label	Get	SHORT_ STRING	Interface name. The content of the string is vendor-specific.

Tab. 5: Ethernet Link-Objekt

Der Switch unterstützt zusätzliche herstellerspezifische Attribute.

Id	Attribute	Access rule	Data type	Description
100 (64 H)	Ethernet Interface Index	Get	UDINT	Interface/Port Index (ifIndex from MIB II)
101 (65 H)	Port Control	Get/Set	DWORD	Bit 0 (RO): Link state (0: link down, 1: link up) Bit 1 (R/W): Link admin state (0: disabled, 1: enabled) Bit 8 (RO:) Access violation alarm Bit 9 (RO): Utilization alarm
102 (66 H)	Interface Utilization	Get	UDINT	The existing Counter from the private MIB hmIfaceUtilization is used. Utilization in percentage[a]. RX Interface Utilization.
103 (67 H)	Interface Utilization Alarm Upper Threshold	Get/Set	UDINT	Within this parameter the variable hmIface-UtilizationAlarmUpperThreshold can be accessed. Utilization in percentage[a]. RX Interface Utilization Upper Limit.
104 (68 H)	Interface Utilization Alarm Lower Threshold	Get/Set	UDINT	Within this parameter the variable hmIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage[a]. RX Interface Utilization Lower Limit.

Tab. 6: Hirschmann-Erweiterungen des Ethernet Link-Objekts

Id	Attribute	Access rule	Data type	Description
105 (69 H)	Broadcast Limit	Get/Set	UDINT	Broadcast limiter Service (Egress BC-Frames limitation, 0: disabled), Frames/second
106 (6A H)	Ethernet Interface Description	Get	STRING [max. 64 Bytes] even number of Bytes	Interface/Port Description (from MIB II ifDescr), e.g. "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX", or "unavailable", max. 64 Bytes.

Tab. 6: Hirschmann-Erweiterungen des Ethernet Link-Objekts

a. Einheit: 1 Hundertstel von 1%, d.h., 100 entspricht 1%

2.2.4 Ethernet Switch Agent-Objekt

Der Switch unterstützt das Hirschmann-spezifische Ethernet Switch Agent Object (Class Code $95_{H,}$ 149) für die Switch-Konfigurations- und Informationsparameter mit einer Instanz (Instance 1).
Weitere Informationen zu diesen Parametern, und wie Sie die Parameter einstellen, finden Sie im Referenz-Handbuch „GUI“ (Graphical User Interface / Web-based Interface).

Attribute	ID/Bit No.	Description
Switch Status	ID 01	DWORD (32 bit) RO
	Bit 0	Overall state (0: ok, 1: failed) Like the signal contact.
	Bit 1	Power Supply 1 (0: ok, 1: failed or does not exist)
	Bit 2	Power Supply 2 (0: ok, 1: failed or does not exist)
	Bit 3	Power Supply 3 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 4	Power Supply 4 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 5	Power Supply 5 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 6	Power Supply 6 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 7	Power Supply 7 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 8	Power Supply 8 (0: ok or not possible on this platform, 1: failed or does not exist)
	Bit 9	DIP RM (ON: 1, OFF: 0)
	Bit 10	DIP Standby (ON: 1, OFF: 0)
	Bit 11	Signal Contact 1 (0: closed, 1: open)
	Bit 12	Signal Contact 2 (0: closed, 1: open)
	Bit 13	Quick Connect (1: ON, 0: OFF)
	Bit 16	Temperature (0: ok, 1: threshold exceeded)
	Bit 17	Fan (0: ok or no fan, 1: inoperable)
	Bit 21	DIP Ring ports, 0: module 1 ports 1&2, 1: module 2, ports 1&2
	Bit 22	DIP Configuration (1: enabled, 0: disabled)
	Bit 23	DIP HIPER-Ring state (1: ON, 0: OFF)
	Bit 24	Module removed (1: removed)
	Bit 25	ACA removed (1: removed)
	Bit 28	Hiper-Ring (1: loss of redundancy reserve)
	Bit 29	Ring-/Netcoupling (1: loss of redundancy reserve)

Tab. 7: Hirschmann Ethernet Switch Agent Object

Attribute	ID/Bit No.	Description
	Bit 30	Connection Error (1: link inoperable)
Switch Temperature	ID 02	Struct{INT RO Temperature °F, INT RO Temperature °C}
Reserved	ID 03	Always 0, attribute is reserved for future use.
Switch Max Ports	ID 04	UINT (16 bit) RO Maximum number of Ethernet Switch Ports
Multicast Settings (IGMP Snooping)	ID 05	WORD (16 bit) RW
	Bit 0 RW	IGMP Snooping (1: enabled, 0: disabled)
	Bit 1 RW	IGMP Querier (1: enabled, 0: disabled)
	Bit 2 RO	IGMP Querier Mode (1: Querier, 0: Non-Querier)
	Bit 4-6 RW	IGMP Querier Packet Version 1: V1, 2: V2, 3: V3, 0: Off (IGMP Querier disabled)
	Bit 8-10 RW	Treatment of Unknown Multicasts (Railswitch only): 0: Send To All Ports, 1: Send To Query Ports, 2: Discard
Switch Existing Ports	ID 06	ARRAY OF DWORD[a] RO Bitmask of existing Switch Ports
	Per Bit starting with Bit 0 (means Port 1)	1: Port existing, 0: Port not available. Array (bit mask) size is adjusted to the size of maximum number of Switch ports (e.g. a max. no of 28 ports means that 1 DWORD is used (32 bit)).
Switch Port Control	ID 07	ARRAY OF DWORD[a] RW Bitmask Link Admin Status Switch Ports
	Per Bit starting with Bit 0 (means Port 1)	0: Port enabled, 1: Port disabled. Array (bit mask) size is adjusted to the size of maximum number of Switch ports (e.g. a max. no of 28 ports means that 1 DWORD is used (32 bit)).
Switch Ports Mapping	ID 08	ARRAY OF USINT (BYTE, 8 bit) RO Instance number of the Ethernet Link Object
	Starting with Index 0 (means Port 1)	All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N (maximum number of ports)). When the entry is 0, the Ethernet Link Object for this port does not exist.
Switch Action Status	ID 09	DWORD (32 bit) RO
	Bit 0	Flash write in progress
	Bit 1	Unable to write to flash or write incomplete

Tab. 7: Hirschmann Ethernet Switch Agent Object

a. RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100 and MACH 1000: 32 bit;
MACH 4000: 64 bit

Das Hirschmann-spezifische Ethernet Switch Agent Object bietet Ihnen den zusätzlichen herstellerspezifischen Service mit dem Service-Code 35_H zum Abspeichern der Switchkonfiguration. Der Switch beantwortet die Aufforderung zur Konfigurationsabspeicherung, sobald er die Konfiguration im Flash-Speicher gespeichert hat.

2.2.5 I/O-Daten

Die genaue Bedeutung der einzelnen Bits des Gerätestatus in den I/O-Daten finden Sie in Abschnitt „Ethernet Switch Agent-Objekt” auf Seite 27.

I/O Data	Value (data types and sizes to be defined)	Direction
Device Status	Bitmask (see Switch Agent Attribute 1)	Input, DWORD 32 Bit
Link Status	Bitmask, 1 Bit per port 0: No link, 1: Link up	Input, DWORD[a]
Output Links Aadmin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, e.g. for controller access port. 0: Port enabled, 1: Port disabled.	Input DWORD[a]
Utilization Alarm	Bitmask, 1 Bit per port 0: No alarm, 1: Alarm on port	Input, DWORD[a]
Access Violation Alarm	Bitmask, 1 Bit per port 0: No alarm, 1: Alarm on port	Input, DWORD[a]
Multicast Connections	Integer, number of connections	Input, 1 DINT 32 bit
TCP/IP Connections	Integer, number of connections	Input, 1 DINT 32 bit
Link Admin State	Bitmask, one Bit per port 0: Port enabled, 1: Port disabled	Output, DWORD[a]

Tab. 8: I/O-Daten

a. RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE, RSR20/RSR30, MACH 100 und MACH 1000: 32 Bit;
MACH 4000: 64 Bit

2.2.6 Zuordnung der Ethernet Link Object-Instanzen

Die Tabelle zeigt die Zuordnung der Switch-Ports zu den Ethernet Link Object-Instanzen.

Ethernet Link Object Instance	RS20/RS30/RS40 RSR20/RSR30, OCTOPUS, MACH 1000	MS20/MS30, PowerMICE, MACH 100	MACH 4000
1	CPU	CPU	CPU
2	1	Modul 1 / Port 1	Modul 1 / Port 1
3	2	Modul 1 / Port 2	Modul 1 / Port 2
4	3	Modul 1 / Port 3	Modul 1 / Port 3
5	4	Modul 1 / Port 4	Modul 1 / Port 4
6	5	Modul 2 / Port 1	Modul 1 / Port 5
7	6	Modul 2 / Port 2	Modul 1 / Port 6
8	7	Modul 2 / Port 3	Modul 1 / Port 7
9	8	Modul 2 / Port 4	Modul 1 / Port 8
10	9	Modul 3 / Port 1	Modul 2 / Port 1
11	10	Modul 3 / Port 2	Modul 2 / Port 2
12	11	Modul 3 / Port 3	Modul 2 / Port 3
13	12	Modul 3 / Port 4	Modul 2 / Port 4
14	13	Modul 4 / Port 1	Modul 2 / Port 5
..	..	..	..

Tab. 9: Zuordnung der Switch-Ports zu den Ethernet Link Object Instanzen

2.2.7 Unterstützte Dienste

Die Tabelle bietet Ihnen einen Überblick über die von der EtherNet/IP-Implementierung für die Objektinstanzen unterstützten Dienste.

Service code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object
Get Attribute All (01H)	All Attributes	All Attributes	All Attributes	All Attributes
Set Attribute All (02H)	-	Settable Attributes (3, 5, 6)	-	-
Get Attribute Single (0EH)	All Attributes	All Attributes	All Attributes	All Attributes
Set Attribute Single (10H)	-	Settable Attributes (3, 5, 6)	Settable Attributes (6, 65H, 67H, 68H, 69H)	Settable Attributes (7)
Reset (05H)	Parameter (0,1)	-	-	-
Save Configuration (35H) Vendor-specific	Parameter (0,1)	-	-	Save Switch Configuration

Tab. 10: Unterstützte Dienste

3 PROFINET IO

PROFINET IO ist ein weltweit akzeptiertes industrielles Kommunikationsnetz auf Basis von Ethernet. Es baut auf den weit verbreiteten Transportprotokollen TCP/IP und UDP/IP (Standard) auf. Dies ist ein wichtiger Aspekt um die Anforderungen an die Konsistenz von der Management-Ebene bis in die Feldebene zu erfüllen.

PROFINET IO ergänzt die bewährte Profibus-Technologie für solche Anwendungen, die schnelle Datenkommunikation und die Nutzung industrieller IT-Funktionen erfordern.

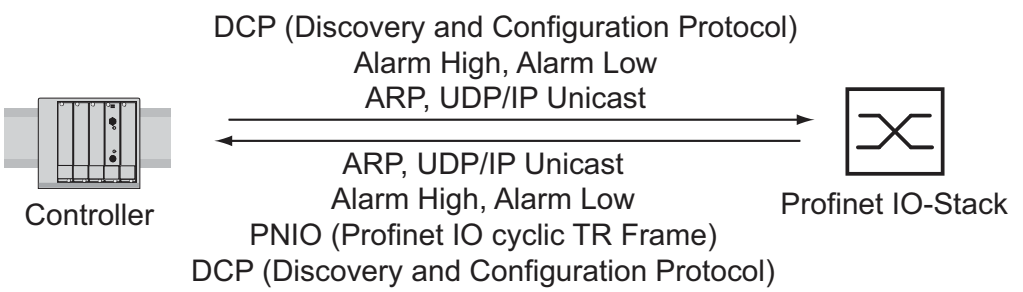


Abb. 6: Kommunikation zwischen Controller und Switch

PROFINET IO treffen Sie insbesondere in Europa und im Umfeld von Siemens-Steuerungen an.
PROFINET IO benutzt die Gerätebeschreibungssprache GSDML (Generic Station Description Markup Language), um Geräte und deren Eigenschaften maschinell verarbeitbar zu beschreiben. Die Gerätebeschreibung finden Sie in der GSDML-Datei des Gerätes.

Ausführliche Informationen zu PROFINET finden Sie auf der Internetseite der PROFIBUS-Organisation unter http://www.profibus.com.
Die Geräte sind konform zur Class B Konformitätsklasse bei PROFINET IO.

Switch-Modelle für PROFINET IO GSDML Version 2.3

Das Gerät erzeugt GSDML-Dateien im Format GSDML V.2.3. Innerhalb der GSDML-Datei ist das Gerät gemäß GSDML-Standard V.2.2 modelliert.

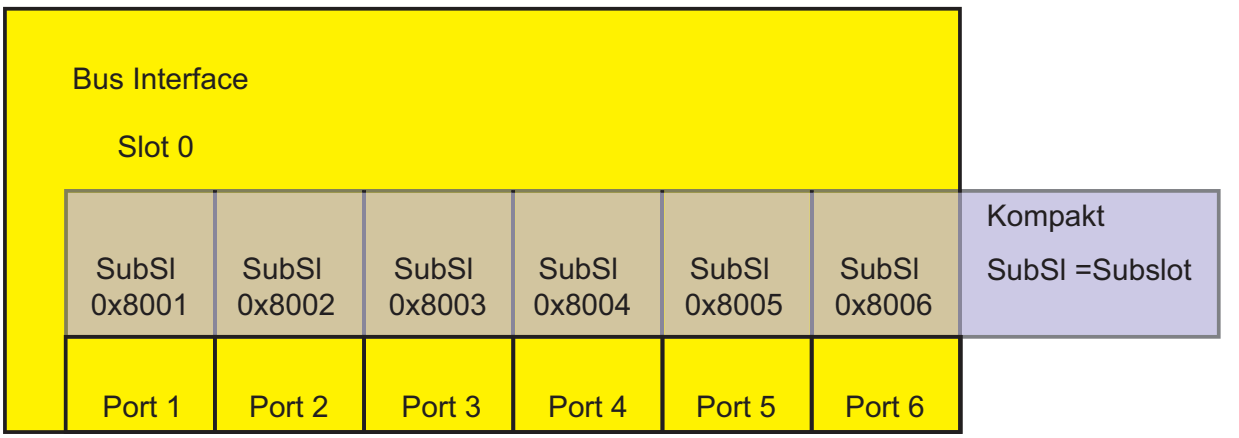


Abb. 7: Kompakter Switch

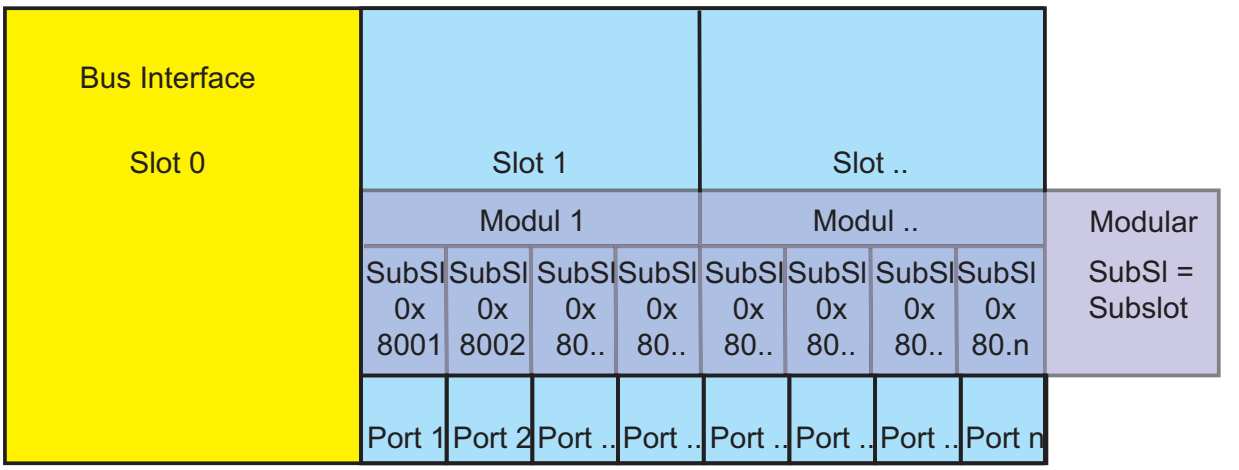


Abb. 8: Modularer Switch

Grafische Benutzeroberfläche und CLI

In Profinet-Umgebungen baut der Automatisierungsprozess eine Application Relation (AR) zum Gerät auf, sobald das Gerät erfolgreich eingerichtet ist. So lange die Application Relation aufgebaut ist, sind gewisse Einstellungen des Gerätes durch andere Benutzer unveränderbar.

Die folgenden Parameter sind bei aufgebauter Application Relation durch grafische Benutzeroberfläche, CLI und SNMP unveränderbar:

- IP-Adresse
- MRP
- Hiper-Ring
- DCP-Konfiguration
- HiDiscovery-Konfiguration
- Kabeltest
- LLDP-Konfiguration
- Portkonfiguration

Das Gerät zeigt nach der Anmeldung eines Benutzers über die grafische Benutzeroberfläche und CLI eine dementsprechende Meldung.

3.1 Integration in ein Steuerungssystem

3.1.1 Vorbereitung des Switch

Nach der Installation und dem Anschließen des Switch konfigurieren Sie ihn nach dem Anwender-Handbuch Grundkonfiguration:

☐ Prüfen Sie im Dialog `Grundeinstellungen:System`, ob im Feld „Name“ ein gültiger Systemname für das Gerät festgelegt ist.
Der Systemname darf ausschließlich alphanumerische Zeichen, Bindestriche und Punkte enthalten.

☐ Prüfen Sie mit Hilfe des Web-based Interfaces im Dialog `Grundeinstellungen:Netz`, ob im Rahmen „Modus“ `Lokal` ausgewählt ist.

☐ Prüfen Sie mit Hilfe des Web-based Interfaces im Dialog `Switching:VLAN:Global`, ob „VLAN 0-Transparent Modus“ markiert ist.

☐ Prüfen Sie mit Hilfe des Web-based Interfaces im Dialog `Erweitert:Industrie-Protokolle:PROFINET IO`, ob PROFINET IO eingeschaltet ist.

☐ Laden Sie die GSDML-Datei zusammen mit dem Icon auf Ihren lokalen Rechner.

Die GSDML-Datei und das Icon erhalten Sie
- mit Hilfe des Web-based Interfaces im Dialog `Erweitert:Industrie-Protokolle` oder
- mit Hilfe der im Lieferumfang enthaltenen Software (Standalone GSD File Generator) zum Erzeugen der GSDML-Datei.

☐ Konfigurieren Sie die Alarmeinstellungen und die Schwellwerte für die Alarme, die Sie überwachen wollen.

3.1.2 Konfiguration der SPS

Die folgende Ausführung bezieht sich auf die Konfiguration der SPS am Beispiel der Software Simatic S7 von Siemens und setzt voraus, dass Sie mit der Bedienung der Software vertraut sind.
Das Gerät unterstützt auch Engineering-Stationen anderer Hersteller, wie z.B. PC Worx von Phönix.

Anmerkung: Wenn z.B. ein Management-Programm die Switch-CPU durch SNMP-Anfragen belastet, kann die I/O-Verbindung zwischen speicherprogrammierbarer Steuerung (SPS) und Switch zeitweise unterbrochen sein. Da der Switch in diesem Fall weiterhin Datenpakete vermitteln kann, kann auch die Anlage weiterhin betriebsbereit sein.
Die Überwachung der I/O-Verbindung zur Switch-CPU als Ausfallkriterium kann zum Anlagenausfall führen und ist deshalb weniger als Ausfallkriterium geeignet.

In der Voreinstellung der SPS nimmt die SPS die Unterbrechung der I/O-Verbindung zum Switch als Ausfallkriterium. Dies führt laut Voreinstellung zum Anlagenausfall. Um diese Voreinstellung zu ändern, ergreifen Sie Step7-progammtechnische Maßnahmen.

GDSML-Datei bereitstellen

Zum Erzeugen von GDSML-Dateien und der Icons bietet Ihnen Hirschmann folgende Möglichkeiten:

- mit Hilfe des Web-based Interfaces im Dialog `Erweitert:Industrie-Protokolle:PROFINET IO` mit der Auswahl `PROFINET IO` die GSDML-Datei und das Icon des Gerätes herunterladen.
- mit Hilfe des Web-based Interfaces im Dialog `Erweitert:Industrie-Protokolle:PROFINET IO` mit der Auswahl `Anderes Gerät` die GSDML-Datei und das Icon eines anderen Gerätes, dessen Bestellbezeichnung Sie eingeben, herunterladen.
- mit Hilfe der im Lieferumfang enthaltenen Software (Standalone GSD File Generator) zum Erzeugen der GSDML-Datei.

Switch in Projektierung aufnehmen

- ☐ Öffnen Sie den „Simatic Manager“ von Simatic S7.
- ☐ Öffnen Sie Ihr Projekt.
- ☐ Wechseln Sie in die Hardware-Konfiguration.
- ☐ Installieren Sie die GSDML-Datei mit `Extras:GSD-Dateien installieren`.
  Wählen Sie die zuvor auf Ihrem PC gespeicherte GSDML-Datei aus. Simatic S7 installiert die Datei zusammen mit dem Icon.
  Den neuen Switch finden Sie unter `Profinet IO:Weitere Feldgeräte:Switching Devices:Hirschmann..` oder unter `Profinet IO:Weitere Feldgeräte:Network Components:Hirschmann...`
- ☐ Ziehen Sie mit Drag & Drop den Switch auf die Busleitung.

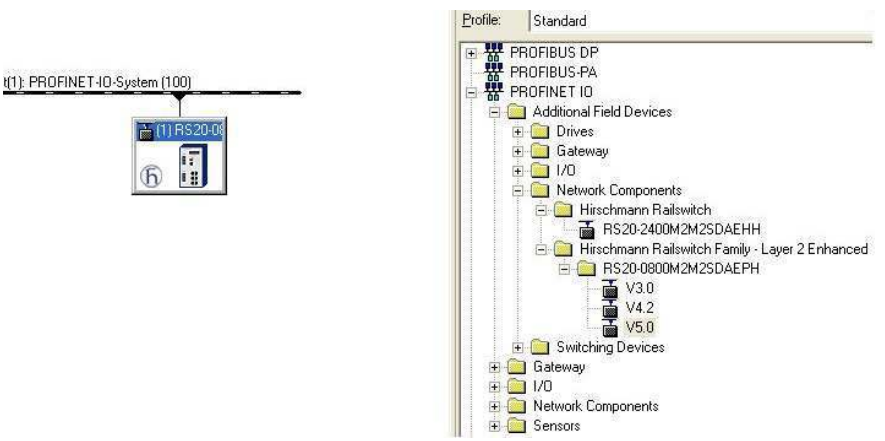


Abb. 9: Einfügen eines Switch aus der Simatic S7-Bibliothek

☐ Um dem Switch seinen Namen zu geben, markieren Sie den Switch und wählen Sie in der Menüleiste `Ziel-system:Ethernet:Ethernet-Teilnehmer bearbeiten...`

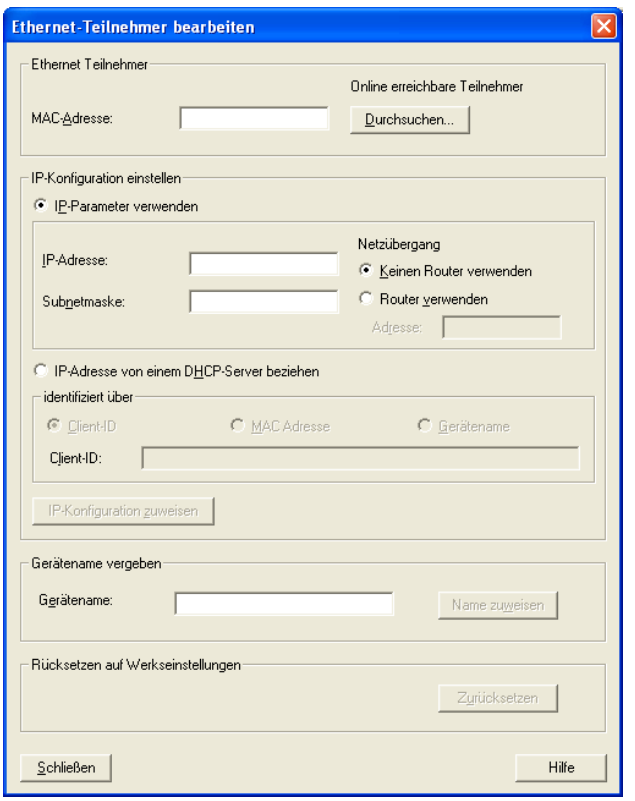


Abb. 10: Dialog zur Eingabe des Switch-Namens

☐ Klicken Sie auf „Durchsuchen“.
Wählen Sie Ihren Switch aus.
Klicken Sie auf „OK“.
☐ Geben Sie dem Switch seinen Namen.
Klicken Sie auf „Name zuweisen“.
☐ Klicken Sie auf „Schließen“.

☐ Klicken Sie in der Hardware-Konfiguration mit der rechten Maustaste auf den Switch und wählen Sie `Objekteigenschaften`.

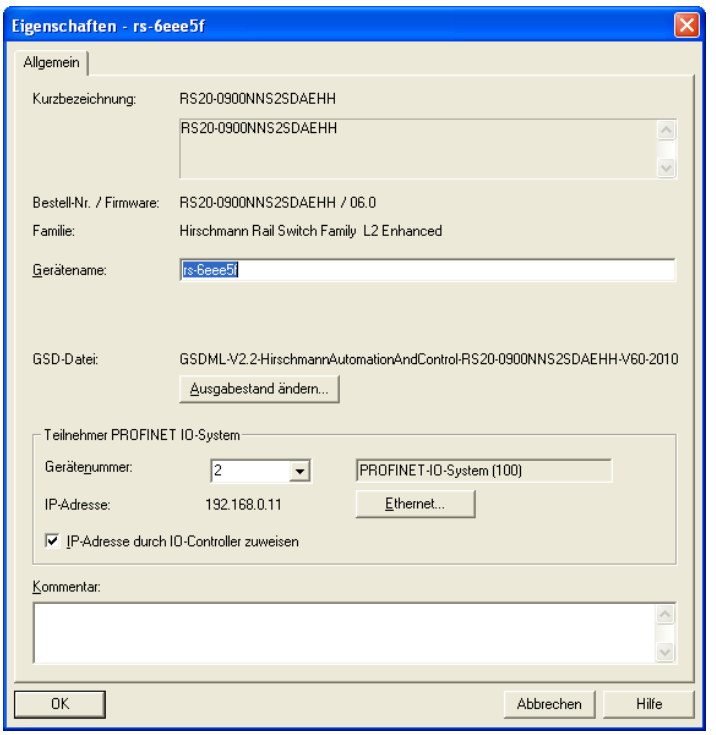


Abb. 11: Dialog zur Eingabe des Objektnamens (= Name des Switch) und der IP-Parameter

☐ Tragen Sie hier den gleichen Gerätenamen ein.
☐ Klicken Sie auf „Ethernet“.
Geben Sie die IP-Parameter ein.
Schließen Sie das Ethernet-Eingabe-Fenster.
☐ Klicken Sie auf „OK“, um das Eigenschaften-Fenster zu schließen.

Der Switch ist nun in der Projektierung aufgenommen.

IO-Zyklus konfigurieren

☐ Klicken Sie in der Hardware-Konfiguration mit der rechten Maustaste auf den Switch und wählen Sie `Objekteigenschaften`.

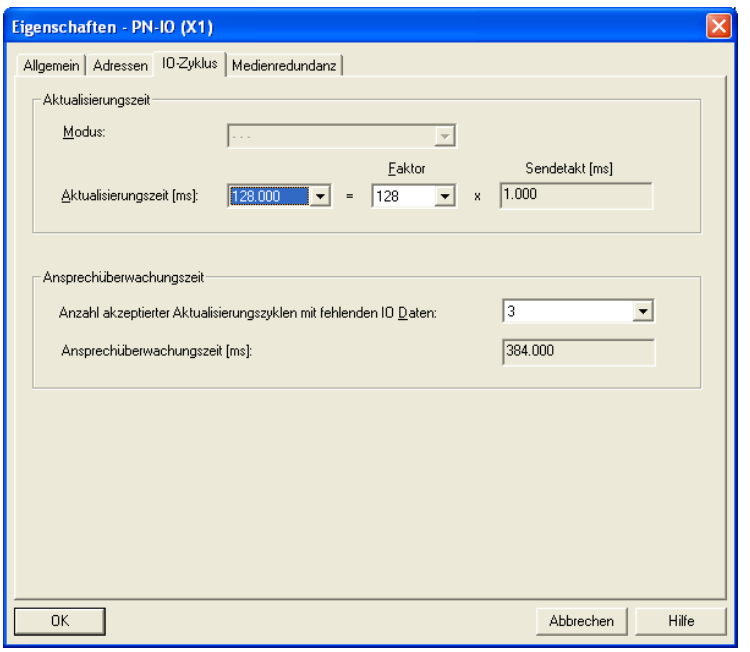


Abb. 12: Dialog zur Eingabe des IO-Zyklus

☐ Wählen Sie im Eigenschaften-Fenster die Karteikarte "IO-Zyklus".
☐ Wählen Sie unter `Aktualisierungszeit/Aktualisierungszeit[ms]`: die gewünschte Aktualisierungszeit (in ms) für den IO-Zyklus aus (siehe Abbildung 12).
☐ Wählen Sie unter `Ansprechüberwachungszeit/Anzahl akzeptierter Aktualisierungszyklen mit fehlenden IO-Daten` die gewünschte Anzahl für den IO-Zyklus aus (siehe Abbildung 12).
☐ Klicken Sie auf „OK“, um das Eigenschaften-Fenster zu schließen.

Medienredundanz konfigurieren

☐ Klicken Sie in der Hardware-Konfiguration mit der rechten Maustaste auf den Switch und wählen Sie `Objekteigenschaften`.

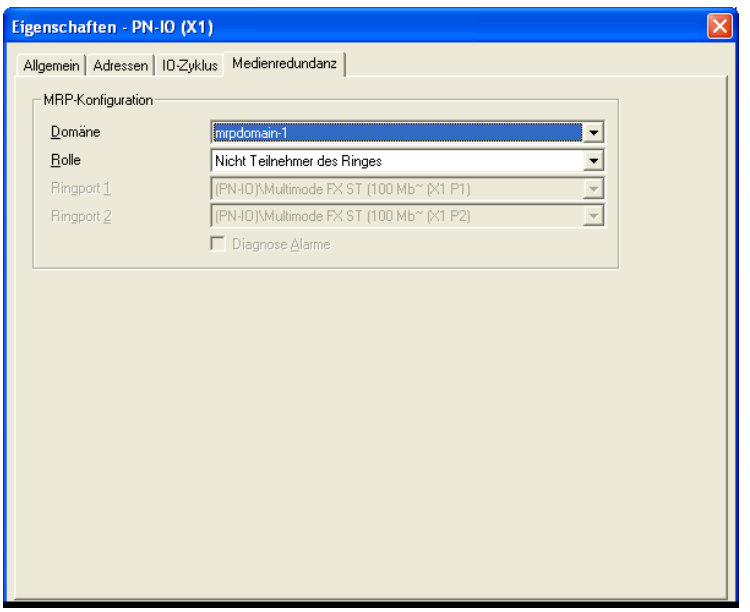


Abb. 13: Dialog zur Eingabe der Medienredundanz

☐ Wählen Sie im Eigenschaften-Fenster die Karteikarte "Medienredundanz".
☐ Wählen Sie unter `MRP-Konfiguration/Domäne` die gewünschte MRP-Domäne für den Teilnehmer aus (siehe Abbildung 13).
☐ Wählen Sie unter `MRP-Konfiguration/Rolle` die gewünschte Rolle des Teilnehmers im Ring aus (siehe Abbildung 13).
☐ Wählen Sie unter "Ring Port 1/2" die aktiven MRP Ring Ports aus.
☐ Klicken Sie auf „OK“, um das Eigenschaften-Fenster zu schließen.

Module für modulare Geräte hinzufügen

☐ Ziehen Sie mit Drag & Drop ein Modul aus der Bibliothek in einen Slot. Simatic S7 fügt über die Modul-Eigenschaften die Ports hinzu.

Geräte-Eigenschaft konfigurieren

Auf dem Steckplatz 0 nehmen Sie Einstellungen für den gesamten Switch vor.

☐ Markieren Sie den Switch.

☐ Klicken Sie mit der rechten Maustaste auf den Steckplatz 0.
Zur Konfiguration des gesamten Gerätes wählen Sie `Objekteigenschaften`.

☐ Wählen Sie im Eigenschaften-Fenster die Karteikarte "Parameter".

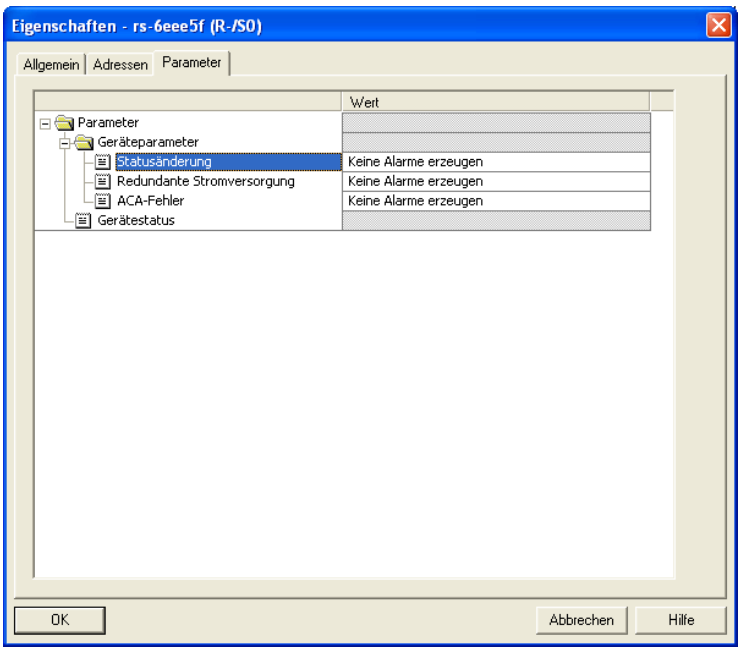


Abb. 14: Geräte-Alarme für z.B. RS20/RS30 konfigurieren.

Port-Eigenschaften konfigurieren

Bei den modularen Geräten stellen die Steckplätze 1 bis n die Module dar. Innerhalb der Steckplätze sind die Ports als Records abgebildet. Bei den nichtmodularen Geräten stellen die Steckplätze 1 bis n die Ports dar.

Alarme konfigurieren

☐ Klicken Sie mit der rechten Maustaste auf einen der Steckplätze 1 bis n und wählen Sie `Objekteigenschaften`.
☐ Wählen Sie im Eigenschaften-Fenster die Karteikarte "Parameter".
☐ Wählen Sie die gewünschten Alarme aus und schließen Sie das Fenster (siehe Abbildung 15).

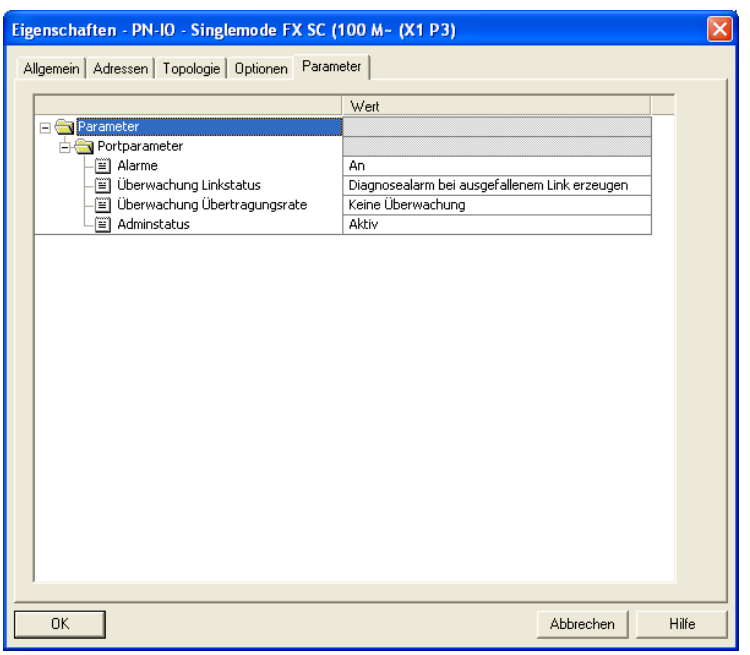


Abb. 15: Port-Eigenschaften

Sonderfall „LinkDown“-Alarm:
Der LinkDown-Alarm setzt sich zusammen aus der UND-Verknüpfung
– des Hirschmann-spezifischen Status für Verbindungsfehler und
– der Simatic S7-spezifischen Option für die Verbindung.

Aktivierung des LinkDown-Alarms:

☐ Wählen Sie unter `Objekteigenschaften` die Karteikarte `Parameter`(Hirschmann-spezifisch).
Schalten Sie „Alarme“ ein und wählen Sie unter „Überwachung Linkstatus“ die Option `Diagnosealarm beim ausgefallenem Link erzeugen`.

☐ Wählen Sie unter `Objekteigenschaften` die Karteikarte `Optionen` (Simatic S7-spezifisch).
Zur Aktivierung der Verbindungsüberwachung wählen Sie unter `Verbindung/Übertragungsmedium/Duplex` eine feste Einstellung für den Port.

Verbindungs-Optionen konfigurieren

☐ Klicken Sie mit der rechten Maustaste auf einen der Steckplätze 1 bis n und wählen Sie `Objekteigenschaften`.

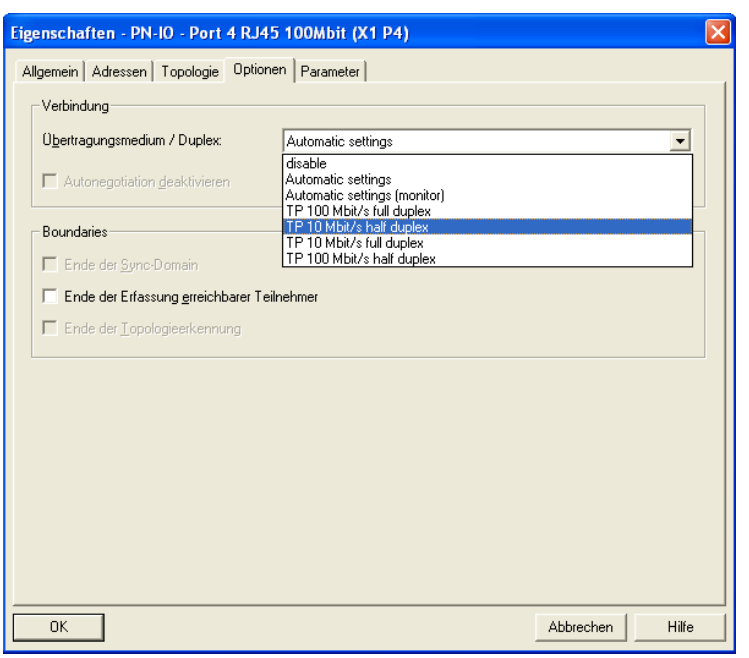


Abb. 16: Dialog zur Eingabe der Verbindungs-Optionen

☐ Wählen Sie im Eigenschaften-Fenster die Karteikarte „Optionen“.
☐ Wählen Sie unter „Verbindung/Übertragungsmedium/Duplex“ die gewünschte Einstellung für den Port aus (siehe Abbildung 16).

Beim Ändern der Port-Einstellung auf einen anderen Wert als `Automatische Einstellung` schaltet das Gerät den Port kurz aus. Wenn sich der Port auf dem Pfad zwischen I/O-Controller und I/O-Gerät befindet, scheitert durch diese Unterbrechung möglicherweise der Aufbau der Application Relation. Treffen Sie folgende Vorkehrungen, bevor Sie die Port-Einstellung ändern:

▶ Vorsicht Loops! Deaktivieren Sie RSTP auf den Ports zwischen I/O-Controller und I/O-Gerät.
  ☐ Öffnen Sie den Dialog „Redundanz:Spanning Tree:Port“.
  ☐ Heben Sie für den betreffenden Port die Markierung im Kontrollkästchen „Stp aktiv“ auf.
  ☐ Speichern Sie die Einstellungen.

▶ Aktivieren Sie "Fast Start Up" auf den Ports zwischen I/O-Controller und I/O-Gerät.
  ☐ Öffnen Sie den Dialog „Erweitert:Industrie-Protokolle:PROFINET“.
  ☐ Legen Sie für den betreffenden Port im Feld „Fast Start Up“ den Wert `enable` fest.
  ☐ Speichern Sie die Einstellungen.

☐ Klicken Sie „OK“, um das Eigenschaften-Fenster zu schließen.

Topologie konfigurieren

☐ Klicken Sie mit der rechten Maustaste auf einen der Steckplätze 1 bis n und wählen Sie `Objekteigenschaften`.

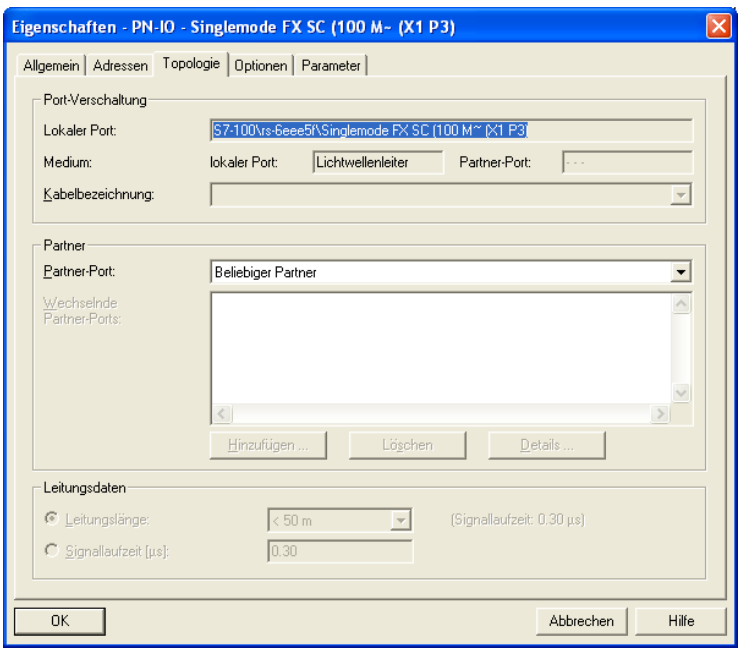


Abb. 17: Dialog zur Eingabe der Topologie

☐ Wählen Sie im Eigenschaften-Fenster die Karteikarte "Topologie".
☐ Wählen Sie unter `Port-Verschaltung/Lokaler Port` die gewünschte Einstellung für den Port aus (siehe Abbildung 17).
☐ Wählen Sie unter `Partner/Partner-Port` die gewünschte Einstellung für den Partner-Port aus (siehe Abbildung 17).
☐ Klicken Sie auf „OK“, um das Eigenschaften-Fenster zu schließen.

3.1.3 Konfiguration des Gerätes

Im Lieferumfang Ihres Gerätes finden Sie das Programm „Hirschmann Tool Calling Interface“, das Sie mit dem Installationsprogramm `HirschmannToolCallingInterfaceXXXXXSetup.exe` installieren können (`XXXXX` = Software-Version, z.B. 01000).
Nach der Installation des Programms „Hirschmann Tool Calling Interface“ haben Sie die Möglichkeit, in Simatic S7 zwei Hirschmann-Bedienprogramme zu starten, um weitergehende Konfigurationen des Gerätes vorzunehmen.

☐ Klicken Sie in Simatic S7 mit der rechten Maustaste auf ein Gerät und wählen Sie im Ausklappmenü das Web-based Interface (WWW) oder Telnet.

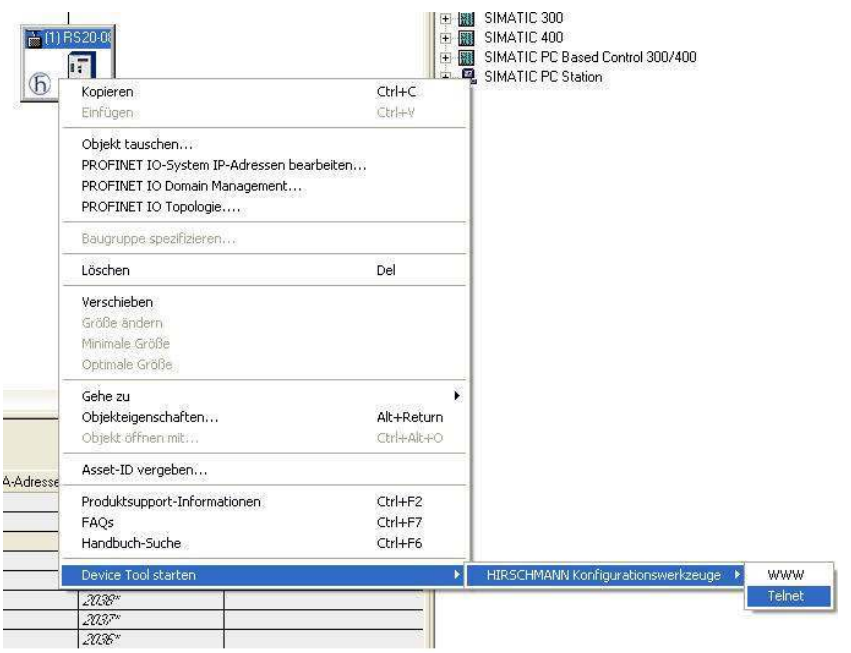


Abb. 18: Hirschmann-Bedienprogramm aufrufen

3.1.4 Tauschen von Geräten

Hirschmann-Geräte unterstützen die Funktion des Gerätetausches mit einer Engineering-Station.
Beim Tauschen gleicher Geräte weist die Engineering-Station dem Austauschgerät die Parameter des ursprünglichen Gerätes zu.

Die Funktion des Gerätetausches mit Simatic S7 erfordert folgende Voraussetzungen:
- S7 300 mit SW Stand ab V2.7 (z.Zt. für CPU 319 verfügbar) oder S7 400 mit SW Stand ab V5.2
- Hirschmann Gerät mit SW Release ab 05.0.00
- Nachbargerät(e) unterstützen LLDP
- Topologie (=Nachbarschaftsbeziehungen) ist konfiguriert und auf SPS geladen

Der Gerätetausch erfordert folgende Voraussetzungen:
- das Tauschgerät ist genau vom gleichen Typ wie das zu tauschende Gerät.
- das Tauschgerät ist genau an der gleichen Stelle im Netz (gleiche Ports und Nachbargeräte) angeschlossen.
- das Tauschgerät besitzt eine Profinet-Default-Konfiguration. Setzen Sie den Gerätenamen auf "" (leerer String).

Wenn alle diese Voraussetzungen erfüllt sind, weist die Engineering-Station dem Tauschgerät automatisch die Parameter des ursprünglichen Gerätes (Gerätename, IP-Parameter und Projektierungsdaten) zu.

Vorgehensweise beim Gerätetausch:
☐ Versetzen Sie das Austauschgerät in den Lieferzustand:
  - SystemName „“ (= Leerstring)
  - IP Adresse = 0.0.0.0 oder DHCP)
  - PROFINET IO eingeschaltet
☐ Notieren Sie sich die Portbelegung des ursprünglichen Gerätes und entfernen Sie das ursprüngliche Gerät aus Anlage.
  Daraufhin erkennt die SPS einen Fehler.
☐ Setzen Sie das Austauschgerät an der gleichen Stelle im Netz wieder ein. Beachten Sie die gleiche Portbelegung wie beim ursprünglichen Gerät.

Die SPS findet das Austauschgerät und konfiguriert es wie das ursprüngliche Gerät.
Die SPS erkennt den ordnungsgemäßen Betrieb.
Setzten Sie gegebenenfalls die SPS wieder auf „Run“.

3.1.5 Tauschen von Modulen

Der PROFINET IO-Stack im Gerät erkennt eine Änderung der Modulbestückung und meldet die Änderung der Engineering-Station. Wenn ein zuvor projektiertes Modul aus dem Gerät entfernt wird, meldet die Engineering-Station Fehler.Wenn ein projektiertes, aber fehlendes Modul gesteckt wird, entfernt die Engineering-Station die Fehlermeldung.

3.1.6 Netz überwachen

Topologie-Erkennung

Nach der Initiierung der Topologie-Erkennung durch den Anwender sucht die Engineering-Station nach angeschlossenen Geräten.

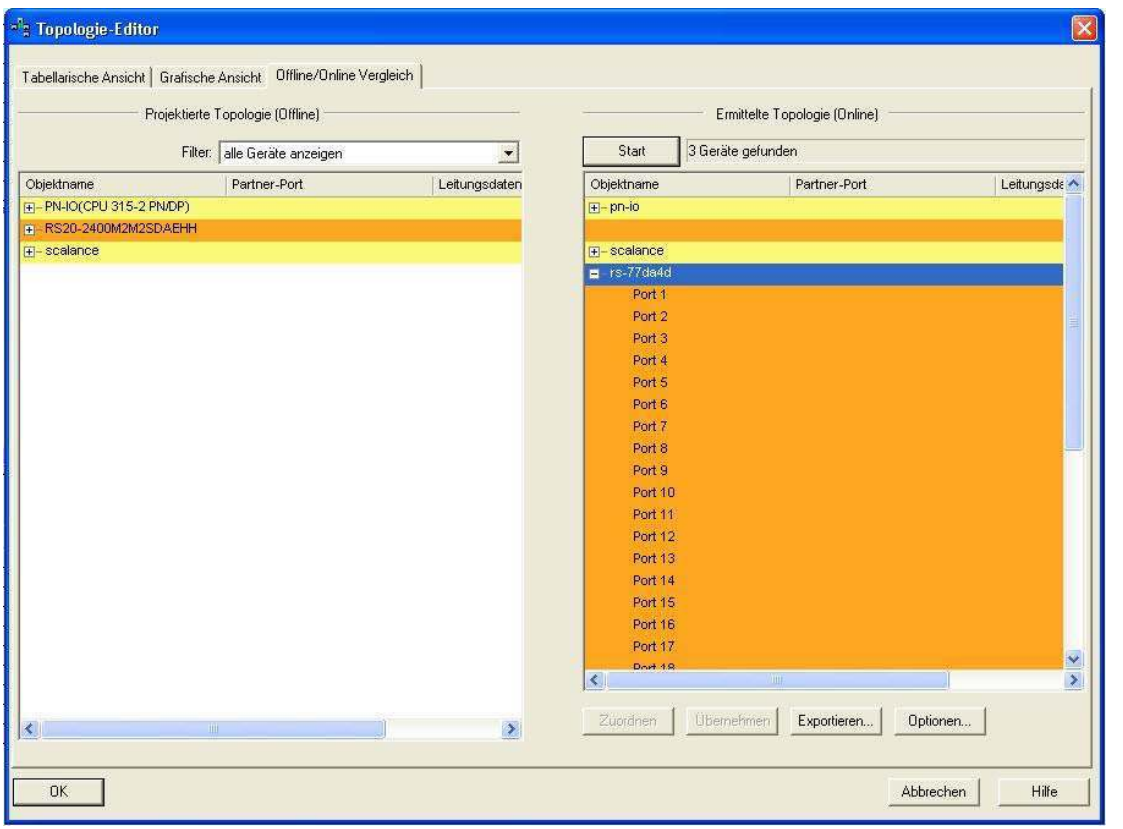


Abb. 19: Topologie-Erkennung

Topologie projektieren

Simatic S7 bietet dem Anwender die Möglichkeit, die Topologie zu konfigurieren und entsprechend zu überwachen.
Simatic S7 stellt Verbindungsparameter (Qualität und Einstellungen) in einer farbigen Grafik dar.

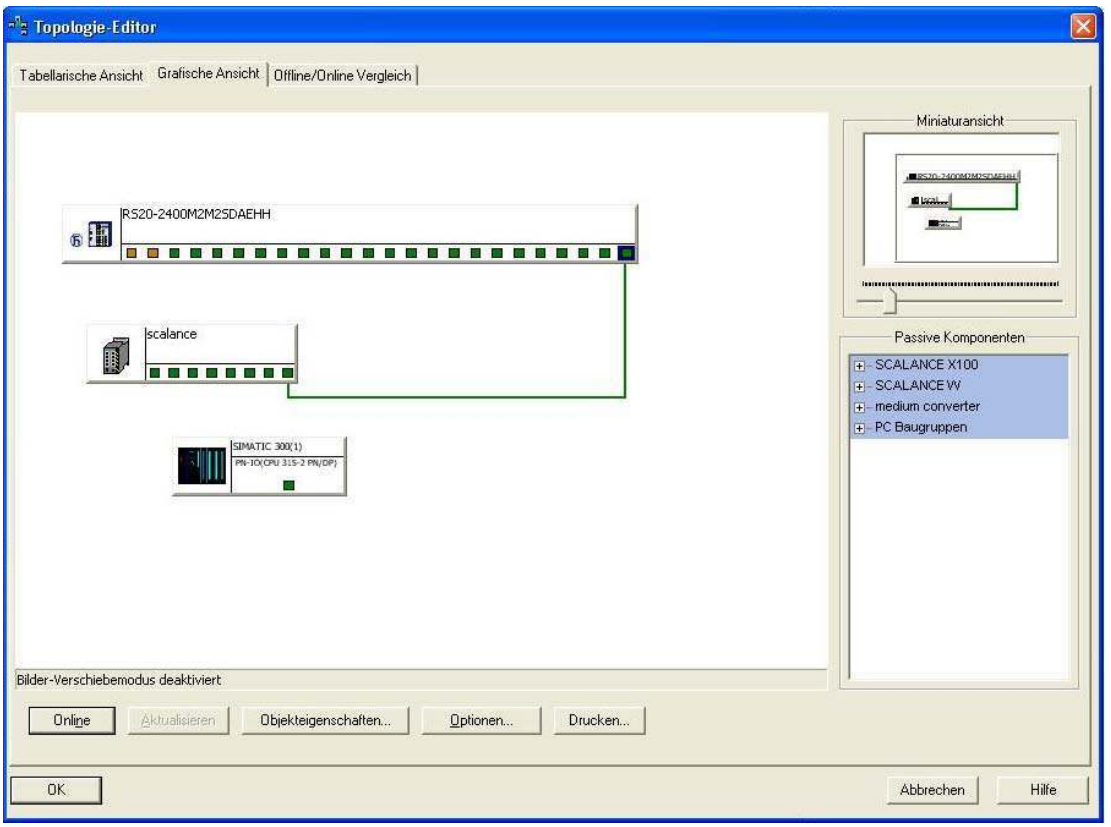


Abb. 20: Projektierung der Topologie

Kommunikationsdiagnose

Simatic S7 überwacht die Kommunikationsqualität und gibt Meldungen bezüglich Kommunikationsproblemen aus.

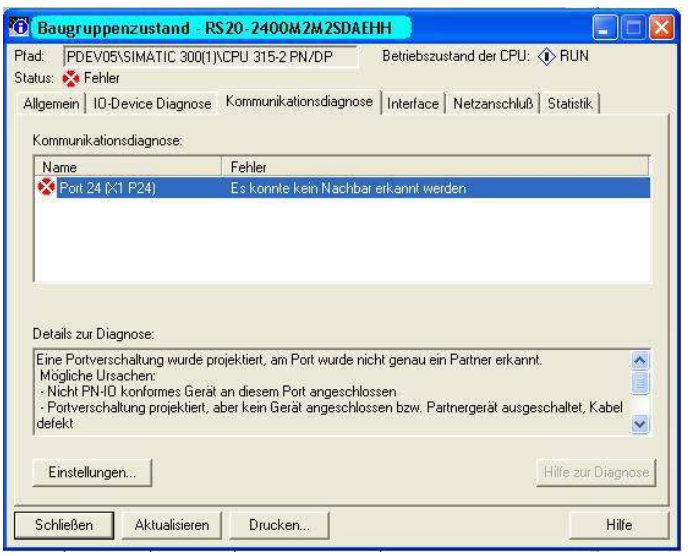


Abb. 21: Diagnosemeldungen zur Kommunikation zwischen den Switches und IO-Geräten

Portstatistiken ausgeben

Simatic S7 zählt je Port die Anzahl empfangener und gesendeter Datenpakete, Kollissionen, usw. Diese Zählerstände können Sie in Form von Statistiktabellen in Simatic S7 einsehen.

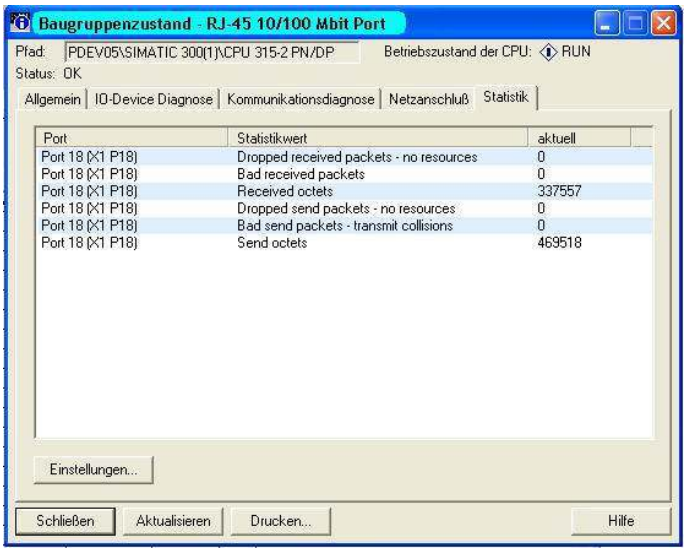


Abb. 22: Beispiel für Portstatistiktabelle

3.2 PROFINET IO-Parameter

3.2.1 Alarme

Der Switch unterstützt Alarme auf Geräte-Ebene und auf Port-Ebene (siehe „Gerätestatus“ im Anwender-Handbuch Grundkonfiguration oder im Referenz-Handbuch Web-based Interface.

Alarme auf Geräte-Ebene	- Änderung des Gerätestatus - Ausfall der redundanten Spannungsversorgung - Ausfall/Entfernen des ACA
Alarme auf Port-Ebene	- Änderung des Linkstatus, - Überschreiten einer vorgegebenen Übertragungsrate.

Tab. 11: Unterstützte Alarme

3.2.2 Record-Parameter

Der Switch bietet Records für:
- Geräte-Parameter
- Geräte-Status
- Port-Status/Parameter

Byte	Inhalt	Zugriff	Wert	Bedeutung
0	Alarm bei Status-wechsel verschicken	rw	0	Keine Alarme verschicken
			1	Alarm verschicken, wenn einer der folgenden Alarmgünde auftritt.
1	Power Alarm	rw	0	Keinen Alarm verschicken
			1	Alarm verschicken, wenn eine Spannungsver-sorgung ausfällt.
2	ACA Alarm	rw	0	Keinen Alarm verschicken
			1	Alarm verschicken, wenn der ACA entfernt wird.
3	Modul Alarm	rw	0	Keinen Alarm verschicken
			1	Alarm verschicken, wenn sich die Modulbe-stückung ändert.

Tab. 12: Geräte-Parameter

Byte	Inhalt	Zugriff	Wert	Bedeutung
0	Gerätestatus	ro	0	Nicht verfügbar
			1	OK
			2	Fehler
1	Netzteil 1	ro	0	Nicht verfügbar
			1	OK
			2	Fehler
2	Netzteil 2	ro	0	Nicht verfügbar
			1	OK
			2	Fehler
3	Netzteil 3	ro	0	Nicht verfügbar
			1	OK
			2	Fehler
4	Netzteil 4	ro	0	Nicht verfügbar
			1	OK
			2	Fehler
5	Netzteil 5	ro	0	Nicht verfügbar
			1	OK
			2	Fehler
6	Netzteil 6	ro	0	Nicht verfügbar
			1	OK
			2	Fehler
7	Netzteil 7	ro	0	Nicht verfügbar
			1	OK
			2	Fehler

Tab. 13: Geräte-Status

Byte	Inhalt	Zugriff	Wert	Bedeutung
8	Netzteil 8	ro	0	Nicht verfügbar
			1	OK
			2	Fehler
9	Meldekontakt 1	ro	0	Nicht verfügbar
			1	Geschlossen
			2	Offen
10	Meldekontakt 2	ro	0	Nicht verfügbar
			1	Geschlossen
			2	Offen
11	Temperatur	ro	0	Nicht verfügbar
			1	OK
			2	Schwellwert für die Temperatur über- oder unterschritten
12	Lüfter	ro	0	Nicht verfügbar
			1	OK
			2	Lüfter ausgefallen
13	Modul entfernen	ro	0	Nicht verfügbar
			1	OK
			2	Ein Modul wurde entfernt.
14	ACA entfernen	ro	0	Nicht verfügbar
			1	OK
			2	Der ACA wurde entfernt.
15	HIPER_Ring	ro	0	Nicht verfügbar
			1	OK
			2	Redundanzgewährleistung entfallen.
16	Ring-/Netzkopplung	ro	0	Nicht verfügbar
			1	OK
			2	Redundanzgewährleistung entfallen.
17	Verbindung	ro	0	Nicht verfügbar
			1	OK
			2	Verbindungsausfall.

Tab. 13: Geräte-Status

Byte	Inhalt	Zugriff	Wert	Bedeutung
0	Portfehler melden	rw	0	Keine Alarme verschicken
			1	Alarm verschicken, wenn einer der folgenden Alarmgünde auftritt.

Tab. 14: Port-Status/Parameter

Byte	Inhalt	Zugriff	Wert	Bedeutung
1	Verbindungsfehler melden	rw	0	Keinen Alarm verschicken
	1		Alarm verschicken, wenn die Verbindung ausgefallen ist.	
2	Übertragungsrate zu hoch	rw	0	Keinen Alarm verschicken
			1	Alarm verschicken, wenn der Schwellwert für die Temperatur überschritten ist
3	Port an	rw	0	nicht verfügbar
			1	Eingeschaltet
			2	Ausgeschaltet
4	Link-Status	ro	0	nicht verfügbar
			1	Verbindung vorhanden
			2	Verbindung unterbrochen
5	Bitrate	ro	0	nicht verfügbar
			1	Unbekannt
			2	10 MBit/s
			2	100 MBit/s
			2	1000 MBit/s
6	Duplex	ro	0	nicht verfügbar
			1	Halbduplex
			2	Vollduplex
7	Autonegotiation	ro	0	nicht verfügbar
			1	Aus
			2	Ein

Tab. 14: Port-Status/Parameter

3.2.3 I/O-Daten

Die Zuordnung der Bits der übertragenen I/O-Daten entnehmen Sie der folgenden Tabelle.

Richtung	Byte	Bit	Bedeutung
Input	0		Allgemein
		0	Gerätestatus
		1	Meldekontakt 1
		2	Meldekontakt 2
		3	Temperatur
		4	Lüfter
		5	Modul entfernen
		6	ACA entfernen
		7	nicht benutzt
Input	1		Netzteil-Zustand
		0	Netzteil 1
		1	Netzteil 2
		2	Netzteil 3
		3	Netzteil 4
		4	Netzteil 5
		5	Netzteil 6
		6	Netzteil 7
		7	Netzteil 8
Input	2		Versorgungsspannungs-Zustand
		0	HIPER-Ring
		1	Ring-/Netzkopplung
		2	VVerbindungsfehler
		3	nicht benutzt
		4	nicht benutzt
		5	nicht benutzt
		6	nicht benutzt
		7	nicht benutzt
Output			nicht definiert
Bedeutung des Bitinhaltes: - 0: in Ordnung oder nicht verfügba - 1: Meldegrund vorhanden			

Tab. 15: Geräte-I/O-Daten

Richtung	Byte	Bit	Bedeutung
Input	0		Verbindungsstatus für die Ports 1 bis 8
		0	Port 1
		1	Port 2
		2	Port 3
		3	Port 4
		4	Port 5
		5	Port 6
		6	Port 7
		7	Port 8
Input	1		Verbindungsstatus für die Ports 9 bis 16
		0	Port 9
		1	Port 10
		2	Port 11
		3	Port 12
		4	Port 13
		5	Port 14
		6	Port 15
		7	Port 16
Input	n		Verbindungsstatus für die Port (n * 8) + 1 bis Port (n * 8) + 8
		0	Port (n * 8) + 1
		1	Port (n * 8) + 2
		2	Port (n * 8) + 3
		3	Port (n * 8) + 4
		4	Port (n * 8) + 5
		5	Port (n * 8) + 6
		6	Port (n * 8) + 7
		7	Port (n * 8) + 8
Bedeutung des Input-Bitinhaltes: - 0: keine Verbindung - 1: aktive Verbindung			
Output	0		„Port eingeschaltet“ für die Ports 1 bis 8
		0	Port 1 eingeschaltet
		1	Port 2 eingeschaltet
		2	Port 3 eingeschaltet
		3	Port 4 eingeschaltet
		4	Port 5 eingeschaltet
		5	Port 6 eingeschaltet
		6	Port 7 eingeschaltet
		7	Port 8 eingeschaltet

Tab. 16: Port-I/O-Daten

Richtung	Byte	Bit	Bedeutung
Output	1		„Port eingeschaltet“ für die Ports 9 bis 16
		0	Port 9 eingeschaltet
		1	Port 10 eingeschaltet
		2	Port 11 eingeschaltet
		3	Port 12 eingeschaltet
		4	Port 13 eingeschaltet
		5	Port 14 eingeschaltet
		6	Port 15 eingeschaltet
		7	Port 16 eingeschaltet
Output	n		„Port eingeschaltet“ für die Port (n * 8) + 1 bis Port (n * 8) + 8
		0	Port (n * 8) + 1 eingeschaltet
		1	Port (n * 8) + 2 eingeschaltet
		2	Port (n * 8) + 3 eingeschaltet
		3	Port (n * 8) + 4 eingeschaltet
		4	Port (n * 8) + 5 eingeschaltet
		5	Port (n * 8) + 6 eingeschaltet
		6	Port (n * 8) + 7 eingeschaltet
		7	Port (n * 8) + 8 eingeschaltet
Bedeutung des Output-Bitinhaltes: - 0: Port eingeschaltet - 1: Port ausgeschaltet			

Tab. 16: Port-I/O-Daten

4 IEC 61850/MMS (RSR20/RSR30/MACH1000)

IEC 61850/MMS ist ein von der International Electrotechnical Commission (IEC) standardisiertes industrielles Kommunikationsprotokoll. Anzutreffen ist das Protokoll in der Schaltanlagenautomatisierung, z. B. in der Leittechnik von Energieversorgern.

Das paketorientiert arbeitende Protokoll basiert auf dem Transportprotokoll TCP/IP und nutzt Manufacturing Messaging Specification (MMS) für die Client-Server-Kommunikation. Das Protokoll ist objektorientiert und definiert eine einheitliche Konfigurationssprache, die u. a. Funktionen für SCADA, Intelligent Electronic Devices (IED) und für die Netzleittechnik umfasst.

Teil 6 der Norm IEC 61850 definiert die Konfigurationssprache SCL (Substation Configuration Language). SCL beschreibt die Eigenschaften des Gerätes sowie die Systemstruktur in maschinell verarbeitbarer Form. Die mit SCL beschriebenen Eigenschaften des Gerätes sind in der ICD-Datei auf dem Gerät gespeichert.

4.1 Switch-Modell für IEC 61850

Der Technical Report IEC 61850 90-4 spezifiziert ein Bridge-Modell. Die Funktionen eines Switches bildet das Bridge-Modell als Objekte eines Intelligent Electronic Devices (IED) ab. Ein MMS-Client (z. B. die Leitstellen-Software) verwendet diese Objekte, um das Gerät zu überwachen und zu konfigurieren.

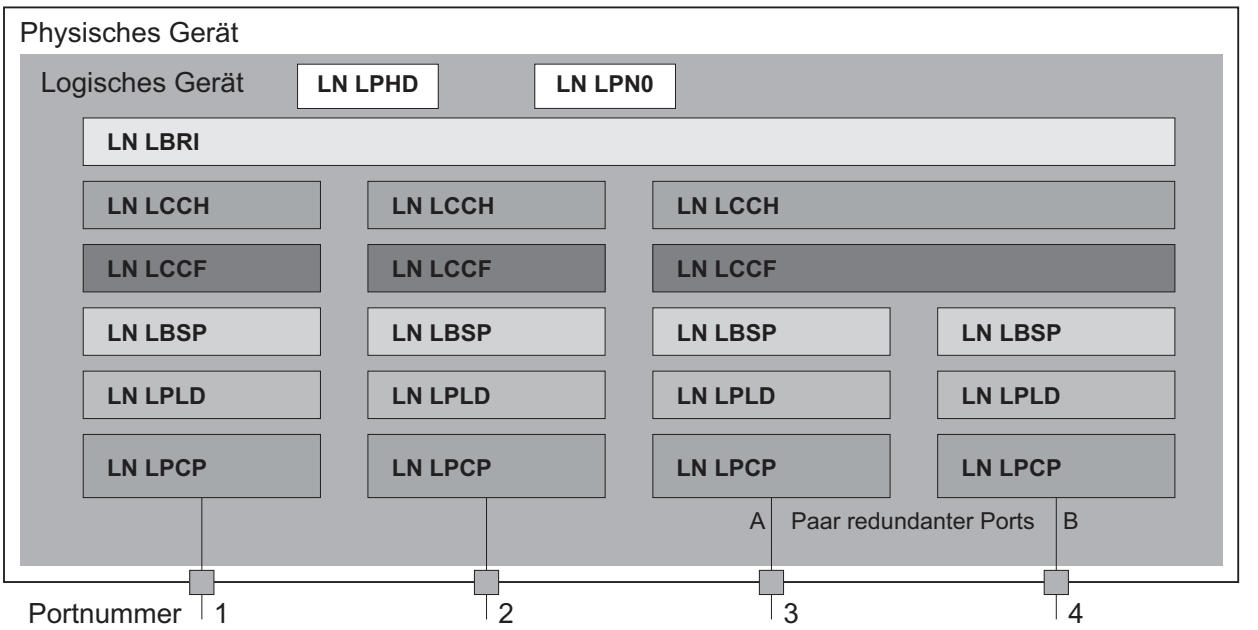


Abb. 23: Bridge-Modell nach Technical Report IEC 61850 90-4

Klasse	Beschreibung
LN LLN0	Logischer Knoten „Zero“ des IED „Bridge“: Definiert die logischen Eigenschaften des Geräts.
LN LPHD	Logischer Knoten „Physical Device“ des IED „Bridge“: Definiert die physischen Eigenschaften des Geräts.
LN LBRI	Logischer Knoten „Bridge“: Bildet generelle Einstellungen der Bridge-Funktionen des Gerätes ab.

Tab. 17: Klassen des Bridge-Modells nach TR IEC61850 90-4

Klasse	Beschreibung
LN LCCH	Logischer Knoten „Communication Channel“: Definiert den logischen „Communication Channel“, der aus einem oder mehreren physischen Geräteports besteht.
LN LCCF	Logischer Knoten „Channel Communication Filtering“: Definiert die VLAN- und Multicast-Einstellungen für den übergeordneten „Communication Channel“.
LN LBSP	Logischer Knoten „Port Spanning Tree Protocol“: Definiert die Spanning-Tree-Zustände und -Einstellungen für den jeweiligen physischen Geräteport.
LN LPLD	Logischer Knoten „Port Layer Discovery“: Definiert die LLDP-Zustände und -Einstellungen für den jeweiligen physischen Geräteport.
LN LPCP	Logischer Knoten „Physical Communication Port“: Repräsentiert den jeweiligen physischen Geräteport.

Tab. 17: Klassen des Bridge-Modells nach TR IEC61850 90-4 (Forts.)

4.2 Integration in ein Steuerungssystem

4.2.1 Vorbereitung des Switch

Nach der Installation und dem Anschließen des Switch konfigurieren Sie ihn nach dem Anwender-Handbuch Grundkonfiguration:

☐ Prüfen Sie, dass dem Gerät eine IP-Adresse zugewiesen ist.

☐ Um den MMS-Server zu starten, schalten Sie in der grafischen Benutzeroberfläche im Dialog `Erweitert:Industrie-Protokolle:IEC61850` die Funktion an.
Anschließend ist ein MMS-Client in der Lage, sich mit dem Gerät zu verbinden sowie die im Bridge-Modell definierten Objekte auszulesen und zu überwachen.

⚠ WARNUNG

GEFAHR DES UNAUTORISIERTEN ZUGRIFFS AUF DAS GERÄT

IEC61850/MMS bietet keine Authentifizierungsmechanismen. Ist der Schreibzugriff für IEC61850/MMS eingeschaltet, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Gerätes ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Gerätes und zu Ausfällen im Netz.
Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (z.B. Firewall, VPN etc.) getroffen haben, um das Risiko unautorisierter Zugriffe auszuschließen.

Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.

☐ Um dem MMS-Client das Konfigurieren der im Bridge-Modell definierten Objekte zu ermöglichen, markieren Sie das Kontrollkästchen „Schreibzugriff“.

4.2.2 Offline-Konfiguration

Das Gerät bietet Ihnen die Möglichkeit, mit Hilfe der grafischen Benutzeroberfläche die ICD-Datei herunterzuladen. Diese Datei enthält die mit SCL beschriebenen Eigenschaften des Gerätes und ermöglicht das Projektieren der Schaltanlage ohne direkte Verbindung zum Gerät.

☐ Laden Sie die ICD-Datei herunter, indem Sie im Dialog `Erweitert:Industrie-Protokolle:IEC61850` die Schaltfläche „Download ICD-Datei“ klicken.

4.2.3 Gerät überwachen

Der im Gerät integrierte IEC61850/MMS-Server bietet die Möglichkeit, mehrere Stati des Gerätes per Report Control Block (RCB) zu überwachen. Bis zu 5 MMS-Clients können sich gleichzeitig für einen Report Control Block anmelden.

Das Gerät ermöglicht das Überwachen der folgenden Stati:

Klasse	RCB-Objekt	Beschreibung
LN LPHD	PwrSupAlm	Ändert sich, wenn eine der redundanten Spannungsversorgungen ausfällt oder wieder in Betrieb geht.
	TmpAlm	Ändert sich, wenn die im Gerät gemessene Temperatur die festgelegten Temperaturgrenzen über- oder unterschreitet.
	PhyHealth	Ändert sich, wenn sich der Zustand der RCB-Objekte „LPHD.PwrSupAlm“ oder „LPHD.TmpAlm“ ändert.
LN LBRI	Health	Ändert sich, wenn sich der Zustand der RCB-Objekte „LPHD.PwrSupAlm“ oder „LPHD.TmpAlm“ ändert.
	RstpRoot	Ändert sich, wenn das Gerät die Rolle der Root-Bridge übernimmt oder abgibt.
	RstpTopoCnt	Ändert sich, wenn sich die Topologie auf Grund eines Wechsels der Root-Bridge ändert.
LN LCCH	ChLiv	Ändert sich, wenn sich der Link-Status des physischen Ports ändert.
LN LPCP	PhyHealth	Ändert sich, wenn sich der Link-Status des physischen Ports ändert.

Tab. 18: Mit IEC 61850/MMS überwachbare Stati des Gerätes

A GSD-Datei-Generator

Das Programm „Standalone GSD-Datei-Generator“ finden Sie auf der Produkt-CD. Das Programm bietet Ihnen die Möglichkeit, von einem fiktiven Gerät eine GSDML-Datei (PROFINET IO) mit Icon zu erzeugen. Mit Hilfe dieser Dateien können Sie Geräte, die noch nicht im Netz installiert sind, in Ihrer Engineering-Station projektieren.

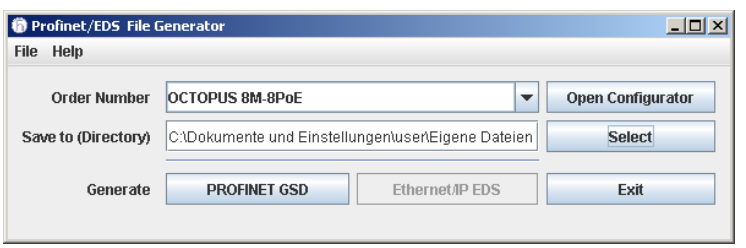


Abb. 24: Standalone GSD-Datei-Generator

B Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, um Sie beim Einsatz dieses Produkts zu unterstützen. Ihre Kommentare und Anregungen helfen uns dabei, die Qualität und den Informationsgrad dieser Dokumentation weiter zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	**gut**	**befriedigend**	**mäßig**	**schlecht**
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Leserkritik

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer +49 (0)7127 14-1600 oder
- per Post an

  Hirschmann Automation and Control GmbH
  Abteilung 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

C Stichwortverzeichnis

A
Alarm 56
Alarmeinstellung 37

C
CIP 15
Common Industrial Protocol 15

E
EDS 17, 69
Engineering-Station 50, 51
Engineering-System 38
EtherNet/IP-Web-Site 16

F
FAQ 75

G
Generic Ethernet Module 18
Gerätebeschreibungssprache 33
GSD 36, 69
GSDML 33
GSDML file Generator 37
GSDML-Datei 39

I
Icon 17, 36, 39
IEC 61850 63
IGMP-Snooping 17
Industrial HiVision 8
Industrieprotokolle 7

K
Konformitätsklasse 33

M
MMS 63
Modul-Eigenschaften 43

O
ODVA 15
ODVA-Web-Site 16

P
PC Worx 38
PROFIBUS-Organisation 33
PROFINET IO 7

R
Record 45, 56
Redundanz 7
Request Packet Intervall 19
Router-Funktion 17
RPI 19
RS Who 17

S
Schulungsangebote 75
Schwellwert 37
Simatic S7 38
Standalone GSD File Generator 38
Symbol 9

T
TCP/IP 15, 33
Technische Fragen 75

U
UDP/IP 15, 33

D Weitere Unterstützung

Technische Fragen

Bei technischen Fragen wenden Sie sich bitte an den Hirschmann-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann.

Die Adressen unserer Vertragspartner finden Sie im Internet unter http://www.hirschmann.com

Unser Support steht Ihnen zur Verfügung unter https://hirschmann-support.belden.eu.com

Sie erreichen uns

in der Region EMEA unter
- Tel.: +49 (0)1805 14-1538
- E-Mail: hac.support@belden.com

in der Region Amerika unter
- Tel.: +1 (717) 217-2270
- E-Mail: inet-support.us@belden.com

in der Region Asien-Pazifik unter
- Tel.: +65 6854 9860
- E-Mail: inet-ap@belden.com

Hirschmann Competence Center

Das Hirschmann Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen hat vor den Wettbewerbern gleich dreifach die Nase vorn:

- Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
  Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter http://www.hicomcenter.com
- Der Support reicht von der Inbetriebnahme über den Bereitschafts-service bis zu Wartungskonzepten.

