



HIRSCHMANN

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

Classic L2P Rel. 09000

Referenz-Handbücher

Grafische Benutzeroberfläche
Command Line Interface

Anwender-Handbücher

Grundkonfiguration
Industrie-Protokolle
Redundanz-Konfiguration



HIRSCHMANN

A **BELDEN** BRAND

Referenz-Handbuch

**Grafische Benutzeroberfläche (GUI)
Industrial ETHERNET (Gigabit-)Switch
RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE,
RSR20/RSR30, MACH 100, MACH 1000, 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

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	104
2.6.3	802.1X-Port-Clients	112
2.6.4	802.1X-Port-Statistiken	115
2.7	RADIUS	117
2.7.1	Global	117
2.7.2	RADIUS-Server	120
2.8	Login-/CLI-Banner	125
2.8.1	Login-Banner	126
2.8.2	CLI-Banner	128
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	168

4.3	Lastbegrenzer	172
4.3.1	Lastbegrenzer-Einstellungen für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS	173
4.3.2	Lastbegrenzer-Einstellungen (PowerMICE und MACH 4000)	175
4.4	Multicasts	177
4.4.1	IGMP (Internet Group Management Protocol)	177
4.4.2	GMRP (GARP Multicast Registration Protocol)	184
4.5	VLAN	188
4.5.1	VLAN Global	188
4.5.2	VLAN Aktuell	194
4.5.3	VLAN Statisch	196
4.5.4	VLAN Port	199
4.5.5	Voice-VLAN	204
5	QoS/Priorität	209
5.1	Global	210
5.2	Portkonfiguration	214
5.2.1	Port-Priorität eingeben	216
5.2.2	Trust-Modus wählen (PowerMICE, MACH 104, MACH 1040 und MACH 4000)	218
5.2.3	Untrusted Traffic Class anzeigen (PowerMICE, MACH 104, MACH 1040 und MACH 4000)	218
5.3	802.1D/p-Mapping	220
5.4	IP-DSCP-Mapping	222
6	Redundanz	225
6.1	Link-Aggregation	226
6.2	Ring-Redundanz	230
6.2.1	HIPER-Ring konfigurieren	233
6.2.2	MRP-Ring konfigurieren	237
6.2.3	Fast HIPER-Ring konfigurieren (RSR20, RSR30, MACH 1000)	244
6.3	Sub-Ring	247
6.3.1	Sub-Ring-Konfiguration	248
6.3.2	Sub-Ring – Neuer Eintrag	251
6.4	Ring-/Netzkopplung	254
6.4.1	Ring-/Netzkopplung vorbereiten	254

6.5	Spanning Tree	260
6.5.1	Global	263
6.5.2	MSTP (Multiple Spanning Tree)	269
6.5.3	Port	277
7	Diagnose	291
7.1	Syslog	292
7.2	Trap-Log	296
7.3	Ports	298
7.3.1	Portstatistiken	298
7.3.2	Auslastung (Netzlant)	300
7.3.3	SFP-Transceiver	302
7.3.4	TP-Kabeldiagnose	303
7.3.5	Port Monitor	306
7.3.6	Auto-Disable	318
7.4	Konfigurations-Check	322
7.5	Topologie-Erkennung	325
7.5.1	LLDP-Informationen von Nachbargeräten	325
7.5.2	LLDP-MED (Media Endpoint Discovery)	327
7.6	Port-Mirroring	331
7.7	Gerätstatus	334
7.8	Meldekontakt	337
7.8.1	Manuelle Einstellung	337
7.8.2	Funktionsüberwachung	338
7.8.3	Gerätstatus	340
7.8.4	Trapeinstellung	341
7.9	Alarmer (Traps)	343
7.10	Bericht	346
7.10.1	Systeminformationen	349
7.10.2	Event-Log	349
7.11	IP-Adressen-Konflikterkennung	351
7.12	MAC-Benachrichtigung	354
7.12.1	Funktion	354
7.12.2	Konfiguration	355
7.12.3	Tabelle	355
7.13	Selbsttest	357
7.14	Service-Mode	359
7.14.1	Service-Mode aktivieren	360
7.14.2	Service-Mode deaktivieren	362

8	Erweitert	365
8.1	DHCP-Relay-Agent	366
	8.1.1 Global	366
	8.1.2 Server	369
8.2	DHCP-Server	371
	8.2.1 Global	371
	8.2.2 Pool	374
	8.2.3 Lease-Tabelle	379
8.3	Industrieprotokolle	382
	8.3.1 PROFINET IO	382
	8.3.2 EtherNet/IP	385
	8.3.3 IEC61850 MMS Protokoll (RSR, MACH 1000)	386
	8.3.4 Digital IO-Module	388
8.4	DIP-Switch via Software überschreiben (Mice, PowerMICE und RS)	397
8.5	Command Line	401
A	Anhang	403
A.1	Technische Daten	404
A.2	Liste der RFCs	405
A.3	Zugrundeliegende IEEE-Normen	407
A.4	Zugrundeliegende IEC-Normen	408
A.5	Zugrundeliegende ANSI-Normen	409
A.6	Literaturhinweise	410
A.7	Copyright integrierter Software	411
	A.7.1 Bouncy Castle Crypto APIs (Java)	411
	A.7.2 Broadcom Corporation	412
B	Leserkritik	413
C	Stichwortverzeichnis	415
D	Weitere Unterstützung	419

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.

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.
<code>Courier</code>	ASCII-Darstellung in der grafischen Benutzeroberfläche

Verwendete Symbole:

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

Legende



Hub



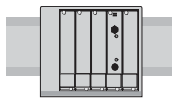
Beliebiger Computer



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.

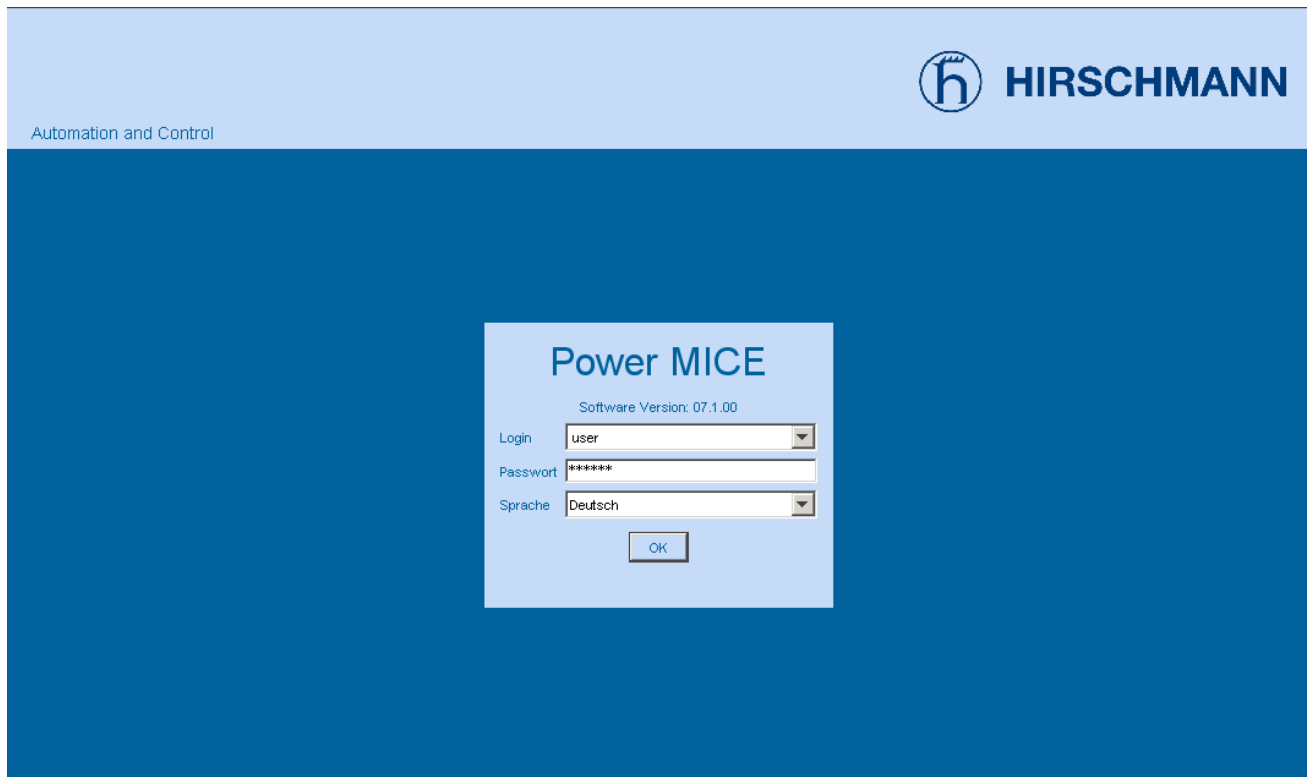


Abb. 1: Login-Fenster

- 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.

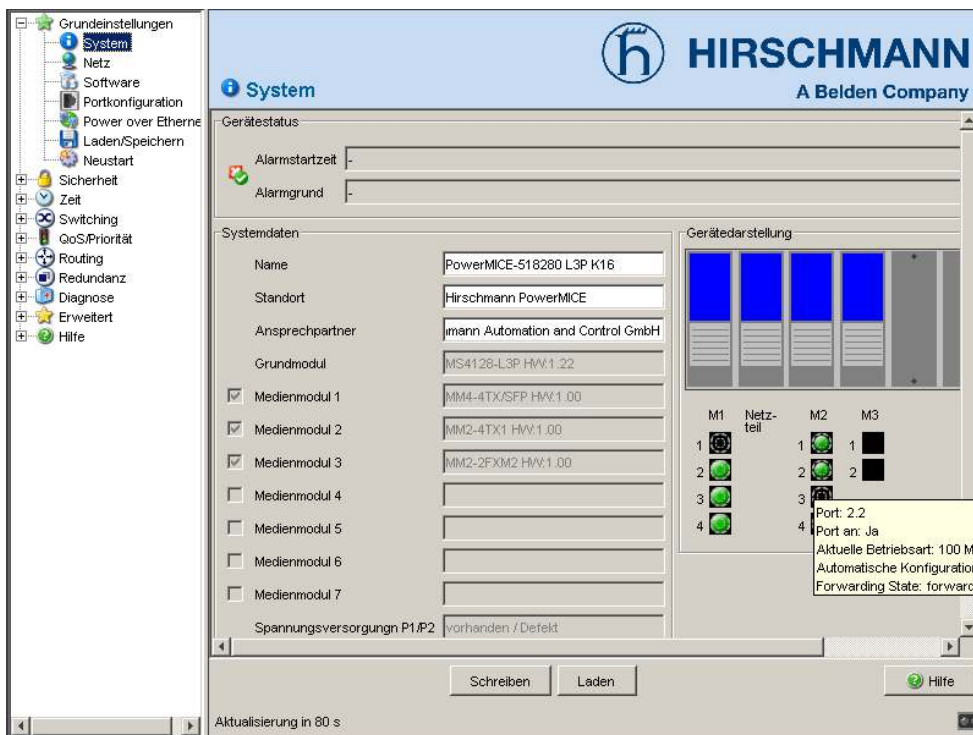
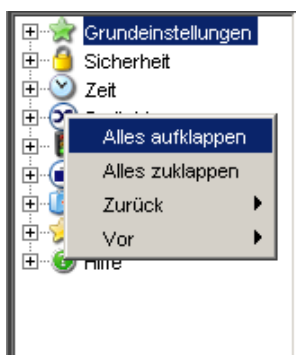


Abb. 2: Benutzeroberfläche (Web-based Interface) des Gerätes mit Tooltip

■ 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

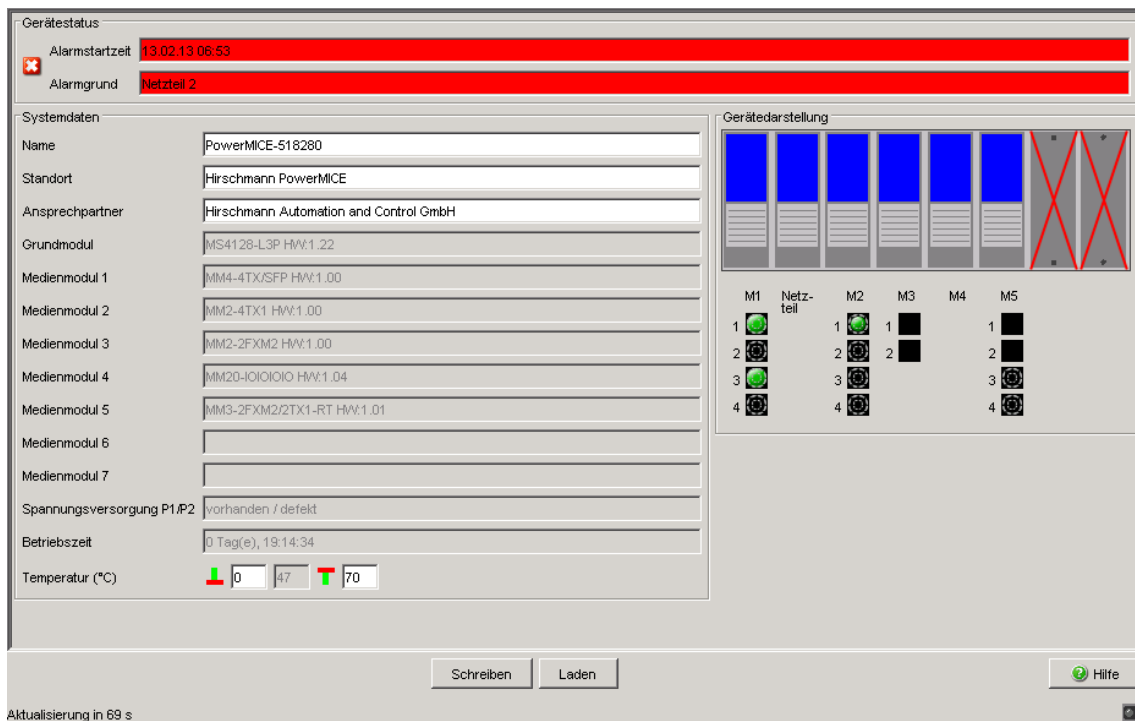


Abb. 3: Untermenü „System“

■ Gerätestatus

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

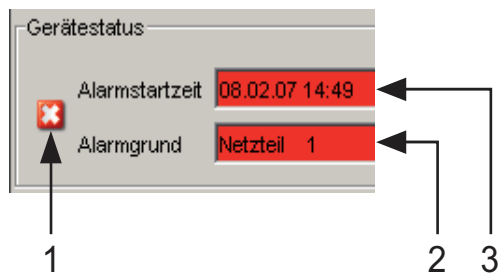


Abb. 4: Gerätestatus- und Alarm-Anzeige
 1 - Das Symbol zeigt den Gerätestatus an
 2 - Ursache des ältesten, bestehenden Alarms
 3 - Beginn des ältesten, bestehenden Alarms

■ 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.

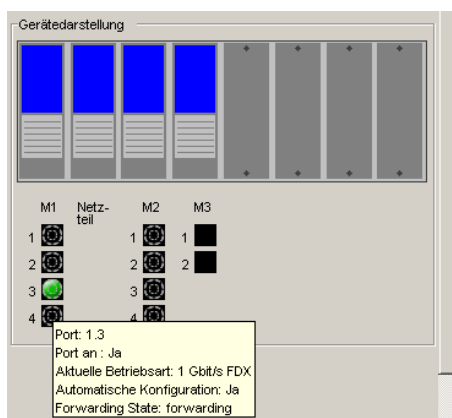









Abb. 5: Gerätedarstellung

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.

Aktualisierung in 80 s

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 <i>Grundeinstellungen:Laden/Speichern</i> , 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 Modulparameter 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.

ID	Aktiv	Typ	Beschreibung	Version	Ports	Seriennummer	Status
1	<input checked="" type="checkbox"/>	mm4-4tx-sfp	MM4-4TX/SFP	1.00	4	943010001000001196	physical
2	<input checked="" type="checkbox"/>	mm2-4tx1	MM2-4TX1	1.00	4		physical
3	<input checked="" type="checkbox"/>	mm2-2fxm2	MM2-2FXM2	1.00	2		physical
4	<input checked="" type="checkbox"/>	mm20-ioioioio	MM20-IOIOIOIO	1.04	0		physical
5	<input checked="" type="checkbox"/>	mm3-2fxm2-2tx1-rt	MM3-2FXM2/2TX1-RT	1.01	4		physical
6	<input type="checkbox"/>	none			0		remove
7	<input type="checkbox"/>	none			0		remove

Schreiben Laden Modul entfernen Hilfe

Abb. 7: Dialog „Module“

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

- ▶ Die Spalte „ID“ bezeichnet 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 <code>Grundeinstellungen:Laden/Speichern</code> , 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 <i>Grundeinstellungen:Laden/Speichern</i> , 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.

The screenshot shows a software update dialog box with the following fields and controls:

- Version:**
 - Gespeicherte Version: L2P-08.0.00-A14 2013-02-05 00:49
 - Laufende Version: L2P-08.0.00-A14 2013-02-05 00:49
 - Backup Version: <not available>
 - Wiederherstellen button
- tftp-Software-Update:**
 - Typ: Firmware Bootcode
 - URL: tftp://192.168.1.100/device/device_bootrom.bin
 - Update button
- Software-Update:**
 - Datei: [Empty field] ... Update button
- Bottom:**
 - Laden button
 - Hilfe button

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 226 „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“.

Geräte mit Power over ETHERNET- (PoE-) Medienmodulen oder PoE-Ports bieten Ihnen die Möglichkeit, Endgeräte wie z.B. IP-Telefone über das Twisted-Pair-Kabel mit Strom zu versorgen. PoE-Medienmodule und PoE-Ports unterstützen Power over ETHERNET nach IEEE 802.3af.

Die Funktion Power over Ethernet ist global aktiv. Die PoE-fähigen Ports sind aktiv, sobald eine Auslieferung an sie erfolgt.

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 OCTOPUS 8M-PoE und OCTOPUS 24M-8PoE:

Das Gerät bietet die nominale Leistung für die Summe aller PoE-Ports zuzüglich einer Reserve. Da das Gerät 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 15 Watt pro PoE-Port 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.

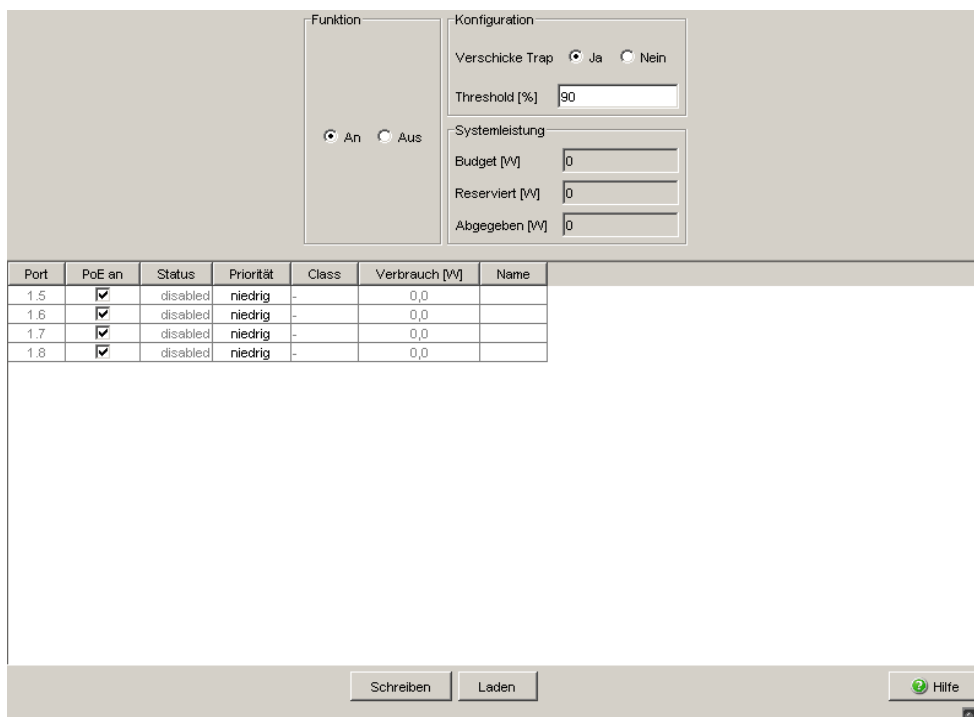


Abb. 10: Dialog Power over Ethernet

■ 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: <ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ 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: <ul style="list-style-type: none"> ▶ 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

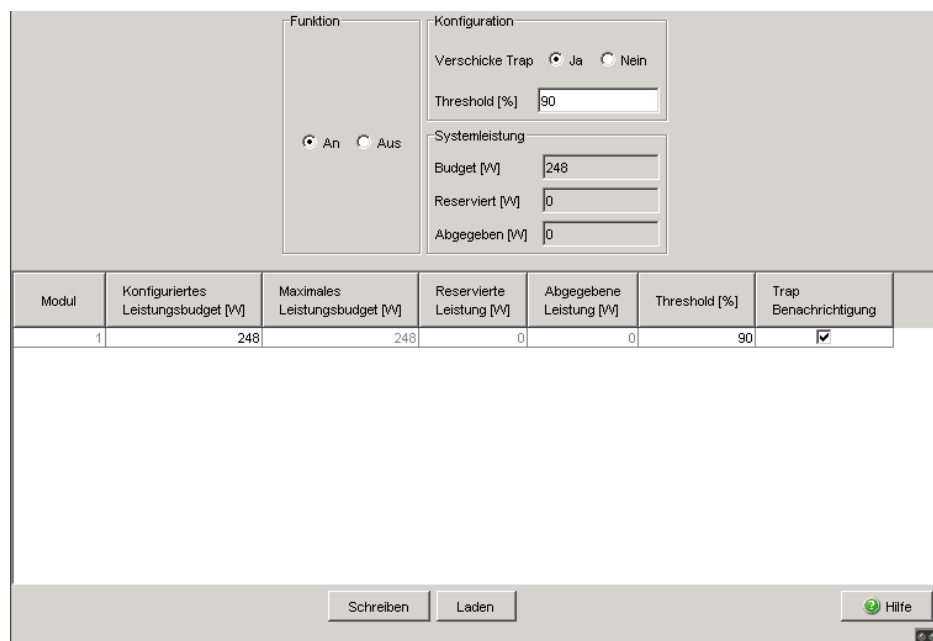


Abb. 11: Dialog Power over Ethernet Plus:Global

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]	<p>Legt die Leistung in Watt fest, die der Port maximal abgibt.</p> <p>Diese Funktion bietet Ihnen die Möglichkeit, das zur Verfügung stehende Leistungs-Budget bedarfsgerecht auf die PoE-Ports zu verteilen.</p> <p>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.</p> <p>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.</p> <p>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]“.</p> <p>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.</p>	0 - 30,0	0
Maximal überwacht [mW]	<p>Zeigt, welche maximale Leistung in Watt das Gerät bisher aufgenommen hat.</p> <p>Den Wert setzen Sie zurück, wenn Sie PoE auf dem Port deaktivieren oder wenn die Verbindung zum angeschlossenen Gerät trennen.</p>	0 - 30,0	-
Name	<p>Zeigt den Namen des Ports an, siehe Grundeinstellungen:Portkonfiguration</p>	-	-

Tab. 14: Power over Ethernet Plus - Port

Port	PoE an	Status	Priorität	Class	Verbrauch [W]	Leistungslimit [mW]	Maximal überwacht [mW]	Name
1.5	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.6	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.7	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.8	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.9	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.10	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.11	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.12	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.13	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.14	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.15	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.16	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.17	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.18	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.19	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			
1.20	<input checked="" type="checkbox"/>	searching	niedrig	-	0,0			

kritisch
 hoch
 niedrig

Schreiben Laden Hilfe

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.

The screenshot shows a dialog box titled 'Laden/Speichern' (Load/Save) with several sections:

- Laden:** Radio buttons for 'vom Gerät', 'vom URL', 'vom URL & auf dem Gerät speichern', and 'via PC'. A 'Wiederherstellen' button is on the right.
- Speichern:** Radio buttons for 'auf dem Gerät', 'auf URL (binär)', 'auf URL (script)', 'auf dem PC (binär)', and 'auf dem PC (script)'. A 'Sichern' button is on the right.
- URL:** A text input field containing 'ftp://192.168.1.100/product/product.cfg'.
- Löschen:** Radio buttons for 'aktuelle Konfiguration' and 'aktuelle Konfiguration und vom Gerät'. A 'Konfiguration löschen' button is on the right.
- AutoConfiguration Adapter:** A dropdown menu with 'notPresent' selected.
- Konfigurationsänderung widerrufen:** A checkbox for 'Funktion', a text input for 'Periode bis zum Widerruf bei Verbindungsunterbrechung [s]' with '600', and a text input for 'Watchdog IP-Adresse' with '0.0.0.0'.

At the bottom, there are buttons for 'Schreiben', 'Laden', and 'Hilfe'.

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

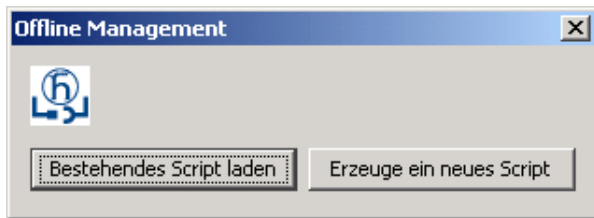


Abb. 14: Auswahl Offline Management

- ▶ 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

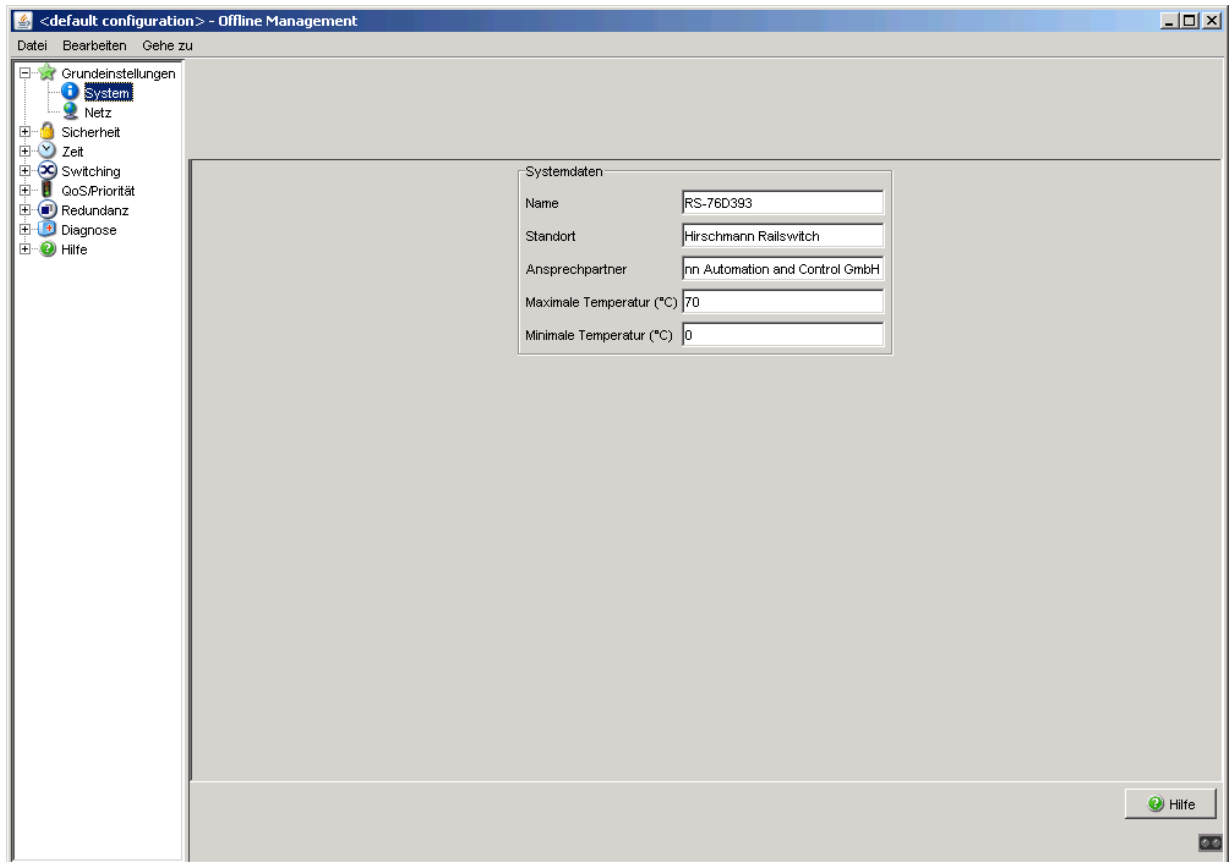


Abb. 16: Dialog Grundeinstellungen: System im Offline-Konfigurator

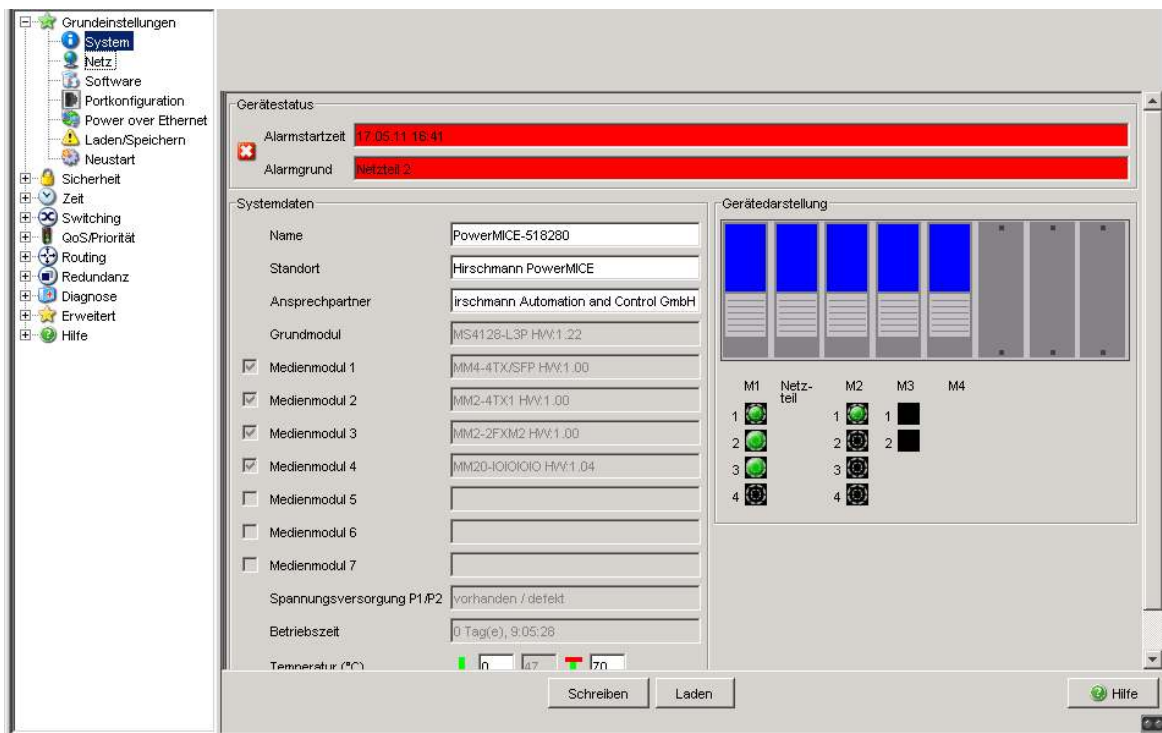


Abb. 17: Dialog Grundeinstellungen: System in der grafischen Benutzeroberfläche

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.

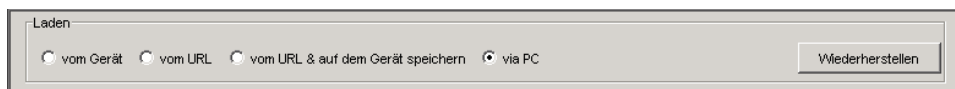


Abb. 18: Dialog Konfiguration laden - Via PC

- 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.

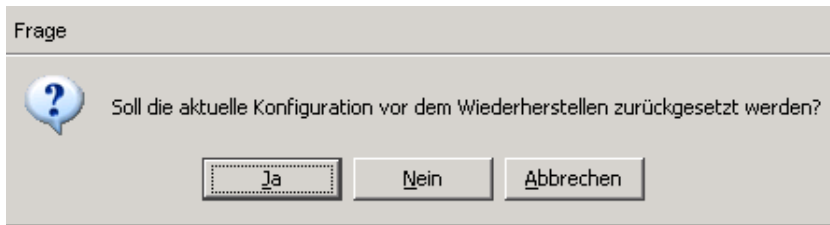


Abb. 19: Abfrage - Konfiguration zurücksetzen

- 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

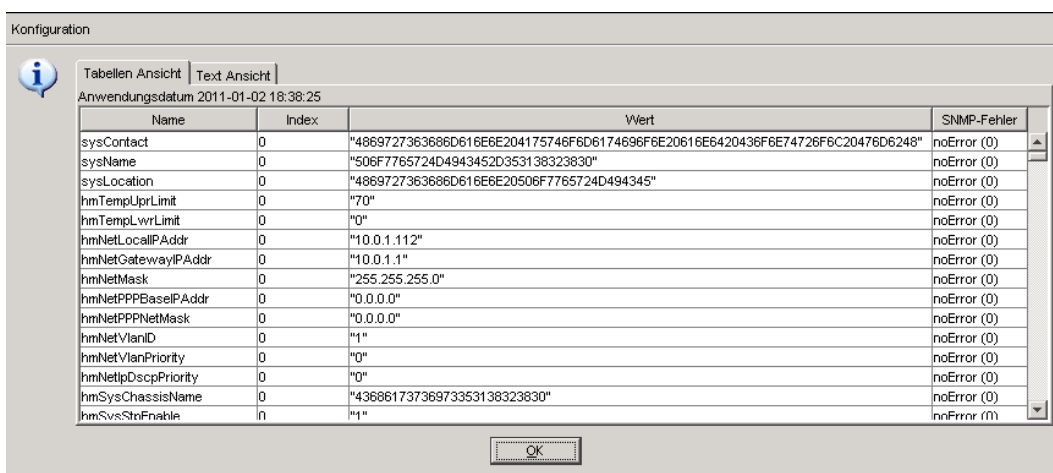


Abb. 20: Information - Konfiguration - Tabellen Ansicht

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	<ul style="list-style-type: none"> ▶ (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

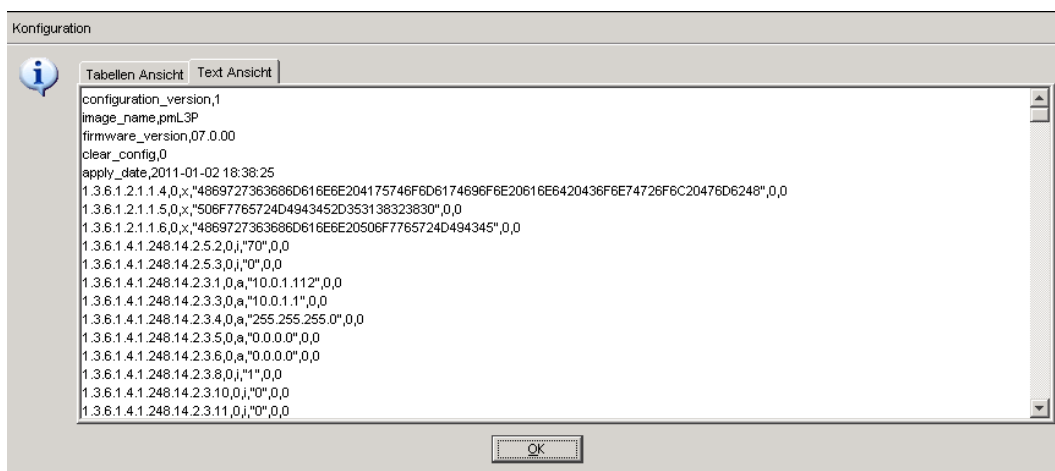


Abb. 21: Information - Konfiguration - Text Ansicht

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.