Mit dem Hirschmann Competence Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

Anwender-Handbuch

Redundanz-Konfiguration
Industrial ETHERNET (Gigabit-)Switch
PowerMICE, MACH 104, MACH 1040, MACH 4000

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

© 2015 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken. Bei Geräten mit eingebetteter Software gilt die Endnutzer-Lizenzvereinbarung auf der mitgelieferten CD/DVD.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die jeweils neueste Version dieses Handbuches finden Sie im Internet auf den Hirschmann-Produktseiten (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Rel. 9.0 - 02/2015 – 27.02.2015

Inhalt

Sicherheitshinweise 7

Über dieses Handbuch 9

Legende 11

1 Einleitung 13

1.1 Übersicht Redundanz-Topologien 14

1.2 Übersicht Redundanzverfahren 16

2 Link-Aggregation 19

2.1 Beispiel für Link-Aggregation 20
2.1.1 Link-Aggregation anlegen und konfigurieren 21

2.2 HIPER-Ring und Link-Aggregation (PowerMICE und MACH 4000) 26

3 Ring-Redundanz 29

3.1 Beispiel für HIPER-Ring 31
3.1.1 HIPER-Ring einrichten und konfigurieren 33

3.2 Beispiel für MRP-Ring 37

4 Multiple Ringe 43

4.1 Sub-Ring 44
4.1.1 Sub-Ring-Beschreibung 44
4.1.2 Sub-Ring-Beispiel 48
4.1.3 Konfiguration des Sub-Ring-Beispiels 51

5 Ring-/Netzkopplung 57

5.1 Die Varianten der Ring-/Netzkopplung 58

5.2 Ring-/Netzkopplung vorbereiten 60
5.2.1 STAND-BY-Schalter 60
5.2.2 Ein-Switch-Kopplung 64
5.2.3 Zwei-Switch-Kopplung 70
5.2.4 Zwei-Switch-Kopplung mit Steuerleitung 79

6 Spanning Tree 89

6.1 Das Spanning Tree Protokoll 91
6.1.1 Die Aufgaben des STP 91
6.1.2 Die Bridge-Parameter 92
6.1.3 Bridge-Identifikation (Bridge-Identifier) 92
6.1.4 Root-Pfadkosten 93
6.1.5 Portidentifikation 95

6.2 Regeln für die Erstellung der Baumstruktur 96
6.2.1 Bridge-Information 96
6.2.2 Aufbauen der Baumstruktur 96

6.3 Beispiel für die Bestimmung des Root-Pfads 99

6.4 Beispiel für die Manipulation des Root-Pfads 101

6.5 Beispiel für die Manipulation der Baumstruktur 103

6.6 Das Rapid Spanning Tree Protokoll 104
6.6.1 Port-Rollen 104
6.6.2 Port-Stati 107
6.6.3 Spanning Tree Priority Vector 108
6.6.4 Schnelle Rekonfiguration 108
6.6.5 Rapid Spanning Tree konfigurieren 109

6.7 Kombinieren von RSTP und MRP 120
6.7.1 Anwendungsbeispiel für die Kombination von RSTP und MRP 122

7 VRRP/HiVRRP 125

7.1 VRRP/HiVRRP Konfiguration 126
7.1.1 Generelle Einstellungen 126
7.1.2 VRRP-Instanz-Einstellungen 127
7.1.3 VRRP-Router-Instanz einrichten 129
7.1.4 VRRP-Router-Instanz konfigurieren 130
7.1.5 VRRP-Router-Instanz löschen 131

7.2 HiVRRP-Domänen 132
7.2.1 HiVRRP-Domänen anzeigen 132
7.2.2 HiVRRP-Domänen-Instanzen auf verschiedenen Ports 133

7.3 Statistik 134
7.3.1 VRRP-Statistik über alle Ports 134
7.3.2 VRRP-Statistik pro Port 134

7.4 Tracking 136
7.4.1 Tracking-Objekt löschen 137

A Leserkritik 138

B Stichwortverzeichnis 141

C Weitere Unterstützung 143

Sicherheitshinweise

⚠ WARNUNG
UNKONTROLLIERTE MASCHINENBEWEGUNGEN Um unkontrollierte Maschinenbewegungen aufgrund von Datenverlust zu vermeiden, konfigurieren Sie alle Geräte zur Datenübertragung individuell. Nehmen Sie eine Maschine, die mittels Datenübertragung gesteuert wird, erst in Betrieb, wenn Sie alle Geräte zur Datenübertragung vollständig konfiguriert haben. **Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.**

Über dieses Handbuch

Das Dokument „Anwender-Handbuch Redundanzkonfiguration“ enthält die Informationen, die Sie zur Auswahl des geeigneten Redundanzverfahrens und dessen Konfiguration benötigen.

Das Dokument „Anwender-Handbuch Grundkonfiguration“ enthält die Informationen, die Sie zur Inbetriebnahme des Gerätes benötigen. Es leitet Sie Schritt für Schritt von der ersten Inbetriebnahme bis zu den grundlegenden Einstellungen für einen Ihrer Umgebung angepassten Betrieb.

Das Dokument „Anwender-Handbuch Installation“ enthält eine Gerätebeschreibung, Sicherheitshinweise, Anzeigebeschreibung und weitere Informationen, die Sie zur Installation des Gerätes benötigen, bevor Sie mit der Konfiguration des Gerätes beginnen.

Das Dokument „Anwender-Handbuch Industrie-Protokolle“ beschreibt die Anbindung des Gerätes über ein in der Industrie übliches Kommunikationsprotokoll wie z.B. EtherNet/IP und PROFINET IO.

Das Dokument „Anwender-Handbuch Routing-Konfiguration“ enthält Informationen, die Sie zur Inbetriebnahme der Routing-Funktion benötigen. Das Handbuch versetzt Sie in die Lage, durch Ableitung aus den Beispielen Ihre Router zu konfigurieren.

Das Dokument „Referenz-Handbuch Grafische Benutzeroberfläche“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über die grafische Benutzeroberfläche.

Das Dokument „Referenz-Handbuch Command Line Interface“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über das Command Line Interface.

Die Netzmanagement-Software Industrial HiVision bietet Ihnen weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:

- ActiveX-Control für SCADA-Integration
- Autotopologie-Erkennung
- Browser-Interface
- Client/Server-Struktur
- Ereignisbehandlung
- Ereignislogbuch
- Gleichzeitige Konfiguration mehrerer Geräte
- Grafische Benutzeroberfläche mit Netz-Layout
- SNMP/OPC-Gateway

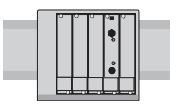
Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
☐	Arbeitsschritt
■	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	ASCII-Darstellung in der grafischen Benutzeroberfläche
	Ausführung in der grafischen Benutzeroberfläche
	Ausführung im Command Line Interface

Verwendete Symbole:

	WLAN-Access-Point
	Router mit Firewall
	Switch mit Firewall
	Router
	Switch

	Bridge
	Hub
	Beliebiger Computer
	Konfigurations-Computer
	Server
	SPS - Speicherprogrammier-bare Steuerung
	I/O - Roboter

1 Einleitung

Das Gerät enthält eine Vielfalt von Redundanzfunktionen:

- Link-Aggregation
- HIPER-Ring
- MRP-Ring
- Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 und MACH 4000)
- Ring-/Netzkopplung
- Rapid Spanning Tree Algorithmus (RSTP)
- VRRP/HiVRRP

1.1 Übersicht Redundanz-Topologien

Um auf Schicht 2 eines Netzes Redundanz einzuführen, legen Sie zunächst fest, welche Netz-Topologie Sie benötigen. In Abhängigkeit von der gewählten Netz-Topologie wählen Sie danach unter den Redundanzprotokollen aus, die sich mit dieser Netz-Topologie einsetzen lassen.

Folgende Topologien sind möglich:

Netz-Topologie	Mögliche Redundanzverfahren	Bemerkungen
Baumstruktur ohne Schleifen (zyklenfrei)	Ausschließlich im Zusammenhang mit physikalischer Schleifenbildung möglich	-
Topologie mit 1 Schleife	RSTP Ring-Redundanz	Ring-Redundanz-Verfahren (HIPER-Ring, Fast HIPER-Ring oder MRP) bieten kürzere Umschaltzeiten als RSTP.
Topologie mit 2 Schleifen	RSTP Ring-Redundanz Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 und MACH 4000)	Ring-Redundanz: ein Basis-Ring mit einem Sub-Ring oder ein MRP-Ring mit RSTP-Ring.
Topologie mit 3 nicht verschachtelten Schleifen	RSTP Ring-Redundanz Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 und MACH 4000) Ringkopplung	Die Ringkopplung bietet besondere Unterstützung bei redundanter Kopplung eines redundanten Rings an einen anderen redundanten Ring oder an eine beliebige Struktur, die ausschließlich mit Hirschmann-Geräten arbeitet
Topologie mit verschachtelten Schleifen	RSTP Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 und MACH 4000) Ringkopplung	Die Ringkopplung koppelt ausschließlich nichtverschachtelte Ringe, diese können jedoch wieder lokale Sub-Ringe ankoppeln.

Tab. 1: Übersicht über Redundanz-Topologien

Das Ring-Redundanz-Protokoll MRP bietet besondere Eigenschaften:

- Sie haben die Möglichkeit, MRP-Ringe zu verschachteln. Ein angekoppelter Ring heißt Sub-Ring (siehe auf Seite 44 „Sub-Ring“).
- Sie haben die Möglichkeit, an MRP-Ringe weitere Ringstrukturen anzukoppeln, die mit RSTP arbeiten (siehe auf Seite 120 „Kombinieren von RSTP und MRP“).

1.2 Übersicht Redundanzverfahren

Redundanz-verfahren	Netz-Topologie	Umschaltzeit
RSTP	beliebige Struktur	typ. < 1 s (STP < 30 s) bis zu < 30 s - stark abhängig von der Anzahl der Geräte
	Anmerkung: Bis zu 79 Geräte je nach Topologie und Konfiguration möglich. Bei Verwendung der Vorgabewerte (Fabrikeinstellungen) je nach Topologie bis zu 39 Geräte möglich (siehe auf Seite 89 „Spanning Tree“).	
HIPER-Ring	Ring	typ. 80 ms, bis zu < 500 ms oder < 300 ms (wählbar) - nahezu unabhängig von der Anzahl der Geräte.
MRP-Ring	Ring	typ. 80 ms, bis zu < 500 ms oder < 200 ms (wählbar) - nahezu unabhängig von der Anzahl der Geräte.
	Anmerkung: Bei Kombination mit RSTP im MRP-Kompatibilität-Modus je nach Konfiguration bis zu 39 Geräte möglich. Bei Verwendung der Vorgabe-werte (Fabrikeinstellungen) für RSTP bis zu 19 Geräte möglich (siehe auf Seite 89 „Spanning Tree“).	
Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 und MACH 4000)	An einen Basis-Ring angekoppeltes Ringsegment	typ. 80 ms, bis zu < 500 ms oder < 200 ms (wählbar) - nahezu unabhängig von der Anzahl der Geräte.
Link-Aggrega-tion	Kopplung von Netz-segmenten über parallele aktive Stre-cken mit dynamischer Lastverteilung und Streckenredundanz	
VRRP/HiVRR P	Beliebige Struktur; Stellt Endgeräten Redundanz für „Default Gateway“ bereit.	< 400 ms bei HiVRRP

Tab. 2: Redundanzverfahren im Vergleich

Anmerkung: Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Geräte-Ports. Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt.

2 Link-Aggregation

Das LACP (Link-Aggregation Control Protocol nach IEEE 802.3ad) ist ein Netzwerkprotokoll zur dynamischen Bündelung von physikalischen Netzverbindungen. Zur Datenübertragung steht die volle Bandbreite aller Verbindungsleitungen zur Verfügung. Im Falle des Ausfalls einer Verbindung übernehmen die verbleibenden Verbindungen den gesamten Datenverkehr (Redundanz). Die Lastverteilung zwischen den Verbindungsleitungen erfolgt automatisch.
Eine Link-Aggregation konfigurieren Sie, indem Sie zwischen 2 Geräten mindestens 2 vorhandene, parallele redundante Verbindungsleitungen (Leitungsbündel, engl.: Trunk) zu einer logischen Verbindung zusammengefassen. Mit Link-Aggregation können Sie max. 8 (optimal bis zu 4) Verbindungsleitungen zwischen Geräten zu einem Trunk zusammenfassen. Sie können in beliebiger Kombination Twisted-Pair- oder LWL-Kabel als Verbindungsleitungen eines Trunks verwenden. Konfigurieren Sie alle Verbindungen so, dass die Datenrate und die Duplexeinstellungen der beteiligten Ports übereinstimmen.
Von einem Gerät können maximal

– 2 Trunks bei Rail-Geräten mit 4 Ports,
– 4 Trunks bei Rail- und MICE-Geräten mit 8-10 Ports,
– 7 Trunks bei allen anderen Geräten

ausgehen.

2.1 Beispiel für Link-Aggregation

In einem Netz aus sieben Geräten in Linientopologie gibt es zwei Segmente mit besonders großem Datenaufkommen. Deshalb entscheiden Sie in diesen Segmenten Link-Aggregationen einzurichten. Neben der Lastverteilung auf mehrere Leitungen erhalten Sie so in diesen Segmenten auch eine höhere Ausfallsicherheit durch redundante Leitungen.
Die Link-Aggregation LATP (Link-Aggregation Twisted Pair) besteht aus 3 Twisted Pair Leitungen, die Link-Aggregation LAFO (Link-Aggregation Fiber Optic) aus zwei Glasfaserleitungen.

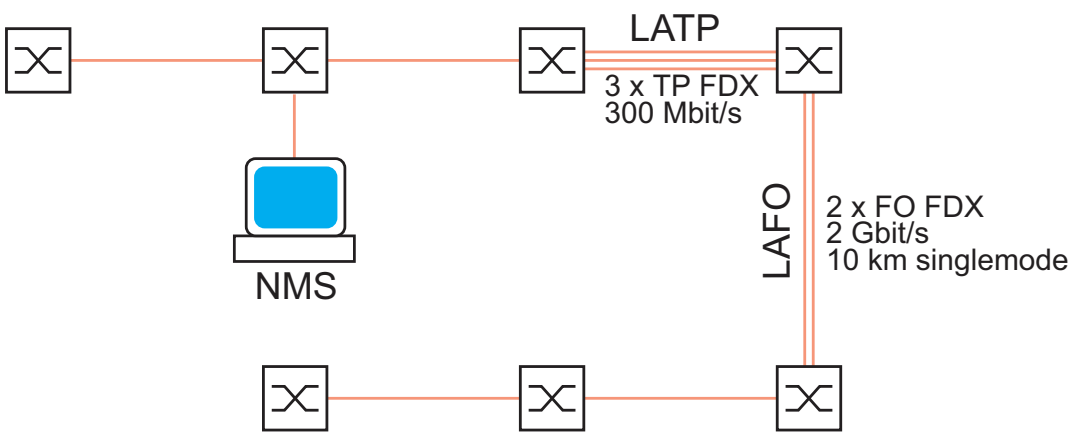


Abb. 1: Beispiel für Link-Aggregation
NMS = Netz-Management-Station
LATP = Link-Aggregation Twisted Pair
LAFO = Link-Aggregation Fiber Optic

Das folgende Beispiel beschreibt die Konfiguration der Link-Aggregation LATP. Stellen Sie für diese Link-Aggregation an den beiden beteiligten Geräten je drei freie Twisted Pair Ports zur Verfügung. (Annahme: Modul 1, Port 1 bis Port 3).

2.1.1 Link-Aggregation anlegen und konfigurieren

Anmerkung: Zu einer Link-Aggregation gehören genau 2 Geräte. Konfigurieren Sie die Link-Aggregation jeweils an beiden beteiligten Geräten. Schließen Sie während der Konfigurationsphase höchstens eine Verbindungsleitung zwischen den Geräten an. Dadurch vermeiden Sie Schleifen (Loops).

- ☐ Konfigurieren Sie unter `Grundeinstellungen:Portkonfiguration` alle 3 Verbindungen so, dass die Datenrate und die Duplexeinstellungen der beteiligten Ports an beiden Geräten übereinstimmen.
- ☐ Bestimmen Sie von den an einer Link-Aggregation beteiligten Geräten das Gerät, das zwischen sich und dem Gerät, an dem der Konfigurations-PC /(Netzmanagementstation NMS) angeschlossen ist, die meisten Geräte aufweist. Beginnen Sie die Konfiguration an diesem Gerät, Andernfalls kann das Link-Aggregation Control Protocol (LACP) Ports blockieren und Geräte so vom Netz trennen, dass sie nicht mehr konfigurierbar sind.
- ☐ Im Beipiel unten (siehe Abbildung 2) konfigurieren Sie die Link-Aggregation zuerst am Gerät 3 und dann an Gerät 2. Sollten Sie das Gerät 3 unbeabsichtigt vom Netz trennen, können Sie es wieder erreichen, indem Sie bei Gerät 2 im Dialog `Redundanz:Link Aggregation` oder über das CLI den Punkt „Statische Link-Aggregation zulassen“ auswählen bzw. einschalten.

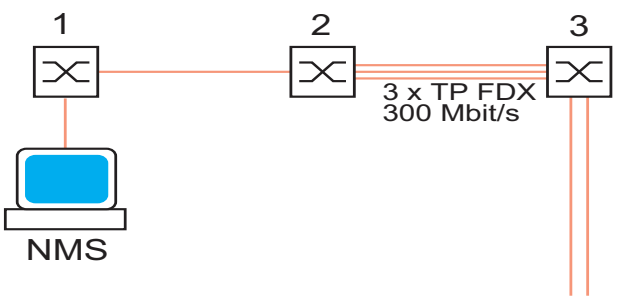


Abb. 2: Beispiel „erstes Gerät bestimmen“
NMS = Netzmanagementstation

☐ Verfahren Sie wie folgt, um eine Link-Aggregation aus 3 Twisted Pair Leitungen an Gerät 3 zu konfigurieren:

☐ Wählen Sie den Dialog `Redundanz:Link Aggregation` (siehe Abbildung 3).

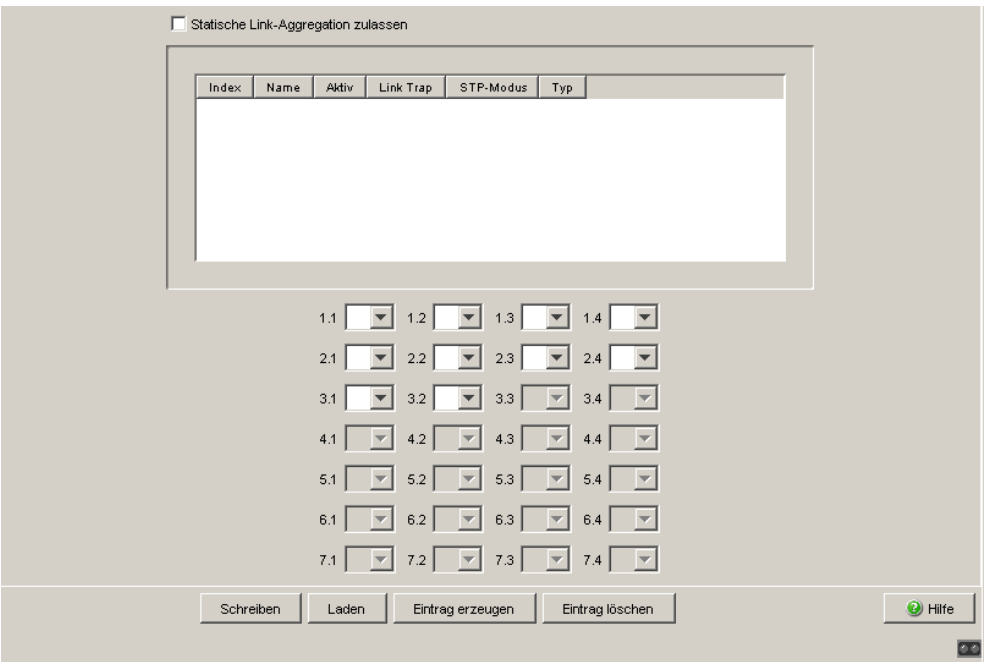


Abb. 3: Link Aggregation anlegen

☐ Wählen Sie `Statische Link-Aggregation zulassen`, wenn das Partner-Gerät das Link-Aggregation-Control-Protokoll (LACP) nicht unterstützt (z.B. MACH 3000).

☐ Klicken Sie auf „Eintrag erzeugen“, um eine neue Link-Aggregation zu erzeugen.

☐ Die Spalte `Index` zeigt Ihnen die Bezeichnung an, unter der das Gerät eine Link-Aggregation (Trunk) als virtuellen Port führt. Das Gerät legt den Port im physikalisch nicht existierenden Modul 8 an, die erste Link-Aggregation hat dann die Bezeichnung 8.1.

☐ Die Spalte `Name` bietet Ihnen die Möglichkeit, dieser Verbindung einen beliebigen Namen zuzuweisen. Benennen Sie die neue Link-Aggregation in diesem Beispiel mit „LATP“

☐ Die Spalte `Aktiv` bietet Ihnen die Möglichkeit, eine eingerichtete Link-Aggregation zu aktivieren/deaktivieren. Belassen Sie den Haken in der Spalte „Aktiv“, solange Sie die Link-Aggregation verwenden.

- ☐ Belassen Sie den Haken in der Spalte „`Link Trap`“, wenn das Gerät einen Alarm generieren soll, sobald alle Verbindungen der Link-Aggregation unterbrochen sind.
- ☐ In der Spalte „STP-Modus“ wählen Sie
  `on`, wenn die Link-Aggregation-Verbindung in einen Spanning Tree eingebunden ist,
  `off`, wenn kein Spanning Tree aktiv ist, bzw. die Link-Aggregation Segment eines HIPER-Rings ist.
- ☐ „Typ“ zeigt an, ob Sie diese Link-Aggregation-Verbindung manuell (`Statische Link-Aggregation zulassen` ist angewählt) angelegt haben, oder ob sie dynamisch mit Hilfe des LACP (`Statische Link Aggregation zulassen` ist nicht angewählt) zustande gekommen ist.
  Hinweis: bestehen die Mehrfachverbindungen zwischen Geräten, die das LACP unterstützen und ist dennoch `Statische Link-Aggregation zulassen` angewählt, wird trotzdem `dynamic` angezeigt, da die Geräte in diesem Fall automatisch auf dynamisch umschalten.

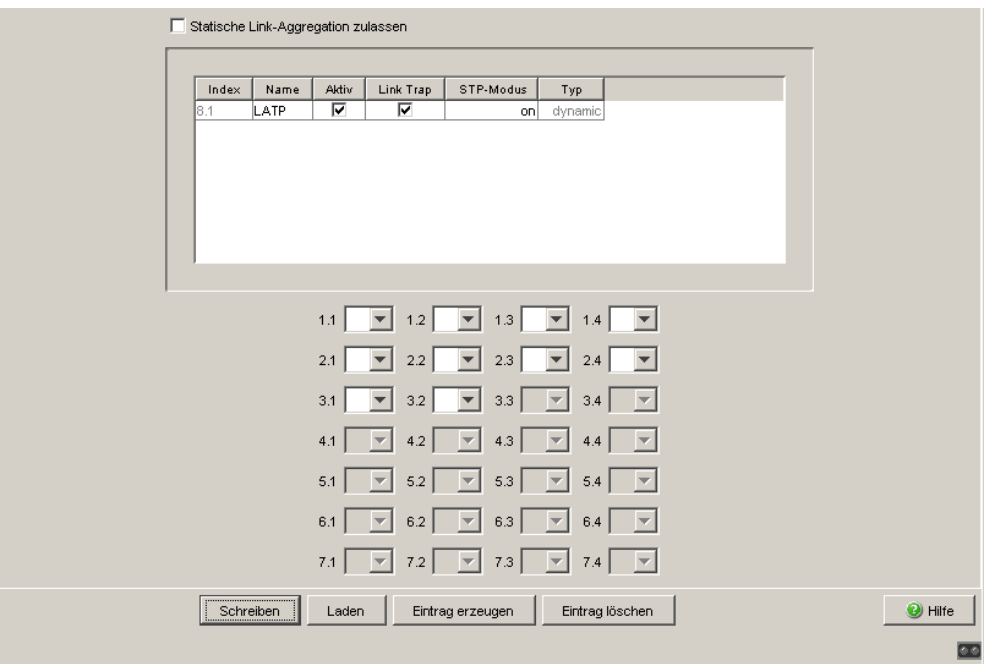


Abb. 4: Link-Aggregation erzeugt und benannt.

- ☐ Weisen Sie nun den an der Link-Aggregation teilnehmenden Ports 1.1, 1.2 und 1.3 den Index der Link-Aggregation-Verbindung LATP (8.1) zu (siehe Abbildung 5).

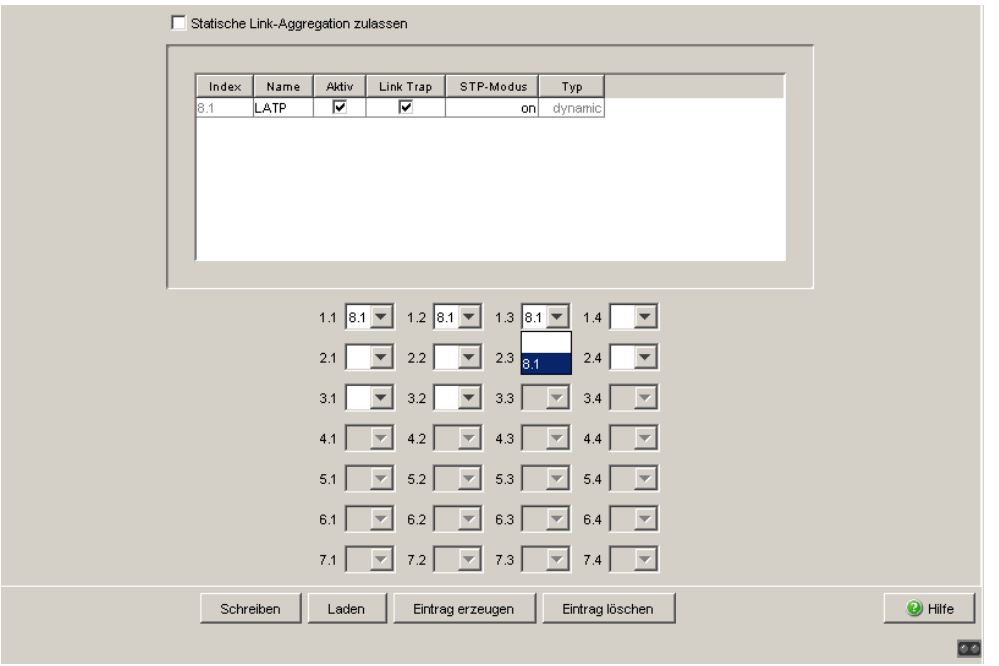


Abb. 5: Ports der Link Aggregation zuweisen

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`link-aggregation LATP`	Legt eine neue Link Aggregation mit dem Namen LATP an.

```
New Link-Aggregation created. Slot/port is 8.1.
```

`Interface 1/1`	Konfiguration für Port 1.1
`addport 8/1`	Zuweisung Port 1.1 zu Link Aggregation 8.1.
`Interface 1/2`	Konfiguration für Port 1.2
`addport 8/1`	Zuweisung Port 1.2 zu Link Aggregation 8.1.
`Interface 1/3`	Konfiguration für Port 1.3
`addport 8/1`	Zuweisung Port 1.3 zu Link Aggregation 8.1.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show link-aggregation brief`	Zeigt die Parameter aller auf dem Gerät angelegten Link Aggregationen an.

```
Max. num. of LAGs: 7
Slot no. for LAGs: 8
Static Capability: Disabled
Logical Interface Link-Aggr. Nam Link State Mbr Ports Active Ports
-------------------------------------------------------------
8/1               LATP          Down       1/1,1/2,
                                            1/3
```

☐ Konfigurieren Sie nun in gleicher Weise das Partnergerät (Gerät 2).
☐ Nach der Konfiguration schließen Sie die weitere(n) Verbindungsleitung(en) zwischen den Geräten an.

Anmerkung: Schließen Sie eine Kombination von Link-Aggregation mit folgenden Redundanzverfahren aus:

- Netz-/Ringkopplung
- MRP-Ring
- Sub-Ring

2.2 HIPER-Ring und Link-Aggregation (PowerMICE und MACH 4000)

Zur Erhöhung der Sicherheit besonders kritischer Verbindungen lassen sich die Redundanzfunktionen HIPER-Ring (siehe auf Seite 29 „Ring-Redundanz“) und Link-Aggregation kombinieren.

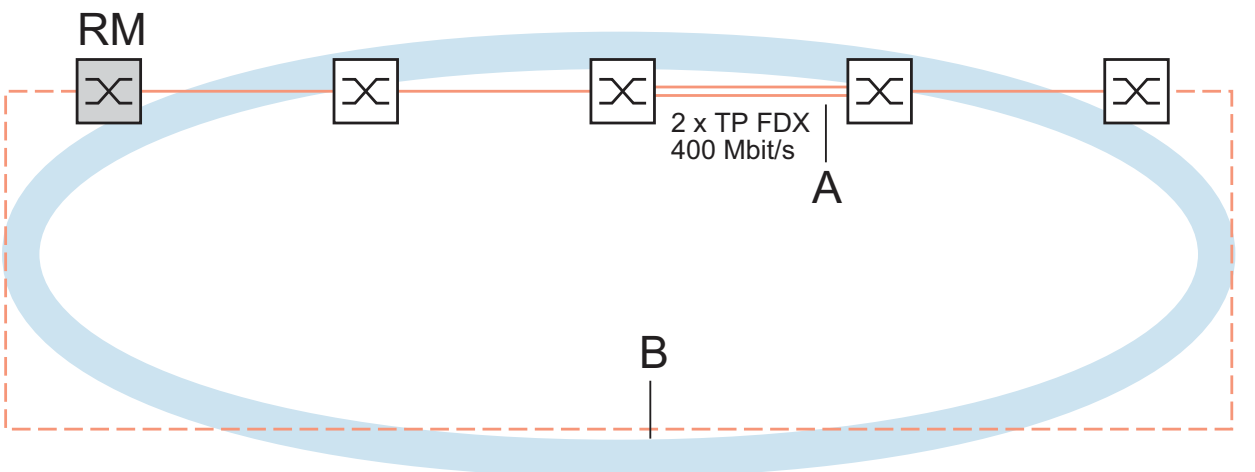


Abb. 6: Beispiel für HIPER-Ring / Link Aggregation Kombination
RM = Ring-Manager
A = Link-Aggregation
B = HIPER-Ring

Das Beispiel oben zeigt einen HIPER-Ring. Eine Link-Aggregation bildet ein Segment des Rings. Wenn alle Verbindungsleitungen der Link-Aggregation unterbrochen sind, aktiviert die HIPER-Ring-Funktion die redundante Leitung des Rings.

Anmerkung: Wenn Sie eine Link-Aggregation in einem HIPER-Ring verwenden wollen, konfigurieren Sie zuerst die Link-Aggregation und danach den HIPER-Ring. Geben Sie im HIPER-Ring-Dialog als Wert für Modul und Port den Index der gewünschten Link-Aggregation an (8.x). Beachten Sie, dass der jeweilige Ring-Port zur gewählten Link-Aggregation dazugehört.

Anmerkung: Schalten Sie RSTP aus, wenn Link-Aggregationen Segmente eines HIPER-Rings sind.

3 Ring-Redundanz

Das Konzept der Ring-Redundanz erlaubt den Aufbau hochverfügbarer, ringförmiger Netzstrukturen.
Mit Hilfe der RM-Funktion (**R**ing-**M**anager) können die beiden Enden eines Backbones in Linienstruktur zu einem redundanten Ring geschlossen werden. Der Ring-Manager hält die redundante Strecke solange offen, wie die Linienstruktur intakt ist. Fällt ein Segment aus, schließt der Ring-Manager sofort die redundante Strecke und die Linienstruktur ist wieder intakt.

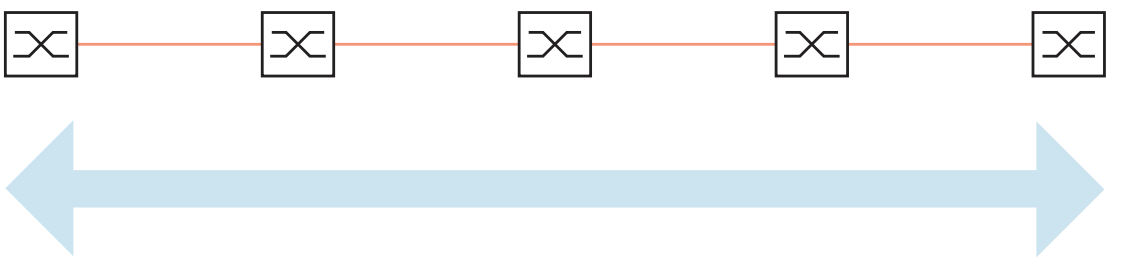


Abb. 7: Linienstruktur

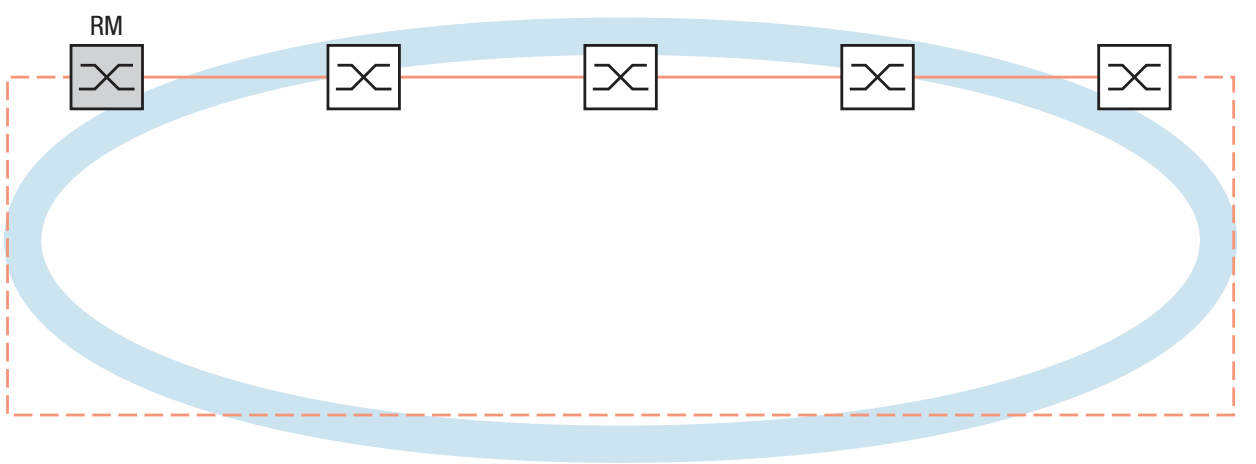


Abb. 8: Redundante Ringstruktur
RM = Ring-Manager
—— Hauptleitung
- - - Redundante Leitung

Beim Ausfall einer Teilstrecke wandelt sich die Ringstruktur eines

- HIPER-(**HI**GH **PE**RFORMANCE **R**EDUNDANCY) Rings mit bis zu 50 Geräten im typischen Fall innerhalb von 80 ms (einstellbar: Standard/Beschleunigt) wieder in eine Linienstruktur zurück.
- MRP (**M**edia **R**edundancy **P**rotocol)-Rings (IEC 62439) bei bis zu 50 Geräten im typischen Fall innerhalb von 80 ms (einstellbar maximal 200 ms/500 ms) wieder in eine Linienstruktur zurück.

Geräte-Voraussetzungen für die Nutzung der HIPER-Ring-Funktion:

- Innerhalb eines HIPER-Ringes können Sie eine beliebige Mischung der folgenden Geräte einsetzen:
  - RS1
  - RS2-./.
  - RS2-16M
  - RS2-4R
  - RS20, RS30, RS40
  - RSR20, RSR30
  - OCTOPUS
  - MICE
  - MS20, MS30
  - PowerMICE
  - MACH 100
  - MACH 1000
  - MACH 1040
  - MACH 3000
  - MACH 4000
- Innerhalb eines MRP-Rings können Sie Geräte einsetzen, die das MRP-Protokol nach IEC 62439 unterstützen.

Anmerkung: Sie können auf einem Gerät zur gleichen Zeit ausschließlich eine Methode der Ring-Redundanz einschalten. Deaktivieren Sie beim Wechsel zu einer anderen Ring-Redundanz-Methode die Funktion.

Anmerkung: Die folgende Verwendung des Begriffes „Ring-Manager“ anstatt „Redundanzmanager“ trägt zum leichteren Verständnis der Funktion bei.

3.1 Beispiel für HIPER-Ring

In einem Netz ist ein Backbone in Linienstruktur mit 3 Geräten vorhanden. Um die Ausfallsicherheit des Backbones zu erhöhen, haben Sie beschlossen, die Linienstruktur in einen HIPER-Ring zu überführen. Als Ports für den Anschluss der Verbindungsstrecken nutzen Sie jeweils die Ports 1.1 und 1.2 der Geräte[1].

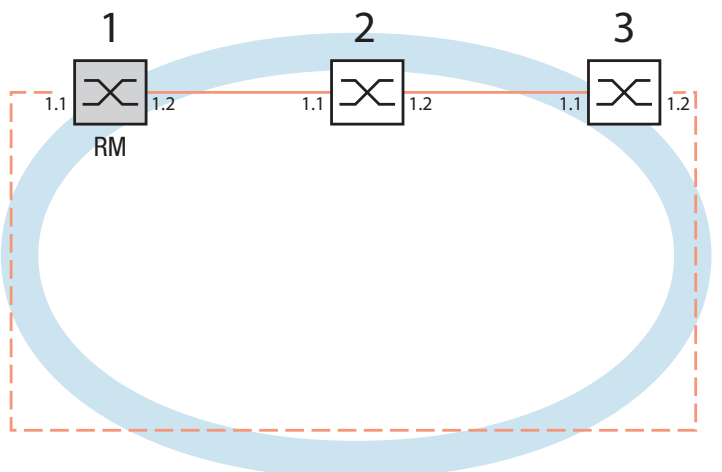


Abb. 9: Beispiel für HIPER-Ring
RM = Ring-Manager
—— Hauptleitung
- - - Redundante Leitung

Die folgende Beispielkonfiguration beschreibt die Konfiguration des Ring-Manager-Gerätes (1). Die beiden anderen Geräte (2 bis 3) sind analog zu konfigurieren, ohne jedoch die Ring-Manager-Funktion einzuschalten. Wählen Sie als Wert für Ringrekonfiguration „Standard“ bzw. lassen Sie das Feld leer.

1. Bei modularen Geräten ist die 1. Ziffer der Portbezeichnung die Modulbezeichnung, die 2. Ziffer beschreibt den Port des Moduls. Auch bei nicht-modularen Geräten wird das Bezeichnungsschema 1.x verwendet, damit Konsistenz gewährleistet ist.

Anmerkung: Alternativ zur Konfiguration des HIPER-Rings per Software, können Sie bei den Switches RS20/30/40, MS20/30 und PowerMICE einige Einstellungen auch mit DIP-Schaltern an den Geräten vornehmen. Mit einem DIP-Schalter können Sie auch einstellen, ob die Konfiguration per DIP-Schalter oder die Konfiguration per Software Vorrang hat. Lieferzustand ist „Software Configuration“ (Konfiguration per Software). Details zu den DIP-Schaltern finden Sie im Anwender-Handbuch Installation.

Anmerkung: Konfigurieren Sie alle Geräte des HIPER-Rings individuell. Warten Sie mit dem Anschließen der redundanten Strecke, bis Sie die Konfiguration aller Geräte des HIPER-Rings abgeschlossen haben. So vermeiden Sie Schleifen während der Konfigurationsphase.

3.1.1 HIPER-Ring einrichten und konfigurieren

☐ Bauen Sie das Netz nach Ihren Erfordernissen auf.
☐ Konfigurieren Sie alle Ports so, dass die Datenrate und die Duplex-einstellungen der Strecken der folgenden Tabelle entsprechen:

Port-Typ	Bitrate	Autonegotiation (Automatische Konfiguration)	Port-Einstellung	Duplex
TX	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
TX	1 Gbit/s	an	an	-
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
Optisch	1 Gbit/s	an	an	-
Optisch	10 Gbit/s	-	an	10 Gbit/s Vollduplex (FDX)

Tab. 3: Port-Einstellungen für Ring-Ports

Anmerkung: Beim Aktivieren der HIPER-Ring-Funktion per Software oder DIP-Schalter setzt das Gerät die entsprechenden Einstellungen für die vordefinierten Ringports in der Konfigurationstabelle (Übertragungsrate und Modus). Schalten Sie die HIPER-Ring-Funktion ab, behalten die zu normalen Ports zurückgewandelten Ports die Ringporteinstellungen bei. Unabhängig von der DIP-Schalter-Stellung können Sie die Port-Einstellungen weiterhin über Software verändern.

☐ Wählen Sie den Dialog `Redundanz:Ring-Redundanz`.
☐ Wählen Sie unter „Version“ `HIPER-Ring`.
☐ Geben Sie den gewünschten Ring Port 1 und 2 an, in dem Sie in den Feldern Modul und Port die entsprechenden Einträge vornehmen. Sollte eine Moduleingabe nicht möglich sein, so ist im Gerät nur ein Modul vorhanden, welches als Vorgabe übernommen wird.

Anzeige im Feld „Operation“:
– `active`: Sie haben diesen Port eingeschaltet und er hat einen Link.
– `inactive`: Sie haben diesen Port ausgeschaltet oder er hat keinen Link.

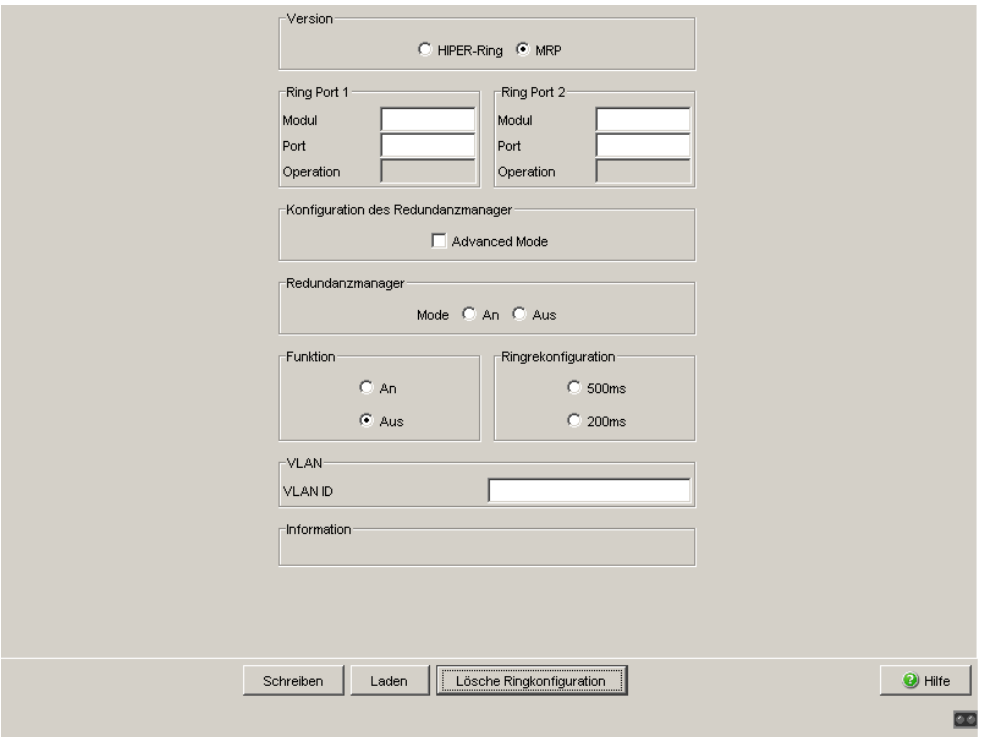


Abb. 10: Ring-Redundanz-Dialog

☐ Schalten Sie bei diesem Gerät den Ring-Manager ein. Schalten Sie bei keinem anderen Gerät im HIPER-Ring den Ring-Manager ein.

☐ Wählen Sie im Rahmen „Ringrekonfiguration“ den Wert „Standard“ (Vorgabe).

Anmerkung: Einstellungen im Rahmen „Ringrekonfiguration“ sind ausschließlich bei Geräten wirksam, die Sie als Ring-Manager konfiguriert haben.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`hiper-ring mode ring-manager`	Wählt die HIPER-Ring Ring-Redundanz und bestimmt das Gerät zum Ring-Manager.
`Switch's HIPER Ring mode set to ring-manager`	
`hiper-ring port primary 1/1`	Definiert den Port 1 im Modul 1 als Ring Port 1.
`HIPER Ring primary port set to 1/1`	
`hiper-ring port secondary 1/2`	Definiert den Port 2 im Modul 1 als Ring Port 2.
`HIPER Ring secondary port set to 1/2`	
`exit`	Wechsel in den Privileged-EXEC-Modus.

```
show hiper-ring                    Zeigt die HIPER-Ring Parameter an.
HIPER Ring Mode of the Switch.................. ring-manager
  configuration determined by.................. management
HIPER Ring Primary Port of the Switch.......... 1/1, state active
HIPER Ring Secondary Port of the Switch........ 1/2, state active
HIPER Ring Redundancy Manager State............ active
HIPER Ring Redundancy State (red. exists).. no (rm is active)
HIPER Ring Setup Info (Config. failure)........ no error
HIPER Ring Recovery Delay...................... 500ms
```

☐ Verfahren Sie nun analog bei den anderen beiden Geräten.

Anmerkung: Haben Sie VLANs konfiguriert, dann beachten Sie die VLAN-Konfiguration der Ringports.
Bei der Konfiguration des HIPER-Rings wählen Sie für die Ringports die
– VLAN-ID 1 und „`Ingress Filtering`“ deaktiviert in der Port-Tabelle und
– VLAN-Zugehörigkeit `U` oder `T` in der statischen VLAN-Tabelle.

Anmerkung: Deaktivieren Sie das Spanning-Tree-Protokoll an den Ports, die an den HIPER-Ring angeschlossen sind, da sich Spanning-Tree und Ring-Redundanz gegenseitig beeinflussen.
Wenn Sie die Funktion des HIPER-Rings über DIP-Schalter aktiviert haben wird RSTP automatisch abgeschaltet.

☐ Schließen Sie jetzt die Linie zum Ring. Verbinden Sie hierzu die beiden Geräte an den Enden der Linie über ihre Ringports.

Die Anzeigen im Rahmen „Status des Redundanzmanagers“ bedeuten:
– „Aktiv (redundante Strecke)“: der Ring ist offen, d.h. eine Datenleitung oder Netzkomponente innerhalb des Rings ist ausgefallen.
– „Inaktiv“: der Ring ist geschlossen, d.h. Datenleitungen und Netzkomponenten funktionieren.

Die Anzeigen im Rahmen “Information“ bedeuten
– „Redundanz vorhanden“: eine von der Funktion betroffene Leitung kann ausfallen wobei dann die redundante Strecke die Funktion der ausgefallenen Strecke übernehmen wird.
– „Konfigurationsfehler“: die Funktion ist falsch konfiguriert oder die Kabelverbindungen an den Ringport sind inkorrekt konfiguriert (z.B. nicht an den Ringsports eingesteckt).

Anmerkung: Wenn Sie Link-Aggregations-Verbindungen im HIPER-Ring verwenden wollen (PowerMICE und MACH 4000), dann geben Sie für Modul und Port des Ringports den Index des gewünschten Link-Aggregation-Eintrags an.

3.2 Beispiel für MRP-Ring

In einem Netz ist ein Backbone in Linienstruktur mit 3 Geräten vorhanden. Um die Verfügbarkeit des Backbones zu erhöhen haben Sie beschlossen, die Linienstruktur in eine Ring-Redundanz zu überführen. Im Unterschied zum vorherigen Beispiel kommen Geräte unterschiedlicher Hersteller zum Einsatz, die nicht alle das HIPER-Ring Protokoll unterstützen. Allen Geräte unterstützen jedoch MRP als Ring-Redundanz-Protokoll, also entscheiden Sie MRP einzusetzen. Als Ports für den Anschluss der Verbindungsstrecken nutzen Sie jeweils die Ports 1.1 und 1.2 der Geräte.

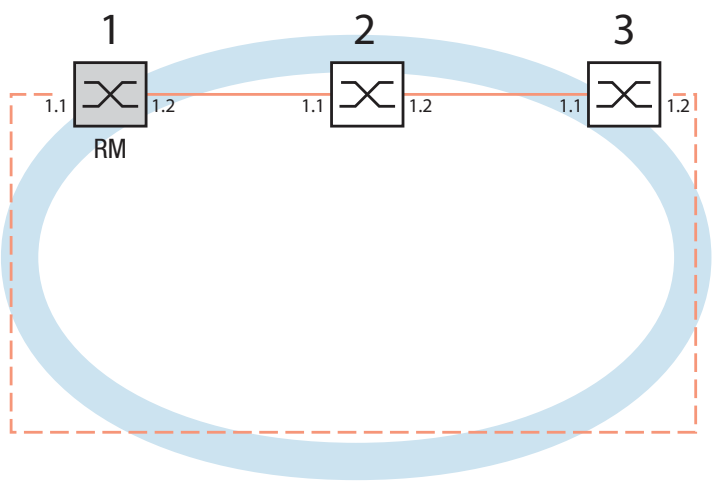


Abb. 11: Beispiel für MRP-Ring
RM = Ring Manager
—— Hauptleitung
- - - Redundante Leitung

Die folgende Beispielkonfiguration beschreibt die Konfiguration des Ring-Manager-Gerätes (1). Die beiden anderen Geräte (2 bis 3) konfigurieren Sie analog, ohne jedoch die Ring-Manager-Funktion einzuschalten. Dieses Beispiel nutzt kein VLAN. Als Ringrekonfigurationszeit haben Sie 200 ms vorgesehen, alle Geräte unterstützen den Advanced Mode des Ring-Managers.

Anmerkung: Bei Geräten mit DIP-Schaltern stellen Sie alle DIP-Schalter auf „Ein“. Das bewirkt, dass Sie mittels Software-Konfiguration die Redundanzfunktion uneingeschränkt konfigurieren können. So vermeiden Sie, dass die Software-Konfiguration durch die DIP-Schalter evtl. behindert wird.

Anmerkung: Konfigurieren Sie alle Geräte des MRP-Rings individuell. Warten Sie mit dem Anschließen der redundanten Strecke, bis Sie die Konfiguration aller Geräte des MRP-Rings abgeschlossen haben. So vermeiden Sie Schleifen während der Konfigurationsphase.

☐ Bauen Sie das Netz nach Ihren Erfordernissen auf.
☐ Konfigurieren Sie alle Ports so, dass die Datenrate und die Duplexeinstellungen der Strecken der folgenden Tabelle entsprechen:

Port-Typ	Bitrate	Autonegotiation (Automatische Konfiguration)	Port-Einstellung	Duplex
TX	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
TX	1 Gbit/s	an	an	-
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
Optisch	1 Gbit/s	an	an	-
Optisch	10 Gbit/s	-	an	10 Gbit/s Vollduplex (FDX)

Tab. 4: Port-Einstellungen für Ring-Ports

☐ Wählen Sie den Dialog `Redundanz:Ring-Redundanz`.
☐ Wählen Sie unter „Version“ `MRP`.
☐ Geben Sie den gewünschten Ring Port 1 und 2 an, in dem Sie in den Feldern Modul und Port die entsprechenden Einträge vornehmen. Sollte eine Moduleingabe nicht möglich sein, so ist im Gerät nur ein Modul vorhanden, welches als Vorgabe übernommen wird.

Anzeige im Feld „Operation“:

- `forwarding`: dieser Port ist eingeschaltet und hat einen Link.
- `blocked`: dieser Port ist blockiert und hat einen Link
- `disabled`: dieser Port ist ausgeschaltet
- `not-connected`: dieser Port hat keinen Link.

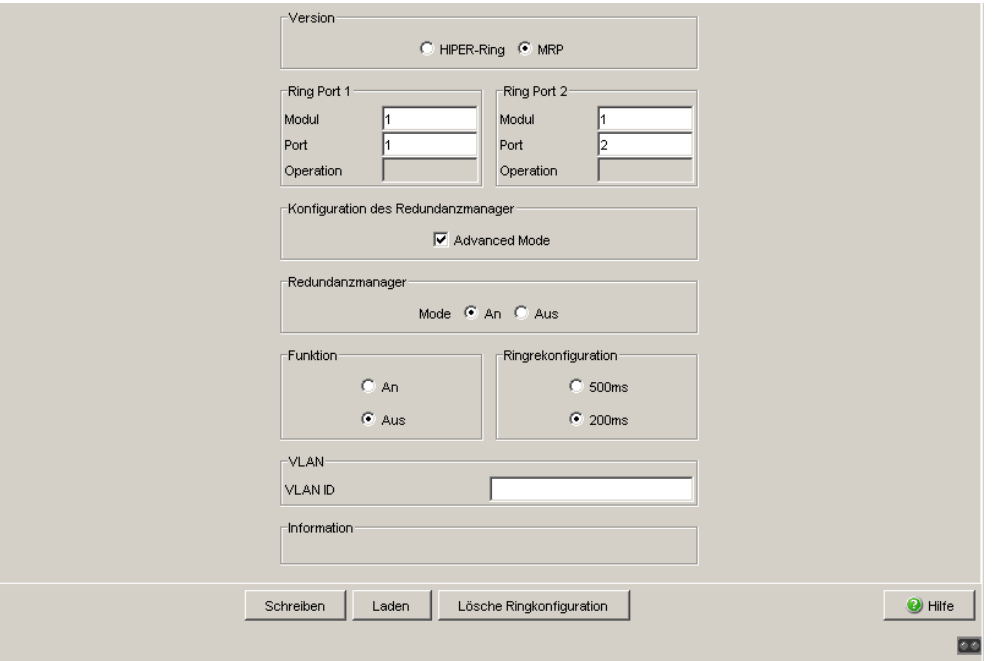


Abb. 12: Ring-Redundanz-Dialog

☐ Wählen Sie im Rahmen „Ringrekonfiguration“ 200 ms.

Anmerkung: Wenn bei der Wahl von 200 ms für die Ringrekonfiguration die Stabilität des Rings nicht den Anforderungen an Ihr Netz entspricht, wählen Sie 500 ms.

Anmerkung: Einstellungen im Rahmen „Ringrekonfiguration“ sind ausschließlich bei Geräten wirksam, die Sie als Ring-Manager konfiguriert haben.

☐ Schalten Sie unter „Konfiguration des Redundanzmanager“ den Advanced Mode ein.

☐ Schalten Sie bei diesem Gerät den Ring Manager ein. Schalten Sie bei keinem anderen Gerät im MRP-Ring den Ring-Manager ein.

☐ Belassen Sie im Feld VLAN die VLAN-ID bei 0.

☐ Schalten Sie die Funktion des MRP-Rings an.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

Die Anzeigen im Rahmen “Information“ bedeuten
– „Redundanz vorhanden“: eine von der Funktion betroffene Leitung kann ausfallen wobei dann die redundante Strecke die Funktion der ausgefallenen Strecke übernehmen wird.
– „Konfigurationsfehler“: die Funktion ist falsch konfiguriert oder die Kabelverbindungen an den Ringport sind inkorrekt konfiguriert (z.B. nicht an den Ringsports eingesteckt).

Der Rahmen "VLAN" bietet Ihnen die Möglichkeit, den MRP-Ring einem VLAN zuzuordnen:

☐ Sind VLANs konfiguriert, dann wählen Sie im Rahmen "VLAN":
  – die VLAN-ID 0, wenn die MRP-Ring-Konfiguration wie in diesem Beispiel keinem VLAN zugeordnet sein soll.
    Wählen Sie für die Ringports die VLAN ID 1 und die VLAN-Zugehörigkeit `U` (Untagged)in der statischen VLAN-Tabelle.
  – eine VLAN-ID > 0, wenn die MRP-Ring-Konfiguration diesem VLAN zugeordnet sein soll.
    Tragen Sie bei allen Geräten in diesem MRP-Ring diese VLAN-ID in der MRP-Ring-Konfiguration ein und wählen Sie für alle Ringports in diesem MRP-Ring dann diese VLAN-ID und die VLAN-Zugehörigkeit Tagged (`T`) in der statischen VLAN-Tabelle.

Anmerkung: Wenn Sie in einem MRP-Ring das Redundanzprotokoll RSTP (siehe auf Seite 89 „Spanning Tree“) verwenden möchten, schalten Sie bei allen Geräten im MRP-Ring die MRP-Kompatibilität im Dialog `Rapid Spanning Tree:Global` an, da sich RSTP (Spanning-Tree) und Ring-Redundanz gegenseitig beeinflussen.
Sollte dies nicht möglich sein, etwa weil einzelne Geräte die MRP-Kompatibilität nicht unterstützen, deaktivieren Sie RSTP an den Ports, die an den MRP-Ring angeschlossen sind.

Anmerkung: Wenn Sie einen MRP-Ring über das Command Line Interface konfigurieren, definieren Sie einen zusätzlichen Parameter. Bei Konfiguration über das CLI wird ein MRP-Ring über seine MRP-Domänen-ID angesprochen. Diese ist eine Folge aus 16 Ziffernblöcken (8-Bit-Werten). Verwenden Sie den Vorgabewert „default domain“, das entspricht einer MRP-Domänen-ID von 255 255 255 255 255 255 255 255 255 255 255 255

255 255 255 255.
Diese „default domain“ wird auch intern bei einer Konfiguration über das Web based Interface genutzt.
Konfigurieren Sie alle Geräte innerhalb eines MRP-Rings mit der gleichen MRP-Domänen-ID.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mrp new-domain default-domain`	Legt einen neuen MRP-Ring mit der Default-Domänen-ID 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255 an.
`MRP domain created: Domain ID: 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255 (Default MRP domain)`	
`mrp current-domain port primary 1/1`	Definiert den Port 1 im Modul 1 als Ring Port 1 (primary).
`Primary Port set to 1/1`	
`mrp current-domain port secondary 1/2`	Definiert den Port 2 im Modul 1 als Ring Port 2. (secondary)
`Secondary Port set to 1/2`	
`mrp current-domain mode manager`	Definiert dieses Gerät als Ring-Manager.
`Mode of Switch set to manager`	
`mrp current-domain recovery-delay 200ms`	Definiert 200ms als Wert für „Ringrekonfiguration“.
`Recovery delay set to 200ms`	
`mrp current-domain advanced-mode enable`	Schaltet den „MRP-Advanced Mode“ ein.
`Advanced Mode (react on link change) set to Enabled`	
`mrp current-domain operation enable`	Schaltet den MRP Ring ein.
`Operation set to Enabled`	
`exit`	Eine Ebene zurück.

```
show mrp
```

Zeigt die aktuellen Parameter des MRP-Rings an (Darstellung gekürzt).

```
Domain ID:
255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255
(Default MRP domain)

Configuration Settings:
Advanced Mode (react on link change).... Enabled
Manager Priority....................... 32768
Mode of Switch (administrative setting). Manager
Mode of Switch (real operating state)... Manager
Domain Name............................ <empty>
Recovery delay......................... 200ms
Port Number, Primary................... 1/1, State: Not Connected
Port Number, Secondary................. 1/2, State: Not Connected
VLAN ID................................ 0 (No VLAN)
Operation.............................. Enabled
```

☐ Schließen Sie jetzt die Linie zum Ring. Verbinden Sie hierzu die beiden Geräte an den Enden der Linie über ihre Ringports.

4 Multiple Ringe

Das Gerät bietet Ihnen die Möglichkeit, multiple Ringe mit verschiedenen Redundanzprotokollen aufzubauen:

- Sie haben die Möglichkeit, MRP-Ringe zu verschachteln. Ein angekoppelter Ring heißt Sub-Ring (siehe auf Seite 44 „Sub-Ring“).
- Sie haben die Möglichkeit, an MRP-Ringe weitere Ringstrukturen anzukoppeln, die mit RSTP arbeiten (siehe auf Seite 120 „Kombinieren von RSTP und MRP“).

4.1 Sub-Ring

4.1.1 Sub-Ring-Beschreibung

Für die Geräte PowerMICE, MACH 1040 und MACH 4000.

Das Sub-Ring-Konzept ermöglicht Ihnen eine einfache Ankopplung neuer Netzsegmente an geeignete Geräte bestehender Redundanz-Ringe (Basis-Ring). Die Geräte des Basis-Rings, an die der neue Sub-Ring angekoppelt wird, heißen Sub-Ring-Manager (SRM).

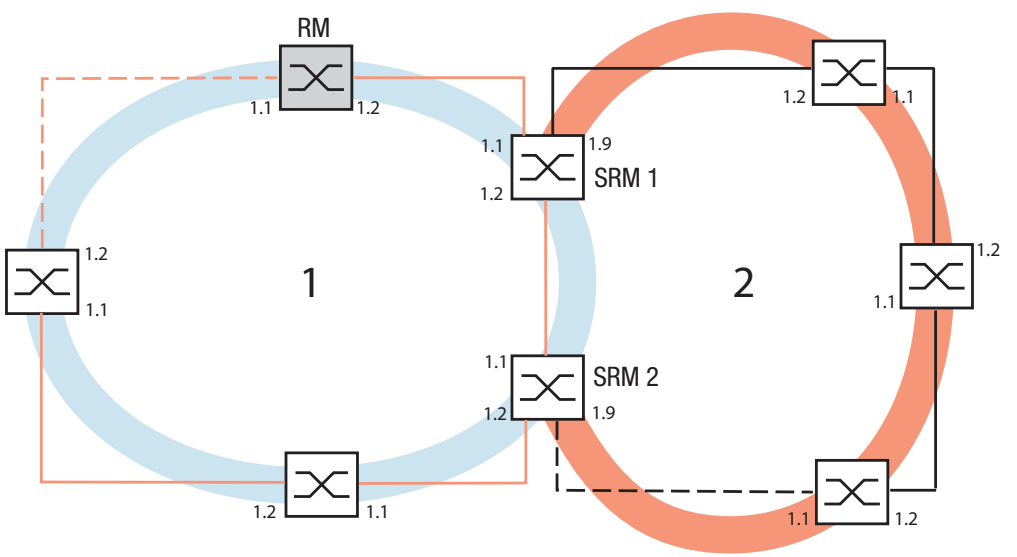


Abb. 13: Beispiel für Sub-Ring-Struktur
1 blauer Ring = Basis-Ring
2 orangefarbener Ring = Sub-Ring
SRM = Sub-Ring-Manager
RM = Ring-Manager

Anmerkung: Folgende Geräte unterstützen die Sub-Ring-Manager-Funktion:
– MACH 1040
– MACH 4000
– PowerMICE

Die SRM-fähigen Geräte unterstützen bis zu 4 SRM-Instanzen (MACH 1040 bis zu 16) und können daher für bis zu 4 Sub-Ringe gleichzeitig Sub-Ring-Manager sein (MACH 1040 für bis zu 16).

In einen Sub-Ring können Sie als Teilnehmer die Geräte integrieren, die MRP unterstützen, die Sub-Ring-Manager-Funktion ist nicht notwendig.

Jeder Sub-Ring kann aus bis zu 200 Teilnehmern bestehen, dabei zählen die beiden SRM und die zwischen den SRMs liegenden Switches im Hauptring nicht mit.
Die Einrichtung von Sub-Ringen hat folgende Vorteile:
- Durch die Ankopplung nehmen Sie das neue Netzsegment in das Redundanz-Konzept auf.
- Sie integrieren hinzukommende Unternehmensbereiche leicht in bestehende Netze.
- Sie bilden die Organisationsstruktur eines Unternehmens einfach in der Netztopologie ab.
- Als MRP-Ring liegen die Umschaltzeiten des Sub-Rings im Redundanzfall bei typ. <100 ms.

Beispiele möglicher Sub-Ring-Topologien zeigen die folgenden Abbildungen:

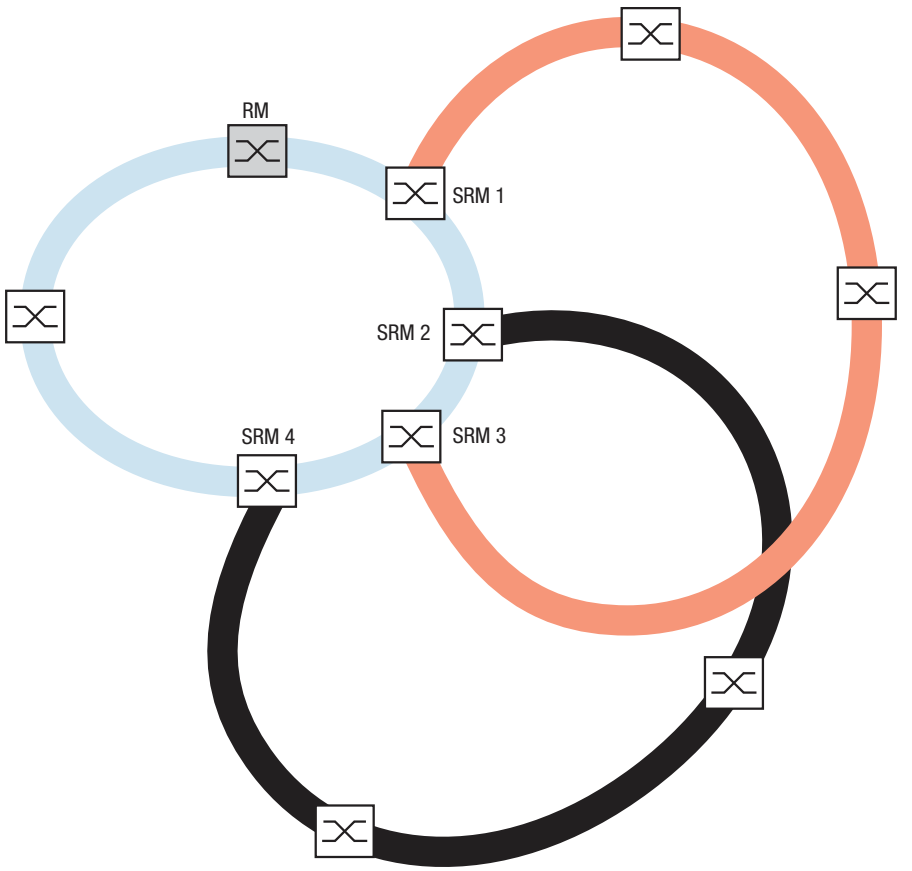


Abb. 14: Beispiel für überlappende Sub-Ring-Struktur

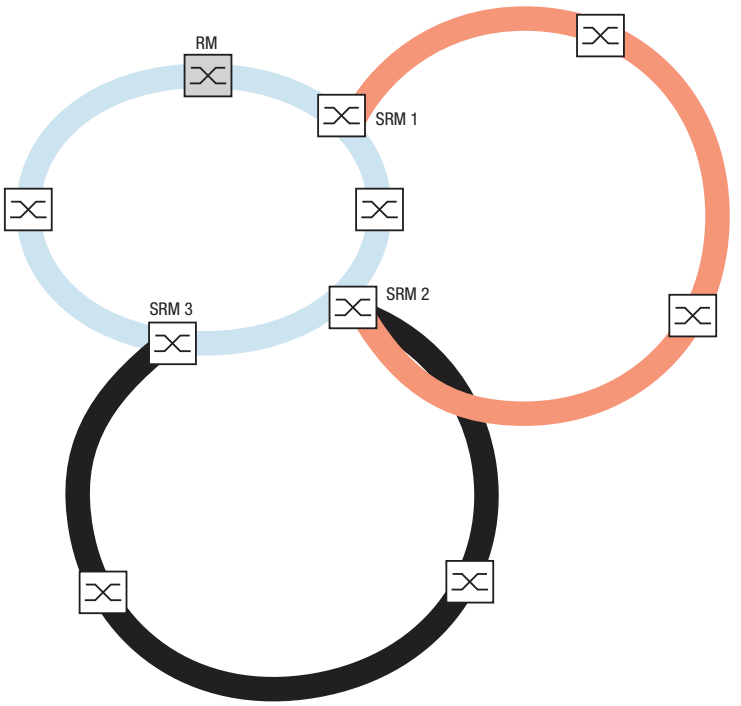


Abb. 15: Sonderfall: ein Sub-Ring-Manager verwaltet 2 Sub-Ringe (2 Instanzen), Je nach Gerätetyp können Sie weitere Instanzen konfigurieren.

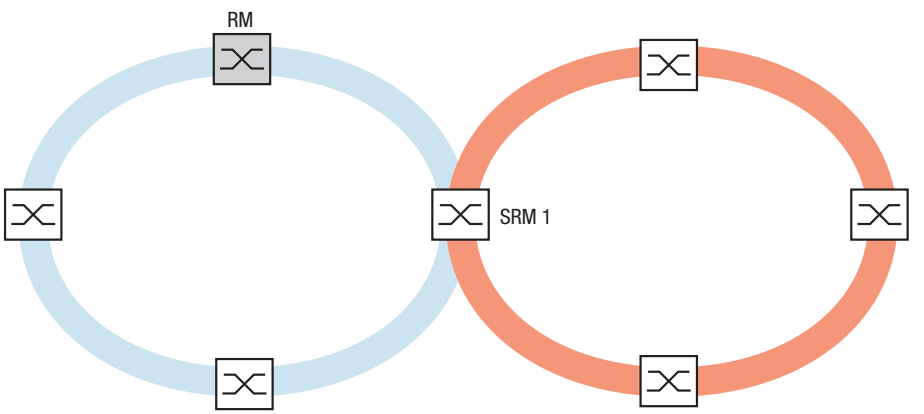


Abb. 16: Sonderfall: ein Sub-Ring-Manager verwaltet beide Enden eines Sub-Rings an unterschiedlichen Ports (Single-Sub-Ring-Manager)

Anmerkung: Schließen Sie Sub-Ringe ausschließlich an bestehende Basis-Ringe an. Kaskadieren Sie keine Sub-Ringe (d.h., ein neuer Sub-Ring darf nicht an einen bestehenden Sub-Ring angeschlossen werden).

Anmerkung: Sub-Ringe nutzen MRP. Sie können Sub-Ringe an bestehende Basis-Ringe mit HIPER-Ring-Protokoll, Fast HIPER-Ring-Protokoll und MRP ankoppeln. Wenn Sie einen Sub-Ring an einen Basis-Ring unter MRP koppeln, dann konfigurieren Sie beide Ringe in unterschiedlichen VLANs. Konfigurieren Sie hierzu

- entweder die Sub-Ring-Ports der Sub-Ring-Manager und die Geräte des Sub-Rings in einem eigenen VLAN. Hierbei können mehrere Sub-Ringe das gleiche VLAN nutzen.
- oder die Geräte des Basis-Rings inklusive der Basis-Ring-Ports der Sub-Ring-Manager in einem eigenen VLAN. Dies verringert den Konfigurationsaufwand, wenn Sie an einen Basis-Ring mehrere Sub-Ringe ankoppeln.

4.1.2 Sub-Ring-Beispiel

Sie möchten an einen bestehenden Redundanz-Ring unter HIPER-Ring-Protokoll ein neues Netzsegment mit 3 Geräten ankoppeln. Wenn Sie das Netzsegment nicht nur an einem, sondern an beiden Enden ankoppeln, erhalten Sie bei entsprechender Konfiguration erhöhte Ausfallsicherheit durch Redundanz.

Das neue Netzsegment wird als Sub-Ring angekoppelt. Die Kopplung erfolgt an bestehende Geräte des Basis-Rings vom Typ

– MACH 4000
– PowerMICE

Konfigurieren Sie diese Geräte zu Sub-Ring-Managern.

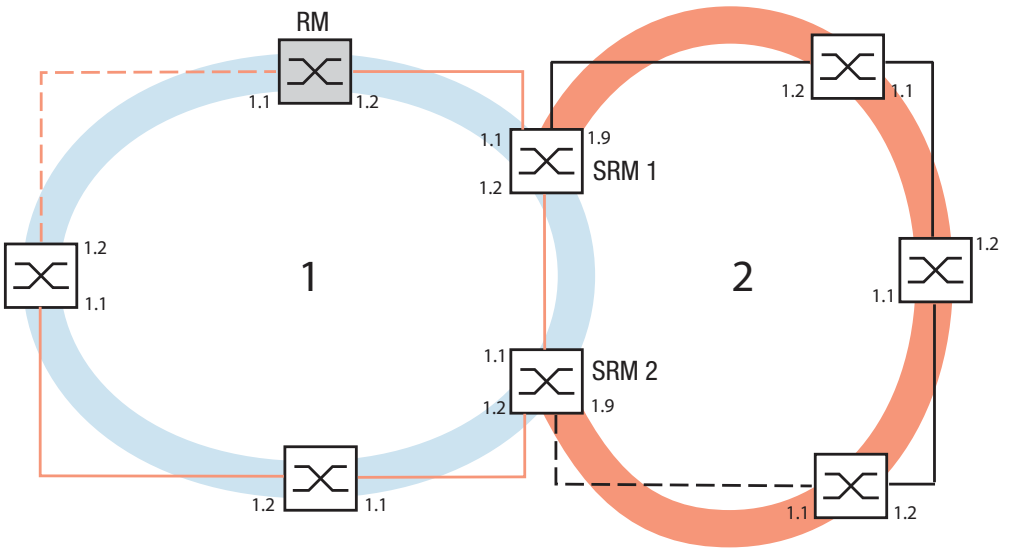


Abb. 17: Beispiel für Sub-Ring-Struktur
1 blauer Ring = Basis-Ring
2 orangefarbener Ring = Sub-Ring
SRM = Sub-Ring-Manager
RM = Ring-Manager

Verfahren Sie wie folgt, um einen Subring zu konfigurieren:

☐ Konfigurieren Sie die 3 Geräte des neuen Netzsegments als Teilnehmer an einem MRP-Ring. Das bedeutet:
– Konfigurieren Sie Übertragungsrate und Duplex-Modus für alle Ringports nach folgender Tabelle:

Port-Typ	Bitrate	Autonegotiation (Automatische Konfiguration)	Port-Einstellung	Duplex
TX	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
TX	1 Gbit/s	an	an	-
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)
Optisch	1 Gbit/s	an	an	-
Optisch	10 Gbit/s	-	an	10 Gbit/s Vollduplex (FDX)

Tab. 5: Port-Einstellungen für Ring-Ports

☐ Weitere Einstellungen:
- Definieren Sie eine unterschiedliche VLAN-Zugehörigkeit von Basis-Ring und Sub-Ring, wenn auch der Basis-Ring das MRP-Protokoll nutzt; z.B. VLAN-ID 1 für den Basis-Ring und VLAN-ID 2 für den Sub-Ring.
- Wählen Sie für alle Ringports im Sub-Ring diese VLAN-ID und die VLAN-Zugehörigkeit Tagged (`T`) in der statischen VLAN-Tabelle.
- Schalten Sie die MRP-Ring-Funktion bei allen Geräten ein.
- Konfigurieren Sie im Ring-Redundanz-Dialog unter MRP-Ring für alle Geräte die beiden im Sub-Ring genutzten Ringports.
- Schalten Sie die Ring-Manager-Funktion bei allen Geräten aus.
- Konfigurieren Sie keine Link-Aggregation.
- Schalten Sie RSTP für die im Sub-Ring genutzten MRP-Ring-Ports aus.

Anmerkung: Die MRP-Domänen-ID ist eine Folge aus 16 Ziffernblöcken (Wertebereich 0 bis 255). Die Default-Domäne (im CLI: „default-domain“) ist die MRP-Domänen-ID von 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255. Eine MRP-Domänen-ID, die ausschließlich aus Nullen besteht, ist ungültig.

Müssen Sie die MRP-Domänen-Bezeichnung anpassen, öffnen Sie das Command Line Interface (CLI) und verfahren wie folgt:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mrp delete-domain current-domain`	Löscht die aktuelle MRP-Domäne. Wenn keine MRP-Domäne besteht, gibt das Gerät eine Fehlermeldung aus.

```
MRP current domain deleted:
Domain ID:
  255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255
  (Default MRP domain)
```

```
mrp new-domain
0.0.1.1.2.2.3.4.4.111.222.12
3.0.0.66.99

MRP domain created:
Domain ID: 0.0.1.1.2.2.3.4.5.111.222.123.0.0.66.99
```

Erzeugt eine neue MRP-Domäne mit der angegebenen MRP-Domänen-ID. Auf diese Domäne können Sie im Anschluß mit „current-domain“ zugreifen.

4.1.3 Konfiguration des Sub-Ring-Beispiels

Verfahren Sie wie folgt, um die beiden Sub-Ring-Manager des Beispiels zu konfigurieren:

- ☐ Wählen Sie den Dialog `Redundanz:Sub-Ring`.
- ☐ Klicken Sie auf „Erzeugen“.

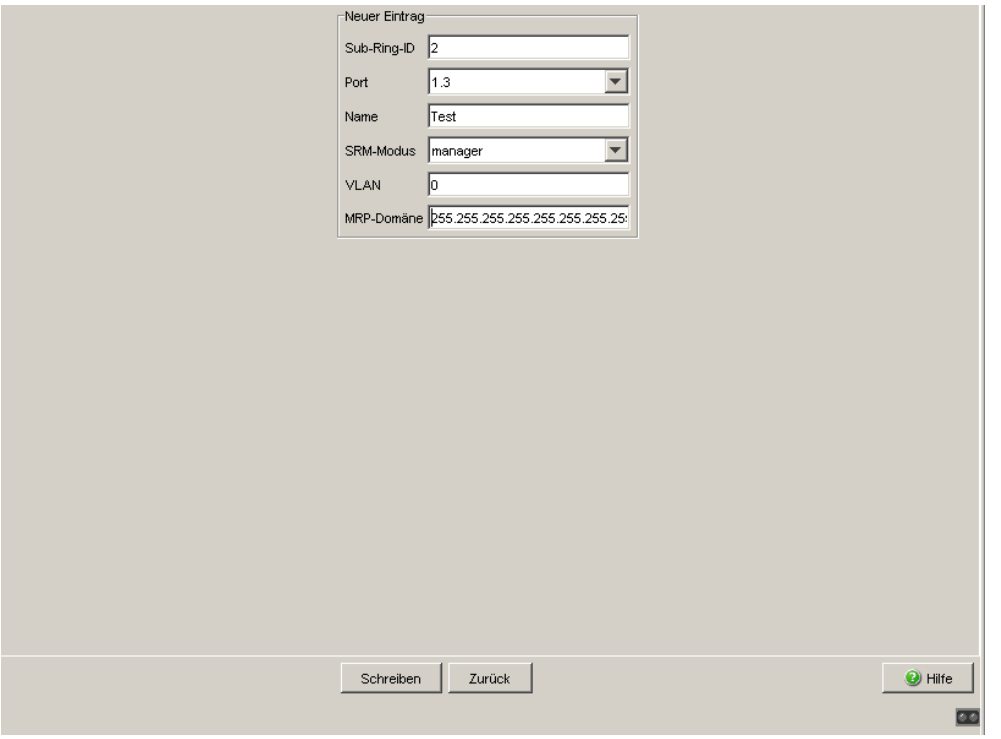


Abb. 18: Sub-Ring - Neuer Eintrag Dialog

- ☐ Geben Sie als Ring-ID den Wert „1“ ein, als Bezeichnung für diesen Sub-Ring.
- ☐ Geben Sie im Feld Modul.Port die Bezeichnung des Ports ein (in der Form X.X), der das Gerät mit dem Sub-Ring verbindet (Im Beispiel 1.9). Als Verbindungsport können Sie alle verfügbaren Ports nutzen, die Sie nicht bereits als Ring-Ports des Basis-Rings konfiguriert haben.
- ☐ Geben Sie optional einen Namen für den Sub-Ring ein (Im Beispiel „Test“).
- ☐ Wählen Sie den Sub-Ring-Manager Modus (SRM-Modus). Hierdurch legen Sie fest, welche Verbindung zwischen Basis-Ring und Sub-Ring zur Redundanzstrecke wird.
  Die Möglichkeiten der Anbindung sind:
  - Beide Sub-Ring Manager haben die gleiche Einstellung (Vorgabe `manager`): - das Gerät mit der höheren MAC-Adresse verwaltet die Redundanzstrecke.
  - Ein Gerät wird durch Auswahl im Feld SRM-Modus `redundant manager`: - dieses Gerät verwaltet die Redundanzstrecke, solange Sie den anderen Sub-Ring-Manager als `manager` konfiguriert haben - ansonsten gilt wieder die höhere MAC-Adresse.