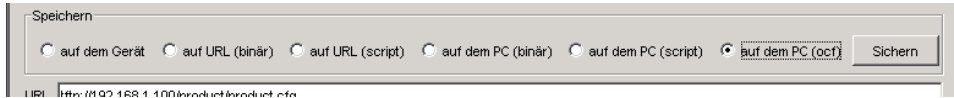


Abb. 22: Dialog Konfiguration speichern - Auf dem PC (.ocf)

- 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 Konfigurator).

■ 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.

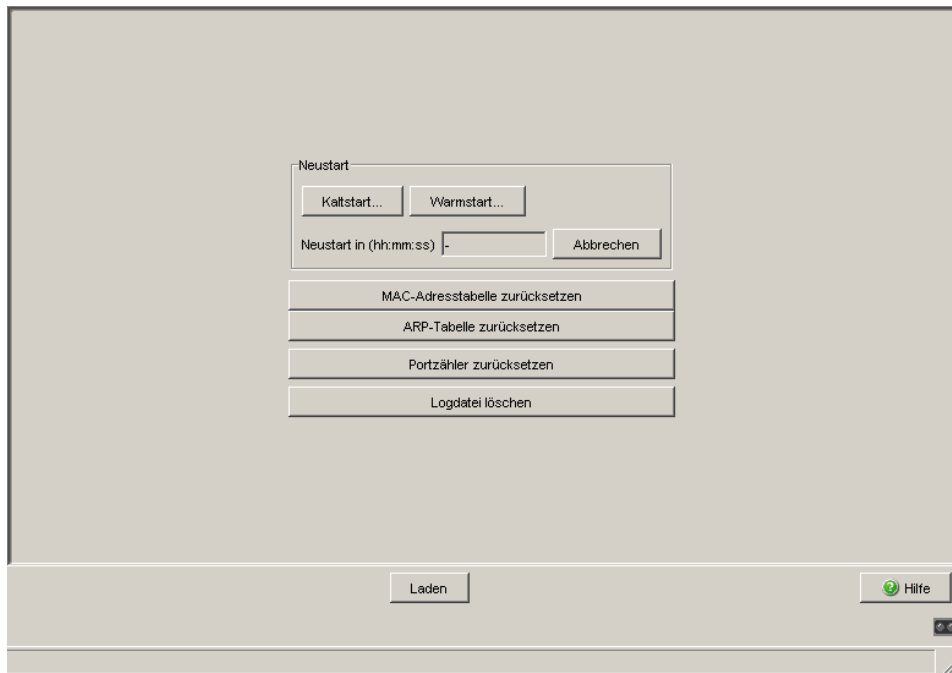


Abb. 23: Dialog Neustart

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 abubrechen, klicken Sie „Abbrechen“.

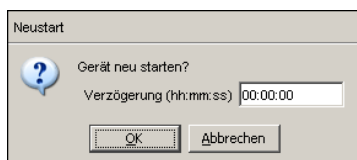


Abb. 24: Dialog verzögerter Neustart

■ 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-Authentifizierung
- ▶ RADIUS
- ▶ Login-Banner

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 Lese Passwort und das Schreib-/Lese Passwort 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 „Lese Passwort ändern (user)“, um das Lese Passwort einzugeben.
- Geben Sie das neue Lese Passwort in der Zeile „Neues Passwort“ ein und wiederholen Sie die Eingabe in der Zeile „Bitte nochmals eingeben“.
- Wählen Sie „Schreib-/Lese Passwort ändern (admin)“, um das Schreib-/Lese Passwort einzugeben.
- Geben Sie das Schreib-/Lese Passwort 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 Passwort 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 Lese Passwort und mit dem Schreib-/Lese Passwort 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-/Lese Passwort 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 Gerätes zugreifen können. Andernfalls erhalten Sie bei einem Zugriffsversuch eine allgemein gehaltene Fehlermeldung.

Passwort auswählen (CLI/WEB/SNMPv3)

Lese/Passwort ändern (user) Schreib/Lese/Passwort ändern (admin)

Neues Passwort

Bitte nochmals eingeben

Nur verschlüsselte Anfragen akzeptieren

Passwort als v1/v2-Community übernehmen

Schreiben Laden Hilfe

Lade Daten ok

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 Lese Passwort (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.

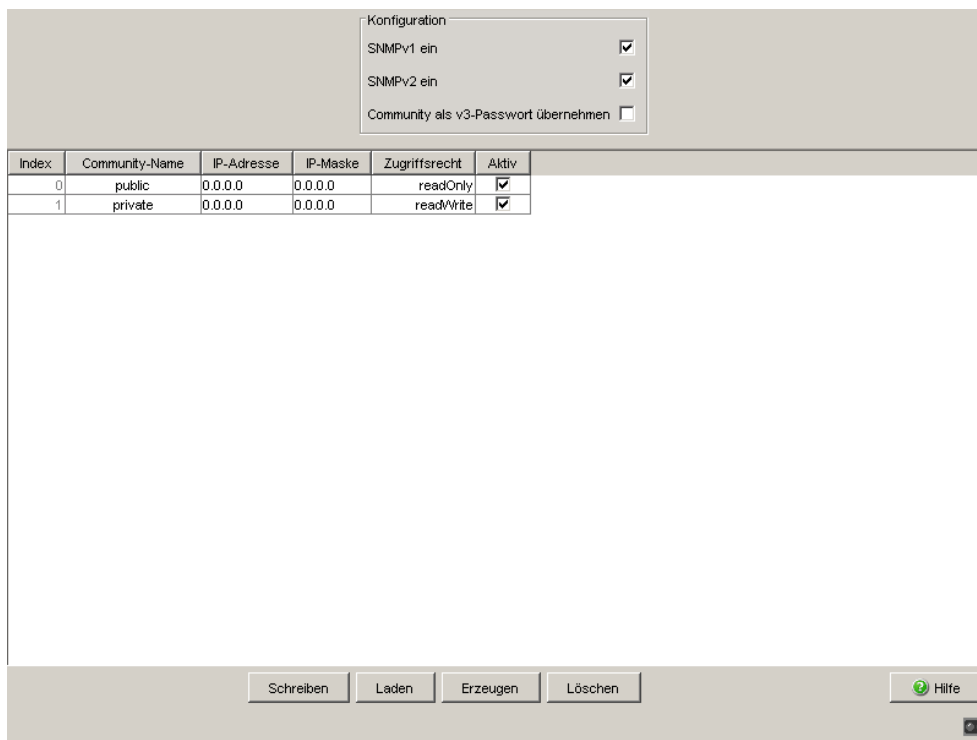


Abb. 26: Dialog SNMPv1/v2-Zugriff

■ 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 auszu-
schalten.

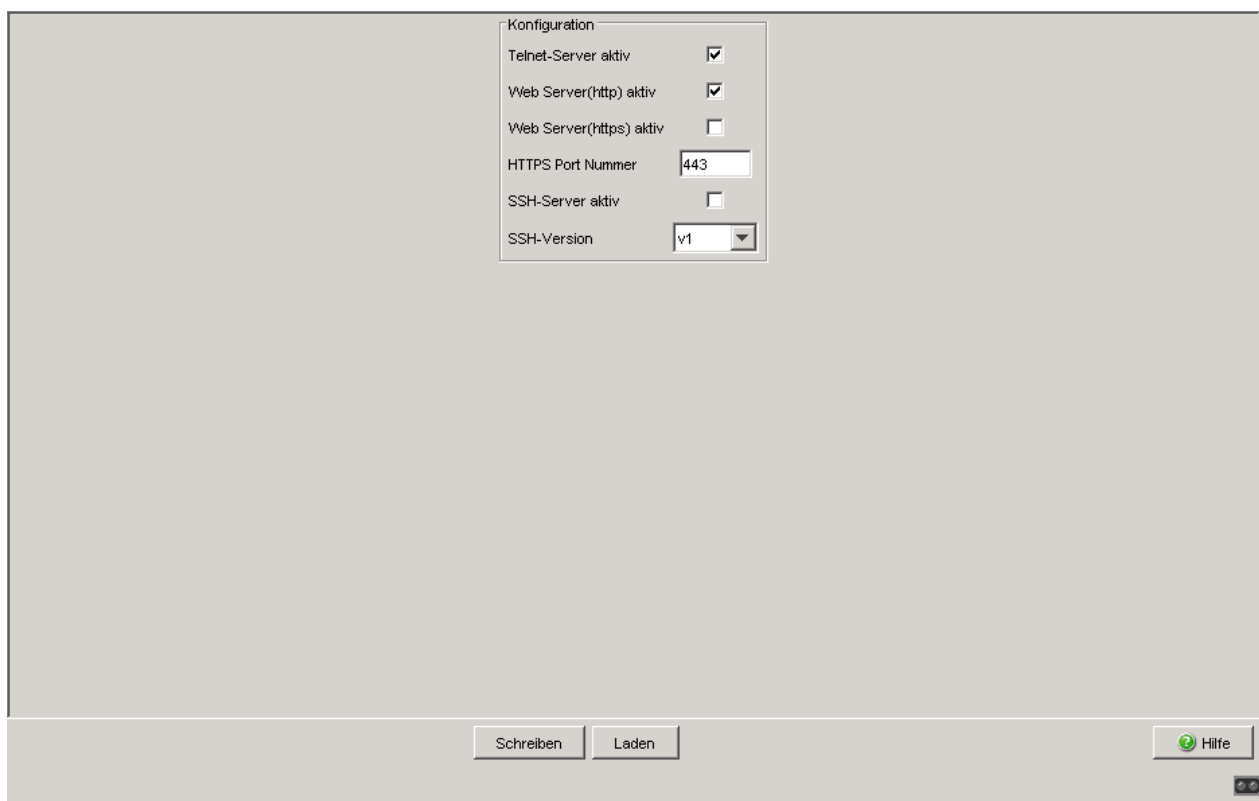


Abb. 27: Dialog Telnet-/Web-/SSH-Zugriff

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, deaktivieren 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.

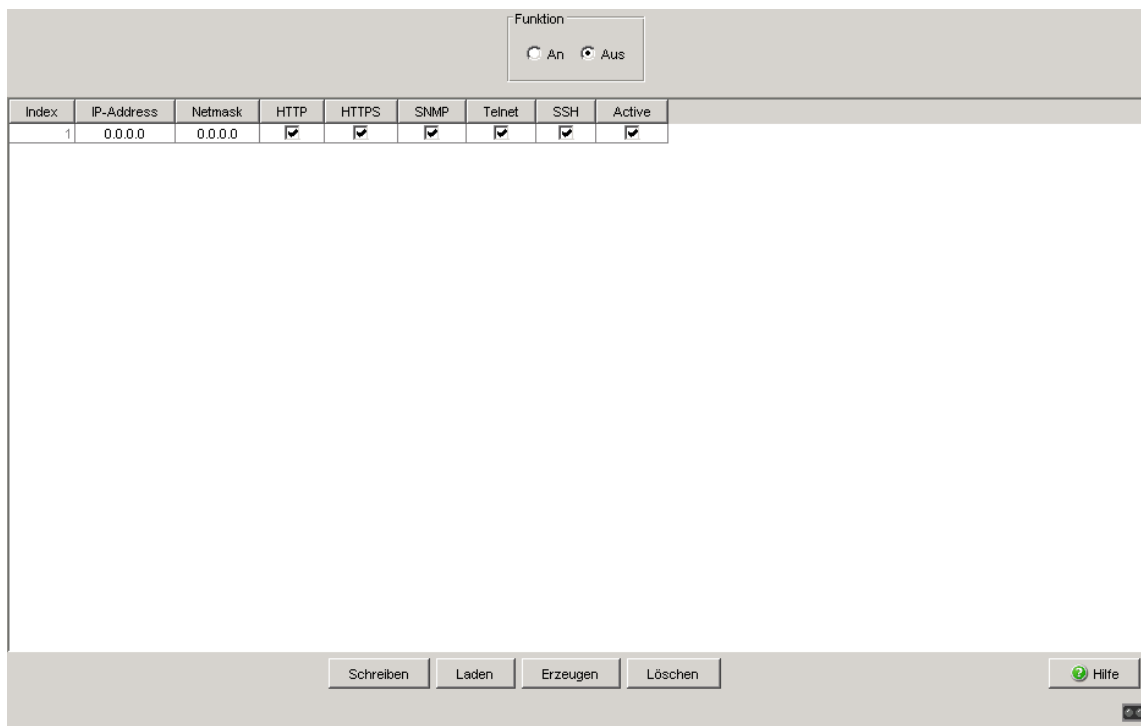


Abb. 28: Dialog Restricted Management Access
(Eingeschränkter Management-Zugriff)

■ 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	<p>enabled: Port ist eingeschaltet und vermittelt. disabled: Port ist ausgeschaltet und vermittelt nicht. Der Port ist eingeschaltet, wenn</p> <ul style="list-style-type: none"> - mit einer erlaubten Adresse auf diesen Port zugegriffen wird oder - versucht wird, mit einer nicht erlaubten Adresse auf den Port zuzugreifen und unter "Aktion" <code>trapOnly</code> oder <code>none</code> angewählt ist. <p>Der Port ist ausgeschaltet, wenn versucht wird, mit einer nicht erlaubten Adresse auf den Port zuzugreifen und unter "Aktion" <code>portDisable</code> angewählt ist.</p>
Erlaubte MAC-Adressen	<p>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.</p>
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	<p>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.</p>

Tab. 27: Konfiguration der Portsicherheit pro Port

Name	Bedeutung
Dynamisches Limit	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 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	<p>Aktion, die das Gerät nach einem unberechtigten Zugriff ausführt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>none</code> (Voreinstellung) Keine Aktion. ▶ <code>trapOnly</code> Alarm verschicken. ▶ <code>portDisable</code> 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 <code>Diagnose:Ports:Auto-Disable</code> folgende Einstellungen festgelegt haben: <ul style="list-style-type: none"> – Im Rahmen „Konfiguration“ ist das Kontrollkästchen für das auslösende Ereignis „Port-Sicherheit“ markiert. – Der Reset-Timer ist für den Port >0 festgelegt. ▶ <code>autoDisable</code> Deaktiviert den Port abhängig von den Einstellungen im Dialog <code>Diagnose:Ports:Auto-Disable</code>, Rahmen „Konfiguration“. <ul style="list-style-type: none"> – 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 <code>Diagnose:Ports:Auto-Disable</code> 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

Konfiguration
 MAC-basierte Portsicherheit IP-basierte Portsicherheit

Port	Port Status	Erlaubte MAC-Adressen	Aktuelle MAC-Adresse	Erlaubte IP-Adressen	Dynamisches Limit	Dynamische Anzahl	Aktion
1.1	enabled		00:00:00:00:00:00				none
1.2	enabled		00:80:63:74:67:C8				none
1.3	enabled		00:00:00:00:00:00				none
1.4	enabled		00:13:3B:00:00:AE				none
2.1	enabled		00:80:63:14:DB:DF				none
2.2	enabled		00:80:63:70:E8:7C				none
2.3	enabled		00:13:3B:00:03:45				none
2.4	enabled		00:80:63:4A:A7:BE				none
3.1	enabled		00:00:00:00:00:00				none
3.2	enabled		00:00:00:00:00:00				none

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	<p>Listet die MAC-Adressen auf, die auf den Port zugreifen dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Gültige Unicast-MAC-Adresse <p>Klicken Sie „Hinzufügen“, um die MAC-Adressen in das Feld „Erlaubte MAC-Adressen“ zu übertragen.</p>
MAC-Adresse	<p>Definiert die MAC-Adressen, die auf den Port zugreifen dürfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Gültige Unicast-MAC-Adresse <p>Geben Sie den Wert in einem der folgenden Formate ein:</p> <ul style="list-style-type: none"> – 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 <p>Klicken Sie „Hinzufügen“, um die MAC-Adressen in das Feld „Erlaubte MAC-Adressen“ zu übertragen.</p>
Mask	<p>Definiert die Anzahl der wesentlichen Stellen im MAC-Adressbereich.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..48 <p>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.</p>
Hinzufügen	Überträgt die im Feld „MAC-Adresse“ 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	<p>Aktion, die das Gerät nach einem unberechtigten Zugriff ausführt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 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 <code>Diagnose:Ports:Auto-Disable</code> folgende Einstellungen festgelegt haben: <ul style="list-style-type: none"> – 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 <code>Diagnose:Ports:Auto-Disable</code>, Rahmen „Konfiguration“. <ul style="list-style-type: none"> – 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 <code>Diagnose:Ports:Auto-Disable</code> 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. <p>Anmerkung: Voraussetzungen, damit das Gerät einen Alarm (Trap) senden kann:</p> <ul style="list-style-type: none"> – 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-Authentifizierung benötigt einen RADIUS-Server, der zur Authentifizierung und Autorisierung 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	Lieferzustand
Funktion	Schaltet die Funktion an oder aus	An, Aus	Aus
VLAN-Zuweisung aktivieren	<p>Aktiviert oder deaktiviert das Zuweisen einer VLAN-ID durch den RADIUS-Server an einen Port.</p> <p>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 ungetaggttes Mitglied in das angegebene VLAN auf und setzt die Port-VLAN-ID auf diesen Wert.</p> <p>Beachten Sie die folgenden Hinweise zur VLAN-Zuweisung.</p>	An, Aus	Aus

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

Anmerkung:**► Für die Geräte MACH 104 und MACH 1040:**

Der Switch kann eingehende ungetaggten Frames einem VLAN basierend auf der MAC-Absender-Adresse zuweisen. Haben Sie mehrere Endgeräte an einem Port angeschlossen, kann der Switch auch die ungetaggten Frames dieser Geräte verschiedenen VLANs zuweisen.

► 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	Lieferzustand
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	<p>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.</p> <p>► 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.</p> <p>► 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).</p>	An Aus	Aus

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

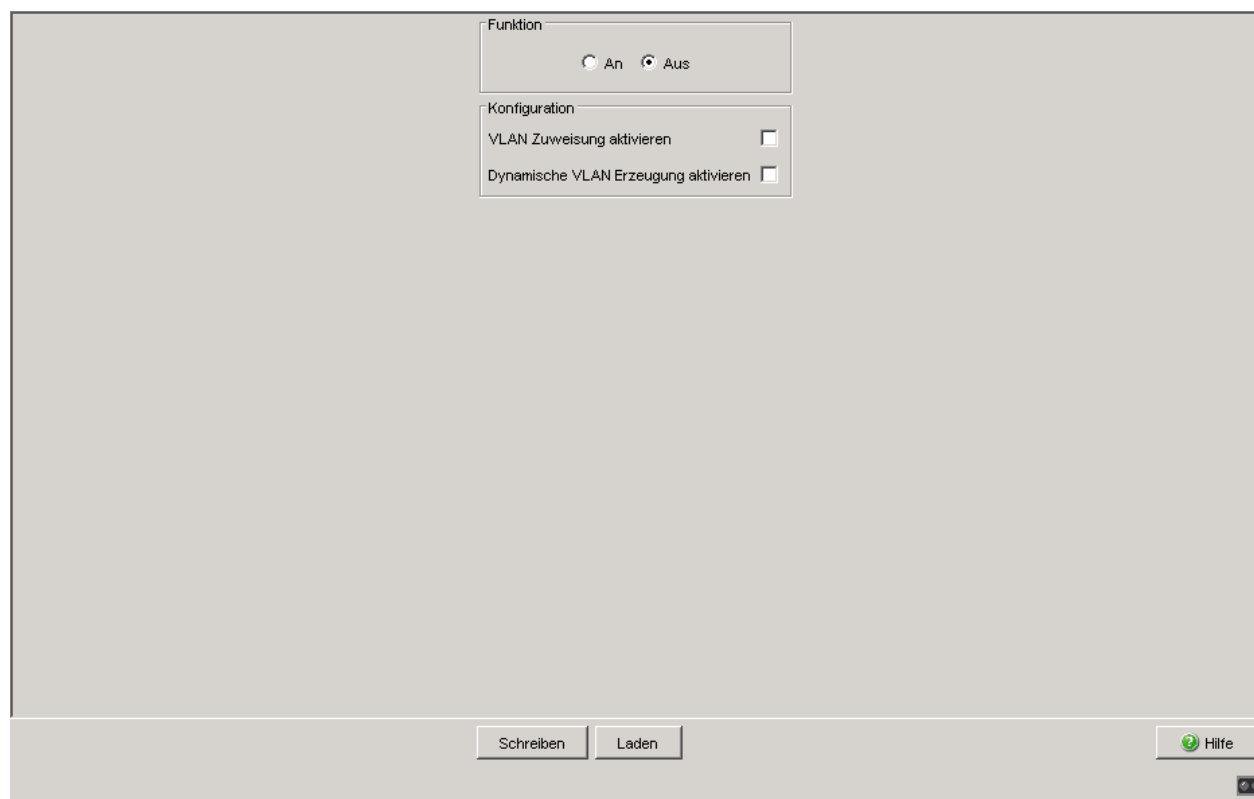


Abb. 30: Dialog 802.1X Global für die Gerätefamilien MACH 104 und MACH 1040

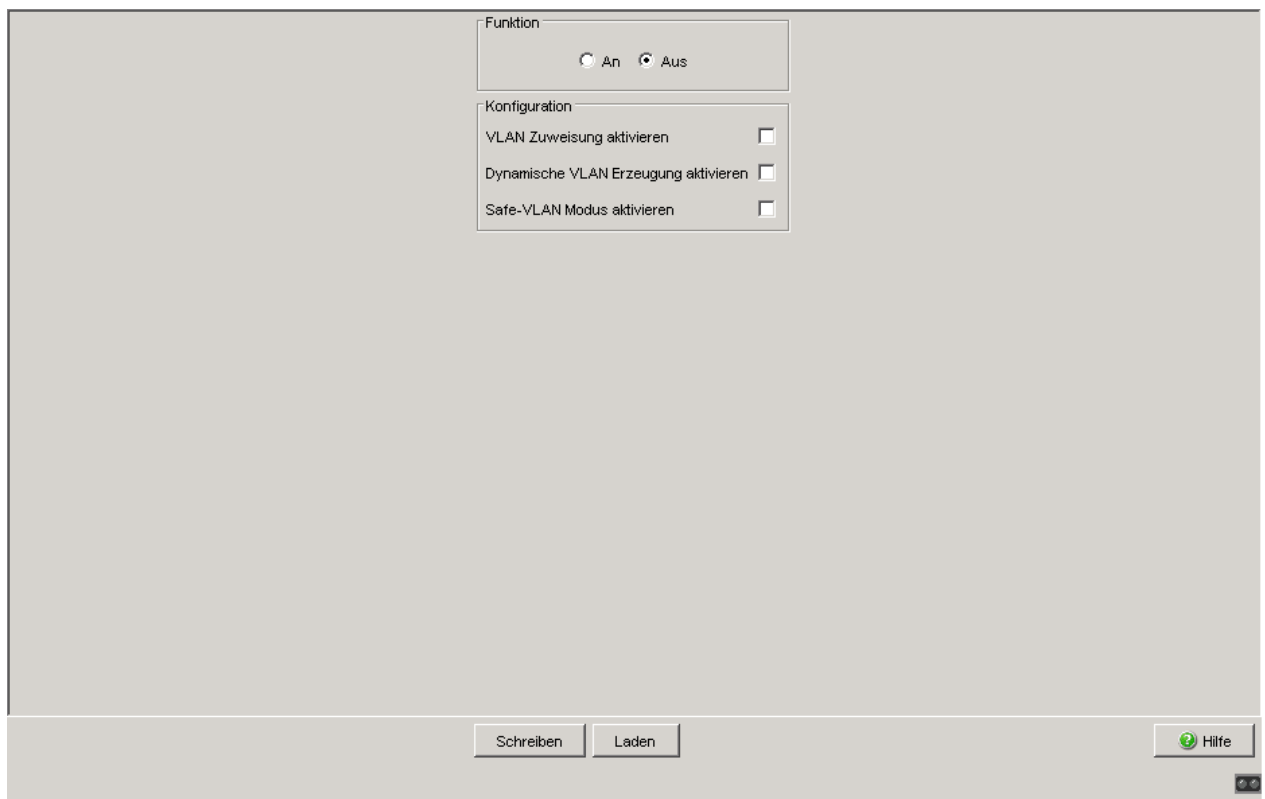


Abb. 31: Dialog 802.1X Global

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

Port ▲	Port Initialisierung	Port Reauthentifizierung	Authentifizierungsvorgang	Authentifizierungsstatus Server	Authentifizierungsstatus	Maximale Benutzeranzahl	Port Kontrolle
1.1	false	false	initialize	initialize		16	forceAuthorize
1.2	false	false	initialize	initialize		16	forceAuthorize
1.3	false	false	initialize	initialize		16	forceAuthorize
1.4	false	false	initialize	initialize		16	forceAuthorize
2.1	false	false	initialize	initialize		16	forceAuthorize
2.2	false	false	initialize	initialize		16	forceAuthorize
2.3	false	false	initialize	initialize		16	forceAuthorize
2.4	false	false	initialize	initialize		16	forceAuthorize
3.1	false	false	initialize	initialize		16	forceAuthorize
3.2	false	false	initialize	initialize		16	forceAuthorize

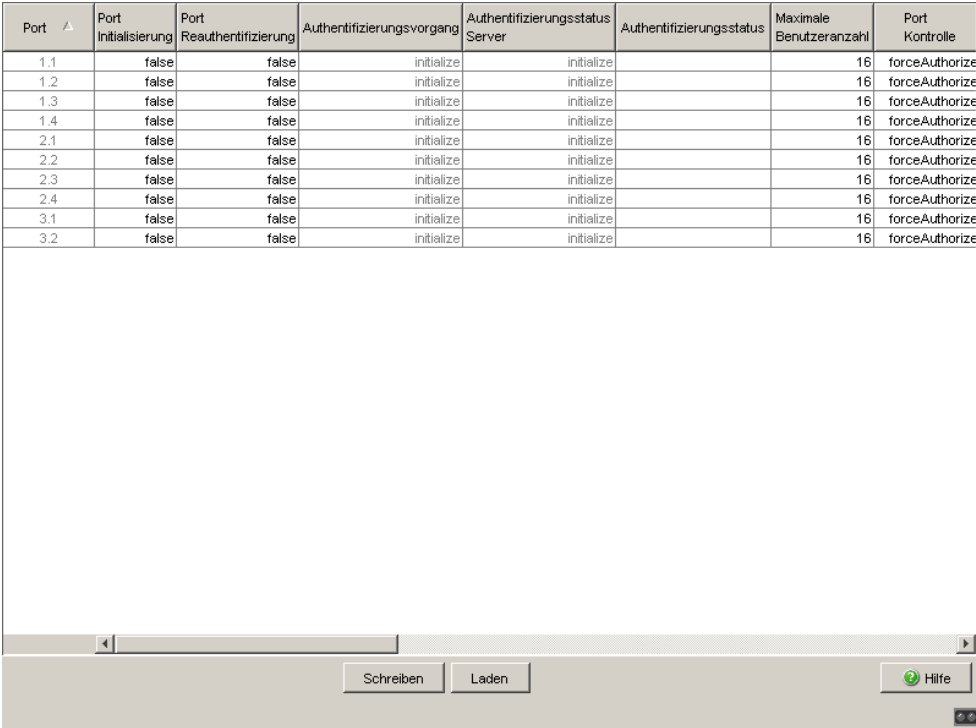


Abb. 32: 802.1X-Port-Konfigurationstabelle

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 Authentifizierungsvorganges 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 <code>macBased</code> eingestellt haben.	1 - 16	16
Port-Kontrolle	Einstellen der Portzugangskontrolle. Anmerkung: ▶ In den Modi <code>ForceAuthorized</code> , <code>ForceUnauthorized</code> und <code>auto</code> 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 <code>macBased</code> 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.	▶ <code>ForceAuthorized</code> : Zugang auch ohne Authentifizierung für alle Clients offen. ▶ <code>ForceUnauthorized</code> : Zugang für alle Clients gesperrt, auch für Clients mit Authentifizierung. ▶ <code>auto</code> : der Zugang zum Port ist vom Authentifizierungsergebnis abhängig. ▶ <code>macBased</code> : Verhalten wie bei <code>auto</code> . Zusätzlich Zugang für Clients mit einer MAC-Adresse, die der Client bei der Authentifizierung verwendet.	<code>ForceAuthorized</code>
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 ungetaggt Mitglied in diesem VLAN und die Port-VLAN-ID hat den selben Wert.	0 - 4094	0

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-Zuweisungskonflikten 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 112 „802.1X-Port-Clients“)

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 <code>auto</code> gesetzt.	<code>notAssigned</code> <code>radius</code> <code>unauthenticated-VLAN</code>	<code>notAssigned</code>
<p>Anmerkung: Wenn Sie die Multi-Client-Einstellung verwenden, indem Sie die „Port-Kontrolle“ auf <code>macBased</code> setzen, beachten Sie:</p> <ul style="list-style-type: none"> ▶ die geräteabhängige Auflösung von etwaigen VLAN-Zuweisungskonflikten 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 112 „802.1X-Port-Clients“) 			
Reauthenti- fizierungs- periode	Zeit in Sekunden, nach der das Gerät eine erneute Authentifizierung vom Supplikanten anfordert.	1-65.535	3.600
Reauthenti- fikation ein	Ein- oder Ausschalten der Reauthentifizierung	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	<p>ID eines VLANs, das der Switch dem Port zuweist, wenn:</p> <ul style="list-style-type: none"> ▶ das Protokoll 802.1X an dem Port aktiv ist und die Port-Kontrolle auf <code>auto</code> oder <code>macBased</code> gesetzt ist, ▶ ein Client Datenverkehr aufnehmen will ▶ und EAPOL-Frames vom Client ausbleiben, der Client also das 802.1X-Protokoll nicht unterstützt. <p>Der Switch:</p> <ul style="list-style-type: none"> ▶ schaltet den Port in den authentifizierten Zustand, ▶ lässt den Datenverkehr zu, ▶ jedoch ausschließlich in das Gast-VLAN. <p>Geben Sie eine Gast-VLAN-ID an, wenn Sie Geräten ohne 802.1X-Unterstützung einen Zugang in ein Gast-VLAN erlauben möchten.</p> <p>Anmerkung:</p> <ul style="list-style-type: none"> ▶ 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-Authenticated-Bypass (MAB) aktivieren, setzt Gerät die Gast-VLAN-ID automatisch auf 0. 	0 - 4094	0
Gast-VLAN-Intervall	<p>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.</p> <p>Läuft diese Zeit ab, stellt der Switch dem angeschlossenen Gerät einen Zugang ausschließlich ins Gast-VLAN zur Verfügung.</p>	1 - 300 s	90 s

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

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Unauthenticated VLAN ID	<p>ID eines VLANs, das der Switch dem Port zuweist, wenn:</p> <ul style="list-style-type: none"> ▶ 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. <p>Der Switch:</p> <ul style="list-style-type: none"> ▶ schaltet den Port in den authentifizierten Zustand, ▶ lässt den Datenverkehr zu, ▶ jedoch ausschließlich in das unauthentifizierte VLAN. <p>Geben Sie eine VLAN-ID für unauthentifizierte Geräte an, wenn:</p> <ul style="list-style-type: none"> ▶ 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. <p>Anmerkung:</p> <ul style="list-style-type: none"> ▶ Verwenden Sie als unauthentifiziertes VLAN ausschließlich ein VLAN, das Sie im Switch statisch eingerichtet haben. 	0 - 4094	0

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

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
MAC-Autho- rized- Bypass ein	<p>Durch MAB stellt der Switch einen authentifizierten Zugang zur Verfügung, wenn:</p> <ul style="list-style-type: none"> ▶ Sie die „Port-Kontrolle“ auf <code>macBased</code> 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. <p>Der Switch:</p> <ul style="list-style-type: none"> ▶ 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. <p>Aktivieren Sie diese Funktion, wenn:</p> <ul style="list-style-type: none"> ▶ Sie bestimmten Geräten einen normalen Zugang erlauben möchten, obwohl diese Geräte 802.1X nicht unterstützen. <p>Anmerkung:</p> <ul style="list-style-type: none"> ▶ 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 <code>Grundeinstellungen:Laden/Speichern</code> 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.

Port	Benutzer Name	MAC-Adresse	Zugewiesene VLAN ID	Zuweisungsgrund	Session-Timeout	Termination-Action

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.	0 - 4094	-
<p>Anmerkung: Wenn Sie die Multi-Client-Einstellung verwenden, indem Sie die „Port-Kontrolle“ auf <code>macBased</code> setzen, beachten Sie:</p> <ul style="list-style-type: none"> ▶ die geräteabhängige Auflösung von etwaigen VLAN-Zuweisungskonflikten 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 112 „802.1X-Port-Clients“) 			
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

Port	EAPOL Empfangene Frames	EAPOL Gesendete Frames	EAPOL Start-Frames	EAPOL Abmelde-Frames	EAPOL Antwort/ID Frames	EAPOL Antwort Frames	EAPOL Anforderung/ID F
1.1	0	0	0	0	0	0	0
1.2	0	0	0	0	0	0	0
1.3	0	0	0	0	0	0	0
1.4	0	0	0	0	0	0	0
2.1	0	0	0	0	0	0	0
2.2	0	0	0	0	0	0	0
2.3	0	0	0	0	0	0	0
2.4	0	0	0	0	0	0	0
3.1	0	0	0	0	0	0	0
3.2	0	0	0	0	0	0	0

Abbildung zeigt eine GUI-Tabelle mit den oben genannten Daten. Die Tabelle ist in einer Web-Oberfläche eingebettet, die einen Scrollbalken und zwei Schaltflächen 'Laden' und 'Hilfe' enthält.

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-Statistiktable

■ 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.