  Konfigurieren Sie nach der Übersichtszeichnung für dieses Beispiel den Sub-Ring-Manager 1 als „manager“ und den Sub-Ring-Manager 2 als Verwalter der redundanten Strecke als „redundant manager“.

☐ Belassen Sie die Felder VLAN-ID (Vorgabe: 0) und MRP-Domain (Vorgabe 255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255) im Grundzustand. Die Beispielkonfiguration erfordert hier keine Änderung.

☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

☐ Klicken Sie auf „Zurück“, um zum Sub-Ring Dialog zurückzukehren.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`sub-ring new-ring 1`	Legt einen neuen Sub-Ring mit der Sub-Ring-ID 1 an.
`Sub-Ring ID created:ID: 1`	
`sub-ring 1 port 1/9`	Definiert den Port 9 im Modul 1 als Sub Ring Port.
`Port set to 1/9`	
`sub-ring 1 ring-name Test`	Vergibt den Namen „Test“ für den Sub-Ring 1
`Sub-Ring Ring name set to "Test"`	
`sub-ring 1 mode manager`	Konfiguriert den Modus dieses Sub-Ring-Manager als „manager“.
`Mode of Switch set to manager`	

☐ Klicken Sie auf „Laden“, um die Sub-Ring-Übersicht zu aktualisieren und überprüfen Sie alle Einträge.

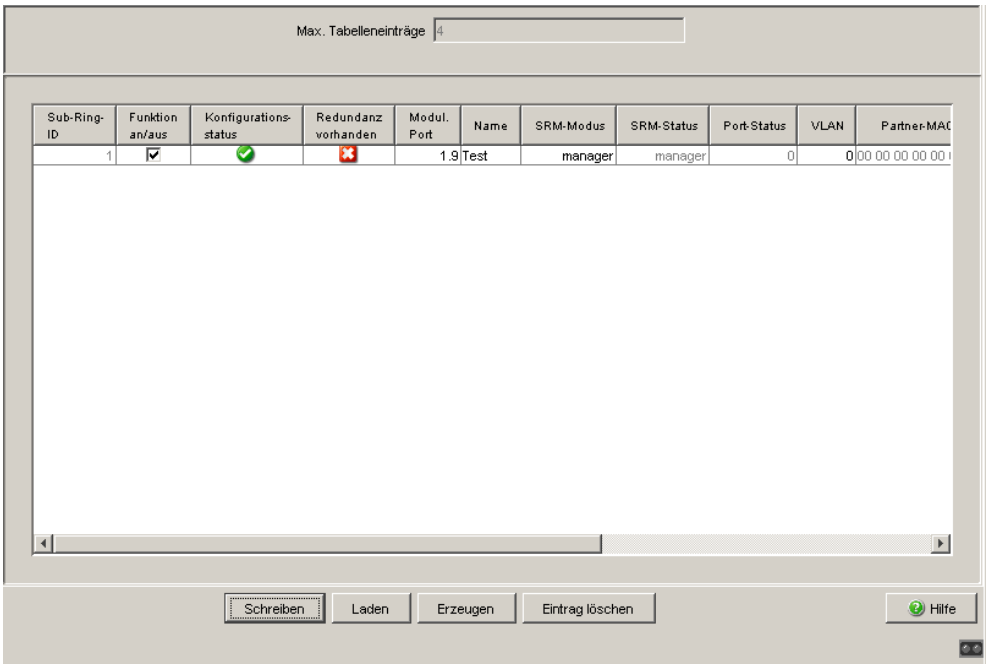


Abb. 19: Vollständig konfigurierter Sub-Ring-Manager

- ☐ Konfigurieren Sie den 2. Sub-Ring-Manager analog. Wenn Sie dem SRM 1 explizit den SRM-Modus `manager` zugewiesen haben, so konfigurieren Sie den SRM 2 als `redundant manager`. Anderenfalls erfolgt die Zuweisung automatisch über die höhere MAC Adresse (s.o.)
- ☐ Schalten Sie die beiden Sub-Ring-Manager in der Übersicht des Sub-Ring-Dialogs unter „Funktion an/aus“ an.
- ☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
- ☐ Wählen Sie den Dialog `Grundeinstellungen:Laden/Speichern`.
- ☐ Wählen Sie im Rahmen „Speichern“ den Speicherort „auf dem Gerät“ und klicken Sie auf „Sichern“, um die Konfiguration nichtflüchtig in der aktiven Konfiguration zu speichern.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`sub-ring 1 operation enable`	Schaltet den Sub-Ring mit der Sub-Ring-ID 1 ein.
`Operation set to Enabled`	
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show sub-ring`	Zeigt den Status für alle Sub-Ringe auf diesem Gerät an.

```
Ring ID: 1
Mode of Switch (administrative setting)... manager
Mode of Switch (real operating state)..... manager
Port Number............................... 1/9,  State: Forwarding
Protocol.................................. Standard MRP
MRP Domain ID.............................
255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255Ri
ng Name................................... Test
Partner MAC............................... 02:E3:00:1B:00:09
VLAN ID................................... 0 (No VLAN)
Operation................................. Enabled

General Operating States:
SRM Setup Info (Config. Failure)......... No Error

Manager-related Operating States:
Ring State................................ Open
Redundancy Guaranteed..................... No
```

```
copy system:running-config
  nvram:startup-config
```

Die aktuelle Konfiguration in den nichtflüchtigen Speicher sichern.

☐ Haben Sie beide SRM und ggf. die im Sub-Ring eingebundenen Geräte konfiguriert, schließen Sie die redundante Strecke des Sub-Rings.

5 Ring-/Netzkopplung

Die Ring-/Netzkopplung erlaubt, ausgehend von einem Ring, die redundante Kopplung von redundanten Ringen oder Netzsegmenten. Die Ring-/Netzkopplung verbindet 2 Ringe/Netzsegmente über 2 getrennte Pfade.

Die Ring-/Netzkopplung unterstützt die Kopplung eines Rings (HIPER-Ring, Fast HIPER-Ring oder MRP) an einen zweiten Ring (ebenfalls HIPER-Ring, Fast HIPER-Ring oder MRP) oder an ein Netzsegment beliebiger Struktur, wenn alle Geräte im angekoppelten Netz Hirschmann-Geräte sind.

Anmerkung: Je nach Ausführung besitzen die Geräte einen DIP-Schalter, mit dem zwischen der Software-Konfiguration und der DIP-Schalter-Konfiguration gewählt werden kann. Ab Software-Version 8.x bietet Ihnen das Gerät die Möglichkeit, die Einstellungen der DIP-Schalter zu deaktivieren oder mit Software-Einstellungen zu überschreiben. Dadurch haben Sie die Möglichkeit, die Port-Einstellungen frei zu wählen.

Die Ring-/Netzkopplung unterstützen die folgenden Geräte:

- RS2-./.
- RS2-16M
- RS20, RS30, RS40
- OCTOPUS
- MICE (ab Rel. 3.0)
- PowerMICE
- MS20, MS30
- RSR20, RSR30
- MACH 100
- MACH 1000
- MACH 1040
- MACH 3000 (ab Rel. 3.3),
- MACH 4000

5.1 Die Varianten der Ring-/Netzkopplung

Die redundante Kopplung erfolgt bei der **Ein-Switch-Kopplung** von zwei Ports **eines** Geräts im ersten Ring/Netzsegment zu je einem Port zweier Geräte im zweiten Ring/Netzsegment (siehe Abbildung 21). Eine der beiden Verbindungen, die redundante, ist während des Normalbetriebs für normalen Datenverkehr gesperrt.
Wenn die Hauptstrecke nicht mehr funktioniert, öffnet das Gerät sofort die redundante Strecke. Wenn die Hauptstrecke später wieder funktioniert, wird die redundante Strecke wieder für normalen Datenverkehr gesperrt und wieder die Hauptstrecke verwendet.
Die Ringkopplung erkennt und behandelt einen Ausfall innerhalb von 500 ms (typisch 150 ms).

Die redundante Kopplung erfolgt bei der **Zwei-Switch-Kopplung** von je einem Port **zweier** Geräte im ersten Ring/Netzsegment zu je einem Port zweier Geräte im zweiten Ring/Netzsegment (siehe Abbildung 27).
Das Gerät in der redundanten Strecke und das Gerät in der Hauptstrecke teilen sich mit Steuerpaketen über das Ethernet oder über die Steuerleitung ihre Betriebszustände mit.
Wenn die Hauptstrecke nicht mehr funktioniert, öffnet das redundante Gerät (Slave genannt) die redundante Strecke. Wenn die Hauptstrecke später wieder funktioniert, teilt das Gerät in der Hauptstrecke dies dem redundanten Gerät mit. Die redundante Strecke wird wieder für normalen Datenverkehr gesperrt und wieder die Hauptstrecke verwendet.
Die Ringkopplung erkennt und behandelt einen Ausfall innerhalb von 500 ms (typisch 150 ms).

Die Art der Kopplung wird in erster Linie von den topologischen Gegebenheiten und dem gewünschten Grad der Verfügbarkeit bestimmt (siehe Tabelle 6).

	Ein-Switch-Kopplung	Zwei-Switch-Kopplung	Zwei-Switch-Kopplung mit Steuerleitung
Anwendung	Die beteiligten Geräte sind topologisch ungünstig verteilt. Die Leitungsführung wäre bei einer Zwei-Switch-Kopplung dadurch aufwändig.	Die beteiligten Geräte sind topologisch günstig verteilt. Die Verlegung einer Steuerleitung ist aufwändig.	Die beteiligten Geräte sind topologisch günstig verteilt. Die Verlegung einer Steuerleitung ist nicht aufwändig.
Nachteil	Bei Ausfall des für die redundante Kopplung konfigurierten Switches ist keine Verbindung zwischen den Netzen mehr vorhanden.	Höherer Aufwand, die beteiligten Geräte zu vernetzen - im Vergleich zu Ein-Switch-Kopplung.	Höherer Aufwand, die beteiligten Geräte zu vernetzen - im Vergleich zu Ein-Switch-Kopplung und Zwei-Switch-Kopplung.
Vorteil	Weniger Aufwand, die beteiligten Geräte zu vernetzen - im Vergleich zu Zwei-Switch-Kopplung.	Bei Ausfall eines der für die redundante Kopplung konfigurierten Geräte ist immer noch eine Verbindung zwischen den Netzen vorhanden.	Bei Ausfall eines der für die redundante Kopplung konfigurierten Geräte ist immer noch eine Verbindung zwischen den Netzen vorhanden. Die Partnerfindung zwischen den koppelnden Geräten verläuft sicherer und schneller als ohne Steuerleitung.

Tab. 6: Auswahlkriterien für die Typen der redundanten Kopplungkonfiguration

Anmerkung: Wählen sie eine Konfiguration nach den bestehenden topologischen Umständen und dem Maß an Verfügbarkeit, das Sie benötigen, aus (siehe Tabelle 6).

5.2 Ring-/Netzkopplung vorbereiten

5.2.1 STAND-BY-Schalter

Alle Geräte besitzen einen STAND-BY-Schalter, mit dem Sie die Rolle des Geräts innerhalb einer Ring-/Netzkopplung bestimmen.
Dieser Schalter ist je nach Gerätetyp ausgeführt als ein DIP-Schalter an den Geräten oder ausschließlich als eine Software-Einstellung (Dialog `Redundanz:Ring-/Netzkopplung`). Sie bestimmen durch das Einstellen dieses Schalters, ob das Gerät innerhalb einer Ring-/Netzkopplung die Haupt- oder die redundante Kopplungs-Rolle ausführt. Details zu den DIP-Schaltern finden Sie im Anwender-Handbuch Installation.

Gerätetyp	Ausführung STAND-BY Schalter
RS2-./.	DIP-Schalter
RS2-16M	DIP-Schalter
RS20/RS30/RS40	Schaltbar zwischen DIP-Schalter und Software-Einstellung
MICE/PowerMICE	Schaltbar zwischen DIP-Schalter und Software-Einstellung
MS20/MS30	Schaltbar zwischen DIP-Schalter und Software-Einstellung
OCTOPUS	Software-Schalter
RSR20/RSR30	Software-Schalter
MACH 100	Software-Schalter
MACH 1000	Software-Schalter
MACH 3000/MACH 4000	Software-Schalter

Tab. 7: Übersicht Ausführung des STAND-BY Schalters

Setzen Sie den STAND-BY-Schalter abhängig von Gerät und Ausführung anhand der folgenden Tabelle:

Gerät mit	Wahl zwischen Hauptkopplung und redundanter Kopplung
DIP-Schalter	Am DIP-Schalter „STAND-BY“
DIP-Schalter-/Software-Schalter-Alternative	Entsprechend der gewählten Option - am DIP-Schalter „STAND-BY“ oder im - Dialog `Redundanz:Ring-/Netzkopplung` durch Wahl in „Konfiguration auswählen“. **Hinweis:** Diese Geräte besitzen einen DIP-Schalter, mit dem zwischen der Software-Konfiguration und der DIP-Schalter-Konfiguration gewählt werden kann. Details zu den DIP-Schaltern an den Geräten finden Sie im Anwender-Handbuch Installation.
Software-Schalter	Im Dialog `Redundanz:Ring-/Netzkopplung`

Tab. 8: Einstellen des STAND-BY-Schalters

Anmerkung: In den folgenden Screen-Shots und Diagrammen werden die folgenden Konventionen verwendet:

- Blaue Farbe bezeichnet Geräte oder Verbindungen im aktuellen Betrachtungsumfang,
- schwarze Farbe bezeichnet Geräte oder Verbindungen, die an den aktuellen Betrachtungsumfang anschließen,
- dicke Linien bezeichnen Verbindungen im aktuellen Betrachtungsumfang,
- dünne Linien bezeichnen Verbindungen, die an den aktuellen Betrachtungsumfang anschließen,
- die gestrichelte Linie bezeichnet die redundante Verbindung,
- die punktierte Linie bezeichnet die Steuerleitung.

☐ Wählen Sie den Dialog `Redundanz:Ring-/Netzkopplung`.

☐ Wählen Sie als erstes die gewünschte Konfiguration Ein-Switch-Kopplung („1“), Zwei-Switch-Kopplung („2“) oder Zwei-Switch-Kopplung mit Steuerleitung („3“), (siehe Abbildung 20).

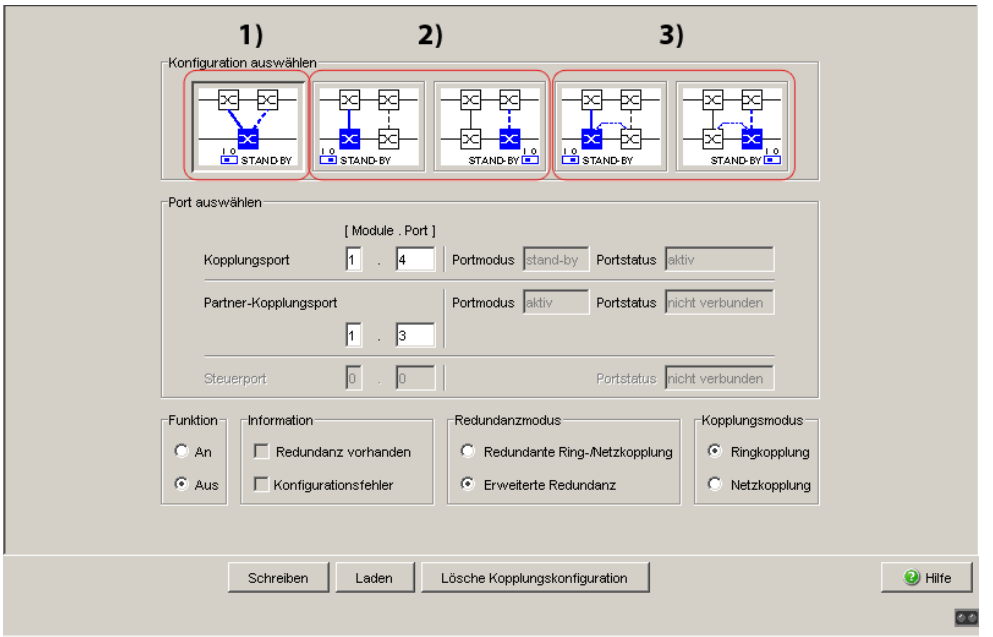


Abb. 20: Ringkopplungs-Konfiguration auswählen (bei deaktivierten DIP-Schaltern oder bei Geräten ohne DIP-Schalter)

Bei Geräten ohne DIP-Schalter sind die Software-Einstellungen nicht eingeschränkt.
Bei Geräten **mit** DIP-Schaltern zeigt der Dialog in Abhängigkeit der DIP-Schalterstellung die möglichen Konfigurationen farbig, die nicht möglichen Konfigurationen jedoch ausgegraut an.
Die möglichen Konfigurationen sind:

- DIP-Schalter RM: ON oder OFF, STAND-BY: OFF:
  Zwei-Switch-Kopplung als Master (mit oder ohne Steuerleitung)
- DIP-Schalter RM: OFF, STAND-BY: ON:
  Ein-Switch-Kopplung und Zwei-Switch-Kopplung als Slave (mit oder ohne Steuerleitung)
- DIP-Schalter RM: ON, STAND-BY: ON:
  DIP-Schalter sind deaktiviert, Software-Einstellungen sind uneingeschränkt möglich

Sind die DIP-Schalter aktiviert und möchten Sie per Software eine der nicht möglichen (ausgegrauten) Konfigurationen wählen, bringen Sie die DIP-Schalter am Gerät in eine andere Stellung und laden Sie den Dialog erneut.

Anmerkung: Unterlassen Sie die Kombination von Rapid Spanning Tree und Ring-/Netzkopplung. Konkurrierende Redundanz-Funktionen sind unzulässig.

5.2.2 Ein-Switch-Kopplung

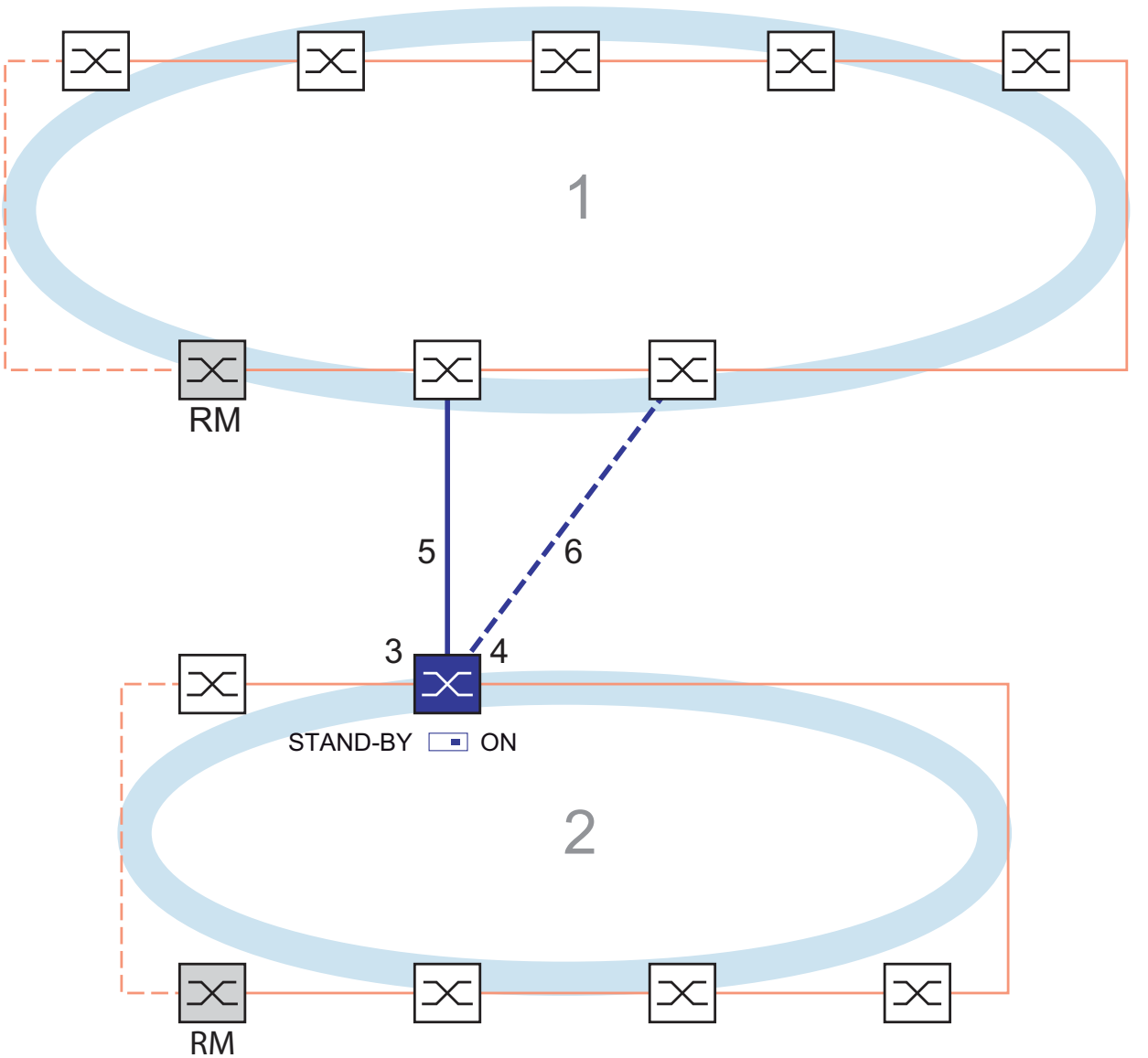


Abb. 21: Beispiel Ein-Switch-Kopplung
1: Backbone
2: Ring
3: Partner-Kopplungsport
4: Kopplungsport
5: Hauptleitung
6: Redundante Leitung

Die Kopplung zwischen zwei Netzen erfolgt im Normalbetrieb über die Hauptleitung (durchgezogene blaue Linie), die mit dem Partner-Kopplungsport verbunden ist. Beim Ausfall der Hauptleitung übernimmt die redundante Leitung (gestrichelte blaue Line), die mit dem Kopplungsport verbunden ist, die Kopplung der beiden Netze. Die Kopplung erfolgt über **einen** Switch.

☐ Wählen Sie den Dialog `Redundanz:Ring-/Netzkopplung`.
☐ Wählen Sie die „Ein-Switch-Kopplung“ mit Hilfe des Dialog-Buttons mit der selben Grafik wie die untenstehende (siehe Abbildung 22).

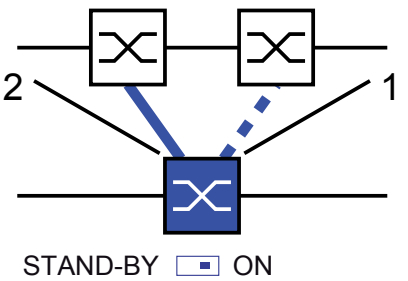


Abb. 22: Ein-Switch-Kopplung
1: Kopplungsport
2: Partner-Kopplungsport

Die folgenden Einstellungen betreffen den in der ausgewählten Grafik blau dargestellten Switch.

☐ Wählen Sie den Partner-Kopplungsport aus (siehe Abbildung 23). Mit „Partner-Kopplungsport“ legen Sie fest, an welchen Port Sie die Hauptleitung anschließen.
Die Portzuordnung für die redundante Kopplung finden Sie in Tabelle 9.

Die folgenden Tabellen zeigen Auswahlmöglichkeiten und Voreinstellungen für die in der Ring-/Netzkopplung genutzten Ports.

Gerät	Partner-Kopplungsport	Kopplungsport
RS2-./.	nicht möglich	nicht möglich
RS2-16M	alle Ports (Lieferzustand: Port 2)	alle Ports (Lieferzustand: Port 1)

Tab. 9: Portzuordnung Ein-Switch-Kopplung

Gerät	Partner-Kopplungsport	Kopplungsport
RS20, RS30, RS40	alle Ports (Lieferzustand: Port 1.3)	alle Ports (Lieferzustand: Port 1.4)
OCTOPUS	alle Ports (Lieferzustand: Port 1.3)	alle Ports (Lieferzustand: Port 1.4)
MICE	alle Ports (Lieferzustand: Port 1.3)	alle Ports (Lieferzustand: Port 1.4)
PowerMICE	alle Ports (Lieferzustand: Port 1.3)	alle Ports (Lieferzustand: Port 1.4)
MS20	alle Ports (Lieferzustand: Port 1.3)	alle Ports (Lieferzustand: Port 1.4)
MS30	alle Ports (Lieferzustand: Port 2.3)	alle Ports (Lieferzustand: Port 2.4)
RSR20/30	alle Ports (Lieferzustand: Port 1.3)	alle Ports (Lieferzustand: Port 1.4)
MACH 100	alle Ports (Lieferzustand: Port 2.3)	alle Ports (Lieferzustand: Port 2.4)
MACH 1000	alle Ports (Lieferzustand: Port 1.3)	alle Ports (Lieferzustand: Port 1.4)
MACH 3000	alle Ports	alle Ports
MACH 4000	alle Ports (Lieferzustand: Port 1.3)	alle Ports (Lieferzustand: Port 1.4)

Tab. 9: Portzuordnung Ein-Switch-Kopplung

Anmerkung: Konfigurieren Sie den Partner-Kopplungsport und die Ring-Redundanz-Ports auf verschiedenen Ports.

☐ Wählen Sie den Kopplungsport aus (siehe Abbildung 23).
Mit „Kopplungsport“ legen Sie fest, an welchen Port Sie die Verbindung der Netzsegmente anschließen.
Die Portzuordnung für die redundante Kopplung finden Sie in Tabelle 9.

Anmerkung: Konfigurieren Sie den Kopplungsport und die Redundanz-Ring-Ports auf verschiedenen Ports.

☐ Schalten Sie im Rahmen „Funktion“ die Funktion an (siehe Abbildung 23).

☐ Schließen Sie nun die redundante Leitung an.

Die Anzeigen im Rahmen „Port auswählen“ bedeuten:

– „Portmodus“: Der Port ist entweder aktiv oder im Stand-by-Modus.
– „Portstatus“: Der Port ist entweder aktiv, im Stand-by-Modus oder nicht verbunden.

Die Anzeigen im Rahmen „Information“ bedeuten:

– „Redundanz gewährleistet“: Die Redundanz-Funktion ist aktiv.
  – Am Partner-Kopplungsport, an dem die Hauptleitung angeschlossen ist, leuchtet die Link-LED permanent.
  – Am Kopplungsport, an dem die redundante Leitung angeschlossen ist, blinkt die Link-LED gleichmäßig.

  Wenn die Hauptleitung nicht mehr funktioniert, übernimmt die redundante Strecke die Funktion der Hauptleitung.
– „Konfigurationsfehler“: Die Funktion ist unvollständig oder falsch konfiguriert.

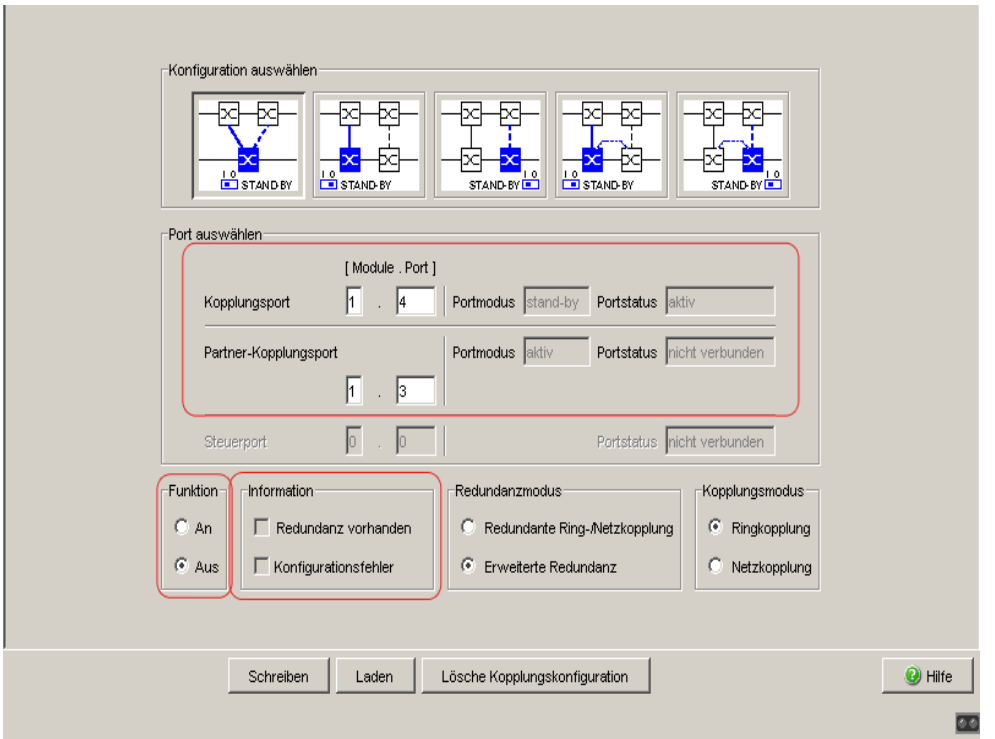


Abb. 23: Ein-Switch-Kopplung: Port auswählen und Funktion ein-/ausschalten

Anmerkung: Für die Kopplungsports sind folgende Einstellungen erforderlich (Wählen Sie hierzu den Dialog `Grundeinstellungen:Portkonfiguration`):
Siehe Tabelle 3 auf Seite 33.

Anmerkung: Wenn VLANs konfiguriert sind, stellen Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports wie folgt ein:

– im Dialog `Switching:VLAN:Port` Port-VLAN-ID 1 und „Ingress Filtering“ deaktiviert
– im Dialog `Switching:VLAN:Statisch` für sämtliche redundanten Verbindungen VLAN 1 und VLAN-Zugehörigkeit `T` (Tagged)
Das Gerät sendet die Redundanzpakete in VLAN 1 mit höchster Priorität.

Redundanzmodus

☐ Wählen Sie im Rahmen „Redundanzmodus“ (siehe Abbildung 24)
– „Redundante Ring-/Netzkopplung“ oder
– „Erweiterte Redundanz“.

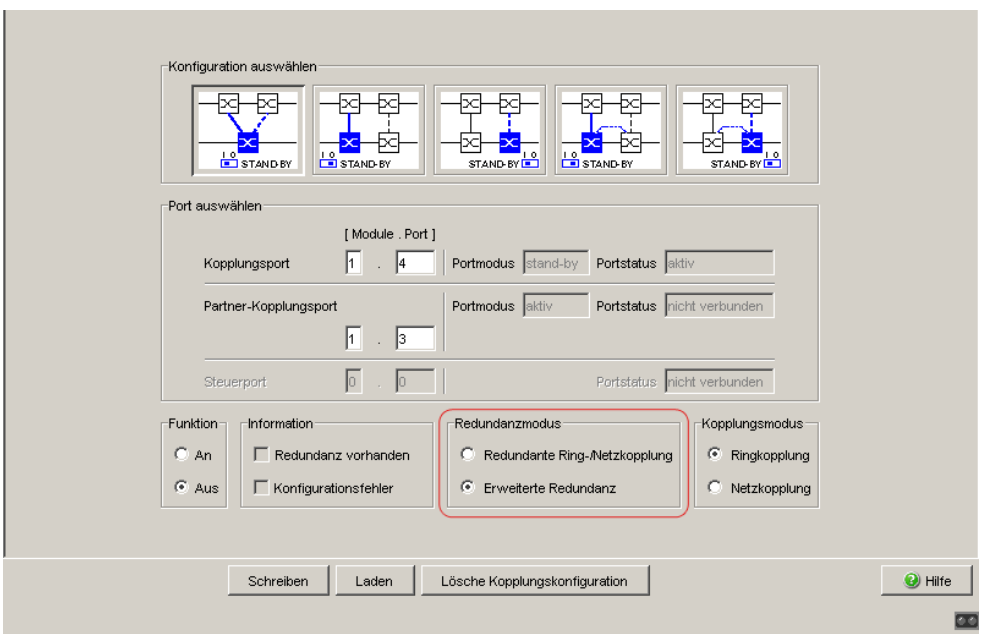


Abb. 24: Ein-Switch-Kopplung: Redundanzmodus auswählen

Bei der Einstellung „`Redundante Ring-/Netzkopplung`“ ist entweder die Hauptleitung oder die redundante Leitung aktiv. Niemals sind beide Leitungen gleichzeitig aktiv.

Bei der Einstellung „`Erweiterte Redundanz`“ sind Hauptleitung und redundante Leitung gleichzeitig aktiv, wenn die Verbindungsleitung zwischen den Geräten im angekoppelten (d.h, dem entfernten) Netz funktionsuntüchtig wird (siehe Abbildung 25).
Während der Rekonfigurationszeit kann es zu Paketdoppelungen kommen. Wählen Sie daher diese Einstellung ausschließlich dann, wenn Ihre Anwendung Paketdoppelungen erkennt.

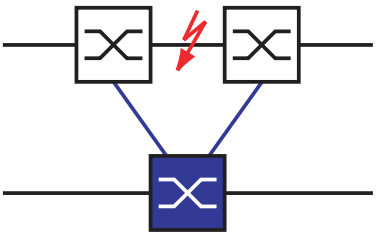


Abb. 25: Erweiterte Redundanz

Kopplungsmodus

Der Kopplungsmodus bezeichnet die Art des angekoppelten Netzes.

☐ Wählen Sie im Rahmen „Kopplungsmodus“ (siehe Abbildung 26)

– „Ringkopplung“ oder

– „Netzkopplung“

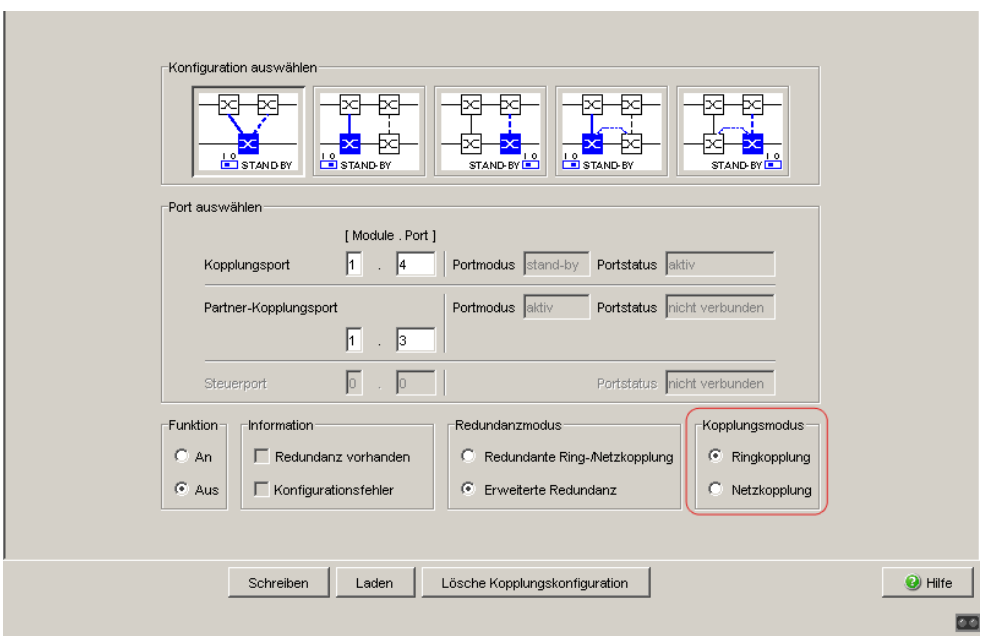


Abb. 26: Ein-Switch-Kopplung: Kopplungsmodus auswählen

☐ Wählen Sie **„Ringkopplung“**, wenn Sie an einen Redundanz-Ring ankoppeln.

☐ Wählen Sie **„Netzkopplung“**, wenn Sie an eine Linien- oder Baumstruktur ankoppeln.

Lösche Kopplungskonfiguration

☐ Die „Lösche Kopplungskonfiguration“-Bedientaste im Dialog bietet Ihnen die Möglichkeit, alle Kopplungs-Einstellungen des Gerätes in den Lieferzustand zurück zu versetzen.

5.2.3 Zwei-Switch-Kopplung

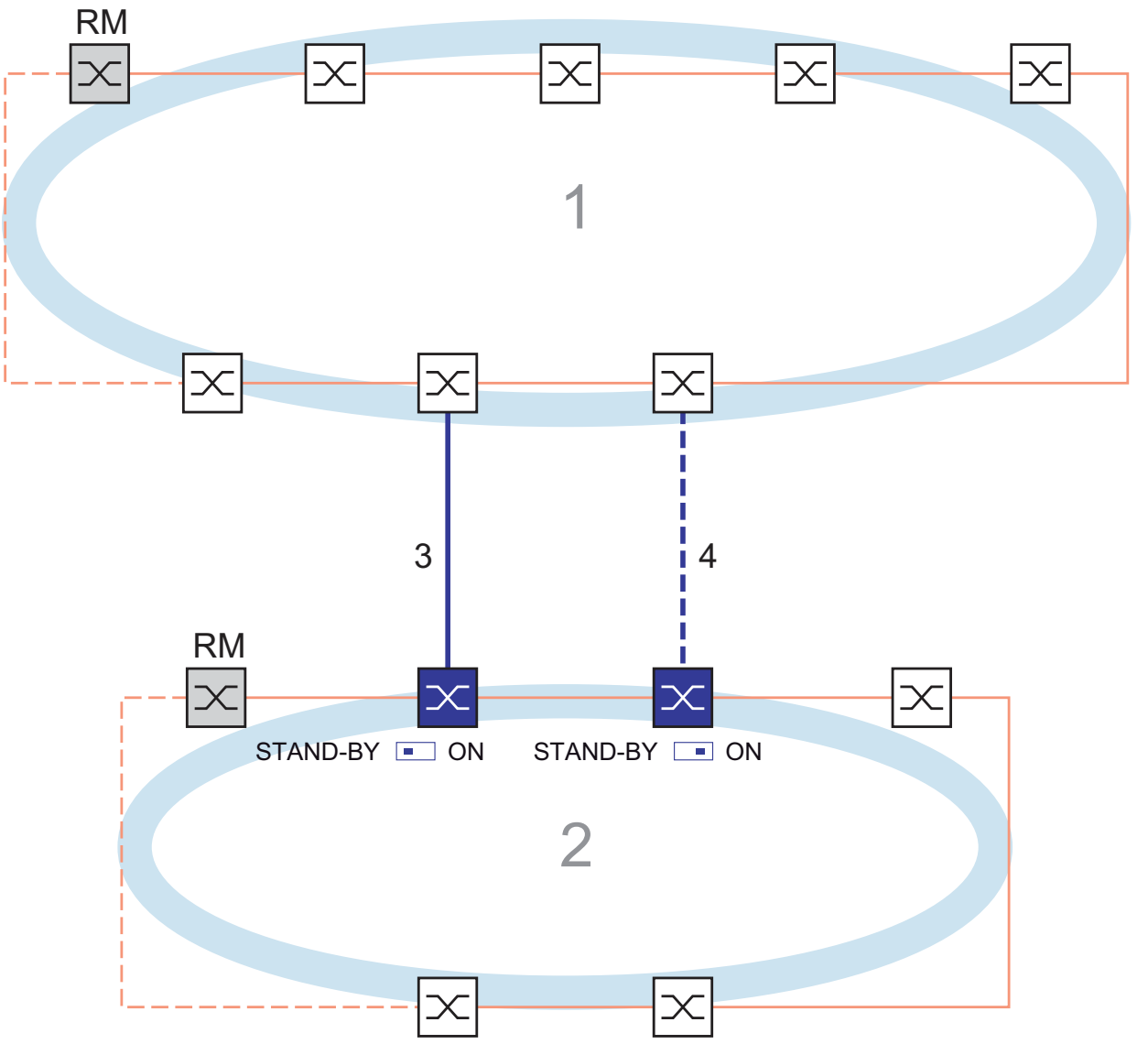


Abb. 27: Beispiel Zwei-Switch-Kopplung
1: Backbone
2: Ring
3: Hauptleitung
4: Redundante Leitung

Die Kopplung zwischen 2 Netzen erfolgt über die Hauptleitung (durchgezogene blaue Linie). Beim Ausfall der Hauptleitung oder einem der angrenzenden Switche übernimmt die redundante Leitung (gestrichelte schwarze Linie) die Kopplung der beiden Netze.
Die Kopplung erfolgt über zwei Switche.
Die Switche übermitteln ihre Kontrollpakete über das Ethernet.
Der an die Hauptleitung angeschlossene Switch und der an die redundante Leitung angeschlossene Switch sind Partner bezüglich der Kopplung.

☐ Verbinden Sie die beiden Partner über ihre Ringports.

☐ Wählen Sie den Dialog `Redundanz:Ring-/Netzkopplung`.
☐ Wählen Sie die „Zwei-Switch-Kopplung“ mit Hilfe des Dialog-Buttons mit der selben Grafik wie die untenstehende (siehe Abbildung 28).

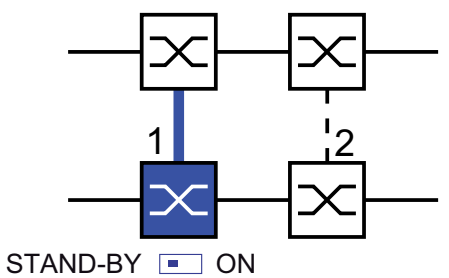


Abb. 28: Zwei-Switch-Kopplung
1: Kopplungsport
2: Partner-Kopplungsport

Die folgenden Einstellungen betreffen den in der ausgewählten Grafik blau dargestellten Switch.

☐ Wählen Sie den Kopplungsport aus (siehe Abbildung 29).
Mit „Kopplungsport“ legen Sie fest, an welchen Port Sie die Verbindung der Netzsegmente anschließen.
Die Portzuordnung für die redundante Kopplung finden Sie in Tabelle 10.

☐ Bei einem Gerät mit DIP-Schaltern schalten Sie den STAND-BY-Schalter auf OFF oder deaktivieren Sie die DIP-Schalter. Schließen Sie die Hauptleitung am Kopplungsport an.

Gerät	Kopplungsport
RS2-./.	nicht möglich
RS2-16M	Einstellbar für alle Ports (Lieferzustand: Port 1)
RS20, RS30, RS40	Einstellbar für alle Ports (Lieferzustand: Port 1.4)
OCTOPUS	Einstellbar für alle Ports (Lieferzustand: Port 1.4)
MICE	Einstellbar für alle Ports (Lieferzustand: Port 1.4)
PowerMICE	Einstellbar für alle Ports (Lieferzustand: Port 1.4)
MS20	Einstellbar für alle Ports (Lieferzustand: Port 1.4)
MS30	einstellbar für alle Ports (Lieferzustand: Port 2.4)
RSR20/30	Einstellbar für alle Ports (Lieferzustand: Port 1.4)
MACH 100	einstellbar für alle Ports (Lieferzustand: Port 2.4)
MACH 1000	Einstellbar für alle Ports (Lieferzustand: Port 1.4)
MACH 3000	Einstellbar für alle Ports
MACH 4000	Einstellbar für alle Ports (Lieferzustand: Port 1.4)

Tab. 10: Portzuordnung für die redundante Kopplung (Zwei-Switch-Kopplung)

Anmerkung: Konfigurieren Sie den Kopplungsport und die Redundanz-Ring-Ports auf verschiedenen Ports.

☐ Schalten Sie im Rahmen „Funktion“ die Funktion an (siehe Abbildung 29).

☐ Schließen Sie nun die redundante Leitung an.

Die Anzeigen im Rahmen „Port auswählen“ bedeuten:

– „Portmodus“: Der Port ist entweder aktiv oder im Stand-by-Modus.
– „Portstatus“: Der Port ist entweder aktiv, im Stand-by-Modus oder nicht verbunden.
– „IP-Adresse“: Die IP-Adresse des Partners, soweit dieser im Netz schon in Betrieb ist.

Die Anzeigen im Rahmen „Information“ bedeuten:

– „Redundanz gewährleistet“: Die Redundanz-Funktion ist aktiv.
  – Am Partner-Kopplungsport, an dem die Hauptleitung angeschlossen ist, leuchtet die Link-LED permanent.
  – Am Kopplungsport, an dem die redundante Leitung angeschlossen ist, blinkt die Link-LED gleichmäßig.

  Wenn die Hauptleitung nicht mehr funktioniert, übernimmt die redundante Strecke die Funktion der Hauptleitung.
– „Konfigurationsfehler“: Die Funktion ist unvollständig oder falsch konfiguriert.

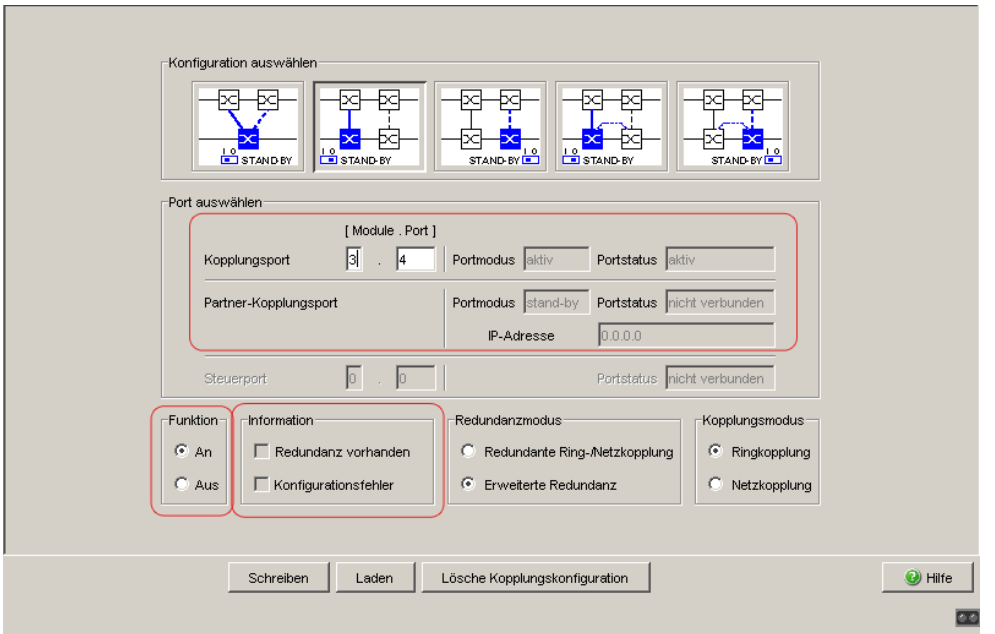


Abb. 29: Zwei-Switch-Kopplung: Port auswählen und Funktion ein-/ausschalten

Um dauerhafte Schleifen (Loops) zu vermeiden, setzt der Switch den Portstatus des Kopplungsports auf „aus“, wenn Sie:
– die Funktion ausschalten oder
– die Konfiguration wechseln
während die Verbindungen an diesen Ports in Betrieb sind.

Anmerkung: Für die Kopplungsports sind folgende Einstellungen erforderlich (Wählen Sie hierzu den Dialog `Grundeinstellungen:Portkonfiguration`):
Siehe Tabelle 3 auf Seite 33.

Anmerkung: Wenn VLANs konfiguriert sind, stellen Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports wie folgt ein:
– im Dialog `Switching:VLAN:Port` Port-VLAN-ID 1 und „Ingress Filtering“ deaktiviert
– im Dialog `Switching:VLAN:Statisch` für sämtliche redundanten Verbindungen VLAN 1 und VLAN-Zugehörigkeit `T` (Tagged)
Das Gerät sendet die Redundanzpakete in VLAN 1 mit höchster Priorität.

Anmerkung: Wenn Sie die Funktionen Ring-Manager und Zwei-Switch-Kopplung in einem Gerät betreiben, besteht die Möglichkeit einer Schleifenbildung (Loop).

☐ Wählen Sie die „Zwei-Switch-Kopplung“ mit Hilfe des Dialog-Buttons mit der selben Grafik wie die untenstehende (siehe Abbildung 30).

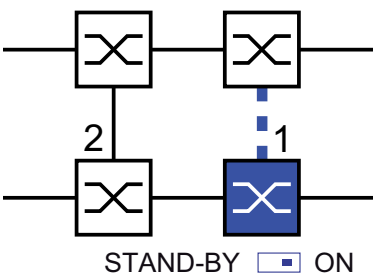


Abb. 30: Zwei-Switch-Kopplung
1: Kopplungsport
2: Partner-Kopplungsport

Die folgenden Einstellungen betreffen den in der ausgewählten Grafik blau dargestellten Switch.

☐ Wählen Sie den Kopplungsport aus (siehe Abbildung 29).
Mit „Kopplungsport“ legen Sie fest, an welchen Port Sie die Verbindung der Netzsegmente anschließen.
Die Portzuordnung für die redundante Kopplung finden Sie in Tabelle 10.

☐ Bei einem Gerät mit DIP-Schaltern schalten Sie den STAND-BY-Schalter auf ON oder deaktivieren Sie die DIP-Schalter. Schließen Sie die redundante Leitung am Kopplungsport an.

Anmerkung: Konfigurieren Sie den Kopplungsport und die Redundanz-Ring-Ports auf verschiedenen Ports.

☐ Schalten Sie im Rahmen „Funktion“ die Funktion an (siehe Abbildung 29).

Die Anzeigen im Rahmen „Port auswählen“ bedeuten:
– „Portmodus“: Der Port ist entweder aktiv oder im Stand-by-Modus.
– „Portstatus“: Der Port ist entweder aktiv, im Stand-by-Modus oder nicht verbunden.
– „IP-Adresse“: Die IP-Adresse des Partners, soweit dieser im Netz schon in Betrieb ist.

Die Anzeigen im Rahmen „Information“ bedeuten:
– „Redundanz gewährleistet“: Die Redundanz-Funktion ist aktiv.
  – Am Partner-Kopplungsport, an dem die Hauptleitung angeschlossen ist, leuchtet die Link-LED permanent.
  – Am Kopplungsport, an dem die redundante Leitung angeschlossen ist, blinkt die Link-LED gleichmäßig.

  Wenn die Hauptleitung nicht mehr funktioniert, übernimmt die redundante Strecke die Funktion der Hauptleitung.
– „Konfigurationsfehler“: Die Funktion ist unvollständig oder falsch konfiguriert.

Um dauerhafte Schleifen (Loops) zu vermeiden, setzt der Switch den Portstatus des Kopplungsports auf „aus“, wenn Sie:
– die Funktion ausschalten oder
– die Konfiguration wechseln,

während die Verbindungen an diesen Ports in Betrieb sind.

Anmerkung: Für die Kopplungsports sind folgende Einstellungen erforderlich (Wählen Sie hierzu den Dialog `Grundeinstellungen:Portkonfiguration`):
Siehe Tabelle 3 auf Seite 33.

Anmerkung: Wenn VLANs konfiguriert sind, stellen Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports wie folgt ein:
– im Dialog `Switching:VLAN:Port` Port-VLAN-ID 1 und „Ingress Filtering“ deaktiviert
– im Dialog `Switching:VLAN:Statisch` für sämtliche redundanten Verbindungen VLAN 1 und VLAN-Zugehörigkeit `T` (Tagged)
  Das Gerät sendet die Redundanzpakete in VLAN 1 mit höchster Priorität.

Anmerkung: Wenn Sie die Funktionen Ring-Manager und Zwei-Switch-Kopplung in einem Gerät betreiben, besteht die Möglichkeit einer Schleifenbildung (Loop).

Redundanzmodus

☐ Wählen Sie im Rahmen „Redundanzmodus“ (siehe Abbildung 31)

– „Redundante Ring-/Netzkopplung“ oder

– „Erweiterte Redundanz“.

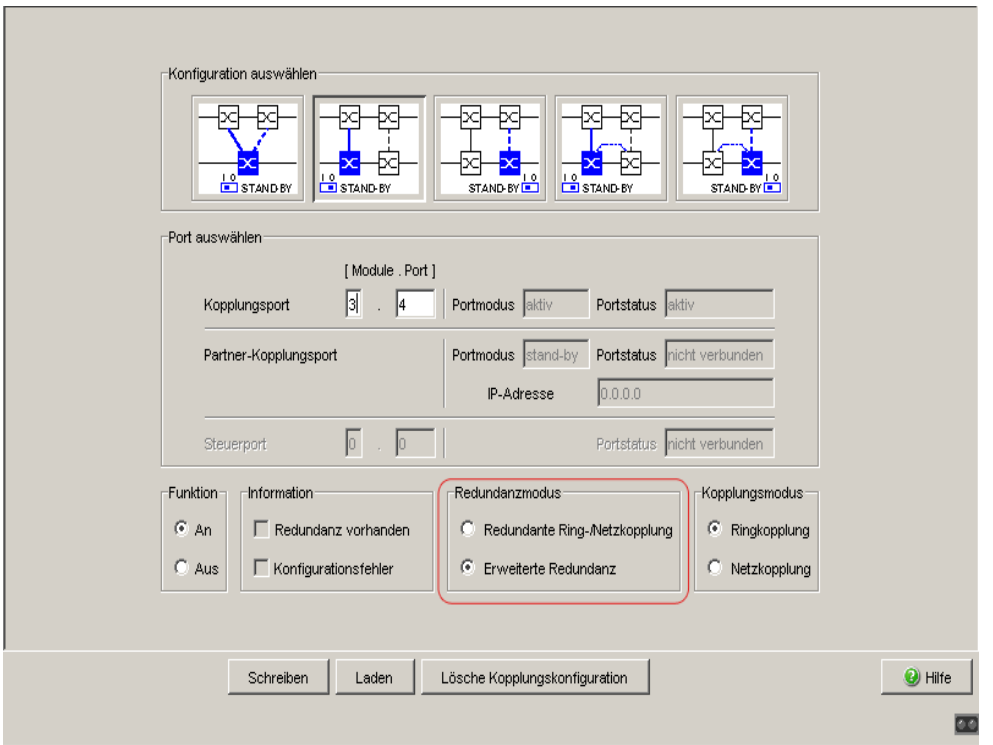


Abb. 31: Zwei-Switch-Kopplung: Redundanzmodus auswählen

Bei der Einstellung „`Redundante Ring-/Netzkopplung`“ ist entweder die Hauptleitung oder die redundante Leitung aktiv. Niemals sind beide Leitungen gleichzeitig aktiv.

Bei der Einstellung „`Erweiterte Redundanz`“ sind Hauptleitung und redundante Leitung gleichzeitig aktiv, wenn die Verbindungsleitung zwischen den Geräten im angekoppelten (d.h, dem entfernten) Netz funktionsuntüchtig wird (siehe Abbildung 25).
Während der Rekonfigurationszeit kann es zu Paketdoppelungen kommen. Wählen Sie daher diese Einstellung ausschließlich dann, wenn Ihre Anwendung Paketdoppelungen erkennt.

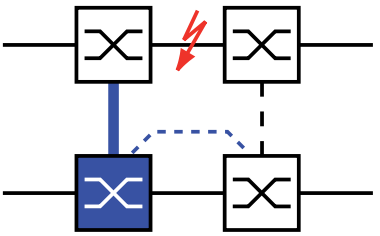


Abb. 32: Erweiterte Redundanz

Kopplungsmodus

Der Kopplungsmodus bezeichnet die Art des angekoppelten Netzes.

☐ Wählen Sie im Rahmen „Kopplungsmodus“ (siehe Abbildung 33)
– „Ringkopplung“ oder
– „Netzkopplung“

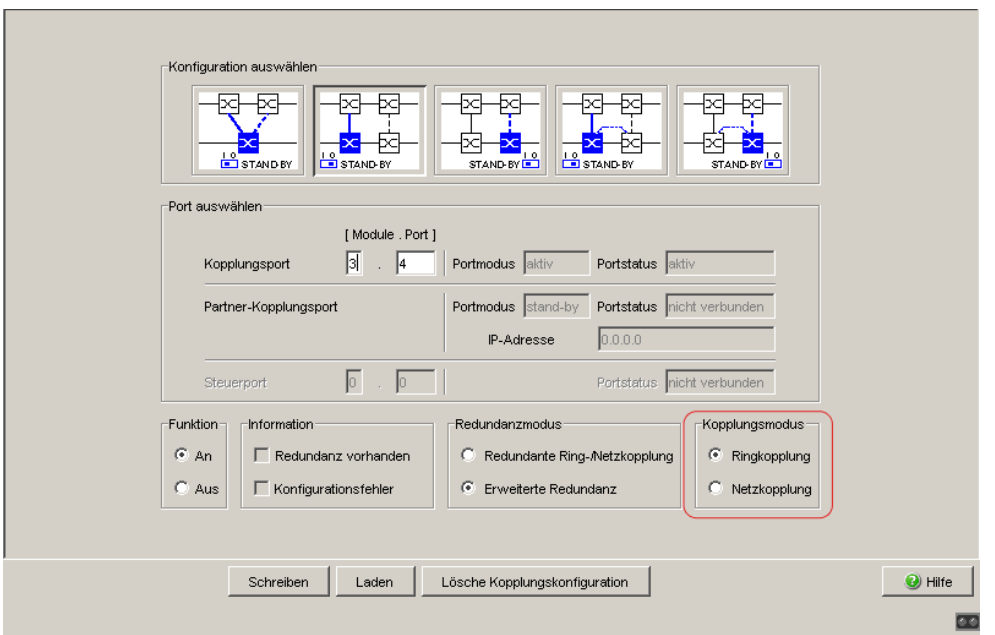


Abb. 33: Zwei-Switch-Kopplung: Kopplungsmodus auswählen

☐ Wählen Sie **„Ringkopplung“**, wenn Sie an einen Redundanz-Ring ankoppeln.
☐ Wählen Sie **„Netzkopplung“**, wenn Sie an eine Linien- oder Baumstruktur ankoppeln.

Lösche Kopplungskonfiguration

☐ Die „Lösche Kopplungskonfiguration“-Bedientaste im Dialog bietet Ihnen die Möglichkeit, alle Kopplungs-Einstellungen des Gerätes in den Lieferzustand zurück zu versetzen.

5.2.4 Zwei-Switch-Kopplung mit Steuerleitung

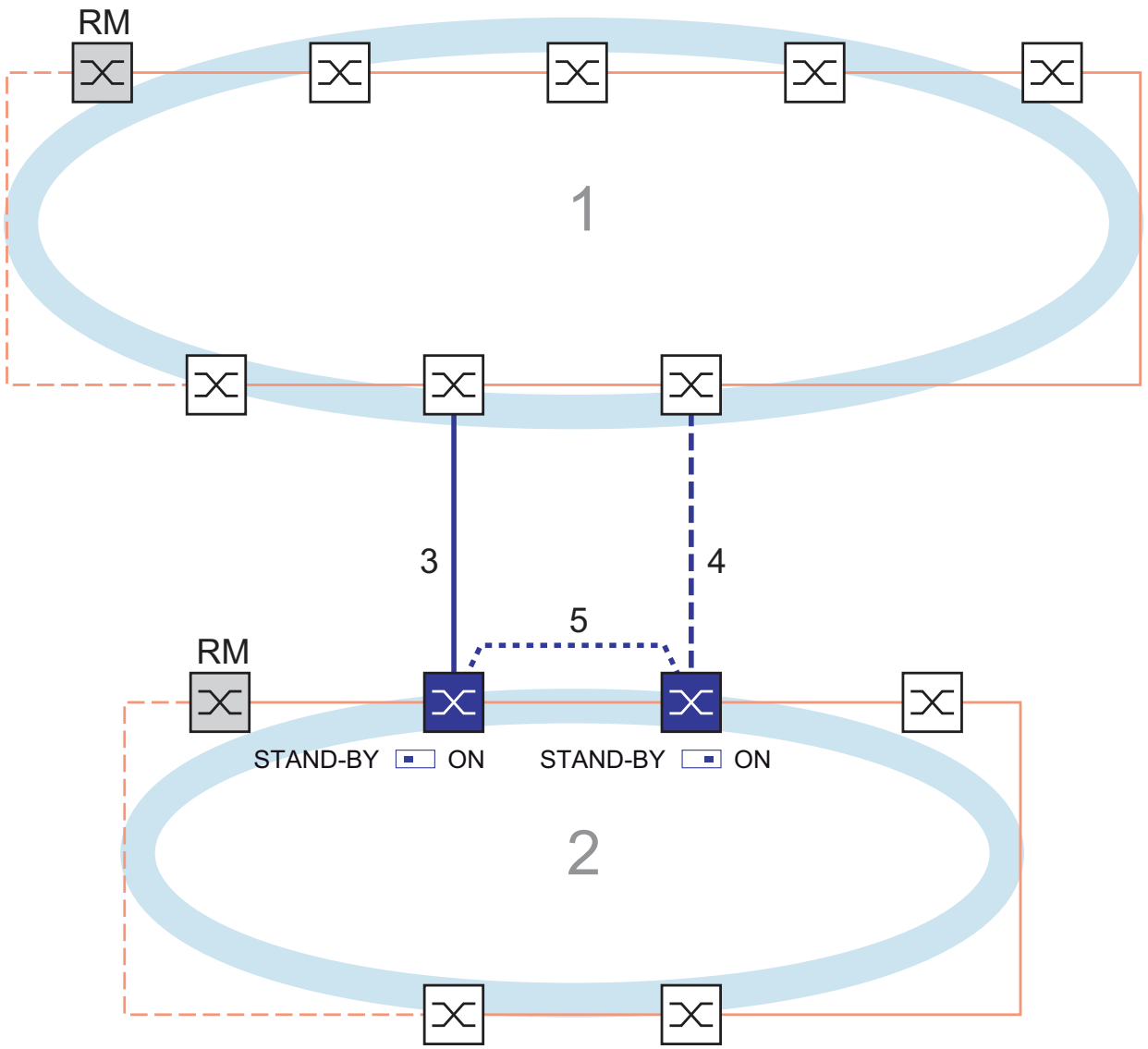


Abb. 34: Beispiel Zwei-Switch-Kopplung mit Steuerleitung
1: Backbone
2: Ring
3: Hauptleitung
4: Redundante Leitung
5: Steuerleitung

Die Kopplung zwischen 2 Netzen erfolgt über die Hauptleitung (durchgezogene blaue Linie). Beim Ausfall der Hauptleitung oder einem der angrenzenden Switche übernimmt die redundante Leitung (gestrichelte schwarze Linie) die Kopplung der beiden Netze.
Die Kopplung erfolgt über zwei Switche.
Die Switche übermitteln ihre Kontrollpakete über eine Steuerleitung (punktierte Linie).
Das Gerät, an dem Sie die Hauptleitung und das Gerät, an dem Sie die redundante Leitung anschließen, sind Partner bezüglich der Kopplung.

☐ Verbinden Sie die beiden Partner über ihre Ringports.

☐ Wählen Sie den Dialog `Redundanz:Ring-/Netzkopplung`.
☐ Wählen Sie die „Zwei-Switch-Kopplung mit Steuerleitung“ mit Hilfe des Dialog-Buttons mit der selben Grafik wie die untenstehende (siehe Abbildung 35).

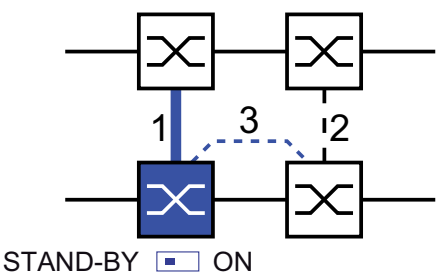


Abb. 35: Zwei-Switch-Kopplung mit Steuerleitung
1: Kopplungsport
2: Partner-Kopplungsport
3: Steuerleitung

Die folgenden Einstellungen betreffen den in der ausgewählten Grafik blau dargestellten Switch.
☐ Wählen Sie den Kopplungsport aus (siehe Abbildung 36).
Mit „Kopplungsport“ legen Sie fest, an welchen Port Sie die Verbindung der Netzsegmente anschließen.
Die Portzuordnung für die redundante Kopplung finden Sie in Tabelle 11.
☐ Bei einem Gerät mit DIP-Schaltern schalten Sie den STAND-BY-Schalter auf OFF oder deaktivieren Sie die DIP-Schalter. Schließen Sie die Hauptleitung am Kopplungsport an.

☐ Wählen Sie den Steuerport aus (siehe Abbildung 36).
Mit „Steuerport" legen Sie fest, an welchen Port Sie die Steuerleitung anschließen.
Die Portzuordnung für die redundante Kopplung finden Sie in Tabelle 11.

Gerät	Kopplungsport	Steuerport
RS2-./.	Port 1	Stand-by-Port (ausschließlich mit RS2-../.. kombinierbar)
RS2-16M	Einstellbar für alle Ports (Lieferzustand: Port 1)	Einstellbar für alle Ports (Lieferzustand: Port 2)
RS20, RS30, RS40	Einstellbar für alle Ports (Lieferzustand: Port 1.4)	Einstellbar für alle Ports (Lieferzustand: Port 1.3)
OCTOPUS	Einstellbar für alle Ports (Lieferzustand: Port 1.4)	Einstellbar für alle Ports (Lieferzustand: Port 1.3)
MICE	Einstellbar für alle Ports (Lieferzustand: Port 1.4)	Einstellbar für alle Ports (Lieferzustand: Port 1.3)
PowerMICE	Einstellbar für alle Ports (Lieferzustand: Port 1.4)	Einstellbar für alle Ports (Lieferzustand: Port 1.3)
MS20	Einstellbar für alle Ports (Lieferzustand: Port 1.4)	Einstellbar für alle Ports (Lieferzustand: Port 1.3)
MS30	Einstellbar für alle Ports (Lieferzustand: Port 2.4)	Einstellbar für alle Ports (Lieferzustand: Port 2.3)
RSR20/RSR30	Einstellbar für alle Ports (Lieferzustand: Port 1.4)	Einstellbar für alle Ports (Lieferzustand: Port 1.3)
MACH 100	Einstellbar für alle Ports (Lieferzustand: Port 2.4)	Einstellbar für alle Ports (Lieferzustand: Port 2.3)
MACH 1000	Einstellbar für alle Ports (Lieferzustand: Port 1.4)	Einstellbar für alle Ports (Lieferzustand: Port 1.3)
MACH 3000	Einstellbar für alle Ports	Einstellbar für alle Ports
MACH 4000	Einstellbar für alle Ports (Lieferzustand: Port 1.4)	Einstellbar für alle Ports (Lieferzustand: Port 1.3)

Tab. 11: Portzuordnung für die redundante Kopplung (Zwei Switch-Kopplung mit Steuerleitung)

Anmerkung: Konfigurieren Sie den Kopplungsport und die Redundanz-Ring-Ports auf verschiedenen Ports.

☐ Schalten Sie im Rahmen „Funktion“ die Funktion an (siehe Abbildung 36).

☐ Schließen Sie nun die redundante Leitung und die Steuerleitung an.

Die Anzeigen im Rahmen „Port auswählen“ bedeuten:

– „Portmodus“: Der Port ist entweder aktiv oder im Stand-by-Modus.
– „Portstatus“: Der Port ist entweder aktiv, im Stand-by-Modus oder nicht verbunden.
– „IP-Adresse“: Die IP-Adresse des Partners, soweit dieser im Netz schon in Betrieb ist.

Die Anzeigen im Rahmen „Information“ bedeuten:

– „Redundanz gewährleistet“: Die Redundanz-Funktion ist aktiv.
  – Am Partner-Kopplungsport, an dem die Hauptleitung angeschlossen ist, leuchtet die Link-LED permanent.
  – Am Kopplungsport, an dem die redundante Leitung angeschlossen ist, blinkt die Link-LED gleichmäßig.

  Wenn die Hauptleitung nicht mehr funktioniert, übernimmt die redundante Strecke die Funktion der Hauptleitung.
– „Konfigurationsfehler“: Die Funktion ist unvollständig oder falsch konfiguriert.

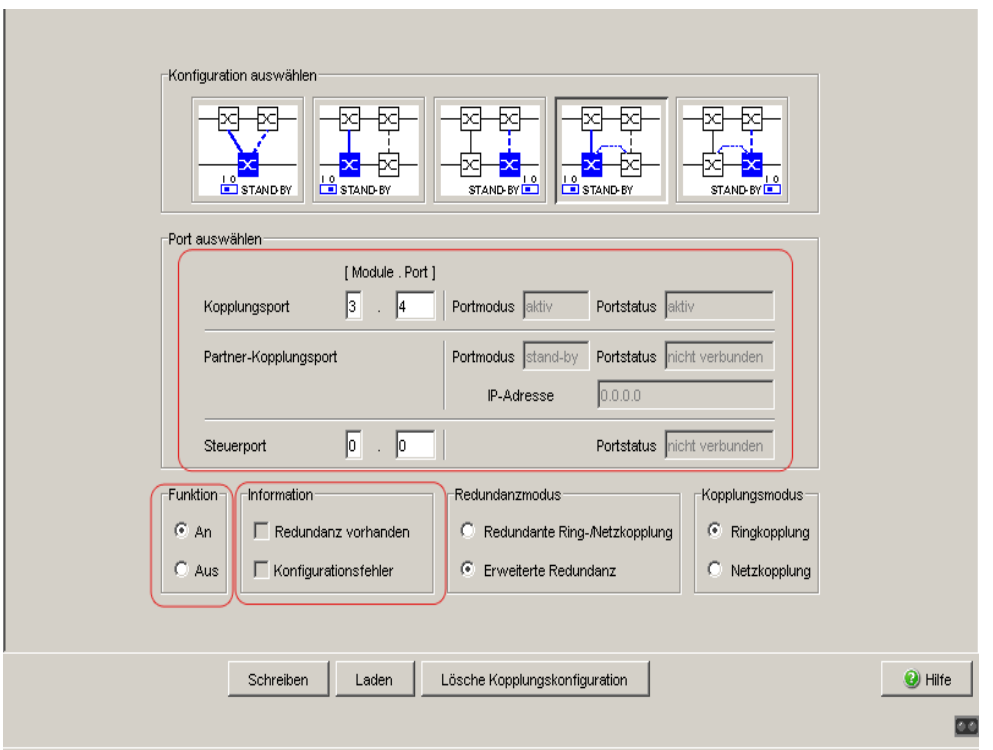


Abb. 36: Zwei-Switch-Kopplung mit Steuerleitung: Port auswählen und Funktion ein-/ausschalten

Um dauerhafte Schleifen (Loops) zu vermeiden, setzt der Switch den Portstatus des Kopplungsports auf „aus“, wenn Sie:
– die Funktion ausschalten oder
– die Konfiguration wechseln
während die Verbindungen an diesen Ports in Betrieb sind.

Anmerkung: Für die Kopplungsports sind folgende Einstellungen erforderlich (Wählen Sie hierzu den Dialog `Grundeinstellungen:Portkonfiguration`):
Siehe Tabelle 3 auf Seite 33.

Anmerkung: Wenn VLANs konfiguriert sind, stellen Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports wie folgt ein:
– im Dialog `Switching:VLAN:Port` Port-VLAN-ID 1 und „Ingress Filtering“ deaktiviert
– im Dialog `Switching:VLAN:Statisch` für sämtliche redundanten Verbindungen VLAN 1 und VLAN-Zugehörigkeit `T` (Tagged)
Das Gerät sendet die Redundanzpakete in VLAN 1 mit höchster Priorität.

☐ Wählen Sie die „Zwei-Switch-Kopplung mit Steuerleitung“ mit Hilfe des Dialog-Buttons mit der selben Grafik wie die untenstehende (siehe Abbildung 37).

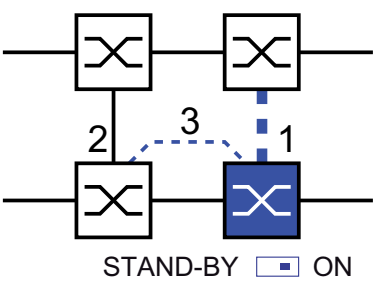


Abb. 37: Zwei-Switch-Kopplung mit Steuerleitung
1: Kopplungsport
2: Partner-Kopplungsport
3: Steuerleitung

Die folgenden Einstellungen betreffen den in der ausgewählten Grafik blau dargestellten Switch.

☐ Wählen Sie den Kopplungsport aus (siehe Abbildung 36).
Mit „Kopplungsport“ legen Sie fest, an welchen Port Sie die Verbindung der Netzsegmente anschließen.
Die Portzuordnung für die redundante Kopplung finden Sie in Tabelle 11.

☐ Bei einem Gerät mit DIP-Schaltern schalten Sie den STAND-BY-Schalter auf ON oder deaktivieren Sie die DIP-Schalter. Schließen Sie die redundante Leitung am Kopplungsport an.
☐ Wählen Sie den Steuerport aus (siehe Abbildung 36).
Mit „Steuerport" legen Sie fest, an welchen Port Sie die Steuerleitung anschließen.

Anmerkung: Konfigurieren Sie den Kopplungsport und die Redundanz-Ring-Ports auf verschiedenen Ports.

☐ Schalten Sie im Rahmen „Funktion“ die Funktion an (siehe Abbildung 36).
☐ Schließen Sie nun die redundante Leitung und die Steuerleitung an.

Die Anzeigen im Rahmen „Port auswählen“ bedeuten:
– „Portmodus“: Der Port ist entweder aktiv oder im Stand-by-Modus.
– „Portstatus“: Der Port ist entweder aktiv, im Stand-by-Modus oder nicht verbunden.
– „IP-Adresse“: Die IP-Adresse des Partners, soweit dieser im Netz schon in Betrieb ist.

Die Anzeigen im Rahmen „Information“ bedeuten:
– „Redundanz gewährleistet“: Die Redundanz-Funktion ist aktiv.
  – Am Partner-Kopplungsport, an dem die Hauptleitung angeschlossen ist, leuchtet die Link-LED permanent.
  – Am Kopplungsport, an dem die redundante Leitung angeschlossen ist, blinkt die Link-LED gleichmäßig.

  Wenn die Hauptleitung nicht mehr funktioniert, übernimmt die redundante Strecke die Funktion der Hauptleitung.
– „Konfigurationsfehler“: Die Funktion ist unvollständig oder falsch konfiguriert.

Um dauerhafte Schleifen (Loops) zu vermeiden, setzt der Switch den Portstatus des Kopplungsports auf „aus“, wenn Sie:
– die Funktion ausschalten oder
– die Konfiguration wechseln

während die Verbindungen an diesen Ports in Betrieb sind.

Anmerkung: Wenn VLANs konfiguriert sind, stellen Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports wie folgt ein:

– im Dialog `Switching:VLAN:Port` Port-VLAN-ID 1 und „Ingress Filtering“ deaktiviert
– im Dialog `Switching:VLAN:Statisch` für sämtliche redundanten Verbindungen VLAN 1 und VLAN-Zugehörigkeit `T` (Tagged)
Das Gerät sendet die Redundanzpakete in VLAN 1 mit höchster Priorität.

Redundanzmodus

☐ Wählen Sie im Rahmen „Redundanzmodus“:

– „Redundante Ring-/Netzkopplung“
oder
– „Erweiterte Redundanz“

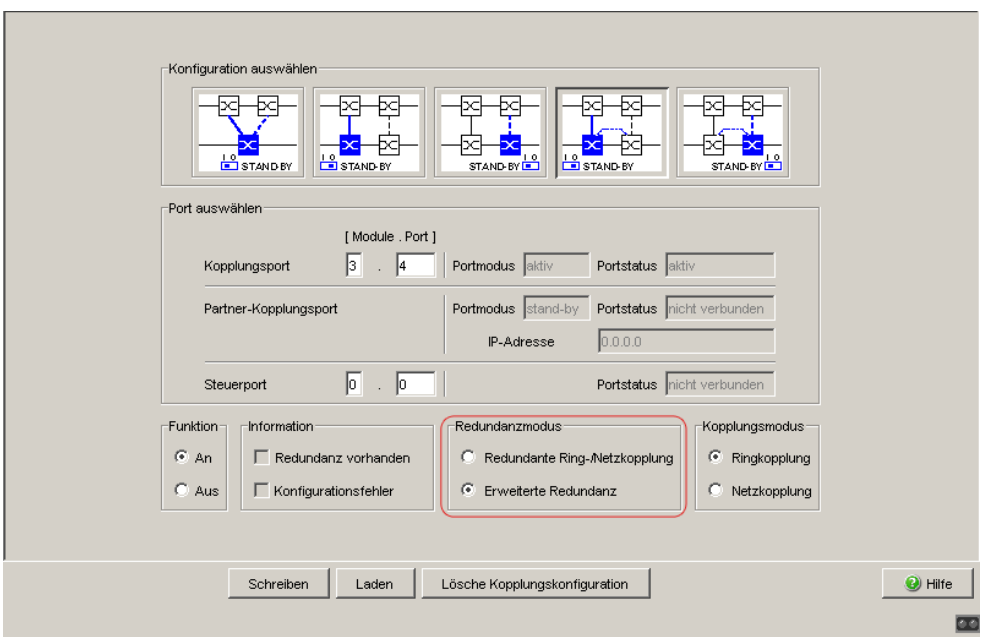


Abb. 38: Zwei-Switch-Kopplung mit Steuerleitung: Redundanzmodus auswählen

Bei der Einstellung „`Redundante Ring-/Netzkopplung`“ ist entweder die Hauptleitung oder die redundante Leitung aktiv. Niemals sind beide Leitungen gleichzeitig aktiv.

Bei der Einstellung „`Erweiterte Redundanz`“ sind Hauptleitung und redundante Leitung gleichzeitig aktiv, wenn die Verbindungsleitung zwischen den Geräten im angekoppelten (d.h, dem entfernten) Netz funktionsuntüchtig wird (siehe Abbildung 25).
Während der Rekonfigurationszeit kann es zu Paketdoppelungen kommen. Wählen Sie daher diese Einstellung ausschließlich dann, wenn Ihre Anwendung Paketdoppelungen erkennt.

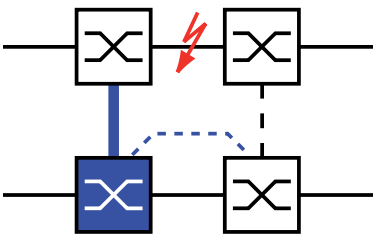


Abb. 39: Erweiterte Redundanz

Kopplungsmodus

Der Kopplungsmodus bezeichnet die Art des angekoppelten Netzes.