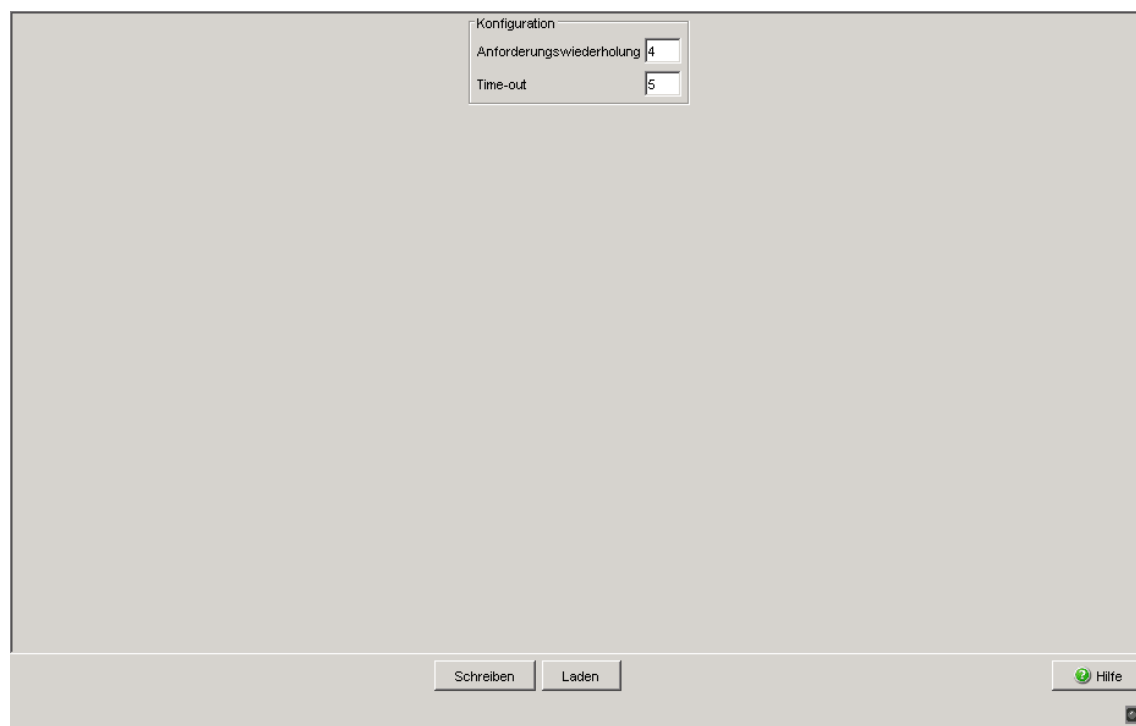


Abb. 35: Dialog *Sicherheit:RADIUS:Global*

■ Konfiguration

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Anforderungswiederholung	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 <code>Grundeinstellungen:Laden/Speichern</code> 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 angegebenen Primär-Server. Bleibt dessen Antwort aus, kontaktiert das Gerät den jeweils nächsten Server aus der Tabelle.

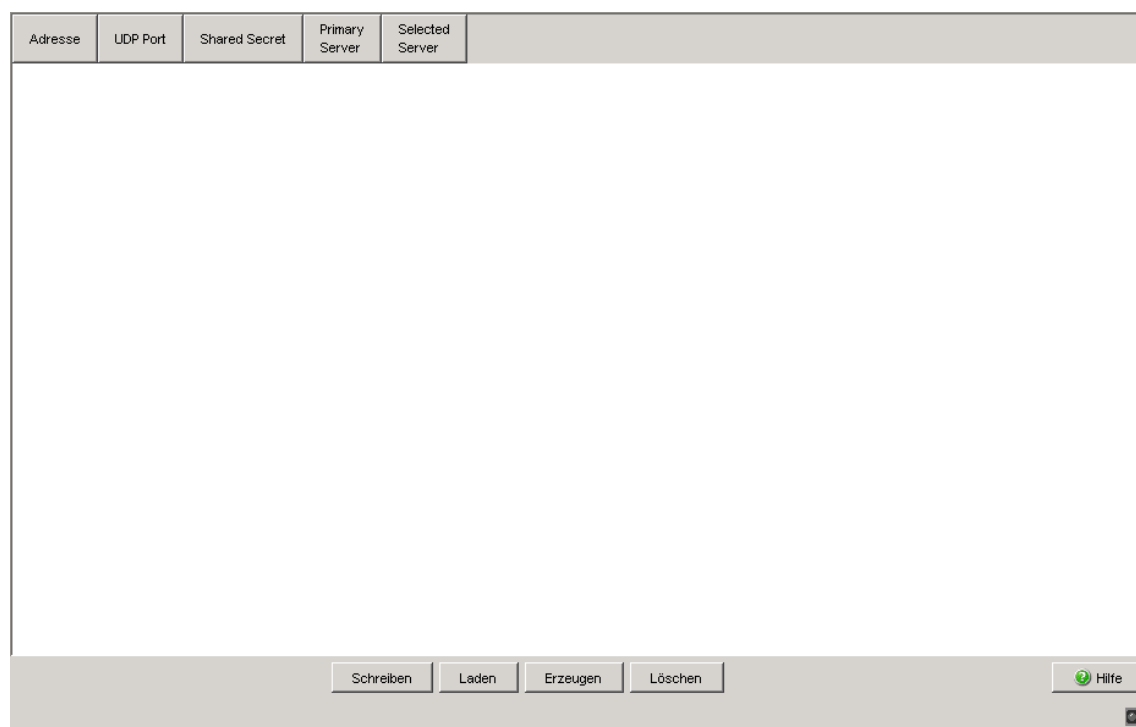


Abb. 36: Dialog *Sicherheit:RADIUS:RADIUS-Server* für das Gerät Power MICE

Adresse	UDP Port	Shared Secret	Primary Server	Selected Server
10.0.1.1	1812		<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
10.0.1.2	1812		<input type="checkbox"/>	<input type="checkbox"/>
10.0.1.3	1812		<input type="checkbox"/>	<input type="checkbox"/>

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	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..20 alphanumerische Zeichen <p>Das Passwort erfahren Sie vom Administrator des RADIUS-Servers.</p>
Primary Server	<p>Kennzeichnet den Authentication-Server als primär oder sekundär.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> 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. ▶ <code>unmarkiert</code> (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	<p>Zeigt die Verbindung zu einem aktiven Server an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Die Verbindung ist aktiv. Sofern die oben beschriebenen Bedingungen erfüllt sind, sendet das Gerät die Anmeldedaten zur Authentifizierung der Benutzer an diesen Server. ▶ <code>unmarkiert</code> 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 <code>Grundeinstellungen:Laden/Speichern</code> 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

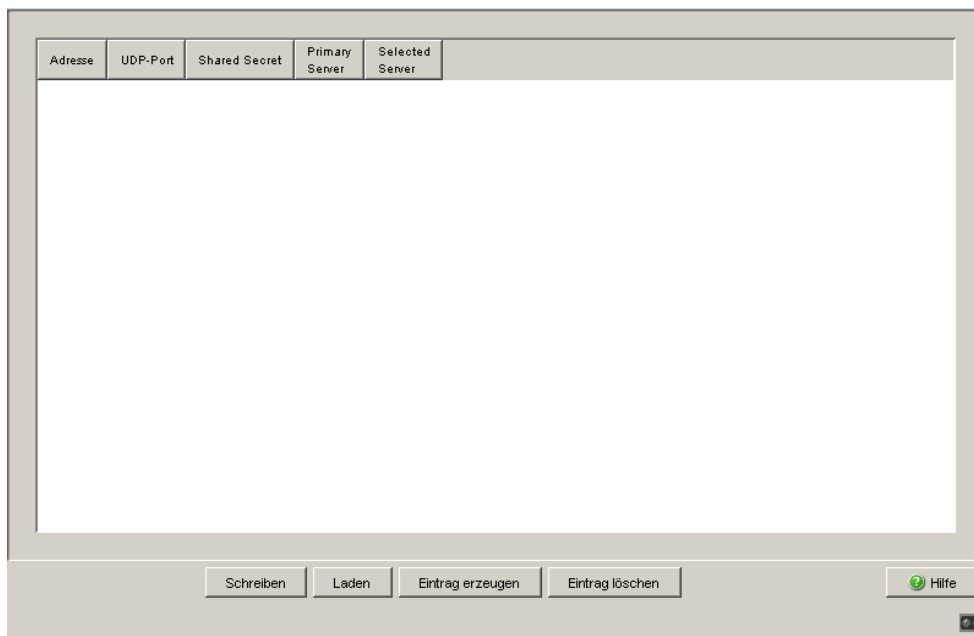


Abb. 38: Dialog RADIUS-Server

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.

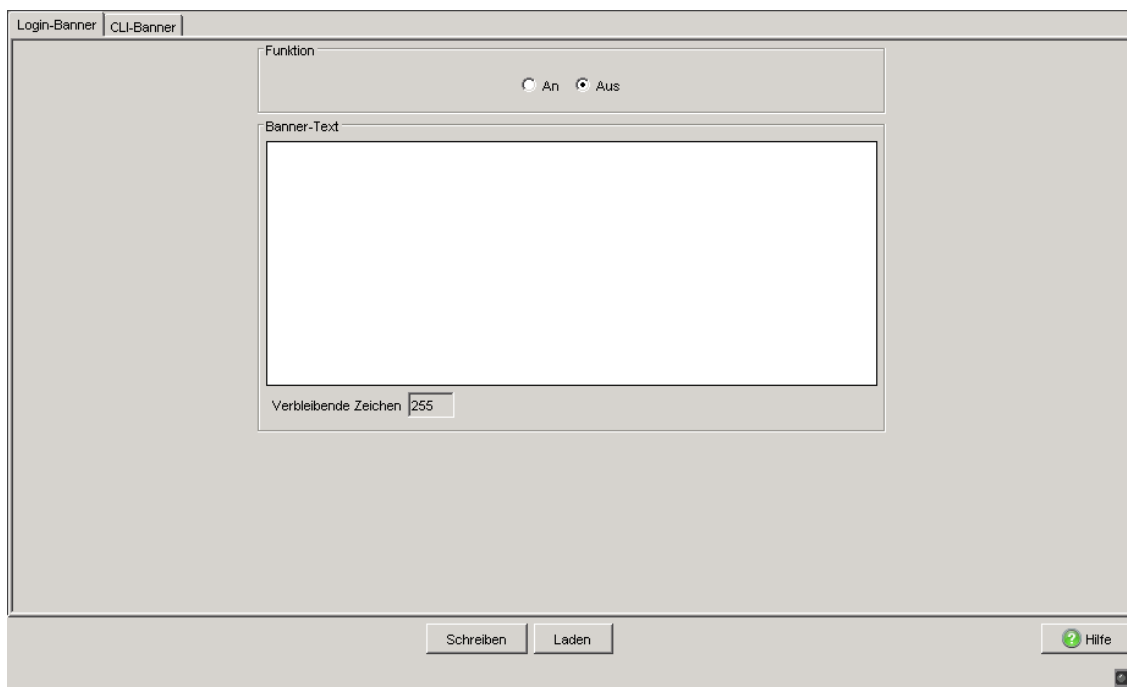


Abb. 39: Dialog „Login-/CLI-Banner“, Registerkarte „Login-Banner“

■ 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: <ul style="list-style-type: none"> ▶ Aus (Voreinstellung) ▶ An

■ Banner-Text

Parameter	Bedeutung
Banner-Text	<p>Legt den Text fest, den das Gerät im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface anzeigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen (0x20..0x7E) inklusive Leerzeichen▶ Tabulator \t▶ Zeilenumbruch \n
Verbleibende Zeichen	<p>Zeigt, wie viele Zeichen im Feld „Banner-Text“ noch zur Verfügung stehen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 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.

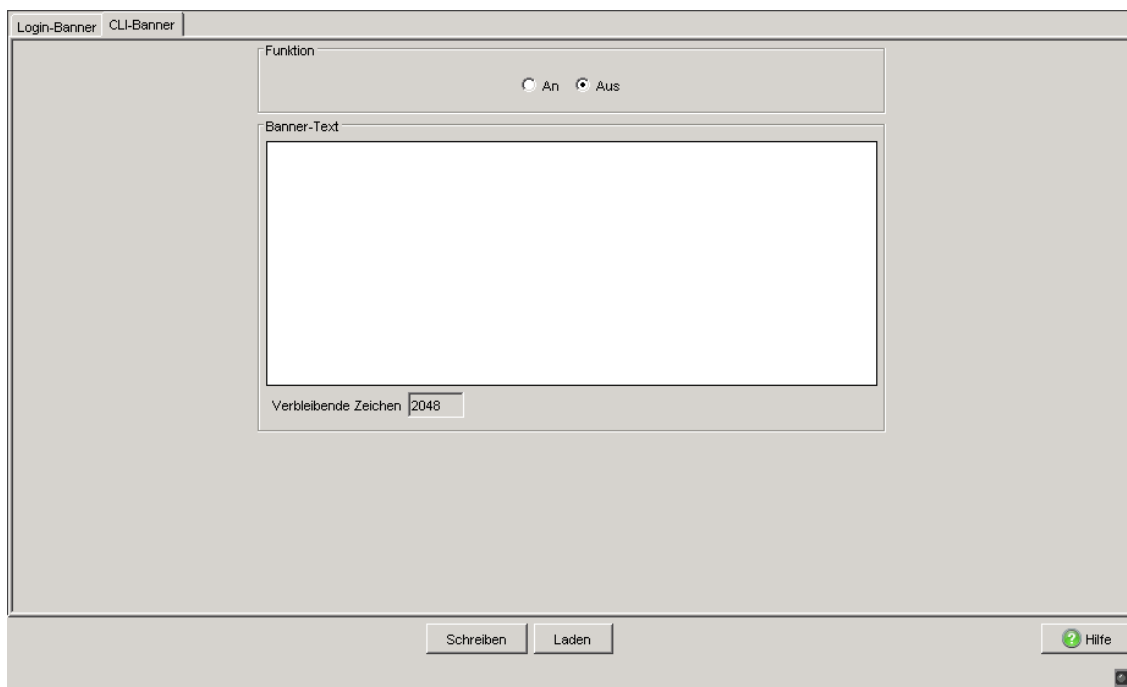


Abb. 40: Dialog „Login-/CLI-Banner“, Registerkarte „CLI-Banner“

■ Funktion

Parameter	Bedeutung
Funktion	<p>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.</p> <p>Bei ausgeschalteter Funktion zeigt der CLI-Startbildschirm Informationen über das Gerät. Die Textinformation im Feld „Banner-Text“ bleibt erhalten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Aus (Voreinstellung) ▶ An

■ Banner-Text

Parameter	Bedeutung
Banner-Text	<p>Legt die Textinformation fest, die das Gerät den Benutzern anstatt der voreingestellten Informationen anzeigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ alphanumerische ASCII-Zeichenfolge mit 0..2048 Zeichen (0x20..0x7E) inklusive Leerzeichen ▶ Tabulator \t ▶ Zeilenumbruch \n
Verbleibende Zeichen	<p>Zeigt, wie viele Zeichen im Feld „Banner-Text“ noch für die Textinformation zur Verfügung stehen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 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 <code>Grundeinstellungen:Laden/Speichern</code> 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

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 Zeitemstellung 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.

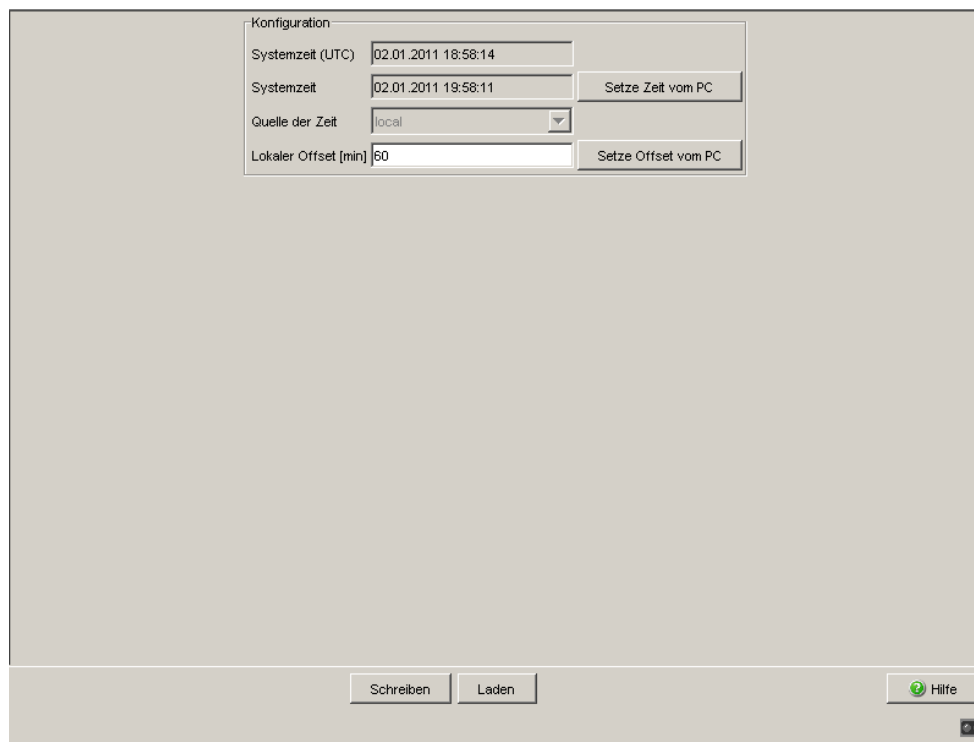


Abb. 41: Dialog Zeit, Grundeinstellungen

■ 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	Lieferzustand
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	Lieferzustand
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-Sendeintervall	Zeitabstand, in dem das Gerät SNTP-Pakete verschickt.	1 - 3.600	120
Server deaktivieren bei lokaler Zeitquelle	Ein-/Ausschalten der SNTP-Server-Funktion, wenn der Status der Quelle der Zeit <code>local</code> 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 Zeitstempelinheit 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 Zeitstempeln aufweisen, unterstützen abhängig von der Ausführung der Zeitstempeln 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.

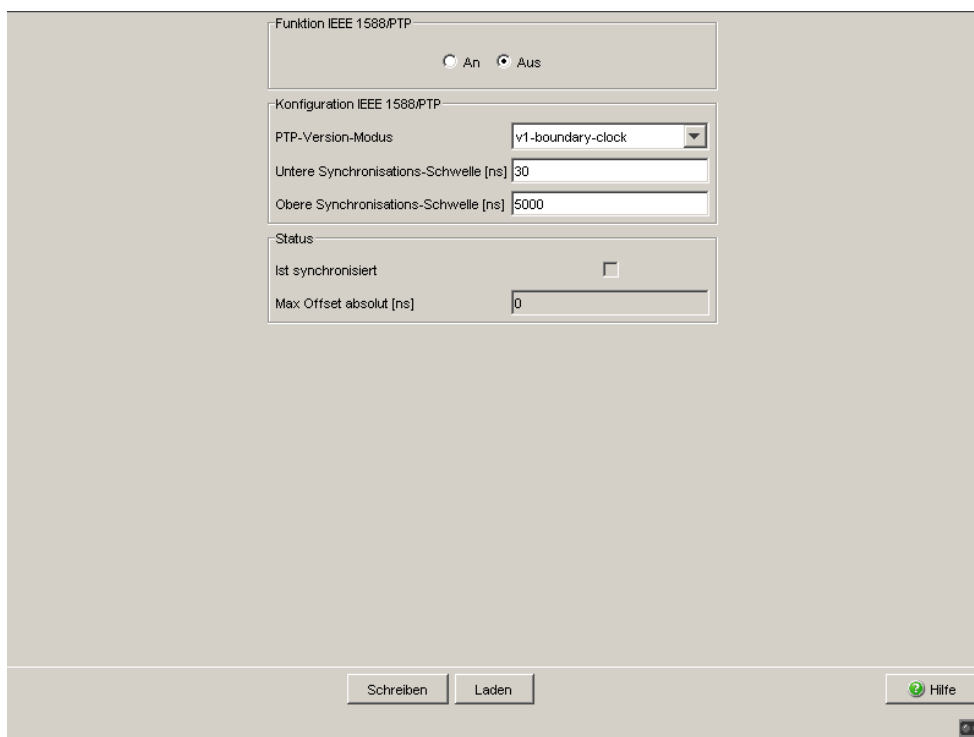


Abb. 43: Dialog PTP Global

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 Zeitstempereinheit	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
	v2-boundary-clock-twostep	Version 2	Ja	bearbeiten
	v2-transparent-clock	Version 2	Ja	weiterleiten

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.

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

Die PTP-Modi

- ▶ v1-boundary-clock
- ▶ v2-boundary-clock-onestep¹
- ▶ 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	<p>Boundary-Clock-Funktion nach IEEE1588-2002 (PTPv1)</p> <p>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.</p>
v1-simple-mode	<p>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.</p> <p>Wählen Sie diesen Modus, wenn das Gerät ausschließlich Ports ohne Zeitstempelinheit besitzt.</p>
v2-boundary-clock-onestep	<p>Boundary-Clock-Funktion nach IEEE 1588-2008 (PTPv2). Der One-Step-Modus übermittelt die präzise PTP-Zeit mit 1 Nachricht.</p> <p>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.</p>
v2-boundary-clock-twostep	<p>Boundary-Clock-Funktion nach IEEE 1588-2008 (PTPv2). Der Two-Step-Modus übermittelt die präzise PTP-Zeit mit 2 Nachrichten.</p>
v2-transparent-clock	<p>Transparent-Clock-Funktion nach IEEE 1588-2008 (PTPv2).</p> <p>Die Geräte MS20, MS30 und PowerMICE mit den Modulen MM23 oder MM33 verwenden dabei ausschließlich den One-Step-Modus.</p> <p>Die Geräte MACH 104 und MACH 1040 verwenden dabei ausschließlich den Two-Step-Modus. Sie unterstützen eine Empfangsrate von max. 8 Frames/s.</p>
v2-simple-mode	<p>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.</p> <p>Wählen Sie diesen Modus, wenn das Gerät ausschließlich Ports ohne Zeitstempelinheit besitzt.</p>

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	<p>an: Während eines Synchronisationsintervalls finden 2 bis 8 Synchronisationsabläufe statt. Dies ermöglicht eine schnellere Synchronisation bei entsprechend erhöhter Netzlast.</p> <p>aus: Während eines Synchronisationsintervalls findet ein Synchronisationsablauf statt.</p>	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
Domänennummer	Zuordnung der Uhr zu einer PTPv2 Domäne. Ausschließlich Uhren der gleichen Domäne werden synchronisiert.	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 internalOscillator	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-Laufzeitmess-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-Laufzeitmess-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.	none, 0 - 4042	none
	<p>Anmerkung:</p> <ul style="list-style-type: none"> ▶ Beachten Sie dabei auch die VLAN-Einstellungen des Ports (siehe auf Seite 196 „VLAN Statisch“), besonders, ob das VLAN existiert und ob der Port getaggt oder ungetaggt Mitglied in dem VLAN ist. ▶ none: das Gerät sendet PTP-Frames stets ohne VLAN-Tag, auch wenn der Port getaggt Mitglied des VLANs ist. ▶ VLANs, die Sie im Gerät bereits eingerichtet haben, können Sie mit Hilfe der Drop-down-Liste der Tabellenzelle auswählen. 		
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: <ul style="list-style-type: none"> ▶ 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 Hinweismessages 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.	none, 0 - 4042	none
	<p>Anmerkung:</p> <ul style="list-style-type: none"> ▶ Beachten Sie dabei auch die VLAN-Einstellungen des Ports (siehe auf Seite 196 „VLAN Statisch“), besonders, ob das VLAN existiert und ob der Port getaggt oder ungetaggt Mitglied in dem VLAN ist. ▶ none: das Gerät sendet PTP-Frames stets ohne VLAN-Tag, auch wenn der Port getaggt Mitglied des VLANs ist. ▶ VLANs, die Sie im Gerät bereits eingerichtet haben, können Sie mit Hilfe der Drop-down-Liste der Tabellenzeile auswählen. 		
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: <ul style="list-style-type: none"> ▶ 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 <i>Grundeinstellungen:Laden/Speichern</i> , 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-Laufzeitmess-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.		
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.	PowerMICE, MACH 104, MACH 1040, MACH 4000: 10-630 RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS: 15-3.825	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.	An, Aus	An
Paketgröße	Einstellen der maximalen Paketgröße (Frame Size) in Bytes.	MACH 104, MACH 1040: 1522, 1552, 9022 PowerMICE, MACH 4000: 1.522, 1.552 RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS: 1.522, 1.632	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
Address-Relearn-Threshold	Anzahl der gelernten MAC-Adressen an unterschiedlichen Ports innerhalb eines Prüfindervalls. 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 speziellen 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

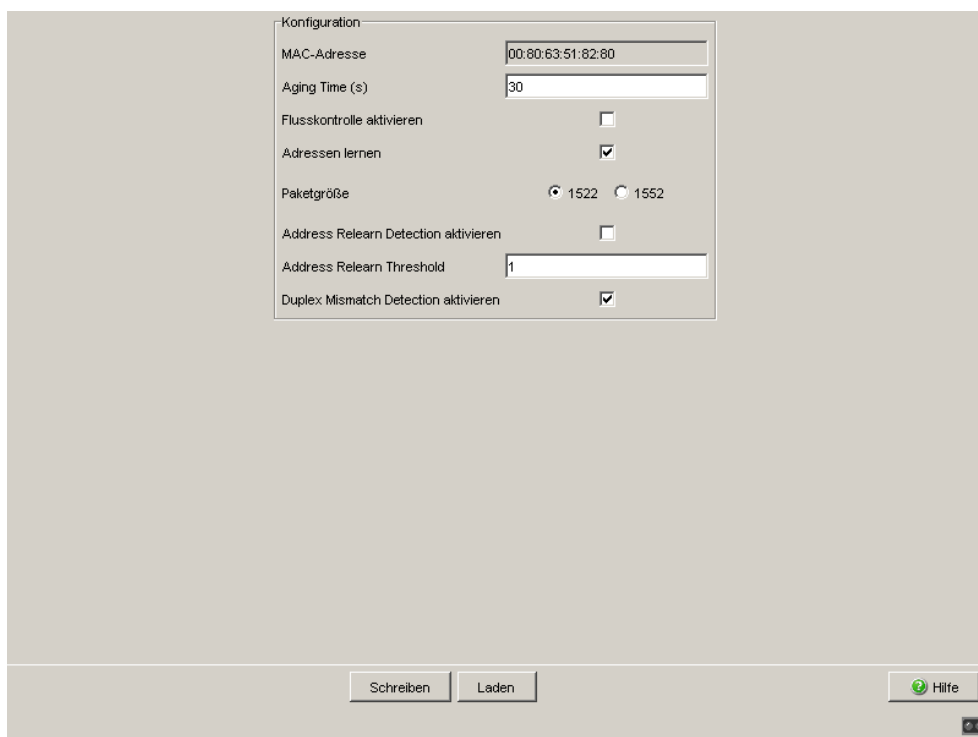


Abb. 44: Dialog Switching Global

■ 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.

Adresse Δ	Status	VLAN-ID	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2	8.1	8.2
00 15 58 7c f5 15	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 14 db df	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 2f fb c0	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 4a a7 be	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 51 74 0b	learned	1	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 51 7a 8a	learned	1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
00 80 63 51 82 80	mgmt	1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Buttons: Schreiben, Laden, Anlegen, Hilfe

Abb. 45: Dialog Filtertabelle

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: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> <input type="checkbox"/> Wählen Sie einen Port aus, wenn die Ziel-MAC-Adresse eine Unicast-Adresse ist. <input type="checkbox"/> Wählen Sie einen oder mehrere Ports aus, wenn die Ziel-MAC-Adresse eine Multicast-Adresse ist. <input type="checkbox"/> 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. <ul style="list-style-type: none"> <input type="checkbox"/> Wählen Sie einen Port aus, wenn die Ziel-MAC-Adresse eine Unicast-Adresse ist. <input type="checkbox"/> Wählen Sie einen oder mehrere Ports aus, wenn die Ziel-MAC-Adresse eine Multicast-Adresse ist. <input type="checkbox"/> 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 <i>Grundeinstellungen:Laden/Speichern</i> 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 226 „Link-Aggregation“](#)) eingebunden sind, sind von der Lastbegrenzung ausgenommen, unabhängig von den Einträgen im Dialog „Lastbegrenzer“.

4.3.1 Lastbegrenzer-Einstellungen für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS

- ▶ „Eingangsbegrenzer (kbit/s)“ bietet Ihnen die Möglichkeit, die Eingangsbegrenzerfunktion für alle Ports ein-/auszuschalten.
- ▶ „Ausgangsbegrenzer (Pkt/s)“ bietet Ihnen die Möglichkeit, die Broadcast-Ausgangsbegrenzung an allen Ports ein/auszuschalten.
- ▶ „Ausgangsbegrenzer (kbit/s)“ bietet Ihnen die Möglichkeit, die Ausgangsbegrenzung für alle Pakettypen an allen Ports ein/auszuschalten.

Einstellmöglichkeiten pro Port:

- ▶ „Eingangspakettypen“ bietet Ihnen die Möglichkeit, den Pakettyp auszuwählen, für den die Begrenzung gelten soll:
 - ▶ All, Begrenzung des gesamten eingangsseitigen Datenvolumens an diesem Port.
 - ▶ BC, Begrenzung des eingangsseitigen Broadcast-Volumens an diesem Port.
 - ▶ BC + MC, Begrenzung des eingangsseitigen Broadcast- und Multicast-Volumens an diesem Port.
 - ▶ BC + MC + uUC, Begrenzung des eingangsseitigen Broadcast-, Multicast- und unbekanntem Unicast-Volumens an diesem Port.
- ▶ „Eingangsbegrenzerrate (kbit/s)“ für den gewählten Eingangspakettyp:
 - ▶ = 0, keine Begrenzung eingangsseitig an diesem Port.
 - ▶ > 0, maximale Übertragungsrate in kbit/s, die an diesem Port empfangen werden darf.
- ▶ „Ausgangsbegrenzerrate (Pkt/s)“ 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.
- ▶ „Ausgangsbegrenzerrate (kbit/s)“ für den gesamten Datenstrom:
 - ▶ = 0, keine Begrenzung des Datenstroms ausgangsseitig an diesem Port.
 - ▶ > 0, maximale Übertragungsrate in kbit/s, die ausgangsseitig an diesem Port gesendet wird.

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“.

Modul	Port	Eingangsbegrenzer (kbit/s)	Ausgangsbegrenzer (Pkt/s) Pakettyp: BC	Ausgangsbegrenzer (kbit/s) Pakettypen: alle
1	1	BC	0	0
1	2	All	0	0
1	3	BC	0	0
1	4	BC + MC	0	0
1	5	BC + MC + uJK	0	0
1	6	BC	0	0
1	7	BC	0	0
1	8	BC	0	0
1	9	BC	0	0
1	10	BC	0	0
1	11	BC	0	0
1	12	BC	0	0
1	13	BC	0	0
1	14	BC	0	0
1	15	BC	0	0

Abb. 46: Dialog Lastbegrenzer

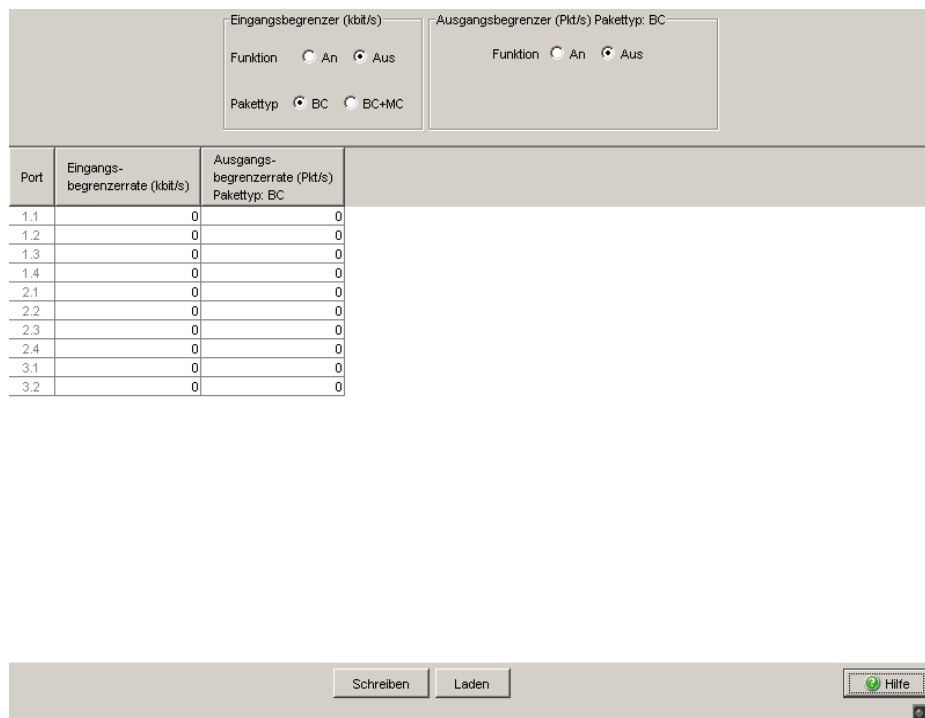
4.3.2 Lastbegrenzer-Einstellungen (PowerMICE und MACH 4000)

- ▶ „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“.



Port	Eingangsbegrenzer (kbit/s)	Ausgangsbegrenzer (Pkt/s) Paketty: BC
1.1	0	0
1.2	0	0
1.3	0	0
1.4	0	0
2.1	0	0
2.2	0	0
2.3	0	0
2.4	0	0
3.1	0	0
3.2	0	0

Abb. 47: 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.

Port	IGMP an	IGMP Forw. All	IGMP Automatic Query Port	Statischer Query Port	Gelernter Query Port
1.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
2.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
2.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
2.3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
2.4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
3.1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
3.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>

Abb. 48: 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: <ul style="list-style-type: none"> ▶ 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

- ▶ unbekanntes -nicht mit IGMP-Snooping gelerntes- MAC-/IP-Multicast-Adressen
- ▶ bekanntes -mit IGMP-Snooping gelerntes- MAC-/IP-Multicast-Adressen

vermittelt.

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

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Unbekannte Multicasts	<ul style="list-style-type: none"> ▶ 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	<ul style="list-style-type: none"> ▶ 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 Porteeinstellungen. 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 ungelerten 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 <code>Forward All</code> ein-/ausschalten. Mit der Einstellung <code>IGMP Forward All</code> vermittelt das Gerät an diesem Port alle Datenpakete mit einer Multicast-Adresse im Zieladressfeld. Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.	An Aus	Aus
<p>Anmerkung: Sind mehrere Router an ein Subnetz angeschlossen, dann verwenden Sie IGMP-Version 1, damit alle Router alle IGMP-Reports erhalten.</p> <p>Anmerkung: Wenn Sie IGMP-Version 1 in einem Subnetz verwenden, dann verwenden Sie IGMP-Version 1 auch im gesamten Netz.</p>			
IGMP Automatic Query Port	Anzeige, welche Ports das Gerät als Query-Ports gelernt hat, wenn in „Statischer Query Port“ <code>automatic</code> 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.