☐ Wählen Sie im Rahmen „Kopplungsmodus“:

– „Ringkopplung“
oder
– „Netzkopplung“

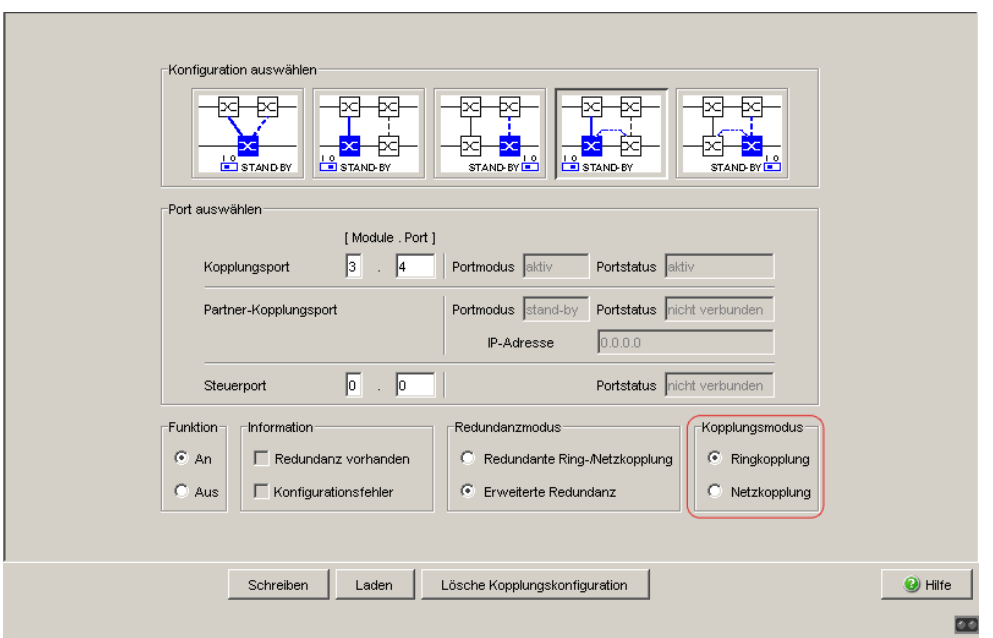


Abb. 40: Zwei-Switch-Kopplung mit Steuerleitung: Kopplungsmodus auswählen

- ☐ Wählen Sie **„Ringkopplung“**, wenn Sie an einen Redundanz-Ring ankoppeln.
- ☐ Wählen Sie **„Netzkopplung“**, wenn Sie an eine Linien- oder Baumstruktur ankoppeln.

Lösche Kopplungskonfiguration

- ☐ Die „Lösche Kopplungskonfiguration“-Bedientaste im Dialog bietet Ihnen die Möglichkeit, alle Kopplungs-Einstellungen des Gerätes in den Lieferzustand zurück zu versetzen.

6 Spanning Tree

Anmerkung: Das Spanning-Tree-Protokoll ist ein Protokoll für MAC-Bridges (Brücken). Daher verwendet die folgende Beschreibung den Begriff Bridge für Switch.

Lokale Netze werden immer größer. Dies gilt sowohl für die geografische Ausdehnung als auch für die Anzahl der Netzteilnehmer. Deshalb ist der Einsatz mehrerer Bridges vorteilhaft, z. B. um:

- die Netzlast in Teilbereichen zu verringern,
- redundante Verbindungen aufzubauen und
- Entfernungseinschränkungen zu überwinden.

Der Einsatz mehrerer Bridges mit mehrfachen, redundanten Verbindungen zwischen den Teilnetzen kann jedoch zu Schleifen/Loops und zum Verlust der Kommunikation durch das Netz führen. Als Hilfe, um dies zu verhindern, haben Sie die Möglichkeit, Spanning Tree einzusetzen. Spanning Tree erzielt Schleifenfreiheit durch das gezielte Deaktivieren von redundanten Verbindungen. Das gezielte Wieder-Aktivieren einzelner Verbindungen bei Bedarf ermöglicht die Redundanz.

RSTP ist eine Weiterentwicklung des Spanning-Tree-Protokolls (STP) und ist zu diesem kompatibel. Das STP benötigte bei Betriebsunfähigkeit einer Verbindung oder einer Bridge eine Rekonfigurationszeit von max. 30 s. Dies ist für zeitkritische Anwendungen nicht mehr akzeptabel. RSTP erreicht durchschnittliche Rekonfigurationszeiten von unter einer Sekunde. Wenn Sie RSTP in einer Ringtopologie mit 10 bis 20 Geräten einsetzen, können Sie auch Rekonfigurationszeiten im Millisekundenbereich erreichen.

Anmerkung: RSTP löst eine Layer 2-Netztopologie mit redundanten Pfaden in eine Baumstruktur (Spanning Tree) auf, die keine redundanten Pfade mehr enthält. Einer der Switches übernimmt dabei die Rolle der Root-Bridge. Die maximal erlaubte Anzahl der Geräte in einem aktiven Ast von der Root-Bridge bis zur Astspitze können Sie durch die Variable `Max Age` der aktuellen Root-Bridge vorgeben. Der voreingestellte Wert für `Max Age` ist 20, er kann bis auf 40 erhöht werden.
Wenn das als Root arbeitende Gerät ausfällt und ein anderes Gerät dessen Funktion übernimmt, bestimmt die neue Root-Bridge die größtmögliche erlaubte Anzahl der Geräte in einem Ast durch ihre `Max Age`-Einstellung.

Anmerkung: Der RSTP-Standard schreibt vor, dass alle Geräte innerhalb eines Netzes mit dem (Rapid-) Spanning-Tree-Algorithmus arbeiten. Bei gleichzeitigem Einsatz von STP und RSTP gehen in den Netz-Segmenten, die gemischt betrieben werden, die Vorteile der schnelleren Rekonfiguration bei RSTP verloren.
Ein Gerät, das lediglich RSTP unterstützt, arbeitet mit MSTP-Geräten zusammen, indem es sich keiner MST-Region, sondern dem CST (Common Spanning Tree) zuordnet.

Anmerkung: Das Standardisierungskomitee hat bei einer Änderung des RSTP-Standards IEEE 802.1D-2004 den maximalen Wert für „Hello Time“ von 10 auf 2 reduziert. Wenn Sie die Switch-Software von einer Release vor 5.0 auf eine Release 5.0 oder höher aktualisieren, reduziert die neue Software-Release automatisch lokal eingetragene „Hello Time“-Werte, die größer als 2 s sind, auf 2 s.
Ist das Gerät nicht RSTP-Root, so können abhängig von der Software-Release des Root-Gerätes weiterhin „Hello Time“ Werte > 2 s gültig sein.

6.1 Das Spanning Tree Protokoll

Da RSTP eine Weiterentwicklung des STP ist, gelten alle folgenden Beschreibungen des STP auch für das RSTP.

6.1.1 Die Aufgaben des STP

Der Spanning Tree-Algorithmus reduziert Netztopologien, die mit Bridges aufgebaut sind und Ringstrukturen durch redundante Verbindungen aufweisen, auf eine Baumstruktur. Dabei trennt STP die Ringstrukturen nach vorgegebenen Regeln auf, indem es redundante Pfade deaktiviert. Wird ein Pfad unterbrochen, weil eine Netzkomponente betriebsunfähig wird, aktiviert das STP den zuvor deaktivierten Pfad wieder. Dies erlaubt redundante Verbindungen zur Erhöhung der Kommunikationsverfügbarkeit.
Das STP ermittelt bei der Bildung der Baumstruktur eine Bridge, die die Basis der STP-Baumstruktur repräsentiert. Diese Bridge heißt Root-Bridge.

Merkmale des STP-Algorithmus:

- automatische Rekonfiguration der Baumstruktur bei Bridge-Ausfällen oder Unterbrechung eines Datenpfades,
- Stabilisierung der Baumstruktur bis zur maximalen Netzausdehnung (bis zu 39 Hops, abhängig von der Einstellung für `Max Age`, (siehe Tabelle 14)
- Stabilisierung der Topologie innerhalb einer vorhersehbaren Zeit,
- durch den Administrator vorbestimmbare und reproduzierbare Topologie,
- Transparenz für die Endgeräte,
- geringe Netzlast gegenüber der verfügbaren Übertragungskapazität durch Einrichtung der Baumstruktur.

6.1.2 Die Bridge-Parameter

Jede Bridge und ihre Verbindungen werden im Kontext von Spanning Tree eindeutig durch die folgenden Parameter beschrieben:

- Bridge-Identifikation (Bridge-Identifier),
- Root-Pfadkosten der Bridge-Ports,
- Port-Identifikation (Port-Identifier).

6.1.3 Bridge-Identifikation (Bridge-Identifier)

Die Bridge-Identifikation besteht aus 8 Bytes. Die 2 höchstwertigen Bytes sind die Priorität. Die Voreinstellung für die Prioritätszahl ist 32.768 (8000H), jedoch kann der Management-Administrator diese zur Konfiguration des Netzes verändern. Die 6 niederwertigen Bytes der Bridge-Identifikation sind die MAC-Adresse der Bridge. Die MAC-Adresse ermöglicht, dass alle Bridges eine eindeutige Bridge-Identifikation besitzen.
Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation besitzt die höchste Priorität.

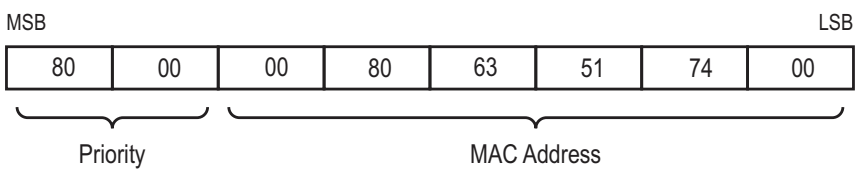


Abb. 41: Bridge-Identifikation, Beispiel (Werte in Hexadezimalschreibweise)

6.1.4 Root-Pfadkosten

Jedem Pfad, der 2 Bridges miteinander verbindet, ordnen die Bridges Kosten für die Übertragung (Pfadkosten) zu. Die Bridge bestimmt diesen Wert in Abhängigkeit von der Datenrate (siehe Tabelle 12). Dabei ordnet sie Pfaden mit niedrigerer Datenrate die höheren Pfadkosten zu.

Alternativ dazu kann auch der Administrator die Pfadkosten festlegen. Dabei ordnet er - wie die Bridge - Pfaden mit niedrigerer Datenrate die höheren Pfadkosten zu. Da er aber diesen Wert letztendlich frei wählen kann, verfügt er hiermit über ein Werkzeug, bei redundanten Pfaden einem bestimmten Pfad den Vorzug zu geben.

Die Root-Pfadkosten sind die Summe aller Einzelpfadkosten der Pfade, die ein Datenpaket zwischen dem angeschlossenen Port einer Bridge und der Root-Bridge passiert.

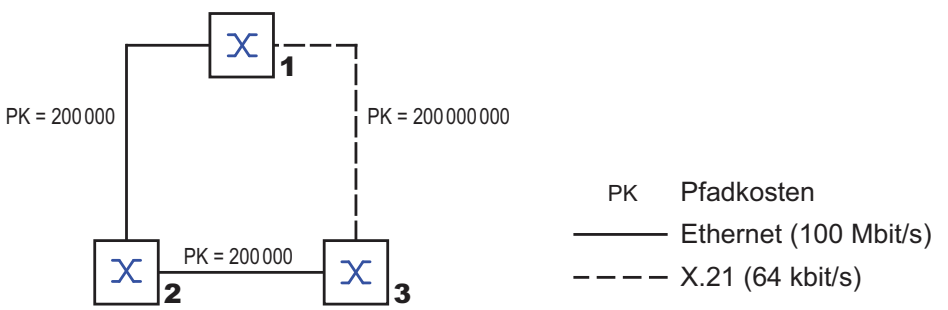


Abb. 42: Pfadkosten

Datenrate	Empfohlener Wert	Empfohlener Bereich	Möglicher Bereich
≤100 Kbit/s	200.000.000[a]	20.000.000-200.000.000	1-200.000.000
1 Mbit/s	20.000.000[a]	2.000.000-200.000.000	1-200.000.000
10 Mbit/s	2.000.000[a]	200.000-20.000.000	1-200.000.000
100 Mbit/s	200.000[a]	20.000-2.000.000	1-200.000.000
1 Gbit/s	20.000	2.000-200.000	1-200.000.000
10 Gbit/s	2.000	200-20.000	1-200.000.000
100 Gbit/s	200	20-2.000	1-200.000.000

Tab. 12: Empfohlene Pfadkosten beim RSTP in Abhängigkeit von der Datenrate.

Datenrate	Empfohlener Wert	Empfohlener Bereich	Möglicher Bereich
1 Tbit/s	20	2-200	1-200.000.000
10 Tbit/s	2	1-20	1-200.000.000

Tab. 12: Empfohlene Pfadkosten beim RSTP in Abhängigkeit von der Datenrate.

a. Bridges, die zu IEEE 802.1D-1998 konform sind, und ausschließlich 16 Bit-Werte für Pfadkosten unterstützen, sollten als Pfadkosten den Wert 65.535 (FFFFH) verwenden, wenn Sie sie zusammen mit Bridges benutzen, die 32 Bit-Werte für die Pfadkosten unterstützen.

Anmerkung: Sind mit Link-Aggregation (siehe auf Seite 19 „Link-Aggregation“) Verbindungsleitungen zwischen Geräten zu einem Trunk zusammengefasst, so reduzieren sich die automatisch bestimmten Pfadkosten auf die Hälfte.

6.1.5 Portidentifikation

Die Portidentifikation besteht aus 2 Bytes. Ein Teil, das niederwertigste Byte, enthält die physikalischen Portnummer. Dies gewährleistet eine eindeutige Bezeichnung des Port dieser Bridge. Der zweite, höherwertige Teil ist die Port-Priorität, die der Administrator festlegt (Voreinstellung: 128). Auch hier gilt: Der Port mit dem kleinsten Zahlenwert für die Portidentifikation besitzt die höchste Priorität.

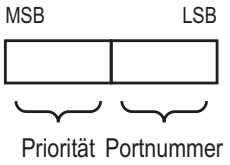


Abb. 43: Portidentifikation

6.2 Regeln für die Erstellung der Baumstruktur

6.2.1 Bridge-Information

Zur Berechnung der Baumstruktur benötigen die Bridges nähere Informationen über die anderen Bridges, die sich im Netz befinden.
Um diese Informationen zu erhalten, sendet jede Bridge eine BPDU (Bridge Protocol Data Unit) an andere Bridges.

Bestandteil einer BPDU ist unter anderem die

- Bridge-Identifikation,
- Root-Pfadkosten und
- Port-Identifikation.

(siehe IEEE 802.1D).

6.2.2 Aufbauen der Baumstruktur

- Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation nennt man auch Root-Bridge. Sie bildet die Root (Wurzel) der Baumstruktur
- Der Aufbau des Baumes hängt von den Root-Pfadkosten ab. Spanning Tree wählt die Struktur so, dass die minimalen Pfadkosten zwischen jeder einzelnen Bridge zur Root-Bridge entstehen.

- Bei mehreren Pfaden mit gleichen Root-Pfadkosten entscheidet die von der Root weiter entfernte Bridge, welchen Port sie blockiert. Sie verwendet dazu die Bridge-Identifikationen der näher an der Root liegenden Bridges. Die Bridge blockiert den Port, der zu der Bridge mit der numerisch höheren ID führt (eine numerisch höhere ID ist die logisch schlechtere). Haben 2 Bridges die gleiche Priorität, hat die Bridge mit der numerisch größeren MAC-Adresse die numerisch höhere ID, dies ist die logisch schlechtere.
- Wenn von einer Bridge mehrere Pfade mit den gleichen Root-Pfadkosten zu der selben Bridge führen, zieht die von der Root weiter entfernte Bridge als letztes Kriterium die Port-Identifikation der anderen Bridge heran (siehe Abbildung 43). Die Bridge blockiert dabei den Port, der zu dem Port mit der schlechteren ID führt. Haben 2 Ports die selbe Priorität, ist die ID mit der höheren Port-Nr. die schlechtere.

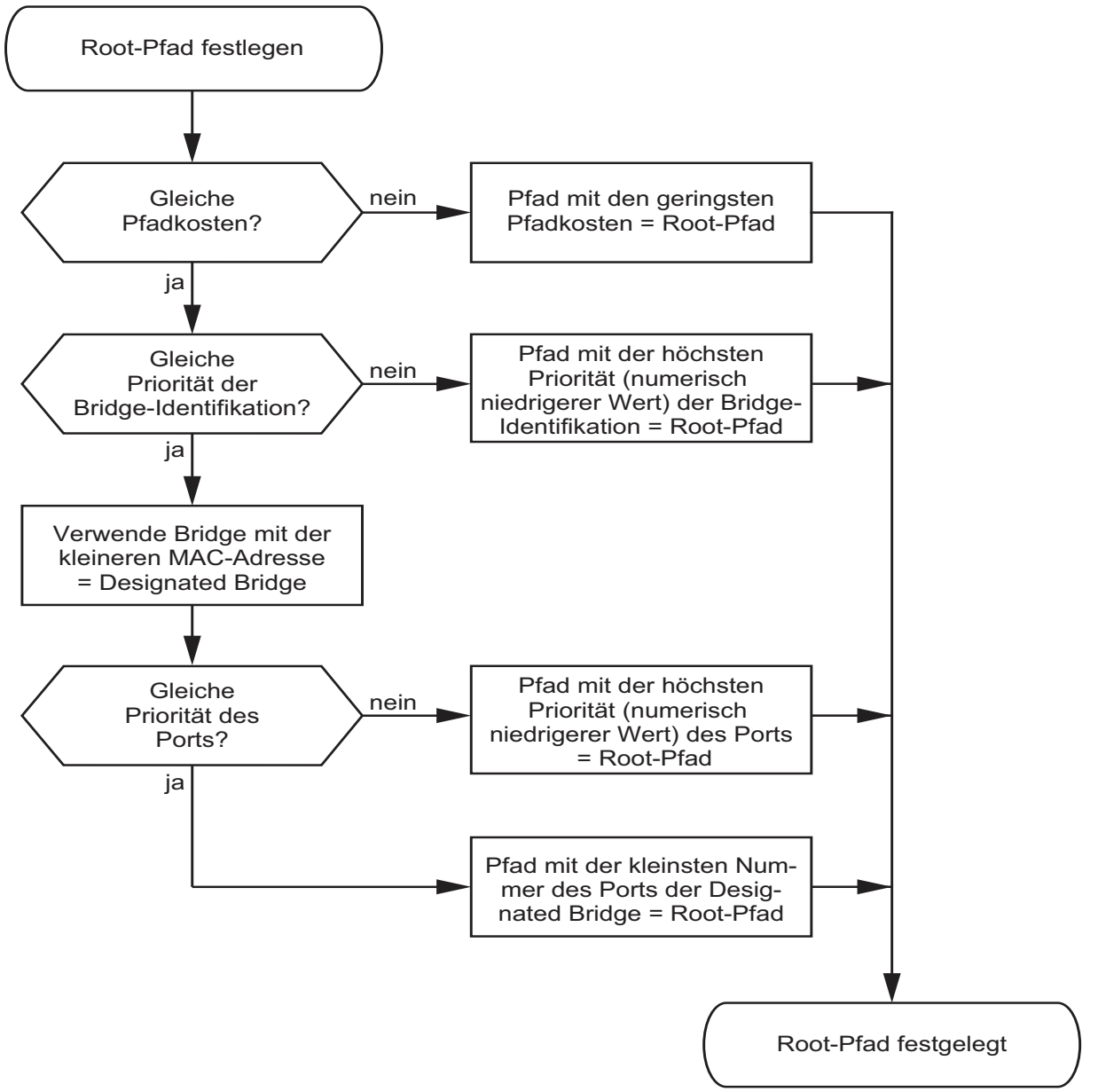


Abb. 44: Flussdiagramm Root-Pfad festlegen

6.3 Beispiel für die Bestimmung des Root-Pfads

Anhand des Netzplanes (siehe Abbildung 45) kann man das Flussdiagramm (siehe Abbildung 44) zur Festlegung des Root-Pfads nachvollziehen. Der Administrator hat für jede Bridge eine Priorität in der Bridge-Identifikation festgelegt. Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation übernimmt die Rolle der Root-Bridge, in diesem Fall die Bridge 1. Im Beispiel belasten alle Teilpfade die gleichen Pfadkosten. Das Protokoll blockiert den Pfad zwischen Bridge 2 und Bridge 3, da eine Verbindung von Bridge 3 über Bridge 2 zur Root-Bridge höhere Pfadkosten verursachen würde.

Interessant ist der Pfad von der Bridge 6 zur Root-Bridge:

- Der Pfad über Bridge 5 und Bridge 3 verursacht die gleichen Root-Pfadkosten wie der Pfad über Bridge 4 und Bridge 2.
- Die Bridges wählen den Pfad über Bridge 5, da der Zahlenwert 28.672 für ihre Priorität in der Bridge-Identifikation kleiner ist als der Zahlenwert 32.768.
- Zwischen Bridge 6 und Bridge 4 gibt es ebenfalls 2 Pfade.
  Hier entscheidet die Portidentifikation (Port 1 < Port 3).

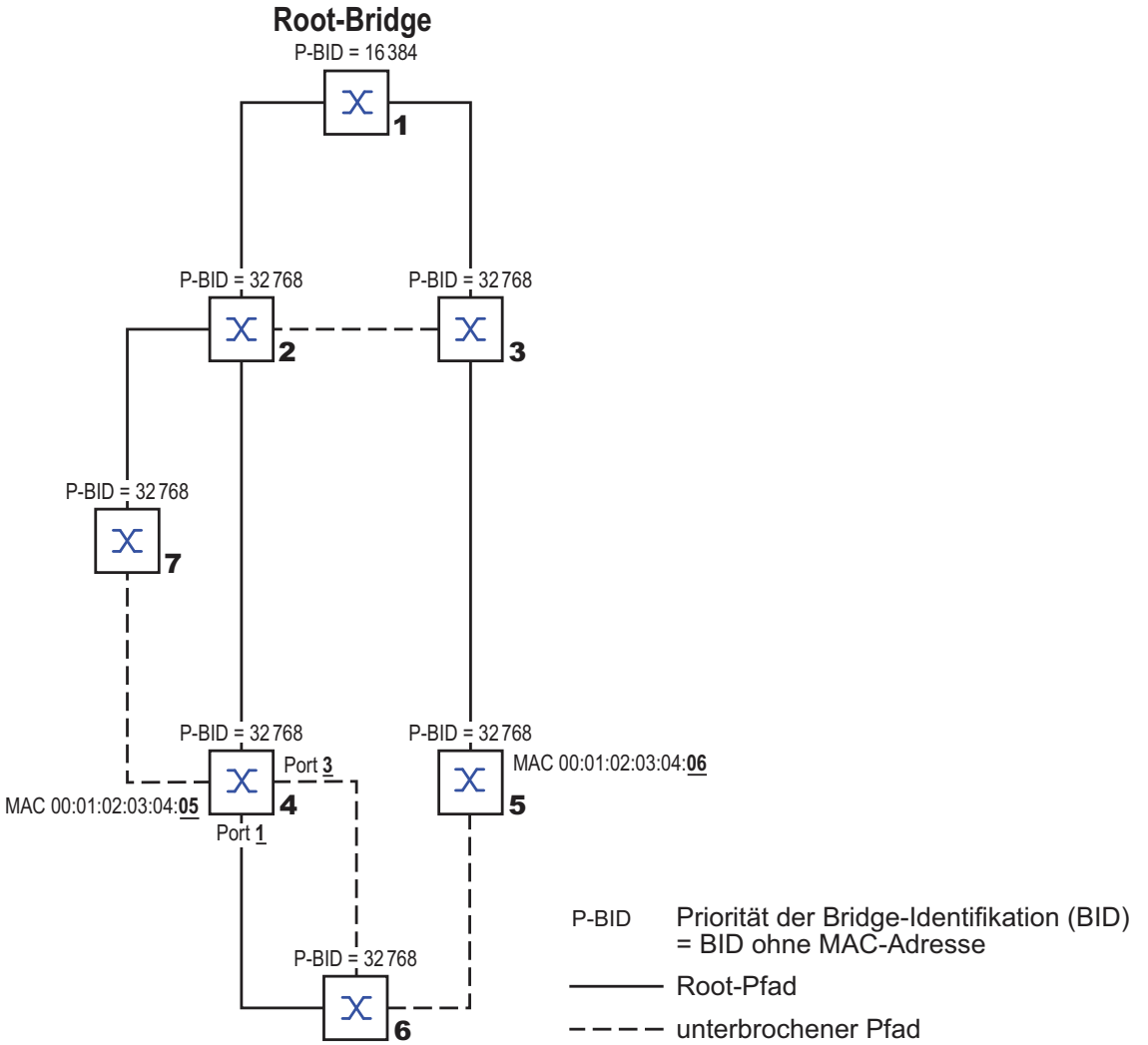


Abb. 45: Beispiel für die Bestimmung des Root-Pfads

6.4 Beispiel für die Manipulation des Root-Pfads

Anhand des Netzplanes (siehe Abbildung 45) kann man das Flussdiagramm (siehe Abbildung 44) zur Festlegung des Root-Paths nachvollziehen. Der Administrator hat folgendes getan:

– Für jede Bridge außer Bridge 1 und Bridge 5 hat er den im Lieferzustand voreingestellten Wert von 32.768 (8000H) belassen und
– der Bridge 1 hat er den Wert 16.384 (4000H) zugewiesen und damit zur Root-Bridge bestimmt.

Das Protokoll blockiert den Pfad zwischen Bridge 2 und Bridge 3, da eine Verbindung von Bridge 3 über Bridge 2 zur Root-Bridge höhere Pfadkosten bedeutet.

Interessant ist der Pfad von der Bridge 6 zur Root-Bridge:

- Der Pfad über Bridge 5 und Bridge 3 verursacht die gleichen Root-Pfadkosten wie der Pfad über Bridge 4 und Bridge 2.
- STP wählt den Pfad über die Bridge, die in der Bridge-Identifikation die niedrigere MAC-Adresse hat (im Bild dargestellt Bridge 4).
- Zwischen Bridge 6 und Bridge 4 gibt es auch noch 2 Pfade. Hier entscheidet die Portidentifikation.

Anmerkung: Indem der Administrator für jede Bridge außer der Root-Bridge den im Lieferzustand voreingestellten Wert der Priorität in der Bridge-Identifikation belässt, bestimmt allein die MAC-Adresse in der Bridge-Identifikation, welche Bridge bei Ausfall der momentanen Root-Bridge die Rolle der neuen Root-Bridge übernimmt.

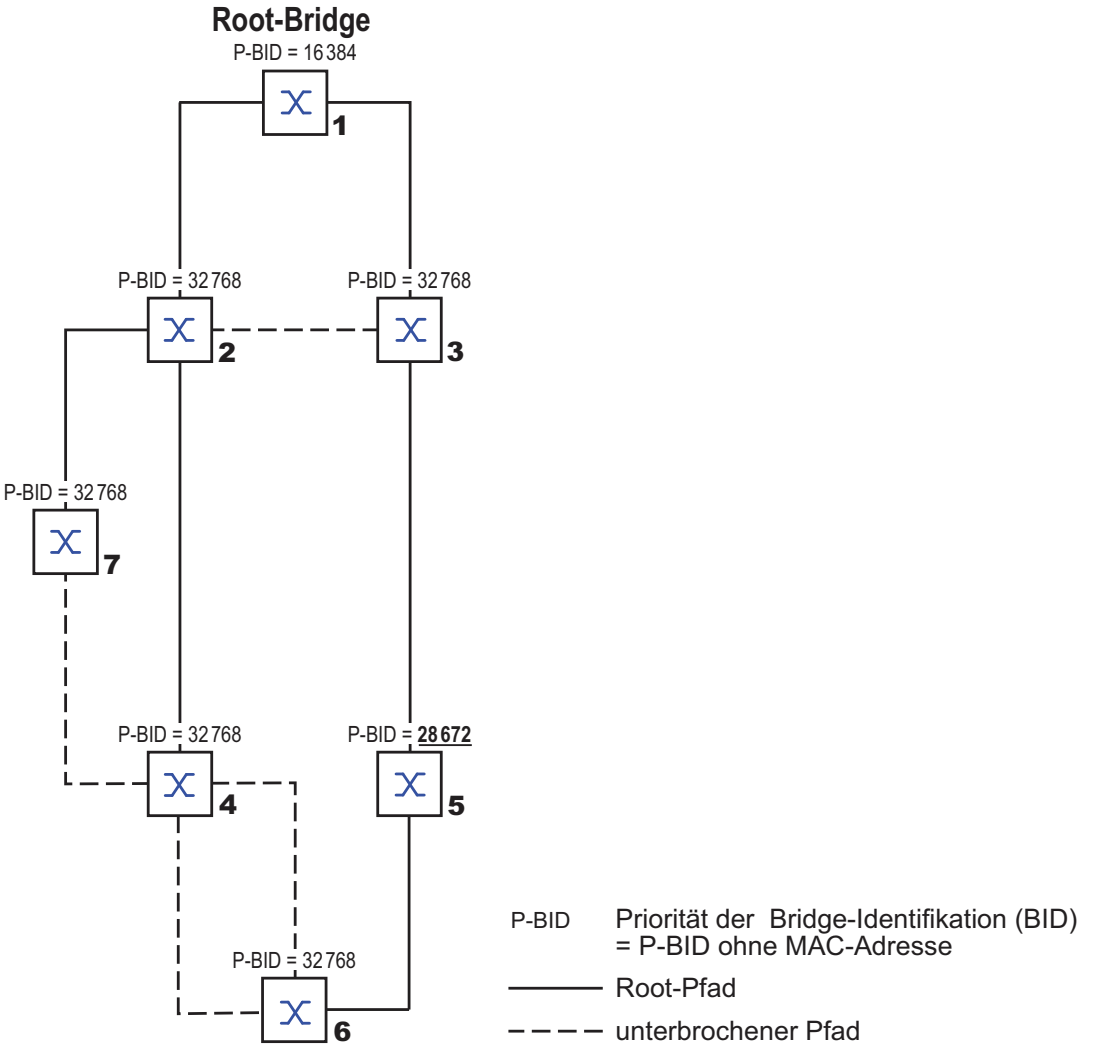


Abb. 46: Beispiel für die Manipulation des Root-Pfads

6.5 Beispiel für die Manipulation der Baumstruktur

Der Management-Administrator des Netzes stellt bald fest, dass diese Konfiguration mit Bridge 1 als Root-Bridge (siehe auf Seite 99 „Beispiel für die Bestimmung des Root-Pfads“) ungünstig ist. Auf den Pfaden zwischen Bridge 1 zu Bridge 2 und Bridge 1 zu Bridge 3 summieren sich die Kontrollpakete, die die Root-Bridge zu allen anderen Bridges sendet.
Konfiguriert der Management-Administrator die Bridge 2 als Root-Bridge, dann verteilt sich die Belastung der Teilnetze durch Kontrollpakete wesentlich besser. Hieraus entsteht die dargestellte Konfiguration (siehe Abbildung 47). Die Pfadkosten der meisten Bridges zur Root-Bridge sind kleiner geworden.

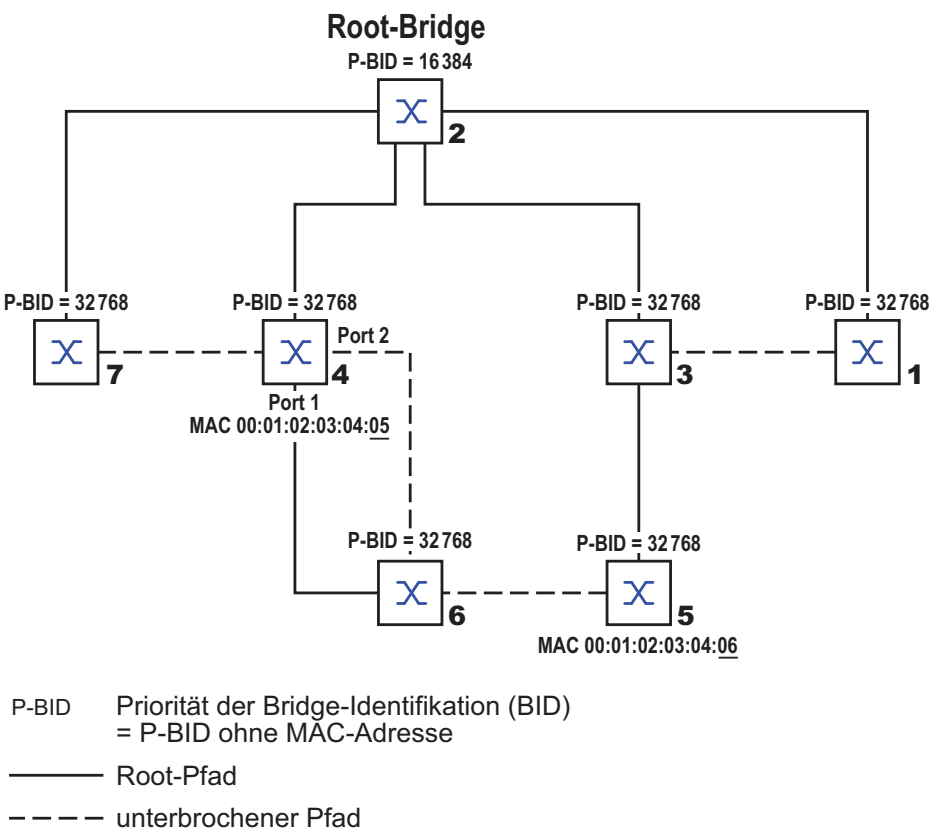


Abb. 47: Beispiel für die Manipulation der Baumstruktur

6.6 Das Rapid Spanning Tree Protokoll

Das RSTP behält die Berechnung der Baumstruktur vom STP unverändert bei. RSTP ändert lediglich Parameter und fügt neue Parameter und Mechanismen hinzu, die die Rekonfiguration beschleunigen, falls eine Verbindung oder eine Bridge ausfällt.
Eine zentrale Bedeutung erfahren in diesem Zusammenhang die Ports.

6.6.1 Port-Rollen

RSTP weist jedem Bridge-Port eine der folgenden Rollen zu (siehe Abbildung 48):

- Root-Port:
  Dies ist der Port, an dem eine Bridge Datenpakete mit den niedrigsten Pfadkosten von der Root-Bridge empfängt.
  Existieren mehrere Ports mit gleich niedrigen Pfadkosten, dann entscheidet die Bridge-Identifikation der zur Root führenden Bridge (Designated Bridge), welchem ihrer Ports die weiter von der Root entfernte Bridge die Rolle des Root-Ports gibt.
  Hat eine Bridge mehrere Ports mit gleich niedrigen Pfadkosten zur selben Bridge, entscheidet die Bridge anhand der Portidentifikation der zur Root führenden Bridge (Designated Bridge), welchen Port sie lokal als Root-Port wählt (siehe Abbildung 44).
  Die Root-Bridge selbst besitzt keinen Root-Port.
- Designierter Port (Designated-Port):
  Die Bridge in einem Netzsegment, die die niedrigsten Root-Pfadkosten hat, ist die designierte Bridge (Designated Bridge).
  Haben mehrere Bridges die gleichen Root-Pfadkosten, übernimmt die Bridge mit der zahlenmäßig kleinsten Bridge-Identifikation die Rolle der

designierten Bridge. Der designierte Port an dieser Bridge ist der Port, der ein von der Root-Bridge wegführendes Netzsegment verbindet. Ist eine Bridge mit mehr als einem Port mit einem Netzsegment verbunden (z. B. über einen Hub), gibt sie ihrem Port mit der besseren Port-Identifikation die Rolle des Designated Ports.

- Edge-Port[1]:
  Jedes Netzsegment, in dem sich keine weitere RSTP-Bridge befindet, ist mit genau einem designierten Port verbunden. Dieser designierte Port ist dann gleichzeitig ein Edge-Port, wenn er keine BPDUs (Spanning Tree Bridge Protocol Data Units) empfangen hat.
- Alternativer Port (Alternate-Port):
  Dies ist ein blockierter Port, der beim Ausfall der Verbindung zur Root-Bridge die Aufgabe des Root-Ports übernimmt. Der alternative Port stellt die Verbindung der Bridge zur Root-Bridge hin sicher.
- Ersatzport (Backup-Port):
  Dies ist ein blockierter Port, der als Ersatz zur Verfügung steht, falls die Verbindung zum designierten Port dieses Netzsegmentes (ohne RSTP-Bridges, z. B. ein Hub) ausfällt.
- Deaktivierter Port (Disabled-Port):
  Dies ist ein Port, der innerhalb des Spanning-Tree-Protokolls keine Rolle spielt, also abgeschaltet ist oder keine Verbindung hat.

1. Ein Edge-Port ist ein Endgeräte-Port am „Rand“ (engl. „Edge“) eines geswitchten Netzes.

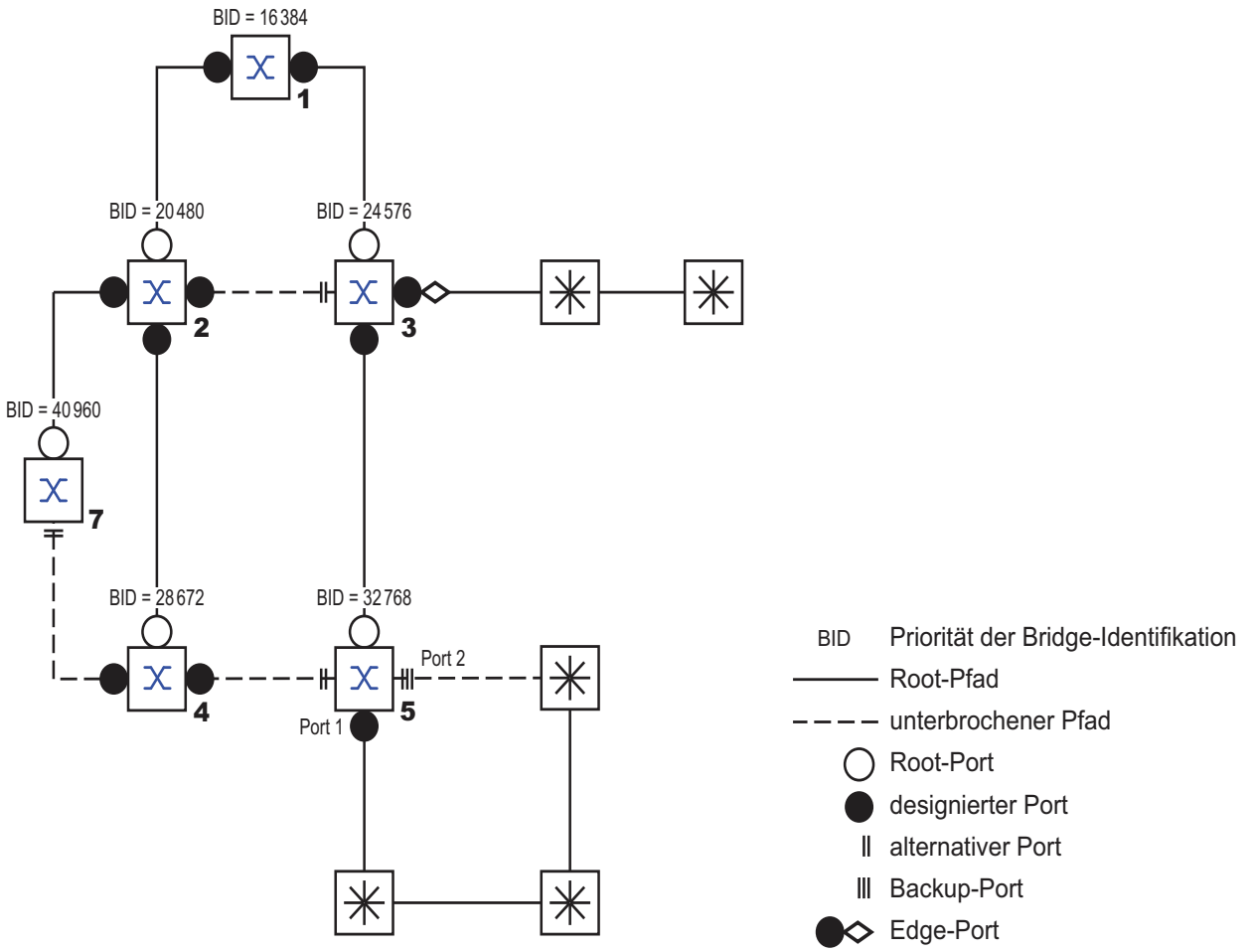


Abb. 48: Port-Rollen-Zuordnung

6.6.2 Port-Stati

In Abhängigkeit von der Baumstruktur und dem Status der ausgewählten Verbindungswege weist RSTP den Ports ihren Status zu.

STP Port Status	Administrative Bridge Port-Status	MAC Operational	RSTP Port-Status	Aktive Topology (Port Rolle)
DISABLED	Disabled	FALSE	Discarding[a]	Excluded (Disabled)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (Disabled)
BLOCKING	Enabled	TRUE	Discarding[b]	Excluded (Alternate, Backup)
LISTENING	Enabled	TRUE	Discarding[b]	Included (Root, Designated)
LEARNING	Enabled	TRUE	Learning	Included (Root, Designated)
FORWARDING	Enabled	TRUE	Forwarding	Included (Root, Designated)

Tab. 13: Beziehung zwischen Port-Status-Werten bei STP und RSTP

a. Die dot1d-MIB zeigt „Disabled“ an
b. Die dot1d-MIB zeigt „Blocked“ an

Bedeutung der RSTP-Port-Stati:

- Disabled: Port gehört nicht zur aktiven Topologie
- Discarding: kein Addess Learning in FDB, kein Datenverkehr außer STP-BPDUs
- Learning: Address Learning aktiv (FDB), kein Datenverkehr außer STP-BPDUs
- Forwarding: Address Learning aktiv (FDB), Senden und Empfangen aller Frame-Typen (nicht ausschließlich STP-BPDUs)

6.6.3 Spanning Tree Priority Vector

Um den Ports Rollen zuzuteilen, tauschen die RSTP-Bridges Konfigurationsinformationen untereinander aus. Diese Informationen heißen "Spanning Tree Priority Vector". Sie sind Teil der RST BPDUs und enthalten folgende Informationen:

- Bridge-Identifikation der Root-Bridge
- Root-Pfadkosten der sendenden Bridge
- Bridge-Identifikation der sendenden Bridge
- Portidentifikation des Ports, durch den die Nachricht gesendet wurde
- Portidentifikation des Ports, durch den die Nachricht empfangen wurde

Auf Basis dieser Informationen sind die am RSTP beteiligten Bridges in der Lage, selbständig Port-Rollen zu bestimmen und den Port-Status ihrer lokalen Ports zu definieren.

6.6.4 Schnelle Rekonfiguration

Warum kann RSTP schneller als STP auf eine Unterbrechung des Root-Pfades reagieren?

- Einführung von Edge-Ports:
  Bei einer Rekonfiguration setzt RSTP einen Edge-Port nach Ablauf von 3 Sekunden (Voreinstellung) in den Vermittlungsmodus und wartet dann "Hello Time" (siehe Tabelle 14) ab, um sich zu vergewissern, dass keine BPDU-sendende Bridge angeschlossen ist.
  Wenn der Anwender sicherstellt, dass an diesem Port ein Endgerät angeschlossen ist und bleibt, dann kann er an diesem Port RSTP ausschalten. Dann entstehen im Rekonfigurationsfall an diesem Port keine Wartezeiten
- Einführung von alternativen Ports:
  Da schon im regulären Betrieb die Portrollen verteilt sind, kann eine Bridge sofort nach dem Verlust der Verbindung zur Root-Bridge vom Root-Port zu einem alternativen Port umschalten.

- Kommunikation mit Nachbar-Bridges (Punkt-zu-Punkt-Verbindungen):
  Die dezentrale, direkte Kommunikation zwischen benachbarten Bridges erlaubt ohne Wartezeiten eine Reaktion auf Zustandsänderungen der Spanning-Tree-Topologie.
- Adresstabelle:
  Beim STP bestimmt das Alter der Einträge in der FDB über die Aktualisierung der Kommunikation. Das RSTP löscht sofort und gezielt die Einträge der Ports, die von einer Umkonfiguration betroffen sind.
- Reaktion auf Ereignisse:
  Ohne Zeitvorgaben einhalten zu müssen, reagiert RSTP sofort auf Ereignisse wie Verbindungsunterbrechung, Verbindung vorhanden, u.a.

Anmerkung: Die Kehrseite dieser schnelle Rekonfiguration ist die Möglichkeit, dass Datenpakete während der Rekonfigurationsphase der RSTP-Topologie dupliziert und/oder mit vertauschter Reihenfolge beim Empfänger ankommen können. Wenn Sie dies in Ihrer Anwendung nicht akzeptieren können, dann benutzen Sie das langsamere Spanning Tree Protokoll oder wählen Sie eines der anderen in diesem Buch beschriebenen, schnelleren Redundanzverfahren.

6.6.5 Rapid Spanning Tree konfigurieren

☐ Bauen Sie das Netz nach Ihren Erfordernissen auf.

Anmerkung: Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration des RSTP abgeschlossen haben.
Sie vermeiden damit Schleifen während der Konfigurationsphase.

- ☐ Bei Geräten mit DIP-Schaltern stellen Sie diese auf „deaktiviert“ (beide auf ON), damit die Konfiguration per Software uneingeschränkt möglich ist.
- ☐ Wählen Sie den Dialog `Redundanz:Rapid Spanning Tree:Global`.
- ☐ Schalten Sie an jedem Gerät RSTP an

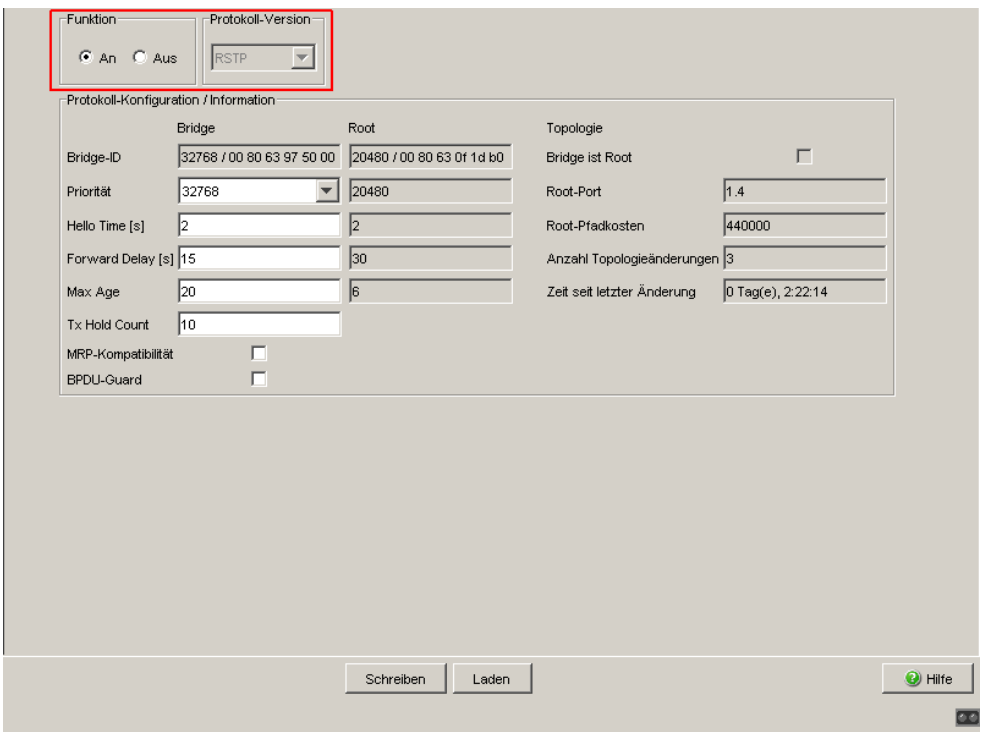


Abb. 49: Funktion ein-/ausschalten

- ☐ Bestimmen Sie den gewünschtem Switch zur Root-Bridge, indem Sie ihm im Rahmen „Protokoll-Konfiguration/-Information“ unter allen Switches im Netz die beste (numerisch niedrigste) Priorität in der Bridge-Identifikation zuweisen. Beachten Sie, dass Sie als Wert ausschließlich Vielfache von 4.096 (1000H) eingegeben können (siehe Tabelle 14).
  Im Rahmen „Root-Information“ zeigt der Dialog dann dieses Gerät als „Root“ an.
  Eine Root-Bridge hat keinen Root-Port und Root-Pfadkosten von 0.

☐ Ändern Sie bei Bedarf bei den anderen Bridges des Netzes in gleicher Weise den voreingestellten Prioritäts-Wert 32.768 in den von Ihnen gewünschten Wert (Vielfache von 4.096).
Überprüfen Sie bei jedem dieser Bridges die Anzeigen im Rahmen „Root-Information“:
– Root-ID: zeigt die Bridge-Identifikation der Root-Bridge an
– Root-Port: zeigt den Port an, der zur Root-Bridge führt
– Root-Kosten: zeigt die Root-Pfadkosten bis zur Root-Bridge an
im Rahmen „Protokoll-Konfiguration/-Information“:
– Priorität: zeigt die Priorität in der Bridge-Identifikation dieses Switches an
– MAC-Adresse: zeigt die MAC-Adresse dieses Switches an
– Topologie-Änderungen: zeigt die Anzahl der Änderungen seit dem Start von RSTP an
– Dauer seit letzter Änderung: zeigt die verstrichene Zeit seit der letzten Rekonfiguration des Netzes an

☐ Ändern Sie bei Bedarf die Werte für „Hello Time“, „Forward Delay“ und „Max. Age“ in der Root-Bridge. Die Root-Bridge überträgt diese Daten dann an die anderen Bridges weiter. Die von der Root-Bridge erhaltenen Daten zeigt der Dialog in der linken Spalte an. In der rechten Spalte geben Sie die Werte ein, die gelten sollen, wenn diese Bridge die Rolle der Root-Bridge übernimmt. Beachten Sie zum Konfigurieren Tabelle 14.

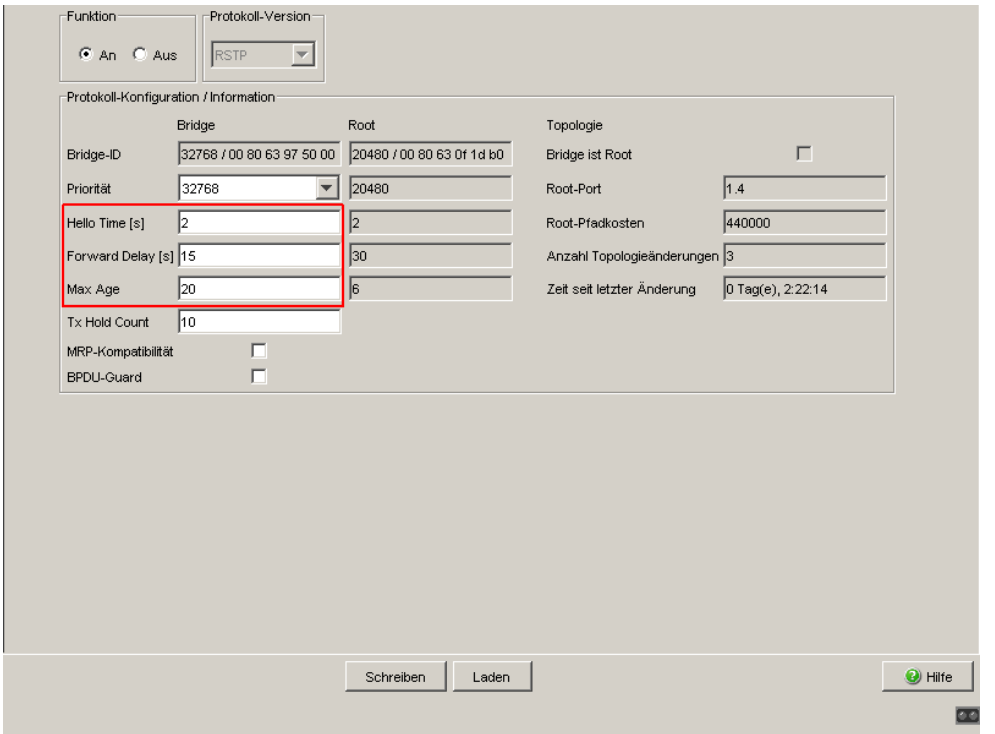


Abb. 50: Hello Time, Forward Delay und Max. Age zuweisen

Die Zeiteingaben im Dialog RSTP Global haben die Einheit 1 s. Beispiel: die Hello Time 2 entspricht 2 Sekunden.

☐ Schließen Sie nun die redundanten Strecken an.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Priorität	Priorität und MAC-Adresse zusammen bilden die Bridge-Identifikation.	0 < n*4.096 (1000H) < 61.440 (F000H)	32.768 (8000H)
Hello Time	Stellt die Hello-Time ein. Die lokale `Hello Time` gibt die Zeit zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Pakete) in Sekunden an. Hat das lokale Gerät die Root-Funktion, übernehmen die anderen Geräte im gesamten Netz diesen Wert. Ansonsten benutzt das lokale Gerät den Wert der Root-Bridge in der rechten Spalte „Root“.	1 - 2	2

Tab. 14: Globale RSTP-Einstellungen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Forward Delay	Stellt den Parameter Forward Delay ein. Beim Vorgängerprotokoll STP wurde der Parameter Forward Delay dazu verwendet, um den Zustandswechsel zwischen den Zuständen `disabled`, `discarding`, `learning`, `forwarding` zu verzögern. Seit der Einführung von RSTP hat dieser Parameter eine untergeordnete Bedeutung, weil die RSTP-Bridges den Zustandswechsel ohne vorgegebene Verzögerung aushandeln. Ist das lokale Gerät Root, übernehmen die anderen Geräte im gesamten Netz diesen Wert. Ansonsten benutzt das lokale Gerät den Wert der Root-Bridge in der rechten Spalte „Root“.	4 - 30 s Beachten Sie den Hinweis, der auf diese Tabelle folgt.	15 s
Max Age	Stellt den Parameter Max. Age ein. Beim Vorgängerprotokoll STP wurde der Parameter Max Age verwendet, um die Gültigkeit von STP-BPDUs in Sekunden anzugeben. Bei RSTP bedeutet Max Age die maximal zulässige Astlänge (Anzahl der Geräte bis zur Root-Bridge). Ist das lokale Gerät Root, übernehmen die anderen Geräte im gesamten Netz diesen Wert. Ansonsten benutzt das lokale Gerät den Wert der Root-Bridge in der rechten Spalte „Root“.	6 - 40 s Beachten Sie den Hinweis, der auf diese Tabelle folgt.	20 s

Tab. 14: Globale RSTP-Einstellungen

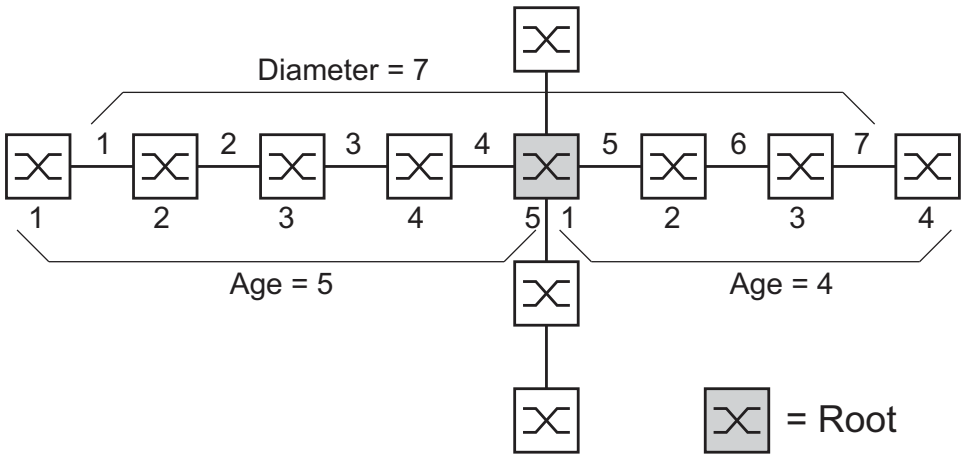


Abb. 51: Definition „Diameter“ und „Age“

Der Netz-Durchmesser (Diameter) ist die Anzahl der Verbindungen zwischen den beiden von der Root-Bridge entferntesten Geräten.

Anmerkung: Die Parameter
– Forward Delay und
– Max Age
stehen in Beziehung zueinander:

Forward Delay ≥ (Max Age/2) + 1

Wenn Sie Werte eingeben, die dieser Beziehung widersprechen, dann ersetzt das Gerät diese Werte durch eine Voreinstellung oder die zuletzt gültigen Werte.

☐ Ändern und kontrollieren Sie bei Bedarf Einstellungen und Anzeigen, die sich auf jeden einzelnen Port beziehen (Dialog: `Rapid Spanning Tree:Port`).

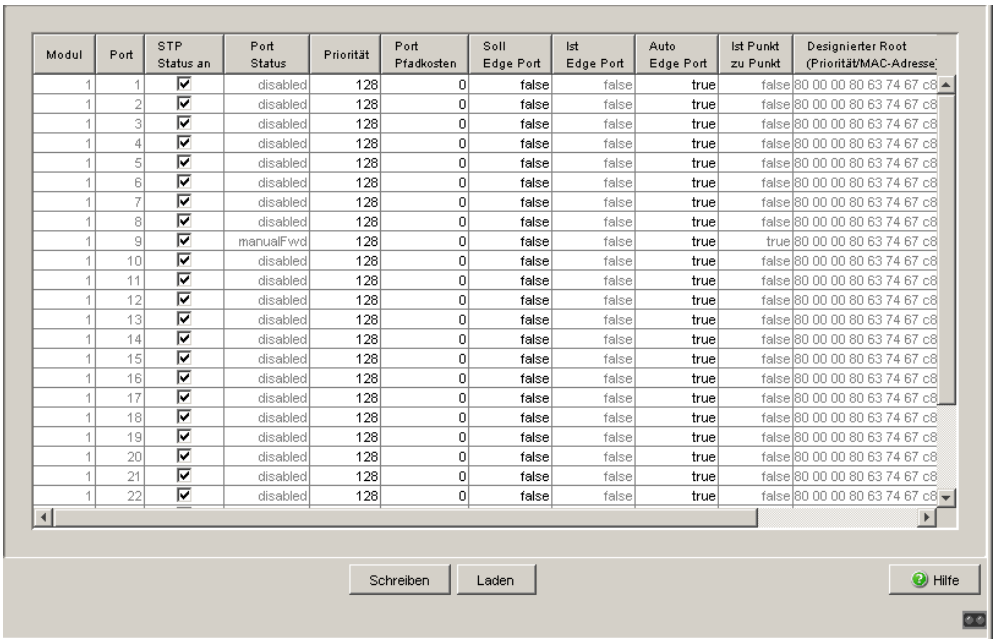


Abb. 52: RSTP pro Port konfigurieren

Anmerkung: Deaktivieren Sie das Spanning Tree Protokoll an den Ports, die an einen redundanten Ring angeschlossen sind, da Spanning Tree und Ring-Redundanz mit unterschiedlichen Reaktionszeiten arbeiten.

Wenn Sie das Gerät in einer Multiple Spanning Tree- (MSTP-) Umgebung einsetzen, nimmt das Gerät lediglich an der allgemeinen Spanning Tree-Instanz (Common Spanning Tree, CST) teil. Dieses Handbuchkapitel verwendet dafür auch den Begriff Globale MST-Instanz, um diesen allgemeinen Fall zu beschreiben.

Parameter	Bedeutung	Wertebereich	Voreinstellung
STP aktiv	Hier können Sie Spanning Tree für diesen Port ein- oder ausschalten. Ist Spanning Tree global eingeschaltet und an einem Port ausgeschaltet, sendet dieser Port keine STP-BPDUs und verwirft empfangene STP-BPDUs. **Anmerkung:** Möchten Sie parallel zu Spanning Tree andere Layer 2-Redundanzprotokolle wie HIPER-Ring oder Ring-/Netzkopplung einsetzen, achten Sie darauf, die Ports, die an diesen Protokollen beteiligt sind, in diesem Dialog für Spanning Tree auszuschalten. Andernfalls arbeitet die Redundanz möglicherweise nicht wie vorgesehen oder es kann zu Loops kommen.	`An`, `Aus`	`An`
Port-Status (read-only)	Zeigt den STP-Port-Status bezüglich der globalen MSTI (IST) an.	`discarding`, `learning`, `forwarding`, `disabled`, `manualForwarding`, `notParticipate`	-
Port-Priorität	Geben Sie hier die Port-Priorität (die vier obersten Bits der Port-Identifikation ein) bezüglich der globalen MSTI (IST) ein, als Dezimalzahl des obersten Bytes der Port-ID.	16 ≤ n·16 ≤ 240	128

Tab. 15: Port-bezogene RSTP-Einstellungen und -Anzeigen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Port-Pfadkosten	Eingabe der Pfadkosten bezüglich der globalen MSTI (IST) zur Bevorzugung redundanter Pfade. Beim Wert 0 ermittelt der Switch für die globale MSTI (IST) automatisch die Pfadkosten abhängig von der Übertragungsrate.	0 - 200.000.000	0 (automatisch)
Admin-Edge-Port	Aktivieren Sie diese Einstellung ausschließlich dann, wenn ein Endgerät an den Port angeschlossen ist (Administrativ: vorgegebene Einstellung) . Dann geht der Port nach Aufbau eines Links sofort in den Forwarding-Status, ohne zuerst die STP-Stati zu durchlaufen. Empfängt der Port trotzdem eine STP-BPDU, blockiert das Gerät den Port und klärt dessen STP-Port-Rolle. Der Port kann dabei in einem anderen Status übergehen, z.B. `forwarding`, `discarding`, `learning`. Deaktivieren Sie die Einstellung, wenn der Port an eine Bridge angeschlossen ist. Der Port durchläuft nach Aufbau eines Links dann zuerst die STP-Stati, bevor er ggf. in den Zustand `forwarding` geht. Diese Einstellung gilt für alle MSTIs.	`aktiv` (Kästchen markiert), `inaktiv` (Kästchen leer)	`inaktiv`
Oper-Edge-Port	Das Gerät setzt den Zustand „Oper-Edge-Port“ (Operational: in Betrieb) auf `true`, wenn es keine STP-BPDUs empfangen hat, also ein Endgerät angeschlossen ist. Es setzt den Zustand auf `false`, wenn es eine STP-BPDUs empfangen hat, also eine Bridge angeschlossen ist. Dieser Zustand gilt für alle MSTIs.	`true`, `false`	-

Tab. 15: Port-bezogene RSTP-Einstellungen und -Anzeigen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Auto-Edge-Port	Die Einstellung Auto-Edge-Port berücksichtigt das Gerät ausschließlich, wenn der Parameter Admin-Edge-Port deaktiviert ist. Ist Auto-Edge-Port aktiv, setzt das Gerät den Port nach dem Aufbau eines Links nach 1,5 · `Hello Time` (in der Voreinstellung 3 s) in den Zustand forwarding. Ist Auto-Edge-Port deaktiviert, wartet das Gerät statt dessen `Max Age` (in der Voreinstellung 20 s). Diese Einstellung gilt für alle MSTIs.	`aktiv` (Kästchen markiert), `inaktiv` (Kästchen leer)	`aktiv`
Ist Punkt-zu-Punkt	Das Gerät setzt den Zustand „Oper Punkt-zu-Punkt“ (Operational: in Betrieb) auf `true`, wenn dieser Port eine Vollduplex-Verbindung zu einem STP-Gerät hat. Ansonsten setzt es den Zustand auf `false` (z.B. wenn ein Hub angeschlossen ist). Die Punkt-zu-Punkt-Verbindung ist eine direkte Verbindung zwischen 2 RSTP-Geräten. Die direkte, dezentrale Kommunikation zwischen den beiden Bridges es bewirkt eine kurze Rekonfigurationszeit. Dieser Zustand gilt für alle MSTIs.	`true`, `false` Das Gerät bestimmt diesen Zustand aus dem Duplex-Modus: FDX: `true` HDX: `false`	
Empfangene Bridge-ID (read-only)	Zeigt die entfernte Bridge-ID an, von der dieser Port zuletzt eine STP-BPDU empfangen hat.[a]	Bridge-Identifikation (Format ppppp / mm mm mm mm mm mm)	-
Empfangene Pfadkosten (read-only)	Zeigt die Pfadkosten der entfernten Bridge an, die diese von ihrem Root-Port zur CIST-Root-Bridge hat.[a]	0-200.000.000	-
Empfangene Port-ID (read-only)	Zeigt die Port-ID auf der entfernten Bridge an, von der dieser Port zuletzt eine STP-BPDU empfangen hat.[a]	Port-Identifikation, Format pn nn, mit p: Port-Priorität / 16, nnn: Port-Nr., (beide hexadezimal)	-

Tab. 15: Port-bezogene RSTP-Einstellungen und -Anzeigen

– [a] Diese Spalten zeigen Ihnen Detail-Informationen, die über die bisher üblichen Details hinausgehen:
Für Designated-Ports zeigt das Gerät die Information der STP-BPDU an, die der Port zuletzt empfangene hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz.
Für die Port-Rollen Alternate-, Backup-, Master- und Root sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Designated-Informationen.
Hat ein Port keinen Link oder hat er noch keine STP-BDPU der aktuellen MSTI empfangen, zeigt das Gerät die Werte an, die der Port als Designated-Port senden würde.

6.7 Kombinieren von RSTP und MRP

Im MRP-Kompatibilitätsmodus bietet Ihnen das Gerät die Kombination von RSTP mit MRP.
In der Kombination RSTP und MRP bleiben die schnellen Umschaltzeiten von MRP erhalten.
Der maximal mögliche RSTP-Netz-Durchmesser (Diameter) (siehe Abbildung 51) ist abhängig von `Max Age`. Er gilt für die Geräte außerhalb des MRP-Rings.

Anmerkung: Die Kombination von RSTP und MRP setzt voraus, dass die Root-Bridge und die Ersatz-Root-Bridge beide im MRP-Ring liegen.

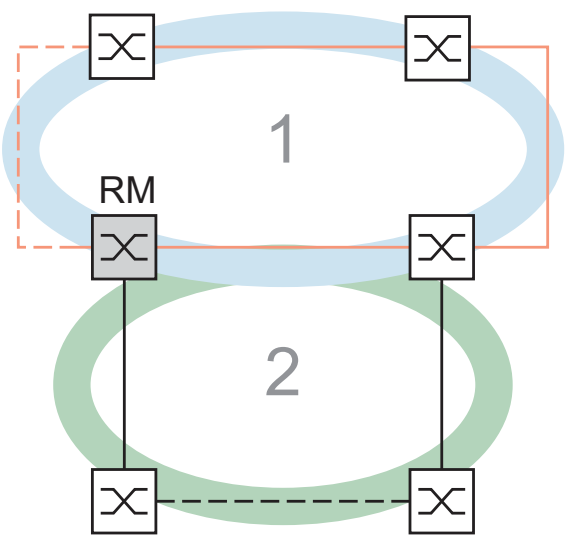


Abb. 53: Kombination von RSTP und MRP
1: MRP-Ring
2: RSTP-Ring
RM: Ring-Manager

Die Kombination von RSTP mit MRP umfasst der Reihe nach folgende Schritte:

- Konfigurieren Sie MRP auf allen Geräten im MRP-Ring.
- Schließen Sie die redundante Strecke im MRP-Ring.
- Aktivieren Sie RSTP an den RSTP-Ports und an den MRP-Ring-Ports.
- Konfigurieren Sie die RSTP-Root-Bridge und die RSTP-Ersatz-Root-Bridge im MRP-Ring :
  - Stellen sie deren Priorität ein.
  - Wenn Sie den durch den voreingestellten Wert von `Max Age` = 20 bedingten RSTP-Diameter überschreiten, passen Sie Max Age und Forward Delay entsprechend an.
- Schalten Sie RSTP global ein.
- Schalten Sie den MRP-Kompatibilitätsmodus ein.
- Nach der Konfiguration aller beteiligter Geräte schließen Sie die redundante RSTP-Verbindung an.

6.7.1 Anwendungsbeispiel für die Kombination von RSTP und MRP

Die Abbildung (siehe Abbildung 54) zeigt ein Beispiel für die Kombination von RSTP und MRP.

Parameter	S1	S2	S3	S4	S5	S6
MRP-Einstellungen						
Ring-Redundanz:MRP-Version	MRP	MRP			MRP	MRP
Ring-Port 1	1.1	1.1			1.1	1.1
Ring-Port 2	1.2	1.2			1.2	1.2
Port von MRP-Ring zum RSTP-Netz	1.3	1.3	-	-	-	-
Redundanzmanager-Modus	An	Aus	–	–	Aus	Aus
MRP-Funktion	An	An	Aus	Aus	An	An
RSTP-Einstellungen						
je RSTP-Port: STP-Status an	An	An	An	An	An	An
Protokoll-Konfiguration: Priorität (S2<S1<S3 und S2<S1<S4)	4.096	0	32.768	32.768	32.768	32.768
RSTP:Global: Funktion	An	An	An	An	An	An
RSTP:Global: MRP-Kompatibilität	An	An	–	–	An	An

Tab. 16: Werte für die Konfiguration der Switches des MRP/RSTP-Beispiels

Voraussetzungen für die weitere Konfiguration:

- Sie haben die MRP-Einstellungen der Geräte entsprechend der Tabelle oben konfiguriert.
- Die redundante Strecke im MRP-Ring ist geschlossen.

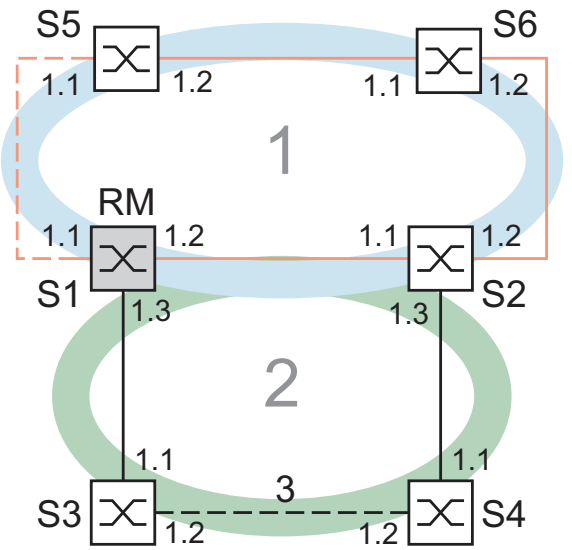


Abb. 54: Anwendungsbeispiel für die Kombination von RSTP und MRP
1: MRP-Ring, 2: RSTP-Ring, 3: redundante RSTP-Verbindung
RM: Ring-Manager
S2 ist RSTP-Root-Bridge
S1 ist RSTP-Ersatz-Root-Bridge

☐ Aktivieren Sie RSTP an den Ports, am Beipiel von S1 (siehe Tabelle 16).

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1/1.
`spanning-tree port mode`	RSTP am Port aktivieren.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
`spanning-tree port mode`	RSTP am Port aktivieren.

`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface 1/3.
`spanning-tree port mode`	RSTP am Port aktivieren.
`exit`	Wechsel in den Konfigurationsmodus.

☐ Konfigurieren Sie die globalen Einstellungen, am Beipiel von S1:
- die RSTP-Priorität
- die globale Funktion
- den MRP-Kompatibilitätsmodus

`spanning-tree mst priority 0 4096`	Die RSTP-Priorität für MST-Instanz 0 auf den Wert 4.096 einstellen. Die MST-Instanz 0 ist die Default-Instanz.
`spanning-tree`	RSTP-Funktion global einschalten.
`spanning-tree stp-mrp-mode`	MRP-Kompatibilität einschalten.

☐ Konfigurieren Sie die anderen Switches S2 - S6 mit ihren jeweiligen Werten (siehe Tabelle 16).

☐ Schließen Sie die redundante RSTP-Verbindung an.

7 VRRP/HiVRRP

Das Virtual Router Redundancy Protocol (VRRP) beschreibt ein Verfahren, das es ermöglicht, auf den Ausfall eines Routers zu reagieren.
VRRP findet seine Anwendung in Netzen mit Endgeräten, die lediglich einen Eintrag für das „Default Gateway“ unterstützen. Fällt das „Default Gateway“ aus, dann sorgt VRRP dafür, dass die Endgeräte ein redundantes Gateway finden.
Die Firma Hirschmann hat das VRRP weiterentwickelt zum Hirschmann Virtual Router Redundancy Protocol (HiVRRP). HiVRRP bietet bei entsprechender Konfiguration Umschaltzeiten von unter 400 ms.

Anmerkung: Detaillierte Informationen zu VRRP und HiVRRP finden Sie im Anwender-Handbuch „Routing-Konfiguration“.

7.1 VRRP/HiVRRP Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, generelle Einstellungen und Einstellungen pro Port für das VRRP vorzunehmen.
Sie können:
– bis zu 8 virtuelle Router pro Port und
– bis zu 16 Einträge mit HiVRRP pro Router
konfigurieren.

7.1.1 Generelle Einstellungen

- Funktion: Ein-/ausschalten der VRRP-Funktion.
- Version: Anzeige der VRRP Version.
- VRRP-Master-Trap senden: Sobald der Router die VRRP-Master-Funktion übernimmt sendet er einen Master-Trap.
- VRRP-Authentifizierungsfehler-Trap senden: Sobald der Router eine VRRP-Information mit falscher Authentifizierung empfängt sendet er einen VRRP-Authentifizierungsfehler-Trap.

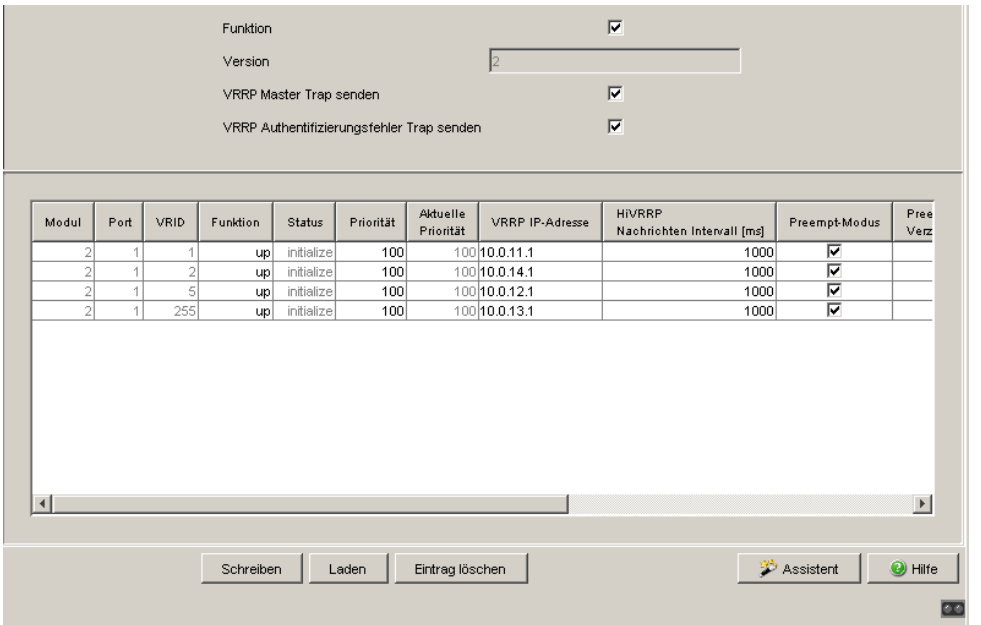


Abb. 55: Dialog VRRP/HiVRRP-Konfiguration

7.1.2 VRRP-Instanz-Einstellungen

- Modul: Modul des Gerätes
- Port: Port, für den dieser Eintrag gilt.
- VRID: Virtuelle Router-Identifikation (Wert 1-255)
- Funktion: Ein-/ausschalten der VRRP-Instanzen
- Status: VRRP-Status
  - „initialize“: VRRP ist in der Initialisierungsphase. Bisher ist kein Master benannt.
  - „backup“: Der Switch beobachtet die Möglichkeit, Master zu werden.
  - „master“: Der Switch ist Master.
- Priorität: Eingestellte VRRP-Priorität (Wert: 1-255, Voreinstellung: 100).
  Der Router mit dem höchsten Wert wird Master. Ist die virtuelle Router-IP-Adresse gleich der IP-Adresse des Router-Interfaces, dann heißt dieser Router „Owner“. Existiert ein Owner, dann weist VRRP ihm die VRRP-Priorität 255 zu und deklariert ihn so zum Master.

- Aktuelle Priorität: Tatsächlich verwendete VRRP-Priorität (Wert: 1-255). Dieser Wert ist normalerweise gleich der eingestellten VRRP-Priorität, kann aber kleiner sein, wenn überwachte Tracking-Objekte im Zustand „down“ sind.
- VRRP IP-Adresse: Primäre virtuelle Router-IP-Adresse.
- HiVRRP Nachrichten-Intervall: Intervall für die Aussendung von Nachrichten (Advertisement) als Master
  (Wert: bei VRRP: 1-255 s,
  Wert bei HiVRRP: 100-255000 ms,
  Voreinstellung: 1 s).
- Preempt-Modus: Diese Einstellung legt fest, ob dieser Router als Backup-Router einem Master-Router mit niedrigerer VRRP-Priorität die Master-Rolle entzieht. Bei ausgeschaltetem Preempt-Modus beansprucht dieser Router die Master-Rolle erst, wenn die IP-Multicast-Nachricht des existierenden Masters ausbleibt
- Preempt-Verzögerung: Der Preempt-Modus im Zusammenwirken mit VRRP-Tracking kann das Umschalten auf einen besseren Router ermöglichen. Dynamische Routing-Verfahren benötigen aber eine gewisse Zeit, auf geänderte Routen zu reagieren und ihre Routingtabelle neu zu befüllen. Um während dieser Zeit Paketverluste zu vermeiden, bietet die verzögerte Umschaltung (Preempt-Verzögerung) vom Master- auf den Backup-Router den dynamischen Routingverfahren die Möglichkeit, ihre Routingtabellen zu befüllen (Wert: 0-65535 s, Voreinstellung 0 s).
- Domänen-ID: Die Domänen-ID ist eine Nummer zur Identifizierung der Domäne (siehe auf Seite 132 „HiVRRP-Domänen“).
  Wert: 0-8, Voreinstellung 0 = keine Domäne.
- Domänen-Rolle:
  `none`: kein Mitglied einer Domäne
  `member`: übernimmt das Verhalten des Supervisors
  `supervisor`: bestimmt das Verhalten der Domäne
- Authentifizierung: Die Art der angewendeten Authentifizierung:
  - „noAuthentication“: Austausch von VRRP-Informationen ohne Authentifizierung.
  - „simpleTextPassword“: Austausch von VRRP-Informationen mit Klartext-Passwort-Authentifizierung.
- Schlüssel: Passwort für Authentifizierung.
  Zur Kommunikation benötigen die Router mit der gleichen virtuellen Router-IP-Adresse die gleiche Authentifizierungseinstellung.
- Master-IP-Adresse: Tatsächliche Router-Interface-IP-Adresse des Masters.

7.1.3 VRRP-Router-Instanz einrichten

- ☐ Klicken Sie im Dialog `Redundanz:VRRP/HiVRRP:Konfiguration` auf „Assistent“ rechts unten.
- ☐ Wählen Sie in der Tabelle des Assistenten-Dialogs eine Port-Zeile aus und geben Sie in der Zeile VRID die Virtuelle Router-Identifikation ein. Sie können bis zu 8 virtuelle Router je Interface konfigurieren.
- ☐ Klicken Sie auf „Weiter“.
- ☐ Geben Sie unter „Eintrag bearbeiten“ im Rahmen „Grundkonfiguration“ ein:
  - die IP-Adresse des virtuellen Routers
  - die VRRP-Priorität
  - die Art der Authentifizierung
  - den Schlüssel für die Authentifizierung
  - die Preempt-Verzögerung
  - das Nachrichten-Intervall.