Funktion

An Aus

Port	GMRP	GMRP Service Requirement
1.1	<input checked="" type="checkbox"/>	Forward all unregistered groups
1.2	<input checked="" type="checkbox"/>	Forward all unregistered groups
1.3	<input checked="" type="checkbox"/>	Forward all unregistered groups
1.4	<input checked="" type="checkbox"/>	Forward all unregistered groups
2.1	<input checked="" type="checkbox"/>	Forward all unregistered groups
2.2	<input checked="" type="checkbox"/>	Forward all unregistered groups
2.3	<input checked="" type="checkbox"/>	Forward all unregistered groups
2.4	<input checked="" type="checkbox"/>	Forward all unregistered groups
3.1	<input checked="" type="checkbox"/>	Forward all unregistered groups
3.2	<input checked="" type="checkbox"/>	Forward all unregistered groups
5.1	<input checked="" type="checkbox"/>	Forward all unregistered groups
5.2	<input checked="" type="checkbox"/>	Forward all unregistered groups
5.3	<input checked="" type="checkbox"/>	Forward all unregistered groups
5.4	<input checked="" type="checkbox"/>	Forward all unregistered groups

Schreiben Laden Hilfe

Abb. 49: Dialog GMRP

■ Funktion

Dieser Rahmen bietet Ihnen die Möglichkeit,

- ▶ die GMRP-Funktion global ein- oder auszuschalten.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
GMRP	<p>GMRP für das gesamte Gerät global einschalten.</p> <p>Ist GMRP ausgeschaltet, dann:</p> <ul style="list-style-type: none"> ▶ generiert das Gerät keine GMRP-Pakete, ▶ wertet empfangene GMRP-Pakete nicht aus und ▶ sendet (flutet) empfangene Datenpakete an allen Ports. <p>Für empfangene GMRP-Pakete ist das Gerät unabhängig von der GMRP-Einstellung transparent.</p>	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
 ▶ unbekanntem -nicht mit GMRP gelernten- MAC-Multicast-Adressen vermittelt.

Voraussetzung: Die GMRP-Funktion ist global eingeschaltet.

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Unbekannte Multicasts	<ul style="list-style-type: none"> ▶ 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 <ul style="list-style-type: none"> – einen statischen Filteradress-Eintrag am Anschluss-Port. – Auswählen von <code>Forward all groups</code>. Ports mit der Auswahl <code>Forward all groups</code> trägt das Gerät in alle Multicast-Filtereinträge ein, die über GMRP gelernt wurden. Voraussetzung: Die GMRP-Funktion ist global eingeschaltet.	<code>Forward all groups</code> , <code>Forward all unregistered groups</code>	<code>Forward all unregistered groups</code>

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 <code>Grundeinstellungen:Laden/Speichern</code> 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 196 „VLAN Statisch“).
Max. Anzahl VLANs	Anzeige der maximal möglichen Anzahl von VLANs (siehe auf Seite 196 „VLAN Statisch“).
Eingerichtete VLANs	Zeigt die Anzahl der eingerichteten VLANs an (siehe auf Seite 196 „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 199 „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	0 - 65.535	33.024 (8100 _H)

Anmerkung: Diese Einstellung wirkt sich ausschließlich bei Core-Port aus. Access-Ports und normale Ports ignorieren diese Einstellung und verwenden immer 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 RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS:
Im „Transparent-Modus“ ignorieren die Geräte die eingestellte Port-VLAN-ID. Stellen Sie die VLAN-Zugehörigkeit der Ports von VLAN 1 auf \cup (Member Untagged) oder \mathbb{T} (Member Tagged), ([siehe auf Seite 196 „VLAN Statisch“](#)).
- ▶ 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 „ \cup “ (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 „ \cup “ (Untagged).

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Modus	<p>Wahl des VLAN-Modus.</p> <p>„Independent VLAN“ (unabhängiges VLAN), unterteilt die Forwarding Database (siehe auf Seite 168 „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.</p> <p>Anwendungsgebiet: Aufbau identischer Netze, die auch gleiche MAC-Adressen benutzen.</p> <p>„Shared VLAN“ (gemeinsames VLAN), benutzt für alle VLANs die gemeinsame Forwarding Database (siehe auf Seite 168 „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.</p> <p>Anwendungsgebiet: Bei sich überlappenden Gruppen kann das Gerät VLAN-übergreifend direkt vermitteln, sofern die betroffenen Ports einem erreichbaren VLANs angehören.</p> <p>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.</p>	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“

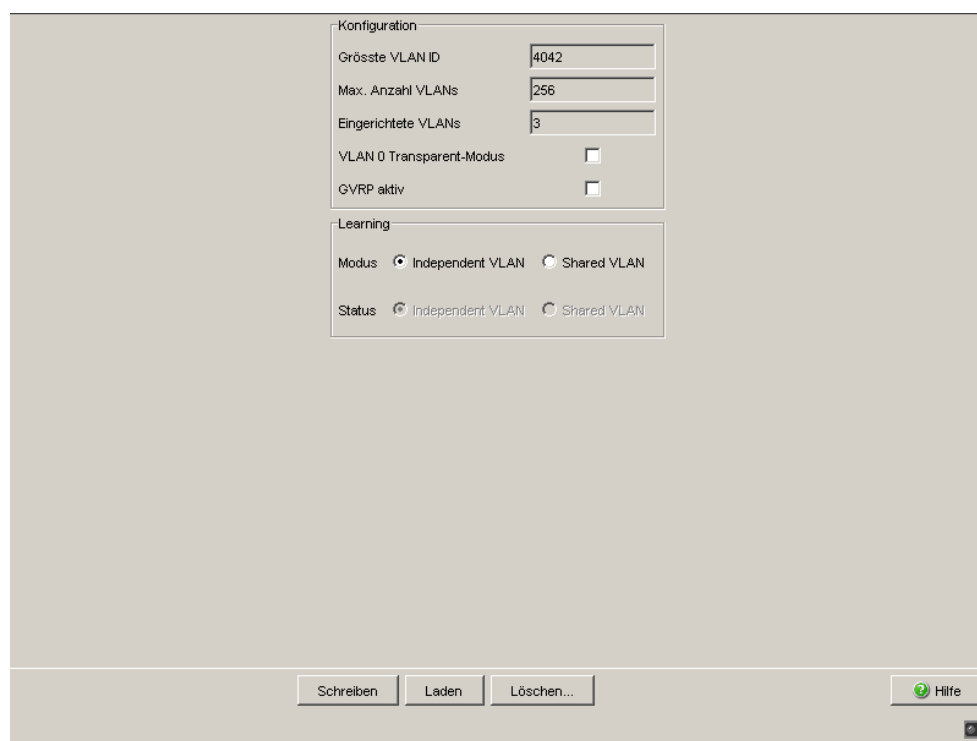


Abb. 50: Dialog VLAN Global

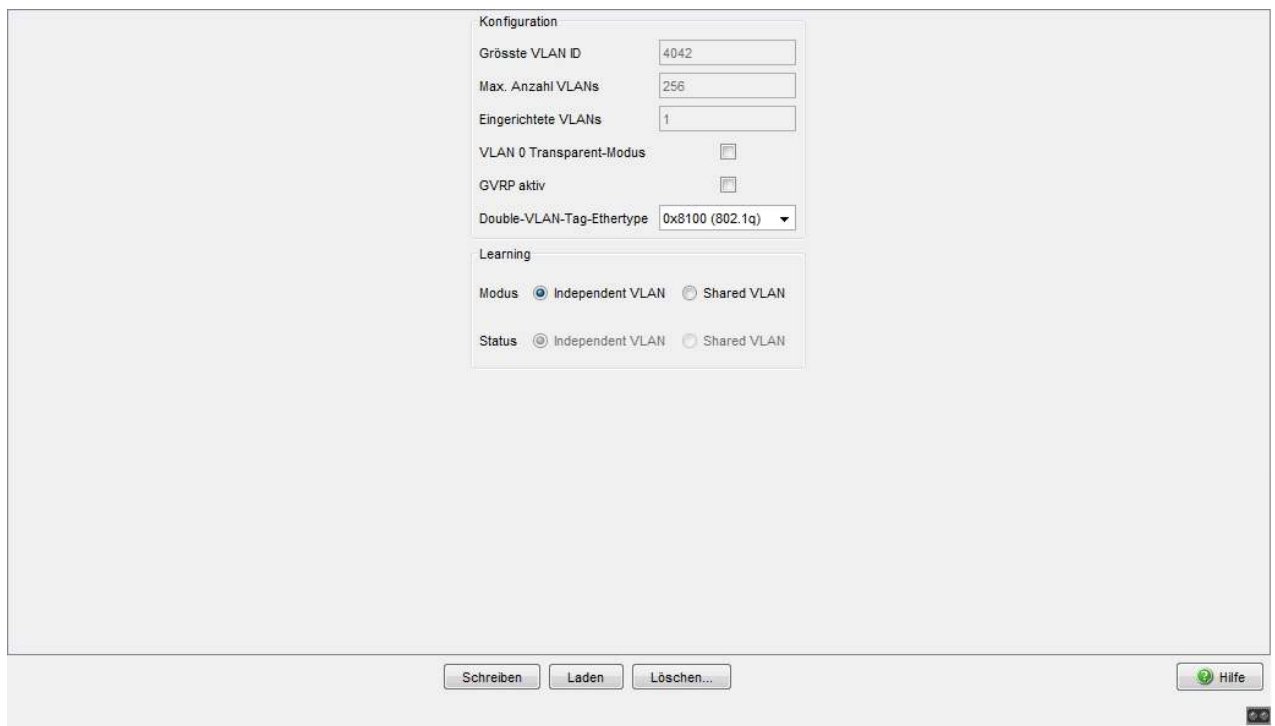


Abb. 51: Dialog *Switching:VLAN:Global* (MACH4000 und MACH 1040)

■ 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 <i>Grundeinstellungen:Laden/Speichern</i> 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 <i>Grundeinstellungen:Netz</i> 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

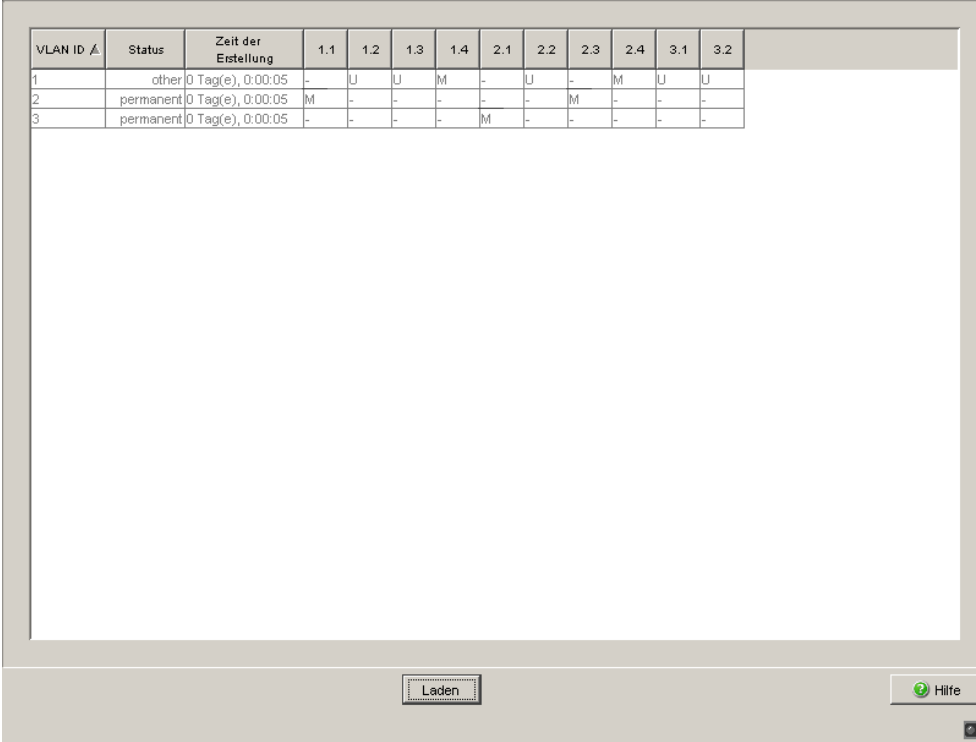
- ▶ manuell konfigurierten VLANs
- ▶ durch Redundanz-Mechanismen konfigurierten VLANs
- ▶ durch GVRP konfigurierten VLANs

Die VLAN Aktuell-Tabelle dient ausschließlich der Anzeige. Änderungen der Einträge nehmen Sie im Dialog `VLAN: Statisch` vor ([siehe auf Seite 196 „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	<p><code>other</code>: Dieser Eintrag tritt ausschließlich bei VLAN 1 auf. Das System gibt das VLAN 1 vor. VLAN 1 ist stets vorhanden.</p> <p><code>permanent</code>: Ein von Ihnen eingegebener statischer Eintrag. Dieser Eintrag bleibt nach einem Neustart des Gerätes erhalten.</p> <p><code>dynamic</code>: Dieses VLAN wurde dynamisch über GVRP erzeugt.</p>
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.	<p>– momentan kein Mitglied (Eintrag per GVRP möglich)</p> <p>T Mitglied im VLAN, Datenpakete mit Tag (Tagged) versenden.</p> <p>U Mitglied im VLAN, Datenpakete ohne Tag (Untagged) versenden.</p> <p>F Mitgliedschaft verboten (Forbidden), also auch kein Eintrag per GVRP möglich.</p>

Tab. 102: VLAN Aktuell



VLAN ID ▲	Status	Zeit der Erstellung	1.1	1.2	1.3	1.4	2.1	2.2	2.3	2.4	3.1	3.2
1	other	0 Tag(e), 0:00:05	-	U	U	M	-	U	-	M	U	U
2	permanent	0 Tag(e), 0:00:05	M	-	-	-	-	-	M	-	-	-
3	permanent	0 Tag(e), 0:00:05	-	-	-	-	M	-	-	-	-	-

Laden

Hilfe

Abb. 52: 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

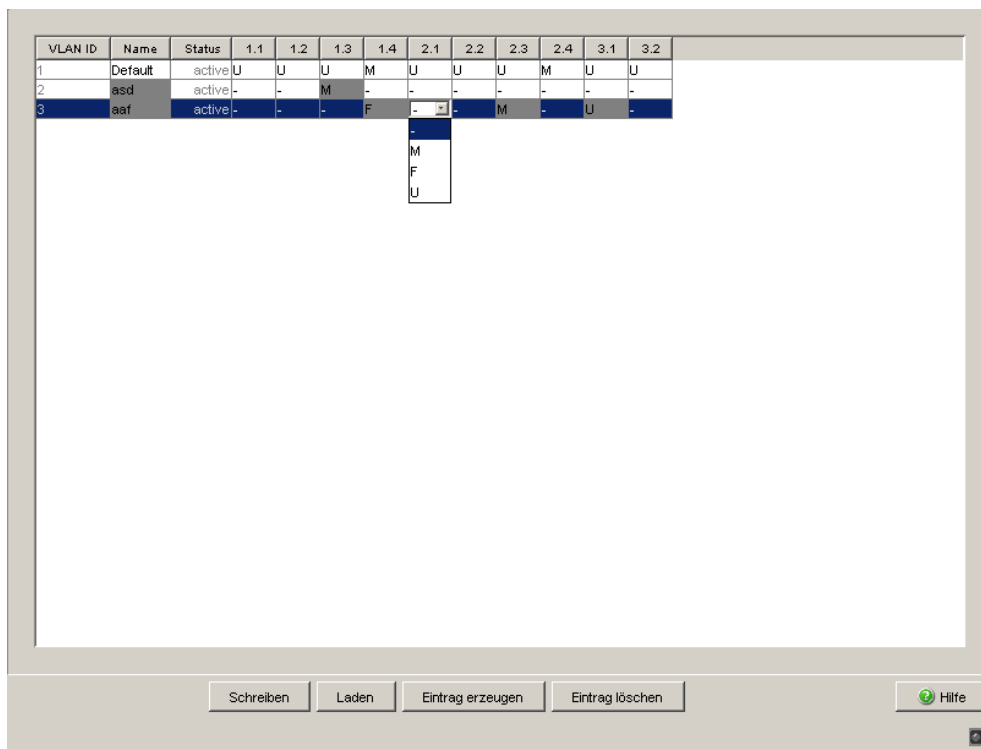


Abb. 53: Dialog VLAN Statisch

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 ∪
MRP-Ring	beliebig
Fast-HIPER-Ring	beliebig
Ring-/Netzkopplung	VLAN 1 ∪

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 <code>Grundeinstellungen:Laden/Speichern</code> 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, ungetaggtetes 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	<p>- ein: Das Gerät sendet und empfängt GVRP-Datenpakete. Das Gerät tauscht VLAN-Konfigurationsdaten mit anderen Geräten aus.</p> <p>- aus: Das Gerät sendet und empfängt keine GVRP-Datenpakete. Das Gerät tauscht keine VLAN-Konfigurationsdaten mit anderen Geräten aus.</p>	An (markiert), Aus (nicht markiert)	Aus
DVLAN-Tag-Modus	<p>- normal: Der Port beteiligt sich nicht am DVLAN-Tagging.</p> <p>- 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.</p> <p>- 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.</p>	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 237 „MRP-Ring konfigurieren“](#)) keinem VLAN zugeordnet ist, wählen Sie die Port-VLAN-ID 1.
 - Wenn die MRP-Ring-Konfiguration ([siehe auf Seite 237 „MRP-Ring konfigurieren“](#)) einem VLAN zugeordnet ist, führt das Gerät die VLAN-Konfiguration für diesen Port automatisch durch.
- ▶ **Fast HIPER-Ring (RSR20, RSR30 und MACH 1000)**
 - Wenn die Fast HIPER-Ring-Konfiguration ([siehe auf Seite 244 „Fast HIPER-Ring konfigurieren \(RSR20, RSR30, MACH 1000\)“](#)) keinem VLAN zugeordnet ist, wählen Sie die Port-VLAN-ID 1.
 - Wenn die Fast HIPER-Ring-Konfiguration ([siehe auf Seite 244 „Fast HIPER-Ring konfigurieren \(RSR20, RSR30, MACH 1000\)“](#)) 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.

Port	Port-VLAN-ID	Acceptable Frame Types	Ingress Filtering	GVRP
1.1	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.2	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.3	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
1.4	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.1	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.2	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.3	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
2.4	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.1	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>
3.2	1	admit.All	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Schreiben Laden Hilfe

Abb. 54: Dialog VLAN Port

Port	Port-VLAN-ID	Acceptable Frame Types	Ingress Filtering	GVRP	Double-VLAN-Tag-Mode
1.1	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.2	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.3	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.4	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.5	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.6	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.7	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.8	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.9	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.10	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.11	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.12	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.13	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.14	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.15	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal
1.16	1	admitAll	<input type="checkbox"/>	<input checked="" type="checkbox"/>	normal

Schreiben Laden Hilfe

Abb. 55: 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 325 „LLDP-Informationen von Nachbargeräten“](#)) als auch LLDP-MED ([siehe auf Seite 327 „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.	An, Aus	Aus

Anmerkung: Voraussetzung für das Senden der Voice-VLAN-Netz-Richtlinien ist, dass Sie auf dem Switch sowohl LLDP ([siehe auf Seite 325 „LLDP-Informationen von Nachbargeräten“](#)) als auch LLDP-MED ([siehe auf Seite 327 „LLDP-MED \(Media Endpoint Discovery\)“](#)) aktiviert haben.

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	<p>Modus der Voice-VLAN-Netz-Richtlinie, die der Switch per LLDP-MED angeschlossenen Geräten mitteilt.</p> <ul style="list-style-type: none"> ▶ 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.	0 - 4094	0

Anmerkung: Verwenden Sie eine VLAN-ID, die im Switch bereits konfiguriert ist. So ermöglichen Sie die Plug-and-Play-Inbetriebnahme eines Voice-Gerätes.

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	<ul style="list-style-type: none"> ▶ 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 <ul style="list-style-type: none"> - sich das Gerät per LLDP-MED als Voice-Gerät identifiziert hat, und - das Gerät getaggte Frames mit der Voice-VLAN-ID sendet. 	An Aus	An

Anmerkung:

- ▶ Wenn Sie für einen Port die Authentifizierung verwenden, aktivieren Sie an diesen Port die 802.1X-basierte Portsicherheit ([siehe auf Seite 104 „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.

Tab. 110: Einstellungen des Voice-VLAN-Dialogs

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

Funktion
 An Aus

Port	Voice VLAN Modus	VLAN-ID	Priorität	Authentifizierung aktiv
1.1	disabled	0	none	✓
1.2	disabled	0	none	✓
1.3	disabled	0	none	✓
1.4	disabled	0	none	✓
2.1	disabled	0	none	✓
2.2	disabled	0	none	✓
2.3	disabled	0	none	✓
2.4	disabled	0	none	✓
3.1	disabled	0	none	✓
3.2	disabled	0	none	✓

Abb. 56: 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

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 118](#)).
- ▶ 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 116](#)).

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).
- ▶ den Trust-Modus global auszuwählen (RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS). Damit bestimmen Sie, wie das Gerät empfangene Datenpakete behandelt, die eine Prioritätsinformation enthalten.
 - ▶ „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 196 „[VLAN Statisch](#)“).
Entsprechend der Traffic Class, der das IP-Paket zugeordnet wurde (siehe oben), ordnet das Gerät anhand der [Tabelle 120](#) dem IP-Paket die neue VLAN-Priorität zu.
Beispiel: ein empfangenes IP-Paket mit einem DSCP-Wert von 32 (cs4) wird der Traffic Class 2 zugeordnet (Voreinstellung). Das Paket sei auf einem Port mit Port-Priorität 2 empfangen worden. Damit wird nach [Tabelle 120](#) die VLAN-Priorität auf 4 gesetzt.

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.

Traffic Class	Neue VLAN-Priorität wenn Empfangsport gerade Port-Priorität hat	Neue VLAN-Priorität wenn Empfangsport ungerade Port-Priorität hat
0	0	1
1	2	3
2	4	5
3	6	7

Tab. 112: VLAN-Prio-Remarking

VLAN Priorität für Management-Pakete: 0

IP-DSCP Wert für Management-Pakete: 0 (be/cs0)

Anzahl Queues per Port: 4

Trust Mode: trustDot1p

Schreiben Laden Hilfe

Abb. 57: Dialog Global (RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS)

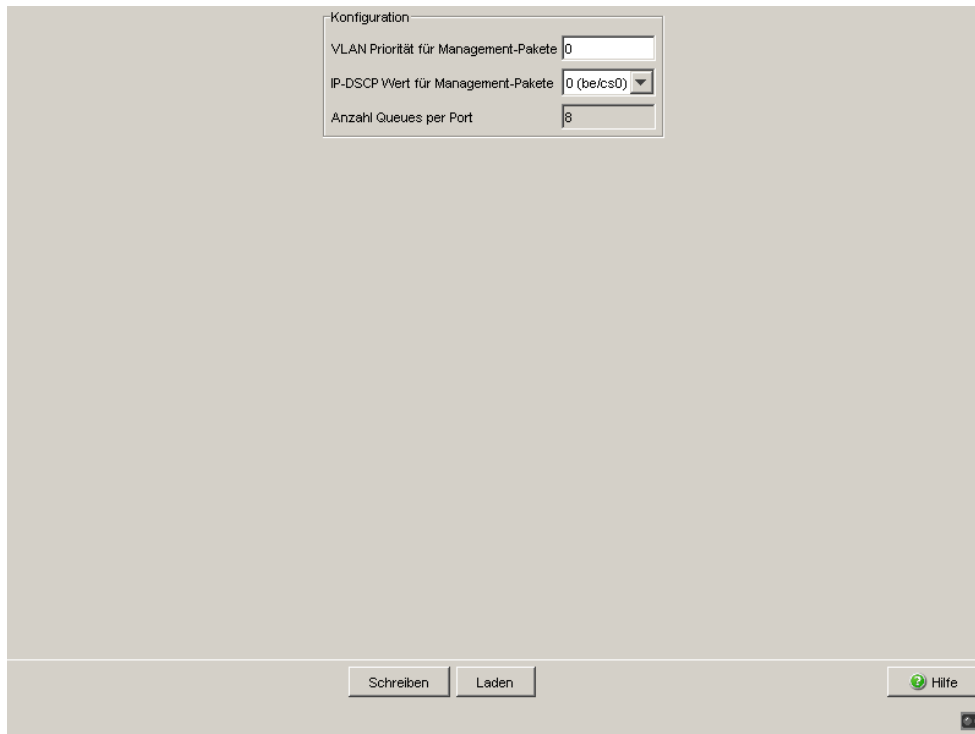


Abb. 58: Dialog Global (PowerMICE, MACH 104, MACH 1040 und MACH 4000)

■ 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. 113: 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 (PowerMICE, MACH 104, MACH 1040 und MACH 4000),
- ▶ die Untrusted Traffic Class anzeigen (PowerMICE, MACH 104, MACH 1040 und MACH 4000).

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

Tab. 114: Portkonfiguration-Tabelle für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 1000 und OCTOPUS

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.

Tab. 115: Portkonfiguration-Tabelle für PowerMICE, MACH 104, MACH 1040 und MACH 4000

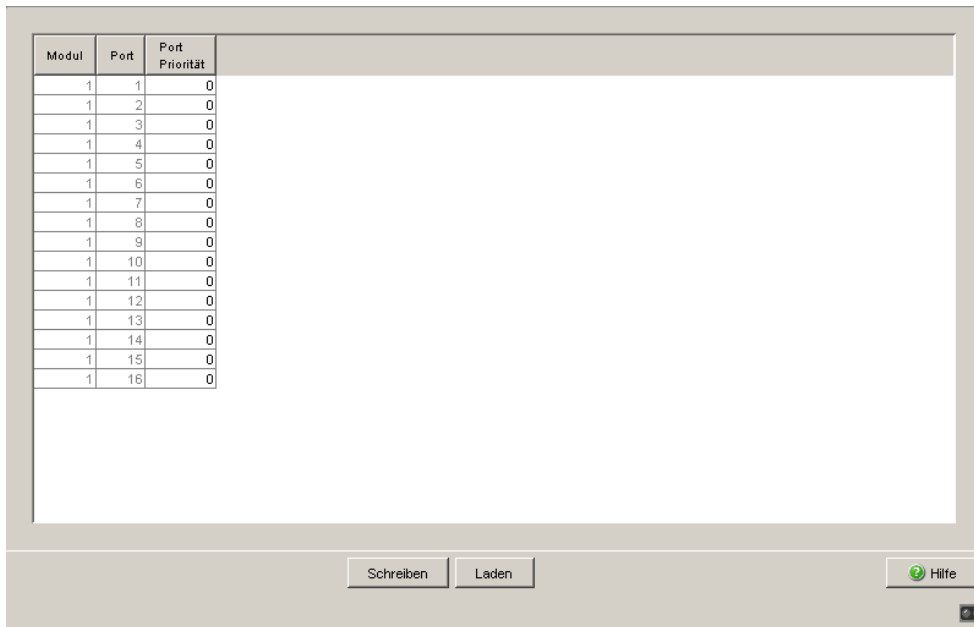


Abb. 59: Dialog Portkonfiguration für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 1000 und OCTOPUS

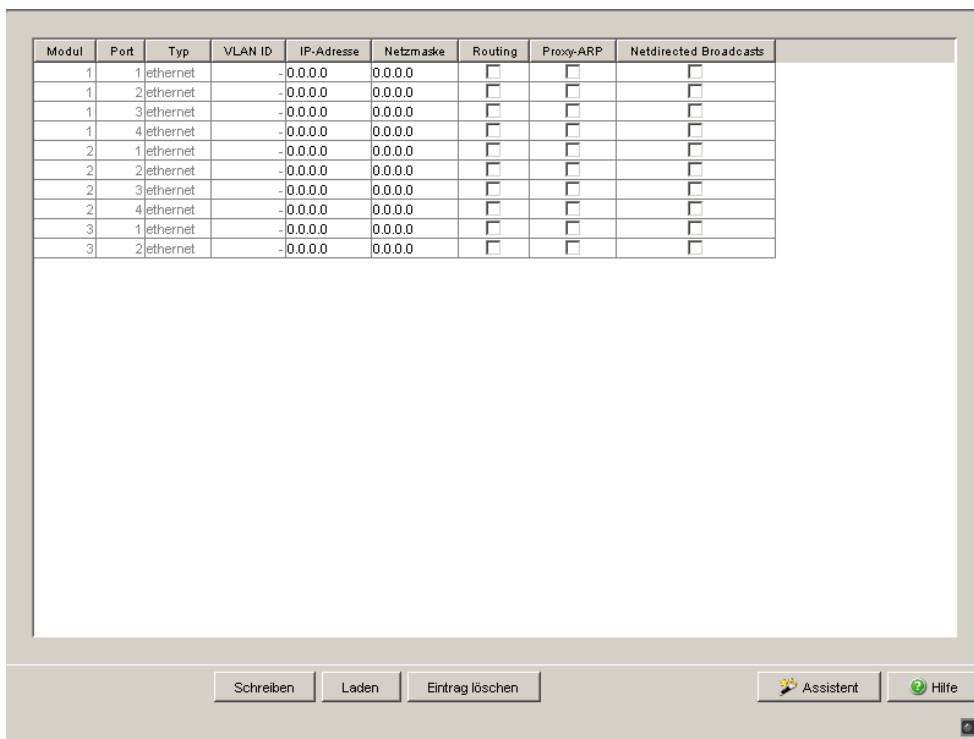


Abb. 60: Dialog Portkonfiguration für PowerMICE, MACH 104, MACH 1040 und MACH 4000

5.2.1 Port-Priorität eingeben

- RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS:
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 116](#)).
Voraussetzung:
Einstellung im Dialog `Global: Trust Modus: untrusted` (siehe auf [Seite 210 „Global“](#)) oder
Einstellung im Dialog `Global: Trust Modus: trustDot1p` (siehe auf [Seite 210 „Global“](#)) und die Datenpakete enthalten kein VLAN-Tag oder
Einstellung im Dialog `Global: Trust Modus: trustIpDscp` (siehe auf [Seite 210 „Global“](#)) und die Datenpakete sind keine IP-Pakete.
- Power MICE, MACH 104, MACH 1040 und MACH 4000:
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 116](#)).
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 für RS20/RS30/RS4 0, MS20/MS30, RSR20/RSR30, MACH 100 MACH 1000, OCTOPUS (Voreinstellung)	Traffic Class für MACH 4000, MACH 104, MACH 1040 und PowerMICE (Voreinstellung)	IEEE 802.1D Verkehrstyp
0	1	2	Best Effort (default)
1	0	0	Background
2	0	1	Standard
3	1	3	Excellent Effort (business critical)
4	2	4	Controlled load (streaming multimedia)
5	2	5	Video, < 100 ms of latency and jitter
6	3	6	Voice; < 10 ms of latency and jitter
7	3	7	Network Control reserved traffic

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

5.2.2 Trust-Modus wählen (PowerMICE, MACH 104, MACH 1040 und MACH 4000)

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.
 - ▶ Entsprechend der Traffic Class, der das IP-Paket zugeordnet wurde (siehe oben), ordnet das Gerät anhand der [Tabelle 120](#) 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 120](#) die VLAN-Priorität 2.

5.2.3 Untrusted Traffic Class anzeigen (PowerMICE, MACH 104, MACH 1040 und MACH 4000)

„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 216 „Port-Priorität eingeben“](#)), dann ändert sich auch die Untrusted Traffic Class ([siehe Tabelle 120](#)).

■ 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 <code>Grundeinstellungen:Laden/Speichern</code> 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

5.3 802.1D/p-Mapping

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

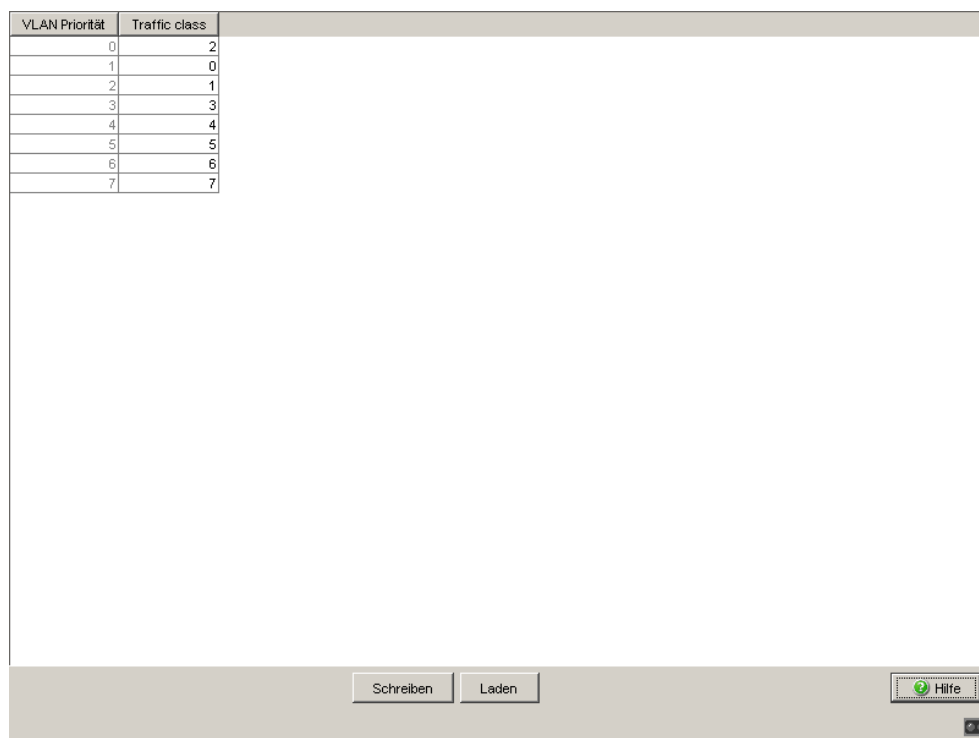


Abb. 61: Dialog 802.1D/p-Mapping

- Tragen Sie für jede VLAN-Priorität im Feld Traffic Class den gewünschten Wert zwischen
 - ▶ 0 und 3 bei RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS
 - ▶ 0 und 7 bei MACH 4000, MACH 104, MACH 1040 und PowerMICE ein.

VLAN-Priorität	Traffic Class für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS (Voreinstellung)	Traffic Class für MACH 4000, MACH 104, MACH 1040 und PowerMICE (Voreinstellung)	IEEE 802.1D Verkehrstyp
0	1	2	Best Effort (default)
1	0	0	Background
2	0	1	Standard
3	1	3	Excellent Effort (business critical)
4	2	4	Controlled Load (streaming multimedia)
5	2	5	Video, < 100 ms of latency and jitter
6	3	6	Voice; < 10 ms of latency and jitter
7	3	7	Network Control reserved traffic

Tab. 118: Zuordnung der VLAN-Priorität zu den Traffic Classes

Anmerkung: Netzprotokolle und Redundanzmechanismen nutzen die höchste Traffic Class 3 (RS20/30/40, MS20/30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS) bzw. 7 (PowerMICE, MACH 104, MACH 1040, MACH 4000). Wählen Sie deshalb andere Traffic Classes für Anwendungsdaten.

■ Schaltflächen

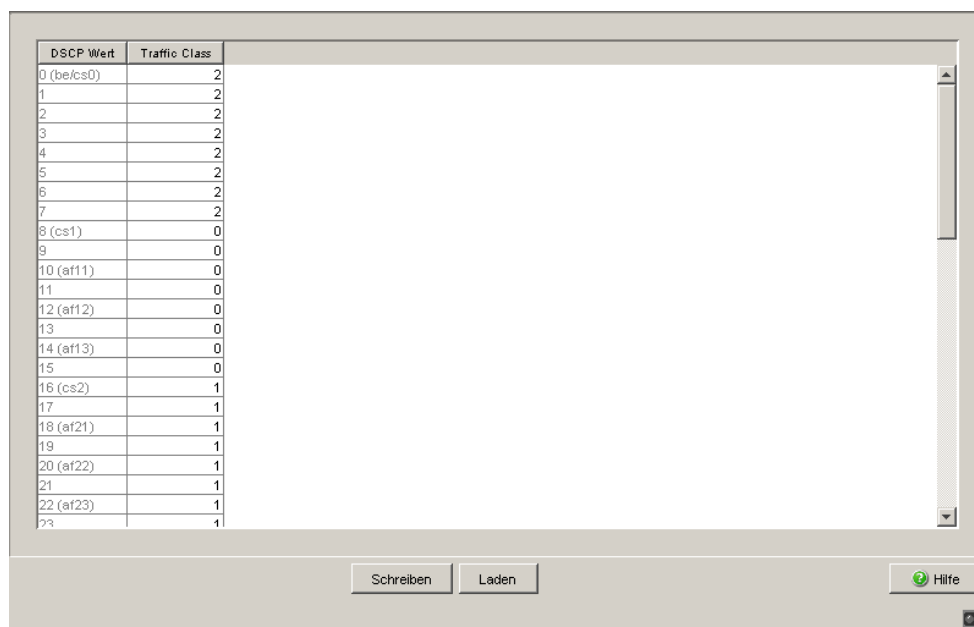
Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen anschließend permanent zu speichern, öffnen Sie den Dialog Grundeinstellungen:Laden/Speichern und klicken auf „Speichern“.
Laden	Aktualisiert die Felder mit den Werten, die im flüchtigen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

Tab. 119: 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 3 bei RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS
 - ▶ 0 und 7 bei MACH 4000, MACH 104, MACH 1040 und PowerMICE ein.



DSCP Wert	Traffic Class
0 (be/cs0)	2
1	2
2	2
3	2
4	2
5	2
6	2
7	2
8 (cs1)	0
9	0
10 (af11)	0
11	0
12 (af12)	0
13	0
14 (af13)	0
15	0
16 (cs2)	1
17	1
18 (af21)	1
19	1
20 (af22)	1
21	1
22 (af23)	1
23	1

Abb. 62: 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 für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS (Voreinstellung)	Traffic Class für MACH 4000 und PowerMICE (Voreinstellung)
0	Best Effort /CS0	1	2
1-7		1	2
8	CS1	0	0
9,11,13,15		0	0
10,12,14	AF11,AF12,AF13	0	0
16	CS2	0	1
17,19,21,23		0	1
18,20,22	AF21,AF22,AF23	0	1
24	CS3	1	3
25,27,29,31		1	3
26,28,30	AF31,AF32,AF33	1	3
32	CS4	2	4
33,35,37,39		2	4
34,36,38	AF41,AF42,AF43	2	4
40	CS5	2	5
41,42,43,44,45,47		2	5
46	EF	2	5
48	CS6	3	6
49-55		3	6

Tab. 120: Abbildung der DSCP-Werte auf die Traffic Classes

DSCP-Wert	DSCP-Name	Traffic Class für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000, OCTOPUS (Voreinstellung)	Traffic Class für MACH 4000 und PowerMICE (Voreinstellung)
56	CS7	3	7
57-63		3	7

Tab. 120: 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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 121: Schaltflächen

6 Redundanz

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

- ▶ Link-Aggregation
- ▶ Ring-Redundanz
- ▶ Sub-Ring
- ▶ Ring-/Netzkopplung
- ▶ Spanning Tree

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

6.1 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 zusammenfassen. 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.

Anmerkung: Schließen Sie eine Kombination von Link-Aggregation mit folgenden Redundanzverfahren aus:

- ▶ Netz-/Ringkopplung
- ▶ MRP-Ring
- ▶ Fast HIPER-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 <i>Statische Link-Aggregation zulassen</i> , 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 <i>on</i> , wenn Sie die Link-Aggregation in einen Spanning-Tree eingebunden haben, <i>off</i> , wenn nicht.
Typ	<ul style="list-style-type: none"> - <i>manuell</i> Das Partnergerät unterstützt kein LACP und Sie haben „Statische Link-Aggregation zulassen“ angewählt. - <i>dynamic</i> Beide Geräte unterstützen LACP und Sie haben „Statische Link-Aggregation zulassen“ nicht angewählt. <p>Hinweis: Bestehen die Mehrfachverbindungen zwischen Geräten, die alle LACP unterstützen, zeigt das Gerät <i>dynamic</i> an auch wenn „Statische Link-Aggregation zulassen“ angewählt wurde. In diesem Fall schalten die Geräte automatisch auf <i>dynamic</i> um.</p>

Tab. 122: Link-Aggregation

Statische Link-Aggregation zulassen

Trunk-Port	Quellports	Name	Aktiv	Link Trap	STP-Modus	Typ
8.1		<new>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	on	dynamic
8.2		<new>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	on	dynamic
8.3		<new>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	on	dynamic

Schreiben Laden Erzeugen Löschen Quellports hinzufügen Quellports entfernen Hilfe

Abb. 63: Link-Aggregation einstellen

Anmerkung: Für PowerMICE und MACH 4000

Zur Erhöhung der Verfügbarkeit besonders wichtiger Verbindungen können Sie HIPER-Ring ([siehe auf Seite 230 „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 <i>Grundeinstellungen:Laden/Speichern</i> , 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. 123: Schaltflächen

6.2 Ring-Redundanz

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

Beim Ausfall einer Teilstrecke wandelt sich die Ringstruktur eines

- ▶ HIPER-(**HIGH PERFORMANCE REDUNDANCY**) Rings mit bis zu 50 Geräten im typischen Fall innerhalb von 80 ms (einstellbar: Standard/Beschleunigt) wieder in eine Linienstruktur zurück.
- ▶ MRP (**Media Redundancy Protocol**)-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.
- ▶ Fast HIPER-Rings bei bis zu 5 Geräten im typischen Fall innerhalb von 5 ms (maximal 10 ms) wieder in eine Linienstruktur zurück. Beim Einsatz einer größeren Anzahl von Geräten erhöht sich die Rekonfigurationszeit.

Mit Hilfe der **Ring-Manager**- (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-Protokoll 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 240 „Erweiterte Ringkonfiguration/-diagnose \(ARC\)“](#)).

Parameter	Bedeutung
Version	Wählen Sie, welche Ring-Redundanz-Version Sie einsetzen: HIPER-Ring MRP FAST HIPER-Ring (RSR20/30, MACH 1000)
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. 124: Ring-Redundanz Basiskonfiguration

6.2.1 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. 125: 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“: <i>active</i> : Sie haben diesen Port eingeschaltet und er hat einen Link. <i>inactive</i> : Sie haben diesen Port ausgeschaltet oder er hat keinen Link.
Status des Ringmanagers	Statusinformation, keine Eingabe möglich: <i>Aktiv (redundante Strecke)</i> : die redundante Strecke wurde geschlossen, weil eine Datenleitung oder Netzkomponente innerhalb des Rings ausgefallen ist. <i>Inaktiv</i> : 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 verlorengegangen betrachtet. <ul style="list-style-type: none"> ▶ <i>Standard</i>: Testpakete-Timeout 480 ms ▶ <i>Beschleunigt</i>: Testpakete-Timeout 280 ms <p>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 Verbindungsunterbrechungen kann so deutlich beschleunigt werden.</p>
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. 126: HIPER-Ring-Konfiguration

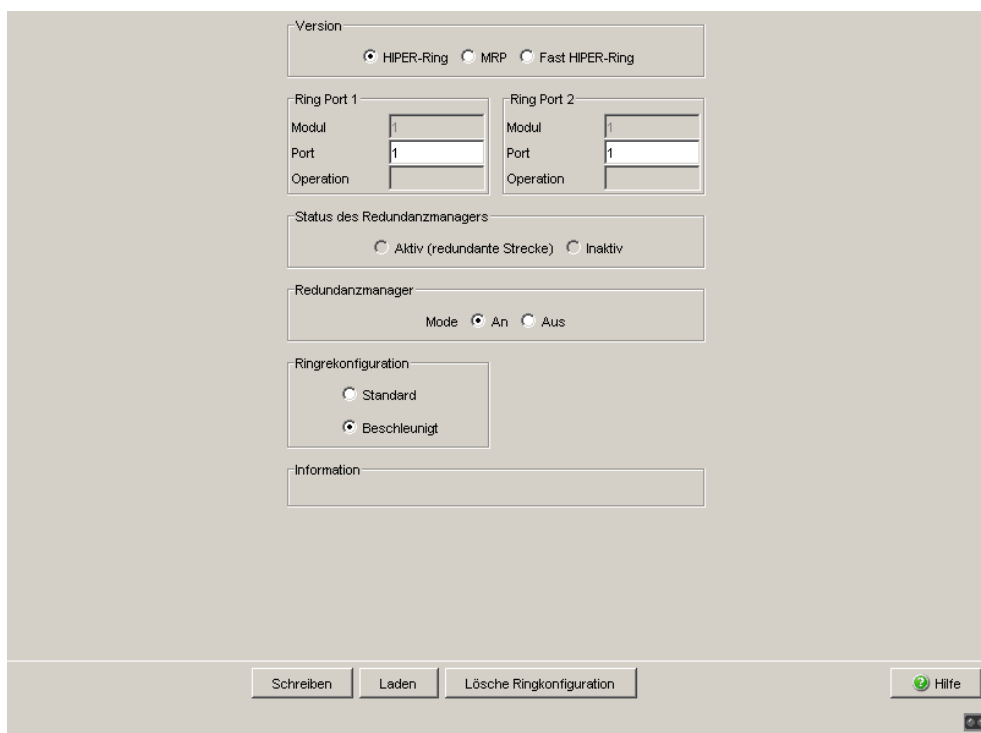


Abb. 64: Hiper-Ring-Version wählen, Ringports eingeben, Ring-Manager ein-/ausschalten und Ringrekonfiguration wählen (RSR20, RSR30, MACH 1000)

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.

6.2.2 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. 127: 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“: <code>forwarding</code> : Sie haben diesen Port eingeschaltet und er hat einen Link. <code>blocked</code> : dieser Port ist blockiert und hat einen Link <code>disabled</code> : Sie haben diesen Port ausgeschaltet <code>not-connected</code> : 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: ▶ <code>VLAN-ID 0</code> , 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. ▶ <code>VLAN-ID > 0</code> , 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. 128: MRP-Ring Konfiguration

The screenshot shows a configuration window for a ring network. The 'Version' section has three radio buttons: 'HIPER-Ring', 'MRP' (selected), and 'Fast HIPER-Ring'. Below are two columns for 'Ring Port 1' and 'Ring Port 2'. 'Ring Port 1' has 'Modul' set to '1' and 'Port' set to '1'. 'Ring Port 2' has 'Modul' set to '1' and 'Port' set to '2'. The 'Konfiguration des Redundanzmanager' section has an unchecked checkbox for 'Advanced Mode'. The 'Redundanzmanager' section has 'Mode' set to 'An'. The 'Funktion' section has 'An' selected. The 'Ringrekonfiguration' section has '200ms' selected. The 'VLAN' section has 'VLAN ID' set to an empty text box. The 'Information' section is empty. At the bottom are buttons for 'Schreiben', 'Laden', 'Lösche Ringkonfiguration', and 'Hilfe'.

Abb. 65: MRP-Ring-Version wählen, Ringports eingeben und Ring-Manager ein-/ausschalten.
(RSR20, RSR30, MACH 1000)

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 nicht-flüchtig 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 263 „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 277 „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.

The screenshot displays the 'Ring-Redundanz' configuration dialog. At the top, the 'Version' section has radio buttons for 'HIPER-Ring' and 'MRP', with 'MRP' selected. Below this, 'Ring Port 1' and 'Ring Port 2' are configured with ports 1.1 and 1.2 respectively. The 'Konfiguration des Ringmanager' section includes an unchecked 'Advanced-Mode' checkbox. The 'Ringmanager' section has a 'Mode' set to 'Aus'. The 'Funktion' section has 'An' selected, and the 'Ringrekonfiguration' section has '500ms' selected. The 'VLAN' section has an empty 'VLAN ID' field. The 'Information' section is empty. The 'Erweiterte Ringkonfiguration/-diagnose' section, highlighted with a red box, contains radio buttons for 'Aus', 'Lesen', and 'Lesen /Schreiben', with 'Lesen /Schreiben' selected. At the bottom, there are buttons for 'Schreiben', 'Laden', 'Lösche Ringkonfiguration', and 'Hilfe'.

Abb. 66: 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.

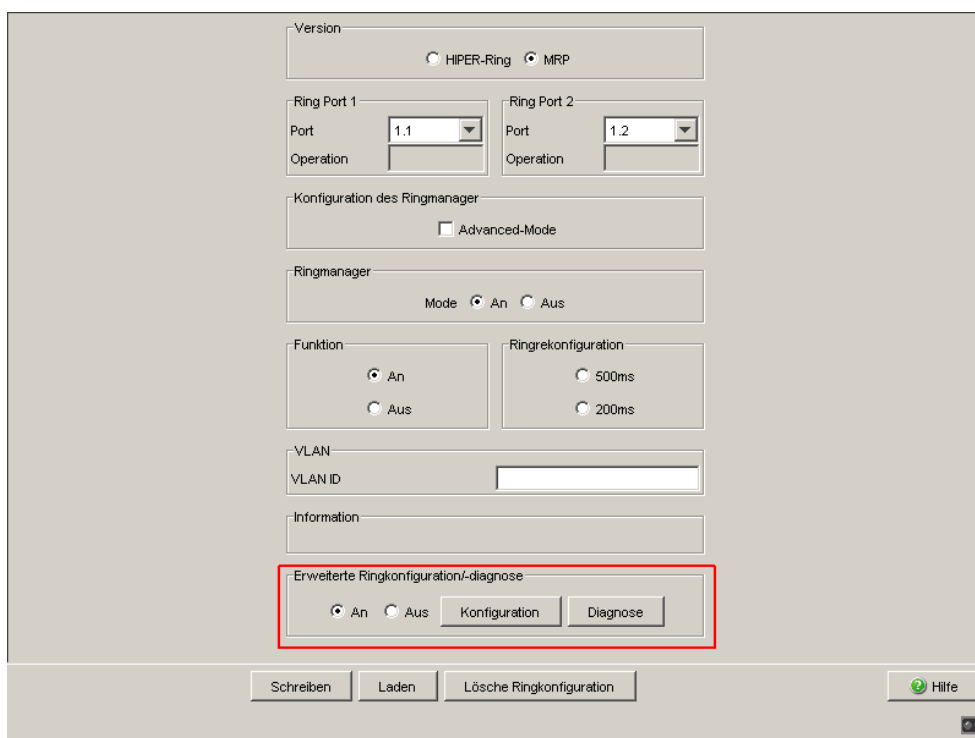


Abb. 67: Dialog Ring-Redundanz, Erweiterte Ringkonfiguration/-diagnose eines MRP-Managers

6.2.3 Fast HIPER-Ring konfigurieren (RSR20, RSR30, MACH 1000)

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. 129: Port-Einstellungen für Ring-Ports

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

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“: <i>forwarding</i> : Sie haben diesen Port eingeschaltet und er hat einen Link. <i>blocked</i> : dieser Port ist blockiert und hat einen Link <i>disabled</i> : Sie haben diesen Port ausgeschaltet <i>not-connected</i> : 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	<i>Ringumlaufzeit</i> : Vom Ring-Manager gemessene Ringumlaufzeit der Prüfpakete in μ s. Die Anzeige beginnt mit 100 μ s, in Schritten von 100 μ s. Werte um 1000 μ s 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: <i>VLAN-ID</i> 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. <i>VLAN-ID</i> >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. 130: Fast HIPER-Ring Konfiguration

Abb. 68: 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. 131: Schaltflächen

6.3 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 237 „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.

6.3.1 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)	-
Funktion an/aus	Schalten Sie den Sub-Ring erst nach vollständiger Konfiguration an. Schließen Sie dann den Sub-Ring.	An Aus	An
Konfigurationsstatus	Ein Icon zeigt den aktuellen Status des Sub-Rings an.		

Tab. 132: 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 <code>redundant Manager</code>) 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 <code>redundantManager</code> . <code>singleManager</code> 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 redundantMa- nager singleMa- nager	manager
SRM-Status	Istzustand: Zeigt an, ob dieser SRM die redundante Verbindung verwaltet (Modus <code>redundant Manager</code>) 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 <code>redundantManager</code> . <code>SingleManager</code> 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 redundantMa- nager singleMa- nager	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. 132: 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 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
Protokoll		standardMRP	standardMRP

Tab. 132: Sub-Ring Basiskonfiguration

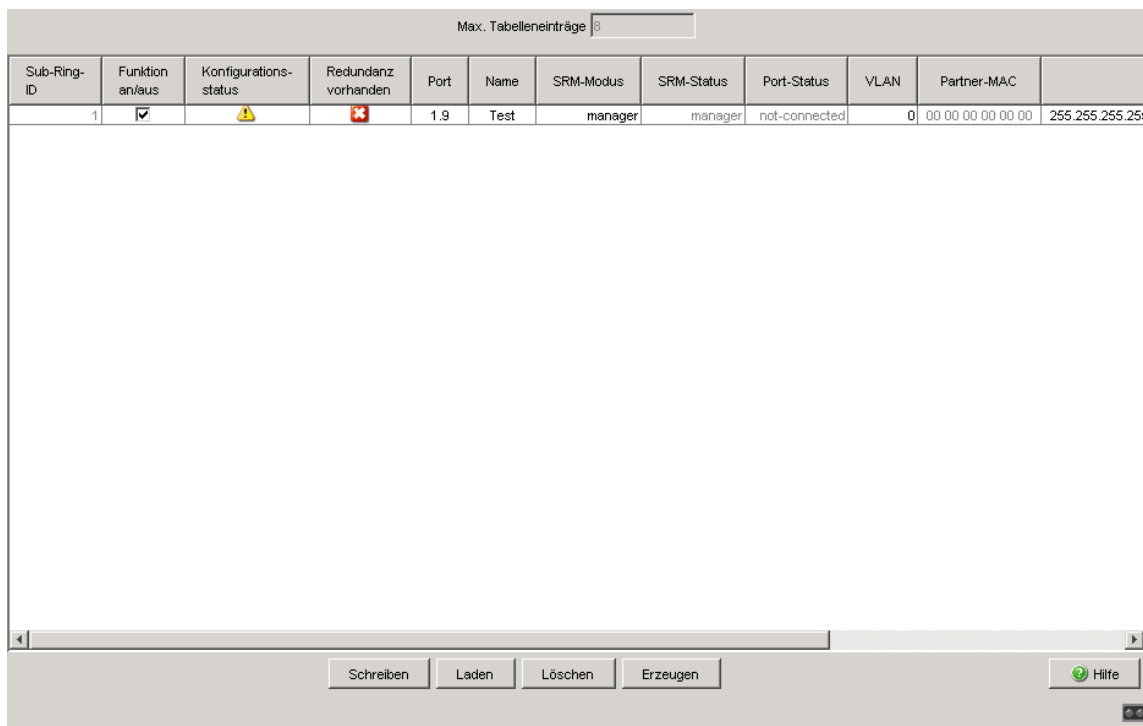


Abb. 69: Sub-Ring Basiskonfiguration

6.3.2 Sub-Ring – Neuer Eintrag

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
.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 <code>redundant Manager</code>) 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 <code>redundant Manager</code> . <code>singleManager</code> 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.	<code>manager</code> <code>redundantManager</code> <code>singleManager</code>	<code>manager</code>
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. 133: Sub-Ring - Neuer Eintrag

Anmerkung: Für einen Sub-Ring im `singleManager`-Modus legen Sie 2 Einträge mit unterschiedlichen Sub-Ring-IDs an.

Neuer Eintrag

Sub-Ring-ID: 1

Port: 1.9

Name: Test

SRM-Modus: manager

VLAN: 0

MRP-Domäne: 255.255.255.255.255.255.255

Schreiben Schreiben und zurück Zurück Hilfe

Abb. 70: 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. 134: Schaltflächen

Schaltfläche	Bedeutung
Zurück	Zeigt die vorherige Seite wieder an. Änderungen gehen dabei verloren.
Hilfe	Öffnet die Online-Hilfe.

Tab. 134: Schaltflächen (Forts.)

6.4 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.

6.4.1 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
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. 135: 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 <code>Redundanz:Ring-/Netzkopplung</code> 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 <code>Redundanz:Ring-/Netzkopplung</code>

Tab. 136: Einstellen des STAND-BY-Schalters

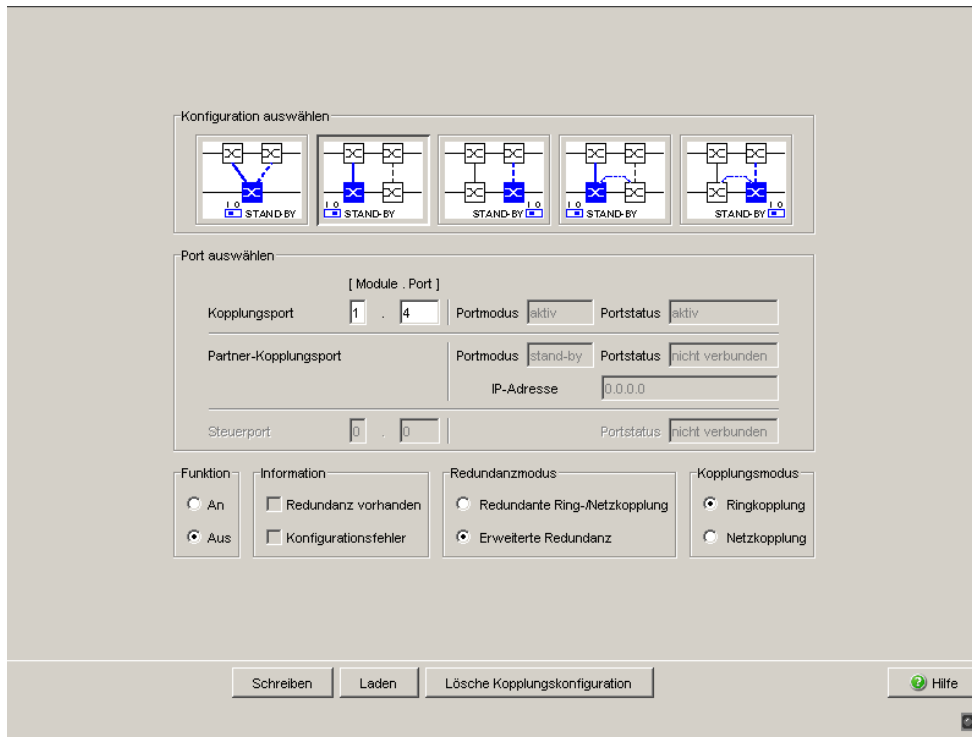


Abb. 71: Software-Konfiguration des STAND-BY-Schalters

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
Kopplungsport	Dies ist der Port, an dem Sie eine Redundanzverbindung abgeschlossen 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	- <code>aktiv</code> : Sie haben den Port eingeschaltet. - <code>stand-by</code> : Der Port befindet sich im Stand-by-Modus.
Portstatus	- <code>aktiv</code> : Sie haben den Port eingeschaltet. - <code>stand-by</code> : Der Port befindet sich im Stand-by-Modus. - <code>nicht verbunden</code> : 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.
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 Fast HIPER-Ring) oder von Netzsegmenten ist.

Tab. 137: 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. 138: 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 \mathbb{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 ungetaggt 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. 139: Schaltflächen

6.5 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.

6.5.1 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. 140: 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 Konfigurationsparameter 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 <code>Bridge-ID</code> . 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 <code>Bridge-ID</code> unter allen Geräten im Netz zuweisen. Geben Sie den Wert als Vielfaches von 4.096 ein.	$0 \leq n \cdot 4.096 \leq 61.440$	32.768
Hello Time	Stellt die Hello-Time ein. Die lokale <code>Hello Time</code> gibt die Zeit zwischen dem Senden zweier Konfigurationmeldungen (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. 141: 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 <code>disabled</code> , <code>discarding</code> , <code>learning</code> , <code>forwarding</code> 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. 141: 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“ <code>true</code>). Empfängt ein solcher Port eine beliebige STP-BPDU, setzt das Gerät den Port-Zustand „BPDU Guard Effect“ auf <code>true</code> und den Vermittlungszustand des Ports in <code>discarding</code> (siehe Tabelle 152). 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. 141: 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:

$$\text{Forward Delay} \geq (\text{Max Age}/2) + 1$$

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	Lieferzustand
Spalte „Root“	Informationen des Geräts, das aktuell Root-Bridge ist		
Bridge-ID	Die <code>Bridge-ID</code> der aktuellen Root-Bridge. Das Format ist ppppp / mm mm mm mm mm mm, mit: ppppp: Priorität (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).		
Priorität	Die <code>Priorität</code> der aktuellen Root-Bridge.	$0 \leq n \cdot 4.096 \leq 61.440$	32.768
Hello Time	Die <code>Hello Time</code> der aktuellen Root-Bridge.	1 - 2	2
Forward Delay	Das <code>Forward Delay</code> der aktuellen Root-Bridge.	4 - 30 s	15 s
Max Age	Der Parameter <code>Max Age</code> der aktuellen Root-Bridge.	6 - 40 s	20 s

Tab. 142: 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 <code>Forwarding</code> gesetzt hat.	
Zeit seit letzter Änderung	Zeit seit der letzten Topologie-Änderung.	

Tab. 143: 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. 144: Globale Spanning-Tree-Einstellungen, Rahmen Information

The screenshot shows a configuration window for Spanning Tree. At the top, there are two sections: 'Funktion' with radio buttons for 'An' (selected) and 'Aus', and 'Protokoll-Version' with a dropdown menu set to 'MSTP'. Below this is a large box titled 'Protokoll-Konfiguration / Information' containing several fields:

- Bridge**: Bridge-ID (32768 / 00 80 63 51 7a 80), Priorität (32768), Hello Time [s] (2), Forward Delay [s] (15), Max Age (20), Tx Hold Count (10).
- Root**: Root (20480 / 00 80 63 0f 1d b0), Root (20480), Root (6).
- Topologie**: Bridge ist Root (checkbox), Root-Port (1.3), Root-Pfadkosten (240000), Anzahl Topologieänderungen (1), Zeit seit letzter Änderung (0 Tag(e), 4:11:08).

At the bottom of the dialog, there are three buttons: 'Schreiben', 'Laden', and 'Hilfe'.

Abb. 72: 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. 145: Schaltflächen

6.5.2 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. 146: 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 <code>Bridge-ID</code> 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 <code>Bridge-ID</code> der aktuellen Root-Bridge 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. 147: *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-Pfadkosten	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. 147: 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. 73: 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. 148: 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. 148: Multiple Spanning-Tree-Einstellungen, MST-Instanz, VLANs

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
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.	$0 \leq n \cdot 4.096 \leq 61.440$	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, 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. 149: Multiple Spanning-Tree-Einstellungen, MST-Instanz, Parameter

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Root-ID	Die Bridge-ID der aktuellen Root-Bridge des ausgewählten MST-Bereichs. Das Format ist ppppp / 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. 149: Multiple Spanning-Tree-Einstellungen, MST-Instanz, Parameter

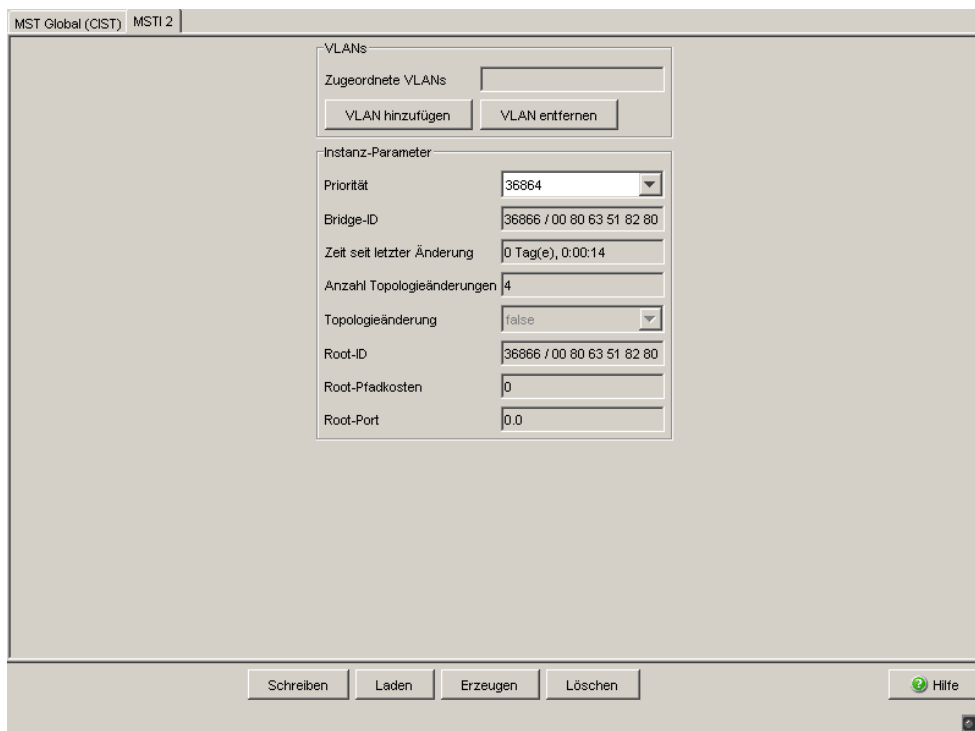


Abb. 74: Dialog Multiple Spanning Tree, MSTI <ID>

■ 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. 150: Schaltflächen

6.5.3 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 abzufragen 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.	An, Aus	An

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.

Tab. 151: Port-bezogene STP-Einstellungen und -Anzeigen, CIST

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
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.	$16 \leq n \cdot 16 \leq 240$	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. 151: Port-bezogene STP-Einstellungen und -Anzeigen, CIST

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Admin-Edge-Port	<p>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-Status 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. <code>forwarding</code>, <code>discarding</code>, <code>learning</code>.</p> <p>Deaktivieren Sie die Einstellung, wenn der Port an eine Bridge angeschlossen ist. Der Port durchläuft nach Aufbau eines Links dann zuerst die STP-Status, bevor er ggf. in den Zustand <code>forwarding</code> geht. Diese Einstellung gilt für alle MSTIs.</p>	<p>aktiv (Kästchen markiert), inaktiv (Kästchen leer)</p>	inaktiv
Auto-Edge-Port	<p>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 $1,5 \cdot \text{Hello Time}$ (in der Voreinstellung 3 s) in den Zustand <code>forwarding</code>.</p> <p>Ist Auto-Edge-Port deaktiviert, wartet das Gerät statt dessen <code>Max Age</code> (in der Voreinstellung 20 s). Diese Einstellung gilt für alle MSTIs.</p>	<p>aktiv (Kästchen markiert), inaktiv (Kästchen leer)</p>	aktiv

Tab. 151: Port-bezogene STP-Einstellungen und -Anzeigen, CIST

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Oper-Edge-Port	Das Gerät setzt den Zustand „Oper-Edge-Port“ (Operational: in Betrieb) auf <code>true</code> , wenn es keine STP-BPDUs empfangen hat, also ein Endgerät angeschlossen ist. Es setzt den Zustand auf <code>false</code> , wenn es eine STP-BPDUs empfangen hat, also eine Bridge angeschlossen ist. Dieser Zustand gilt für alle MSTIs.	<code>true, false</code>	-
Ist Punkt-zu-Punkt	Das Gerät setzt den Zustand „Oper Punkt-zu-Punkt“ (Operational: in Betrieb) auf <code>true</code> , wenn dieser Port eine Vollduplex-Verbindung zu einem STP-Gerät hat. Ansonsten setzt es den Zustand auf <code>false</code> (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.	<code>true, false</code> Das Gerät bestimmt diesen Zustand aus dem Duplex-Modus: FDX: <code>true</code> HDX: <code>false</code>	

Tab. 151: 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.

Port	Stp aktiv	Port Status	Port Funktion	Port Pfadkosten	Port Priorität	Received Bridge ID	Received Port ID	Received Path Cost	Oper Edge Port	Admin Edge Port	Auto Edge Port	Ist Punkt zu Punkt
1.1	<input checked="" type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 51 82 80	00 00	0	<input type="checkbox"/>	<input type="checkbox"/>	true	false
1.2	<input checked="" type="checkbox"/>	forwarding	designated	20000	128	32768 / 00 80 63 51 7a 80	80 03	220000	<input type="checkbox"/>	<input type="checkbox"/>	true	true
1.3	<input checked="" type="checkbox"/>	forwarding	designated	20000	128	32768 / 00 80 63 51 74 00	80 04	220000	<input type="checkbox"/>	<input type="checkbox"/>	true	true
1.4	<input checked="" type="checkbox"/>	forwarding	root	20000	128	32768 / 00 80 63 2f fb b8	80 01	200000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	true	true
2.1	<input checked="" type="checkbox"/>	forwarding	designated	200000	128	32768 / 00 80 63 51 82 80	80 05	220000	<input type="checkbox"/>	<input type="checkbox"/>	true	true
2.2	<input checked="" type="checkbox"/>	forwarding	designated	200000	128	32768 / 00 80 63 70 e8 70	80 0b	220000	<input type="checkbox"/>	<input type="checkbox"/>	true	true
2.3	<input checked="" type="checkbox"/>	forwarding	designated	200000	128	32768 / 00 80 63 51 82 80	00 00	220000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	true	true
2.4	<input checked="" type="checkbox"/>	forwarding	designated	200000	128	32768 / 00 80 63 51 82 80	00 00	220000	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	true	true
3.1	<input checked="" type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 51 82 80	00 00	0	<input type="checkbox"/>	<input type="checkbox"/>	true	true
3.2	<input checked="" type="checkbox"/>	disabled	disabled	0	128	32768 / 00 80 63 51 82 80	00 00	0	<input type="checkbox"/>	<input type="checkbox"/>	true	true

Abb. 75: Dialog Multiple Spanning Tree, Port, Karteikartenreiter CIST

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Karteikartenreiter „Guards“	Schutzeinstellungen für die Ports.		
Modul.Port	Portbezeichnung durch Modul- und Portnummer des Gerätes, z.B. 2.1 für den Port eins des zweiten Moduls.		

Tab. 152: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Root-Guard	<p>Die Einstellung „Root-Guard“ ist ausschließlich für Ports in der STP-Rolle <code>designated</code> relevant.</p> <p>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 <code>discarding</code>, statt dem Port die STP-Port-Rolle <code>root</code> zuzuweisen.</p> <p>So hilft das Gerät, Ihr Netz vor Angriffen mit STP-BPDUs, die die Topologie zu verändern versuchen, und vor Fehlkonfigurationen zu schützen.</p> <p>Bleiben STP-BPDUs mit einer besseren Pfadinformation zur Root aus, dann setzt das Gerät den Vermittlungszustand des Ports wieder entsprechend der Port-Rolle.</p>	<p><code>aktiv</code> (Kästchen markiert),</p> <p><code>inaktiv</code> (Kästchen leer)</p>	<code>inaktiv</code>

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.