  Wählen Sie nach Bedarf den Preempt-Modus.
  Schalten Sie die VRRP-Funktion ein.
  Wenn Sie
  - Umschaltzeiten unter 3 s erzielen wollen,
  - erreichen wollen, dass die Router miteinander mittels Unicasts kommunizieren,
  - Domänen einrichten wollen oder
  - Link-Down Meldungen verschicken wollen,

  aktivieren Sie das Feld "HiVRRP".
  Geben Sie im Rahmen „HiVRRP“ ein:
  - das "Nachrichten-Intervall"
  - die "Zieladresse". Die HiVRRP-Zieladresse ist die IP-Adresse des Partner-HiVRRP-Routers.
  - die IP-Adresse des zweiten Routers an den die Link-Down-Meldungen verschickt werden. Diese Funktion kann verwendet werden, wenn der virtuelle Router aus zwei VRRP-Routern besteht.
  - die Domänen-ID
  - die Domänen-Rolle
- ☐ Klicken Sie auf „Fertig“, um das VRRP-Router-Interface in die VRRP-Router-Interface-Tabelle zu übernehmen
  oder

☐ Klicken Sie auf „Weiter", um unter „Tracking" dem virtuellen Router Tracking-Objekte zuzuordnen. Der Wechsel eines Tracking-Objektes in den Zustand „Down" führt zur Dekrementierung der VRRP-Priorität.
Wählen sich einen bestehenden Tracking-Eintrag aus und klicken Sie auf „Hinzufügen". Sie können bis zu 8 Tracking-Objekte hinzufügen. Achten Sie darauf, dass die Summe der Dekremente aller zugewiesenen Tracking-Einträge kleiner ist als die VRRP-Priorität dieses VRRP-Interfaces.

Anmerkung: Da der IP-Adress-Owner per Definition die feste VRRP-Priorität 255 besitzt, setzt die VRRP-Tracking-Funktion voraus, dass die IP-Adressen der VRRP-Router-Interfaces ungleich der virtuellen Router-IP-Adresse sind.

Anmerkung: Damit nach der Dekrementierung der VRRP-Priorität des Masters durch die Tracking-Funktion der Backup-Router die Master-Rolle übernehmen kann, aktivieren Sie den Preempt-Modus.

☐ Klicken Sie auf „Fertig", um das VRRP-Router-Interface in die VRRP-Router-Interface-Tabelle zu übernehmen
oder

☐ Klicken Sie auf „Weiter", falls Sie unter „Assoziierte IP-Adressen" (Multinetting) weitere IP-Adressen eintragen möchten.

☐ Klicken Sie auf „Fertig", um das VRRP-Router-Interface in die VRRP-Router-Interface-Tabelle zu übernehmen.

7.1.4 VRRP-Router-Instanz konfigurieren

☐ Doppelklicken Sie im Dialog `Redundanz:VRRP/HiVRRP:Konfiguration` in eine Zelle der Tabelle und bearbeiten Sie den Eintrag
oder
klicken Sie mit der rechten Maustaste in eine Zelle und wählen einen Wert aus.

☐ Alternativ zur direkten Bearbeitung in der Tabelle können Sie eine Zeile in der Tabelle markieren und mit Hilfe des Assistenten bearbeiten.

7.1.5 VRRP-Router-Instanz löschen

☐ Wählen Sie im Dialog `Redundanz:VRRP/HiVRRP:Konfiguration` eine Zeile aus und klicken Sie auf „Eintrag löschen“. Damit löschen Sie die Zeile.

7.2 HiVRRP-Domänen

Eine HiVRRP-Instanz ist eine als HiVRRP konfigurierte Router-Instanz mit Funktionen, die das HiVRRP beinhaltet. In einer HiVRRP-Domäne fassen Sie mehrere HiVRRP-Instanzen eines Routers zu einer Management-Einheit zusammen. Eine HiVRRP-Instanz ernennen Sie zum Supervisor der HiVRRP-Domäne. Dieser Supervisor regelt das Verhalten aller HiVRRP-Instanzen seiner Domäne.
Der Router unterstützt bis zu 8 Domänen.

7.2.1 HiVRRP-Domänen anzeigen

- Domain-ID: Identifikation der Domäne
- Status: Status des Supervisors der Domäne
  Supervisor: Supervisor ist aktiv
  SupervisorDown: Supervisor ist nicht aktiv
  noSupervisor: kein Supervisor festgelegt
- Supervisor Port: HiVRRP-Instanz (Modul und Port, in der Schreibweise <Slot>.<Port>), die zum Supervisor bestimmt wurde
- Supervisor VRID: VRID des Supervisors
- Supervisor Status: Status des Supervisors
  - „initialize“: VRRP ist in der Initialisierungsphase. Bisher ist kein Master benannt
  - „backup“: Der Switch beobachtet die Möglichkeit, Master zu werden
  - „master“: Der Switch ist Master
  - „unknown“: kein Supervisor
- Current Priority: Aktuelle VRRP-Priorität

7.2.2 HiVRRP-Domänen-Instanzen auf verschiedenen Ports

Sind Domänen-Instanzen (Member) auf verschiedene physikalische Ports verteilt, überwacht der Router per Voreinstellung ausschließlich die Verbindung des Supervisors auf Leitungsunterbrechung („Redundancy-Check per Member“ ausgeschaltet).
Sie haben die Möglichkeit, die Überwachung der weiteren Verbindungen innerhalb der Domäne auf Leitungsunterbrechung einzuschalten. Überwachen bedeutet, dass der Router zur Erkennung einer Leitungsunterbrechung HiVRRP-Nachrichten sendet. Wählen Sie bei geringer Wahrscheinlichkeit für eine Leitungsunterbrechung ein langes HiVRRP Nachrichten-Intervall (siehe auf Seite 127 „VRRP-Instanz-Einstellungen“), um die Netzlast gering zu halten.

☐ Schalten Sie in der Spalte „Redundancy-Check per Member“ für die gewünschte Domäne die Funktion bei Bedarf ein.

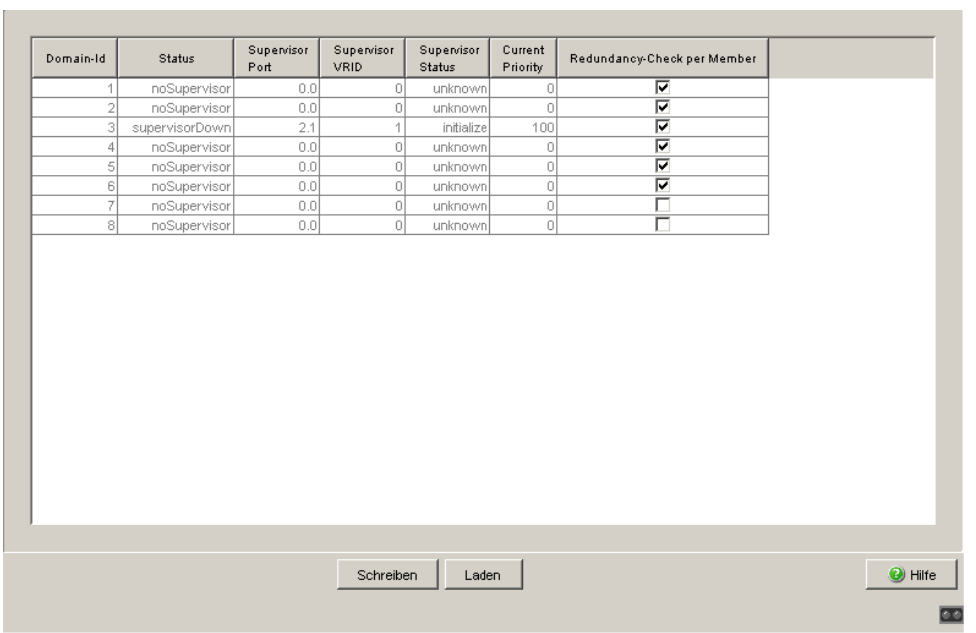


Abb. 56: Dialog HiVRRP-Domänen

7.3 Statistik

Das VRRP-Statistik-Fenster zeigt Zählerstände von Zählern an, die VRRP-relevante Ereignisse zählen.

7.3.1 VRRP-Statistik über alle Ports

- Prüfsummenfehler: Anzahl empfangener VRRP-Nachrichten mit falscher Prüfsumme.
- Versionsfehler: Anzahl empfangener VRRP-Nachrichten mit unbekannter oder nicht unterstützter Versionsnummer.
- VRID-Fehler: Anzahl empfangener VRRP-Nachrichten mit einer ungültigen VRID für diesen virtuellen Router.

7.3.2 VRRP-Statistik pro Port

- Modul: Modul des Gerätes
- Port: Port, für den dieser Eintrag gilt.
- VRID: Virtuelle Router-Identifikation.
- Master geworden: Anzahl, wie oft der Switch schon Master geworden ist.
- Nachrichten empfangen: Anzahl empfangener VRRP-Nachrichten.
- Intervall-Fehler: Anzahl der vom Router außerhalb des Nachrichten-intervalls empfangenen VRRP-Nachrichten.
- Authentifizierungsfehler: Anzahl empfangener VRRP-Nachrichten mit Authentifizierungsfehler.

- IP-TTL-Fehler: Anzahl empfangener VRRP-Nachrichten mit einer IP-TTL ungleich 255.
- Null-Prioritätspakete empfangen: Anzahl der VRRP-Nachrichten, über einen VRRP-Teilnehmer mit der Priorität 0.
- Null-Prioritätspakete gesendet: Anzahl der VRRP-Nachrichten, die der Switch mit der Priorität 0 verschickt hat.
- Empfangene ungültige Pakete: Anzahl der empfangenen VRRP-Nachrichten mit ungültigem Typ.
- Adressfehler: Anzahl der empfangenen VRRP-Nachrichten, für die die Adressliste nicht mit der lokal für den virtuellen Router konfigurierten Adressliste übereinstimmt.
- Ungültiger Authentifizierungstyp: Anzahl empfangener VRRP-Nachrichten mit ungültigem Authentifizierungstyp.
- Unpassender Authentifizierungstyp: Anzahl empfangener VRRP-Nachrichten mit falschem Authentifizierungstyp.
- PaketlängenfehlerAnzahl der empfangenen VRRP-Nachrichten mit falscher Paketlänge.

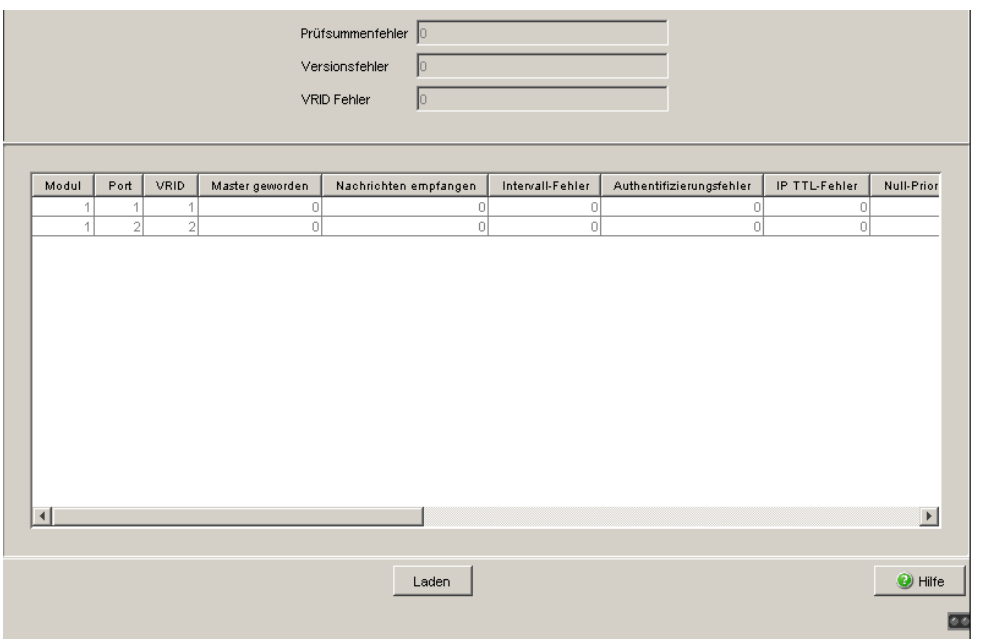


Abb. 57: Dialog VRRP-Statistiken

7.4 Tracking

Das VRRP-Tracking-Fenster zeigt den Zustand aller zu VRRP-Objekten zugeordneten Tracking-Objekte an.

- Port: Port, für den dieser Eintrag gilt in der Schreibweise <Slot>.<Port>
- VRID: Virtuelle Router-Identifikation des zugeordneten virtuellen Routers.
- TrackId: ID-Nummer desTracking-Objekts.
- Decrement: Ändern des Wertes, um den die aktuelle VRRP-Priorität des zugeordneten VRRP-Routers erniedrigt wird, wenn das Tracking-Objekt den Zustand „down“ annimmt.
- Status: Momentaner Zustand des Tracking-Objekts: „up“ oder „down“.
- Aktiv: Anzeige des Eintrags als „aktiv“, wenn das Tracking-Objekt vollständig eingerichtet und aktiviert ist.
  Ist der Eintrag aktiv, können Sie im „Dialog Tracking“ (siehe auf Seite NOT DEFINED) mehr Informationen über ihn finden.
  Ist der Eintrag nicht aktiv, ist sein Zustand immer „up“.

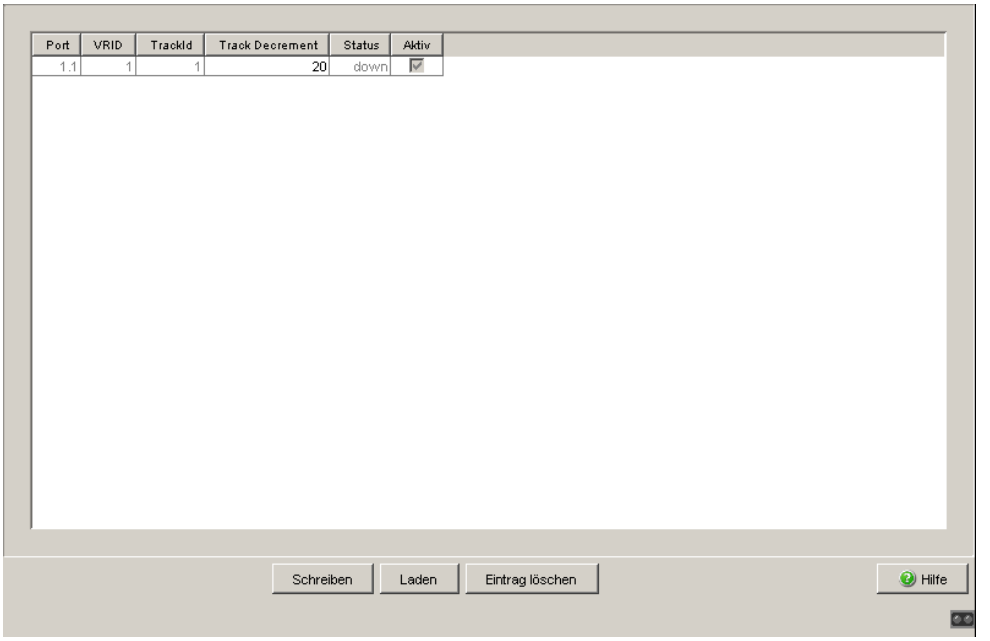


Abb. 58: Dialog Tracking

7.4.1 Tracking-Objekt löschen

☐ Wählen Sie im Dialog `Redundanz:VRRP:Tracking` eine Zeile aus und klicken Sie auf „Eintrag löschen“. Damit löschen Sie die Zeile.

A Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, damit der Einsatz dieses Produkts problemlos erfolgen kann. Ihre Kommentare und Anregungen unterstützen uns, die Qualität und den Informationsgrad dieser Dokumentation noch zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	**gut**	**befriedigend**	**mäßig**	**schlecht**
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Leserkritik

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer +49 (0)7127 14-1600 oder
- per Post an

  Hirschmann Automation and Control GmbH
  Abteilung 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

B Stichwortverzeichnis

A
Advanced Mode 37
Age 114
Alternate-Port 105
Authentifizierung 129

B
Backup-Port 105
Baumstruktur (Spanning Tree) 96, 103
BPDU 96
Bridge Identifier 92
Bridge Protocol Data Unit 96

D
Deaktivierter Port (Spanning Tree) 105
Designated Bridge 104
Designated Port 105, 105
DIP-Schalter 32
Diameter 114
Disabled-Port 105

E
Edge-Port 105
Ersatzport 105

F
FAQ 143
Forward Delay 113

H
Hello Time 112
HIPER-Ring 13, 16, 26
HIPER-Ring konfigurieren 32
HiVRRP 125
HiVRRP-Domänen 132

I
Industrial HiVision 10
Industrieprotokolle 9

K
Konfigurationsfehler 36, 40

L
LACP Link Aggregation Control Protocol 19
Link Aggregation 13, 16, 26
Loops 73, 75, 83, 84

M
Max Age 113
MRP-Ring 13, 16, 25

N
Netzlast 89, 91

P
Pfadkosten 93, 96
Portnummer 95
Port-Identifikation 92, 95
Port-Priorität (Spanning Tree) 95
Port-Rollen (RSTP) 104
Port-Status 107
PROFINET IO 9

R
Rapid Spanning Tree 13, 104
Redundanz 9, 89
Redundanzfunktionen 13
Redundanzmanager 30
Redundanz vorhanden 36, 40
Rekonfiguration 91
Ring 29
Ringstruktur 30
Ring-Manager 29, 30
Ring-Redundanz 14, 14, 14
Ring-/Netzkopplung 13
RM-Funktion 29
Root Bridge 96
Root-Pfad 99, 101
Root-Pfadkosten 92
Root-Port 104
Router 9
RSTP 13
RST BPDU 105, 108

S
Schleifen 73, 75, 83, 84
Schulungsangebote 143
STP-BPDU 96
Sub-Ring 13, 44
Symbol 11

T
Technische Fragen 143
Tracking 136
Trunk 19

V

Virtual Router Redundancy Protocol 125
VLAN (HIPER-Ring) 35
VRRP 125
VRRP/HiVRRP 13
VRRP-Authentifizierungsfehler-Trap 126
VRRP-Instanz 127
VRRP-Master-Trap 126
VRRP-Nachrichten-Intervall 129
VRRP-Router-Instanz 129
VRRP-Statistik 134
VRRP-Tracking 136

C Weitere Unterstützung

Technische Fragen

Bei technischen Fragen wenden Sie sich bitte an den Hirschmann-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann.

Die Adressen unserer Vertragspartner finden Sie im Internet unter http://www.hirschmann.com

Unser Support steht Ihnen zur Verfügung unter https://hirschmann-support.belden.eu.com

Sie erreichen uns

in der Region EMEA unter
- Tel.: +49 (0)1805 14-1538
- E-Mail: hac.support@belden.com

in der Region Amerika unter
- Tel.: +1 (717) 217-2270
- E-Mail: inet-support.us@belden.com

in der Region Asien-Pazifik unter
- Tel.: +65 6854 9860
- E-Mail: inet-ap@belden.com

Hirschmann Competence Center

Das Hirschmann Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen hat vor den Wettbewerbern gleich dreifach die Nase vorn:

- Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
  Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter http://www.hicomcenter.com
- Der Support reicht von der Inbetriebnahme über den Bereitschafts-service bis zu Wartungskonzepten.

Mit dem Hirschmann Competence Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

Anwender-Handbuch

Routing-Konfiguration
Industrial ETHERNET (Gigabit-)Switch
PowerMICE, MACH 104, MACH 1040, MACH 4000

Die Nennung von geschützten Warenzeichen in diesem Handbuch berechtigt auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

© 2015 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken. Bei Geräten mit eingebetteter Software gilt die Endnutzer-Lizenzvereinbarung auf der mitgelieferten CD/DVD.

Die beschriebenen Leistungsmerkmale sind nur dann verbindlich, wenn sie bei Vertragsschluss ausdrücklich vereinbart wurden. Diese Druckschrift wurde von Hirschmann Automation and Control GmbH nach bestem Wissen erstellt. Hirschmann behält sich das Recht vor, den Inhalt dieser Druckschrift ohne Ankündigung zu ändern. Hirschmann gibt keine Garantie oder Gewährleistung hinsichtlich der Richtigkeit oder Genauigkeit der Angaben in dieser Druckschrift.

Hirschmann haftet in keinem Fall für irgendwelche Schäden, die in irgendeinem Zusammenhang mit der Nutzung der Netzkomponenten oder ihrer Betriebssoftware entstehen. Im Übrigen verweisen wir auf die im Lizenzvertrag genannten Nutzungsbedingungen.

Die jeweils neueste Version dieses Handbuches finden Sie im Internet auf den Hirschmann-Produktseiten (www.hirschmann.com).

Hirschmann Automation and Control GmbH
Stuttgarter Str. 45-51
72654 Neckartenzlingen
Deutschland
Tel.: +49 1805 141538

Rel. 9.0 - 02/2015 – 09.01.2015

Inhalt

Sicherheitshinweise 7

Über dieses Handbuch 9

Legende 11

1 Konfiguration 13

2 Routing - Grundlagen 15

2.1 ARP 18

2.2 CIDR 21

2.3 Net-directed Broadcasts 23

2.4 Multinetting 24

3 Statisches Routing 25

3.1 Portbasiertes Router-Interface 26
3.1.1 Konfiguration der Router-Interfaces 27

3.2 VLAN-basiertes Router-Interface 29

3.3 Konfiguration einer statischen Route 34
3.3.1 Konfiguration einer einfachen statischen Route 35
3.3.2 Konfiguration einer redundanten statischen Route 36
3.3.3 Konfiguration einer redundanten statischen Route mit Lastteilung 38

3.4 Statisches Routen-Tracking 39
3.4.1 Beschreibung der statisches Routen-Tracking-Funktion 39
3.4.2 Anwendungsbeispiel für die statisches Routen-Tracking-Funktion 40

3.5 Anpassung für nicht IP-konforme Geräte 43

4 Tracking 45

4.1 Interface-Tracking 46

4.2 Ping-Tracking 48

4.3 Logical-Tracking 50

4.4 Tracking konfigurieren 51
4.4.1 Interface-Tracking konfigurieren 51
4.4.2 Anwendungsbeispiel für Ping-Tracking 53
4.4.3 Anwendungsbeispiel für Logical-Tracking 54

5 VRRP/HiVRRP 57

5.1 VRRP 58
5.1.1 Konfiguration von VRRP 61

5.2 HiVRRP 63

5.3 HiVRRP-Domäne 67
5.3.1 Konfiguration von HiVRRP-Domänen 68
5.3.2 Beispiel für die Konfiguration von HiVRRP-Domänen 69

5.4 VRRP-Tracking 73

5.5 VRRP mit Load Sharing 80

5.6 VRRP mit Multinetting 82

6 RIP 85

6.1 Konvergenz 87

6.2 Maximale Netzgröße 90

6.3 Allgemeine Eigenschaften von RIP 91

6.4 RIP konfigurieren 92

7 OSPF 95

7.1 OSPF-Topologie 97
7.1.1 Autonomes System 97
7.1.2 Router-ID 98
7.1.3 Areas 99
7.1.4 Virtual Link 101
7.1.5 OSPF-Router 103
7.1.6 Link State Advertisement 104

7.2 Prinzipielle Arbeitsweise von OSPF 106

7.3 Aufbau der Adjacency 107

7.4 Synchronisation der LSD 110

7.5 Routenberechnung 112

7.6 OSPF konfigurieren 113

8 Protokollbasierte VLANs 117

8.1 Prinzipielle Konfiguration 119

8.2 Konfiguration des Beispiels 120

9 Multicast-Routing 123

9.1 Multicast-Adressen 125
9.1.1 IP-Multicast-Adressen 125
9.1.2 MAC-Multicast-Adressen 127
9.1.3 IP-MAC-Multicast-Adress-Abbildung 128

9.2 Multicast-Gruppenregistrierung 129

9.3 PIM-DM/PIM-SM/DVMRP 131
9.3.1 Die Funktionsweise von PIM-DM und DVMRP 133
9.3.2 Die Funktionsweise von PIM-SM 136

9.4 Scoping 145

9.5 Multicast-Konfiguration 146
9.5.1 Beispiel mit Layer 3-Redundanz 146
9.5.2 Beispiel mit Layer 2-Redundanz (HIPER-Ring) 151
9.5.3 Tipps für die Konfiguration 152

A Anhang 157

A.1 Verwendete Abkürzungen 158

A.2 Zugrundeliegende IEEE-Normen 160

A.3 Liste der RFCs 161

A.4 IP-Parameter eingeben 164

A.5 Copyright integrierter Software 169
A.5.1 Bouncy Castle Crypto APIs (Java) 169
A.5.2 Broadcom Corporation 170

B Leserkritik 171

C Stichwortverzeichnis 173

D Weitere Unterstützung 177

Sicherheitshinweise

⚠ WARNUNG
UNKONTROLLIERTE MASCHINENBEWEGUNGEN Um unkontrollierte Maschinenbewegungen aufgrund von Datenverlust zu vermeiden, konfigurieren Sie alle Geräte zur Datenübertragung individuell. Nehmen Sie eine Maschine, die mittels Datenübertragung gesteuert wird, erst in Betrieb, wenn Sie alle Geräte zur Datenübertragung vollständig konfiguriert haben. **Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.**

Über dieses Handbuch

Das Dokument „Anwender-Handbuch Routing-Konfiguration“ enthält Informationen, die Sie zur Inbetriebnahme der Routing-Funktion benötigen. Es leitet Sie Schritt für Schritt von einer kleinen Router-Anwendung bis hin zur Router-Konfiguration eines komplexen Netzes.
Das Handbuch versetzt Sie in die Lage, durch Ableitung aus den Beispielen Ihre Router zu konfigurieren.

Das Anwender-Handbuch „Routing-Konfiguration“ setzt voraus, dass Sie den Inhalt des Anwender-Handbuchs „Grundkonfiguration“ kennen.

Einfache Netze können Sie ohne Spezialkenntnisse anhand dieses Handbuchs konfigurieren. Die Konfiguration komplexer Netze setzt fundierte Kenntnisse auf dem Gebiet des Routings und der Protokolle IP, RIP, OSPF, IGMP und VRRP voraus.

Das Dokument „Anwender-Handbuch Installation“ enthält eine Gerätebeschreibung, Sicherheitshinweise, Anzeigebeschreibung und weitere Informationen, die Sie zur Installation des Gerätes benötigen, bevor Sie mit der Konfiguration des Gerätes beginnen.

Das Dokument „Anwender-Handbuch Grundkonfiguration“ enthält die Informationen, die Sie zur Inbetriebnahme des Gerätes benötigen. Es leitet Sie Schritt für Schritt von der ersten Inbetriebnahme bis zu den grundlegenden Einstellungen für einen Ihrer Umgebung angepassten Betrieb.

Das Dokument „Anwender-Handbuch Redundanzkonfiguration“ enthält die Informationen, die Sie zur Auswahl des geeigneten Redundanzverfahrens und dessen Konfiguration benötigen.

Das Dokument „Anwender-Handbuch Industrie-Protokolle“ beschreibt die Anbindung des Gerätes über ein in der Industrie übliches Kommunikationsprotokoll wie z.B. EtherNet/IP und PROFINET IO.

Detaillierte Beschreibungen zur Bedienung der einzelnen Funktionen finden Sie in den Referenz-Handbüchern „Web-based Interface“ und „Command Line Interface“.

Die Netzmanagement-Software Industrial HiVision bietet Ihnen weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:

- ActiveX-Control für SCADA-Integration
- Autotopologie-Erkennung
- Browser-Interface
- Client/Server-Struktur
- Ereignisbehandlung
- Ereignislogbuch
- Gleichzeitige Konfiguration mehrerer Geräte
- Grafische Benutzeroberfläche mit Netz-Layout
- SNMP/OPC-Gateway

Wartung

Hirschmann arbeitet ständig an der Verbesserung und Weiterentwicklung der Software. Prüfen Sie regelmäßig, ob ein neuerer Stand der Software Ihnen weitere Vorteile bietet. Informationen und Software-Downloads finden Sie auf den Hirschmann-Produktseiten im Internet (www.hirschmann.com).

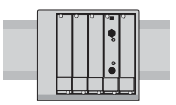
Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
☐	Arbeitsschritt
■	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	ASCII-Darstellung in der grafischen Benutzeroberfläche
	Ausführung in der grafischen Benutzeroberfläche
	Ausführung im Command Line Interface

Verwendete Symbole:

	WLAN-Access-Point
	Router mit Firewall
	Switch mit Firewall
	Router
	Switch

	Bridge
	Hub
	Beliebiger Computer
	Konfigurations-Computer
	Server
	SPS - Speicherprogrammier-bare Steuerung
	I/O - Roboter

1 Konfiguration

Da die Konfiguration eines Routers stark von den Gegebenheiten Ihres Netzes abhängt, finden Sie zunächst eine grobe Aufzählung der einzelnen Schritte zur Konfiguration. Um die Vielzahl der Möglichkeiten optimal abzudecken, finden sie im Anhang Beispiele für Netze, wie Sie in den meisten Fällen in der Industrie vorkommen.

Die Konfiguration der Routing-Funktion beinhaltet in der Regel folgende Schritte:

☐ Netzplan zeichnen
Machen Sie sich ein Bild von Ihrem Netz, um sich über die Aufteilung in Subnetze und die damit verbundene Verteilung der IP-Adressen klar zu werden. Dieser Schritt ist sehr wichtig. Eine gute Planung der Subnetze mit den entsprechenden Netzmasken erleichtert Ihnen die Routerkonfiguration.

☐ Router-Grundeinstellungen
Die Router-Grundeinstellungen beinhaltet neben dem globalen Einschalten der Routing-Funktion auch die Zuordnung von IP-Adressen und Netzmasken an die Router-Interfaces.

Anmerkung: Beachten Sie die Reihenfolge der einzelnen Konfigurationsschritte, damit der Konfigurations-Computer während der ganzen Konfigurationsphase Zugang zu allen Layer-3-Switches hat.

Anmerkung: Sobald Sie einem Router-Interface eine IP-Adresse aus dem Subnetz der Management-IP-Adresse zuweisen, löscht der Switch die Management-IP-Adresse. Sie erreichen den Switch über die IP-Adressen der Router-Interfaces.
Schalten Sie Routing global ein, bevor Sie einem Router-Interface eine IP-Adresse aus dem Subnetz der Management-IP-Adresse zuweisen.

Anmerkung: Sobald Sie einem Router-Interface die VLAN-ID des Management-VLANs zuweisen, deaktiviert der Switch die Management-IP-Adresse. Sie erreichen den Switch über die IP-Adressen der Router-Interfaces. Das Management-VLAN ist das VLAN, über das Sie zum Verwalten aller Switche zugreifen.

Anmerkung: Abhängig von Ihren Konfigurationsschritten kann das Ändern der IP-Parameter Ihres Konfigurations-Computers notwendig werden, um die Erreichbarkeit der Layer 3-Switche zu gewährleisten.

☐ Routing-Verfahren wählen
Wählen Sie anhand des Netzplans und des Kommunikationsbedarfs der angeschlossenen Geräte das für Ihren Fall optimale Routing-Verfahren (statische Routen, RIP, OSPF) aus. Berücksichtigen Sie dabei, welche Routing-Verfahren die Router entlang einer Route beherrschen.

☐ Routing-Verfahren konfigurieren
Konfigurieren Sie das ausgewählte Routing-Verfahren.

2 Routing - Grundlagen

Ein Router ist ein Netzknoten zur Vermittlung von Daten auf Schicht 3 (Layer 3) des ISO/OSI-Schichtenmodells.

Das ISO/OSI-Schichtenmodell (-Referenzmodell) verfolgt die Ziele:

- einen Standard für den Informationsaustausch zwischen offenen Systemen zu definieren;
- eine gemeinsame Basis für die Entwicklung von weiteren Standards für offene Systeme zur Verfügung zu stellen;
- internationale Expertenteams mit einem funktionellen Gerippe zur unabhängigen Entwicklung für jede Schicht des Modells zu versorgen;
- schon bestehende oder in der Entwicklung befindliche Protokolle zur Kommunikation verschiedener Systeme untereinander in diesem Modell zu berücksichtigen;
- genügend Raum und Flexibilität für zukünftige Erweiterungen zu lassen.

Das Schichtenmodell definiert 7 Schichten von der Anwender- bis zur Bitübertragungsschicht.

7	Anwendung	Aus einem Anwenderprogramm auf Kommunikationsdienste zugreifen
6	Darstellung	Definition der Syntaxdarstellung für den Datenverkehr
5	Sitzung	Auf- und Abbau von Verbindungen durch Synchronisation und Organisation des Dialogs
4	Transport	Festlegung der Endsystemverbindung mit der erforderlichen Transportqualität
3	Vermittlung	Transparenter Datenaustausch zwischen zwei Transporteinheiten
2	Sicherung	Zugang zum physikalischen Medium, sowie Erkennen von Übertragungsfehlern
1	Bitübertragung	Übertragung von Bitströmen auf physikalisch vorhandenen Medien

Tab. 1: OSI-Schichtenmodell

Was bedeutet Vermittlung von Daten auf Layer 3 im Vergleich zu Vermittlung von Daten auf Layer 2?

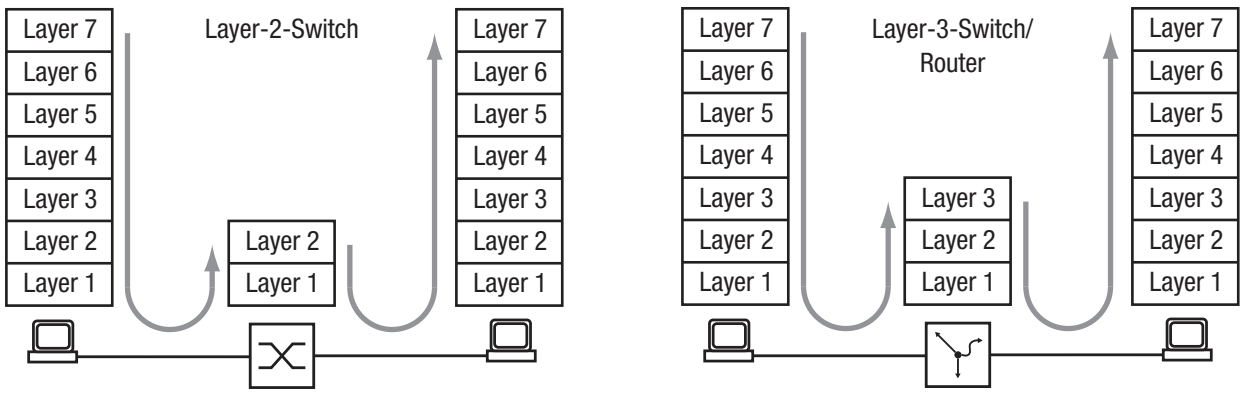


Abb. 1: Datentransport durch einen Switch und einen Router in den Schichten des OSI-Referenzmodells

Auf Layer 2 kennzeichnet die MAC-Adresse das Ziel eines Datenpaketes. Die MAC-Adresse ist eine Adresse, die an die Hardware eines Gerätes gebunden ist. Die Schicht 2 erwartet den Empfänger im angeschlossenen Netz. Die Vermittlung in ein anderes Netz ist Aufgabe von Layer 3. Layer 2-Datenverkehr breitet sich im ganzen Netz aus. Jeder Teilnehmer filtert aus dem Datenstrom die für ihn relevanten Daten heraus. Layer 2-Switche sind in der Lage, Datenverkehr, der an eine bestimmte MAC-Adresse gerichtet ist, zu lenken. Somit erzielt er eine Teilentlastung des Netzes. Broadcast- und Multicast-Datenpakete leiten Layer 2-Switche an allen Ports weiter.

IP ist ein Protokoll auf Layer 3. IP bietet die IP-Adresse zur Adressierung von Datenpaketen. Die IP-Adresse vergibt der Administrator des Netzes. Somit ist er in der Lage, durch die systematische Vergabe von IP-Adressen sein Netz zu strukturieren, das heißt in Teilnetze zu untergliedern (siehe auf Seite 21 „CIDR“). Je größer ein Netz wird, um so höher wird das Datenaufkommen. Da die verfügbare Bandbreite an physikalische Grenzen gebunden ist, ist die Größe eines Netzes beschränkt. Das Aufteilen großer Netze in Teilnetze begrenzt das Datenaufkommen auf diese Teilnetze. Router trennen die Teilnetze voneinander und vermitteln nur die Daten, die für ein anderes Teilnetz bestimmt sind.

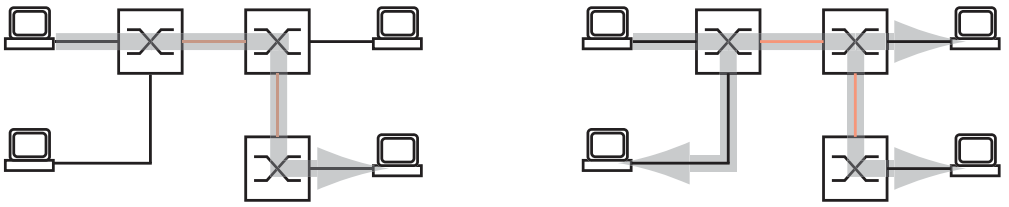


Abb. 2: MAC-Datenvermittlung: Unicast-Datenpaket (links) und Broadcast-Datenpaket (rechts)

Die Abbildung zeigt deutlich, dass Broadcast-Datenpakete bei größeren Netzen eine starke Netzlast erzeugen können. Darüber hinaus gestalten Sie Ihr Netz übersichtlich durch die Bildung von Teilnetzen, die Sie durch Router miteinander verbinden und, so paradox es klingen mag, auch sicher voneinander trennen.

Ein Switch vermittelt anhand der MAC-Zieladresse und somit auf Layer 2.
Ein Router vermittelt anhand der IP-Zieladresse und somit auf Layer 3.
Den Zusammenhang von MAC- zu IP-Adresse ordnen die Teilnehmer mit Hilfe des Address Resolution Protocols (ARP) zu.

2.1 ARP

Das Address Resolution Protocol (ARP) ermittelt zu einer IP-Adresse die zugehörige MAC-Adresse. Wozu ist das nützlich?

Angenommen, Sie möchten Ihren Switch über das Web-based Interface konfigurieren. Dann geben Sie in Ihrem Browser die IP-Adresse Ihres Switch in die Adresszeile ein. Doch an welche MAC-Adresse soll nun Ihr PC sich wenden, um die Informationen des Switchs in Ihrem Browserfenster anzuzeigen?

Befindet sich die IP-Adresse des Switchs im gleichen Subnetz wie Ihr PC, dann schickt Ihr PC einen sogenannten ARP-Request, eine ARP-Anfrage. Das ist ein MAC-Broadcast-Datenpaket mit der Aufforderung an den Inhaber der IP-Adresse, seine MAC-Adresse zurückzusenden. Der Switch antwortet mit einem Unicast-Datenpaket, in dem er seine MAC-Adresse mitteilt. Dieses Unicast-Datenpaket heißt ARP-Reply, ARP-Antwort.

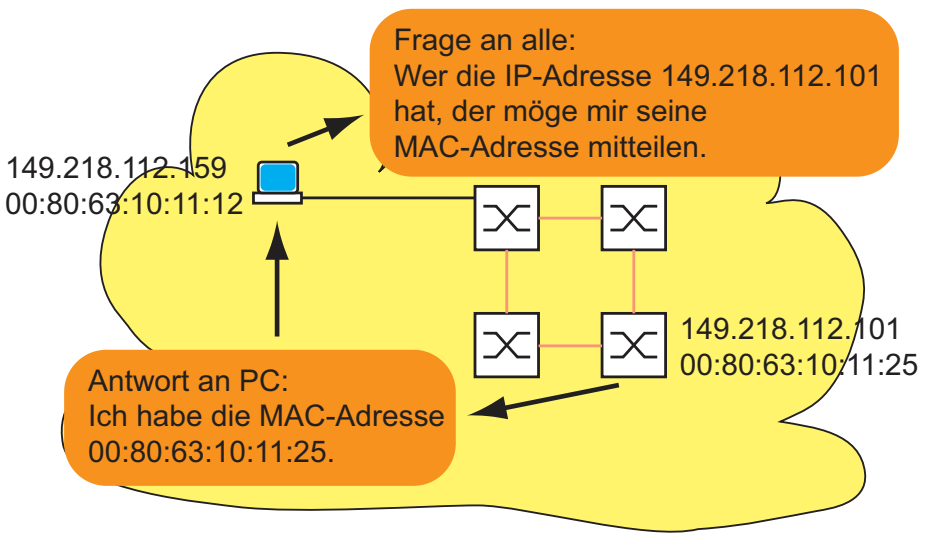


Abb. 3: ARP-Anfrage und -Antwort

Befindet sich die IP-Adresse des Switchs in einem anderen Subnetz, dann fragt der PC nach der MAC-Adresse des im PC eingetragenen Gateways. Das Gateway/Router antwortet mit seiner MAC-Adresse.
Nun verpackt der PC das IP-Datenpaket mit der IP-Adresse des Switch, dem endgültigen Ziel, in einen MAC-Rahmen mit der MAC-Zieladresse des Gateways/Router und verschickt die Daten.
Der Router empfängt die Daten und löst das IP-Datenpaket aus dem MAC-Rahmen heraus, um es dann entsprechend seiner Vermittlungsregeln weiter zu vermitteln.

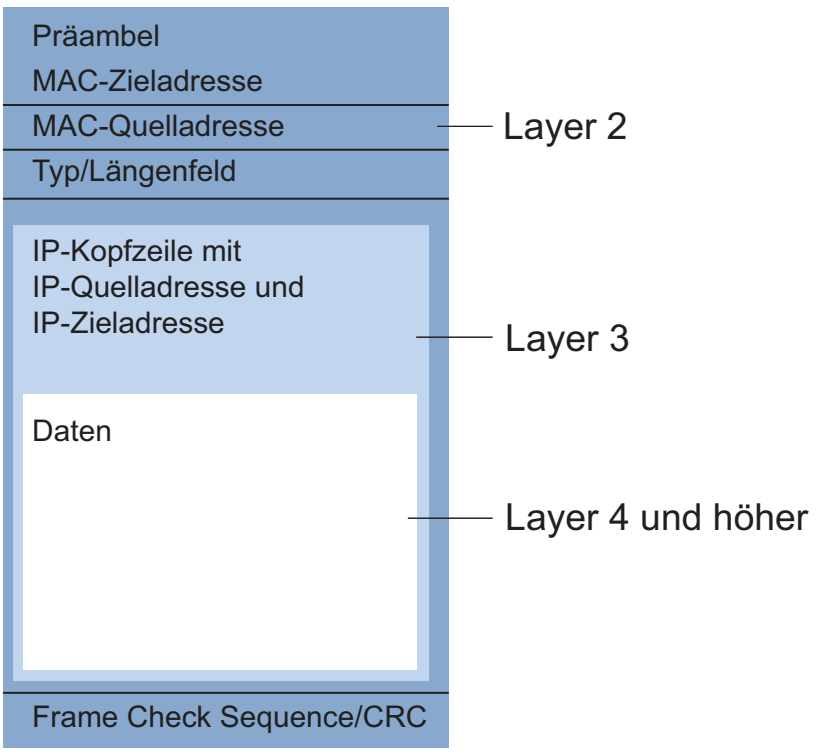


Abb. 4: Aufbau eines Datenpaketes aus Sicht des ISO/OSI-Schichtenmodells

Älteren Endgeräten, die z.B. noch mit IP der ersten Generation arbeiten, ist der Begriff Subnetz noch nicht geläufig. Sie senden eine ARP-Anfrage auch, wenn sie die MAC-Adresse zu einer IP-Adresse in einem anderen Subnetz suchen. Sie haben weder eine Netzmaske, anhand derer sie die Verschiedenheit der Subnetze erkennen könnten noch einen Gateway-Eintrag. Im Beispiel unten sucht der linke PC die MAC-Adresse des rechten PC, der sich in einem anderen Subnetz befindet. Normalerweise würde er in diesem Beispiel unten keine Antwort erhalten.

Da der Router die Route zum rechten PC kennt, antwortet die Proxy-ARP-Funktion auf diesem Router-Interface stellvertretend für den rechten PC mit seiner eigenen MAC-Adresse. So kann der linke PC seine Daten an die MAC-Adresse des Routers adressieren, der die Daten dann an den rechten PC weiterleitet.

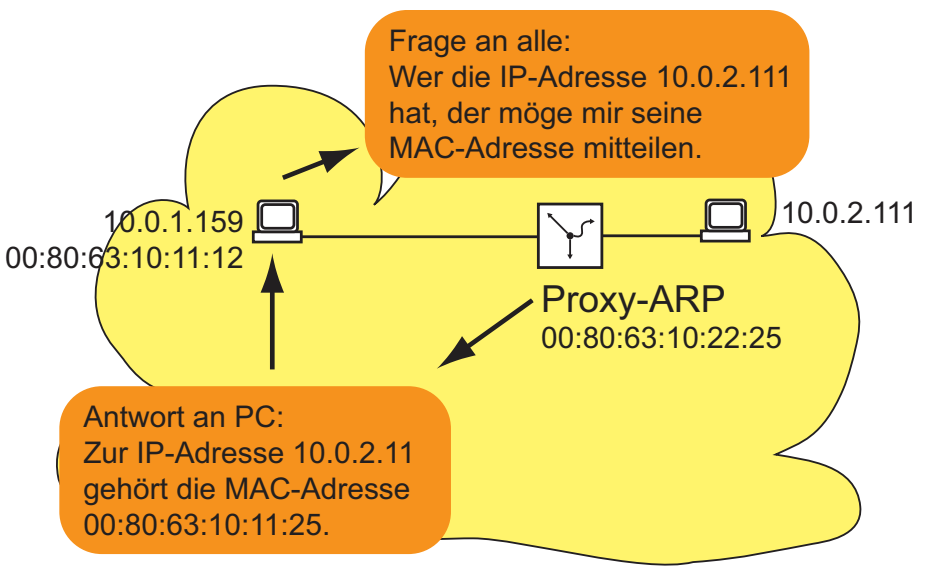


Abb. 5: ARP-Proxy-Funktion

Die Proxy-ARP-Funktion steht an den Router-Interfaces zur Verfügung, an denen Sie Proxy-ARP einschalten.

2.2 CIDR

Die ursprüngliche Klasseneinteilung der IP-Adressen sah nur 3 für Anwender nutzbare Adressklassen vor (siehe „Grundlagen IP-Parameter“ in Anwender-Handbuch Grundkonfiguraton).

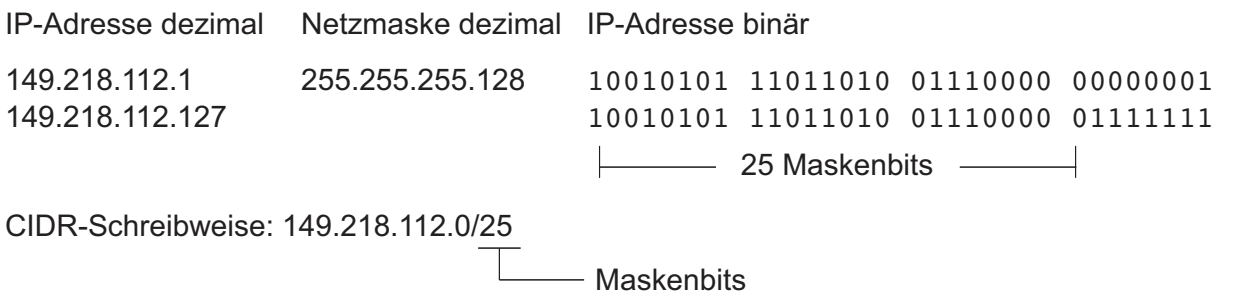
Seit 1992 sind im RFC 1340 fünf Klassen von IP-Adressen definiert.

Class	NetzTeil	Host-Teil	Adressbereich
A	1 Byte	3 Bytes	1.0.0.0 bis 126.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 bis 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 bis 223.255.255.255
D			224.0.0.0 bis 239.255.255.255
E			240.0.0.0 bis 255.255.255.255

Tab. 2: Klassen der IP-Adressen

Die Klasse C mit maximal 254 Adressen war zu klein und die Klasse B mit maximal 65534 Adressen war für die meisten Anwender zu groß, da sie diese Fülle an Adressen nie ausschöpfen werden. Hieraus resultierte eine nicht effektive Nutzung der zur Verfügung stehenden Klasse B Adressen. Die Klasse D enthält reservierte Multicast-Adressen. Die Klasse E ist für experimentelle Zwecke reserviert. Ein Gateway, das nicht an diesen Experimenten teilnimmt, ignoriert Datagramme mit diesen Zieladressen.
Das Classless Inter Domain Routing (CIDR) bietet eine Lösung, diese Probleme zu umgehen. Das CIDR überwindet diese Klassenschranken und unterstützt klassenlose IP-Adressbereiche.

Mit CIDR geben Sie die Anzahl der Bits an, die den IP-Adressbereich kennzeichnen. Hierzu stellen Sie den IP-Adressbereich in binärer Form dar und zählen die Maskenbits zur Bezeichnung der Netzmaske. Die Netzmaske gibt die Anzahl der Bits an, die für alle IP-Adressen in einem gegebenen Adressbreich, dem Netz-Teil identisch sind. Beispiel:



Die Zusammenfassung mehrerer Klasse C-Adressbereiche heißt „Supernetting“. Auf diese Weise lassen sich Klasse-B-Adressbereiche sehr fein untergliedern.

Das Benutzen der Maskenbits vereinfacht die Routingtabelle. Der Router vermittelt in die Richtung, in der am meisten Maskenbits übereinstimmen (longest prefix match).

2.3 Net-directed Broadcasts

Ein net-directed Broadcast ist ein IP-Datenpaket, das ein Gerät an die Netz-Broadcast-Adresse[1] eines Netzes sendet, um alle Empfänger des Netzes anzusprechen. Ein net-directed Broadcast wird in einem Transfernetz als MAC-Unicast-Frame versandt. Unterstützt der Router, der für dieses Netz lokal zuständig ist, net-directed Broadcasts, dann sendet er dieses Datenpaket als einen MAC-Broadcast-Frame in sein lokales Netz aus. Bei VLAN-basierten Router-Interfaces sendet er den Frame an allen Ports aus, die Mitglied im VLAN des Router-Interfaces sind.

So können net-directed Broadcasts Ihr Transfernetz von mehrfachen IP-Unicasts entlasten, die als Ersatz für einen net-directed Broadcast nötig wären.

Unterstützt der Router keine net-directed Broadcasts oder schalten Sie diese Funktion für ein Router-Interface ab, verwirft der Router empfangene IP-Datenpakete an die Netz-Broadcast-Adresse des Router-Interface. Dies gilt bei Multinetting auch für die sekundären IP-Adressen des Router-Interface.

1. Die Netz-Broadcast-Adresse ist die oberste IP-Adresse eines IP-Netzes, für die ein Router-Interface zuständig ist. Das Gerät bestimmt die Broadcast-Adresse aus seiner Interface-IP-Adresse und der zugehörigen Netzmaske. Wenn ein Router-Interface z.B. die IP-Adresse 192.168.1.1 und die Netzmaske 255.255.255.0 hat, ist es für das Netz 192.168.1.0/24 zuständig. Die Netz-Broadcast-Adresse ist dabei 192.168.1.255.

2.4 Multinetting

Multinetting bietet Ihnen die Möglichkeit, mehrere Subnetze an einem Routerport anzuschließen. Multinetting bietet sich als Lösung an, wenn Sie bestehende Subnetze innerhalb eines physikalischen Mediums mit einem Router verbinden wollen. In diesem Fall können Sie mit Multinetting dem Router-Interface, an dem Sie das physikalische Medium anschließen, mehrere IP-Adressen für die unterschiedlichen Subnetze zuordnen.

Für eine langfristige Strategie bieten andere Netzgestaltungsstrategien mehr Vorteile in Bezug auf Problembehebung und Bandbreitenverwaltung an.

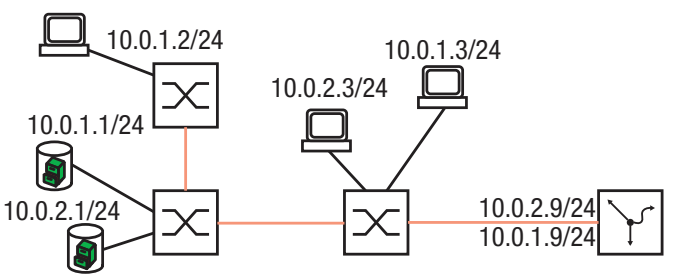


Abb. 6: Beispiel für Multinetting

3 Statisches Routing

Statische Routen sind benutzerdefinierte Routen, mit deren Hilfe der Switch Daten von einem Subnetz in ein anderes Subnetz vermittelt.
Der Benutzer legt fest, an welchen Router (Next-Hop) der Switch Daten für ein bestimmtes Subnetz weiterleitet. Statische Routen stehen in einer Tabelle, die permanent im Switch gespeichert ist.

Im Vergleich zum dynamischen Routing steht dem Vorteil einer transparenten Wegewahl ein erhöhter Aufwand bei der Konfiguration statischer Routen gegenüber. Deshalb findet das statische Routing Anklang in sehr kleinen Netzen oder in ausgesuchten Bereichen größerer Netze. Das statische Routing macht die Routen transparent für den Administrator und ist in kleinen Netzen leicht konfigurierbar.
Ändert sich z.B. durch eine Leitungsunterbrechung die Topologie, dann kann das dynamische im Gegensatz zum statischen Routing automatisch darauf reagieren. Wenn Sie statische und dynamische Routen kombinieren, dann können Sie statische Routen so konfigurieren, dass sie eine höhere Priorität haben, als eine durch ein dynamisches Routing-Verfahren gewählte Route.

Der erste Schritt zur Router-Konfiguration ist das globale Einschalten der Router-Funktion und das Konfigurieren der Router-Interfaces.
Der Switch ermöglicht Ihnen portbasierte und VLAN-basierte Router-Interfaces zu definieren (siehe Abbildung 7).

Beispiel: Verbinden zweier Fertigungszellen

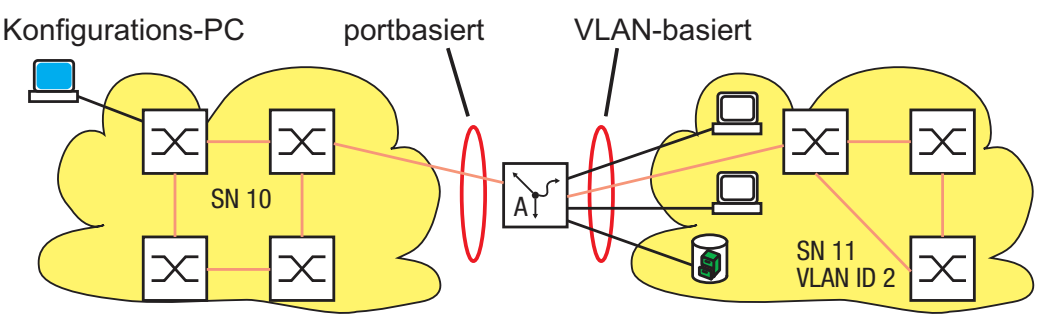


Abb. 7: Statische Routen

3.1 Portbasiertes Router-Interface

Kennzeichnend für das portbasierte Router-Interface ist, dass ein Subnetz an einem Port angeschlossen ist (siehe Abbildung 7).

Besonderheiten von portbasierten Router-Interfaces:

- Wenn keine aktive Verbindung vorhanden ist, dann entfällt der Eintrag aus der Routingtabelle, da der Router ausschließlich an die Ports vermittelt, bei denen auch Aussicht auf eine erfolgreiche Datenübertragung besteht.
  In der Interface-Konfigurationstabelle bleibt der Eintrag erhalten.
- Ein portbasiertes Router-Interface kennt keine VLANs, d.h. der Router verwirft getaggte Frames, die er an einem portbasierten Router-Interface empfängt.
- Ein portbasiertes Router-Interface verwirft alle nicht-routbaren Pakete.

Unten (siehe Abbildung 8) finden Sie ein Beispiel für den einfachsten Fall einer Routing-Anwendung mit portbasierten Router-Interfaces.

3.1.1 Konfiguration der Router-Interfaces

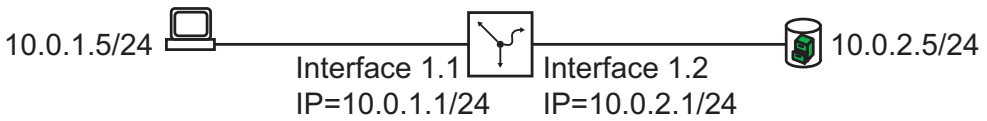


Abb. 8: Einfachster Fall einer Route

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip routing`	Router-Funktion global einschalten.
`interface 2/1`	Auswahl des ersten Ports für die Eingabe der Router-Interface-IP-Adresse.
`ip address 10.0.1.1 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Port .
`exit`	Wechsel in den Konfigurationsmodus.
`interface 2/2`	Auswahl des zweiten Ports für die Eingabe der Router-Interface-IP-Adresse.
`ip address 10.0.2.1 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Port .
`ip netdirbcast`	Einschalten der Vermittlung von Netdirected Broadcasts an diesem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show ip interface brief`	Prüfung der Eingaben.

```
                                                Netdir   Multi
Interface IP Address      IP Mask               Bcast    CastFwd
--------- --------------- --------------- -------- --------
2/1       10.0.1.1        255.255.255.0   Disable  Disable
2/2       10.0.2.1        255.255.255.0   Enable   Disable
```

`show ip interface 2/1`	Überprüfung der restlichen Einstellungen des Interfaces 2/1.

```
Primary IP Address..... ..... 10.0.1.1/255.255.255.0
Routing Mode.............................  Enable
Administrative Mode..... Enable
Forward Net Directed Broadcasts..... Enable
Proxy ARP..... Disable
Active State..... Active
Link Speed Data Rate..... 100 Full
MAC Address..... 00:80:63:51:74:0C
Encapsulation Type..... Ethernet
IP MTU..... 1500
```

`show ip route` Überprüfung der Routingtabelle:

```
Total Number of Routes..... 2
   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------- --------------- ------------  ------  ------------
10.0.1.0        255.255.255.0   Local          2/1       10.0.1.1
10.0.2.0        255.255.255.0   Local          2/2       10.0.2.1
```

`show ip route bestroutes` Überprüfung der Routen, die der Router tatsächlich zur Vermittlung benutzt.

```
   Network          Subnet                   Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------  ---------------  -----------  ---------  --------
10.0.1.0         255.255.255.0    Local        2/1        10.0.1.1
10.0.2.0         255.255.255.0    Local        2/2        10.0.2.1

Total Number of Routes..... 2
```

Anmerkung: Um diese Einträge in der Routingtabelle sehen zu können, benötigen Sie eine aktive Verbindung an den Ports.

3.2 VLAN-basiertes Router-Interface

Kennzeichnend für das VLAN-basierte Router-Interface ist, dass mehrere Geräte eines VLANs an verschiedenen Ports angeschlossen sind. Die Geräte innerhalb eines Subnetzes gehören einem VLAN an (siehe Abbildung 7).

Innerhalb eines VLANs vermittelt der Switch Datenpakete auf Layer 2. Datenpakete mit einer Zieladresse in einem anderen Subnetz adressieren die Endgeräte an den Router als Gateway. Dieser vermittelt die Datenpakete auf Layer 3.

Unten finden Sie ein Beispiel für den einfachsten Fall einer Routing-Anwendung mit VLAN-basierten Router-Interfaces. Für das VLAN fasst der Router die Ports 3.1 und 3.2 zusammen zum VLAN-Router-Interface 9.1. Ein VLAN-Router-Interface bleibt solange in der Routingtabelle, solange mindestens ein Port des VLANs eine Verbindung hat.

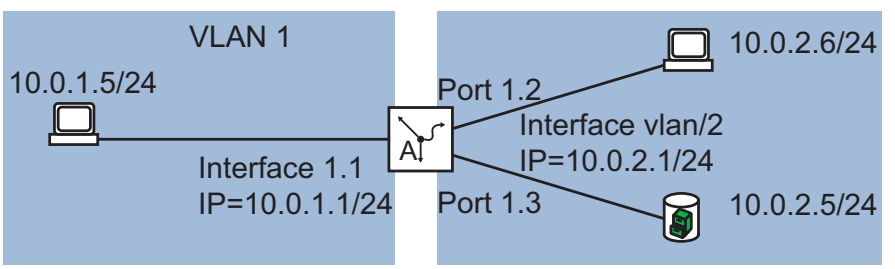


Abb. 9: VLAN-basiertes Router-Interface

VLAN-Router-Interface konfigurieren:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Modus.
`vlan 2`	Anlegen eines VLANs durch Eingabe der VLAN-ID. Die VLAN-ID liegt zwischen 1 und 4.042 (MACH 4000: 3.966).
`vlan name 2 Gerhard`	Dem VLAN 2 den Namen „Gerhard” zuweisen.

```
vlan routing 2
```
Erzeugen eines virtuellen Router-Interfaces und Einschalten der Router-Funktion an diesem Interface.

```
exit
```
Wechsel in den Privileged-EXEC-Modus.

```
show ip vlan
```
Anzeigen des virtuelles-Router-Interfaces, das der Router für das VLAN eingerichtet hat.

```
show ip vlan
         Logical
VLAN ID Interface  IP Address  Subnet Mask   MAC Address
------- ---------- ---------- ------------ -----------------
2       9/1        0.0.0.0    0.0.0.0      00:80:63:51:74:2C
```

```
show ip interface brief
```
Prüfung des Eintrags des virtuellen Router-Interfaces.

```
                                          Netdir   Multi
Interface IP Address      IP Mask         Bcast    CastFwd
--------- --------------- --------------- -------- --------
9/1       0.0.0.0         0.0.0.0         Disable  Disable
```

```
configure
```
Wechsel in den Konfigurationsmodus.

```
interface 9/1
```
Wechsel in den Interface-Konfigurations-Modus von Interface 9/1.

```
ip address 10.0.2.1
  255.255.255.0
```
Dem Interface seine IP-Parameter zuweisen.

```
routing
```
Einschalten der Router-Funktion an diesem Interface.

```
ip netdirbcast
```
Einschalten der Vermittlung von Netdirected Broadcasts an diesem Interface.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
interface 3/1
```
Wechsel in den Interface-Konfigurations-Modus von Interface 3/1.

```
vlan participation include 2
```
Port 3.1 zum Mitglied in VLAN 2 erklären.

```
vlan participation exclude 1
```
Port 3.1 aus dem VLAN 1 herausnehmen.
Im Lieferzustand ist jeder Port dem VLAN 1 zugewiesen.

```
vlan pvid 2
```
Port-VLAN-ID auf 2 setzen, d.h. Datenpakete, die ohne Tag an diesem Port empfangen werden, ordnet der Switch dem VLAN 2 zu.

```
exit
```
Wechsel in den Konfigurationsmodus.

`interface 3/2`	Wechsel in den Interface-Konfigurations-Modus von Interface 3/2.
`vlan participation include 2`	Port 3.2 zum Mitglied in VLAN 2 erklären.
`vlan participation exclude 1`	Port 3.2 aus dem VLAN 1 herausnehmen. Im Lieferzustand ist jeder Port dem VLAN 1 zugewiesen..
`vlan pvid 2`	Port-VLAN-ID auf 2 setzen, d.h. Datenpakete, die ohne Tag an diesem Port empfangen werden, ordnet der Switch dem VLAN 2 zu.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show vlan 2`	Überprüfung Ihrer Einträge in der statischen VLAN-Tabelle

```
VLAN ID: 2
VLAN Name: Gerhard
VLAN Type: Static

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Untagged
1/2         Exclude   Autodetect   Untagged
1/3         Exclude   Autodetect   Untagged
1/4         Exclude   Autodetect   Untagged
2/1         Exclude   Autodetect   Untagged
2/2         Exclude   Autodetect   Untagged
2/3         Exclude   Autodetect   Untagged
2/4         Exclude   Autodetect   Untagged
3/1         Include   Include      Untagged
3/2         Include   Include      Untagged
3/3         Exclude   Autodetect   Untagged
3/4         Exclude   Autodetect   Untagged
4/1         Exclude   Autodetect   Untagged
4/2         Exclude   Autodetect   Untagged
4/3         Exclude   Autodetect   Untagged
4/4         Exclude   Autodetect   Untagged
8/1         Exclude   Autodetect   Untagged
```

`show vlan port all`	Überprüfung der VLAN-spezifischen Porteinstellungen.

```
           Port    Acceptable   Ingress     Default
Interface  VLAN ID Frame Types  Filtering   Priority
---------- ------- ------------ ----------- --------
1/1        1       Admit All    Disable       0
1/2        1       Admit All    Disable       0
1/3        1       Admit All    Disable       0
1/4        1       Admit All    Disable       0
2/1        1       Admit All    Disable       0
2/2        1       Admit All    Disable       0
2/3        1       Admit All    Disable       0
2/4        1       Admit All    Disable       0
3/1        2       Admit All    Disable       0
3/2        2       Admit All    Disable       0
3/3        1       Admit All    Disable       0
3/4        1       Admit All    Disable       0
4/1        1       Admit All    Disable       0
4/2        1       Admit All    Disable       0
4/3        1       Admit All    Disable       0
4/4        1       Admit All    Disable       0
8/1        1       Admit All    Disable       0
```

- ☐ Wählen Sie den Dialog `Routing:Interfaces:Konfiguration`.
- ☐ Klicken Sie auf „Assistent“ rechts unten, um das VLAN-Router-Interface zu konfigurieren.

- ☐ Geben Sie eine Zahl zwischen 1 und 4.042 (MACH 4000: 3.966) als VLAN-ID ein, in diesem Beispiel: 2.
- ☐ Klicken Sie unten auf „Next“.

- ☐ Geben Sie oben in der Zeile „VLAN-Name“ einen beliebigen Namen ein, mit dem Sie das VLAN kennzeichnen wollen.
- ☐ Wählen Sie in der Tabelle in der Spalte „Mitglied“ die Ports aus, die Mitglied dieses VLANs sein sollen.
- ☐ Klicken Sie unten auf „Next“.

☐ Geben Sie im Rahmen „Primary Address“ in der Zeile „IP-Adresse“ die IP-Adresse für das VLAN ein.
☐ Geben Sie in der Zeile „Netzmaske“ die zugehörige Netzmaske ein.
☐ Klicken Sie auf „Abschließen“, um die Konfiguration des VLAN-basierten Router-Interfaces abzuschließen.

In der Router-Interface-Tabelle erscheint das Router-Interface 9.1.
In der statischen VLAN-Tabelle erscheint das VLAN.

☐ Markieren Sie in der Spalte „Netdirected Broadcasts“ das Kästchen für das Router-Interface 9.1.

Mit „Löschen“ haben Sie die Möglichkeit, ein ausgewähltes virtuelles Router-Interface aus der Tabelle zu löschen oder den Eintrag eines physikalischen Router-Interfaces zurückzusetzen.

Anmerkung: Beim Löschen eines VLAN-Router-Interfaces bleibt der Eintrag des VLANs in der VLAN-Tabelle bestehen.
Das Löschen eines VLANs löscht den Eintrag des VLAN-Router-Interfaces in der Router-Interface-Tabelle.

3.3 Konfiguration einer statischen Route

Im Beispiel unten benötigt der Router A die Information, dass er das Subnetz 10.0.3.0/24 über den Router B (Next Hop) erreicht. Diese Information kann er über ein dynamisches Routing-Protokoll oder über einen statischen Routing-Eintrag erhalten. Mit dieser Information ist Router A in der Lage, Daten vom Subnetz 10.0.1.0/24 über Router B in das Subnetz 10.0.3.0/24 zu vermitteln.

Damit umgekehrt auch Router B die Daten von Subnetz 10.0.1.0/24 weiterleiten kann, benötigt auch er eine entsprechende Route.

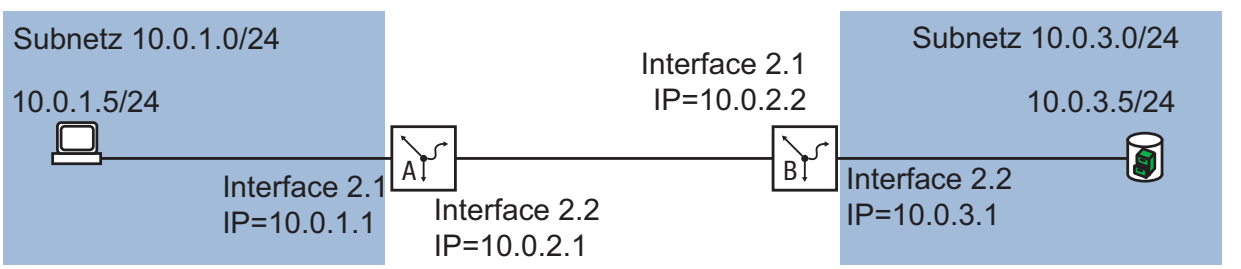


Abb. 10: Statisches Routing

Sie können statische Routen für portbasierte und VLAN-basierte Router-Interface eingeben.

3.3.1 Konfiguration einer einfachen statischen Route

Statische Route eingeben für Router A, ausgehend von der Konfiguration der Router-Interface aus dem vorhergehenden Beispiel (siehe Abbildung 8):

```
enable                              Wechsel in den Privileged-EXEC-Modus.
configure                           Wechsel in den Konfigurationsmodus.
ip routing                          Router-Funktion global einschalten.
ip route 10.0.3.0                   Erstellung des statischen Routing-Eintrags
  255.255.255.0 10.0.2.2
exit                                Wechsel in den Privileged-EXEC-Modus.

show ip route                       Überprüfung der Routingtabelle:

Total Number of Routes..................... 3

   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol      Intf     IP Address
--------------- --------------- ------------  ------  -------------
10.0.1.0        255.255.255.0   Local          2/1       10.0.1.1
10.0.2.0        255.255.255.0   Local          2/2       10.0.2.1
10.0.3.0        255.255.255.0   Static         2/2       10.0.2.2
```

☐ Konfigurieren Sie Router B entsprechend.

3.3.2 Konfiguration einer redundanten statischen Route

Um eine erhöhte Zuverlässigkeit der Verbindung zwischen den beiden Routern zu schaffen, können Sie die beiden Router mit 2 oder mehreren Leitungen verbinden.

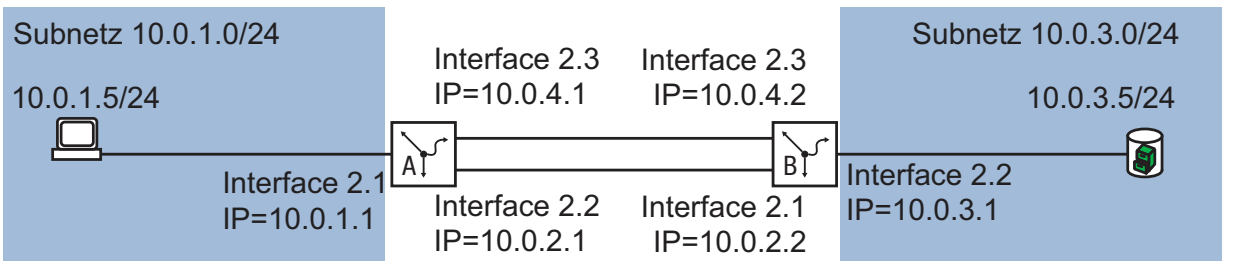


Abb. 11: Redundante statische Route

Sie haben die Möglichkeit, einer Route eine Wichtigkeit (Distanz) zuzuweisen. Bestehen mehrere Routen zu einem Ziel, dann wählt der Router die Route mit der höchsten Wichtigkeit. Geben Sie bei der Konfiguration keinen Wert für die Wichtigkeit an, dann übernimmt der Router den voreingestellten Wert „1“ für die Wichtigkeit. Das ist die höchste Wichtigkeit.

☐ Konfigurieren Sie Router A.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/3`	Auswahl des Ports, an dem Sie die redundante Route anschließen wollen.
`ip address 10.0.4.1 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Port .
`exit`	Wechsel in den Konfigurationsmodus.

```
ip route 10.0.3.0
  255.255.255.0 10.0.4.2 2
```

Erstellung des statischen Routing-Eintrags für die redundante Route. Die „2“ am Ende des Befehls kennzeichnet den Wert der Wichtigkeit.
Wenn beide Routen verfügbar sind, dann benutzt der Router die Route über das Subnetz 10.0.2.0/24, da diese Route die höhere Wichtigkeit (voreingestellt = 1) hat (siehe auf Seite 35 „Konfiguration einer einfachen statischen Route“)

```
show ip route
```

Überprüfung der Routingtabelle:

```
Total Number of Routes..................... 5

   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------- --------------- ------------  ------  -------------
10.0.1.0        255.255.255.0   Local          2/1       10.0.1.1
10.0.2.0        255.255.255.0   Local          2/2       10.0.2.1
10.0.3.0        255.255.255.0   Static         2/2       10.0.2.2
10.0.3.0        255.255.255.0   Static         2/3       10.0.4.2
10.0.4.0        255.255.255.0   Local          2/3       10.0.4.1
```

```
show ip route bestroutes
```

Überprüfung der Routen, die der Router tatsächlich zur Vermittlung benutzt.

```
   Network          Subnet                   Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
---------------  ---------------  ----------  ---------  ---------
10.0.1.0         255.255.255.0    Local        2/1        10.0.1.1
10.0.2.0         255.255.255.0    Local        2/2        10.0.2.1
10.0.3.0         255.255.255.0    Static       2/2        10.0.2.2
10.0.4.0         255.255.255.0    Local        2/3        10.0.4.1

Total Number of Routes..................... 4
```

☐ Konfigurieren Sie Router B entsprechend.

3.3.3 Konfiguration einer redundanten statischen Route mit Lastteilung

Der Router teilt die Last auf die beiden Routen auf (load sharing), wenn die Routen die gleiche Wichtigkeit (Distanz) haben.

```
ip route 10.0.3.0
  255.255.255.0 10.0.2.2 2
```

Zuordnung der Wichtigkeit „2" für die bestehende statische Route (siehe auf Seite 35 „Konfiguration einer einfachen statischen Route").
Wenn beide Routen verfügbar sind, dann benutzt der Router beide Routen zur Datenübertragung.

```
show ip route
```

Überprüfung der Routingtabelle:

```
Total Number of Routes..... 4

   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------- --------------- ------------  ------  -------------
10.0.1.0        255.255.255.0   Local          2/1       10.0.1.1
10.0.2.0        255.255.255.0   Local          2/2       10.0.2.1
10.0.3.0        255.255.255.0   Static         2/2       10.0.2.2
                                               2/3       10.0.4.2
10.0.4.0        255.255.255.0   Local          2/3       10.0.4.1
```

```
show ip route bestroutes
```

Überprüfung der Routen, die der Router tatsächlich zur Vermittlung benutzt.