Tab. 152: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
TCN-Guard	<p>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.</p> <p>So schützt das Gerät Ihr Netz vor Angriffen mit STP-BPDUs, die die Topologie zu verändern versuchen.</p> <p>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.</p>	<p>aktiv (Kästchen markiert), inaktiv (Kästchen leer)</p>	inaktiv

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.

Tab. 152: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Loop-Guard	<p>Die Einstellung „Loop-Guard“ ist ausschließlich sinnvoll für Ports in der STP-Rolle <code>alternate</code>, <code>backup</code> oder <code>root</code>. Ist die Einstellung „Loop-Guard“ aktiv und empfängt der Port eine Zeitlang keine STP-BPDUs mehr, setzt das Gerät den Port in den Zustand <code>discarding</code> (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.</p> <p>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.</p> <p>Empfängt der Port wieder BPDUs, setzt das Gerät den Loop-inkonsistenten Zustand des Ports zurück auf <code>false</code> und den Vermittlungszustand des Ports entsprechend der Port-Rolle.</p> <p>Ist die Einstellung „Loop-Guard“ inaktiv, setzt das Gerät den Port dagegen nach dem Ausbleiben von STP-BPDUs in den Zustand <code>forwarding</code>.</p> <p>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.</p>	aktiv (Kästchen markiert), inaktiv (Kästchen leer)	inaktiv
Loop-Zustand (read-only)	<p>Anzeige des Status des Loop-inkonsistenten Zustands.</p> <p>Das Gerät setzt den Loop-inkonsistenten Zustand eines Ports auf <code>true</code>, 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 <code>discarding</code>, und hilft so, einen möglichen Loop zu verhindern.</p> <p>Empfängt der Port wieder STP-BPDUs, setzt das Gerät den Loop-inkonsistenten Zustand zurück auf <code>false</code>.</p>	<code>true</code> , <code>false</code>	-

Tab. 152: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Übergänge in Loop-Zustand (read-only)	Zählt, wie oft das Gerät den Port in den Loop-inkonsistenten Zustand (Spalte „Loop-Zustand“ <code>true</code>) 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“ <code>true</code>) 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“ <code>true</code>) und lediglich dann, wenn die globale Funktion „BPDU Guard“ aktiv ist (siehe Tabelle 141). Empfängt ein solcher Port eine beliebige STP-BPDU, setzt das Gerät den Port-Zustand „BPDU Guard Effect“ auf <code>true</code> und seinen Vermittlungszustand in <code>discarding</code> . 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.	<code>true</code> , <code>false</code>	-

Tab. 152: Port-bezogene STP-Einstellungen und -Anzeigen, Guards

CIST		Guards		MSTI 2					
Port	Root Guard	TCN Guard	Loop Guard	Loop Status	Übergänge in Loop Zustand	Übergänge aus Loop Zustand	BPDU Guard Effect		
1.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		
1.2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		
1.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		
1.4	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	false	0	0	disable		
2.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		
2.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		
2.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		
2.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		
3.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		
3.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	false	0	0	disable		

Abb. 76: Dialog Multiple Spanning Tree, Port, Karteikartenreiter Guards

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Karteikartenreiter „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. 153: 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-ID.	$16 \leq n \cdot 16 \leq 240$	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 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. 153: 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.

Port	Port Status	Port Rolle	Port Pfadkosten	Port Priorität	Empfangene Bridge-ID	Empfangene Port-ID	Empfangene Pfadkosten
1.1	disabled	disabled	0	128	36866 / 00 80 63 51 82 80	00 00	0
1.2	forwarding	designated	20000	128	36866 / 00 80 63 51 82 80	00 00	0
1.3	forwarding	designated	20000	128	36866 / 00 80 63 51 82 80	00 00	0
1.4	forwarding	master	20000	112	36866 / 00 80 63 51 82 80	00 00	0
2.1	forwarding	designated	200000	128	36866 / 00 80 63 51 82 80	00 00	0
2.2	forwarding	designated	200000	128	36866 / 00 80 63 51 82 80	00 00	0
2.3	disabled	disabled	200000	128	36866 / 00 80 63 51 82 80	00 00	0
2.4	forwarding	designated	200000	128	36866 / 00 80 63 51 82 80	00 00	0
3.1	disabled	disabled	0	128	36866 / 00 80 63 51 82 80	00 00	0
3.2	disabled	disabled	0	128	36866 / 00 80 63 51 82 80	00 00	0

Abb. 77: 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. 154: Schaltflächen

7 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
- ▶ Service-Mode

Diese geben im Service-Fall dem Techniker die notwendigen Informationen zur Diagnose.

7.1 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 296 „Trap-Log“](#)) und in der Log-Datei ([siehe auf Seite 349 „Event-Log“](#)). Das Gerät wertet SNMP-Anfragen als Ereignis, wenn Sie "Log SNMP-Set/Get Request" aktivieren ([siehe Tabelle 156](#)).

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
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. 155: Syslog- und SNMP-Logging-Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
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. 155: Syslog- und SNMP-Logging-Einstellungen

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
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. 156: Syslog-Server-Einträge

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Mindest-Schweregrad	Mindest-Schweregrad für ein Ereignis, damit das Gerät dafür einen Log-Eintrag an diesen Syslog-Server schickt.	debug informational notice warning error critical alert emergency	critical
Aktiv	Aktivieren oder Deaktivieren des aktuellen Syslog-Server-Eintrags in dieser Zeile.	aktiv (Kästchen markiert) inaktiv (Kästchen leer)	inaktiv

Tab. 156: 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.

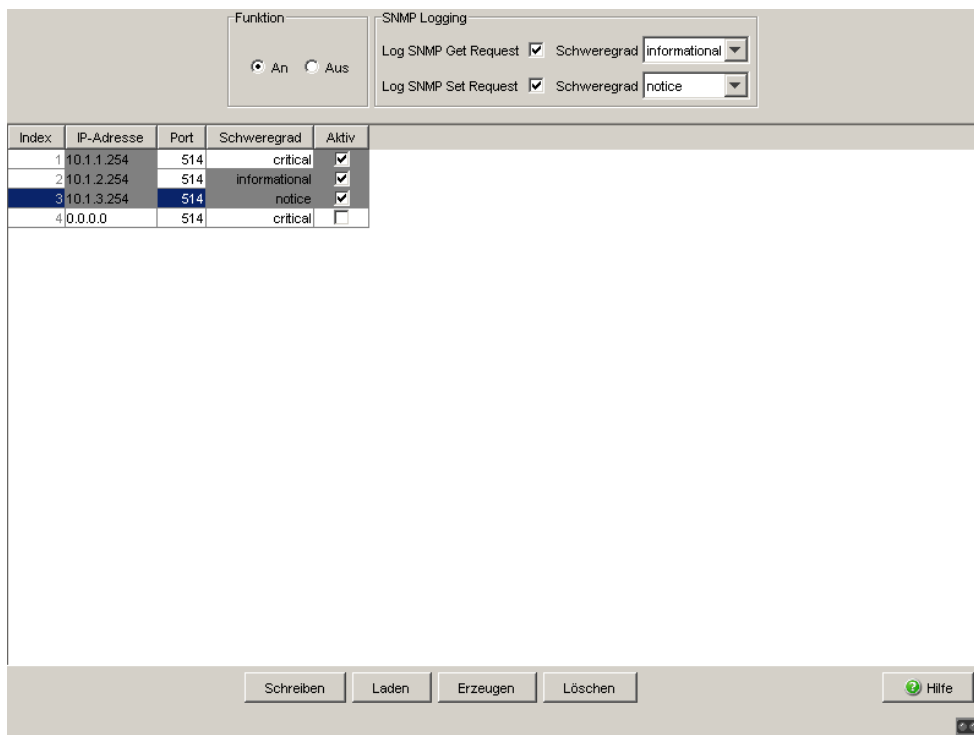


Abb. 78: Dialog Syslog

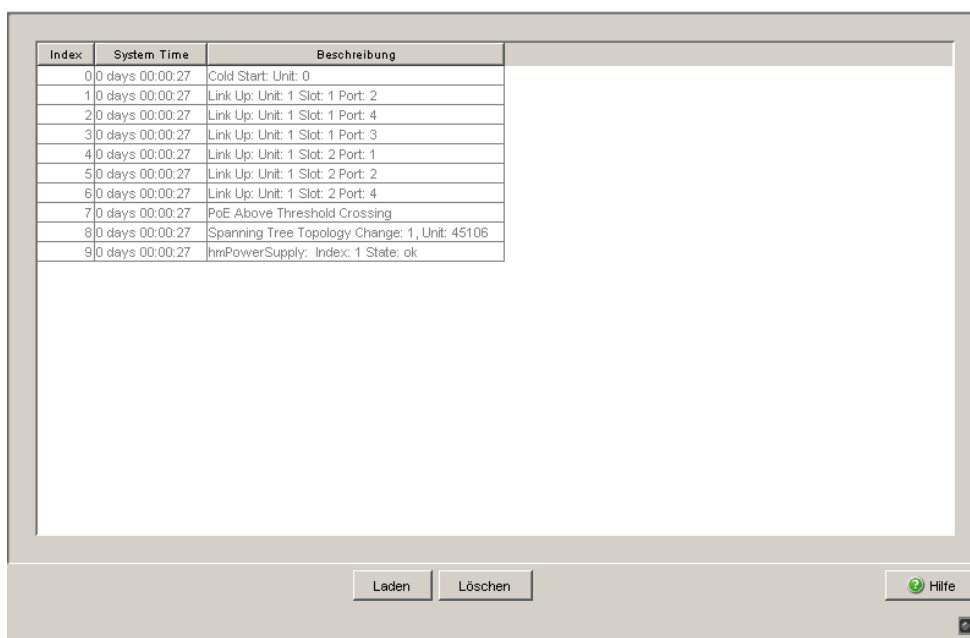
■ Schaltflächen

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. 157: Schaltflächen

7.2 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.



Index	System Time	Beschreibung
0	0 days 00:00:27	Cold Start: Unit: 0
1	0 days 00:00:27	Link Up: Unit: 1 Slot: 1 Port: 2
2	0 days 00:00:27	Link Up: Unit: 1 Slot: 1 Port: 4
3	0 days 00:00:27	Link Up: Unit: 1 Slot: 1 Port: 3
4	0 days 00:00:27	Link Up: Unit: 1 Slot: 2 Port: 1
5	0 days 00:00:27	Link Up: Unit: 1 Slot: 2 Port: 2
6	0 days 00:00:27	Link Up: Unit: 1 Slot: 2 Port: 4
7	0 days 00:00:27	PoE Above Threshold Crossing
8	0 days 00:00:27	Spanning Tree Topology Change: 1, Unit: 45106
9	0 days 00:00:27	hbmPowerSupply: Index: 1 State: ok

Buttons:

Abb. 79: Trap-Log Tabelle

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
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. 158: Trap-Log Tabelle

Sie haben die Möglichkeit, die geloggtten Ereignisse zusätzlich an einen oder mehrere Syslog-Server zu senden ([siehe auf Seite 292 „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. 159: Schaltflächen

7.3 Ports

Das Port-Menü enthält Anzeigen und Tabellen zu den einzelnen Ports:

- ▶ Statistiktabelle
- ▶ Netzlast
- ▶ SFP-Module
- ▶ TP-Kabeldiagnose
- ▶ Port-Monitor

7.3.1 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. 80: 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. 160: Schaltflächen

7.3.2 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.

Port	Netzlast [%]	Unterer Grenzwert [%]	Oberer Grenzwert [%]	Alarm
1.1	0,0	0,0	0,0	<input type="checkbox"/>
1.2	0,0	0,0	0,0	<input type="checkbox"/>
1.3	0,0	0,0	0,0	<input type="checkbox"/>
1.4	0,0	0,0	0,0	<input type="checkbox"/>
2.1	0,0	0,0	0,0	<input type="checkbox"/>
2.2	0,0	0,0	0,0	<input type="checkbox"/>
2.3	0,0	0,0	0,0	<input type="checkbox"/>
2.4	0,0	0,0	0,0	<input type="checkbox"/>
3.1	0,0	0,0	0,0	<input type="checkbox"/>
3.2	0,0	0,0	0,0	<input type="checkbox"/>

Schreiben Laden Hilfe

Abb. 81: Dialog Auslastung (Netzlast)

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
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 <code>Alarm</code> 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 <code>Unterer Grenzwert [%]</code> oder über dem im Feld <code>Oberer Grenzwert [%]</code> festgelegten Wert. Das Gerät sendet eine SNMP-Nachricht (Trap). - unmarkiert Die Netzlast des Geräte-Ports liegt über dem im Feld <code>Unterer Grenzwert [%]</code> und unter dem im Feld <code>Oberer Grenzwert [%]</code> festgelegten Wert.	markiert unmarkiert	unmarkiert

Tab. 161: 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. 162: Schaltflächen

7.3.3 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. 163: Dialog SFP-Module

Port	Modultyp	Unterstützt	Temperatur in °Celsius	Sendeleistung in mW	Empfangsleistung in mW	Sendeleistung in dBm	Empfangsleistung in dBm
1.4	M-SFP-SX/LC	<input checked="" type="checkbox"/>	40	0.2488	0.0138	-6.0	-18.6

Laden Hilfe

Abb. 82: 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.

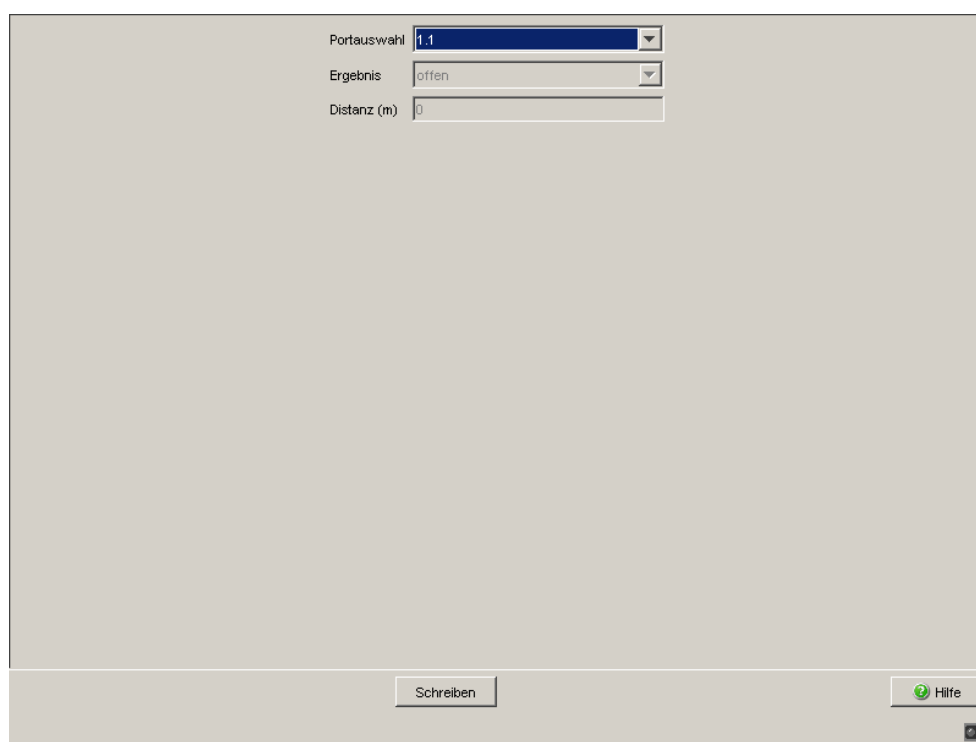
Tab. 164: Schaltflächen

7.3.4 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.



The image shows a software dialog box for TP-cable diagnosis. It has a light gray background. At the top left, there are three input fields: 'Portauswahl' (Port selection) with a dropdown menu showing '1.1', 'Ergebnis' (Result) with a dropdown menu showing 'offen', and 'Distanz (m)' (Distance in meters) with a text input field containing '0'. At the bottom of the dialog, there are two buttons: 'Schreiben' (Write) and 'Hilfe' (Help). The 'Hilfe' button has a small green icon with a question mark.

Abb. 83: 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. 165: 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. 166: Schaltflächen

7.3.5 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.

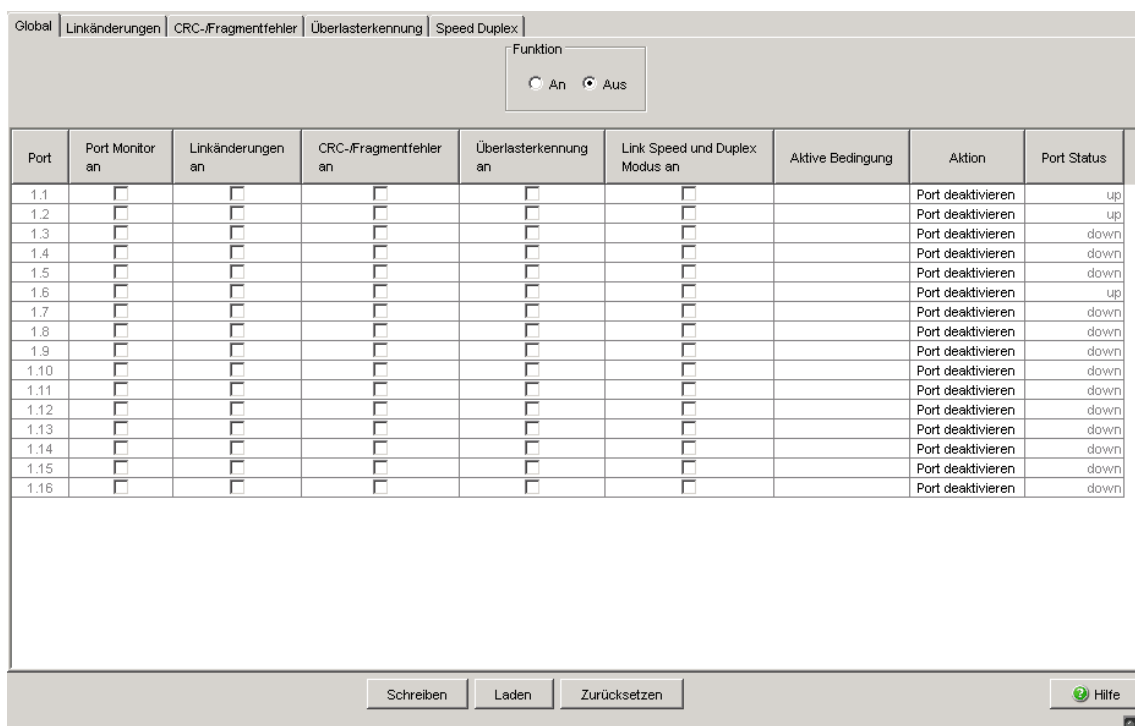


Abb. 84: Dialog Port-Monitor Global

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. 167: Tabelle Port-Monitor Global

Parameter	Bedeutung
Aktion	<p>Hier wählen Sie die Aktion, die das Gerät ausführt, wenn das auslösende Ereignis eintritt. Folgende Aktionen sind möglich:</p> <ul style="list-style-type: none"> ▶ 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 <code>Diagnose:Ports:Auto-Disable</code> folgende Einstellungen festgelegt haben: <ul style="list-style-type: none"> – 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 <code>Diagnose:Ports:Auto-Disable</code>, Rahmen „Konfiguration“. <ul style="list-style-type: none"> – 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 <code>Diagnose:Ports:Auto-Disable</code> 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 312 „Überlasterkennung“). – Der Port bleibt aktiviert, wenn das Kontrollkästchen für das auslösende Ereignis unmarkiert ist.
Port-Status	<p>Zeigt den aktuellen Port-Status an.</p> <ul style="list-style-type: none"> – <code>up</code>: Datenübertragung über den Port ist möglich. – <code>down</code>: Datenübertragung über den Ports ist unterbrochen. – <code>notPresent</code>: Kein physischer Port vorhanden.

Tab. 167: 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.

Port	Letztes Abtastintervall	Gesamt
1.1	0	0
1.2	0	0
1.3	0	0
1.4	0	0
1.5	0	0
1.6	0	0
1.7	0	0
1.8	0	0
1.9	0	0
1.10	0	0
1.11	0	0
1.12	0	0
1.13	0	0
1.14	0	0
1.15	0	0
1.16	0	0

Abb. 85: 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. 168: 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.

Port	Letztes aktives Abtastintervall [ppm]	Gesamt [ppm]
1.1	0	0
1.2	0	0
1.3	0	0
1.4	0	0
1.5	0	0
1.6	0	0
1.7	0	0
1.8	0	0
1.9	0	0
1.10	0	0
1.11	0	0
1.12	0	0
1.13	0	0
1.14	0	0
1.15	0	0
1.16	0	0

Abb. 86: Dialog Port-Monitor CRC-/Fragmentfehler

Parameter	Bedeutung
CRC-/Fragmentfehlerrate [ppm]	Fragmentfehleranteil im abgeschlossenen Abtastintervall, der zu einer Aktion des Gerätes führt.
Abtastintervall [s]	Länge eines Abtastintervalls, in dem das Gerät den CRC-/Fragmentfehleranteil bestimmt.
Port-Tabelle	
Port	Liste der verfügbaren Ports des Gerätes.

Tab. 169: 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. 169: 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.
- Speichern Sie die Einstellungen.

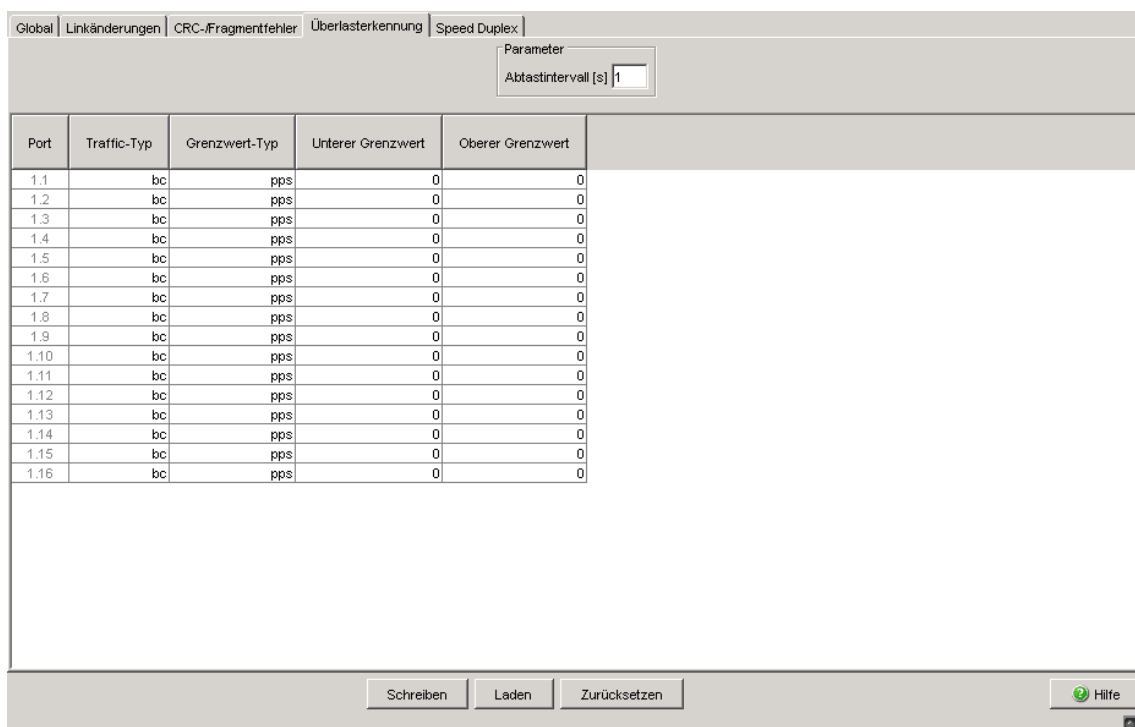


Abb. 87: Dialog Port-Monitor Überlasterkennung

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. 170: Tabelle Port-Monitor CRC-/Fragmentfehler

Parameter	Bedeutung
Traffic-Typ	Legt den Traffic-Typ für die Überlasterkennung fest. Folgende Aktionen sind möglich: <ul style="list-style-type: none"> – 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: <ul style="list-style-type: none"> – pps - Pakete pro Sekunde Verfügbar auf den Geräten MACH1040 und MACH104: <ul style="list-style-type: none"> – 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. 170: 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.

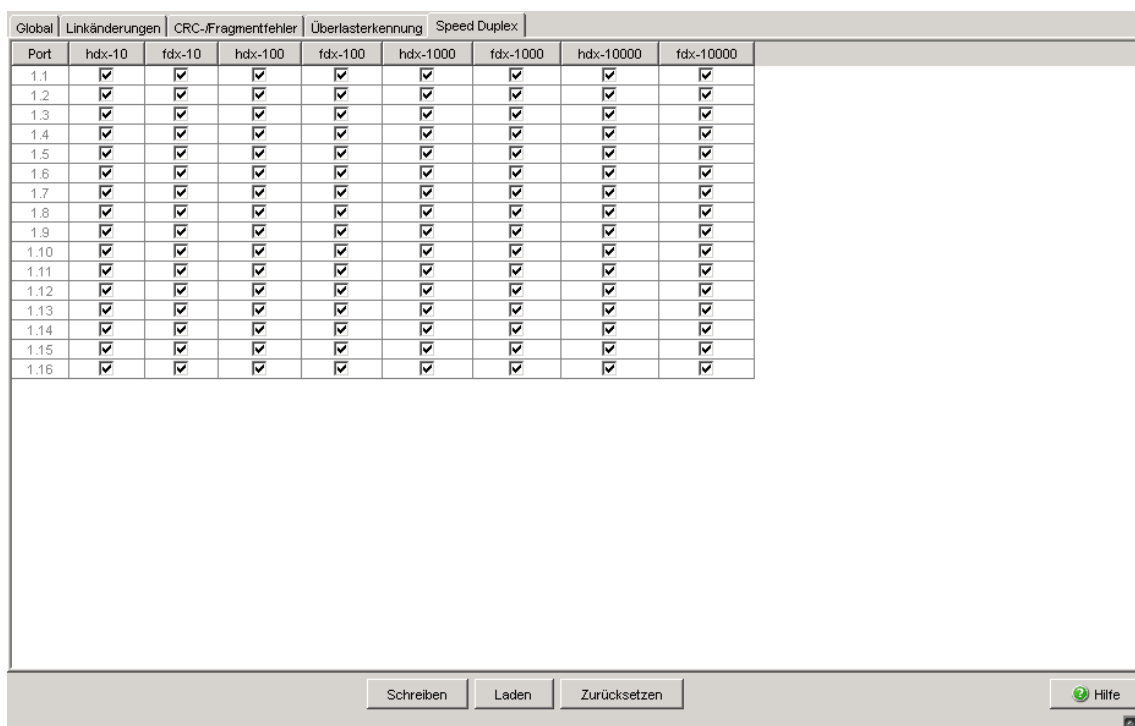


Abb. 88: Dialog Port-Monitor Speed Duplex

Parameter	Bedeutung
Port	Liste der verfügbaren Ports des Gerätes.
hdx-10	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ <code>unmarkiert</code> 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	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ <code>unmarkiert</code> 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. 171: Tabelle Port-Monitor Speed Duplex

Parameter	Bedeutung
hdx-100	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ <code>unmarkiert</code> 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	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ <code>unmarkiert</code> 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	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 1 Gbit/s und Halbduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ <code>unmarkiert</code> 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. 171: Tabelle Port-Monitor Speed Duplex

Parameter	Bedeutung
fdx-1000	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 1 Gbit/s und Vollduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ <code>unmarkiert</code> 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	<p>Verfügbar auf den Geräten MACH4002 24G/48G und MACH104:</p> <p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Gbit/s und Vollduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ <code>unmarkiert</code> 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. 171: 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 <code>Grundeinstellungen:Laden/Speichern</code> , 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. 172: Schaltflächen

7.3.6 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 306 „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.

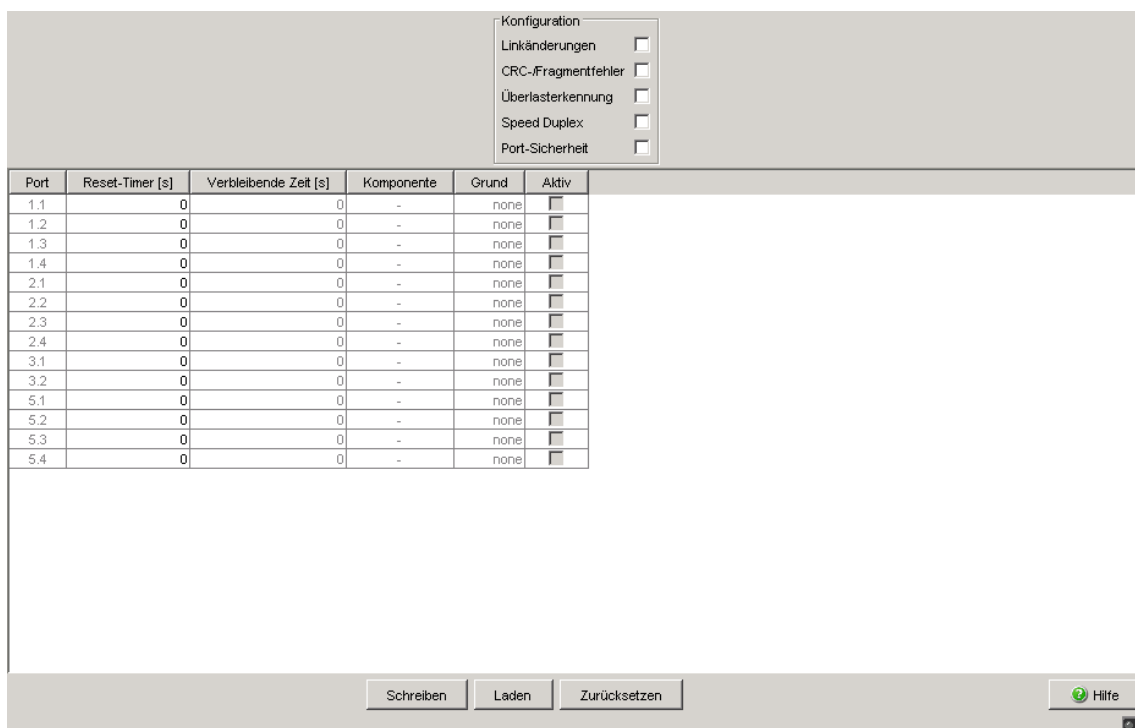


Abb. 89: Dialog „Auto-Disable“

■ Konfiguration

Parameter	Bedeutung
Linkänderungen	<p>Aktiviert/deaktiviert das Überwachen von Linkänderungen auf den Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> 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. ▶ <code>unmarkiert</code> (Voreinstellung) Die Auto-Disable-Funktion ignoriert Linkänderungen auf den Ports.
CRC-/Fragmentfehler	<p>Aktiviert/deaktiviert das Überwachen von CRC-/Fragmentfehlern auf den Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> 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. ▶ <code>unmarkiert</code> (Voreinstellung) Die Auto-Disable-Funktion ignoriert CRC-/Fragmentfehler auf den Ports.
Überlasterkennung	<p>Aktiviert/deaktiviert das Überwachen der Last auf den Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> 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 312. ▶ <code>unmarkiert</code> (Voreinstellung) Die Auto-Disable-Funktion ignoriert die Last auf den Ports.

Tab. 173: Rahmen „Konfiguration“ im Dialog `Diagnose:Ports:Auto-Disable`

Parameter	Bedeutung
Speed Duplex	<p>Aktiviert/deaktiviert das Überwachen der Geschwindigkeits- und Duplex-Kombination auf den Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> 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. ▶ <code>unmarkiert</code> (Voreinstellung) Die Auto-Disable-Funktion ignoriert die Geschwindigkeits- und Duplex-Kombination auf den Ports.
Port-Sicherheit	<p>Aktiviert/deaktiviert das Überwachen von unberechtigten Zugriffen auf den Ports im Zusammenarbeit mit der Funktion „Port-Sicherheit“ (siehe auf Seite 89 „Portsicherheit“).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> 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. ▶ <code>unmarkiert</code> (Voreinstellung) Die Auto-Disable-Funktion ignoriert unberechtigte Zugriffe auf den Ports.

Tab. 173: 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]	<p>Legt die Zeitspanne in Sekunden fest, nach der das Gerät den durch den Port-Monitor deaktivierten Port automatisch re-aktiviert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0 (Voreinstellung) Timer ist deaktiviert. Der Port bleibt deaktiviert. ▶ 30...2147483 <p>Wenn der Port-Monitor den Port auf Grund von Überlast deaktiviert hat, gelten für das Re-Aktivieren des Ports weitere Voraussetzungen (siehe auf Seite 312 „Überlasterkennung“).</p>
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	<p>Zeigt, ob die Auto-Disable-Funktion auf dem betreffenden Port aktiv ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 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. 174: 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 <i>Grundeinstellungen:Laden/Speichern</i> 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. 175: Schaltflächen

7.4 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.

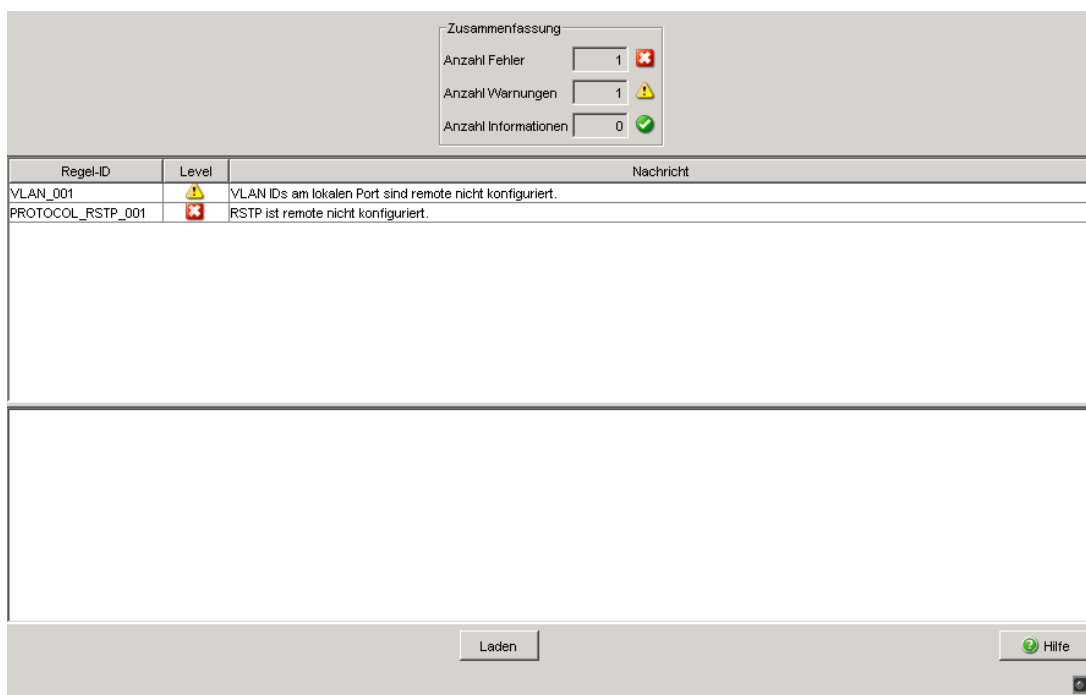





Abb. 90: Dialog Konfigurations-Check

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. 176: 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	<p>Grad der Abweichung zwischen der Konfiguration dieses Gerätes und den erkannten Nachbargeräten. Der Regel-Level kann 3 Zustände annehmen:</p> <ul style="list-style-type: none">  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. 177: 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. 178: Schaltflächen

7.5 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.

7.5.1 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. 179: Topologie-Erkennung (LLDP-Informationen)

Parameter	Bedeutung
Nachbar-Systemname	Systemname des Nachbargerätes. Der Systemname ist eine alphanumerische Zeichenkette.
Nachbar-Systembeschreibung	Systembeschreibung des Nachbargerätes gemäß IEEE 802.1AB.

Tab. 179: Topologie-Erkennung (LLDP-Informationen)

Funktion
 An Aus

LLDP
LLDP-MED

Port	Nachbar-Bezeichner	Nachbar-IP-Adresse	Nachbar-Port-Beschreibung	Nachbar-Systemname	Nachbar-Systembeschreibung
1.3	ec e5 55 49 1d 00	10.0.1.120	Module: 1 Port: 1 - 1 Gbit	MACH-491D00	Hirschmann MACH - SW: L3P-08.0.00-B10
2.2	00 80 63 51 7a 80	10.0.1.116	Module: 2 Port: 1 - 10/100 Mbit TX	PowerMICE-517A80	Hirschmann PowerMICE - SW: L3E-07.0.00-...
2.4	00 80 63 4a a7 b3	10.0.1.10	Module: 1 Port: 4 - 10/100 Mbit TX	RS-4AA7B3	Hirschmann Railswitch - SW: L2B-05.0.11
1.1	00 80 63 2f fb b8	10.0.1.2	Module: 1 Port: 1 - 1 Gbit	MICE-2FFB8	Hirschmann MICE - SW: L2P-08.0.00-B10
2.1	00 80 63 14 db d9	10.0.1.62	10/100 Mbit Ethernet Switch Inter...	Gerhards RS2-16M	Hirschmann Ethernet Railswitch 2

FDB Einträge anzeigen

Schreiben
Laden
Hilfe

Abb. 91: 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 168 „Filter für MAC-Adressen“](#)).

7.5.2 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 325 „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: <ul style="list-style-type: none"> – 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	<ul style="list-style-type: none"> – <code>true</code>: 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. – <code>false</code>: die Netz-Richtlinie für den Applikations-Typ des entfernten Gerätes ist bekannt
Tagged Bit Status	<ul style="list-style-type: none"> – <code>true</code>: die Applikation des entfernten Gerätes verwendet VLAN-getaggte Frames – <code>false</code>: 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. 180: 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. 180: 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 204 „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.

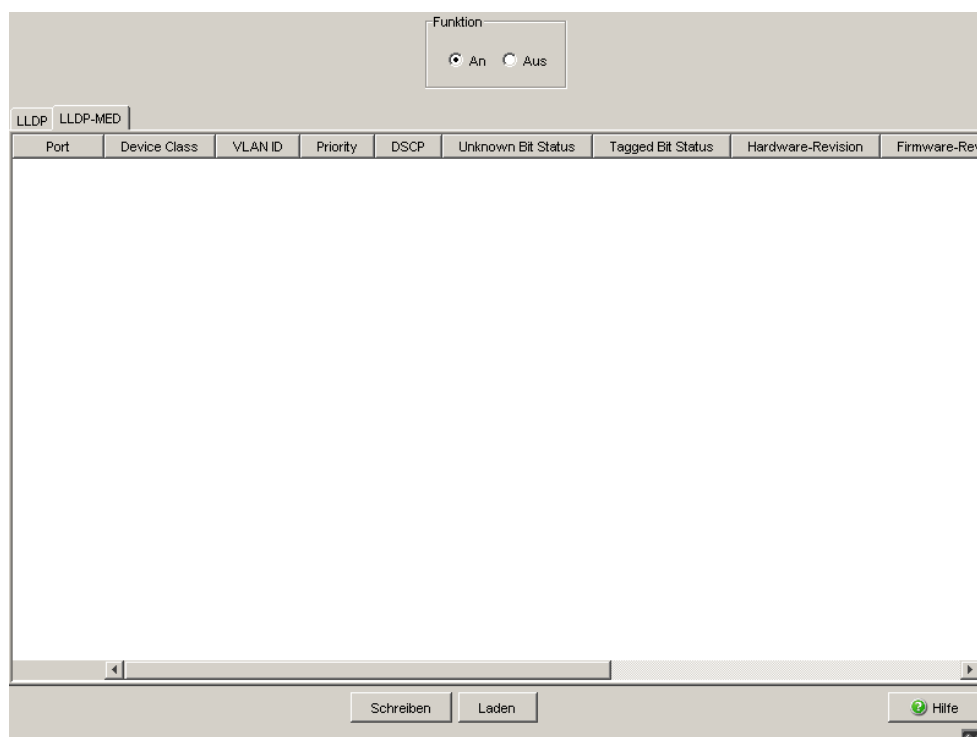


Abb. 92: LLDP-MED-Informationen

■ 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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 181: Schaltflächen

7.6 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**.

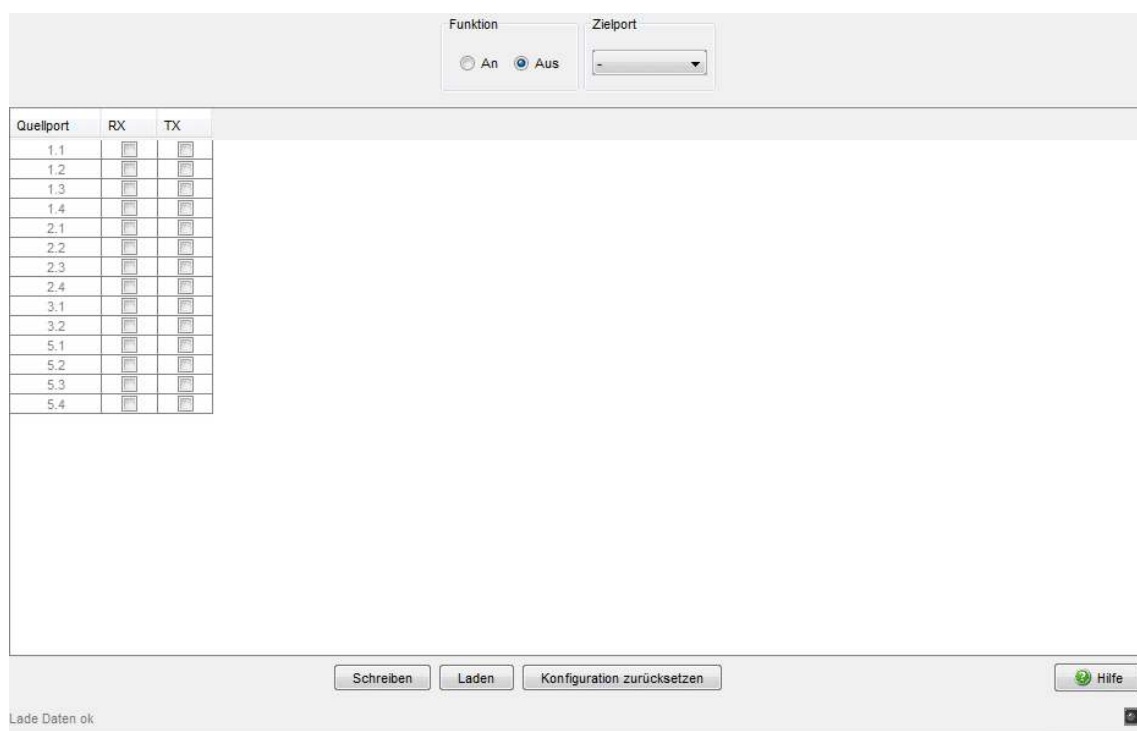


Abb. 93: *Dialog Diagnose:Port-Mirroring N:1*

■ 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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 182: Schaltflächen

7.7 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.

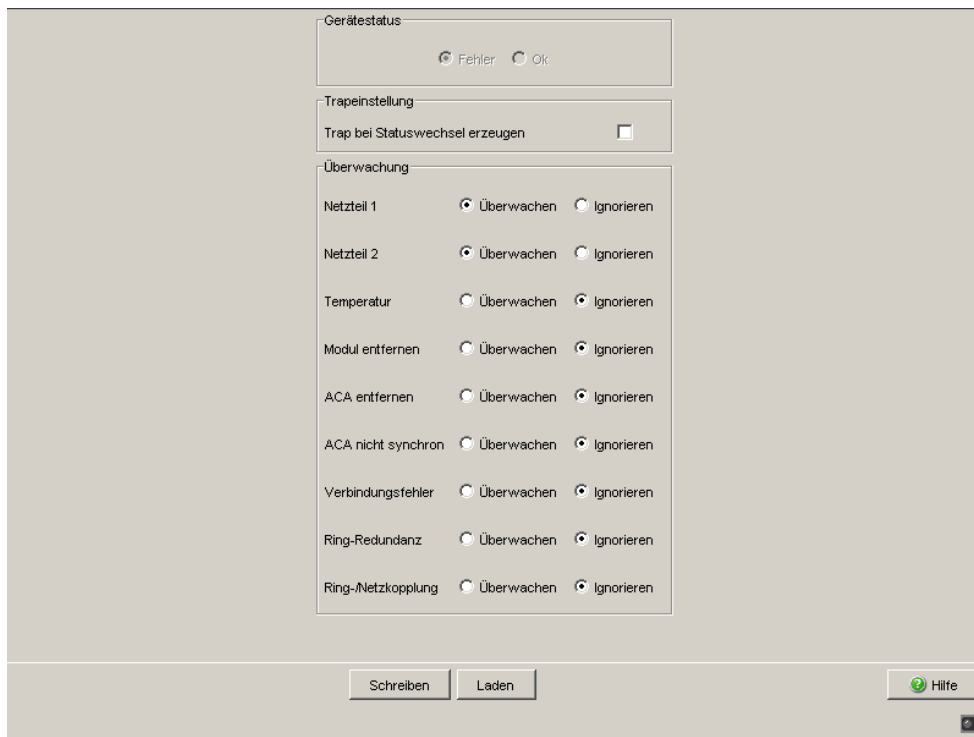


Abb. 94: Dialog Gerätestatus (bei PowerMICE)

- 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 .

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 „Trap-einstellungen“	-
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: <ul style="list-style-type: none"> ▶ nichts (beim HIPER-Ring) ▶ erkannte Fehler in der lokalen Konfiguration (beim Fast HIPER-Ring und bei MRP)

Tab. 183: 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. 183: *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 337](#) „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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 184: *Schaltflächen*

7.8 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.

7.8.1 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.

7.8.2 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 ACA². 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 230 „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 230 „Ring-Redundanz“](#)).
Lieferzustand: keine Überwachung.

Anmerkung: Bei der Zwei-Switch-Kopplung ist Voraussetzung, dass beide Switches ihren jeweiligen Partner gefunden haben.

7.8.3 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.

7.8.4 Trapeinstellung

- Wählen Sie `Trap` bei Statuswechsel erzeugen, damit das Gerät ein `Trap` erzeugt, sobald sich bei aktiver Funktionsüberwachung die Stellung eines Meldekontaktes ändert.

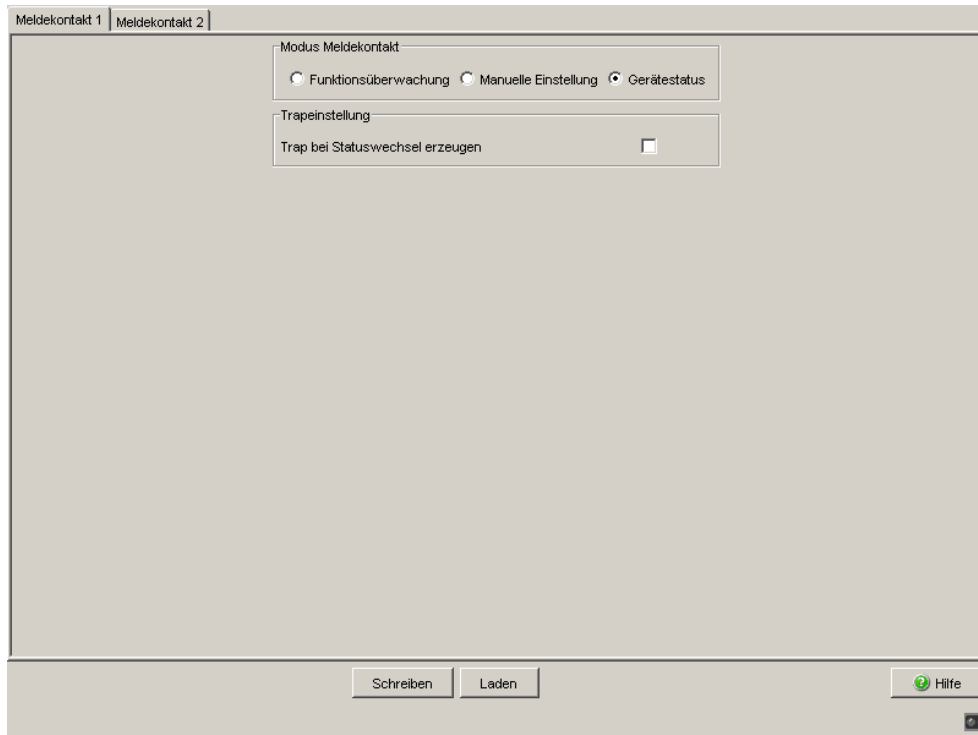


Abb. 95: Dialog Meldekontakt

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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 185: Schaltflächen

7.9 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 10 Trap-Ziele:

- ▶ RS20, RS30, RS40
- ▶ MS20, MS30
- ▶ OCTOPUS
- ▶ MACH 102
- ▶ RSR20, RSR30
- ▶ MACH 1020, MACH 1030

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.

Tab. 186: Trap-Kategorien

Name	Bedeutung
Spanning Tree	Die Topologie des Rapid Spanning Tree hat sich geändert
Chassis	<p>Fasst die folgenden Ereignisse zusammen:</p> <ul style="list-style-type: none"> ▶ 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 <code>Diagnose:Meldekontakt 1/2</code>. ▶ 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 <code>Diagnose:Ports:SFP-Module</code>). ▶ 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 <code>Portsicherheit</code>).

Tab. 186: Trap-Kategorien

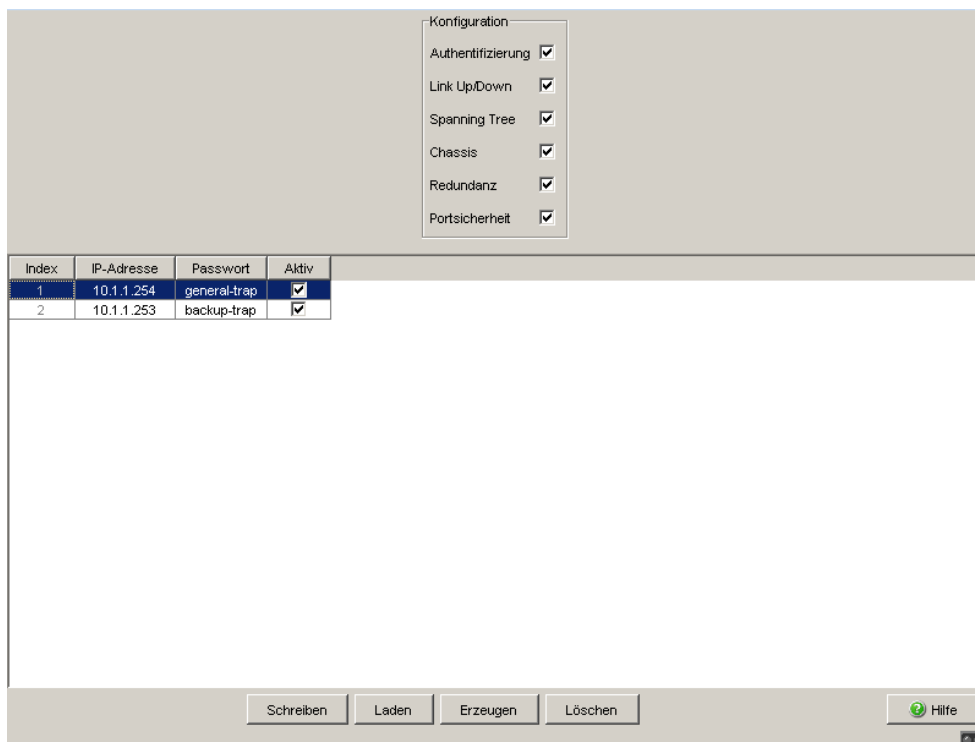


Abb. 96: Dialog Alarme

■ 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. 187: Schaltflächen

7.10 Bericht

Folgende Berichte stehen zur Diagnose zur Verfügung:

- ▶ System Information ([siehe auf Seite 349 „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 349 „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 geloggtten Ereignisse zusätzlich an einen oder mehrere Syslog-Server zu senden ([siehe auf Seite 292 „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 188](#)).
 - 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. 188: 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 :	clicommands.txt	Text	
– show running-config ^b			
– show port all			
– show sysinfo			
– show mac-address-table			
– show mac-filter-table			
– igmpsnooping			

Tab. 188: Dateien im Switch-Dump-Archiv

a: Voraussetzung: eine Telnet-Verbindung ist verfügbar.

b: Voraussetzung: Sie sind als Benutzer mit Schreibrechten angemeldet.

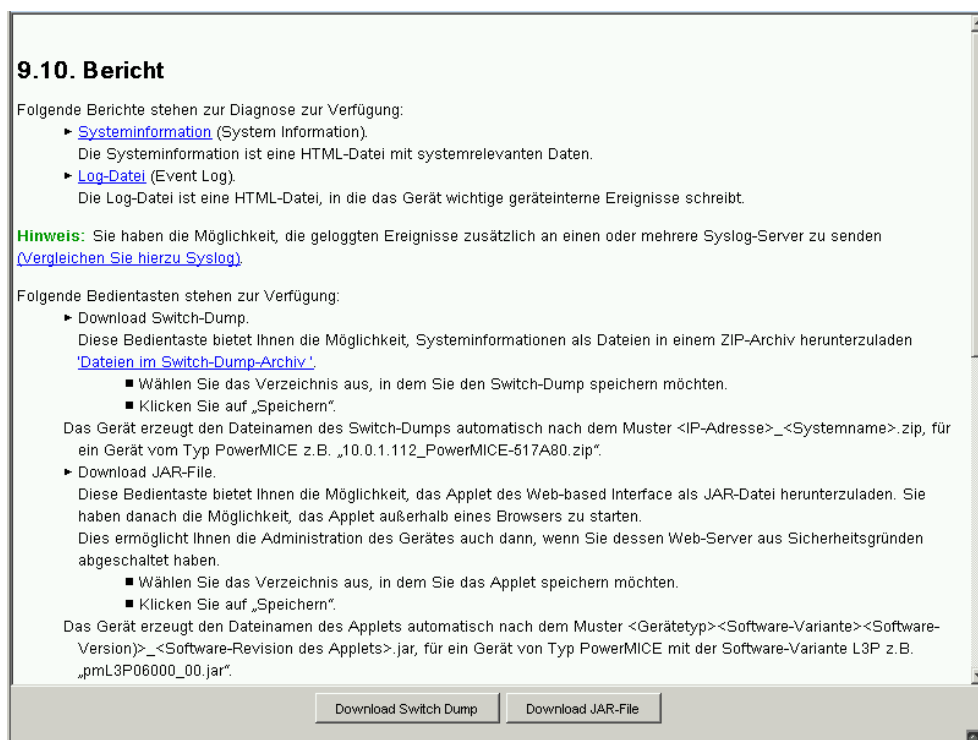


Abb. 97: Dialog Bericht

7.10.1 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. 189: Schaltflächen

7.10.2 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. 190: 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. 190: Schaltflächen (Forts.)

7.11 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 191). 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.
<code>enable</code>	Aktive und passive Erkennung einschalten.
<code>disable</code>	Funktion ausschalten
<code>activeDetectionOnly</code>	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. 191: Mögliche Adresskonflikt-Betriebsmodi

Modus	Bedeutung
passiveDetectionOnly	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 Gratuitous 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. 191: 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.

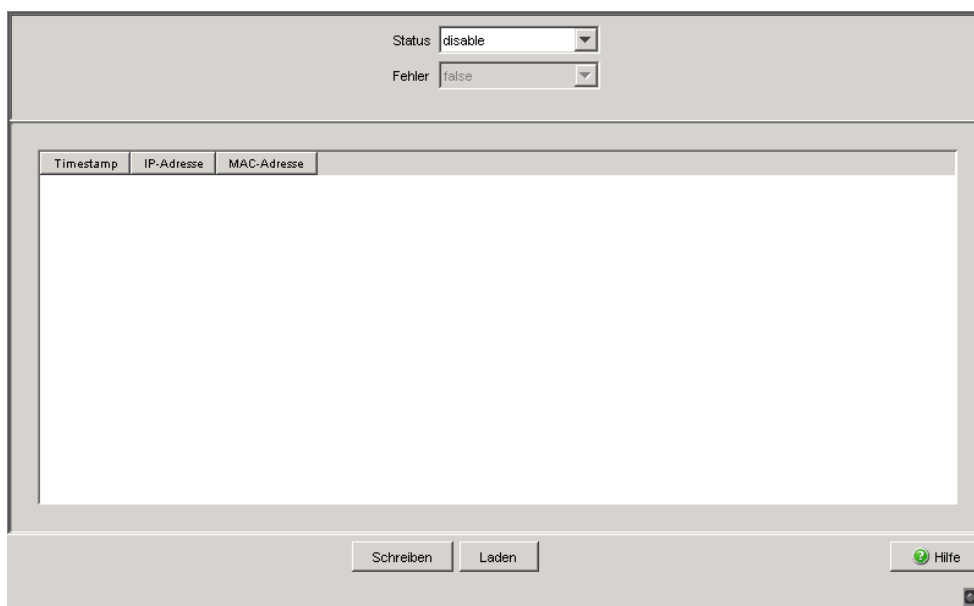


Abb. 98: Dialog IP-Adressen Konflikterkennung

■ 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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 192: Schaltflächen

7.12 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.

7.12.1 Funktion

Parameter	Bedeutung
Funktion	<p>Schaltet die MAC-Benachrichtigungsfunktion des Gerätes global ein oder aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An Das Gerät sendet Traps für die aktiven Zeilen an die im Dialog <code>Diagnose:Statuskonfiguration:Alarme (Traps)</code> konfigurierten aktiven Managementstationen. ▶ Aus (Lieferzustand)

Tab. 193: Rahmen „Funktion“ im Dialog `Diagnose:Statuskonfiguration:MAC Benachrichtigung`

7.12.2 Konfiguration

Parameter	Bedeutung
Intervall [s]	<p>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.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..2147483647

Tab. 194: Rahmen „Konfiguration“ im Dialog *Diagnose:Statuskonfiguration:MAC Benachrichtigung*

7.12.3 Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Geräte-Ports, auf den sich der Tabelleneintrag bezieht.
Aktiv	<p>Schaltet die MAC-Benachrichtigungsfunktion dieses Ports ein oder aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Sofern global aktiviert, sendet das Gerät Traps für diese Zeile an die im Dialog <i>Diagnose:Statuskonfiguration:Alarme (Traps)</i> konfigurierten aktiven Managementstationen. ▶ unmarkiert (Voreinstellung)

Tab. 195: Tabelle im Dialog *Diagnose:Statuskonfiguration:MAC Benachrichtigung*

Parameter	Bedeutung
Modus	<p>Legt fest, wann das Gerät für MAC-Adressereignisse an einer bestimmten Schnittstelle einen Trap sendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>add</code> Das Gerät sendet Benachrichtigungen über neue Einträge in der FDB. ▶ <code>remove</code> Das Gerät sendet Benachrichtigungen über gelöschte Einträge aus der FDB. ▶ <code>add + remove</code> (Voreinstellung) Das Gerät sendet Benachrichtigungen über neue und gelöschte Einträge in/aus der FDB.
Letzte MAC-Adresse	Zeigt für dieses Interface die letzte MAC-Adresse, die der Adresstabelle hinzugefügt oder von ihr entfernt wurde.
Letzter MAC-Status	<p>Zeigt den Status der letzten MAC-Adresse an diesem Interface an.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>other</code> ▶ <code>added</code> ▶ <code>removed</code>

Tab. 195: *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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 196: *Schaltflächen*

7.13 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.

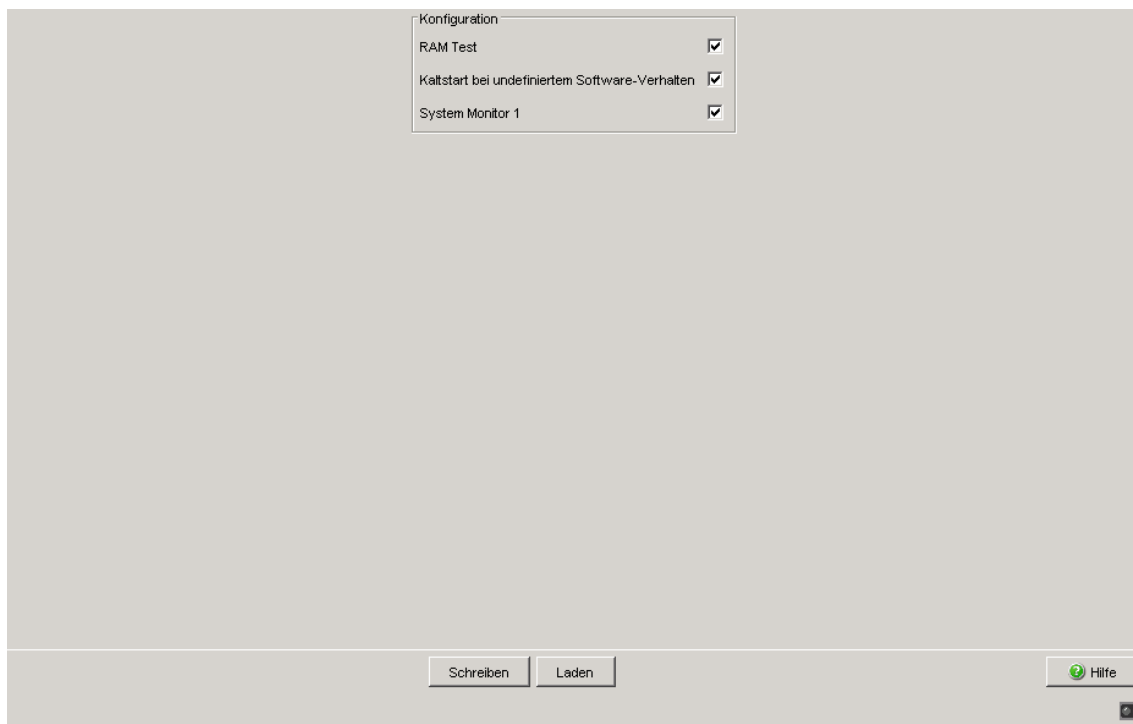


Abb. 99: Dialog Selbsttest

■ 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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 197: Schaltflächen

7.14 Service-Mode

Folgende Geräte unterstützen den Service-Mode:
RS20/RS30/RS40 und MS20/MS30.

Der Service-Mode ermöglicht Ihnen, das Gerät in 2 Vermittlungsbereiche aufzuteilen. Damit können Sie z.B. im Feldbereich eines Netzes Test- oder Servicekonfigurationen vornehmen, während der laufende Betrieb im Backbone-Bereich aufrecht erhalten bleibt.

Das Gerät bestimmt die beiden Vermittlungsbereiche durch die HIPER-Ring-Ports: Zum Vermittlungsbereich 1 gehören ausschließlich die HIPER-Ring Ports des Gerätes, zum Vermittlungsbereich 2 gehören alle anderen Ports. Mit dem Aktivieren des Service-Mode legt das Gerät ein neues VLAN an, in dem alle Ports des Vermittlungsbereichs 2 Mitglied werden. Den Service-Mode aktivieren Sie mit Hilfe der redundanten Versorgungsspannung (siehe unten). Sie können in den Dialogen unter Switching/VLAN die Konfiguration des neu angelegten VLAN einsehen, das Gerät verhindert jedoch das Ändern dieser Einträge, um die Service-Konfiguration beizubehalten.

Mit dem Generieren des VLANs

- ▶ stellt das Gerät an allen Ports dieses VLANs die Port-VLAN-IDs auf die neue VLAN-ID um.
- ▶ schaltet das Gerät an allen Ports dieses VLANs GVRP ab. Damit verhindert das Gerät das dynamische Ändern der Service-Mode-Porteinstellungen durch GVRP.
- ▶ aktiviert das Gerät an allen Ports dieses VLANs "Ingress Filtering". Damit vermittelt das Gerät Pakete ausschließlich, wenn der Eingangs- und Ausgangsport diesem VLAN angehören.

■ 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 <code>Grundeinstellungen:Laden/Speichern</code> 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. 198: Schaltflächen

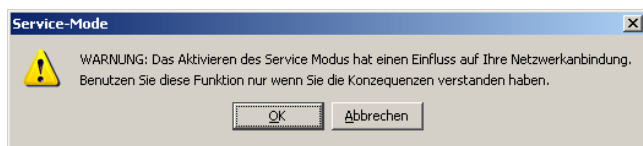
7.14.1 Service-Mode aktivieren

Voraussetzungen:

- HIPER-Ring-Ports sind definiert (HIPER-Ring oder MRP-Ring).
- Die Versorgungsspannung liegt redundant an P1 und P2 an.

Anmerkung: Fehlt beim Einschalten des Service-Mode (Klicken auf „Schreiben“, siehe unten) die redundante Spannung, erzeugt der Switch sofort die beiden Vermittlungsbereiche. Abhängig von den zuvor gemachten Einstellungen kann dies Ihre Verbindung zum Switch trennen.

- Wählen Sie den Dialog `Diagnose:Service-Mode`.
- Aktivieren Sie „Mode“.
- Geben Sie in „VLAN“ eine VLAN-ID ungleich 0 und 1 ein. Geben Sie eine VLAN-ID eines neuen VLANs ein, um Einstellungen bestehender VLANs beizubehalten.
- Klicken Sie auf „Schreiben“. Das Gerät gibt folgende Systemmeldung aus:



- Wenn Sie sicher sind, dass Ihre Verbindung zum Switch erhalten bleibt, klicken Sie auf „OK“, um den Service-Mode einzuschalten.

Das Gerät weist in allen Dialogen auf den eingeschalteten Service-Mode hin.

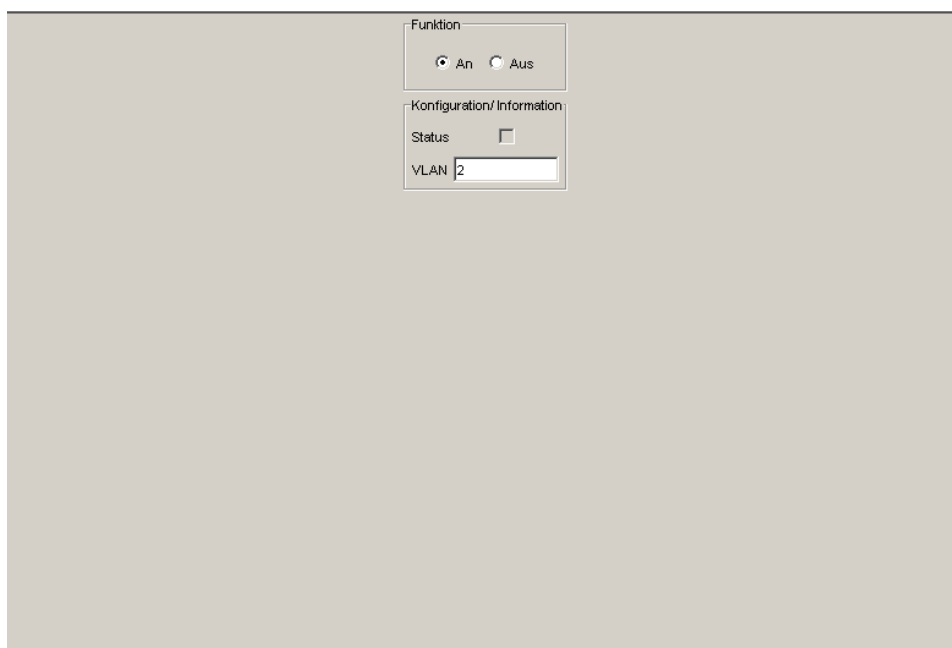


Abb. 100: Dialog Service-Mode - Mode eingeschaltet

- Deaktivieren Sie die redundante Versorgungsspannung.

Der Service-Mode ist jetzt aktiviert, das Gerät zeigt dies durch einen Haken im Feld "Status" an.

Anmerkung: Deaktivieren Sie zum Speichern der Konfiguration des Gerätes (Dialog: Grundeinstellungen:Laden/Speichern:Speichern:auf dem Switch) den Service-Mode (siehe unten).

7.14.2 Service-Mode deaktivieren

Reaktivieren Sie die redundante Spannung.

Der Service-Mode ist jetzt deaktiviert.

Wählen Sie den Dialog `Diagnose:Service-Mode`.

Deaktivieren Sie „Mode“.

Klicken Sie auf „Schreiben“, um den Service-Mode auszuschalten, so dass beim Ausfall der redundanten Spannungsversorgung das Gerät nicht in den Service-Mode wechselt.

Anmerkung: Nach dem Deaktivieren des Service-Mode nimmt das Gerät seine vorherigen Einstellungen wieder an.