```
   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------- --------------- ------------  ------  -------------
10.0.1.0        255.255.255.0   Local          2/1       10.0.1.1
10.0.2.0        255.255.255.0   Local          2/2       10.0.2.1
10.0.3.0        255.255.255.0   Static         2/2       10.0.2.2
                                               2/3       10.0.4.2
10.0.4.0        255.255.255.0   Local          2/3       10.0.4.1

Total Number of Routes..... 4
```

3.4 Statisches Routen-Tracking

3.4.1 Beschreibung der statisches Routen-Tracking-Funktion

Bestehen beim statischen Routing mehrere Routen zu einem Ziel, dann wählt der Router die Route mit der höchsten Wichtigkeit. Der Router erkennt eine bestehende Route am Zustand des Router-Interfaces. Nun kann die Verbindung L 1 (siehe Tabelle 3) am Router-Interface zwar in Ordnung sein, aber die Verbindung zu einem entfernten Router B an anderer Stelle L 2 unterbrochen sein. In diesem Fall vermittelt der Router nach wie vor über die unterbrochene Route.

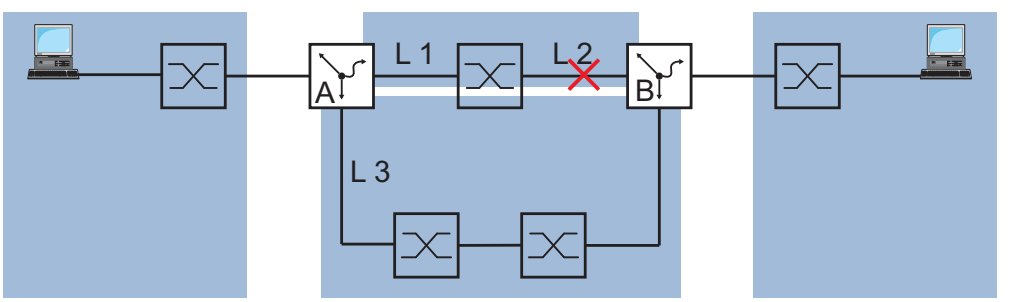


Abb. 12: Beispiel für statisches Routen-Tracking

Bei der statisches Routen-Tracking-Funktion erkennt der Router mit Hilfe eines Tracking-Objektes, z.B. Ping-Tracking-Objekt (siehe auf Seite 48 „Ping-Tracking“), die Verbindungsunterbrechung. Die aktive statisches Routen-Tracking-Funktion löscht daraufhin die unterbrochene Route aus der aktuellen Routingtabelle. Nimmt das Tracking-Objekt wieder den Zustand „up“ an, dann trägt der Router die statische Route wieder in die aktuelle Routingtabelle ein.

3.4.2 Anwendungsbeispiel für die statisches Routen-Tracking-Funktion

Die Abbildung (siehe Abbildung 13) zeigt ein Beispiel für die statisches Routen-Tracking-Funktion:
Router A überwacht die beste Route über L 1 mit Ping-Tracking. Bei einer Verbindungsunterbrechung vermittelt der Router A über die redundante Verbindung L 3.
Bekannt sind:

Parameter	Router A	Router B
IP-Adresse Interface (IF) 1.1	10.0.4.1	
IP-Adresse Interface (IF) 1.2	10.0.2.1	10.0.4.2
IP-Adresse Interface (IF) 1.3		10.0.2.53
IP-Adresse Interface (IF) 1.4	10.0.1.112	
IP-Adresse Interface (IF) 2.2		10.0.5.1
Netzmaske	255.255.255.0	255.255.255.0

Voraussetzungen für die weitere Konfiguration:

- Die IP-Parameter der Router-Interface sind konfiguriert. (siehe auf Seite 27 „Konfiguration der Router-Interfaces“)
- Die Router-Funktion ist global und an den Ports/Router Interface eingeschaltet.
- Ping-Tracking am Interface 1.2 von Router A ist konfiguriert (siehe auf Seite 53 „Anwendungsbeispiel für Ping-Tracking“).

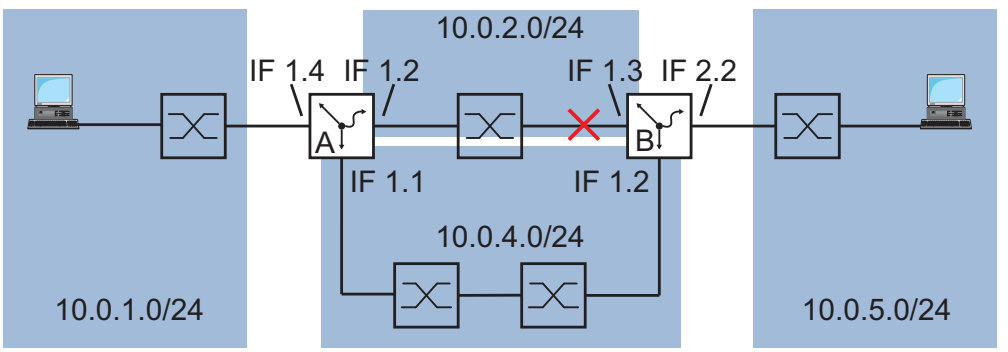


Abb. 13: Statisches Routen-Tracking konfigurieren

☐ Tragen Sie die beiden Routen zum Zielnetz 10.0.5.0/24 in die statische Routingtabelle von Router A ein.

☐ Wählen Sie den Dialog `Routing:Routing-Tabelle:Statisch`.

☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch öffnen Sie das Eingabefenster für einen neuen Eintrag.

☐ Tragen Sie die Daten für die erste statische Route ein:

„Zielnetz“	`10.0.5.0`
„Zielnetzmaske“	`255.255.255.0`
„Next Hop“	`10.0.2.53`
„Track-ID“	`21`

☐ Klicken Sie „OK“.

☐ Klicken Sie auf „Eintrag erzeugen“.
Hierdurch öffnen Sie das Eingabefenster für einen neuen Eintrag.

☐ Tragen Sie die Daten für die erste statische Route ein:

„Zielnetz“	10.0.5.0
„Zielnetzmaske“	255.255.255.0
„Next Hop“	10.0.4.2
„Track-ID“	0

☐ Klicken Sie „OK“.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip route 10.0.5.0 255.255.255.0 10.0.2.53 1 track 21`	Erstellung des statischen Routing-Eintrags mit der Präferenz 1 und der Track-ID 21.
`ip route 10.0.5.0 255.255.255.0 10.0.4.2 2`	Erstellung des statischen Routing-Eintrags mit der Präferenz 2.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show ip route`	Überprüfung der Routingtabelle:

```
Total Number of Routes..................... 3

   Network          Subnet                    Next Hop     Next Hop
   Address           Mask          Protocol     Intf      IP Address
-------------- --------------- ------------  ------  -------------
10.0.1.0       255.255.255.0   Local          1/4       10.0.1.112
10.0.2.0       255.255.255.0   Local          1/2       10.0.2.1
10.0.5.0       255.255.255.0   Static         1/2       10.0.2.53
```

☐ Legen Sie auf dem Router B ein Ping-Tracking-Objekt mit der Track-ID z.B. 22 zur IP-Adresse 10.0.2.1 an.

☐ Tragen Sie die beiden Routen zum Zielnetz 10.0.1.0/24 in die statische Routingtabelle von Router B ein.

Zielnetz	Zielnetzmaske	Next Hop	Präferenz	Track-ID
10.0.1.0	255.255.255.0	10.0.2.1	1	22
10.0.1.0	255.255.255.0	10.0.4.1	2	

Tab. 3: Statische Routing-Einträge von Router B

3.5 Anpassung für nicht IP-konforme Geräte

Manche Geräte benutzen einen vereinfachten IP-Stack, der nicht dem IP-Standard entspricht. Ohne eine ARP-Anfrage schicken diese Geräte ihre Antworten an die MAC-Adresse, die als Quelladresse im anfragenden Paket enthalten ist (siehe Bild unten, keine MAC/IP-Adressauflösung). Dieses Verhalten zeigen diese Geräte besonders bei Ping-Anfragen (ICMP Echo Request). Manche dieser Geräte zeigen dieses Verhalten auch bei anderen Datenpaketen.
Solange das Router-Interface des Routers, an dem ein solches Gerät angeschlossen ist, an die MAC-Adresse des physikalischen Ports gebunden ist, kann der Router das Paket auch empfangen und vermitteln.
Gehört der physikalische Port aber einem VLAN an, dann hat das VLAN-Router-Interface eine eigene MAC-Adresse. Somit verwirft der Router Pakete, die an die Port-MAC-Adresse gerichtet sind.

Ein Endgerät, das die MAC/IP-Adressauflösung nach dem IP-Standard durchführt, startet eine ARP-Anfrage, um die korrekte MAC-Adresse zu ermitteln, bevor es dann die Antwort an die ermittelte VLAN-MAC-Adresse sendet (siehe Bild unten, MAC/IP-Adressauflösung nach Standard über ARP).

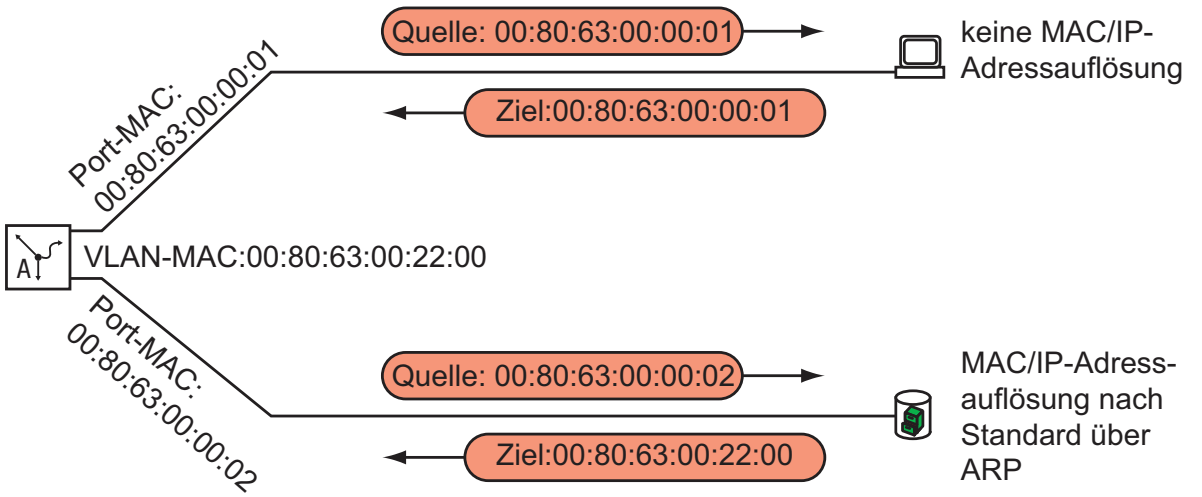


Abb. 14: Adressierung mit vereinfachtem IP-Stack und konform zum Standard

Damit Sie auch Geräte mit vereinfachtem IP-Stack an ein VLAN-basiertes Router-Interface anschließen können, bietet Ihnen der Router den VLAN-Single-MAC-Modus.
Im VLAN-Single-MAC-Modus benutzen alle VLAN-Interfaces und alle physikasischen Ports die selbe MAC-Adresse mit Ausnahme der portbasierten Router-Interfaces.

☐ VLAN-Single-MAC-Modus einschalten:

```
enable                          Wechsel in den Privileged-EXEC-Modus.
configure                       Wechsel in den Konfigurationsmodus.
ip vlan-single-mac              Einschalten des VLAN-Single-MAC-Modus.
exit                            Wechsel in den Privileged-EXEC-Modus.

show ip vlan                    Anzeigen der VLAN-IP-Parameter
        Logical
VLAN ID Interface IP Address     Subnet Mask     MAC Address
------- --------- -------------  -------------  -----------------
100     9/1       192.168.100.1  255.255.255.0  00:80:63:51:74:2B
200     9/2       192.168.200.1  255.255.255.0  00:80:63:51:74:2B
```

4 Tracking

Die Tracking-Funktion bietet Ihnen die Möglichkeit, bestimmte Objekte wie z.B. die Verfügbarkeit eines Interfaces zu überwachen.
Das Besondere an dieser Funktion ist die Weiterleitung einer Objekt-Zustandsänderung an eine Anwendung wie z.B. VRRP, die sich zuvor als Interessent für diese Information registriert hat.

Das Tracking kann folgende Objekte überwachen:

- Verbindungsstatus eines Interfaces (Interface-Tracking)
- Erreichbarkeit eines Gerätes (Ping-Tracking)
- Ergebnis logischer Verknüpfungen von Tracking-Einträgen (Logic-Tracking)

Ein Objekt kann folgende Zustände annehmen:

- up (in Ordnung)
- down (nicht in Ordnung)

Die Definition von „up” und „down” hängt ab vom Typ des Tracking-Objekts (z.B. Interface-Tracking)

Das Tracking kann Zustandsänderungen eines Objekts an folgende Anwendungen weiterleiten:

- VRRP (siehe auf Seite 73 „VRRP-Tracking“)
- Statisches Routing (siehe auf Seite 39 „Statisches Routen-Tracking“)

4.1 Interface-Tracking

Beim Interface-Tracking überwacht der Switch den Verbindungsstatus (Link-Status) von:

- physikalischen Ports
- Link-Aggregation-Interfaces (Interfaces 8.x)
- VLAN-Router-Interfaces (Interfaces 9.x)

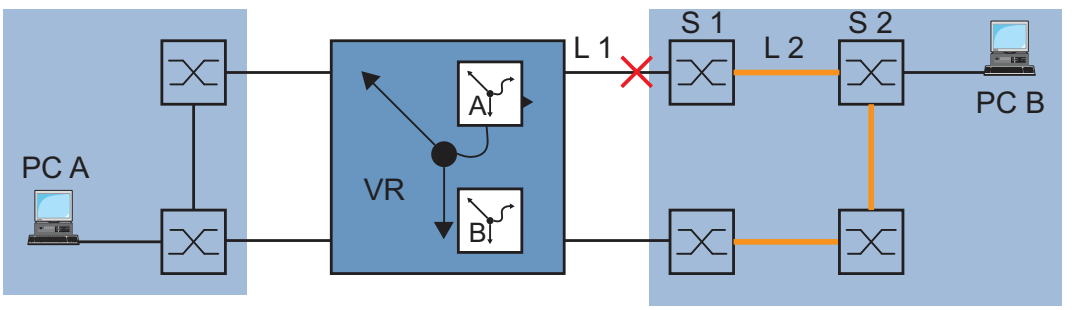


Abb. 15: Überwachen einer Leitung mit Interface-Tracking

Ports/Interfaces können folgende Verbindungstati haben:

- unterbrochene physikalische Verbindung (link down) und
- bestehende physikalische Verbindung (link up).

Ein Link-Aggregation-Interface hat den Verbindungsstatus „down”, wenn die Verbindung aller teilnehmenden Ports unterbrochen ist.

Ein VLAN-Router-Interface hat den Verbindungsstatus „down”, wenn die Verbindung unterbrochen ist von allen physikalischen Ports/Link-Aggregation-Interfaces, die Mitglied im entsprechenden VLAN sind.

Das Einstellen einer Verzögerungszeit bietet Ihnen die Möglichkeit, die Anwendung verzögert über die Objekt-Zustandänderung zu informieren.

Ein Interface-Tracking-Objekt nimmt den Zustand „down” an, sobald die physikalische Verbindung länger als die Verzögerungszeit „Link-Down-Verzögerung” anhält.

Ein Interface-Tracking-Objekt nimmt den Zustand „up” an, sobald die physikalische Verbindung länger als die Verzögerungszeit „Link-Up-Verzögerung” anhält.

Lieferzustand: Verzögerungszeiten = 0 Sekunden.
Das heißt, eine Zustandsänderung führt zur sofortigen Information der registrierten Anwendung.
Sie können die Verzögerungszeiten „Link-Down-Verzögerung“ und „Link-Up-Verzögerung“ unabhängig voneinander einstellen im Bereich von 0 bis 255 Sekunden.
Je Interface können Sie ein Interface-Tracking-Objekt definieren.

4.2 Ping-Tracking

Beim Ping-Tracking überwacht das Gerät den Verbindungsstatus zu anderen Geräten durch Ping-Anfragen.

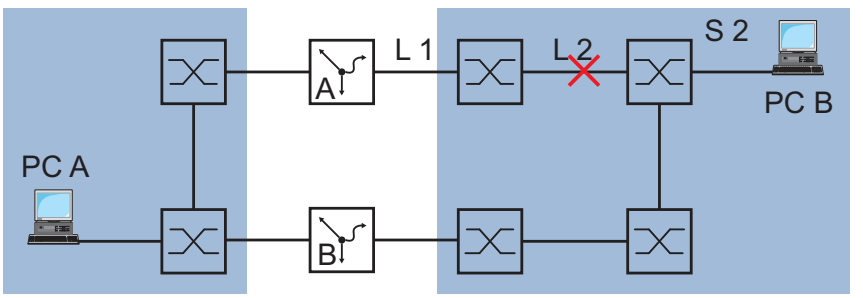


Abb. 16: Überwachen einer Verbindung mit Ping-Tracking

Das Gerät sendet Ping-Anfragen an das Gerät mit der IP-Adresse, welche Sie in der Spalte „IP-Adresse“ eingetragen haben.
Die Spalte „Ping-Intervall“ bietet Ihnen die Möglichkeit, die Häufigkeit des Versendens von Ping-Anfragen und damit die zusätzliche Netzlast zu definieren.
Kommt die Antwort innerhalb der in der Spalte „Ping-Timeout“ eingetragenen Zeit zurück, dann gilt diese Antwort als gültige „Ankommende Ping-Antwort“.
Kommt die Antwort nach der in der Spalte „Ping-Timeout“ eingetragenen Zeit oder gar nicht zurück, dann gilt diese Antwort als „Ausbleibende Ping-Antwort“.

Ping-Tracking-Objekte können folgende Stati annehmen:

- Die Anzahl der „ausbleibenden Ping-Antworten“ übersteigt den eingetragenen Betrag (down) und
- Die Anzahl der „ankommenden Ping-Antworten“ übersteigt den eingetragenen Betrag (up).

Das Vorgeben einer Anzahl für ausbleibende oder ankommende Ping-Antworten bietet Ihnen die Möglichkeit, die Empfindlichkeit für das Ping-Verhalten des Gerätes einzustellen. Das Gerät informiert die Anwendung über eine Objekt-Zustandänderung.

Ping-Tracking bietet Ihnen die Möglichkeit, die Erreichbarkeit definierter Geräte zu überwachen. Sobald ein überwachtes Gerät nicht mehr erreichbar ist, kann das Gerät über die Anwendung einen alternativen Pfad wählen.

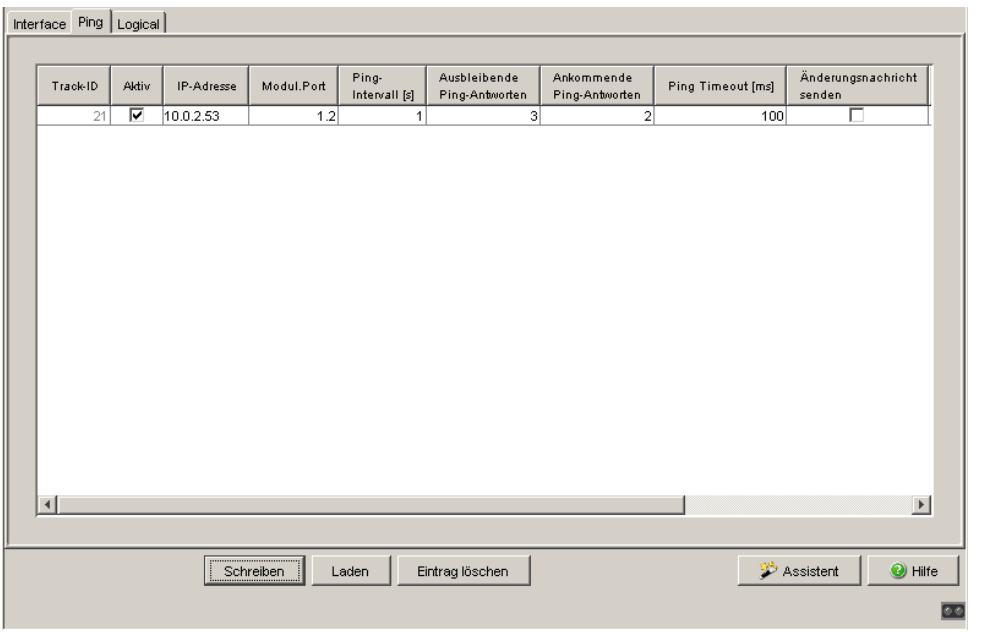


Abb. 17: Dialog Ping-Tracking

4.3 Logical-Tracking

Logical-Tracking bietet Ihnen die Möglichkeit, mehrere Tracking-Objekte logisch miteinander zu verknüpfen und somit recht komplexe Überwachungsaufgaben zu realisieren.
Mit Logical-Tracking können Sie z.B. den Verbindungsstatus zu einem Netzknoten überwachen, zu welchem redundante Pfade führen (siehe auf Seite 54 „Anwendungsbeispiel für Logical-Tracking“).

Das Gerät bietet folgende Operatoren für eine logische Verknüpfung:
- UND
- ODER

Für eine logische Verknüpfung können Sie bis zu 8 Operanden mit einem Operator verknüpfen.

Logical-Tracking-Objekte können folgende Stati annehmen:
- Das Ergebnis der logischen Verknüpfung ist falsch (down).
- Das Ergebnis der logischen Verknüpfung ist wahr (up).

Sobald eine logische Verknüpfung das Ergebnis „falsch“ liefert, kann das Gerät über die Anwendung einen alternativen Pfad wählen.

4.4 Tracking konfigurieren

Tracking konfigurieren Sie durch das Einrichten von Tracking-Objekten. Das Einrichten von Tracking-Objekten erfordert folgende Schritte:

- geben Sie die Tracking-Objekt-Identifikationsnummer (Track-ID) ein.
- wählen Sie den Tracking-Typ, z.B. Interface, aus.
- geben Sie, in Abhängigkeit des Track-Typs, weitere Optionen ein, wie z.B. beim Interface-Tracking „Port”, „Link-Up-Verzögerung”.

Anmerkung: Die Registrierung der Anwendung (z.B. VRRP), an welche die Tracking-Funktion eine Zustandsänderung meldet, nehmen Sie in der Anwendung vor (siehe auf Seite 73 „VRRP-Tracking“).

4.4.1 Interface-Tracking konfigurieren

☐ Interface-Tracking am Port 1.1 mit einer Link-Down-Verzögerung von 0 Sekunden und einer Link-Up-Verzögerung von 3 Sekunden einrichten.

☐ Klicken Sie im Dialog `Routing:Tracking:Konfiguration` auf „Assistent“ rechts unten.

Typ auswählen:

☐ Tragen Sie die gewünschten Werte ein:

Track ID:	`1`
Typ:	`interface`

☐ Klicken Sie auf „Weiter“.

Eigenschaften:

☐ Tragen Sie die gewünschten Werte ein:

Modul.Port:	1.1
Link-Up-Verzögerung:	3
Link-Down-Verzögerung:	0

☐ Klicken Sie auf „Fertig“, um den Assistenten zu beenden und den Eintrag in der Konfiguration flüchtig zu speichern.

```
enable                                  Wechsel in den Privileged-EXEC-Modus.
configure                               Wechsel in den Konfigurationsmodus.
track 1 interface 1/1                   Eingabe der Tracking-Parameter und Aktivieren
  link-down-delay 0                     dieses Tracking-Objektes.
  link-up-delay 3
Tracking ID 1 created
  Tracking type set to Interface
  Target interface set to 1/1
  Link Down Delay for target interface set to 0 sec
  Link Up Delay for target interface set to 3 sec
Tracking ID 1 activated
exit                                    Wechsel in den Privileged-EXEC-Modus.
show track                              Anzeige der konfigurierten Tracks
             Link Delay                       No. of
ID Type  Intf Down  Up   Status  Mode  Changes Time since last change
-- ----  ---- ----- ----- ------ ------ ------- --------------------
1 Intf  1/1    0s    3s  DOWN  Enable      0   0 day(s), 00:00:29
Unconfigured Track-IDs with registered applications:
-------------------------------------------------
```

4.4.2 Anwendungsbeispiel für Ping-Tracking

Während das Interface-Tracking die direkt angeschlossene Verbindung überwacht (siehe Abbildung 15), überwacht das Ping-Tracking die gesamte Verbindung bis zum Switch S2 (siehe Abbildung 16).

☐ Ping-Tracking am Port 1.2 zur IP-Adresse 10.0.2.53 mit den voreingestellten Parametern einrichten.

☐ Klicken Sie im Dialog `Routing:Tracking:Konfiguration` auf „Assistent“ rechts unten.

Typ auswählen:

☐ Tragen Sie die gewünschten Werte ein:

Track ID:	`21`
Typ:	`ping`

☐ Klicken Sie auf „Weiter“.

Eigenschaften:

☐ Tragen Sie die gewünschten Werte ein:

IP-Adresse:	`10.0.2.53`
Modul.Port:	`1.2`
Ping-Intervall [s]:	`1`
Ausbleibene Ping-Antworten:	`3`
Ankommende Ping-Antworten:	`2`
Ping-Timeout [ms]:	`100`

☐ Klicken Sie auf „Fertig“, um den Assistenten zu beenden und den Eintrag in der Konfiguration flüchtig zu speichern.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`track 21 ping 10.0.2.53 interface 1/2 interval 1 miss 3 success 2 timeout 100`	Eingabe der Tracking-Parameter und Aktivieren dieses Tracking-Objektes.

```
Tracking ID 21 created
  Tracking type set to Ping
  Target IP address set to 10.0.2.53
  Interface used for sending pings to target set to 1/2
  Ping Interval for target set to 1 sec
  Max. no. of missed ping replies from target set to 3
  Min. no. of received ping replies from target set to 2
  Timeout for ping replies from target set to 100 ms
Tracking ID 21 activated
exit                              Wechsel in den Privileged-EXEC-Modus.
show track                        Anzeige der konfigurierten Tracks
Ping Tracking
                                                 No. of   Time since
  ID Type IP Address  Intvl Status Mode Changes  last change
 --- ---- ----------- ----- ------ ------ ------- -----------------
  21 Ping  10.0.2.53    1s  DOWN   Enable   1    0 day(s), 00:13:39
```

4.4.3 Anwendungsbeispiel für Logical-Tracking

Die Abbildung (siehe Abbildung 15), zeigt ein Beispiel für die Überwachung der Verbindung zu einem redundanten Ring.
Durch die Überwachung der Leitungen L 2 und L 4 können Sie die Verbindungsunterbrechung des Routers A zum redundanten Ring erkennen.
Mit einem Ping-Tracking-Objekt am Port 1.1 des Routers A überwachen Sie die Verbindung zum Switch S2.
Mit einem weiteren Ping-Tracking-Objekt ebenfalls am Port 1.1 des Routers A überwachen Sie die Verbindung zum Switch S4.
Erst die ODER-Verknüpfung beider Ping-Tracking-Objekte liefert das präzise Ergebnis, dass der Router A keine Verbindung zum Ring hat.
Zwar könnte ein Ping-Tracking-Objekt zum Switch S3 auch auf eine unterbrochene Verbindung zum redundanten Ring hinweisen, aber in diesem Fall könnte auch aus einem anderen Grund die Ping-Antwort von Switch S3 ausbleiben. Zum Beispiel könnte die Stromversorgung des Switch S3 ausgefallen sein.

Bekannt sind:

Parameter	Wert
Operand Nr. 1 (Track-ID)	21
Operand Nr. 2 (Track-ID)	22

Voraussetzungen für die weitere Konfiguration:

- Die Ping-Tracking-Objekte für die Operanden 1 und 2 sind konfiguriert (siehe auf Seite 53 „Anwendungsbeispiel für Ping-Tracking“).

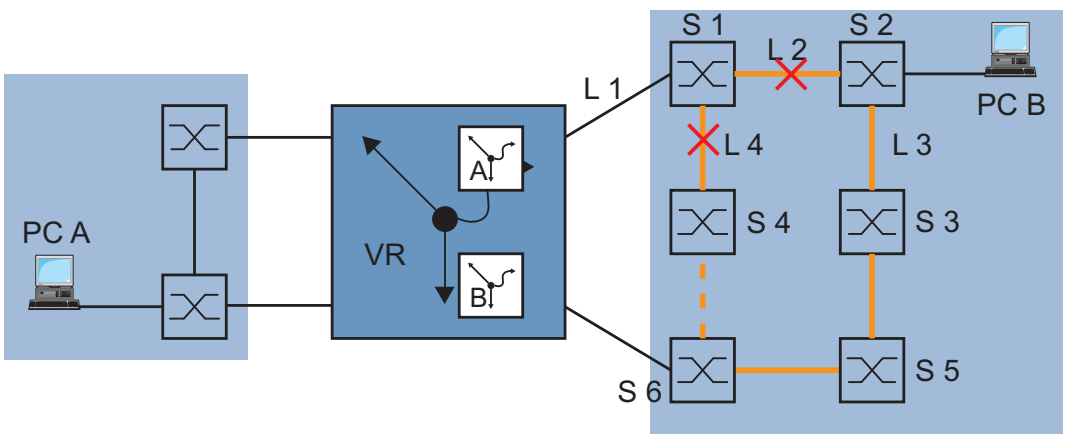


Abb. 18: Überwachen der Erreichbarkeit eines Gerätes in einem redundanten Ring

☐ Logical-Tracking-Objekt als ODER-Verknüpfung einrichten.

☐ Klicken Sie im Dialog `Routing:Tracking:Konfiguration` auf „Assistent“ rechts unten.

Typ auswählen:

☐ Tragen Sie die gewünschten Werte ein:

Track ID:	`31`
Typ:	`Logical`

☐ Klicken Sie auf „Weiter“.

Eigenschaften:

☐ Tragen Sie die gewünschten Werte ein:

Operator:	or
Operand 1 (Track-ID):	21
Operand 2 (Track-ID):	22

☐ Klicken Sie auf „Fertig“, um den Assistenten zu beenden und den Eintrag in der Konfiguration flüchtig zu speichern.

```
enable                              Wechsel in den Privileged-EXEC-Modus.
configure                           Wechsel in den Konfigurationsmodus.
track 31 logical or 21 22           Eingabe der Tracking-Parameter und Aktivieren
                                    dieses Tracking-Objektes.
Tracking ID 31 created
  Tracking type set to Logical
  Logical Operator set to or
  Logical Instance 21 included
  Logical Instance 1 included
Tracking ID 31 activated
exit                                Wechsel in den Privileged-EXEC-Modus.
show track                          Anzeige der konfigurierten Tracks
Ping Tracking
                                                 No. of   Time since
  ID Type IP Address  Intvl Status Mode Changes  last change
 --- ---- ----------- ----- ------ ------ ------- -----------------
  21 Ping  10.0.2.53    1s  DOWN   Enable   1    0 day(s), 00:13:39

Ping Tracking
                                                 No. of   Time since
  ID Type IP Address  Intvl Status Mode Changes  last change
 --- ---- ----------- ----- ------ ------ ------- -----------------
  22 Ping  10.0.2.54    1s  DOWN   Enable   1    0 day(s), 00:14:39

Logical Tracking
                                      No. of
 ID Type  Instances  Status  Mode    Changes Time since last change
--- ---- ----------- ------ ------- ------- ---------------------
 31  OR  21,22       DOWN   Enable        0   0 day(s), 00:04:58
```

5 VRRP/HiVRRP

Endgeräte bieten in der Regel die Möglichkeit, ein Default-Gateway für die Vermittlung von Datenpaketen in fremde Subnetze einzutragen. An dieser Stelle bezeichnet der Begriff „Gateway” einen Router, über den das Endgerät in andere Subnetze kommunizieren kann.

Beim Ausfall dieses Routers kann das Endgerät keine Daten mehr in fremde Subnetze senden.
In diesem Fall hilft das Virtual Router Redundancy Protocol (VRRP).
VRRP ist eine Art „Gateway-Redundanz”. VRRP beschreibt ein Verfahren, das mehrere Router zu einem virtuellen Router zusammenfasst. Endgeräte adressieren immer an den virtuellen Router und VRRP sorgt dafür, dass ein physikalischer Router, der dem virtuellen Router angehört, die Vermittlung übernimmt.
Selbst wenn ein physikalischer Router ausfällt, sorgt VRRP dafür, dass ein anderer physikalischer Router als Teil des virtuellen Routers die Vermittlungsaufgaben übernimmt.

VRRP hat beim Ausfall eines physikalischen Routers typische Umschaltzeiten von 3 bis 4 Sekunden.
In vielen Fällen, z.B. Voice over IP, Video over IP, industriellen Steuerungen, usw. sind diese langen Umschaltzeiten nicht akzeptabel.

Die Firma Hirschmann hat das VRRP weiterentwickelt zum Hirschmann Virtual Router Redundancy Protocol (HiVRRP).
HiVRRP garantiert bei entsprechender Konfiguration Umschaltzeiten von höchstens 400 Millisekunden.
HiVRRP ermöglicht dank der garantierten Umschaltzeit den Einsatz der „Gateway-Redundanz” in zeitkritischen Anwendungen. Selbst in Tunnelsteuerungen, die Umschaltzeiten von weniger als einer Sekunde fordern, kann der Anwender die Netzverfügbarkeit durch diese Form der „Gateway-Redundanz” erhöhen.

5.1 VRRP

Alle Router innerhalb eines Netzes auf denen VRRP aktiv ist, regeln unter einander, welcher dieser Router der Master sein soll. Dieser erhält die IP- und die MAC-Adresse des virtuellen Routers. Alle Geräte im Netz, die als „Default Gateway“ diese virtuelle IP-Adresse eingetragen haben, benutzen den Master als Default Gateway.

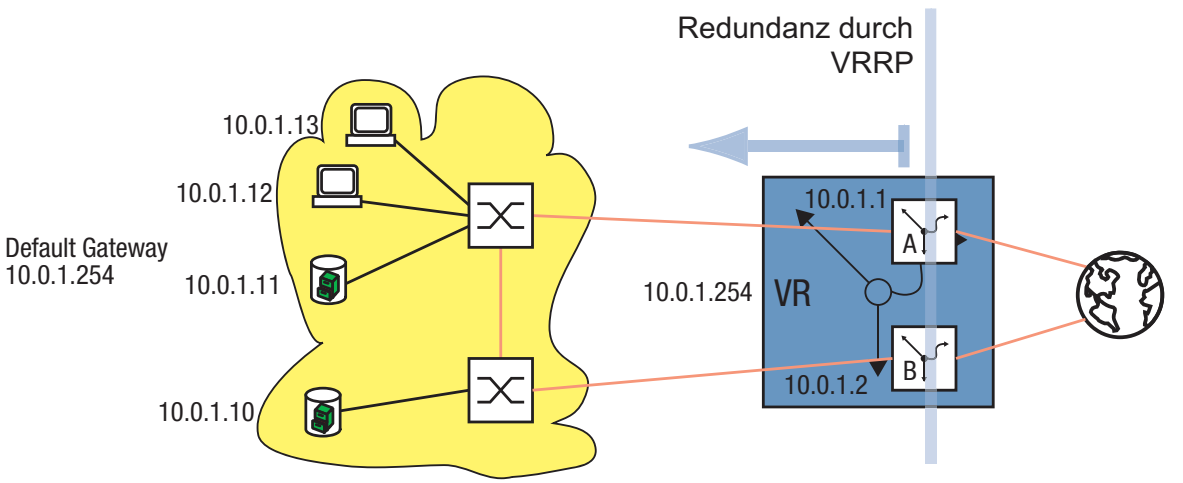


Abb. 19: Darstellung des virtuellen Routers

Fällt der Master aus, dann regeln die verbliebenen Router mit VRRP unter-einander, wer neuer Master wird. Dieser übernimmt dann die IP- und die MAC-Adresse des virtuellen Routers. Somit finden die Geräte über ihr „Default Gateway“ nach wie vor ihre Route. Die Geräte sehen immer nur den Master mit der virtuellen MAC- und IP-Adresse unabhängig davon, welcher Router sich tatsächlich hinter dieser virtuellen Adresse verbirgt.
Die virtuelle Router IP-Adresse vergibt der Administrator.
Die virtuelle MAC-Adresse gibt das VRRP vor mit:
00:00:5e:00:01:<VRID>.
Die ersten 5 Octets bilden laut RFC 2338 den festen Bestandteil.
Das letzte Octet ist die virtuelle Router-ID (VRID). Sie ist eine Zahl zwischen 1 und 255. Demnach kann der Administrator innerhalb eines Netzes 255 virtuelle Router definieren.

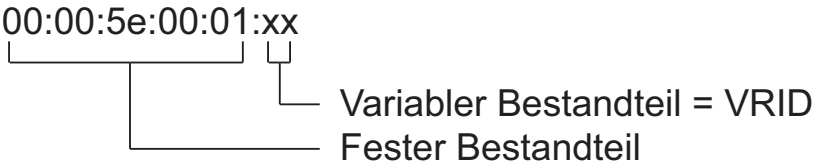


Abb. 20: Virtuelle MAC-Adresse

Die VRRP-Router senden IP-Multicast-Nachrichten an die IP-Multicast-Adresse 224.0.0.18, um den Master zu ermitteln. Master wird der Router mit der höchsten VRRP-Priorität. Die VRRP-Priorität legt der Administrator fest. Bei gleicher VRRP-Priorität entscheidet die höchste IP-Interface-Adresse der beteiligten VRRP-Router.
Ist die virtuelle IP-Adresse identisch mit der IP-Adresse eines Router-Interfaces, dann ist dieser Router der IP-Address-Owner. VRRP setzt die VRRP-Priorität eines IP-Address-Owners auf den Wert 255 und deklariert ihn auf diese Weise zum Master. Ist kein IP-Address-Owner vorhanden, dann deklariert VRRP den Router mit der höchsten VRRP-Priorität zum Master.

Der Master schickt regelmäßig (voreingestellt: 1 s) IP-Multicast-Nachrichten an die anderen VRRP-Router, um ihnen seine Betriebsbereitschaft zu signalisieren. Bleibt diese Nachricht zum dritten Mal in Folge aus, dann erklärt sich der VRRP-Router mit der höchsten verbleibenden VRRP-Priorität zum neuen Master.

1.	IP-Address-Owner, da er per Definition die höchste VRRP-Priorität (255) hat.
2.	Der VRRP-Router mit der höchsten VRRP-Priorität.
3.	Bei gleicher Priorität der VRRP-Router mit der höchsten IP-Adresse.

Tab. 4: Wer wird Master?

VRRP-Begriffe:

- Virtueller Router
  Ein virtueller Router ist ein oder eine Gruppe von Routern, die als default Gateway in einem Netz agieren und das Virtual Router Redandancy Protocol anwenden.
- VRRP-Router
  Ein VRRP-Router ist ein Router, der VRRP anwendet. Er kann Teil eines oder mehrerer virtueller Router sein.
- Master-Router
  Der Master-Router ist der Router innerhalb des virtuellen Routers, der gerade verantwortlich ist für die Weiterleitung von Datenpaketen und beantwortet ARP-Anfragen. Der Master-Router sendet periodisch Nachrichten (Advertisements) an die anderen VRRP-Router (Backup-Router), um diese über seine Existenz zu informieren.
- IP-Address-Owner
  Der IP-Address-Owner ist der VRRP-Router, dessen IP-Adresse identisch ist mit der IP-Adresse des virtuellen Routers. Per Definition hat er die höchste VRRP-Priorität (255) und ist somit automatisch Master-Router.
- Backup-Router
  Der Backup-Router ist ein VRRP-Router, der nicht Master-Router ist. Ein Backup-Router hält sich bereit, die Master-Rolle zu übernehmen, falls der Master ausfällt.
- VRRP-Priorität
  Die VRRP-Priorität ist eine Zahl zwischen 1 und 255. Sie dient der Bestimmung des Master-Routers. Der Wert 255 ist reserviert für den IP-Address-Owner.
- VRID
  Die VRID (virtueller Router Identifikation) zur eindeutigen Kennzeichnung eines virtuellen Routers.
- Virtuelle Router MAC-Adresse
  Die virtuelle Router MAC-Adresse ist die MAC-Adresse des virtuellen Routers (siehe Abbildung 20).
- Virtuelle Router IP-Adresse
  Die virtuelle Router-IP-Adresse ist die IP-Adresse des virtuellen Routers.

- Advertisement-Intervall
  Das Advertisement-Intervall beschreibt die Häufigkeit, mit der der Master-Router seine Existenznachricht (Advertisement) an alle VRRP-Router seines virtuellen Routers verschickt. Die Werte für das Advertisement-Intervall liegen zwischen 1 und 255 Sekunden. Voreingestellt ist der Wert 1 Sekunde.
- Skew-Time
  Die Skew-Time ist der von der VRRP-Priorität abhängige Zeitanteil, der den Zeitpunkt bestimmt, zu welchem der Backup-Router sich zum Master-Router erklärt.
  Skew-Time = ((256 - VRRP-Priorität) / 256) · 1 Sekunde
- Master-Down-Intervall
  Das Master-Down-Intervall bestimmt den Zeitpunkt, zu welchem sich der Backup-Router zum Master-Router erklärt.
  Master-Down-Intervall = 3 · Advertisement-Intervall + Skew-Time

5.1.1 Konfiguration von VRRP

Die Konfiguration von VRRP erfordert folgende Schritte:

- Routing global einschalten (falls nicht schon geschehen).
- VRRP global einschalten.
- Port konfigurieren – IP-Adresse, Netzmaske zuweisen.
- Routing am Port einschalten.
- Virtuelle Router ID (VRID) anlegen, da Sie die Möglichkeit haben, mehrere virtuelle Router pro Port zu aktivieren.
- Virtuelle Router-IP-Adresse zuweisen.
- Virtuellen Router einschalten.
- VRRP-Priorität zuweisen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip routing`	Router-Funktion global einschalten.
`ip vrrp`	VRRP global einschalten.
`interface 2/3`	Auswahl des Ports zum Einrichten von VRRP.
`ip address 10.0.1.1 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Interface.
`ip vrrp 1`	Anlegen der VRID für den ersten virtuellen Router an diesem Port.
`ip vrrp 1 mode`	Einschalten des ersten virtuellen Routers an diesem Port.
`ip vrrp 1 ip 10.0.1.100`	Dem virtuellen Router 1 seine IP-Adresse zuweisen.
`ip vrrp 1 priority 200`	Dem virtuellen Router 1 die Routerpriorität 200 zuweisen.

☐ Konfigurieren Sie jeden Port, an dem VRRP aktiv sein soll, auf die gleiche Weise.

☐ Nehmen Sie die gleiche Konfiguration auch auf dem redundanten Router vor.

5.2 HiVRRP

HiVRRP bietet mehrere Mechanismen, um die Umschaltzeiten zu verkürzen oder die Anzahl der Multicasts zu reduzieren:

- kürzere Advertisement-Intervalle
- Verbindungsunterbrechungs-Meldung
- Preempt-Verzögerung
- Unicast Advertisement
- Domänen

Konform zu RFC 2338 verschickt der Master im Sekundentakt eine IP-Multicast-Nachricht (Advertisement) an die anderen VRRP-Router. Erst wenn diese Nachricht zum dritten Mal ausbleibt, wählen die verbleibenden Router einen neuen Master.
VRRP hat Umschaltzeiten von typisch 3 bis 4 Sekunden.

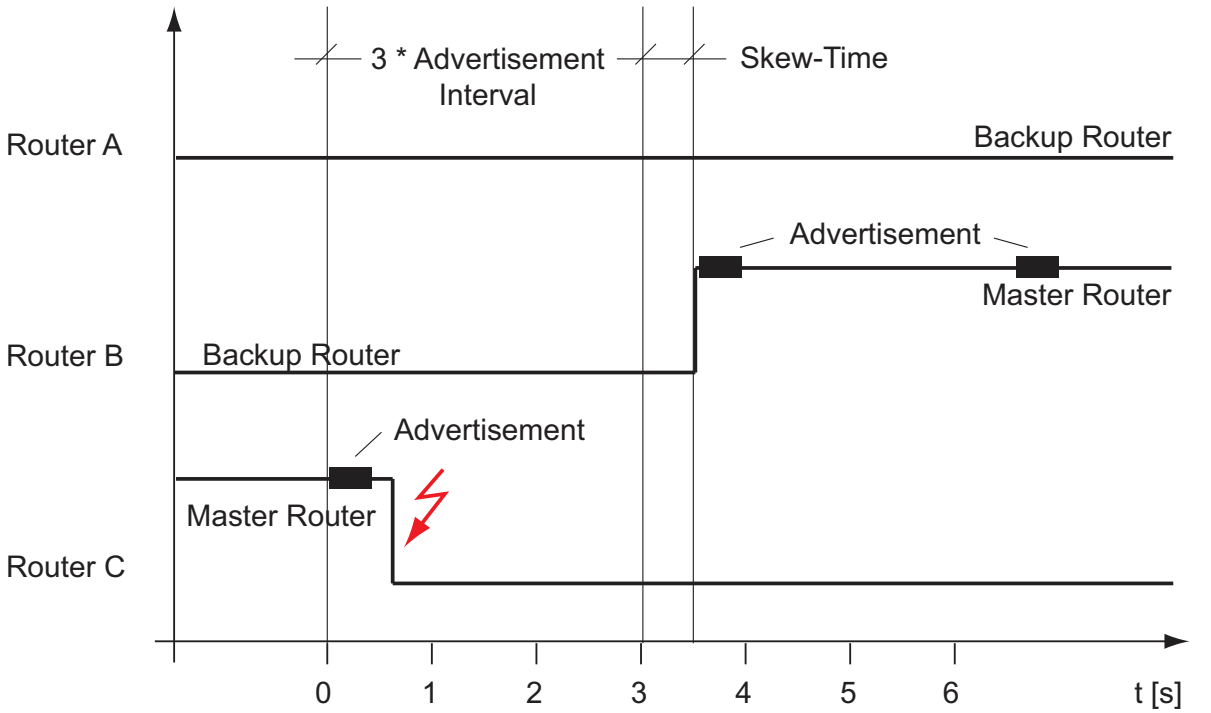


Abb. 21: Umschaltzeiten Master-Router <-> Backup-Router nach RFC 2338
VRRP-Priorität Router A = 64
VRRP-Priorität Router B = 128
VRRP-Priorität Router C = 254

Um schnellere Umschaltzeiten realisieren zu können, bietet Hirschmann mit HiVRRP die Möglichkeit, den Zyklus für das Versenden der IP-Multicast-Nachricht zu verkürzen auf bis zu 0,1 Sekunden. So können Sie bis zu 10-mal schnellere Umschaltzeiten erzielen.

Der Router unterstützt bis zu 16 VRRP-Router-Interfaces mit diesem verkürzten Sendezyklus.

- HiVRRP-Skew-Time
  Die HiVRRP-Skew-Time ist der von der VRRP-Priorität abhängige Zeitanteil, der den Zeitpunkt bestimmt, zu welchem der HiVRRP-Backup-Router sich zum HiVRRP-Master-Router erklärt.
  HiVRRP-Skew-Time =
  (256 - VRRP-Priorität) / 256 · Advertisement-Intervall
  Zeitangaben in Millisekunden
- HiVRRP-Master-Down-Intervall
  Das HiVRRP Master-Down-Intervall bestimmt den Zeitpunkt, zu welchem sich der HiVRRP-Backup-Router zum HiVRRP-Master-Router erklärt.
  HiVRRP-Master-Down-Intervall =
  3 · Advertisement-Intervall + HiVRRP-Skew-Time
  Zeitangaben in Millisekunden

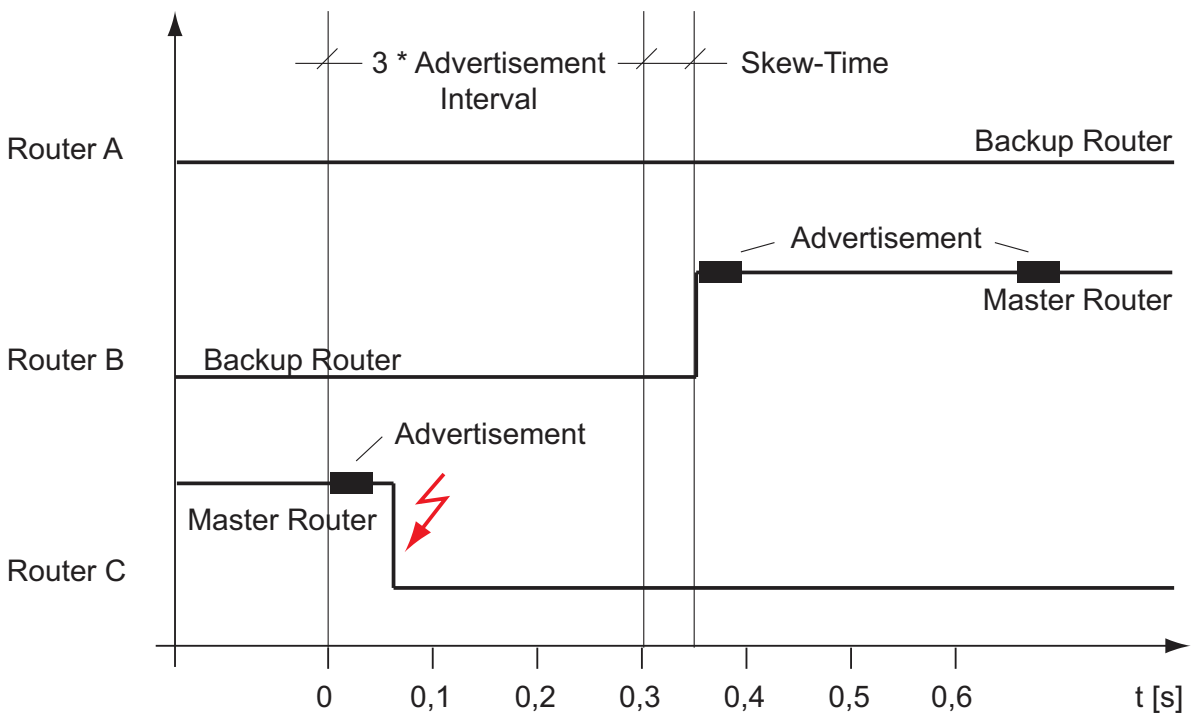


Abb. 22: Umschaltzeiten Master-Router <-> Backup-Router nach HiVRRP
VRRP-Priorität Router A = 64
VRRP-Priorität Router B = 128
VRRP-Priorität Router C = 254

Eine weitere Möglichkeit, die Umschaltzeit dramatisch zu verkürzen, bietet Ihnen HiVRRP mit der Verbindungsunterbrechungs-Meldung (Link-Down Meldung). Diese Funktion können Sie nutzen, wenn der virtuelle Router aus 2 VRRP-Routern besteht. Da 2 VRRP-Router beteiligt sind, genügt das Versenden der Verbindungsunterbrechungs-Meldung in Form einer Unicast-Nachricht. Im Gegensatz zur Multicast-Nachricht gelangt die Unicast-Nachricht über Subnetzgrenzen hinweg. Das bedeutet, dass bei einer Unterbrechung zum eigenen Subnetz die Verbindungsunterbrechungs-Meldung auch über ein anderes Subnetz zum zweiten Router des virtuellen Routers gelangen kann.
Sobald HiVRRP eine Verbindungsunterbrechung erkennt, schickt HiVRRP die Verbindungsunterbrechungs-Meldung über einen anderen Weg an den zweiten Router. Der zweite Router übernimmt sofort nach dem Erhalt der Verbindungsunterbrechungs-Meldung die Master-Funktion.

Im Preempt-Modus kann der Backup-Router dem Master-Router die Master-Funktion entziehen, sobald der Backup-Router vom Master-Router ein Advertisement empfängt, dessen VRRP-Priorität kleiner ist als seine eigene. So kann der Preempt-Modus im Zusammenwirken mit VRRP-Tracking (siehe auf Seite 73 „VRRP-Tracking“) das Umschalten auf einen besseren Router ermöglichen. Dynamische Routing-Verfahren benötigen aber eine gewisse Zeit, auf geänderte Routen zu reagieren und ihre Routingtabelle neu zu befüllen.
Um während dieser Zeit Paketverluste zu vermeiden, bietet die verzögerte Umschaltung (Preempt-Verzögerung) vom Master- auf den Backup-Router den dynamischen Routingverfahren die Möglichkeit, ihre Routingtabellen zu befüllen.

Für Netze mit Geräten, die mit hohem Aufkommen von Multicasts Probleme haben, bietet HiVRRP einen weiteren Vorteil. Anstatt Advertisements in Form von Multicasts zu verschicken, kann HiVRRP beim Einsatz von bis zu 2 HiVRRP-Routern die Advertisements in Form von Unicast-Datenpaketen (VRRP-Zieladresse) verschicken.

Anmerkung: Wenn Sie die Vorteile von HiVRRP nutzen wollen, dann verwenden Sie für einen virtuellen Router ausschließlich VRRP-Router, die über die HiVRRP-Funktion von Hirschmann verfügen.

5.3 HiVRRP-Domäne

Bei großen flachen Netzstrukuren bieten Ihnen die HiVRRP-Domänen die Möglichkeit,

- im Redundanzfall alle HiVRRP-Router in kürzester Zeit umzuschalten,
- die verfügbare Bandbreite effektiver zu nutzen,
- mehr als 16 VRRP-Router-Interfaces pro Router mit HiVRRP zu konfigurieren.
- multicastempfindliche Endgeräte in großen HiVRRP-Netzen zu betreiben.

Eine HiVRRP-Instanz ist ein als HiVRRP konfiguriertes Router-Interface mit Funktionen, die das HiVRRP beinhaltet. In einer HiVRRP-Domäne fassen Sie mehrere HiVRRP-Instanzen eines Routers zu einer Verwaltungseinheit zusammen. Eine HiVRRP-Instanz ernennen Sie zum Supervisor der HiVRRP-Domäne. Dieser Supervisor regelt das Verhalten aller HiVRRP-Instanzen seiner Domäne.

- Der Supervisor verschickt seine Advertisements stellvertretend für alle HiVRRP-Instanzen seiner Domäne.
- Der Supervisor schaltet sich und die anderen HiVRRP-Instanzen zusammen in die Master-Rolle oder die Backup-Rolle.

Die Abbildung 23 zeigt ein Beispiel für eine flache Netzstruktur. Alle VLAN-übergreifenden Datenströme passieren den Ring.

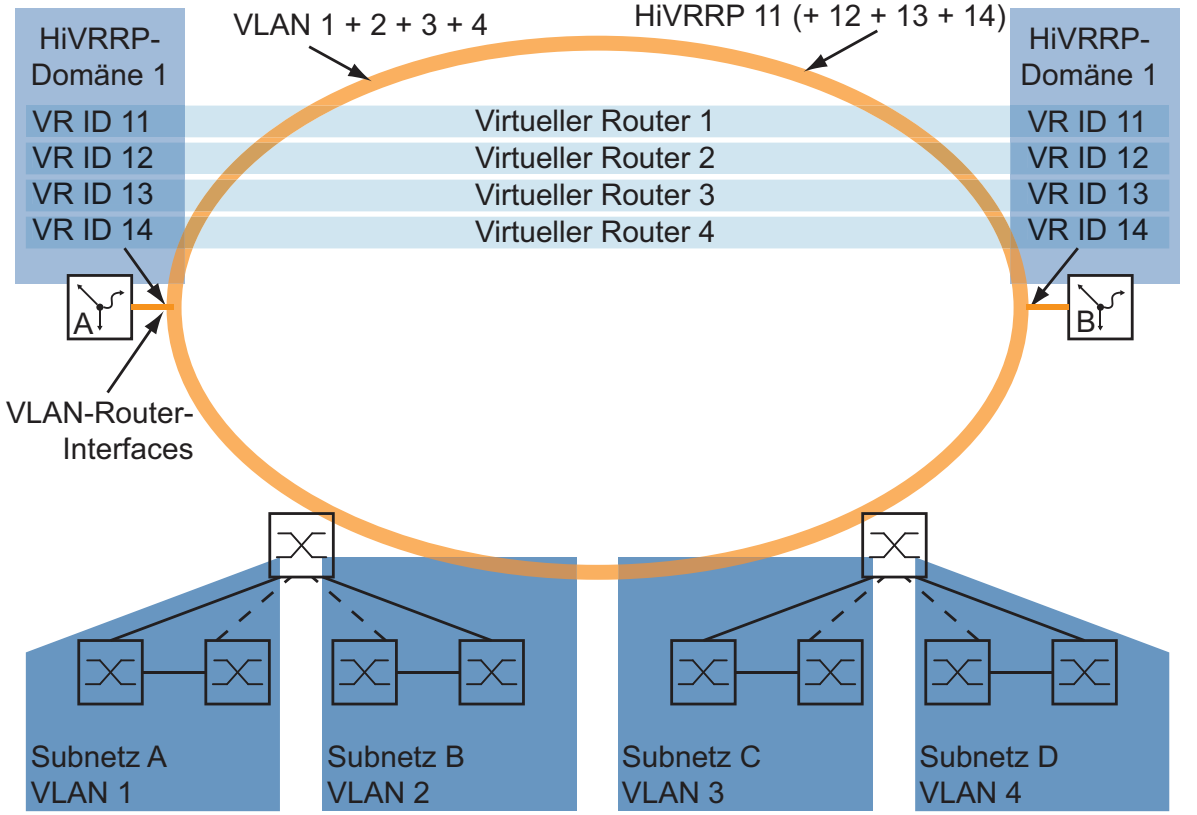


Abb. 23: Beispiel für die Anwendung einer HiVRRP-Domäne

5.3.1 Konfiguration von HiVRRP-Domänen

Die Konfiguration von HiVRRP-Domänen umfasst folgende Schritte:

- VLANs anlegen
- VLAN-Router-Interfaces konfigurieren
- Den Router-Interfaces ihre IP-Adressen zuweisen
- HiVRRP-Instanzen konfigurieren
  - VRRP-Instanz einschalten (alle Instanzen)
  - IP-Adresse zuweisen (alle Instanzen)
    Innerhalb eines Routers entweder alle Instanzen als IP-Address-Owner konfigurieren oder keine Instanz als IP-Address-Owner konfigurieren.

  - Priorität zuweisen (Supervisor)
    Den Supervisoren unterschiedliche Prioritäten zuweisen, damit die VRRP-Router sich auf einen Master-Router einigen können.
  - HiVRRP einschalten (alle Instanzen)
  - Der Domäne zuweisen (alle Instanzen)
  - Sende-Intervall festlegen (Supervisor)

- HIPER-Ring konfigurieren (in Anwendungen wie im Beispiel oben)
- (Ring-)Ports als Member der VLANs definieren
- Routing und VRRP global einschalten

5.3.2 Beispiel für die Konfiguration von HiVRRP-Domänen

Beispiel möglicher Einstellungen für die Anwendung in Abbildung 23:

Subnetz	IP-Adress-Bereich	VLAN	VLAN ID
A	10.0.11.0/24	1	11
B	10.0.12.0/24	2	12
C	10.0.13.0/24	3	13
D	10.0.14.0/24	4	14

Tab. 5: Konfiguration der Switche im Subnetz

Virueller Router	VR ID	IP-Adresse des Virtuellen Routers	Router-Interface von Router A: IP-Adresse	Router-Interface von Router B: IP-Adresse	VLAN ID
1	11	10.0.11.1/24	10.0.11.2/24	10.0.11.3/24	11
2	12	10.0.12.1/24	10.0.12.2/24	10.0.12.3/24	12

Tab. 6: Konfiguration der beiden Router

Virueller Router	VR ID	IP-Adresse des Virtuellen Routers	Router-Interface von Router A: IP-Adresse	Router-Interface von Router B: IP-Adresse	VLAN ID
3	13	10.0.13.1/24	10.0.13.2/24	10.0.13.3/24	13
4	14	10.0.14.1/24	10.0.14.2/24	10.0.14.3/24	14

Tab. 6: Konfiguration der beiden Router

☐ VLAN-Router-Interface konfigurieren und IP-Adresse zuweisen:

```
enable
```
Wechsel in den Privileged-EXEC-Modus.

```
vlan database
```
Wechsel in den VLAN-Modus.

```
vlan 11
```
Anlegen eines VLANs durch Eingabe der VLAN-ID.

```
vlan name 11 VLAN1
```
Dem VLAN 11 den Namen „VLAN1” zuweisen.

```
vlan routing 11
```
Erzeugen eines virtuellen Router-Interfaces und Einschalten der Router-Funktion an diesem Interface.

```
exit
```
Wechsel in den Privileged-EXEC-Modus.

```
show ip vlan
```
Anzeigen des virtuelles-Router-Interfaces, das der Router für das VLAN eingerichtet hat.

```
show ip vlan          Logical
VLAN ID  Interface    IP Address    Subnet Mask     MAC Address
-------  ----------   -----------   -------------   ------------
11       9/1          0.0.0.0       0.0.0.0         00:80:63:51:74:2C
```

```
show ip interface brief
```
Prüfung des Eintrags des virtuellen Router-Interfaces.

```
                                                Netdir    Multi
Interface IP Address       IP Mask              Bcast     CastFwd
--------- ---------------- -------------------- --------- ---------
9/1       0.0.0.0          0.0.0.0              Disable   Disable
```

```
configure
```
Wechsel in den Konfigurationsmodus.

```
interface 9/1
```
Wechsel in den Interface-Konfigurations-Modus von Interface 9/1.

```
ip address 10.0.11.2
  255.255.255.0
```
Dem Interface seine IP-Parameter zuweisen.

```
routing
```
Einschalten der Router-Funktion an diesem Interface.

☐ Virtuellen Router einrichten und Port konfigurieren

`ip vrrp 1`	Anlegen der VRID für den ersten virtuellen Router an diesem Port.
`ip vrrp 1 priority 200`	Dem virtuellen Router 1 die Routerpriorität 200 zuweisen.
`ip vrrp 1 mode`	Einschalten des ersten virtuellen Routers an diesem Port.
`ip vrrp 1 ip 10.0.11.1`	Dem viruellen Router 1 seine IP-Adresse zuweisen
`ip vrrp 1 domain 1 supervisor`	Dem Interface die HiRRP-Domäne und die Domänen-Rolle zuweisen.
`ip vrrp 1 timers advertise milliseconds 100`	Dem Interface das HiVRRP Nachrichten-Intervall zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.

`show ip vrrp interface 9/1 1` Anzeige der Konfiguration von VLAN 11

```
Primary IP Address.............................. 10.0.11.1
VMAC Address.................................... 00:00:5e:00:01:01
Authentication Type............................. None
Base Priority................................... 200
Advertisement Interval (milliseconds).......... 100
Pre-empt Mode................................... Enable
Administrative Mode............................. Enable
State........................................... Initialized
Current Priority................................ 200
Preeption Delay (seconds)....................... 0
Link Down Notification.......................... Disabled
VRRP Domain..................................... 1
VRRP Domain Role................................ Supervisor
VRRP Domain State............................... Supervisor is down
Advertisement Address........................... 224.0.0.18
```

☐ (Ring-)Port als Member des VLANs konfigurieren

`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/1.
`vlan participation include 11`	Das Interface dem VLAN zuordnen.
`exit`	Wechsel in den Konfigurationsmodus.

```
exit                                  Wechsel in den Privileged-EXEC-Modus.
show vlan 11                          Anzeige der Konfiguration von VLAN 11
```

```
VLAN ID           : 11
VLAN Name         : VLAN1
VLAN Type         : Static
VLAN Creation Time: 0 days, 00:00:06 (System Uptime)

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Exclude   Autodetect   Untagged
1/2         Exclude   Autodetect   Untagged
1/3         Exclude   Autodetect   Untagged
1/4         Exclude   Autodetect   Untagged
2/1         Include   Include      Untagged
2/2         Exclude   Autodetect   Untagged
2/3         Exclude   Autodetect   Untagged
2/4         Exclude   Autodetect   Untagged
3/1         Exclude   Autodetect   Untagged
3/2         Exclude   Autodetect   Untagged
9/1         Exclude   Autodetect   Untagged
```

Routing und VRRP global einschalten

```
enable                                Wechsel in den Privileged-EXEC-Modus.
configure                             Wechsel in den Konfigurationsmodus.
ip routing                            Router-Funktion global einschalten.
ip vrrp                               VRRP global einschalten.
```

5.4 VRRP-Tracking

Durch die Überwachung bestimmter Router-Zustände (z.B. Leitungsunterbrechung) ermöglicht VRRP-Tracking beim Ausfall einer Verbindung das Umschalten auf einen besseren Router.

Bei einer Leitungsunterbrechung zwischen Switch S1 und Router A (siehe Abbildung 25) übernimmt Router B die Masterfunktion für den virtuellen Router 10.0.1.254.
Für den virtuellen Router 10.0.2.254 bleibt Router A Master. Router A hat aber keine Verbindung mehr in das Subnetz 10.0.1.0.
Die virtuellen Router-Interfaces sind unabhängig voneinander.

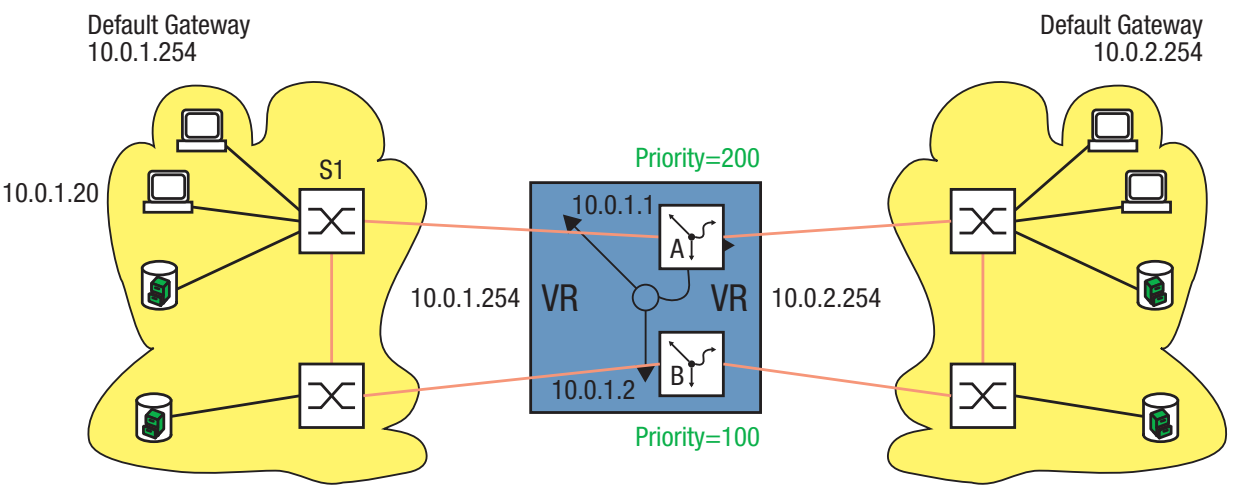


Abb. 24: Typische VRRP-Anwendung

Sobald der VRRP-Master-Router mit aktiver VRRP-Tracking-Funktion eine Unterbrechung einer seiner Verbindung erkennt, setzt er seine VRRP-Priorität herunter und teilt diese den anderen VRRP-Routern mit.
Daraufhin kann ein anderer VRRP-Router, der auf Grund der veränderten Situation nun die höchste VRRP-Priorität hat, schon innerhalb der Skew-Time die Master-Funktion übernehmen.

Lösung ohne Tracking:
Konfigurieren Sie Router A mit einer statischen Route zu Router B oder mit einem dynamischen Routing-Verfahren, damit Router A eine Route in das Subnetz 10.0.1.0 findet.
Die direkte Verbindung mit der Präferenz 0 ist die beste Route.
Die statische Route mit der Präferenz 1 ist die zweitbeste Route. Danach folgt die dynamische Route.

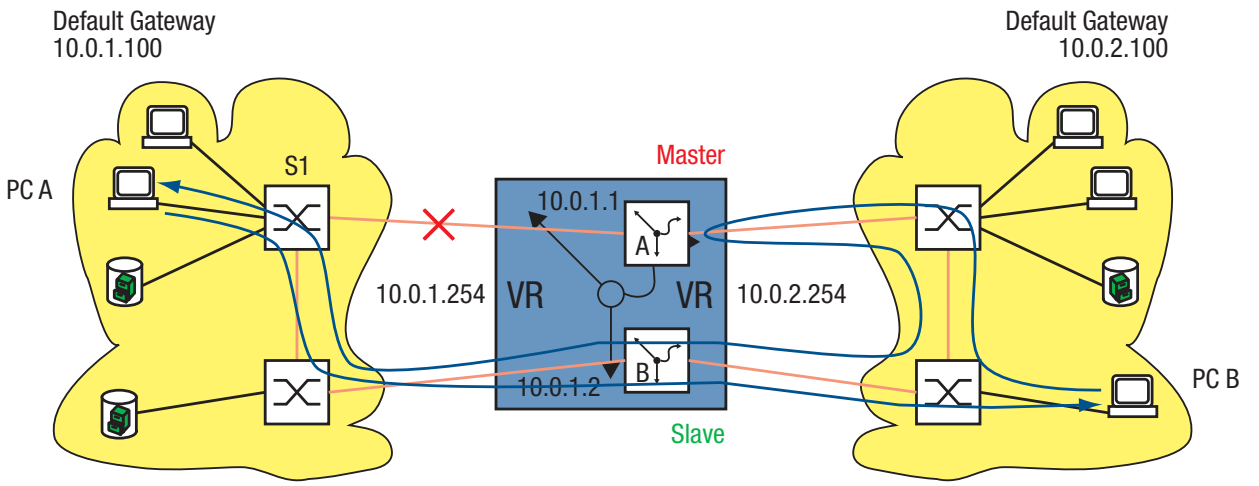


Abb. 25: Übertragungsweg von PC B zu PC A bei Leitungsunterbrechung ohne Tracking

Die Daten von PC B gelangen dann über den Umweg Router A und Router B zu PC A.

Lösung mit Tracking:
Für eine optimale Routenführung können Sie nun mit Hilfe der Tracking-Funktion auch den Router B für den virtuellen Router 10.0.2.254 zum Master werden lassen.
Durch das „Tracken" der unterbrochenen Verbindung und das Registrieren der Virtuellen Router für dieses Tracking-Objekt (siehe auf Seite 45 „Tracking") dekrementiert der Router A seine VRRP-Priorität. Somit erkennt Router B beim Empfang des nächsten Advertisements von Router A, dass seine eigene VRRP-Priorität höher ist als die von Router A und übernimmt die Master-Funktion (siehe Abbildung 26).

Anmerkung: Da der IP-Adress-Owner per Definition die feste VRRP-Priorität 255 besitzt, setzt die VRRP-Tracking-Funktion voraus, dass die IP-Adressen der VRRP-Router-Interfaces ungleich der virtuellen Router-IP-Adresse sind.

Anmerkung: Damit der Backup-Router dem Master-Router mit niedriger Priorität die Master-Funktion entziehen kann, setzt die VRRP-Tracking-Funktion das Einschalten des Preempt-Modus´ voraus.

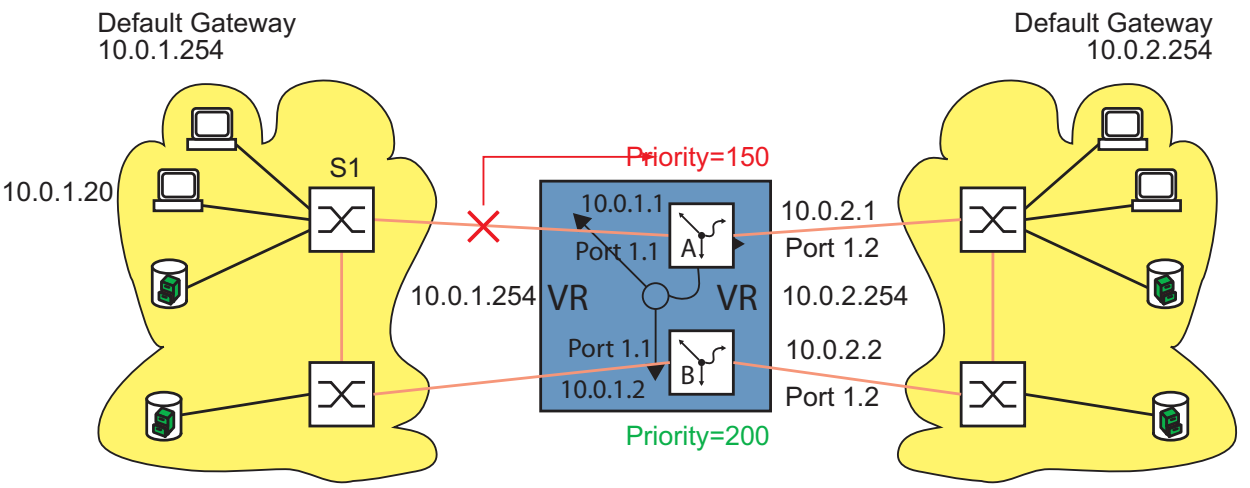


Abb. 26: VRRP-Tracking nach einer Leitungsunterbrechung

	Router A	Router A	Router B	Router B
Interface	1.1	1.2	1.2	1.1
IP-Adresse	10.0.1.1/24	10.0.2.1/24	10.0.2.2/24	10.0.1.2/24
VRID	1	2	2	1
VRRP-IPAdresse	10.0.1.254	10.0.2.254	10.0.2.254	10.0.1.254
VRRP-Priorität	250	250	200	200
VRRP-Preemption	Enabled	Enabled	Enabled	Enabled
Track ID	2	1	-	-
Track Decrement	100	100	-	-

Tab. 7: VRRP-Tracking-Konfiguration für das Beispiel oben

	Router A	Router A	Router B	Router B
Track ID	1	2	-	-
Typ	Interface	Interface	-	-
Interface	1.1	1.2	-	-

Tab. 8: Tracking-Konfiguration für das Beispiel oben

Die Konfiguration von VRRP-Tracking erfordert folgende Schritte:

- Tracking-Objekt konfigurieren
  (siehe auf Seite 51 „Tracking konfigurieren“).
- VRRP konfigurieren.
- Dem VRRP-Eintrag die Track ID hinzufügen (= VRRP-Eintrag für das Tracking-Objekt registrieren).

☐ Interface-Tracking am Port 1.1 mit einer Link-Down-Verzögerung von 0 Sekunden und einer Link-Up-Verzögerung von 3 Sekunden einrichten.

☐ Klicken Sie im Dialog `Routing:Tracking:Konfiguration` auf „Assistent“ rechts unten.

Typ auswählen:

☐ Tragen Sie die gewünschten Werte ein:

Track ID:	`1`
Typ:	`interface`

☐ Klicken Sie auf „Weiter“.

Eigenschaften:

☐ Tragen Sie die gewünschten Werte ein:

Modul.Port:	`1.1`
Link-Up-Verzögerung:	`3`
Link-Down-Verzögerung:	`0`

☐ Klicken Sie auf „Fertig“, um den Assistenten zu beenden und den Eintrag in der Konfiguration flüchtig zu speichern.

```
enable
configure
track 1 interface 1/1
  link-down-delay 0
  link-up-delay 3
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Eingabe der Tracking-Parameter und Aktivieren dieses Tracking-Objektes.

☐ Routing und VRRP global einschalten.

☐ Wählen Sie den Dialog `Routing:Global`.
☐ Markieren Sie „Routing“.
☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.
☐ Wählen Sie den Dialog `Redundanz:VRRP/HiVRRP:Konfiguration`.
☐ Markieren Sie „Funktion“.
☐ Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

```
ip routing
ip vrrp
```

Router-Funktion global einschalten.
VRRP global einschalten.

☐ IP-Adresse und VRRP am Port 1.2 konfigurieren.

☐ Klicken Sie im Dialog `Redundanz:VRRP/HiVRRP:Konfiguration` auf „Assistent“ rechts unten.

Eintrag erzeugen:

☐ Tragen Sie die gewünschten Werte ein:

„Modul“:	`1`
„Port“:	`2`
„VRID“:	`2`

☐ Klicken Sie auf „Weiter“.

Eintrag bearbeiten:

☐ Tragen Sie die gewünschten Werte ein:

„VRRP IP-Adresse“:	`10.0.2.254`
„Priorität“:	`250`
„Preempt-Modus“:	`1`

☐ Klicken Sie auf „Weiter“.

`interface 1/2`	Auswahl des Ports zum Einrichten von VRRP.
`ip address 10.0.2.1 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Port .
`ip vrrp 2`	Anlegen der VRID für den ersten virtuellen Router an diesem Port.
`ip vrrp 2 mode`	Einschalten des ersten virtuellen Routers an diesem Port.
`ip vrrp 2 ip 10.0.2.254`	Dem virtuellen Router 1 seine IP-Adresse zuweisen.
`ip vrrp 2 priority 250`	Dem virtuellen Router 1 die Routerpriorität 250 zuweisen.

☐ VRRP für das Tracking-Objekt registrieren.

Tracking

☐ Tragen Sie die gewünschten Werte ein:

„Track-ID“:	`1`
„Decrement“:	`100`

☐ Klicken Sie auf „Hinzufügen“.

☐ Klicken Sie auf „Weiter“.

☐ Klicken Sie auf „Fertig“, um den Assistenten zu beenden und den Eintrag in der Konfiguration flüchtig zu speichern.

`ip vrrp 2 track 1 decrement 100`	Den ersten VRRP-Eintrag für das Tracking-Objekt registrieren.
`exit`	Wechsel in den Konfigurationsmodus.

```
exit                                  Wechsel in den Privileged-EXEC-Modus.
show track applications               Anzeige der registrierten Anwendungen.
TrackId  Application                    Changes  Time since last change
-------  ---------------------------  -------  ----------------------
1        VRRP 1/2 VRID: 2                 0      0 day(s), 00:38:24
```

☐ Nehmen Sie die gleiche Konfiguration auch auf dem redundanten Router vor.

5.5 VRRP mit Load Sharing

Bei der einfachen Konfiguration übernimmt ein Router die Gateway-Funktion für alle Endgeräte. Die Kapazität des redundanten Routers liegt brach. VRRP bietet Ihnen die Möglichkeit, die Kapazität des redundanten Routers mit zu nutzen. Durch das Einrichten mehrerer virtueller Router können Sie den angeschlossenen Endgeräten unterschiedliche „Default Gateways“ eintragen und so den Datenstrom lenken.
Solange beide Router aktiv sind, fließen die Daten über den Router, auf dem die IP-Adresse des „Default-Gateways“ die höhere VRRP-Priorität besitzt. Fällt ein Router aus, dann fließen alle Daten über den verbleibenden Router.

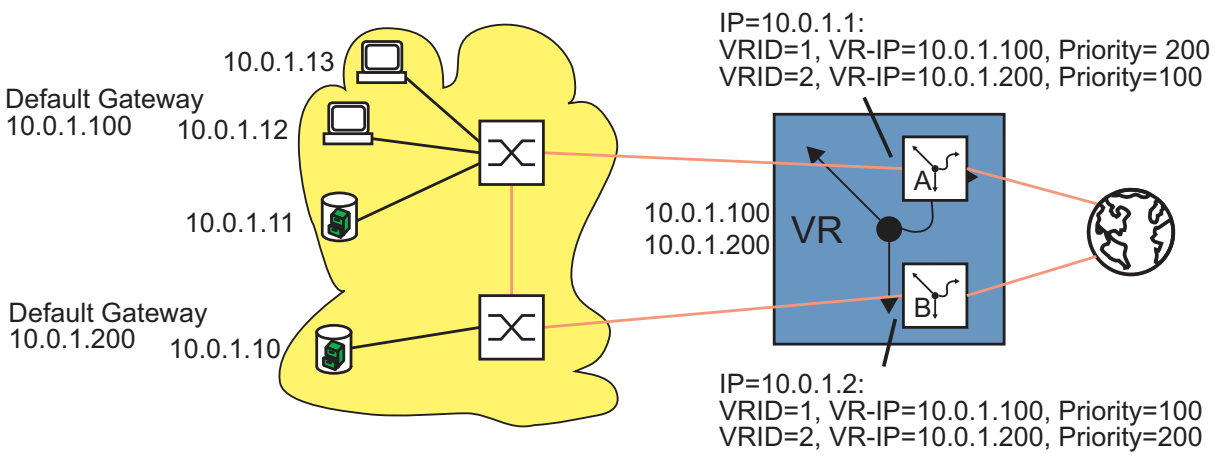


Abb. 27: Virtueller Router mit Load Sharing

Zur Nutzung der Lastverteilung führen Sie folgende Konfigurationsschritte aus:

- ☐ Definieren Sie für das gleiche Router-Interface eine zweite VRID.
- ☐ Weisen Sie dem Router-Interface für die zweite VRID eine eigene IP-Adresse zu.
- ☐ Weisen Sie dem zweiten virtuellen Router eine niedrigere Priorität zu als dem ersten virtuellen Router.

- ☐ Achten Sie bei der Konfiguration des redundanten Routers darauf, dass Sie dem zweiten virtuellen Router eine höhere Priorität zuweisen, als dem ersten.
- ☐ Geben Sie den Endgeräten eine der virtuellen Router IP-Adressen als „Default Gateway“.

5.6 VRRP mit Multinetting

Der Router bietet Ihnen die Möglichkeit, VRRP mit Multinetting zu kombinieren.

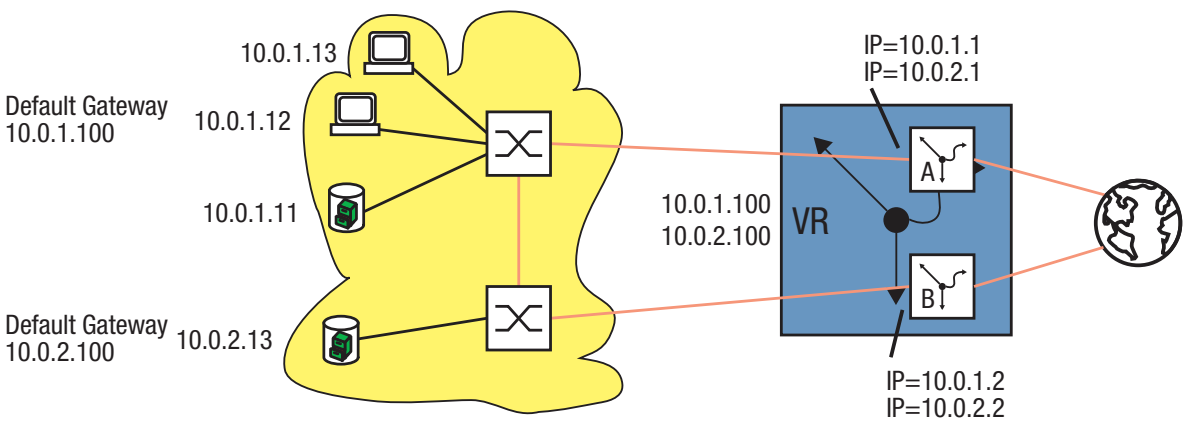


Abb. 28: Virtueller Router mit Multinetting

Zur Nutzung von VRRP mit Multinetting führen Sie folgende Konfigurationsschritte aus ausgehend von einer bestehenden VRRP-Konfiguration (siehe Abbildung 19):

☐ Weisen Sie dem Port eine zweite (secondary) IP-Adresse zu.

☐ Weisen Sie dem virtuellen Router eine zweite (secondary) IP-Adresse zu.

`interface 2/3`	Auswahl des Ports zur Konfiguration von Multinetting.
`ip address 10.0.2.1 255.255.255.0 secondary`	Dem Port seine zweite IP-Adresse zuweisen.
`ip vrrp 1 ip 10.0.2.100 secondary`	Dem virtuellen Router mit der VR-ID 1 die zweite IP-Adresse zuweisen.

☐ Nehmen Sie die gleiche Konfiguration auch auf dem redundanten Router vor.

6 RIP

Das Routing Information Protocol (RIP) ist ein Routing-Protokoll auf Basis des Distanzvektor-Algorithmus. Es dient der dynamischen Erstellung der Routingtabelle von Routern.

Beim Starten eines Routers kennt dieser nur seine direkt angeschlossenen Netze und sendet diese Routingtabelle an die benachbarten Router. Gleichzeitig fordert er von seinen benachbarten Routern deren Routingtabelle an. Mit diesen Informationen ergänzt der Router seine Routingtabelle und lernt somit, welche Netze jeweils über welchen Router aus erreicht werden können und welcher Aufwand damit verbunden ist. Um Änderungen im Netz (Ausfall oder Start eines Routers) zu erkennen, wiederholen die Router den Austausch der gesamten Routingtabellen regelmäßig, üblicherweise alle 30 Sekunden. Dies bedeutet einen beachtlichen Bandbreitenbedarf bei großen Netzen.

Die Kosten, auch Metrik genannt, bezeichnen den Aufwand, um ein bestimmtes Netz zu erreichen. RIP verwendet dazu allein den Hop-Count; er bezeichnet die Anzahl der Router, die entlang eines Pfades bis zum Zielnetz durchlaufen werden. Der Name Distanzvektor leitet sich aus der Tatsache ab, dass die Distanz (Metrik) das Kriterium zur Bestimmung der Route ist und die Richtung durch den Next-Hop (Vektor) vorgegeben ist. Der Next-Hop bezeichnet den benachbarten Router, der im Pfad zur Zieladresse liegt.

Ein Eintrag in die Routingtabelle besteht aus der Adresse des Next-Hop, der Zieladresse und der Metrik. Die RIP-Routingtabelle enthält immer die effizienteste Route zum Ziel. Das ist die Route mit der kleinsten Metrik und dem längsten passenden Präfix der Netzmaske.

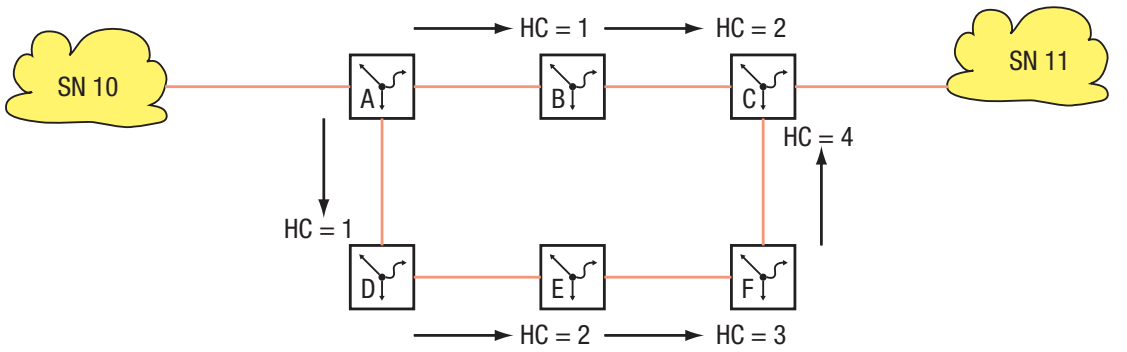


Abb. 29: Zählen des Hop Count

Router A			**Router B**			**Router D**		
Ziel	Next-Hop	Metrik	Ziel	Next-Hop	Metrik	Ziel	Next-Hop	Metrik
SN 10	lokal	0	SN 10	Router A	1	SN 10	Router A	1
SN 11	Router B	2	SN 11	Router C	1	SN 11	Router E	3

Tab. 9: Routingtabelle zum vorhergehenden Bild

Im Gegensatz zu OSPF tauscht ein RIP-Router den Inhalt seiner gesamten Routingtabelle mit seinem direkten Nachbarn zyklisch aus. Jeder Router kennt nur seine eigenen Routen und die Routen seiner direkten Nachbarn. Er hat somit nur eine lokale Sichtweise.

Bei Änderungen im Netz dauert es eine gewisse Zeit, bis alle Router wieder eine einheitliche Sicht auf das Netz haben. Das Erreichen dieses Zustandes heißt Konvergenz.

6.1 Konvergenz

Wie reagiert RIP auf Topologie-Änderungen?
Am folgenden Beispiel der Unterbrechung der Verbindung zwischen Router B und Router C können Sie die daraus resultierenden Änderungen in der Adresstabelle verfolgen.

Annahmen:
- die Unterbrechung tritt 5 Sekunden, nachdem B seine Routingtabelle verschickt hat, auf.
- Die Router verschicken alle 30 Sekunden (= Lieferzustand) ihre Routingtabelle.
- Zwischen dem Verschicken der Routingtabellen besteht ein Zeitversatz von 15 Sekunden zwischen Router A und Router B.

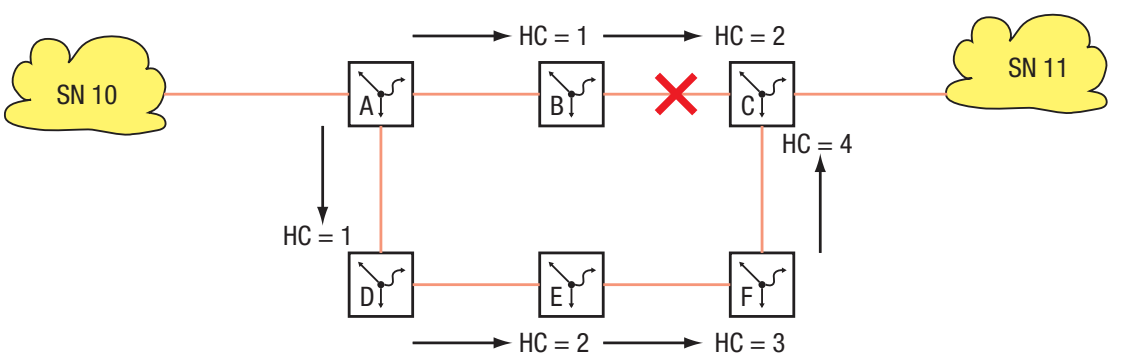


Abb. 30: Hop Count

Zeitlicher Ablauf bis zur Konvergenz:

0 Sekunden:
Unterbrechung

10 Sekunden
Router A verschickt seine Routingtabelle:

Router A		
Ziel	Next-Hop	Metrik
SN 10	local	0
SN 11	Router B	2

Anhand der Routingtabelle von Router A erkennt Router B, dass Router A eine Verbindung zum Ziel SN 11 kennt mit einer Metrik von 2. Da er selbst keine Verbindung mehr zu Router C als Next-Hop zu SN 11 hat, ändert Router B seinen Eintrag zum Ziel SN 11. Als Next-Hop trägt er Router A ein und erhöht die Metrik von Router A um 1 auf 3 (Distanz = gelernte Distanz + 1).

25 Sekunden
Router B verschickt seine Routingtabelle:

Router B		
Ziel	Nex- Hop	Metrik
SN 10	Router A	1
SN 11	Router A	3

Anhand der Routingtabelle von Router B erkennt Router A, dass Router B eine Verbindung zum SN 11 mit der Metrik 3 kennt. Also erhöht Router A seine Metrik für SN 11 um 1 auf 4.

40 Sekunden
Router A verschickt seine Routingtabelle:

Router A		
Ziel	Next-Hop	Metrik
SN 10	local	1
SN 11	Router B	4

Anhand der Routingtabelle von Router A erkennt Router B, dass Router A eine Verbindung zum Ziel SN 11 kennt mit einer Metrik von 4. Also erhöht Router B seine Metrik für SN 11 um 1 auf 5.

55 Sekunden
Router B verschickt seine Routingtabelle:

Router B		
Ziel	Next-Hop	Metrik
SN 10	Router A	1
SN 11	Router A	5

Anhand der Routingtabelle von Router B erkennt Router A, dass Router B eine Verbindung zum SN 11 mit der Metrik 5 kennt. Also erhöht Router A seine Metrik für SN 11 um 1 auf 6. Da Router A aus der Routingtabelle von von Router D weiß, daß Router D eine Verbindung zum SN 11 mit der kleineren Metrik von 3 hat, ändert er seinen Eintrag zum SN 11.

70 Sekunden
Router A verschickt seine Routingtabelle:

Router A		
Ziel	Next-Hop	Metrik
SN 10	Router A	1
SN 11	Router D	4

Nach70 Sekunden ist die Konvergenz wieder erreicht.

6.2 Maximale Netzgröße

Die nur direkte Bekanntschaft seiner Nachbarn ist auch das größte Problem von RIP. Zum einen ergeben sich hohe Konvergenzzeiten und das Count-to-Infinity-Problem. Infinität bezeichnet die Unerreichbarkeit eines Ziels und wird bei RIP mit dem Hop-Count 16 angegeben. Bestünde im Beispiel oben der parallele Pfad über die Router D, E und F nicht, dann würden sich die Router A und B solange ihre Routingtabelle schicken, bis die Metrik den Betrag 16 annimmt. Erst dann erkennen die Router, dass das Ziel nicht erreichbar ist.
Der Einsatz des „Split-Horizon“-Verfahrens eliminiert dieses Schleifenproblem zwischen 2 benachbarten Routern. Split-Horizon verfügt über 2 Betriebsarten.

Simple-Split-Horizon	lässt beim Versenden der Routingtabelle an den Nachbarn die von diesem Nachbarn gelernten Einträge weg.
Simple-Split-Horizon mit Poison-Reverse	versendet die Routingtabelle an den Nachbarn mit den von diesem Nachbarn gelernten Einträgen, teilt diesen aber die Metrik Infinity (=16) zu.

Tab. 10: Split-Horizon-Betriebsarten

Somit bestimmt auch der Hop-Count 16 die maximale Göße eines Netzes mit RIP als Routingverfahren. Die längsten Wege dürfen bis zu 15 Router durchlaufen.

6.3 Allgemeine Eigenschaften von RIP

Das RFC 1058 vom Juni 1988 spezifiziert RIP Version 1. Die Version 1 hat folgende Einschränkungen:

- Verwendung von Broadcasts für Protokollnachrichten.
- Keine Unterstützung von Subnetzen/CIDR
- Keine Authentifizierung.

Die Standadisierung von RIP Version 2 in der RFC 2453 im Jahr 1998 eliminiert die oben genannten Einschänkungen.
RIP V2 sendet seine Protokollnachrichten als Multicast mit der Zieladresse 224.0.0.9, unterstützt Subnetzmasken und Authentifizierung.
Die Einschränkungen bezüglich der Netzausdehnung bleiben jedoch bestehen.

Vorteile	Nachteile
leicht zu implementieren	Routingtabellen in großen Netzen sehr umfangreich
leicht zu administrieren	Routing-Information verteilt sich nur langsam, da feste Sendeintervalle bestehen. Dies gilt insbesondere für den Entfall von Verbindungen, da nur existente Wege in der Routingtabelle stehen.
	Count-to-Infinity

Tab. 11: Vor und Nachteile von Vector Distance Routing

6.4 RIP konfigurieren

Der Vorteil von RIP ist die einfache Konfiguration. Nach der Definition der Router-Interfaces und dem Einschalten von RIP trägt RIP die erforderlichen Routen automatisch in die Routingtabelle ein.

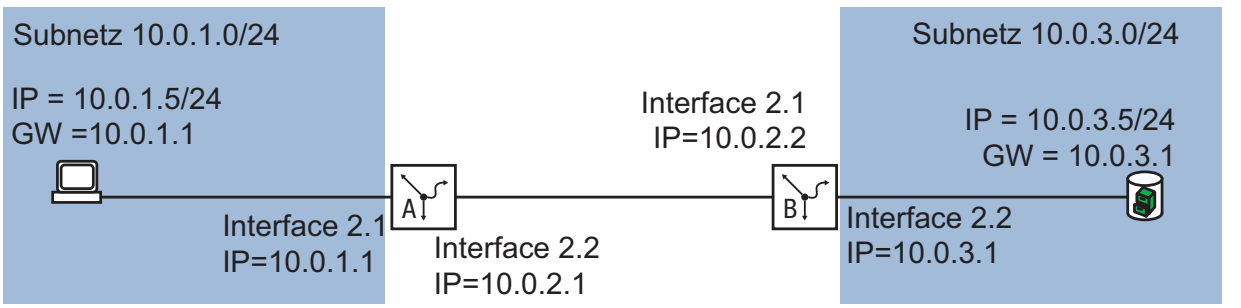


Abb. 31: Beispiel für die Konfiguration von RIP

Die Konfiguration von RIP erfordert folgende Schritte:

- Router Interfaces konfigurieren – IP-Adresse, Netzmaske zuweisen.
- RIP am Port einschalten.
- RIP global einschalten.
- Routing global einschalten (falls nicht schon geschehen).

Konfiguration für Router B

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/2`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/2.
`ip address 10.0.3.1 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Port .
`exit`	Wechsel in den Konfigurationsmodus.

`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/1.
`ip address 10.0.2.2 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Port .
`ip rip`	RIP an diesem Port einschalten.
`exit`	Wechsel in den Konfigurationsmodus.
`show ip rip interface brief`	Prüfung der Einstellungen für die RIP-Konfiguration.

```
                          Send        Receive       RIP         Link
Interface  IP Address     Version      Version     Mode        State
---------  -------------  -----------  ---------  ---------  -----
2/1        0.0.0.0         RIP-2        Both        Enable     Down
```

Die IP-Adress-Einträge stehen auf 0.0.0.0 solange die Routing-Funktion global ausgeschaltet ist.

router rip	Wechel in den Router-Konfigurationsmodus
redistribute connected	RIP anweisen, neben den gelernten Routen auch die Routen der lokal angeschlossenen Interfaces mit den RIP-Informationen zu versenden
`enable`	RIP global einschalten.
`exit`	Wechsel in den Konfigurationsmodus.
`ip routing`	Router-Funktion global einschalten.
`show ip rip interface brief`	Prüfung der Einstellungen für die RIP-Konfiguration.

```
                          Send        Receive       RIP         Link
Interface  IP Address     Version      Version     Mode        State
---------  -------------  -----------  ---------  ---------  -----
2/1        10.0.2.2         RIP-2        Both        Enable     Up
```

`show ip route`	Überprüfung der Routingtabelle:

```
Total Number of Routes..................... 3

   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------- --------------- ------------  ------  ------------
10.0.1.0        255.255.255.0   RIP            2/1       10.0.2.1
10.0.2.0        255.255.255.0   Local          2/1       10.0.2.2
10.0.3.0        255.255.255.0   Local          2/2       10.0.3.1
```

☐ Nehmen Sie die entsprechende Konfiguration auch auf den anderen RIP-Routern vor.

7 OSPF

Open Shortest Path First (OSPF) ist ein dynamisches Routing-Protokoll auf Basis des Link-State-Algorithmus. Dieser Algorithmus beruht auf den Verbindungszuständen (Link-States) zwischen den beteiligten Routern. Massgebliche Metrik in OSPF sind die "OSPF Kosten" (OSPF costs), die sich aus der verfügbaren Bitrate eines Links berechnen.

Der IETF hat das OSPF entwickelt. OSPF ist aktuell als OSPFv2 im RFC 2328 spezifiziert. Neben vielen anderen Vorteilen von OSPF, hat die Tatsache, dass es sich um einen offenen Standard handelt, zur weiten Verbreitung dieses Protokolls beigetragen. OSPF hat das Routing Information Protocol (RIP) als das Standard Interior Gateway Protocol (IGP) in großen Netzen abgelöst.

OSPF bietet einige wesentliche Vorteile:

- Kostenbasierte Routing-Metriken: Anders als RIP, bietet OSPF anschauliche Metriken basierend auf der Bandbreite jeder einzelnen Netzverbindung. OSPF bietet eine große Flexibilität beim Netzdesign, weil der Benutzer diese Kosten einfach verändern kann.
- Routing über mehrere Pfade (Equal cost multiple path/ECMP): OSPF hat die Fähigkeit, mehrere gleichwertige Pfade zu einem gegebenen Ziel zu unterstützen. Dadurch bietet OSPF eine effiziente Ausnutzung der Netzressourcen (Lastverteilung) und verbessert die Verfügbarkeit (Redundanz).
- Hierarchisches Routing: Durch die logische Unterteilung des Netzes in Areas verkürzt OSPF die Zeit zur Verteilung der Routinginformationen. Die Mitteilungen über Änderungen in einem Teilnetz bleiben im Teilnetz, ohne den Rest des Netzes zu belasten.
- Unterstützung von Classless Inter Domain Routing (CIDR) und Variable Length Subnet Mask (VLSM): Dies erlaubt dem Netzadministrator, die IP-Adress-Ressourcen effizient zuzuordnen.
- Schnelle Abstimmungszeit: OSPF unterstützt die Verteilung von Nachrichten über Routenänderungen in kürzester Zeit. Dies beschleunigt die Abstimmungzeit zur Erneuerung der Netztopologie.

- Schonung von Netzressourcen/Bandbreitenoptimierung: Da OSPF nicht wie RIP zyklisch mit einer kurzen Intervallzeit die Routingtabellen austauscht, wird keine unnötige Bandbreite zwischen den Routern „verschwendet".
- Unterstützung der Authentifizierung: OSPF unterstützt die Authentifizierung aller Knoten, die Routinginformationen senden.

Vorteile	Nachteile
Jeder Router berechnet seine Routen unabhängig von anderen Routern.	aufwändig zu implementieren
Alle Router haben die gleichen Basisinformationen.	komplexe Administration wegen der großen Anzahl von Möglichkeiten.
Schnelles Erkennen von Verbindungsausfällen und schnelles Berechnen alternativer Routen.	
Datenmenge für Routerinformation ist relativ gering, da nur bei Bedarf gesendet wird und nur die Information zu den nächsten Nachbarn enthalten ist.	
Optimale Wegewahl durch Bewertung der Verbindungsqualität.	

Tab. 12: Vor und Nachteile von Link State Routing

OSPF ist ein Routing-Protokoll auf Basis der Zustände der Verbindungen zwischen den Routern.
Mit Hilfe der von allen Routern gesammelten Verbindungszustände und des „Shortest Path First“-Algorithmus erstellt ein OSPF-Router dynamisch seine Routingtabelle.

7.1 OSPF-Topologie

Um den Umfang der auszutauschenden OSPF-Informationen in großen Netzen gering zu halten, ist OSPF hierarchisch aufgebaut. Mit Hilfe von sogenannten Areas unterteilen Sie Ihr Netz.

7.1.1 Autonomes System

Ein autonomes System (Autonomous System, AS) ist eine Anzahl von Routern, die unter einer administrativen Verwaltung stehen und ein gemeinsames Interior Gateway Protokoll (IGP) benutzen. Mehrere autonome Systeme hingegen werden über Exterior Gateway Protokolle (EGP) verbunden. OSPF ist ein Interior Gateway Protokoll.

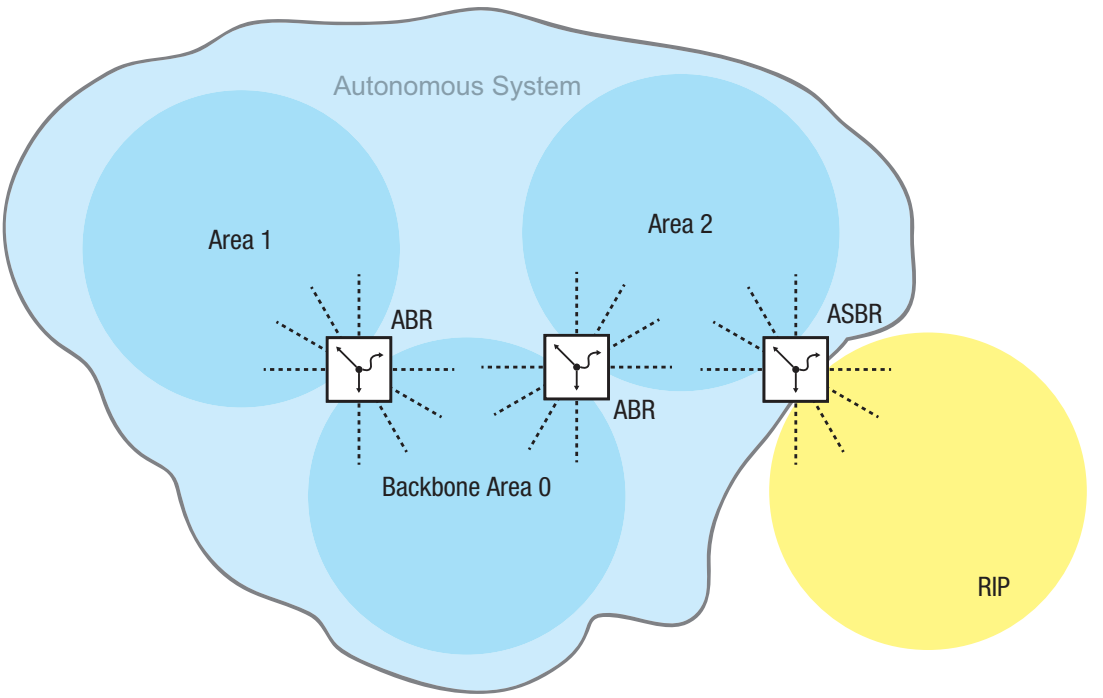


Abb. 32: Autonomes System

Ein AS tritt über einen „Autonomous System Boundary Router“ (ASBR) mit der Außenwelt in Verbindung. Ein ASBR versteht mehrere Protokolle und dient als Gateway zu Routern außerhalb der Areas. Ein ASBR ist in der Lage, Routen unterschiedlicher Protokolle in das OSPF zu übertragen. Dieser Prozess heißt Redistribution.

7.1.2 Router-ID

Die Router-ID im Format einer IP-Adresse gewährleistet die eindeutige Bestimmung eines jeden Routers innerhalb eines autonomen Systems. Zur Verbesserung der Transparenz ist die manuelle Konfiguration der Router-ID eines jeden OSPF-Routers notwendig. Es existiert also kein Automatismus, der die Router-ID aus den IP-Interfaces des Routers auswählt.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`router ospf`	Wechsel in den Router-Konfigurationsmodus.
`router-id 192.168.1.0`	Router-ID (z.B. 192.168.1.0) zuweisen.
`enable`	OSPF global einschalten.

7.1.3 Areas

Zunächst bildet jede Area ihre eigene Datenbank über die Verbindungszustände innerhalb der Area. Der hierzu benötigte Datenaustausch bleibt innerhalb der Area. Jede Area tritt über einen Area Border Router (ABR) mit anderen Areas in Verbindung. Zwischen den Areas werden die Routing-Informationen so weit wie möglich zusammengefasst (Route Summarization).

Jeder OSPF-Router muß Mitglied mindestens einer Area sein.
Ein einzelnes Router-Interface kann nur einer Area zugeordnet werden. Im Lieferzustand ist jedes Router-Interface der Backbone Area zugeordnet.

OSPF unterscheidet folgende besonderen Area-Typen:

- Backbone-Area:
  Per Definition ist das die Area 0 bzw. 0.0.0.0. Ein OSPF-Netz besteht mindestens aus der Backbone-Area. Sie ist die zentrale Area, die mit allen anderen Areas direkt verbunden ist. Die Backbone-Area erhält alle Routing-Informationen und ist für die Weiterleitung dieser Informationen verantwortlich.
- Stub Area:
  Eine Area definieren Sie als Stub-Area, wenn externe LSAs nicht in die Area geflutet werden sollen. Extern heißt außerhalb des autonomen Systems. Das sind die gelben und orangefarbenen Verbindungen in der Abbildung (siehe Abbildung 33). Somit lernen die Router innerhalb einer Stub-Area nur interne (blaue Verbindungen) Routen (z.B. keine Routen, die von einem anderen Protokoll in OSPF exportiert werden / Redistribu-

ting). Alle Ziele außerhalb des autonomen Systems werden einer Default Route zugeordnet. Dementsprechend finden Stub-Areas in der Regel ihre Anwendung, wenn nur eine Route der Area Verbindung nach außen hat. Die Verwendung von Stub-Areas hält die Routingtabelle klein innerhalb der Stub-Area.
Totally-Stubby-Area:
Eine Totally-Stubby-Area definieren Sie, wenn neben den externen (orange und gelb) LSAs auch die LSAs der internen (blaue) Routen nicht in die Area gesendet werden sollen. Intern heißt zwischen den Areas des autonomen Systems. Ein Router innerhalb einer Totally-Stubby-Area kennt somit nur die Routen innerhalb seiner eigenen Area und die Default-Route aus der Area hinaus.

Konfigurationshinweise:

- Eine Stub-Area setzt voraus, dass alle Router innerhalb der Stub-Area als Stub-Router definiert sind.
- Eine Stub-Area läßt keinen Durchgang für eine virtuelle Verbindung zu.
- Die Backbone-Area läßt sich nicht als Stub-Area definieren.

- Not So Stubby Area (NSSA):
  Eine Area definieren Sie als NSSA, wenn externe (gelbe) Routen eines direkt an die NSSA angeschlossenen Systems außerhalb des eigenen autonomen Systems in die Area geleitet (redistributed) werden sollen. Diese externen (gelben) LSAs gelangen dann aus der NSSA zu anderen Areas des eigenen autonomen Systems. Externe (orange) LSAs innerhalb des eigenen autonomen Systems gelangen hingegen nicht in eine NSSA.
  Durch die Verwendung von NSSAs können ASBRs in die Area integriert werden, ohne auf den Vorteil von Stub Areas zu verzichten, nämlich dass externe Routen aus dem Backbone nicht in die entsprechende Area geflutet werden.
  Dadurch bieten NSSAs den Vorteil, daß externe Routen die aus dem Backbone kommen, nicht alle in die Routingtabellen der internen Router eingetragen werden. Gleichzeitig jedoch kann eine begrenzte Anzahl externer Netze (welche über die Grenzen der NSSA erreichbar sind) in die Backbone Area propagiert werden.

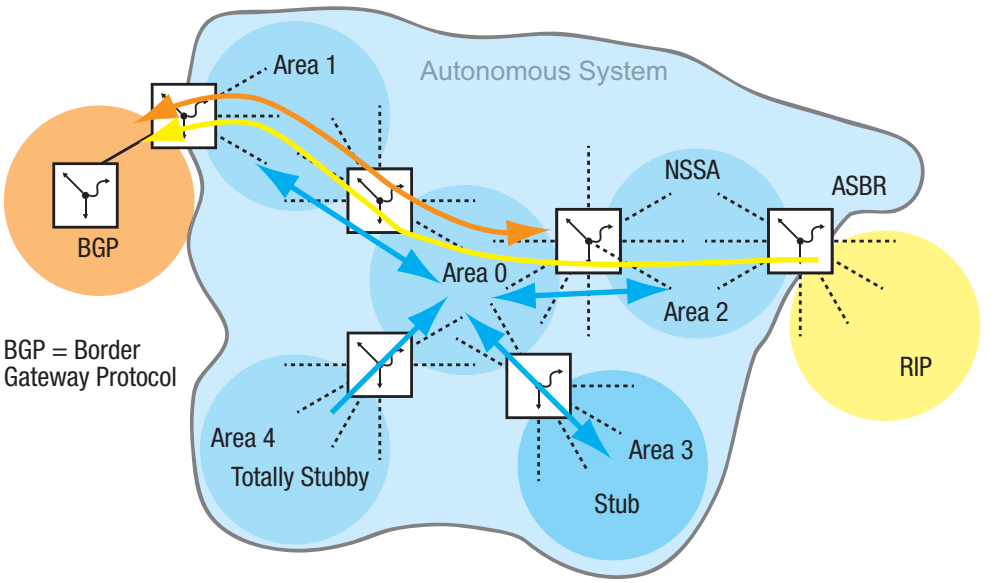


Abb. 33: LSA-Verteilung in die Area-Typen

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`router ospf`	Wechsel in den Router-Konfigurationsmodus.
`area [area-id]`	Der Area seine Area-ID zuweisen.
`area 2 nssa`	Definiert die Area 2 zur NSSA
`area 3 stub`	Definiert die Area 3 zur Stub-Area
`area 3 default-cost 10`	Weist den ABR an, die Default-Route mit der Metrik 10 in die Stub-Area zu injizieren.
`no area 3 stub summerylsa`	Macht die Stub-Area 3 zur Totally-Stubby-Area

7.1.4 Virtual Link

OSPF setzt voraus, dass die Backbone-Area durchgängig ist. Ist das aber in der Realität nicht möglich, dann bietet OSPF eine virtuelle Verbindung (VL) an, um Teile der Backbone-Area miteinander zu verbinden (siehe Abbildung 35). Eine VL erlaubt auch das Anbinden einer Area, die über eine andere Area mit der Backbone Area verbunden ist.

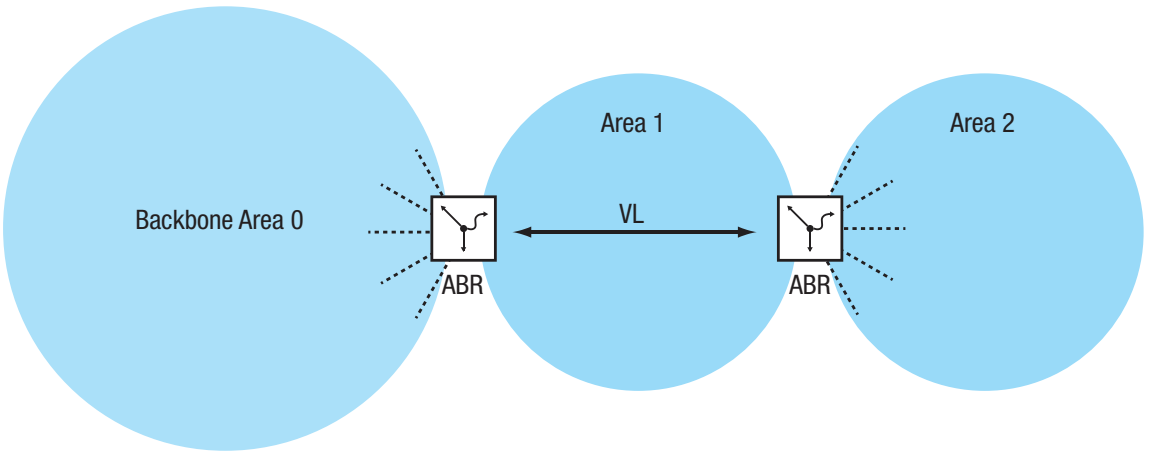


Abb. 34: Anbinden einer entfernten Area an die Backbone Area durch eine virtuelle Verbindung (VL)

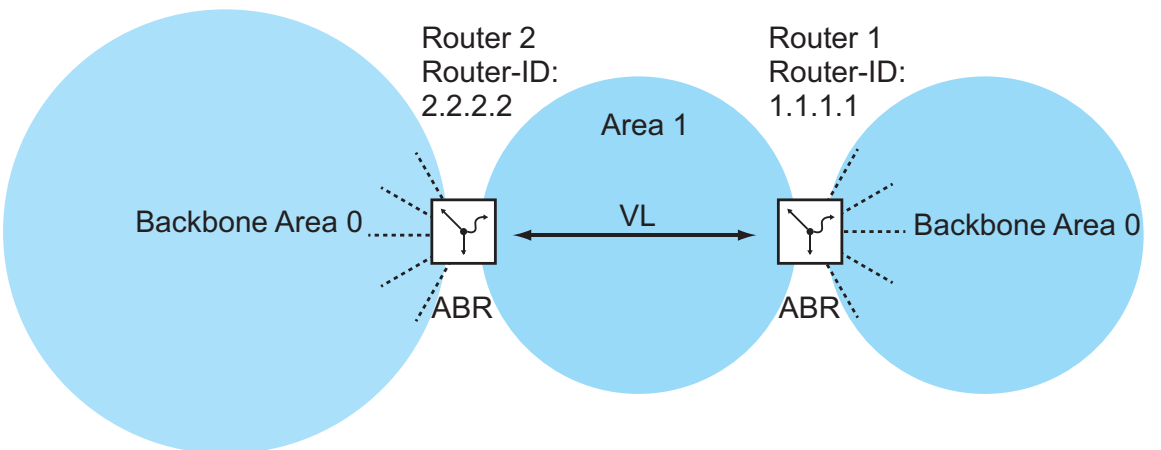


Abb. 35: Erweiterung der Backbone-Area durch eine virtuelle Verbindung (VL)

Konfiguration für die Erweiterung der Backbone-Area (siehe Abbildung 35):

Router 1:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`router ospf`	Wechsel in den Router-Konfigurationsmodus.
`area 1 virtual-link 2.2.2.2`	Eingabe der Nachbar-Router-ID für eine virtuelle Verbindung in der Area 1.

Router 2:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`router ospf`	Wechsel in den Router-Konfigurationsmodus.
`area 1 virtual-link 1.1.1.1`	Eingabe der Nachbar-Router-ID für eine virtuelle Verbindung in der Area 1.

7.1.5 OSPF-Router

OSPF unterscheidet folgende Router-Typen:

- Interner Router:
  Alle OSPF-Interfaces eines internen Routers liegen in der selben Area.
- Area Border Router (ABR)
  ABRs besitzen OSPF-Interfaces in mehrere Areas, darunter auch in der Backbone-Area. ABRs partizipieren somit in mehreren Areas. Wenn möglich fassen sie mehrere Routen zusammen und senden sogenannte "Summary-LSAs" in die Backbone-Area.

  Autonomous System Area Border Router (ASBR)
  Ein ASBR befindet sich an der Grenze eines Autonomen Systems und verbindet OSPF mit anderen Autonomen Systemen / Routing Protokollen. Diese externen Routen werden durch das sogenannte "Redistributing" in OSPF übernommen und dann als "AS-external LSAs" zusammengefaßt und in die Area geflutet.
  Schalten Sie Redistributing explizit ein.
  Wenn Sie Subnetting verweden wollen, dann geben Sie das explizit an.
  In OSPF können folgende "Routing-Protokolle" exportiert werden:
  - connected (lokale Subnetze auf denen kein OSPF eingeschaltet ist),
  - static (statische Routen),
  - RIP.

7.1.6 Link State Advertisement

Als Grundlage für den Aufbau einer Datenbank über die Verbindungszustände benutzt OSPF Verbindungszustandsnachrichten (Link-State-Advertisement, LSA).

Eine LSA beinhaltet Informationen über

- den Router,
- den angeschlossenen Subnetzen,
- erreichbare Routen,
- Netzmasken und
- Metriken.

OSPF unterscheidet folgende LSA-Typen:

- Router LSAs (Type 1 LSAs):
  Jeder Router sendet eine Router LSA in alle seine angeschlossenen Areas. Sie beschreiben den Zustand und die Kosten der Router-Links (Router-Interfaces) die der Router in der entsprechenden Area hat. Router LSAs werden nur innerhalb der Area geflutet.
- Network LSAs (Type 2 LSAs):
  Diese LSAs werden vom Designated Router, DR (siehe auf Seite 107 „Aufbau der Adjacency“) generiert und werden für jedes angeschlossene Netz/Subnetz innerhalb einer Area gesendet.
- Summary LSAs (Type 3 /Type 4 LSAs)
  Summary LSAs werden von ABRs generiert und beschreiben Inter-Area-Ziele, also Ziele in unterschiedlichen Areas des gleichen Autonomen System.
  Type 3-LSAs beschreiben Ziele zu IP-Netzen (einzelne Routen oder zusammengefasste Routen).
  Type 4-LSAs beschreiben Routen zu ASBRs.

- AS-External LSAs (Type 5 LSAs):
  Diese LSAs werden von ASBRs generiert und beschreiben Routen außerhalb des Autonomen Systems. Diese LSAs werden überall geflutet außer in Stub Areas bzw. NSSAs.
- NSSA External LSAs (Type 7 LSAs):
  Eine Stub Area flutet keine externen Routen (repräsentiert durch Type 5-LSAs) und unterstützt somit auch keine Autonomous System Border Router (ASBRs) an ihren Grenzen. Somit kann ein ASBR auch keine Routen aus anderen Protokollen in eine Stub Area portieren.
  RFC 1587 spezifiziert die Funktionsweise von NSSAs. Nach RFC 1587 versenden ASBRs innerhalb einer NSSA "Type 7-LSAs" anstatt "Type 5-LSAs" für die externen Routen. Diese "Type 7 LSAs" werden dann von einem ABR in "Type 5-LSAs" umgewandelt und in die Backbone Area geflutet. Diese sogenannte "Translator-Role" wird zwischen den ABRs einer NSSA ausgehandelt (der Router mit der höchsten Router-ID), kann jedoch auch manuell konfiguriert werden.

7.2 Prinzipielle Arbeitsweise von OSPF

OSPF wurde speziell auf die Bedürfnisse von grösseren Netzen zugeschnitten und bietet eine schnelle Konvergenz sowie eine minimale Verwendung von Protokollnachrichten.

Das Konzept von OSPF basiert auf der Erzeugung, Aufrechterhaltung und Verteilung der sogenannten Link-State-Database. Diese Datenbasis beschreibt

- alle Router innerhalb einer Routing Domäne (Area) und
- ihre aktiven Interfaces bzw. Routen,
- wie sie miteinander verbunden sind und
- die Kosten dieser Verbindungen.

Alle Router innerhalb einer Area besitzen eine identische Datenbasis, d.h. sie kennen alle die exakte Topolgie innerhalb dieser Area.
Jeder Router trägt seinen Teil dazu bei, die entsprechende Datenbasis aufzubauen, indem er seine lokale Sichtweise als sogenannte Link-State Advertisements (LSAs) propagiert. Diese LSAs werden dann an alle anderen Router innerhalb einer Area geflutet.

OSPF unterstützt eine Vielzahl unterschiedlichster Netztypen wie Punkt-zu-Punkt-Netze (z.B. Pakket over SONET/SDH), Broadcast-Netze (Ethernet) oder Nicht-Broadcast-Netze.
Broadcast-Netze zeichnen sich dadurch aus, dass mehrere Systeme (Endgeräte,Switches, Router) am gleichen Segment angeschlossen sind und somit auch alle gleichzeitig über Broadcasts/Multicasts angesprochen werden können.

Prinzipiell führt OSPF folgende drei Schritte aus um seine Aufgaben im Netz wahrzunehmen:

- Aufbau der Nachbarschaftsbeziehungen (Hello-Protokoll)
- Synchronisation der Link State Database
- Routenberechnung

7.3 Aufbau der Adjacency

Beim Starten eines Routers nimmt er über sogenannte „Hello“-Pakete Kontakt zu seinen benachbarten Routern auf. Mit Hilfe dieser „Hello“-Pakete erfährt ein OSPF-Router, welche OSPF-Router in seiner Nähe sind und ob sie geeignet sind, eine Nachbarschaftsbeziehung (Adjacency) aufzubauen.

In Broadcast-Netzen wie Ethernet steigt mit der Anzahl der angeschlossenen Router die Anzahl der Nachbarschaften und der Informationsaustausch zur Klärung und Pflege der Nachbarschaftsbeziehung. Zur Reduzierung innerhalb einer Area ermittelt OSPF über das "Hello"-Protokoll einen (designierten) Designated Router (DR) innerhalb des entsprechenden Segments. So baut jeder Router in einer Area nur die Nachbarschaft zu seinem Designated Router auf anstatt zu jedem Nachbarn. Der Designated Router ist verantwortlich für die Verteilung aller Verbindungsstatusinformationen zu seinen Nachbar-Routern.
Aus Sicherheitsgründen sieht OSPF noch die Wahl eines Backup Designated Routers (BDR) vor, der beim Ausfall des DR dessen Aufgaben übernimmt. Der OSPF-Router mit der höchsten Router-Priorität wird DR. Die Router-Priorität legt der Administrator fest. Haben zwei Router die gleiche Priorität, wird der Router mit der höheren Router-ID gewählt. Die Router-ID ist die kleinste IP-Adresse eines Router-Interfaces. Diese Router-ID konfigurieren Sie bei der Inbetriebnahme des OSPF-Routers manuell (siehe auf Seite 98 „Router-ID“).

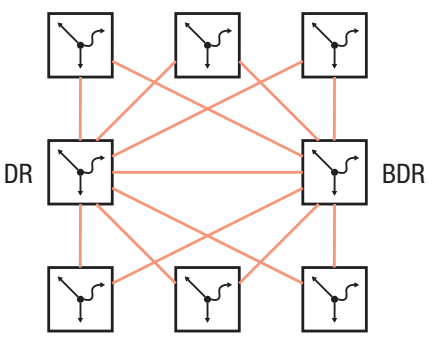


Abb. 36: LSA-Verteilung mit Designated Router und Backup Designated Router

Zum Austausch von Informationen benutzt OSPF reservierte Multicast-Adressen.

Ziel	Multicast-IP-Adresse	abgebildete Multicast-MAC-Adresse
All OSPF routers	224.0.0.5	01:00:5E:00:00:05
Designated routers	224.0.0.6: OSPF	01:00:5E:00:00:06

Tab. 13: OSPF - Multicast-Adressen

Hello Pakete dienen weiterhin zur Überprüfung der Konfiguration innerhalb einer Area (Area ID, Timer-Werte, Prioritäten) und zur Überwachung der Nachbarschaftsbeziehungen. Hello-Pakete werden zyklisch gesendet (Hello-Intervall). Das Ausbleiben des Empfangs von Hello-Paketen innerhalb eines gewissen Zeitraumes (Dead-Intervall) führt zur Kündigung der Nachbarschaftsbeziehung und zum Löschen aller entsprechenden Routen.
Das Hello-Intervall (Voreinstellung: 10 Sekunden) und das Dead-Intervall (Voreinstellung: 30 Sekunden) kann pro Router-Interface konfiguriert werden, muss aber innerhalb einer Area einheitlich sein.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1/1.
`ip ospf hello-intervall 20`	Setzt Hello-Intervall auf 20 Sekunden.
`ip ospf dead-intervall 60`	Setzt Dead-Intervall auf 60 Sekunden.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show ip ospf neighbor brief all`	Anzeigen der Nachbarschaftsbeziehungen des Routers an.

```
  Router ID       IP Address    Neighbor Interface    State
------------      -----------   ------------------    --------
192.168.1.1        10.0.1.1        1/1                 Full
192.168.1.2        11.0.1.1        1/2                 Full
192.168.1.3        12.0.1.1        1/3                 Full
192.168.1.4        13.0.1.1        1/4                 Full
```

Die Nachbarschaftsbeziehungen können folgende Zustände (States) annehmen:

Down	Noch keine Hello-Pakete empfangen
Init	Hello-Pakete empfangen
2-way	Bidirektionale Kommunikation, Ermittlung des DR und BDR
Exstart	Aushandeln von Master/Slave für LSA-Austausch
Exchange	LSAs werden ausgetauscht bzw. geflutet
Loading	Abschluss des LSA-Austauschs.
Full	Datenbasis komplett und in der Area einheitlich. Routen können nun berechnet werden

7.4 Synchronisation der LSD

Kernstück von OSPF ist die Link State Database (LSD). Diese Datenbank enthält eine Beschreibung des Netzes und den Zustand aller Router. Sie ist die Quelle zur Berechnung der Routingtabelle. Sie spiegelt die Topologie des Netzes wieder. Sie wird aufgebaut nachdem der Designated Router bzw. Backup Designated Router innerhalb einer Area (Broadcast Netze) ermittelt wurde.

Zum Aufbau der LSD und zur Aktualisierung bei Topologieänderungen sendet der OSPF-Router Verbindungsstatusmeldungen (LSA) an alle direkt erreichbaren OSPF-Router.
Diese Verbindungsstatusmeldungen bestehen aus den Interfaces und den darüber erreichbaren Nachbarn des sendenden OSPF-Routers. OSPF-Router nehmen diese Information in ihre Datenbank auf und fluten diese Information an allen Ports.

Treten keine Topologieänderungen auf, wiederholt jeder Router seine eigenen LSAs alle 30 Minuten.

Den Inhalt der Link State Database können Sie über das CLI-Kommando "show ip ospf database" ansehen, wobei die Einträge entsprechend der Areas ausgegeben werden.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`show ip ospf database`	Anzeigen der Nachbarschaftsbeziehungen des Routers an.

```
Router Link States (Area 0.0.0.0)

Link Id         Adv Router      Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
192.168.1.1     192.168.1.1     122   80000007 0x5380 -E----  ---E-
192.169.1.1     192.169.1.1     120   80000007 0xbf0e -E----  ---E-

                 Network Link States (Area 0.0.0.0)

Link Id         Adv Router      Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
10.0.1.2         192.169.1.1     129   80000002 0xad5a -E----
11.0.1.2         192.169.1.1     135   80000002 0xa066 -E----
12.0.1.2         192.169.1.1     137   80000002 0x9372 -E----
13.0.1.2         192.169.1.1     132   80000002 0x867e -E----

                 AS External States

Link Id         Adv Router      Age   Sequence Chksm  Options Rtr Opt
--------------- --------------- ----- -------- ------ ------- -----
192.169.0.0      192.169.1.1     178   80000002 0xca1c
```

Die Intepretation der dargestellen Link ID hängt vom entsprechenden LSA-Typ ab:

Router Link States	Link Id entpricht der Router ID der Quelle
Network Link States	Link Id entspricht der Interface IP-Adresse des Designated Routers
Network Summary States	Link Id entspricht dem entsprechenden Netz
Summary ASBR States	Link Id entpricht der Router ID des beschriebenen ASBR
AS External States	Link Id entpricht dem externen Netz

7.5 Routenberechnung

Nach dem Lernen der LSDs und und dem Übergang der Nachbarschaftbeziehungen in den "Full State", berechnet jeder Router einen Pfad zu jedem Ziel mit Hilfe des Shortest Path First (SPF) Algorithmus. Nachdem der optimale Weg zu jedem Ziel ermittelt wurde, werden diese Routen in die Routingtabelle eingetragen. Die Routenberechnung basiert im allgemeinen auf die Erreichbarkeit eines Hops und die Metrik (Kosten). Die Kosten werden über alle Hops zum Ziel aufaddiert.

Die Kosten eines einzelnen Router-Interfaces basieren auf der verfügbaren Bandbreite dieses Links. Der Berechnung für die Standardeinstellung liegt folgende Formel zugrunde:

Metrik = 10 000 000 / Bandbreite (bits/sec) .

Dies führt für Ethernet zu folgenden Kosten:

10 Mbit	10
100 Mbit	1
1000 Mbit	1 (0,1 aufgerundet auf 1)

Die Tabelle zeigt, dass diese Berechnungsform in der Standardkonfiguration keine Unterscheidung zwischen zwischen Fast-Ethernet und Gigabit-Ethernet zulässt.
Sie können die Standardkonfiguration ändern, in dem Sie jedem OSPF-Interface einen anderen Wert für die Kosten zuweisen. Das gibt Ihnen die Möglichkeit, zwischen Fast-Ethernet und Gigabit-Ethernet zu unterscheiden.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Port 1.1.
`ip ospf cost 2`	Weist dem Port 1.1 den Wert 2 für die OSPF-Kosten zu.

7.6 OSPF konfigurieren

Im Lieferzustand sind die Voreinstellungen so gewählt, dass Sie in wenigen Schritten einfache OSPF-Funktionen konfigurieren können.
Nach der Definition der Router-Interfaces und dem Einschalten von OSPF trägt OSPF die erforderlichen Routen automatisch in die Routingtabelle ein.

Das Beispiel (siehe Abbildung 37) zeigt eine einfache OSPF-Konfiguration. Die Area 0 ist im Lieferzustand schon definiert. Die Endgeräte besitzen keine OSPF-Funktion, deshalb entfällt das Aktivieren von OSPF am entsprechenden Router-Interface. Das Aktivieren der Funktion Redistribute bietet Ihnen die Möglichkeit, die Routen zu den Endgeräten in das OSPF zu injizieren.

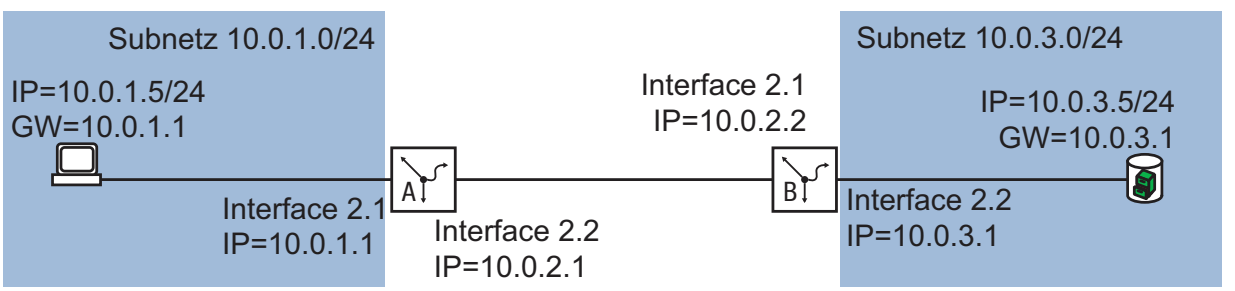


Abb. 37: Beispiel für die Konfiguration von OSPF

Die Konfiguration von OSPF erfordert folgende Schritte:

- Router Interfaces konfigurieren – IP-Adresse, Netzmaske zuweisen.
- OSPF am Port einschalten.
- OSPF global einschalten.
- Routing global einschalten (falls nicht schon geschehen).

Konfiguration für Router B

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/2`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/2.
`ip address 10.0.3.1 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Port .
`exit`	Wechsel in den Konfigurationsmodus.
`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 2.1 zum einrichten von OSPF.
`ip address 10.0.2.2 255.255.255.0`	Dem Port seine IP-Parameter zuweisen.
`routing`	Einschalten der Router-Funktion an diesem Port .
`ip ospf`	Einschalten von OSPF an diesem Port .
`exit`	Wechsel in den Konfigurationsmodus.
`router ospf`	Wechsel in den Router-Konfigurationsmodus.
`enable`	OSPF global einschalten.
`router-id 10.0.2.2`	Dem Router B die Router-ID 10.0.2.2 zuweisen.
`redistribute connected subnets`	OSPF anweisen, - neben den gelernten Routen auch die Routen der lokal angeschlossenen Interfaces mit den OSPF-Informationen zu versenden und - Subnetze ohne OSPF in OSPF einzubeziehen (CIDR).
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show ip ospf`	Prüfung der Einstellungen für die globale OSPF-Konfiguration.

```
Router ID..................................... 10.0.2.2
OSPF Admin Mode............................... Enable
ASBR Mode..................................... Enable
RFC 1583 Compatibility........................ Enable
ABR Status.................................... Disable
Exit Overflow Interval........................ 0
External LSA Count............................ 0
External LSA Checksum......................... 0
New LSAs Originated........................... 0
LSAs Received................................. 0
External LSDB Limit........................... No Limit
Default Metric................................ Not configured

Default Route Advertise....................... Disabled
Always........................................ FALSE
Metric.....................................
Metric Type................................... External Type 2
Maximum Paths................................. 4

Redistributing.............................
Source........................................ Connected
Metric........................................ Not Configured
--More-- or (q)uit
Metric Type................................... 2
Tag........................................... 0
Subnets....................................... Yes
Distribute List............................... Not configured
```

`show ip ospf interface brief`	Prüfung der Einstellungen für die OSPF-Interface-Konfiguration.

```
                          Router   Hello   Dead  Retrax Retrax LSAAck
Interface AdminMode Area ID    Priority Intval Intval Intval Delay
Intval
--------- --------- ----------- -------- ------ ------ ------ -----
2/1       Enable    0.0.0.0     1        10     40     5      1      1
2/2       Disable   0.0.0.0     1        10     40     5      1      1
```

`configure`	Wechsel in den Konfigurationsmodus.
`ip routing`	Router-Funktion global einschalten.
`exit`	Wechsel in den Privileged-EXEC-Modus.

☐ Nehmen Sie die entsprechende Konfiguration auch auf den anderen OSPF-Routern vor.

`show ip ospf neighbor brief`	Prüfung der OSPF-Nachbarschaftsverhältnisse.

```
   Router ID       IP Address    Neighbor Interface    State
---------------   -----------   -------------------   ---------
10.0.2.1          10.0.2.1           2/1              Full

show ip route                  Überprüfung der Routingtabelle:

Total Number of Routes..................... 3

   Network          Subnet                    Next Hop    Next Hop
   Address           Mask         Protocol     Intf     IP Address
--------------- --------------- ------------  ------  -------------
10.0.1.0        255.255.255.0   OSPF Ext T2   2/1       10.0.2.1
10.0.2.0        255.255.255.0   Local         2/1       10.0.2.2
10.0.3.0        255.255.255.0   Local         2/2       10.0.3.1
```

8 Protokollbasierte VLANs

Neben portbasierten VLANs nach IEEE 802.1Q unterstützt der Switch auch protokollbasierte VLANs nach IEEE 802.1v.

Bei portbasierten VLANs bestimmt der Switch die VLAN-Zugehörigkeit eines ohne VLAN-Tag empfangenen Datenpaketes durch die Port-VLAN-ID des Empfangsports.

Bei protokollbasierten VLANs bestimmt der Switch die VLAN-Zugehörigkeit eines ohne VLAN-Tag empfangenen Datenpaketes anhand des Protokolls des empfangenen Datenpaketes. Der Switch unterstützt die Protokolle

- IP,
- ARP,
- IPX.

Ohne VLAN-Tag empfangene Datenpakete anderer Protokolle ordnet der Switch entsprechend der Port-VLAN-ID einem VLAN zu.

Bei der VLAN-Zuordnung beachtet der Switch

- als erstes das VLAN-Tag,
- dann die Protokoll-Zugehörigkeit und
- zuletzt die Port-VLAN-ID.

Protokollbasierte VLANs bieten Ihnen die Möglichkeit, über IP-Subnetz-Grenzen hinweg nicht routingrelevante Datenpakete zu übertragen. Routingrelevante Datenpakete sind IP- und ARP-Datenpakete.

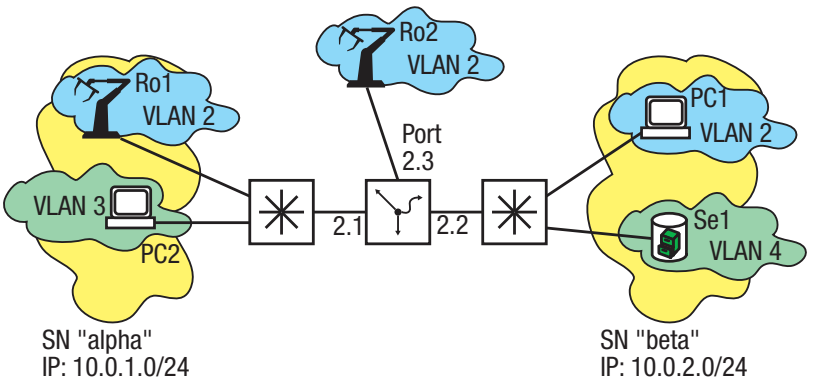


Abb. 38: Beispiel für protokollbasiertes VLAN

Im Beispiel (siehe Abbildung 38) kommunizieren PC2 und Se1 über IP. Diese Datenpakete werden geroutet.
Die Geräte Ro1, Ro2 und PC1 kommunizieren über andere Ethernet-basierte Protokolle. Diese Datenpakete werden im VLAN 2 geswitcht.
So bleiben alle IP-Datenpakete in ihren Subnetzen mit Ausnahme der IP-Datenpakete, die für ein anderes Subnetz bestimmt sind.

8.1 Prinzipielle Konfiguration

- ☐ Je Subnetz eine VLAN-Protokollgruppe erzeugen.
- ☐ Je Subnetz die Protokolle der VLAN-Protokollgruppe zuordnen.
- ☐ VLANs erzeugen.
- ☐ In den betroffenen VLANs das VLAN-Routing einschalten und somit virtuelle Router-Interfaces erzeugen.
- ☐ Die VLAN-Protokollgruppen den VLANs zuordnen.
- ☐ Port-Interfaces konfigurieren:
  - ▶ VLAN-Zugehörigkeit
  - ▶ Port-VLAN-ID für nicht-ARP/IP-Datenpakete,
  - ▶ Port einer VLAN-Protokollgruppe und somit einem VLAN zuordnen.
- ☐ Virtuelle Router-Interfaces konfigurieren:
  - ▶ IP-Adresse zuweisen
  - ▶ Routing einschalten.
- ☐ Routing global einschalten.

8.2 Konfiguration des Beispiels

```
enable                          Wechsel in den Privileged-EXEC-Modus.
configure                       Wechsel in den Konfigurationsmodus.
vlan protocol group alpha       Erzeugen der VLAN-Protokollgruppe 1 für
                                Subnetz alpha.
vlan protocol group beta        Erzeugen der VLAN-Protokollgruppe 2 für
                                Subnetz beta.
exit                            Wechsel in den Privileged-EXEC-Modus.

show protocol all               Anzeigen der erzeugten VLAN-Protokollgruppen.

                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
---------------  ------  -----------  ----  --------------------
alpha            1                    0
beta             2                    0

configure                       Wechsel in den Konfigurationsmodus.
vlan protocol group add         IP der VLAN-Protokollgruppe 1 hinzufügen.
  protocol 1 ip
vlan protocol group add         ARP der VLAN-Protokollgruppe 1 hinzufügen.
   protocol 1 arp
vlan protocol group add         IP der VLAN-Protokollgruppe 2 hinzufügen.
  protocol 2 ip
vlan protocol group add         ARP der VLAN-Protokollgruppe 2 hinzufügen.
   protocol 2 arp
exit                            Wechsel in den Privileged-EXEC-Modus.

show protocol all               Anzeigen der , den Protokollgruppen zugeord-
                                neten, Protokolle.

                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
---------------  ------  -----------  ----  ------------------
alpha            1       IP,ARP       0
beta             2       IP,ARP       0

vlan database                   Wechsel in den VLAN-Modus.
vlan 2                          Anlegen von VLAN 2.
vlan 3                          Anlegen von VLAN 3.
vlan 4                          Anlegen von VLAN 4.
```

```
vlan routing 3
```
Virtuelles Router-Interface erzeugen und die Routing-Funktion für dieses Interface einschalten.

```
vlan routing 4
```
Virtuelles Router-Interface erzeugen und die Routing-Funktion für dieses Interface einschalten.

```
protocol group 1 3
```
Die VLAN-Protokoll-Gruppe 1 dem VLAN 3 zuordnen.

```
protocol group 2 4
```
Die VLAN-Protokoll-Gruppe 2 dem VLAN 4 zuordnen.

```
exit
```
Wechsel in den Privileged-EXEC-Modus.

```
show protocol all
```
Anzeigen der den VLAN-Protokollgruppen zugeordneten Protokolle und VLANs.

```
                  Group
   Group Name       ID    Protocol(s)  VLAN       Interface(s)
---------------  ------  -----------  ----  --------------------
alpha             1       IP,ARP       3
beta              2       IP,ARP       4
```

```
show ip vlan
```
Anzeigen der Zuordnung der virtuellen Router-Interfaces zu den VLANs.

```
           Logical
VLAN ID   Interface    IP Address      Subnet Mask       MAC Address
-------  -----------  ---------------  ---------------  -----------
3       9/1         0.0.0.0         0.0.0.0         00:80:63:51:74:2C
4       9/2         0.0.0.0         0.0.0.0         00:80:63:51:74:2D
```

```
configure
```
Wechsel in den Konfigurationsmodus.

```
interface 2/1
```
Wechsel in den Interface-Konfigurationsmodus von Interface 2/1.

```
vlan participation exclude 1
```
Port 2.1 aus VLAN 1 herausnehmen.

```
vlan participation include 2
```
Port 2.1 zum Mitglied von VLAN 2 erklären.

```
vlan participation include 3
```
Port 2.1 zum Mitglied von VLAN 3 erklären.

```
vlan pvid 2
```
Port-VLAN-ID auf 2 setzen, d.h. nicht-IP/ARP-Datenpakete, ordnet der Switch dem VLAN 2 zu.

```
protocol vlan group 1
```
Dem Interface 2.1 die VLAN-Protokoll-Gruppe 1 zuweisen, d.h. IP/ARP-Datenpakete, ordnet der Switch dem VLAN 3 zu.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
interface 2/2
```
Wechsel in den Interface-Konfigurationsmodus von Interface 2/2.

```
vlan participation exclude 1
```
Port 2.2 aus VLAN 2 herausnehmen.

```
vlan participation include 2
```
Port 2.2 zum Mitglied von VLAN 2 erklären.

```
vlan participation include 4
```
Port 2.2 zum Mitglied von VLAN 4 erklären.

```
vlan pvid 2
```
Port-VLAN-ID auf 2 setzen, d.h. nicht-IP/ARP-Datenpakete, ordnet der Switch dem VLAN 2 zu.

```
protocol vlan group 2
```
Dem Interface 2.2 die VLAN-Protokoll-Gruppe 2 zuweisen, d.h. IP/ARP-Datenpakete, ordnet der Switch dem VLAN 4 zu.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
interface 2/3
```
Wechsel in den Interface-Konfigurationsmodus von Interface 2/3.

```
vlan participation exclude 1
```
Port 2.3 aus VLAN 1 herausnehmen.

```
vlan participation include 2
```
Port 2.3 zum Mitglied von VLAN 2 erklären.

```
vlan pvid 2
```
Port-VLAN-ID auf 2 setzen, d.h. Datenpakete, die ohne Tag an diesem Port empfangen werden, ordnet der Switch dem VLAN 2 zu.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
interface 9/1
```
Wechsel in den Interface-Konfigurations-Modus von Interface 9/1.

```
ip address 10.0.1.1
  255.255.255.0
```
Dem Interface seine IP-Parameter zuweisen.

```
routing
```
Einschalten der Router-Funktion an diesem Interface.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
interface 9/2
```
Wechsel in den Interface-Konfigurations-Modus von Interface 9/2.

```
ip address 10.0.2.1
  255.255.255.0
```
Dem Interface seine IP-Parameter zuweisen.

```
routing
```
Einschalten der Router-Funktion an diesem Interface.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
exit
```
Wechsel in den Privileged-EXEC-Modus.

```
show ip interface brief
```
Anzeige der Eintrage der virtuellen Router-Interface.

```
                                                Netdir   Multi
Interface IP Address      IP Mask               Bcast    CastFwd
--------- --------------- --------------- -------- --------
9/1       10.0.1.1        255.255.255.0   Disable  Disable
9/2       10.0.2.1        255.255.255.0   Disable  Disable
```

```
configure
```
Wechsel in den Konfigurationsmodus.

```
ip routing
```
Router-Funktion global einschalten.

9 Multicast-Routing

Multicast-Datenströme sind Datenpakete, die ein Sender an mehrere Empfänger schickt. Um die Netzlast zu reduzieren, benutzt der Sender eine Multicast-Adresse. So sendet er jedes Paket nur einmal an die Multicast-Adresse, anstatt es mehrmals an jeden Empfänger einzeln zu schicken. Die Empfänger erkennen einen für sie bestimmten Multicast-Datenstrom an der Multicast-Adresse.

Ein häufiger Grund für das Einführen von Subnetzen ist die Eindämmung von Broadcast-Datenströmen. Switche fluten Broadcast-/Multicast-Datenströme an allen Ports, während Router Broadcast-/Multicast-Datenströme blockieren. Multicast-Routing bietet Ihnen die Möglichkeit, Multicast-Datenströme über Subnetzgrenzen hinweg gezielt zu vermitteln. Gezielt zu vermitteln heißt, Datenströme mit definierten Multicast-Adressen ausschließlich zu den Geräten zu leiten, die den Multicast-Datenstrom empfangen wollen.

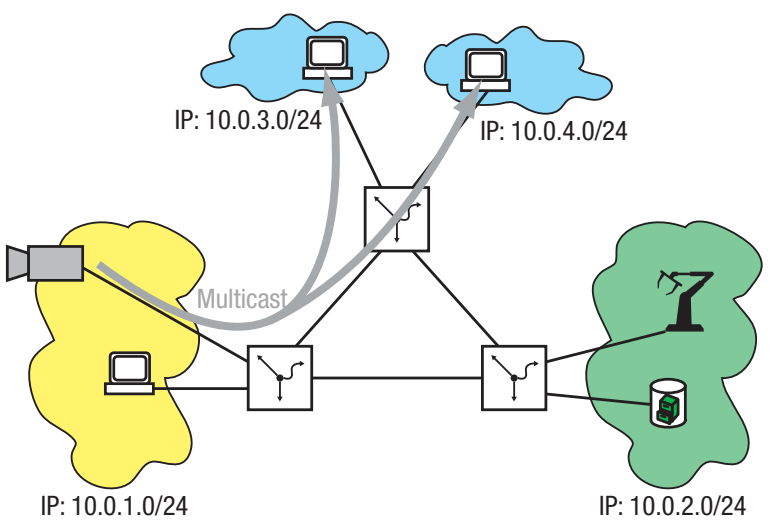


Abb. 39: Beispiel für eine Multicast-Anwendung

Zum Einsatz von Multicast-Routing gehören:

- Definierte Multicast-Adressen
- Ein Protokoll zur Multicast-Gruppen-Registrierung, das den Austausch von Informationen über Multicast-Datenströme organisiert (z.B. IGMP). Diese Informationen betreffen das Kundtun des Wunsches von Netzteilnehmern, Multicast-Datenströme zu emfangen, sowie die Abfrage dieses Interessens durch Vermittlungsgeräte.
- Ein Protokoll, das entsprechend der Informationen über Multicast-Datenströme, die Multicast-Datenströme lenkt (z.B. PIM-DM, DVMRP).

9.1 Multicast-Adressen

9.1.1 IP-Multicast-Adressen

Die IANA (Internet Assigned Numbers Authority) definiert die IP-Adressen des Klasse D IP-Adressraums als Multicast-Adressen. IP-Multicast-Adressen liegen im Bereich von 224.0.0.0 bis 239.255.255.255.

IP-Adressbereich	Zuordnung
224.0.0.0	Basis-Adresse, reserviert
224.0.0.1 - 224.0.0.255	Local network Control Block, reserviert z.B. für Routingprotokolle, IGMP. Z.B.: 224.0.0.1 - alle Hosts eines Subnetzes 224.0.0.2 - alle Router eines Subnetzes 224.0.0.4 - alle DVMRP Router 224.0.0.5 - alle OSPF Router 224.0.0.6 - alle OSPF DR Router 224.0.0.9 - alle RIP v2 Router 224.0.0.13 - alle PIM Router 224.0.0.18 - alle VRRP Router 224.0.0.22 - alle IGMP v3 Reports
224.0.1.0 - 224.0.1.255	Internetwork Control Block
224.0.2.0 - 224.0.255.255	AD-HOC Block
224.1.0.0 - 238.255.255.255	Diverse Organisationen, Protokolle, Anwendungen, Reservierungen. Z.B.: 232.0.0.0-232.255.255.255 - Source Specific Multicasts
239.0.0.0 - 239.255.255.255	Administratively Scoped IPv4 Multicast Space Diese Multicast-Adressen vermittelt kein Router über die lokalen Grenzen hinweg ins Internet. Somit kann der Administrator innerhalb dieser lokalen Grenzen diese Adressen frei vergeben.

Tab. 14: Zuordnung des IP-Multicast-Adressbereichs

Den Administativly Scoped IPv4 Multicast-Bereich unterteilt die IANA noch feiner:

IP-Adressbereich	Zuordnung
239.000.000.000 - 239.191.255.255	Reserviert [IANA]
239.192.000.000 - 239.251.255.255	Organization-Local Scope [Meyer, RFC2365]
239.252.000.000 - 239.254.255.255	Site-Local Scope (reserviert) [Meyer, RFC2365]
239.255.000.000 - 239.255.255.255	Site-Local Scope [Meyer, RFC2365]

Tab. 15: Zuordnung des Administrativly Scoped IP v4 Multicast Bereichs

Letztendlich bleiben für den Administrator einer Organisation folgende Multicast-IP-Adress-Bereiche zur freien Verteilung übrig:

- 239.192.000.000 - 239.251.255.255
  für lokale Teilbereiche einer Organisation.
- 239.255.000.000 - 239.255.255.255
  für den gesamter Bereich einer Organisation.

Anmerkung: Beachten Sie bei der Auswahl der Multicast-IP-Adressen, dass diese eindeutig auf MAC-Multicast-Adressen abgebildet werden können (siehe auf Seite 128 „IP-MAC-Multicast-Adress-Abbildung“).

9.1.2 MAC-Multicast-Adressen

Das IEEE nennt die 48-Bit MAC-Adresse „Extended Unique Identifier“. Sie bildet die einzigartige Beschreibung eines Gerätes. Die ersten 24 Bit der MAC-Adresse (Organizationally Unique Identifier, OUI) vergibt das IEEE an Hersteller. Die letzten 24 Bit benutzen die Hersteller, um ihre Geräteschnittstellen eindeutig zu identifizieren.

Einige MAC-Adressen sind reserviert für bestimmte Anwendungen:

MAC-Adresse	Typ	Anwendung
01-00-5E-00-00-00	0800	Internet Multicast [RFC1112]
01-80-C2-00-00-00	-802-	Spanning tree (for bridges)
FF-FF-FF-FF-FF-FF	0806	ARP (for IP and CHAOS) as needed
FF-FF-FF-FF-FF-FF	8035	Reverse ARP

Tab. 16: Beispiele für reservierte MAC-Adressen

9.1.3 IP-MAC-Multicast-Adress-Abbildung

Da beim Versenden von IP-Datenpaketen über Ethernet die IP-Adresse einer MAC-Adresse zugeordnet wird, werden auch IP-Multicast-Adressen auf MAC-Multicast-Adressen abgebildet.
Die 23 niederwertigen Bits der 32-Bit IP-Multicast-Adresse bilden die 23 niederwertigen Bits der 48-Bit MAC-Multicast-Adresse.
Von den übrigen 9 Bit der IP-Multicast-Adresse entfallen 4 Bit auf die Klasse D-Kennzeichnung als Multicast-Adresse.
Die verbleibenden 5 Bit führen dazu, dass 32 IP-Multicast-Adressen auf ein und die selbe MAC-Multicast-Adresse abgebildet werden können.

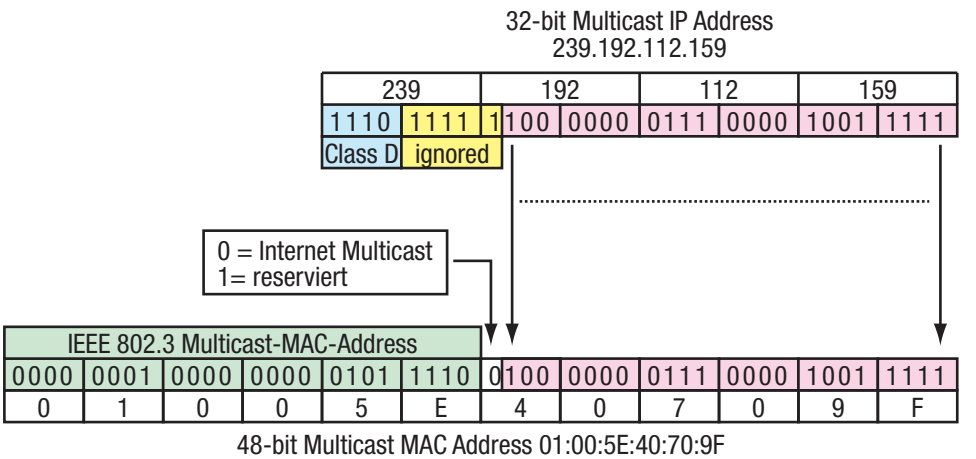


Abb. 40: Umsetzung der IP -Adresse in die MAC-Adresse

9.2 Multicast-Gruppen-registrierung

Das IGMP Internet Group Management Protocol beschreibt die Verteilung von Multicast-Informationen zwischen Routern und Endgeräten auf Schicht 3.
Router mit aktiver IGMP-Funktion verschicken periodisch Anfragen (Query), um zu erfahren, welche IP-Multicast-Gruppen-Mitglieder im Subnetz angeschlossen sind, bzw. wer Interesse an einer Gruppenmitgliedschaft hat. Multicast-Gruppen-Mitglieder antworten mit einer Report-Nachricht. Diese Report-Nachricht enthält alle für das IGMP notwendigen Parameter. Der Router trägt die IP-Multicast-Group-Adresse aus der Report-Nachricht in seine Routing-Tabelle ein. Dies bewirkt, daß er Frames mit dieser IP-Multicast-Group-Adresse im Zieladressfeld ausschließlich gemäß der Routing-Tabelle vermittelt.
Geräte, die nicht mehr Mitglied einer Multicast-Gruppe sein wollen, melden sich mit einer Leave-Nachricht ab (ab IGMP Version 2) und versenden keine Report-Nachrichten mehr. Der Router entfernt den Routing-Tabelleneintrag, wenn er innerhalb einer bestimmten Zeit (Aging Time) keine Report-Nachricht empfängt.

Sind mehrere Router mit aktiver IGMP-Funktion im Subetz, dann

- senden bei IGMP Version 1 alle Router in diesem Subnetz periodisch Queries.
- verhandeln bei IGMP Version 2 und 3 die Router untereinander, welcher Router die Query-Funktion übernimmt (Querier-Election).

Protokoll	Standard
IGMP v1	RFC 1112
IGMP v2	RFC 2236
IGMP v3	RFC 3376

Tab. 17: Standards, die die Multicast-Gruppenregistrierung beschreiben

IGMP Version 2 hat gegenüber IGMP Version 1 den Vorteil, dass ein Multicast-Empfänger seine Mitgliedschaft in einer Multicast-Gruppe kündigen kann und somit seinen Bandbreitenbedarf in kürzerer Zeit wieder frei gibt. Ein weiterer Vorteil ist die Einführung der Querier-Election.

IGMP Version 3 bietet durch die Möglichkeit der Quellfilterung (source filtering) mehr Sicherheit. Multicast-Empfänger können die Quellen definieren, von welchen Sie Multicast-Datenströme empfangen möchten. Multicast-Datenströme mit anderen Quelladressen blockiert der Router.

Die unterschiedlichen Versionen von IGMP sind abwärtskompatibel.
Das bedeutet, dass ein IGMP-Version-3-Router auch Version 1 und Version 2 bearbeiten kann. Bei unterschiedlichen IGMP-Versionen in einem Subnetz einigen sich die beteiligten Router auf die kleinste Version.

9.3 PIM-DM/PIM-SM/DVMRP

Das DVMRP (Distance Vector Multicast Routing Protocoll) ist ein Routing-protokoll, das mit seinem eigenen Distanz-Vektor-Algorithmus seine eigene Multicast-Routing-Tabelle aufbaut. DVMRP arbeitet ähnlich wie RIP und hat eine Begrenzung auf 32 Hops.
In der Vergangenheit war DVMRP sehr verbreitet und kommt heute aus Kompatibilitätsgründen zu bestehenden Anwendungen zum Einsatz.

PIM-DM (Protocol Independent Multicast - Dense Mode) ist ein Routing-protokoll, das die vorliegende Unicast-Routingtabelle anderer Protokolle benutzt, um Multicast Datenströme zu lenken.
Diese Fähigkeit und damit verbunden die schnelle Konvergenz ist wohl der Grund dafür, warum PIM-DM inzwischen sehr verbreitet ist.

DVMRP und PIM-DM sind sogenannte Implizit-Join-Verfahren, d.h. wer sich vom Multicast-Datenstrom abmeldet, den verschont die Datenflut. Um einem Teilnehmer, der sich abgemeldet hat, zu ermöglichen wieder Multicast-Datenströme zu empfangen, vermitteln die Router nach Ablauf der Holdtime wieder an alle Teilnehmer. Bei DVMRP beträgt die Holdtime fest vorgegeben 2 Stunden. Bei PIM-DM beträgt die veränderbare Holdtime 210 Sekunden. PIM-DM setzt voraus, dass Sie die Holdtime auf allen beteiligten Routern auf den gleichen Wert setzen.

DVMRP	PIM-DM
Kennt die Topologie besser, da DVMRP eigenes Protokoll benutzt.	Schnelle Konvergenz Optimierung durch veränderbare Timer

Tab. 18: Vorteile der Protokolle

PIM-SM (Protocol Independent Multicast - Sparse Mode) ist eine erweiterte Variante von PIM-DM.
Diese Version von PIM eignet sich in erster Linie für Netze mit einge-schränkter Bandbreite (z. B. WANs) und für Netze mit wenigen Teilnehmern von Multicast-Gruppen.

PIM-SM unterscheidet sich bei der An- und Abmeldung von Teilnehmern in folgenden Punkten von PIM-DM und DVMRP:

- PIM-DM und DVMRP gehen davon aus, dass sehr viele Teilnehmer Interesse an den Multicast-Gruppen haben. PIM-DM und DVMRP fluten daher zu Beginn der Kommunikation die Information über verfügbare Multicast-Gruppen in das gesamte Netz. Teilnehmer ohne Interesse an einer Multicast-Gruppe melden sich explizit aus dieser Gruppe ab.
- PIM-SM geht hingegen davon aus, dass sehr wenige Teilnehmer im Netz Interesse an den Multicast-Gruppen haben. PIM-SM wartet auf die aktive Anmeldung der Teilnehmer, ohne selbst Informationen über verfügbare Multicast-Gruppen in das Netz zu senden. Alle Teilnehmer, die Interesse an einer Multicast-Gruppe haben, melden sich explizit an einer Gruppe an. Mit diesem Verfahren reduziert PIM-SM den Datenverkehr im Netz.

9.3.1 Die Funktionsweise von PIM-DM und DVMRP

Im ersten Schritt zum Aufbau der Multicast-Routen flutet ein PIM-DM/DVMRP-Router Multicast-Datenströme an allen Ports mit Ausnahme des Empfangports (= Flooding).

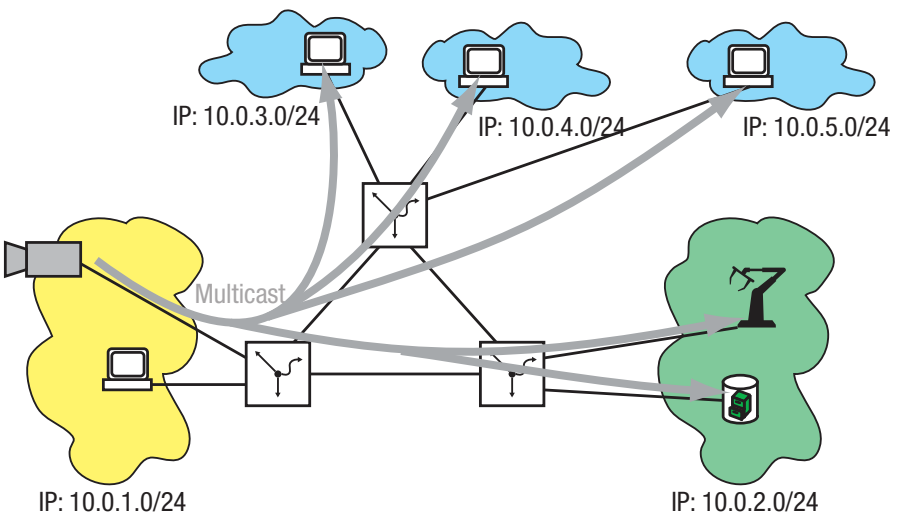


Abb. 41: Multicast Flooding

Router, die kein Interesse an dem Multicast-Datenstrom haben, senden sogenannte Prune-Nachrichten (Ausparnachrichten), um zukünftig von Multicast-Datenströmen dieser Quelle verschont zu bleiben.
Die Router schicken die Prune-Nachrichten zurück in die Richtung, aus welcher sie die Multicast-Datenströme empfangen haben (Upstream).

Ein Router vermittelt einen Multicast-Datenstrom bis zum Ablauf der Hold-time,

- wenn er mittels IGMP einen Multicast-Empfänger ermittelt, welcher direkt oder über einen Switch an einem Port angeschlossen ist oder
- wenn ein Router, der mit einen Multicast-Empfänger verbunden ist, direkt an einem Port angeschlossen ist.

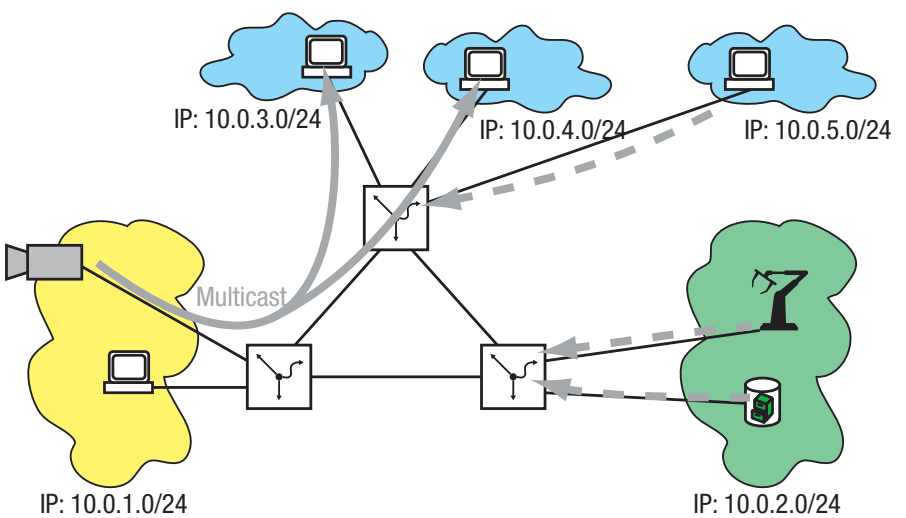


Abb. 42: Multicast Pruning

Im zweiten Schritt berechnet PIM-DM/DVMRP die kürzesten Pfade (SPT - Shortest Path Tree) zwischen der Multicast-Quelle und den Multicast-Empfängern. Das Ergebnis ist der quellengeführte (source routed) Multicast-Verteilungsbaum. Quellengeführt heißt, der Ansatz zur Berechnung ist die Rückwärtsverfolgung vom Empfänger zur Quelle (RPF - Reverse Path Forwarding). Zur Vermeidung von Schleifen verwirft RPF alle Multicast-Datenströme, die ein Port empfängt, der einem längeren Pfad als dem kürzesten angehört.

Die Methode der kürzesten Pfade ist bezüglich der Datenpfade sehr effizient. Sie hat aber den Nachteil, dass je nach Topologie die Router sehr viel Speicherplatz benötigen, um die vielen Multicast-Bäume zu speichern.

Ein Teilnehmer, der sich vom Multicast-Datenstrom abgemeldet hat, kann sich wieder für den Multicast-Datenstrom anmelden. Dieser Vorgang heißt Grafting. Grafting ermöglicht dem Teilnehmer noch vor Ablauf der Holdtime wieder Multicast-Datenströme vermittelt zu bekommen.

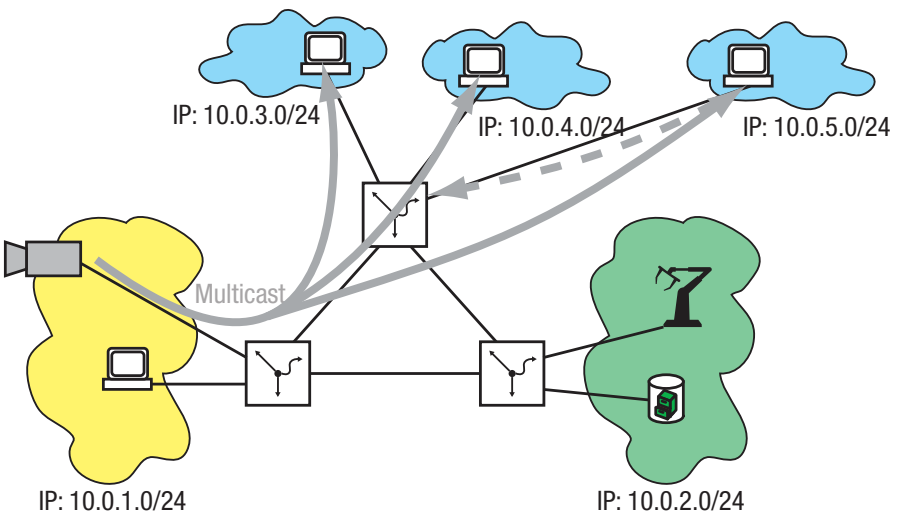


Abb. 43: Multicast Grafting

9.3.2 Die Funktionsweise von PIM-SM

PIM-SM unterscheidet sich gegenüber PIM-DM und DVMRP in der Topologie der Multicast-Verteilung:

- PIM-DM und DVMRP nutzen in jedem Fall die direkten Pfade (SPT – Shortest Path Tree) zwischen der Multicast-Quelle und den Multicast-Empfängern.
- PIM-SM nutzt in der Standardeinstellung den Pfad über einen zentralen Vermittlungspunkt (Rendezvous-Point – RP). Dieser Pfad heißt Rendezvous-Point-Tree (RPT). Die Multicast-Empfänger melden beim Rendezvous-Point das Interesse an einer Multicast-Gruppe an. Die Multicast-Quellen registrieren sich bei einem Rendezvous-Point und senden die Daten ausschließlich an diesen Rendezvous-Point, der die Daten an die Multicast-Empfänger weiterleitet. Für jede Gruppe gibt es genau einen Rendezvous-Point. Ein PIM-SM-Router dient für eine oder mehrere Multicast-Gruppen als Rendezvous-Point. Der Rendezvous-Point-Tree erstreckt sich zwischen dem Rendezvous-Point der Multicast-Gruppe und den Multicast-Empfängern. Die Empfänger einer Multicast-Gruppe teilen sich diesen RPT als Shared-Tree. Mit diesem Verfahren reduziert PIM-SM die Anzahl der gespeicherten Tree-Informationen in den Routern und senkt so die Prozessor-Last der Geräte.

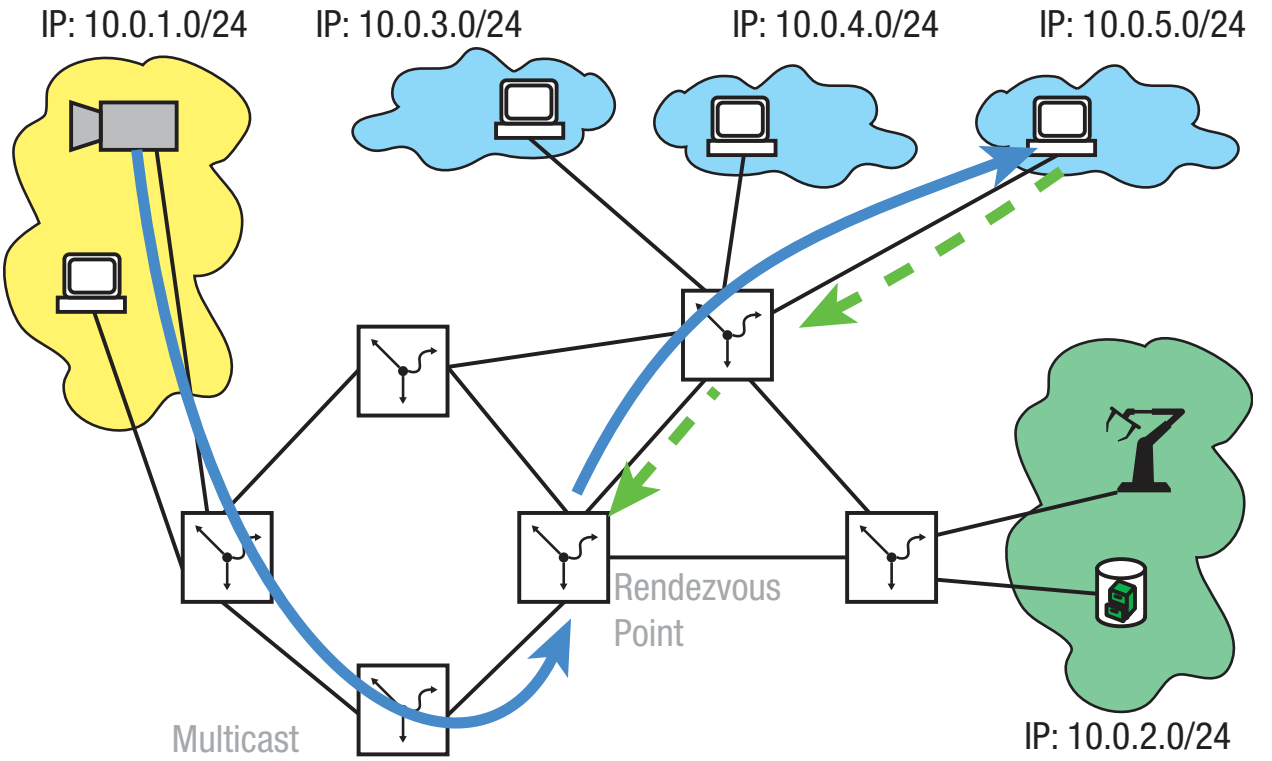


Abb. 44: Rendezvous Point im PIM-SM-Protokoll

Je nach Anwendung existieren kürzere Wege zwischen dem Multicast-Empfänger und der Multicast-Quelle als den Rendezvous-Point-Tree. In diesen Fällen ermöglicht PIM-SM den Wechsel auf den direkten Pfad SPT. Wenn die Datenrate der Multicast-Übertragung über den RPT einen konfigurierbaren Grenzwert übersteigt, meldet sich der Router des Multicast-Empfängers vom Rendezvous-Point ab. Stattdessen erstellt der Router des Multicast-Empfängers eine direkte Verbindung zum letzten Router vor der Multicast-Quelle.

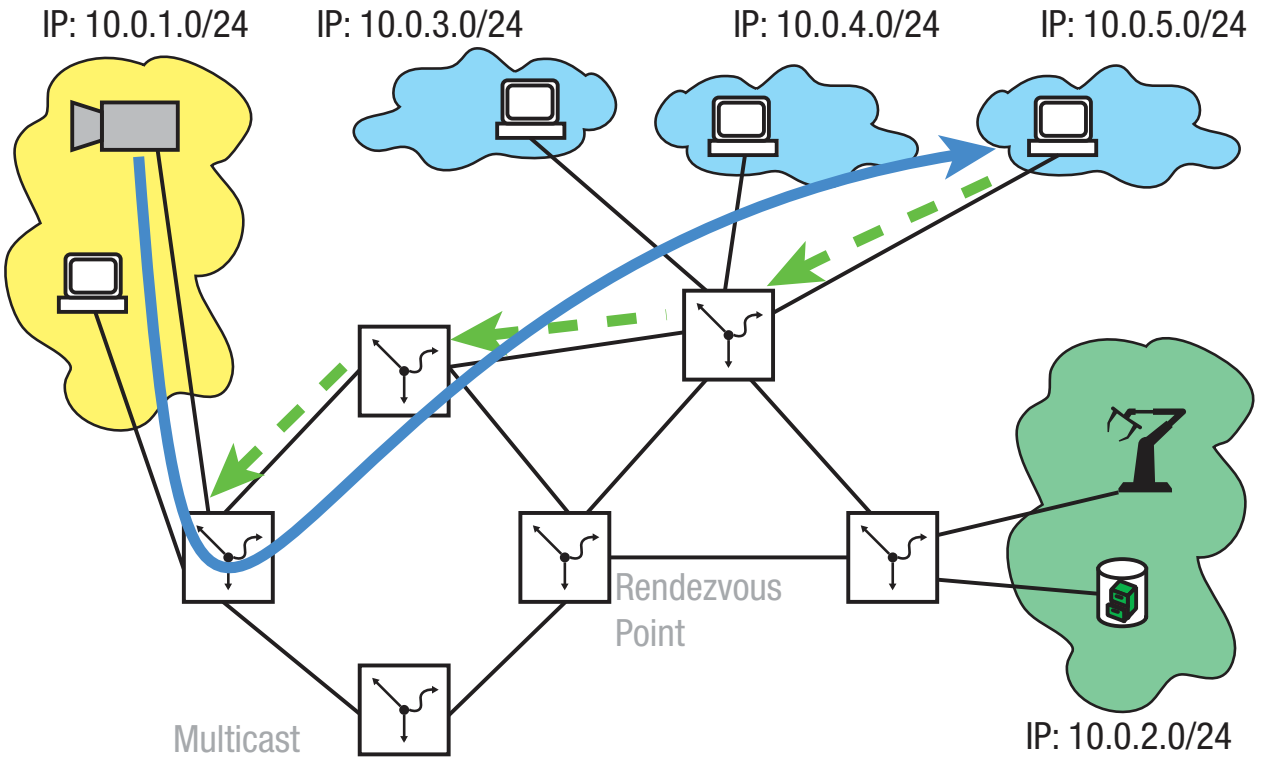


Abb. 45: Topologiewechsel vom RPT auf den direkten Pfad (STP)

- **Designated Router**
  Ein Teilnehmer, der Interesse an einer Multicast-Gruppe hat, sendet eine entsprechende IGMP-Nachricht an den nächsten erreichbaren Router. Dieser Router sendet daraufhin eine Join-Nachricht in Richtung des Rendezvous-Point. Liegen zwischen dem sendenden Router und dem Rendezvous-Point weitere Router, leiten diese die Join-Nachricht weiter. Diese Übertragung endet entweder am Rendezvous-Point selbst oder an einen bereits vorhandenen Zweig des RPT. PIM-SM erzeugt oder ergänzt nach der Anmeldung des Teilnehmers den Pfad zwischen dem Rendezvous-Point und dem Teilnehmer. Wenn sich ein Teilnehmer aus einer Multicast-Gruppe abmeldet, sendet der vom Teilnehmer aus nächste erreichbare Router eine Prune-Nachricht an den Rendezvous-Point. Die Prune-Nachricht reduziert so den RPT um den zugehörigen Zweig.
  In einem Netz mit mehreren PIM-SM-Routern übernimmt genau ein Router die Übertragung der Join- und Prune-Nachrichten zwischen den Multicast-Empfängern und dem Rendezvous-Point. Dieser Vorgang ist in der folgenden Abbildung durch grüne Pfeile dargestellt. Auch auf Seiten der Multicast-Quellen registriert einer der PIM-SM-Router die verfügbaren Multicast-Gruppen beim Rendezvous Point. Diesen Vorgang zeigt

die Abbildung mit blauen Pfeilen. Diese Router heißen Designated-Router (DR). In der Standard-Einstellung wählen die Router den Designated-Routers anhand der IP-Adresse aus. Der PIM-SM-Router mit der höchsten IP-Adresse in einem Netzsegment übernimmt die Aufgabe des Designated-Routers. Die Einstellung einer speziellen Priorität für die Designated-Router ermöglicht die gezielte Steuerung der DR-Auswahl. In diesem Fall übernimmt der Router mit der höchsten Priorität die Aufgaben des Designated-Routers. Ausschließlich bei gleichen Prioritäten fließt die IP-Adresse in den Auswahlprozess mit ein.

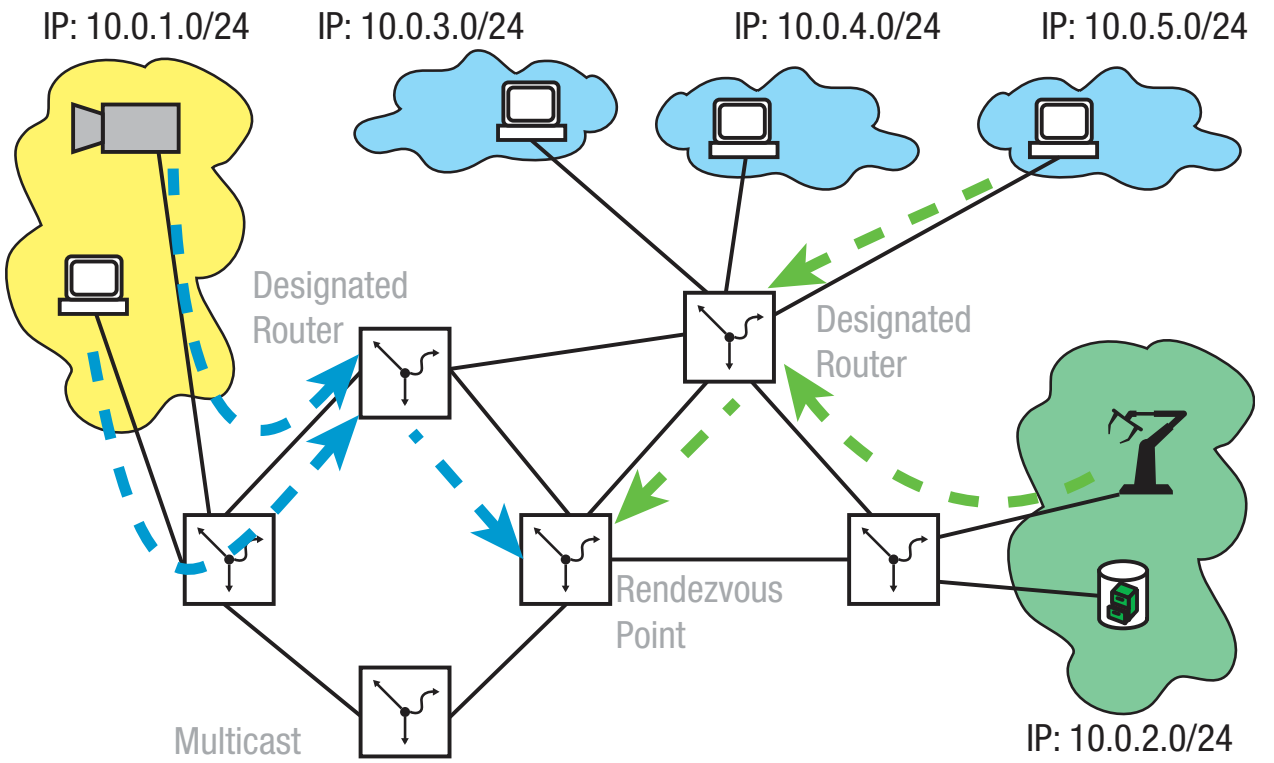


Abb. 46: Designated-Router leiten Nachrichten von Multicast-Quellen und Multicast-Teilnehmern an den Rendezvous-Point weiter

Bootstrap-Router

PIM-SM bietet 2 Verfahren zur Auswahl des Rendezvous-Points für eine Multicast-Gruppe:

- Statische RP-Konfiguration

  Bei diesem Verfahren arbeitet einer der Router im Netz fest als Rendezvous Point für eine Multicast-Gruppe. Die anderen Router enthalten in ihrer Konfiguration die IP-Adresse dieses Routers und die Adresse der zugehörigen Multicast-Gruppe.

- Dynamische RP-Konfiguration nach dem Bootstrap-Router-Verfahren (BSR)

  Bei diesem Verfahren ermitteln die Router im Netz den Rendezvous-Point dynamisch. Ein Router hat die Möglichkeit, sich selbst als Kandidat für die Aufgabe als Rendezvous-Point anzubieten. Das dynamische Verfahren nutzt Bootstrap-Router für die Auswahl des Rendezvous-Points für eine Multicast-Gruppe. Die Bootstrap-Nachrichten informieren auch die anderen Router in der PIM-SM-Domäne über den als Rendezvous-Point ausgewählten Router. Die PIM-SM-Router leiten die Bootstrap-Nachrichten innerhalb der PIM-SM-Domäne weiter. Die PIM-SM-Domäne besteht aus allen erreichbaren Routern mit aktiviertem PIM-SM-Protokoll. Ein aktiver PIM-SM-Router hat die Möglichkeit, als BSR-Border die Domäne gezielt zu begrenzen. Ein so konfigurierter Router verwirft die empfangenen BSR-Nachrichten.

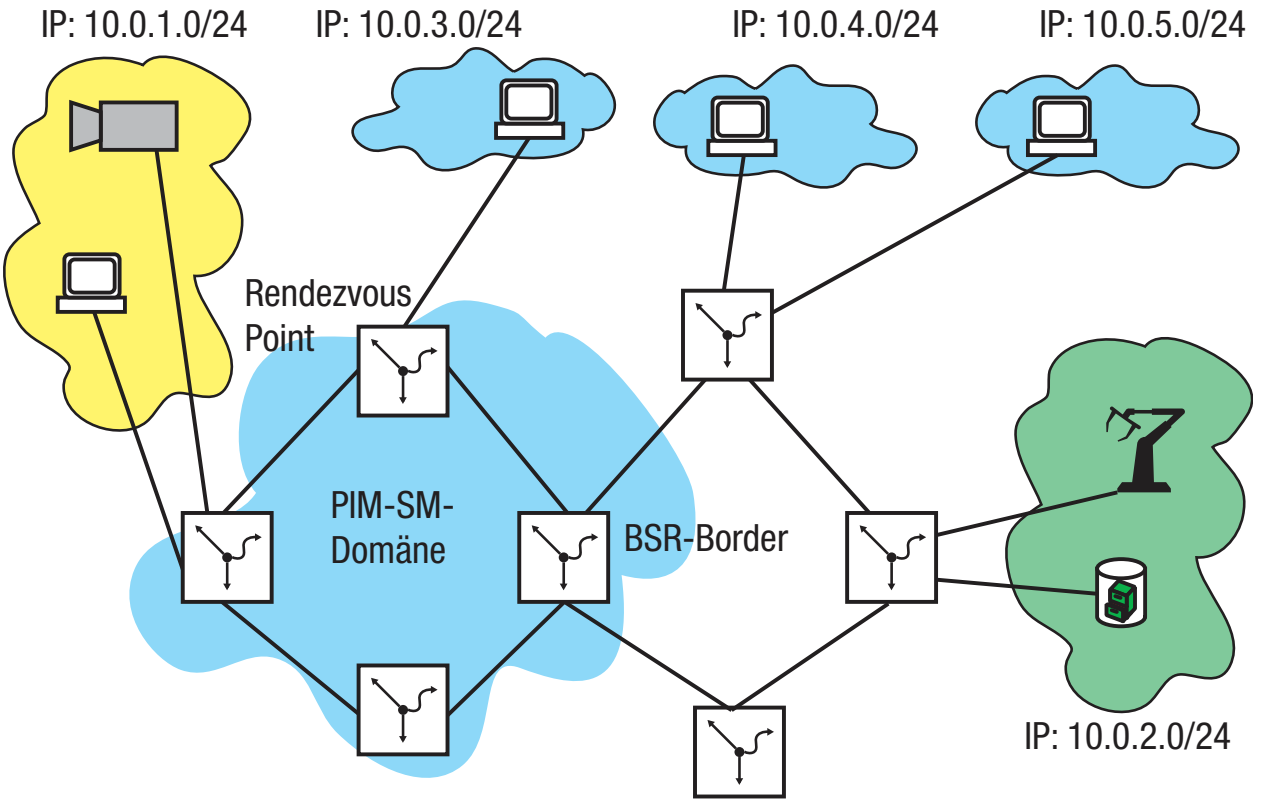


Abb. 47: Router in der Konfiguration als BSR-Border verwerfen Bootstrap-Nachrichten und begrenzen die PIM-SM-Domäne

Anwendungsbeispiel für PIM-SM

Das folgende Beispiel zeigt Ihnen, wie Sie PIM-SM mit Hilfe des Command Line Interface konfigurieren.

Aufgabenstellung:

- PIM-SM Beispielkonfiguration (siehe folgende Abb.) aufbauen.
- IGMP, OSPF und PIM-SM konfigurieren.
- RP statisch konfigurieren.
- Multicast Adressbereich 239.1.0.0/16 verwenden.

Anmerkung: Das im Beispiel verwendete Unicast(UC)-Protokoll ist OSPF. Sie können statt OSPF auch RIP verwenden.

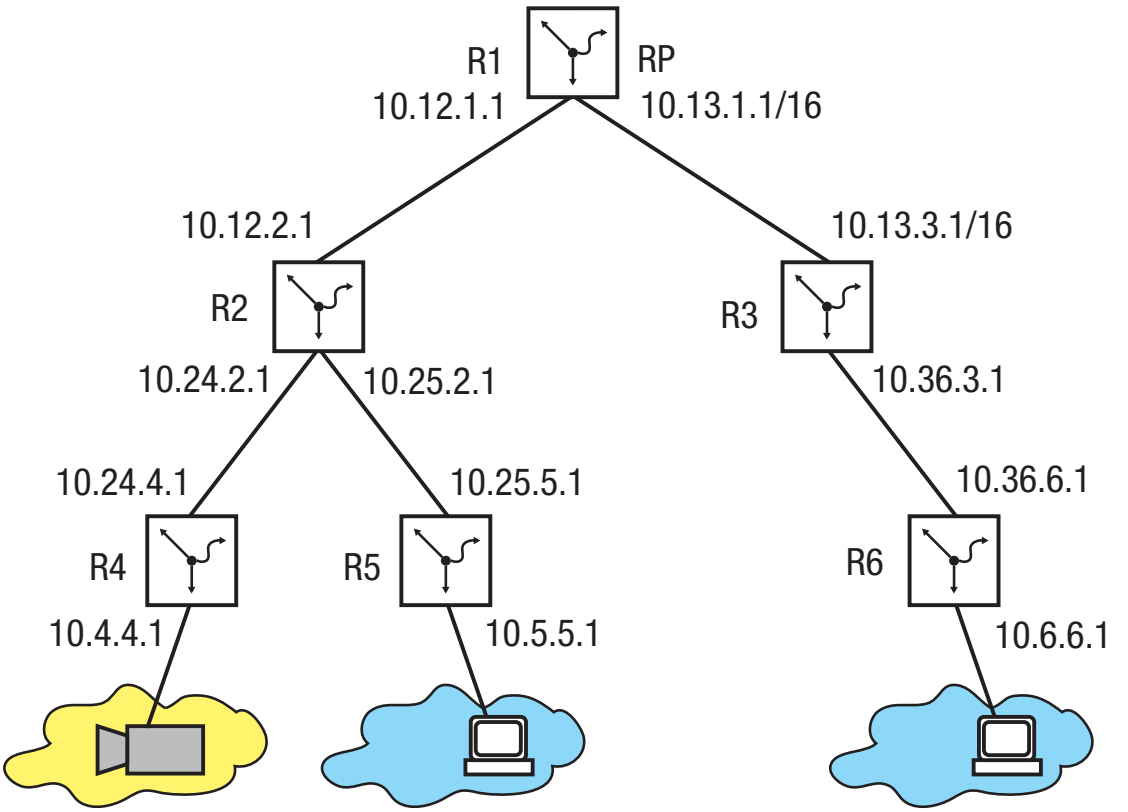


Abb. 48: Beispielkonfiguration für PIM-SM

☐ Mit der folgenden CLI-Kommandosequenz konfigurieren Sie PIM-SM.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`# set prompt Rx`	Zur besseren Orientierung Eingabeprompt setzen (x = Routernummer)
# configure	Wechsel in den Konfigurationsmodus.
(Config)# ip routing	Routing einschalten
(Config)# show ip brief	IP-Informationen im Überblick anzeigen.
(Config)# router ospf	UC-Routing-Protokoll global einschalten. Wechsel in den Router-Konfigurationsmodus für OSPF (Open Shortest Path First).
(Config-router)# router-id x.1.1.1	
(Config-router)# enable	
(Config-router)# redistribute connected [subnets]	
(Config-router)# exit	Wechsel zurück in den Konfigurationsmodus.
(Config)# ip igmp	IGMP global einschalten (automatisch schaltet MC Routing und IGMP Routing ein).
(Config)# ip multicast	Multicast Forwarding (Routing) einschalten.
(Config)# ip pimsm	PIM-SM global einschalten.

(Config)# ip pimsm rp-address <ip-@> <MC @>…	Den statischen Rendezvous-Point für einen Multicast-Bereich setzen.
(Config)# interface <s/p>	Routing Interfaces (Slot/Port) konfigurieren.
(Interface s/p)# ip address <ip-@> <mask>	IP-Adresse und Subnetzmaske für das Interface konfigurieren.
(Interface s/p)# routing	Routing an dem Interface einschalten.
(Interface s/p)# ip ospf area-id 0.0.0.0	UC-Routing-Protokoll pro Interface konfigurieren.
(Interface s/p)# ip ospf	OSPF auf dem Interface aktivieren.
(Interface s/p)# ip igmp	IGMP pro Interface aktivieren.
(Interface s/p)# ip igmp version <1|2|3>	Optional: Version ändern (Lieferzustand: 2).
(Interface s/p)# ip pimsm mode	PIM-SM an den entsprechenden Interfaces einschalten.
(Interface s/p)# exit	Wechsel in den Konfigurationsmodus.
(Config)# exit	Wechsel in den Privileged-EXEC-Modus.
# show ip pimsm	PIM-SM Status des Routers anzeigen.
# copy system:running-config nvram:startup-config	Aktuelle Konfiguration ins NVRAM speichern.
# logout	CLI-Session beenden.

Anmerkung: Konfigurieren Sie den Rendezvous-Point (RP) an allen Routern, an denen Sie PIM-SM eingeschaltet haben, auch am RP selbst. Alternativ definieren Sie mindestens einen Bootstrap-Router (BSR) und mindestens einen RP-Kandidaten.
Wenn Sie die Vorteile der Redundanz-Funktion nutzen wollen, konfigurieren Sie 2 RP-Kandidaten and 2 BSR-Kandidaten.

☐ Die folgenden CLI show-Kommandos zeigen die PIM-SM-, Multicast- und IGMP-Parameter Ihrer aktuellen Konfiguration an.

`(Interface s/p)# show`	Mögliche show-Kommandos anzeigen.
# show ip pimsm	Aktuelle PIM-SM-Konfiguration anzeigen.
# show ip mcast	Aktuelle Multicast-Konfiguration anzeigen.
# show ip igmp	Aktuelle IGMP-Konfiguration anzeigen.

☐ Optional führen Sie anschließend folgende Konfigurationen durch:

`(Interface s/p)# ip pimsm dr-priority <0…2.147.483.647>`	DR-Priorität konfigurieren.
(Interface s/p)# ip pimsm hello-interval <0…18000>	Hello-Intervall in Sekunden konfigurieren (Lieferzustand: 30 s).

☐ Optional: Statt die RPs statisch zu definieren, können Sie BSR- und RP-Kandidaten konfigurieren, aus denen BSR and RP gewählt werden.

`(Config)# ip pimsm bsr-candidate interface <slot/port>`	BSR-Kandidat konfigurieren.
`(Config)# ip pimsm rp-candidate interface <slot/port>`	RP-Kandidat konfigurieren.

9.4 Scoping

Bei der Multicast-Vermittlung stellt das Protokoll zwei Möglichkeiten zur Verfügung, um die Ausdehnung des Multicast-Datenstromes zu begrenzen:

- Multicast Address Scoping / Boundary
  Beim Multicast Adress Scoping weist der Administrator einem Router-Interface einen Multicast-IP-Adressbereich zu (siehe Tabelle 15). Das Router-Interface blockiert Multicast-Datenströme mit Adressen innerhalb dieses Adressbereichs.
  Beispiel:
  `ip mcast boundary 239.193.122.0 255.255.255.0`
  In diesem Beispiel blockiert das Router-Interface Multicast-Datenströme mit einer Multicast-IP-Adresse im Bereich 239.193.122.0-239.193.122.255.
- TTL Scoping
  Jedes Multicast-Datenpaket enthält eine TTL (Time-to-live). Die TTL ist ein Zähler, den jeder Router beim Vermitteln des Multicast-Datenpaketes dekrementiert.
  Beim TTL Scoping weist der Administrator einem Interface eine TTL-Schwelle zu. Das Router-Interface blockiert jedes Multicast-Datenpaket, dessen TTL unterhalb der TTL-Schwelle liegt.
  Beispiel:
  `ip multicast ttl-threshold 64`
  In diesem Beispiel blockiert das Router-Interface Multicast-Datenströme mit einer TTL, deren Wert kleiner 64 ist.

TTL	Reichweite
0	Beschränkt auf denselben Host
1	Beschränkt auf dasselbe Subnetz
< 32	Beschränkt auf einen bestimmten Standort, Organisation oder Abteilung
< 64	Beschränkt auf dieselbe Region
< 128	Beschränkt auf denselben Kontinent
< 255	Unbeschränkt, global

Tab. 19: Übliche Reichweite für TTLs

9.5 Multicast-Konfiguration

Wählen Sie das für Ihre Anwendung günstigste Multicast-Protokoll.
Da die Multicast-Routing-Protokolle unterschiedliche Methoden zur Multicast-Vermittlung anwenden, verhindert der Router den gleichzeitigen Betrieb von mehr als einem Multicast-Routing-Protokoll.
Beim Aktivieren eines Multicast-Routing-Protokolls deaktiviert der Router ein eventuell aktives Multicast-Routing-Protokoll.

9.5.1 Beispiel mit Layer 3-Redundanz

Die Multicast-Konfiguration umfasst folgende Schritte:

- Routing-Funktion auf den beteiligten Routern konfigurieren z.B. mit OSPF (siehe auf Seite 113 „OSPF konfigurieren“).
- Eventuell Multicast-Adressen festlegen.
- Router-Interfaces konfigurieren. Hierzu gehört auch
  - die Festlegung der Multicast-Grenzen,
  - das Einschalten von IGMP und
  - das Einschalten des gewählten Multicast-Routing-Protokolls.
- IGMP und somit auch IGMP-Snooping global einschalten.
- Multicast-Routing-Protokoll global einschalten.
- Multicast-Vermittlung (Forwarding) einschalten.

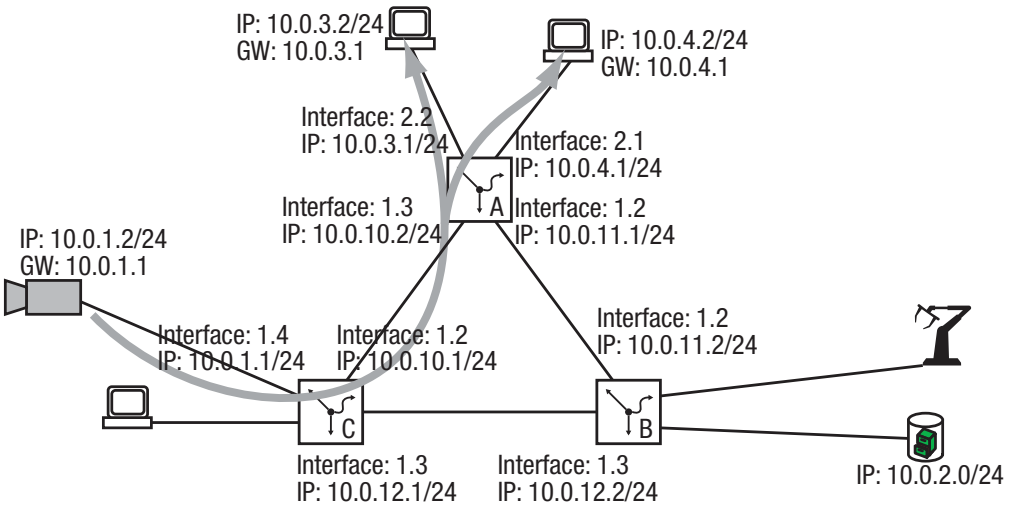


Abb. 49: Multicast-Beispielkonfiguration

☐ Router-Interfaces konfigurieren am Beispiel Router A (siehe Abbildung 49):

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/1.
`ip multicast ttl-threshold 3`	Schwelle für Multicast-Ausdehnung setzen (siehe auf Seite 145 „Scoping“).
`ip igmp`	IGMP am Port einschalten.
`ip pimdm mode`	PIM-DM als Multicast-Protokoll einschalten.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 2/2`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/2.
`ip multicast ttl-threshold 3`	Schwelle für Multicast-Ausdehnung setzen (siehe auf Seite 145 „Scoping“).
`ip igmp`	IGMP am Port einschalten.
`ip pimdm mode`	PIM-DM als Multicast-Protokoll einschalten.
`exit`	Wechsel in den Konfigurationsmodus.

`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface 1/3.
`ip multicast ttl-threshold 3`	Schwelle für Multicast-Ausdehnung setzen (siehe auf Seite 145 „Scoping“).
`ip igmp`	IGMP am Port einschalten.
`ip pimdm mode`	PIM-DM als Multicast-Protokoll einschalten.
`exit`	Wechsel in den Konfigurationsmodus.

☐ IGMP global einschalten am Beispiel Router A (siehe Abbildung 49):

`ip igmp`	IGMP am Port einschalten.

☐ Multicast global einschalten am Beispiel Router A (siehe Abbildung 49):

`ip pimdm`	Im Konfigurationsmodus Multicast-Routing-Protokoll auswählen.
`ip multicast`	Multicast-Vermittlung global einschalten.
`exit`	Wechsel in den Privileged-EXEC-Modus.

☐ Prüfen der Multicast-Routing-Einstellungen

```
#show ip pimdm

Admin Mode..................................... Enable

    PIM-DM INTERFACE STATUS
Interface Interface Mode  Protocol State
--------- --------------- ---------------
1/3       Enable          Operational
2/1       Enable          Operational
2/2       Enable          Operational
#show ip mcast

Admin Mode..................................... Enable
Protocol State................................. Operational
Table Max Size ................................ 256
Number Of Packets For Which Source Not Found .. 0
Number Of Packets For Which Group Not Found ... 0
Protocol....................................... PIMDM
Entry Count ................................... 0
Highest Entry Count ........................... 0
#show ip mcast mroute summary

                  Multicast Route Table Summary
                                          Incoming  Outgoing
Source IP       Group IP        Protocol  Interface Interface List
--------------- --------------- --------  --------- ---------------
10.0.1.159      239.192.1.1     PIMDM     1/3       2/1
10.0.1.159      239.192.1.1     PIMDM     1/3       2/2
```

```
#show ip igmp

IGMP Admin Mode.............................. Enable

    IGMP INTERFACE STATUS
Interface Interface Mode  Protocol State
--------- --------------- ---------------
1/2       Enable          Operational
1/3       Enable          Operational
2/1       Enable          Operational
2/2       Enable          Operational
#show ip igmp interface 2/1

Slot/Port.................................... 2/1
IGMP Admin Mode.............................. Enable
Interface Mode............................... Enable
IGMP Version................................. 2
Query Interval (secs)........................ 125
Query Max Response Time (1/10 of a second)..... 100
Robustness................................... 2
Startup Query Interval (secs) ............... 1
Startup Query Count.......................... 2
Last Member Query Interval (1/10 of a second).. 10
Last Member Query Count...................... 2
```

☐ Konfigurieren Sie Router B und Router C analog zu Router A.

9.5.2 Beispiel mit Layer 2-Redundanz (HIPER-Ring)

Dem HIPER-Ring ist das VLAN 1 zugeordnet.

☐ Weisen Sie den angeschlossenen VLANs andere VLAN-IDs zu und belassen Sie den HIPER-Ring ausschließlich in VLAN 1. So gewährleisten Sie die Vermittlung der Multicast-Datenströme auf Layer 3.

Wenn Sie dem HIPER-Ring mehrere VLANs als Transfernetze zuweisen, dann vermittelt der Switch während der Flut- und Abmeldephase (Flood and Prune) die Multicast-Datenströme in jedes Transfernetz. Das heißt, der Switch vermittelt die Multicast-Datenströme in jedes VLAN und somit vervielfacht sich die Netzlast im HIPER-Ring.

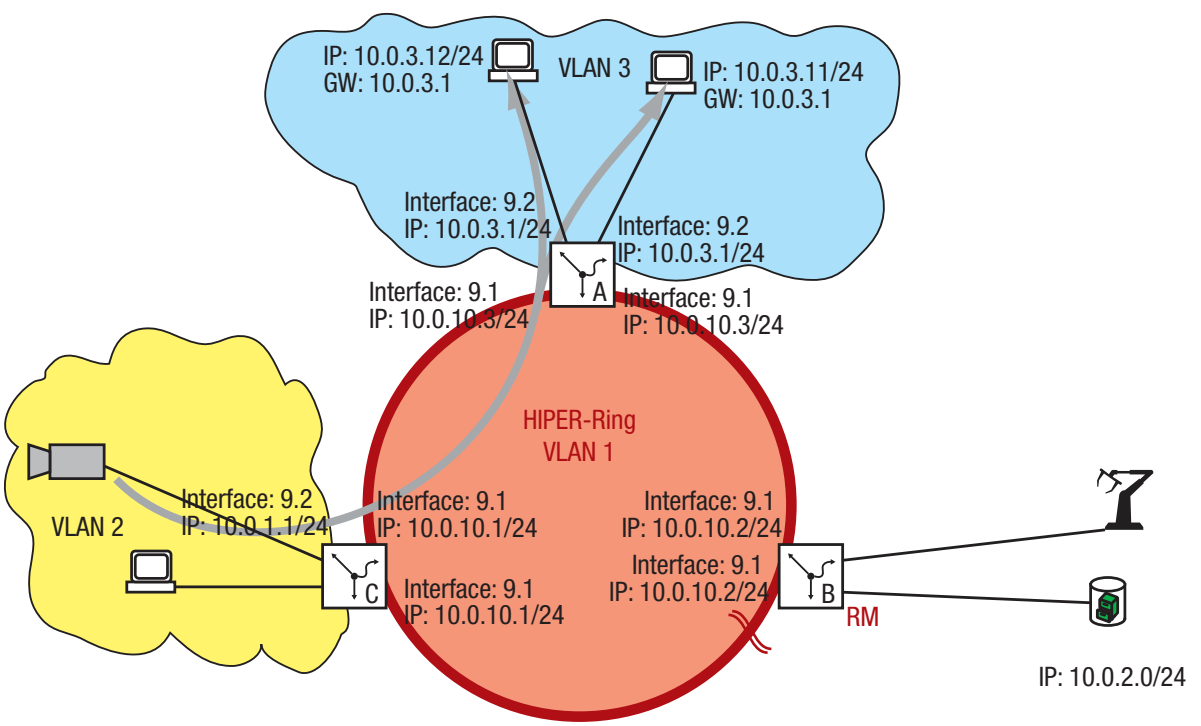


Abb. 50: Multicast-Beispielkonfiguration mit HIPER-Ring

9.5.3 Tipps für die Konfiguration

- **Auswahl des PIM-DM Multicast-Routing-Protokolls**
  PIM-DM wählen Sie, wenn Ihre Anwendung schnelle Umschaltzeiten fordert und eventuelle Paketdoppelungen während der Umschaltzeit tolerieren kann. Schnelle Umschaltzeiten erzielen Sie durch das Reduzieren der „Hello Time“.
  Paketdoppelungen treten auf, wenn mehrere Router an einem Subnetz angeschlossen sind. In diesem Fall klärt der „Assert Prozess“, welcher Router in das Subnetz senden darf. Bis zur Klärung senden alle Router in dieses Subnetz.

- **Auswahl des DVMRP Multicast-Routing-Protokolls**
  DVMRP wählen Sie, wenn Ihre Anwendung keine Paketdoppelungen toleriert und mit höheren Umschaltzeiten zufrieden ist.
  Einen großen Vorteil bietet DVMRP beim Einsatz von verteilten Subnetzen/VLANs in einem HIPER-Ring. Durch die Unicast-Tabelle kennt DVMRP schon die Topologie und verhindert so Paketdoppelungen.

- **Auswahl des PIM-SM Multicast-Routing-Protokolls**
  PIM-SM wählen Sie, wenn Ihre Anwendung wenig Teilnehmer hat und Sie für Ihre Anwendung längere Wege tolerieren.
  In diesem Fall bietet PIM-SM den Vorteil, dass das erzeugte Datenvolumen in den Routern gering bleibt.

- **Konfiguration als Rendevouz-Point bei PIM-SM**
  Bei der Nutzung von PIM-SM haben Sie die Möglichkeit, einen Router als Rendevouz-Point-Kandidaten für eine Multicast-Gruppe zu definieren. Geben Sie dazu die Multicast-Gruppe an, für welche sich der Router als Rendevouz-Point anbietet.

`enable`	Wechsel in den Privilegded-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.

`ip pimsm rp-candidate interface 1/1 225.1.1.1 255.255.255.0`	Aktivierung des Routers als möglicher Rendezvouz-Point für die Gruppe 225.1.1.1/24.
`no ip pimsm rp-candidate interface 1/1 225.1.1.1 255.255.255.0`	Deaktivierung des Routers als möglicher Rendevouz-Point.

Konfiguration des Limits für den Wechsel auf SPT

Bei der Nutzung von PIM-SM haben Sie die Möglichkeit, auf den letzten Routern von den Multicast-Empfängern das Limit für den Wechsel zum SPT zu definieren. Geben Sie dazu das Limit für den Datendurchsatz in Kbit/s an, bei dessen Erreichen der Router auf den kürzesten Pfad SPT wechselt.

`enable`	Wechsel in den Privilegded-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip pimsm spt-threshold 1000`	Aktivierung des Limits von 1000 Kbit/s für den Wechsel auf den SPT.
`no ip pimsm spt-threshold`	Deaktivierung des Limit für den Wechsel auf den SPT.

Konfiguration als Designated-Router bei PIM-SM

Bei der Nutzung von PIM-SM haben Sie die Möglichkeit, einen Router als Designated-Router-Kandidaten zu definieren. Geben Sie dazu die Priorität an, mit der sich der Router als Designated-Router anbietet.

`enable`	Wechsel in den Privilegded-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip pimsm dr-priority 2/1 priority 2000`	Aktivierung des Routers als möglicher Designated-Router mit der Priorität 2000.
`no ip pimsm dr-priority 2/1`	Deaktivierung des Routers als möglicher Designated-Router.

Konfiguration als Bootstrap-Router bei PIM-SM

Bei der Nutzung von PIM-SM haben Sie die Möglichkeit, einen Router als Bootstrap-Router-Kandidaten zu definieren. Geben Sie dazu die Priorität an, mit der sich der Router als Bootstrap-Router anbietet.

`enable`	Wechsel in den Privilegded-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip pimsm bsr-candidate 2/1 priority 20`	Aktivierung des Routers als möglicher Bootstrap-Router mit der Priorität 20.
`no ip pimsm bsr-candidate 2/1`	Deaktivierung des Routers als möglicher Bootstrap-Router.

Begrenzen der PIM-SM-Domäne

Wenn Sie ein Interface des Gerätes als BSR-Border definieren, dann leitet der Router keine BSR-Nachrichten über dieses Interface weiter. Auf diese Weise begrenzt der Router die PIM-SM-Domäne.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 2.1
`ip pimsm bsr-border`	Deaktiviert das Weiterleiten von BSR-Nachrichten über Interface 2.1.
`no ip pimsm bsr-border`	Erlaubt das Weiterleiten von BSR-Nachrichten über das Interface 2.1.

Verkürzen der Umschaltzeiten

Sowohl bei DVMRP als auch bei PIM-DM können Sie durch Herabsetzen des IGMP-Querier-Intervalls am Router-Interface die Umschaltzeiten verkürzen. Diese Verkürzung tritt ein, wenn ein ausgefallener Router, an dem Multicast-Empfänger angeschlossen sind, wieder aktiv wird.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 2/1.
`ip igmp query-max-response-time 10`	Query-Max-Response-Zeit kleiner als das Query-Intervall setzen, in diesem Beispiel: 1 Sekunde, Voreinstellung: 10 Sekunden
`ip igmp query-interval 5`	Query-Intervall setzen, in diesem Beispiel: 5 Sekunden, Voreinstellung: 125 Sekunden.

Bei PIM-DM kann ein Router durch die Verkürzung der „Hello Time“ den Ausfall bzw. das wieder Inbetriebgehen eines Downstream-Routers schneller erkennen.

`ip pimdm query-interval 1`	Das PIM-DM-Query-Intervall („Hello Time“) setzen, in diesem Beispiel: 1 Sekunde, Voreinstellung: 30 Sekunden

Bei PIM-DM kann die Verwendung einer eingetragenen Default-Route die Umschaltzeit verkürzen. Während der Router noch Informationen über den Weg zur Quelle sammelt (RPF) kann der Router eine eingetragene Default-Route benutzen.

`ip route 10.0.3.0 255.255.255.0 10.0.2.2`	Statische Default-Route erstellen.
`exit`	Wechsel in den Konfigurationsmodus.

Besonderheit bei VLAN-Routing

Der Router flutet einen Multicast-Datenstrom an allen Ports eines VLAN-Routing-Interfaces, wenn

– der Multicast-Datenstrom aus einem anderen Subnetz kommt und
– sich mindestens ein Empfänger an diesem VLAN-Interface für diesen Multicast-Datenstrom über IGMP registriert hat.

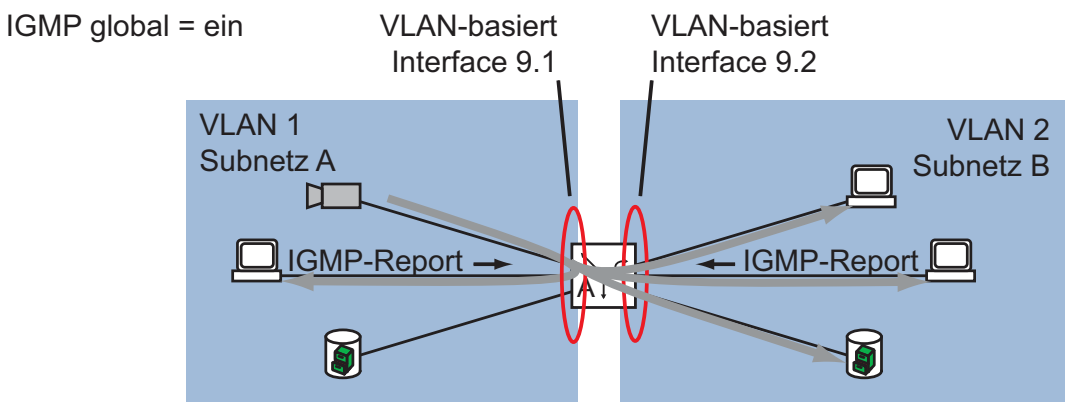


Abb. 51: Registrierter Multicast Datenstrom am VLAN-Routing-Interface

A Anhang

A.1 Verwendete Abkürzungen

ABR	Area Border Router
ACA	AutoConfiguration Adapter
AS	Autonomous System
ASBR	Autonomous System Border Router
BC	Broadcast
BDR	Backup designated Router
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
CIDR	Classless Inter Domain Routing
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol)
DR	Designated Router
DVMRP	Distance Vector Multicast Routing Protocol
EUI	Extended Unique Identifier
FDB	Forwarding Database
GARP	General Attribute Registration Protocol
GMRP	GARP Multicast Registration Protocol
http	Hypertext Transfer Protocol
HiVRRP	Hirschmann Virtual Router Redundancy Protocol
IANA	Internet Assigned Numbers Authority
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IGP	Interior Gateway Protocol
IP	Internet Protocoll
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
LSA	Link Status Advertisement
LSD	Link State Database
LWL	Lichtwellenleiter
MAC	Media Access Control
MC	Multicast
MICE	Modular Industrial Communication Equipment
NSSA	Not So Stubby Area
NTP	Network Time Protocol
OSPF	Open Shortest Path First
OUI	Organizationally Unique Identifier
PC	Personal Computer
PIM-DM	Protocol Independent Multicast-Dense Mode

PIM-SM	Protocol Independent Multicast-Sparse Mode
PTP	Precision Time Protocol
RFC	Request For Comment
RM	Redundanz Manager
RS	Rail Switch
RSTP	Rapid Spanning Tree Protocol
RIP	Routing Information Protocol
RPF	Reverse Path Forwarding
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SPT	Shortest Path Tree
TCP	Transfer Control Protocol
tftp	Trivial File Transfer Protocol
TP	Twisted Pair
TTL	Time-to-live
UDP	User Datagramm Protocol
URL	Uniform Resourve Locator
UTC	Coordinated Universal Time
VL	Virtual Link
VLAN	Virtual Local Area Network
VLSM	Variable Length Subnet Mask
VRID	Virtual Router Identification
VRRP	Virtual Router Redundancy Protocol

A.2 Zugrundeliegende IEEE-Normen

- IEEE 802.1AB
  Topology Discovery (LLDP)
- IEEE 802.1D
  Switching, GARP, GMRP, Spanning Tree (Supported via 802.1S implementation)
- IEEE 802.1D-1998
  Media Access Control (MAC) Bridges (includes IEEE 802.1p Priority and Dynamic Multicast Filtering, GARP, GMRP)
- IEEE 802.1Q-1998
  Virtual Bridged Local Area Networks (VLAN Tagging, Port Based VLANs, GVRP)
- IEEE 802.1S
  Multiple Spanning Tree
- IEEE 802.1v
  Protocol Based VLANs
- IEEE 802.1 w.2001
  Rapid Reconfiguration, Supported via 802.1S implementation
- IEEE 802.1 X
  Port Authentication
- IEEE 802.3 - 2002
  Ethernet
- IEEE 802.3 ac
  VLAN Tagging
- IEEE 802.3 ad
  Link Aggregation with Static LAG and LACP support
- IEEE 802.3 x
  Flow Control

A.3 Liste der RFCs

- RFC 768 (UDP)
- RFC 783 (TFTP)
- RFC 791 (IP)
- RFC 792 (ICMP)
- RFC 793 (TCP)
- RFC 826 (ARP)
- RFC 854 (Telnet)
- RFC 855 (Telnet Option)
- RFC 951 (BOOTP)
- RFC 1112 (Host Extensions for IP Multicasting)
- RFC 1155 (SMIv1)
- RFC 1157 (SNMPv1)
- RFC 1212 (Concise MIB Definitions)
- RFC 1213 (MIB2)
- RFC 1493 (Dot1d)
- RFC 1542 (BOOTP-Extensions)
- RFC 1643 (Ethernet-like -MIB)
- RFC 1757 (RMON)
- RFC 1867 (HTML/2.0 Forms w/ file upload extensions)
- RFC 1901 (Community based SNMP v2)
- RFC 1905 (Protocol Operations for SNMP v2)
- RFC 1906 (Transport Mappings for SNMP v2)
- RFC 1907 (Management Information Base for SNMP v2)
- RFC 1908 (Coexistence between SNMP v1 and SNMP v2)
- RFC 1945 (HTTP/1.0)
- RFC 2068 (HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03)
- RFC 2131 (DHCP)
- RFC 2132 (DHCP-Options)
- RFC 2233 The Interfaces Group MIB using SMI v2
- RFC 2236 (IGMPv2)
- RFC 2246 (The TLS Protocol, Version 1.0)
- RFC 2271 (SNMP Framework MIB)
- RFC 2346 (AES Ciphersuites for Transport Layer Security)
- RFC 2362 (PIM-SM)
- RFC 2365 (Administratively Scoped Boundaries)
- RFC 2570 (Introduction to SNMP v3)
- RFC 2571 (Architecture for Describing SNMP Management Frameworks)

- RFC 2572 (Message Processing and Dispatching for SNMP)
- RFC 2573 (SNMP v3 Applications)
- RFC 2574 (User Based Security Model for SNMP v3)
- RFC 2575 (View Based Access Control Model for SNMP)
- RFC 2576 (Coexistence between SNMP v1,v2 & v3)
- RFC 2578 (SMI v2)
- RFC 2579 (Textual Conventions for SMI v2)
- RFC 2580 (Conformance statements for SMI v2)
- RFC 2613 (SMON)
- RFC 2618 (RADIUS Authentication Client MIB)
- RFC 2620 (RADIUS Accounting MIB)
- RFC 2674 (Dot1p/Q)
- RFC 2818 (HTTP over TLS)
- RFC 2851 (Internet Addresses MIB)
- RFC 2865 (RADIUS Client)
- RFC 2866 (RADIUS Accounting)
- RFC 2868 (RADIUS Attributes for Tunnel Protocol Support)
- RFC 2869 (RADIUS Extensions)
- RFC 2869bis (RADIUS support for EAP)
- RFC 2933 (IGMP MIB)
- RFC 3164 (The BSD Syslig Protocol)
- RFC 3376 (IGMPv3)
- RFC 3580 (802.1X RADIUS Usage Guidelines)
- RFC 4330 (SNTP, obsoletes RFCs 1769 and 2330)

Routing

- RFC 826 Ethernet ARP
- RFC 894 Transmission of IP Datagrams over Ethernet Networks
- RFC 896 Congestion Control in IP/TCP Networks
- RFC 919 IP Broadcast
- RFC 922 IP Broadcast in the presence of subnets
- RFC 950 IP Subnetting
- RFC 1027 Using ARP to implement Transparent Subnet Gateways (Proxy ARP)
- RFC 1256 ICMP Router Discovery Messages
- RFC 1321 Message Digest Algorithm
- RFC 1519 CIDR
- RFC 1724 RIP v2 MIB Extension
- RFC 1765 OSPF Database Overflow
- RFC 1812 Requirements for IP Version 4 Routers

- RFC 1850 OSPF MIB Draft-ietf-ipv6-rfc2096-update-07.txt IP Forwarding Table MIB
- RFC 2082 RIP-2 MD5 Authentication
- RFC 2131 DHCP Relay
- RFC 2328 OSPF Version 2
- RFC 2453 RIP v2
- RFC 2787 VRRP MIB
- RFC 2863 The Interfaces Group MIB
- RFC 2932 IPv4 Multicast Routing MIB
- RFC 2934 PIM MIB for IPv4
- RFC 3046 DHCP/BootP Relay
- RFC 3101 The OSPF "Not So Stubby Area" (NSSA) Option
- RFC 3376 IGMPV3
- RFC 3768 VRRP, Virtual Router Redundancy Protocol
- Draft-holbrook-idmr-igmpv3-ssm-08.txt – IGMPv3 / MLDv2 for SSM
- Draft-ietf-idmr-dvmrp-mib-11.txt – DVMRP MIB
- Draft-ietf-idmr-dvmrp-v3-10 – DVMRP
- Draft-ietf-magma-igmpv3-and-routing-05.txt – IGMPv3 an Multicast Routing Protocol Interaction
- Draft-ietf-magma-mgmd-mib-03.txt – Multicast Group Membership Discovery MIB
- Draft-ietf-pim-v2-dm-03 – PIM-DM
- Draft-ietf-smm-arch-06.txt – Source -Specific Multicast for IP

A.4 IP-Parameter eingeben

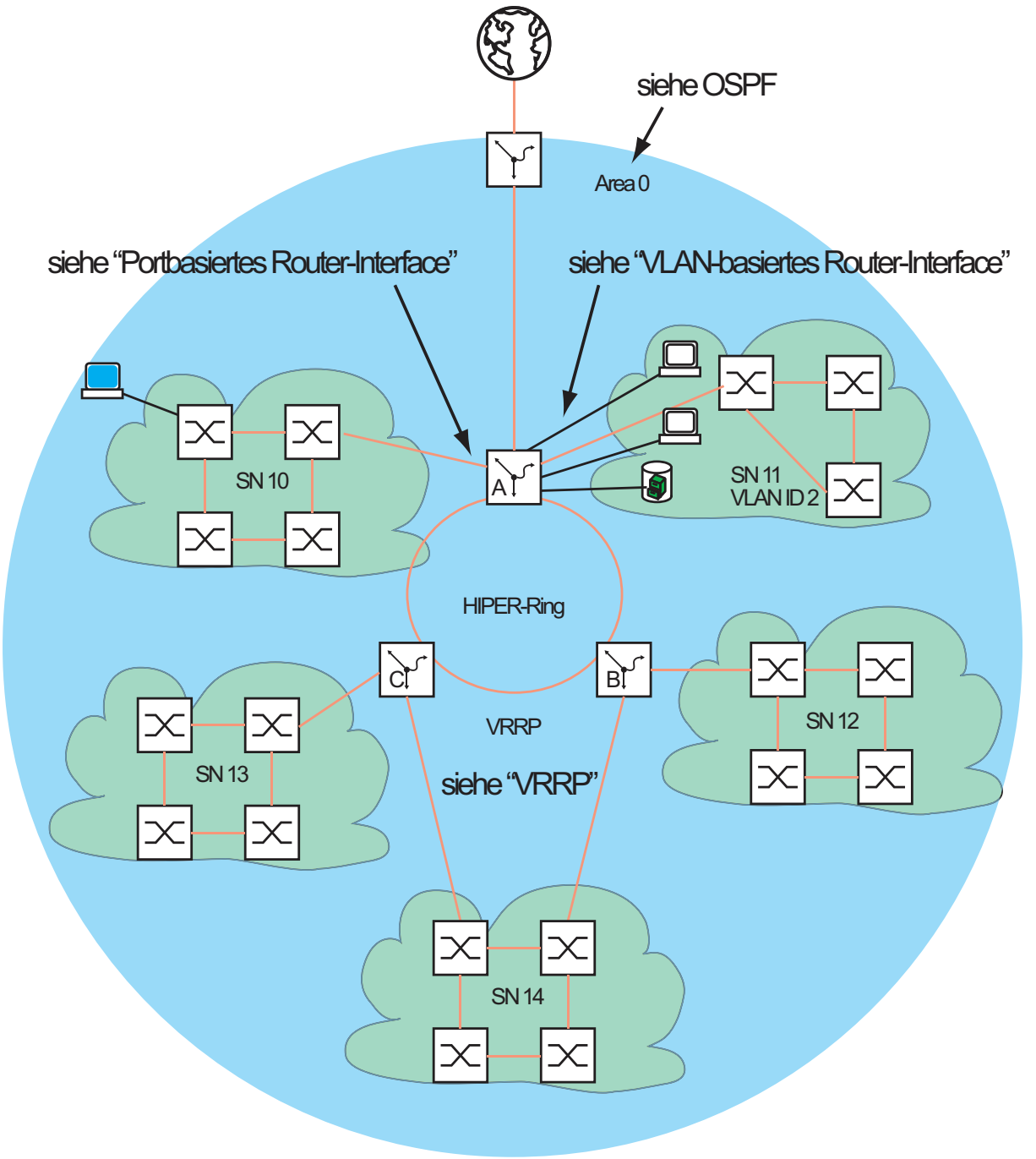


Abb. 52: Netzplan

Zur Konfiguration der Layer 3-Funktion benötigen Sie einen Zugang zur Verwaltung des Switch, wie Sie ihn im Anwender-Handbuch „Grundkonfiguration“ beschrieben finden.
Abhängig von Ihrem Anwendungsfall finden Sie viele Möglichkeiten, den Geräten IP-Adressen zuzuweisen. Das folgende Beispiel beschreibt eine Möglichkeit, die in der Praxis häufig vorkommt. Auch wenn Sie andere Voraussetzungen haben, zeigt dieses Beispiel den prinzipiellen Weg zur Eingabe der IP-Parameter und weist auf wichtige zu beachtende Punkte hin.

Voraussetzungen für das folgende Beispiel sind:

- Alle Layer 2- und Layer 3-Switches haben die IP-Adresse 0.0.0.0 (= Lieferzustand)
- Die IP-Adressen der Switches und Router-Interfaces sowie die Gateway IP-Adressen sind im Netzplan festgelegt.
- Die Geräte und deren Verbindungen sind installiert.
- Redundante Anbindungen sind offen (siehe VRRP und HIPER-Ring). Um in der Konfigurationsphase Schleifen zu vermeiden, schließen Sie die redundanten Verbindungen erst nach der Konfigurationsphase.

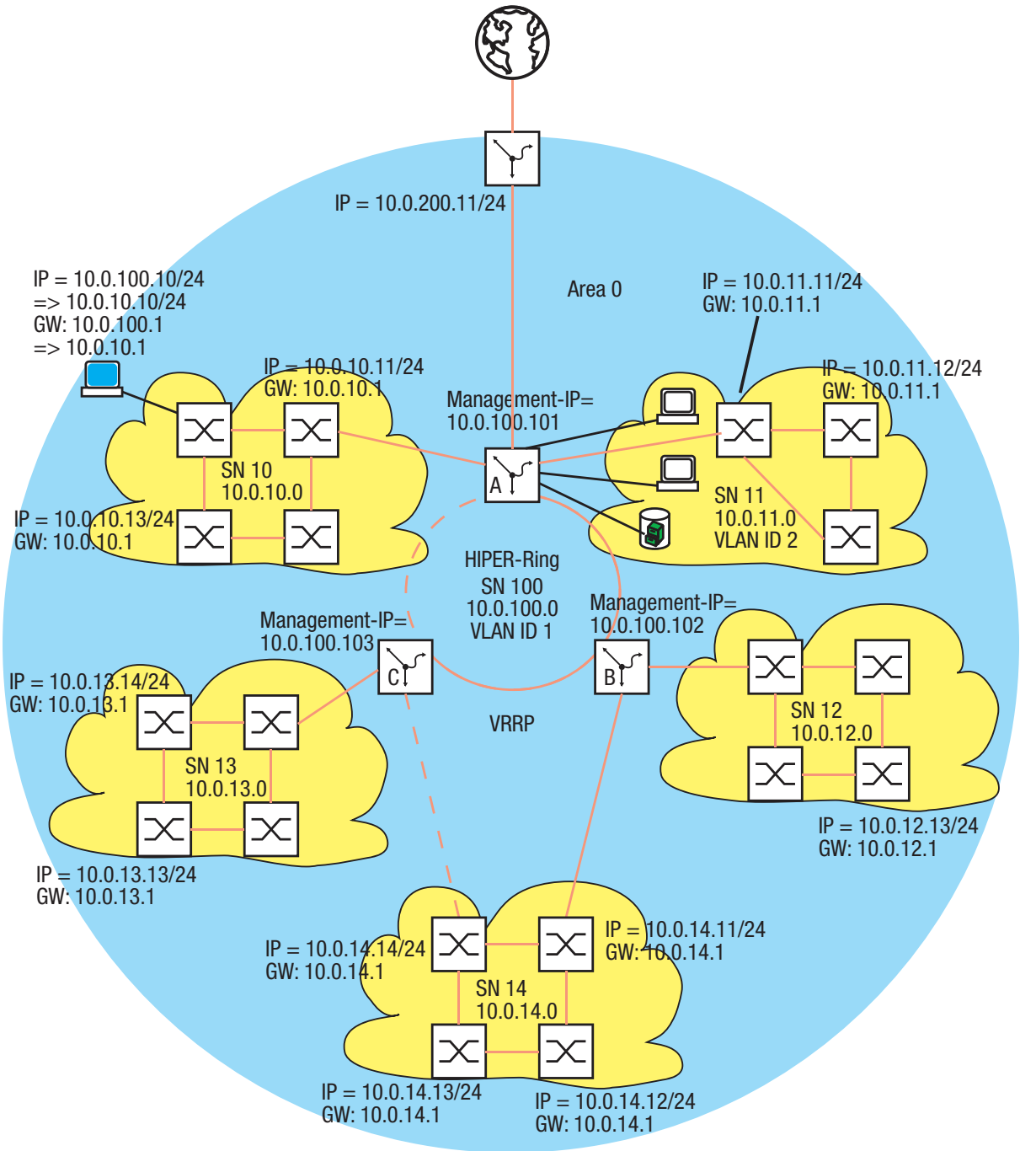


Abb. 53: Netzplan mit Management-IP-Adressen

☐ Weisen Sie Ihrem Konfigurations-Computer die IP-Parameter zu. Während der Konfigurationsphase befindet sich der Konfigurations-Computer im Subnetz 100. Das ist notwendig, damit der Konfigurations-Computer während der ganzen Konfigurationsphase Zugang zu den Layer 3-Switches hat.

☐ Starten Sie HiDiscovery auf Ihrem Konfigurations-Computer.
☐ Geben Sie allen Layer 2 und Layer 3-Switches ihre IP-Parameter gemäß des Netzplans.
Die Geräte der Subnetze 10 bis 14 erreichen Sie wieder, wenn Sie die folgende Router-Konfiguration abgeschlossen haben.
☐ Konfigurieren Sie die Router-Funktion der Layer 3-Switches.
Beachten Sie die Reihenfolge:
1. Layer 3-Switch C
2. Layer 3-Switch B
Die Reihenfolge ist wichtig, damit Sie sich den Zugang zu den Geräten bewahren.
Sobald Sie einem Router-Interface eine IP-Adresse aus dem Subnetz der Management-IP-Adresse (= SN 100) zuweisen, löscht der Switch die Management-IP-Adresse. Sie erreichen den Switch über die IP-Adressen der Router-Interfaces.

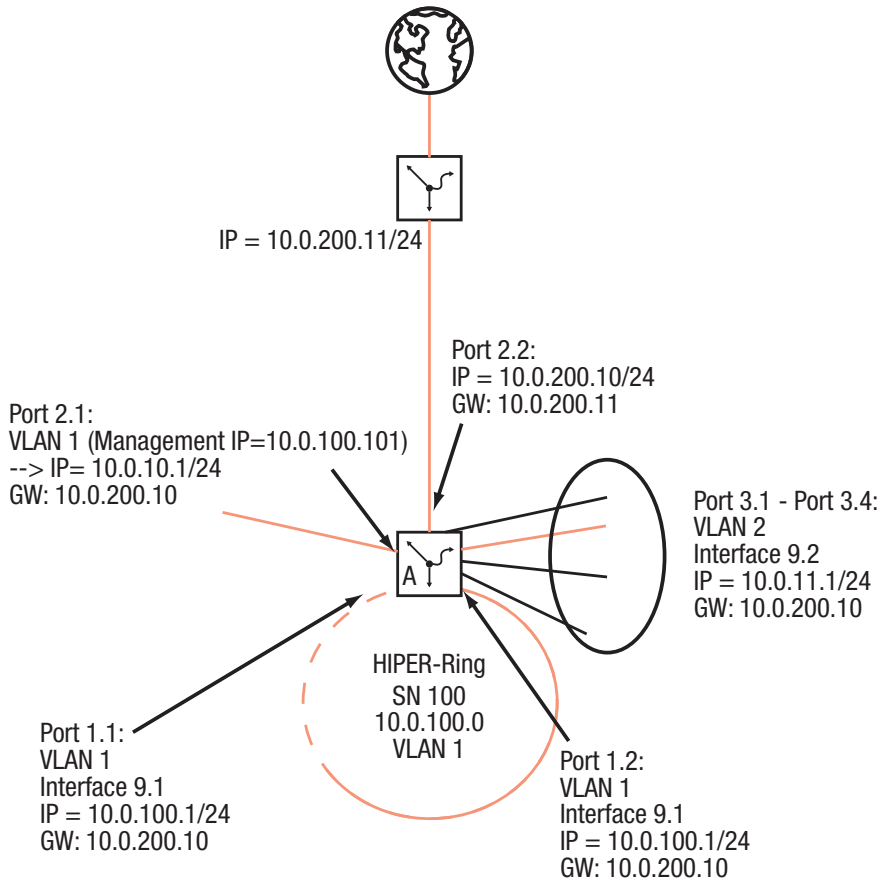


Abb. 54: IP-Parameter für Layer-3-Switch A

- ☐ Konfigurieren Sie die Router-Funktion des Layer 3-Switch A.
  Als erstes konfigurieren Sie das Router-Interface an dem Port, über den der Konfigurations-Computer angeschlossen ist. Dies hat zur Folge, dass Sie den Layer 3-Switch A zukünftig über das Subnetz 10 erreichen.
- ☐ Ändern Sie die IP-Parameter Ihres Konfigurations-Computers auf die Werte für das Subnetz 10. Somit erreichen Sie den Layer 3-Switch A wieder und zwar über die IP-Adresse des zuvor eingerichteten Router-Interfaces.
- ☐ Schließen Sie die Router-Konfiguration des Layer 3-Switch A (siehe Abbildung 54) ab.

Nach der Konfiguration der Router-Funktion auf allen Layer 3-Switches haben Sie Zugang zu allen Geräten.

A.5 Copyright integrierter Software

A.5.1 Bouncy Castle Crypto APIs (Java)

The Legion Of The Bouncy Castle
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle
(http://www.bouncycastle.org)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A.5.2 Broadcom Corporation

(c) Copyright 1999-2007 Broadcom Corporation. All Rights Reserved.

B Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, um Sie beim Einsatz dieses Produkts zu unterstützen. Ihre Kommentare und Anregungen helfen uns dabei, die Qualität und den Informationsgrad dieser Dokumentation weiter zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	**gut**	**befriedigend**	**mäßig**	**schlecht**
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Leserkritik

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer +49 (0)7127 14-1600 oder
- per Post an

Hirschmann Automation and Control GmbH
Abteilung 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen

C Stichwortverzeichnis

A
ABR 99, 103
Address Resolution Protocol 18
Adjacency 107
Advertisement 60, 63
Advertisement-Intervall 61
Aging Time 129
ARP 18, 20, 43
ARP-Datenpaket 117
Area Border Router 99, 103
ASBR 98, 103
Assert Prozess 152
Autonomous System Area Border Router 103
Autonomous System Boundary Router 98

B
Backbone-Area 99
Backup Designated Router 107, 110
Backup-Router 60, 60
BDR 107
Boundary 145
Broadcast 16

C
CIDR 21, 95
Classless Inter Domain Routing 21, 95
Count-to-Infinity 90

D
Default Gateway 58, 60
Designated Router 107, 110
Distance Vector Multicast Routing Protocol 131
Distanz 36, 38
Distanzvektor-Algorithmus 85
DR 107
DVMRP 131

E
Extended Unique Identifier 127

F
FAQ 177
Flooding 133

G
Grafting 135

H
Hello 107
HIPER-Ring 152
HiVRRP 63
Hop-Count 85, 90

I
IANA 126
IGMP 129
IGMP-Querier-Intervall 154
Implizit-Join 131
Industrial HiVision 10
Industrieprotokolle 9
Infinity 90
Interface-Tracking 45, 46, 51, 53, 53, 76
Interface-Tracking-Objekt 46
Interner Router 103
Internet Group Management Protocol 129
IP 16
IP-Address-Owner 59, 60, 60
IP-Adresse 58
IP-Datenpaket 117
IP-Stack 43
ISO/OSI-Schichtenmodell 15

K
Konvergenz 86

L
Leave-Nachricht 129
Link State Advertisement 104
Link State Database 110
Link-Aggregation-Interface 46
Link-Down Meldung 66
Link-Down-Verzögerung 47
Link-Up-Verzögerung 47
Logical-Tracking 50, 54
Logic-Tracking 45
LSA 104, 110
LSD 110
load sharing 38

M
MAC/IP-Adressauflösung 43
MAC-Adresse 16, 58
Master-Router 60, 60, 61
Metrik 85

Multicast 16, 66
Multicast-Adresse 108, 124
Multinetting 24

N
Nachbarschaftsbeziehung 107
Netdirected Broadcasts 23
Netdirected Broadcasts (Port-basiert) 27
Netdirected Broadcasts (VLAN-basiert) 30
Netzplan 13
Next-Hop 85
Not So Stubby Area 100
NSSA 100

O
Open Shortest Path First 95
Operand 55
Operatoren 50
Organizationally Unique Identifier 127
OSI-Referenzmodell 15
OSI-Schichtenmodell 15
OSPF 14, 86, 95
OUI 127

P
Paketdoppelung 152
PIM-DM 131
PIM-SM 131
Ping-Anfrage 48
Ping-Antwort 48
Ping-Intervall 48
Ping-Timeout 48
Ping-Tracking 39, 45, 48
Portbasiertes Router-Interface 26, 44
PROFINET IO 9
Präferenz 74
Preempt-Modus 66
Preempt-Verzögerung 66
Protokoll-basiertes VLAN 117
Proxy-ARP 20
Prune-Nachrichten 134

Q
Quellfilterung 130
Querier-Election 129
Query 129

R
Redistribute 100
Redistributing 99
Redistribution 98
Redundante statische Route 36
Redundanz 9
Report-Nachricht 129
Reverse Path Forwarding 134
RFC 161
RIP 14, 85
Routen-Tracking 39
Router 9
Router-ID 107
Router-Priorität 107
Route Summarization 99
Routingtabelle 28, 29, 39, 85, 131
Routingtabellen 66
Routing Information Protocol 85
RPF 134

S
Schulungsangebote 177
Scoping 145
Shortest Path First 112
Shortest Path Tree 134
Skew-Time 61
Source filtering 130
Source routed 134
SPF 112
SPT 134
Split-Horizon 90
Statisches Routen-Tracking 39
Statisches Routing 45
Statische Routen 14
Stub-Area 99
Symbol 11

T
Technische Fragen 177
Time To Live 145
Totally-Stubby-Area 100
Tracking 39, 45
TTL 145

U
Umschaltzeit 63
Umschaltzeiten 152
Upstream 134

V
Variable Length Subnet Mask 95
Verbindungsunterbrechungs-Meldung 66
Virtueller Router 60
Virtuelles Router-Interface 119
Virtuelle MAC-Adresse 58
Virtuelle Router IP-Adresse 60
Virtuelle Router MAC-Adresse 60
Virtuelle Router-ID 58
Virtuelle Verbindung 101
VL 101
VLAN-basiertes Router-Interface 29, 44

VLAN-Protokollgruppe 119
VLAN-Router-Interface 46
VLAN-Routing 119
VLSM 95
VRID 58, 60
VRRP 45
VRRP-Priorität 59, 60, 60
VRRP-Router 60
VRRP-Zieladresse 66

W

Wichtigkeit 36, 38, 39

D Weitere Unterstützung

Technische Fragen

Bei technischen Fragen wenden Sie sich bitte an den Hirschmann-Vertragspartner in Ihrer Nähe oder direkt an Hirschmann.

Die Adressen unserer Vertragspartner finden Sie im Internet unter http://www.hirschmann.com

Unser Support steht Ihnen zur Verfügung unter https://hirschmann-support.belden.eu.com

Sie erreichen uns

in der Region EMEA unter
- Tel.: +49 (0)1805 14-1538
- E-Mail: hac.support@belden.com

in der Region Amerika unter
- Tel.: +1 (717) 217-2270
- E-Mail: inet-support.us@belden.com

in der Region Asien-Pazifik unter
- Tel.: +65 6854 9860
- E-Mail: inet-ap@belden.com

Hirschmann Competence Center

Das Hirschmann Competence Center mit dem kompletten Spektrum innovativer Dienstleistungen hat vor den Wettbewerbern gleich dreifach die Nase vorn:

- Das Consulting umfasst die gesamte technische Beratung von der Systembewertung über die Netzplanung bis hin zur Projektierung.
- Das Training bietet Grundlagenvermittlung, Produkteinweisung und Anwenderschulung mit Zertifizierung.
  Das aktuelle Schulungsangebot zu Technologie und Produkten finden Sie unter http://www.hicomcenter.com
- Der Support reicht von der Inbetriebnahme über den Bereitschafts-service bis zu Wartungskonzepten.

Mit dem Hirschmann Competence Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.
Internet:
http://www.hicomcenter.com

HIRSCHMANN

A BELDEN BRAND