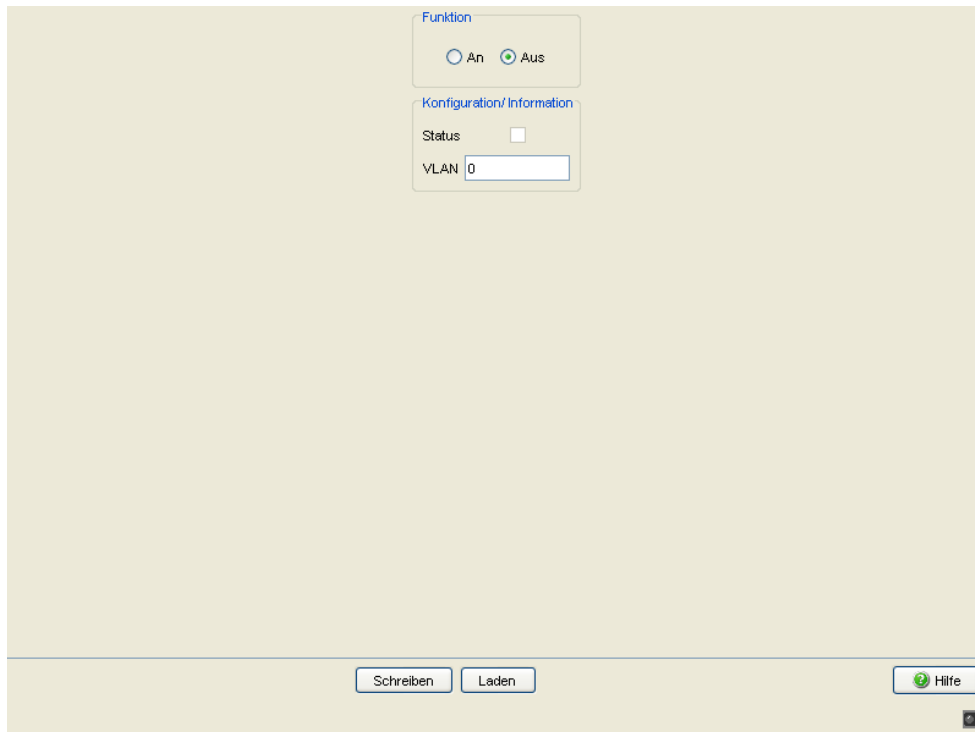


Abb. 101: Dialog Service-Mode - Mode ausgeschaltet

8 **Erweitert**

Das Menü enthält Dialoge, Anzeigen und Tabellen zu:

- ▶ DHCP-Relay-Agent
- ▶ DHCP-Server
- ▶ Industrieprotokolle
- ▶ Command Line Interface

8.1 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.

8.1.1 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:

B306000001000101000600806300061E

- 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.

DHCP Option 82

Funktion An Aus

Typ

konfigurierbarer Wert (Typ other)

RemoteID-Eintrag für DHCP-Server

Typanzeige

DHCP-Relay-Status
DHCP-Relay nicht aktiv

Port	Circuit-ID	DHCP-Relay ein	DHCP-Relay-Status	Option 82 ein	Hirschmann-Gerät
1.1	b4 06 00 00 01 01 01 01	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.2	b4 06 00 00 01 01 01 02	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.3	b4 06 00 00 01 01 01 03	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1.4	b4 06 00 00 01 01 01 04	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.1	b4 06 00 00 01 01 02 01	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.2	b4 06 00 00 01 01 02 02	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.3	b4 06 00 00 01 01 02 03	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2.4	b4 06 00 00 01 01 02 04	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.1	b4 06 00 00 01 01 03 01	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3.2	b4 06 00 00 01 01 03 02	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.1	b4 06 00 00 01 01 05 01	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.2	b4 06 00 00 01 01 05 02	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.3	b4 06 00 00 01 01 05 03	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>
5.4	b4 06 00 00 01 01 05 04	<input checked="" type="checkbox"/>	disable	<input checked="" type="checkbox"/>	<input type="checkbox"/>

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. 199: Schaltflächen

8.1.2 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.

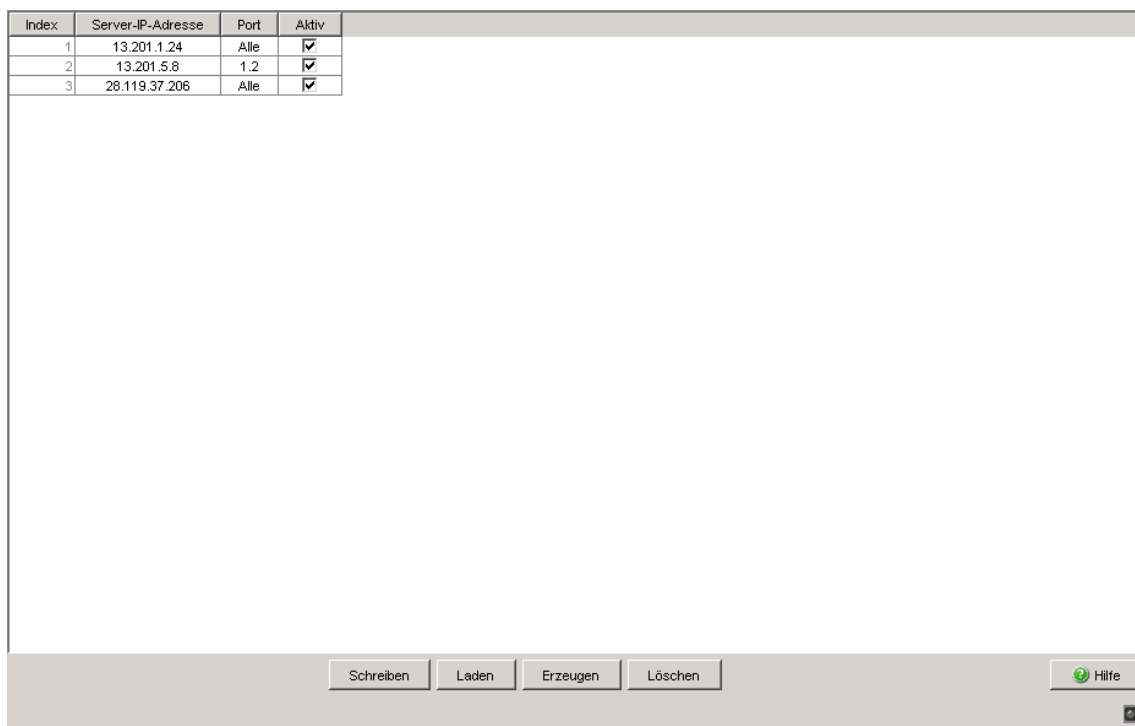


Abb. 103: Dialog *Erweitert:DHCP-Relay-Agent:Port*

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. 200: 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. 200: 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 <i>Grundeinstellungen:Laden/Speichern</i> , 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. 201: *Schaltflächen*

8.2 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.

8.2.1 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 DHCP-Servers auf dem Gerät.	An, Aus	Aus

Tab. 202: Rahmen „DHCP-Server Mode“ im Dialog *Erweitert:DHCP-Server:Global*

Parameter	Bedeutung	Wertebereich	Voreinstellung
IP-Überprüfung	Aktiviert/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. 203: 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. 204: Tabelle im Dialog *Erweitert:DHCP-Server:Global*

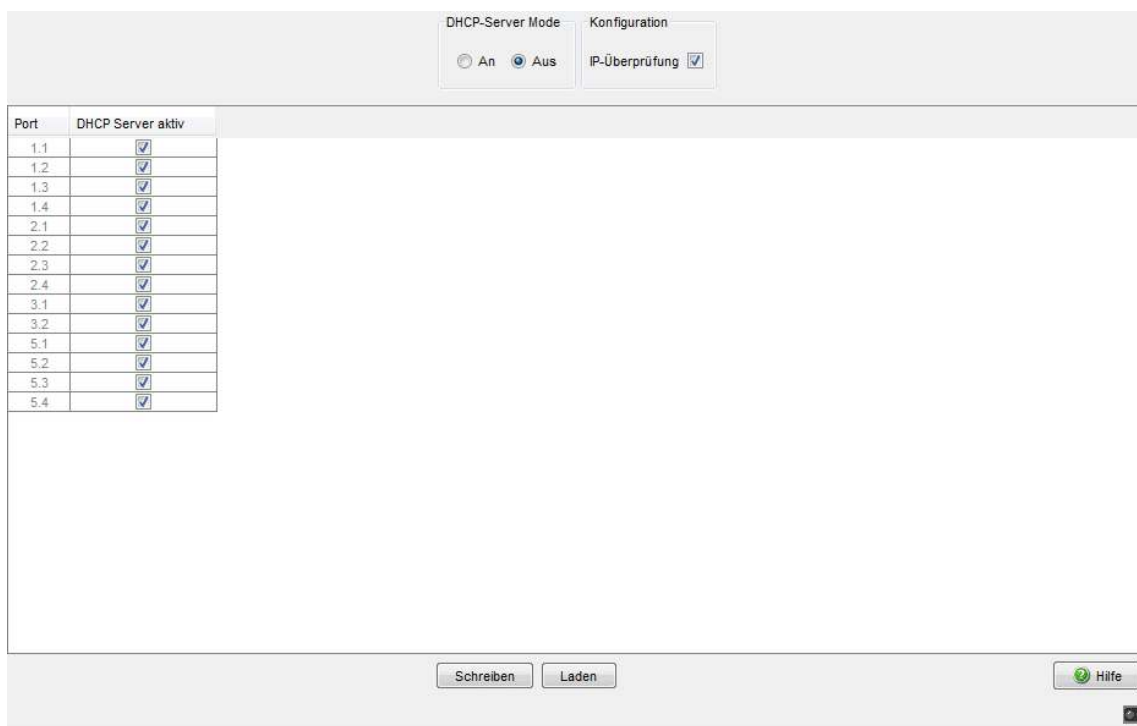


Abb. 104: Dialog DHCP-Server Global

■ 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. 205: Schaltflächen

8.2.2 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 64 Pool-Einträge zu erzeugen (128 für die Geräte PowerMICE und MACH).

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	<ul style="list-style-type: none"> ▶ 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. <ul style="list-style-type: none"> ▶ Für einen dynamischen Adress-Eintrag wählen Sie <code>all</code>. ▶ Für einen statischen Adress-Eintrag wählen Sie <code>all</code> oder eine gültige Modul- und Port-Nr. 	Gültige Modul- und Port-Nr. oder <code>all</code> .	<code>all</code>
VLAN	VLAN-Nummer, für die dieser Eintrag gilt.	Gültige VLAN-Nr.	-
Anmerkung: Diese Spalte ist verfügbar für die Geräte MS, Octopus, RS, RSR, MACH102 und MACH1020/1030.			
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	-

Tab. 206: DHCP-Server-Pool-Einstellungen, IP-Adress-Grundeinstellungen

Parameter	Bedeutung	Wertebereich	Voreinstellung
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.	-
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 <code>tftp://servername-oder-ip-adresse/verzeichnis/datei</code> .	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 Ablauf 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. 206: 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).	Gültiger Hex-String.	-

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 Längfelder. Geben Sie darum einen gültigen Hex-String ein, der die korrekten Längwerte beinhaltet.

Tab. 206: 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.

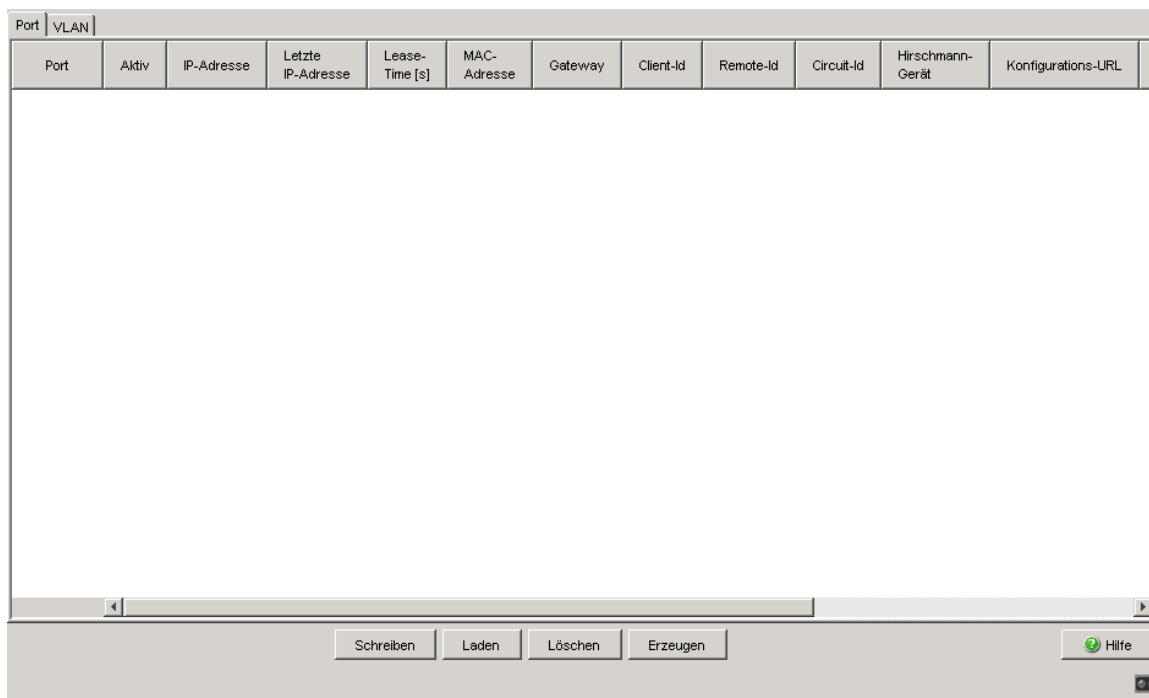


Abb. 105: Dialog DHCP-Server-Pool pro Port

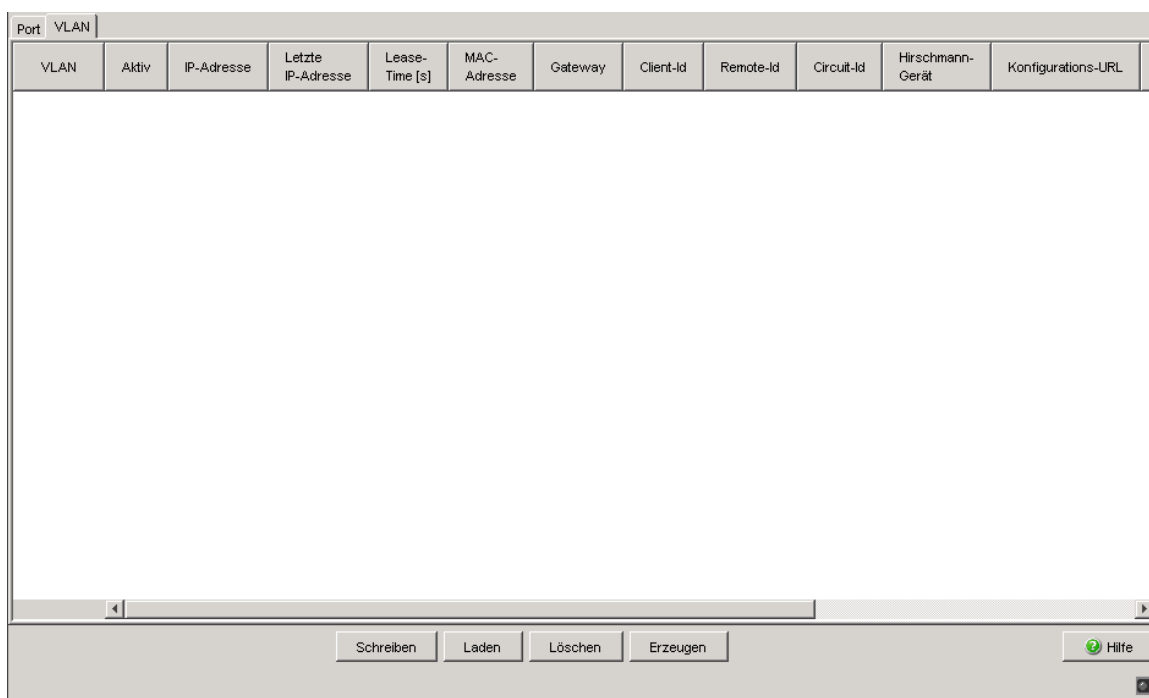


Abb. 106: Dialog DHCP-Server-Pool pro VLAN

■ 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. 207: Schaltflächen

8.2.3 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. 208: 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. 208: DHCP-Lease-Tabelle

- ^a Eine Client-, Remote- oder Circuit-ID besteht aus 1 - 255 Bytes in Hexadezimalschreibweise (00 - ff), durch Leerzeichen getrennt.

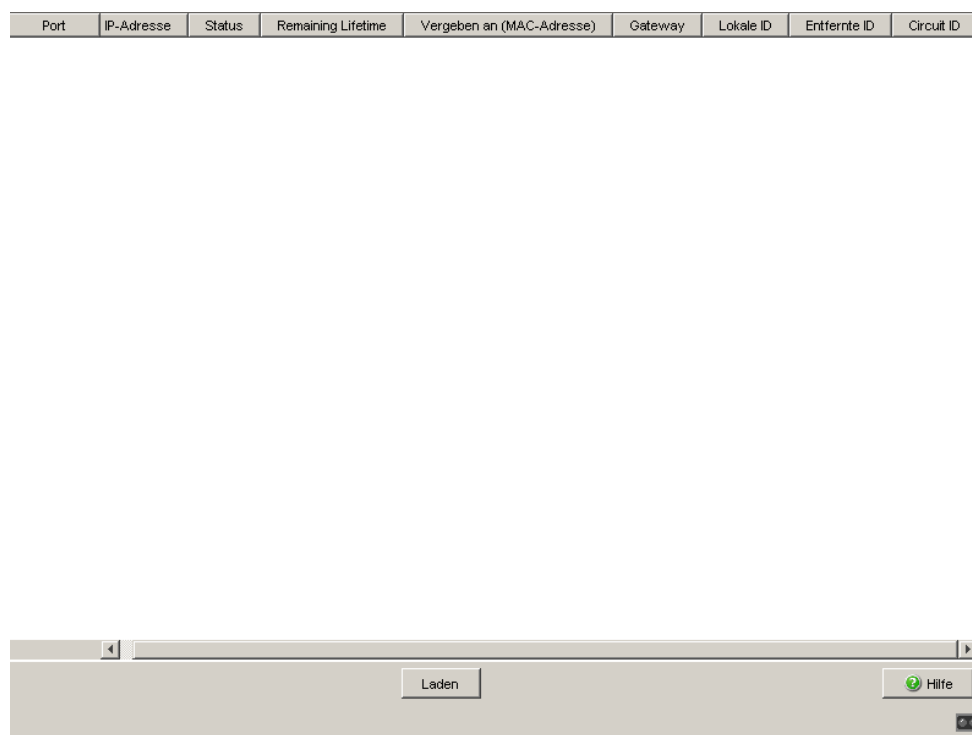


Abb. 107: Dialog DHCP-Server-Lease-Tabelle

■ 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. 209: Schaltflächen

8.3 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“.

8.3.1 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 188 „VLAN Global“](#)).

Anmerkung: Schließen Sie eine Kombination des VLAN 0-Transparent-Modus mit dem Einsatz von MSTP (Multiple Spanning Tree) aus.

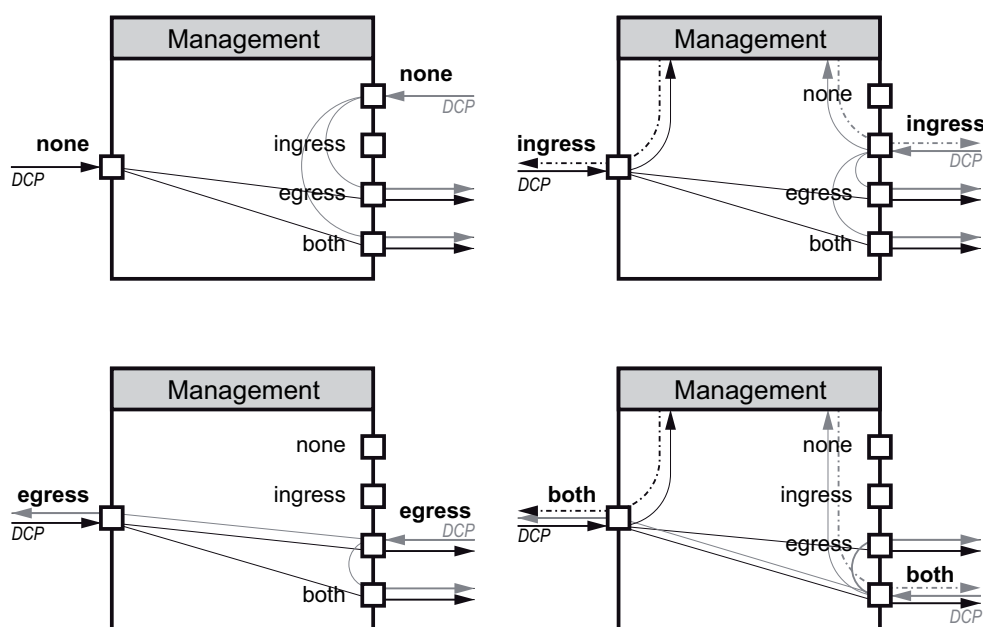
- Konfigurieren Sie die Alarmeinstellungen und die Schwellwerte für die Alarmer, die Sie überwachen wollen ([siehe auf Seite 334 „Gerätstatus“](#)).

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 <code>Grundeinstellungen:Laden/Speichern</code> , 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. 210: Schaltflächen

8.3.2 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 177 „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 „Industrieprotokolle“ 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 <code>Grundeinstellungen:Laden/Speichern</code> , 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. 211: Schaltflächen

8.3.3 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. 212: 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. 213: 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. 214: Rahmen „Download“ im Dialog *Erweitert:Industrie-Protokolle:IEC61850*

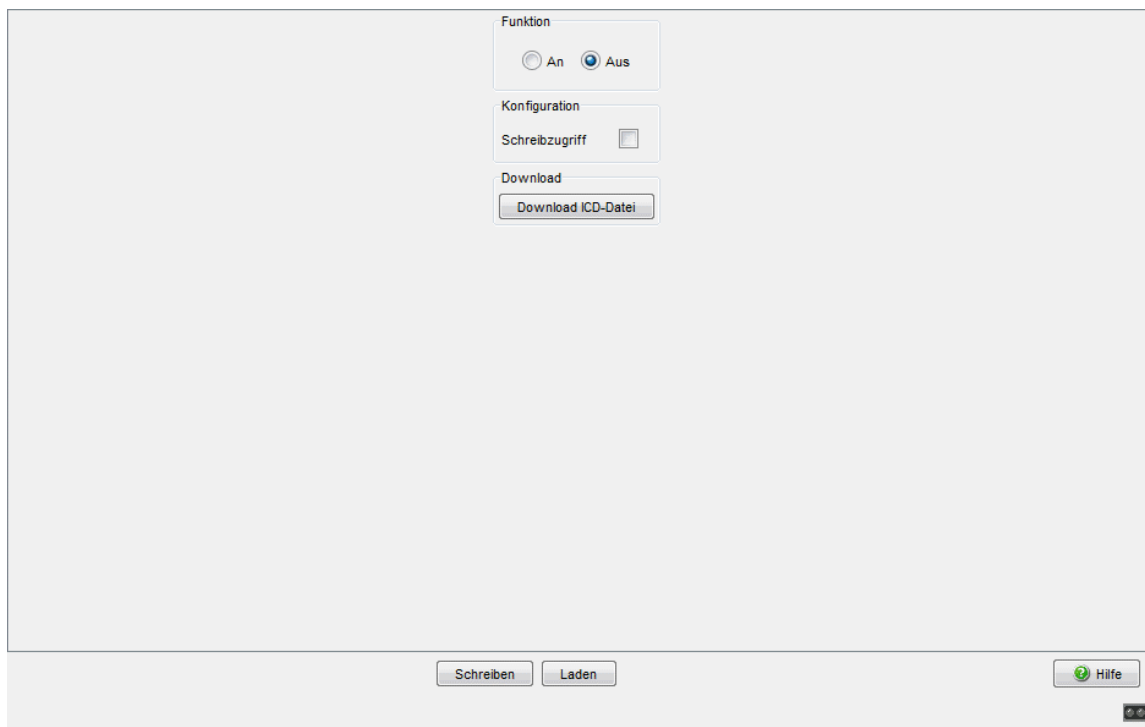


Abb. 108: Dialog *Erweitert:Industrie-Protokolle:IEC61850*

■ Schaltflächen

Schaltfläche	Bedeutung
Schreiben	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Gerätes. Um die Änderungen permanent zu speichern, öffnen Sie den Dialog <i>Grundeinstellungen:Laden/Speichern</i> , 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. 215: *Schaltflächen*

8.3.4 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-Medienmodul Digital I/O MICE-Medienmodul Digital 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.

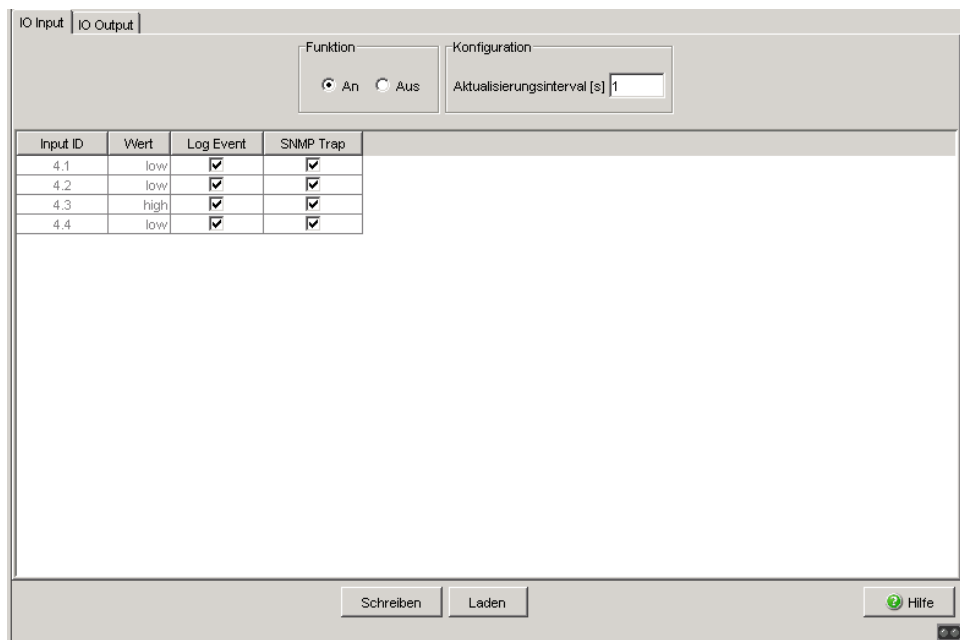


Abb. 109: Dialog IO Input

Funktion

Parameter	Bedeutung	Wertebereich	Voreinstellung
Funktion	Schaltet das zyklische Abfragen der digitalen Eingänge (IO Input) an oder aus.	An, Aus	Aus

Tab. 216: 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. 217: 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. <ul style="list-style-type: none"> - 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. 218: IO Input-Tabelle

Parameter	Bedeutung	Wertebereich	Voreinstellung
Log Event	<p>Aktiviert/deaktiviert die Logging-Funktion für Input-Statusänderungen.</p> <ul style="list-style-type: none"> – An: Das Gerät prüft den Status der digitalen Eingänge des Digital I/O MICE-Medienmoduls in regelmäßigen Zeitabständen gemäß Ihrer Einstellung im Eingabefeld „Aktualisierungsintervall [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	<p>Aktiviert oder deaktiviert das Senden von SNMP-Traps bei Input-Statusänderungen.</p> <ul style="list-style-type: none"> – An: Das Gerät prüft den Status der digitalen Eingänge des Digital I/O MICE-Medienmoduls in regelmäßigen Zeitabständen gemäß Ihrer Einstellung im Eingabefeld „Aktualisierungsintervall [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. 218: 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 221).

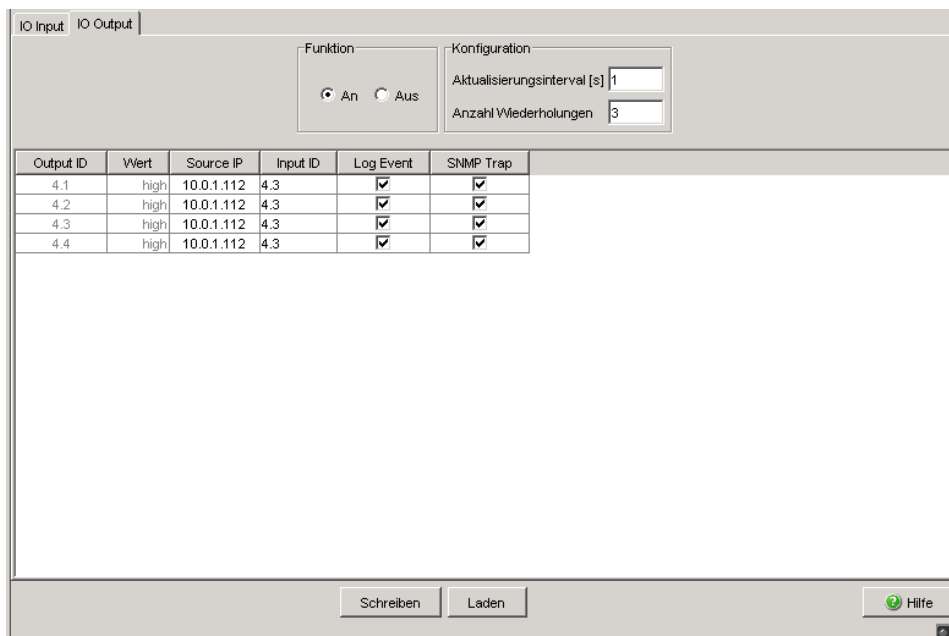


Abb. 110: Dialog IO Output

Funktion

Parameter	Bedeutung	Mögliche Werte	Lieferzustand
Funktion	Schaltet das zyklische Setzen der digitalen Ausgänge (IO Output) an oder aus.	An Aus	Aus

Tab. 219: 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
Aktualisierungsintervall [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. 220: 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 Ausganges 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. <ul style="list-style-type: none"> - 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. 221: IO Output-Tabelle

Parameter	Bedeutung	Wertebereich	Voreinstellung
Log Event	<p>Aktiviert/deaktiviert die Logging-Funktion für Output-Statusänderungen.</p> <ul style="list-style-type: none"> – An: Das Gerät prüft den Status der digitalen Eingänge des Digital I/O MICE-Medienmoduls in regelmäßigen Zeitabständen gemäß der Einstellung im Eingabefeld „Aktualisierungsintervall [s]“. Wenn das Gerät eine Änderung bei einem dieser IO-Output Werte erkennt, schreibt es einen Eintrag in seinen Ereignis-Log. Der Dialog <code>Diagnose:Bericht:EventLog</code> zeigt diese Einträge an. – Aus: Das Gerät schreibt bei einer Output-Statusänderung keinen Eintrag in seinen Ereignis-Log. 	An, Aus	Aus
SNMP Trap	<p>Aktiviert oder deaktiviert das Senden von SNMP-Traps bei Output-Statusänderungen.</p> <ul style="list-style-type: none"> – An: Das Gerät prüft den Status der digitalen Eingänge des Digital I/O MICE-Medienmoduls in regelmäßigen Zeitabständen gemäß der Einstellung im Eingabefeld „Aktualisierungsintervall [s]“. Wenn das Gerät eine Änderung bei einem dieser IO-Output Werte erkennt, sendet es einen SNMP-Trap. – Aus: Das Gerät sendet bei einer Output-Statusänderung keinen SNMP-Trap. 	An, Aus	Aus

Tab. 221: IO Output-Tabelle

Anmerkung: Wenn das Gerät den digitalen Eingang des Digital I/O MICE-Medienmoduls nicht einlesen kann, schreibt es einen Eintrag in seinen Ereignis-Log. Mögliche Ursache: Das Gerät ist nicht erreichbar oder die Konfiguration ist inkorrekt.

8.4 DIP-Switch via Software überschreiben (Mice, PowerMICE und RS)

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. 222: Rahmen „Funktion“ im Dialog *Erweitert:DIP-Switch*

Parameter	Bedeutung	Wertebereich	Voreinstellung
Konflikt mit Hardware-Einstellungen	<p>Zeigt Konflikte zwischen den Einstellungen der DIP-Switches auf dem Gerät und den Software-Einstellungen.</p> <p>Aktiv: Konflikt zwischen den Einstellungen der DIP-Switches auf dem Gerät und den Software-Einstellungen.</p> <p>Inaktiv: Kein Konflikt.</p>	Aktiv, inaktiv	-
DIP-Switch An (Mice)	<p>Zeigt die Einstellung des DIP-Switches, der die Einstellung der anderen DIP-Switches auf dem Gerät aktiviert/deaktiviert.</p> <p>Aktiv: Der DIP-Switch auf dem Gerät ist so eingestellt, dass das Gerät die DIP-Switch-Einstellungen verwendet. Voraussetzung ist, dass im Rahmen „Funktion“ der Wert An ausgewählt ist.</p> <p>Inaktiv: Der DIP-Switch auf dem Gerät ist so eingestellt, dass das Gerät die Software-Einstellungen verwendet.</p>	Aktiv, inaktiv	-
Ringmanager An (Mice, RS)	<p>Zeigt die Einstellung des DIP-Switches für die Ring-Manager-Funktion.</p> <p>Aktiv: Der DIP-Switch auf dem Gerät ist so eingestellt, dass die Ring-Manager-Funktion im Gerät aktiviert ist. Voraussetzung ist, dass im Rahmen „Funktion“ der Wert An ausgewählt ist und „DIP-Switch An“ aktiv ist.</p> <p>Inaktiv: Der DIP-Switch auf dem Gerät ist so eingestellt, dass das Gerät die Software-Einstellungen für die Ring-Manager-Funktion verwendet.</p>	Aktiv, inaktiv	-

Tab. 223: Rahmen „DIP-Switch Zustand“ im Dialog *Erweitert:DIP-Switch*

Parameter	Bedeutung	Wertebereich	Voreinstellung
Standby An (Mice, RS)	<p>Zeigt die Einstellung des DIP-Switches für den STAND-BY-Schalter. Mit dem STAND-BY-Schalter legen Sie fest, ob das Gerät innerhalb einer Ring-/Netzkopplung die Haupt- oder die redundante Kopplungs-Rolle ausführt.</p> <p>Aktiv: Der DIP-Switch auf dem Gerät ist so eingestellt, dass das Gerät die Haupt-Kopplungs-Rolle ausführt. Voraussetzung ist, dass im Rahmen „Funktion“ der Wert <code>An</code> ausgewählt ist und „DIP-Switch An“ aktiv ist.</p> <p>Inaktiv: Der DIP-Switch auf dem Gerät ist so eingestellt, dass das Gerät die redundante Kopplungs-Rolle ausführt. Voraussetzung ist, dass im Rahmen „Funktion“ der Wert <code>An</code> ausgewählt ist und „DIP-Switch An“ aktiv ist.</p>	Aktiv, inaktiv	-
Ring Ports (Mice)	<p>Zeigt die Einstellung des DIP-Switches für die Auswahl der Ring-Ports.</p> <p>1.1 & 1.2: Der DIP-Switch auf dem Gerät ist so eingestellt, dass das Gerät die Ports 1.1 & 1.2 als Ring-Ports verwendet. Voraussetzung ist, dass im Rahmen „Funktion“ der Wert <code>An</code> ausgewählt ist und „DIP-Switch An“ aktiv ist.</p> <p>2.1 & 2.2: Der DIP-Switch auf dem Gerät ist so eingestellt, dass das Gerät die Ports 2.1 & 2.2 als Ring-Ports verwendet. Voraussetzung ist, dass im Rahmen „Funktion“ der Wert <code>An</code> ausgewählt ist und „DIP-Switch An“ aktiv ist.</p>	1.1 & 1.2 2.1 & 2.2	-

Tab. 223: Rahmen „DIP-Switch Zustand“ im Dialog *Erweitert:DIP-Switch*

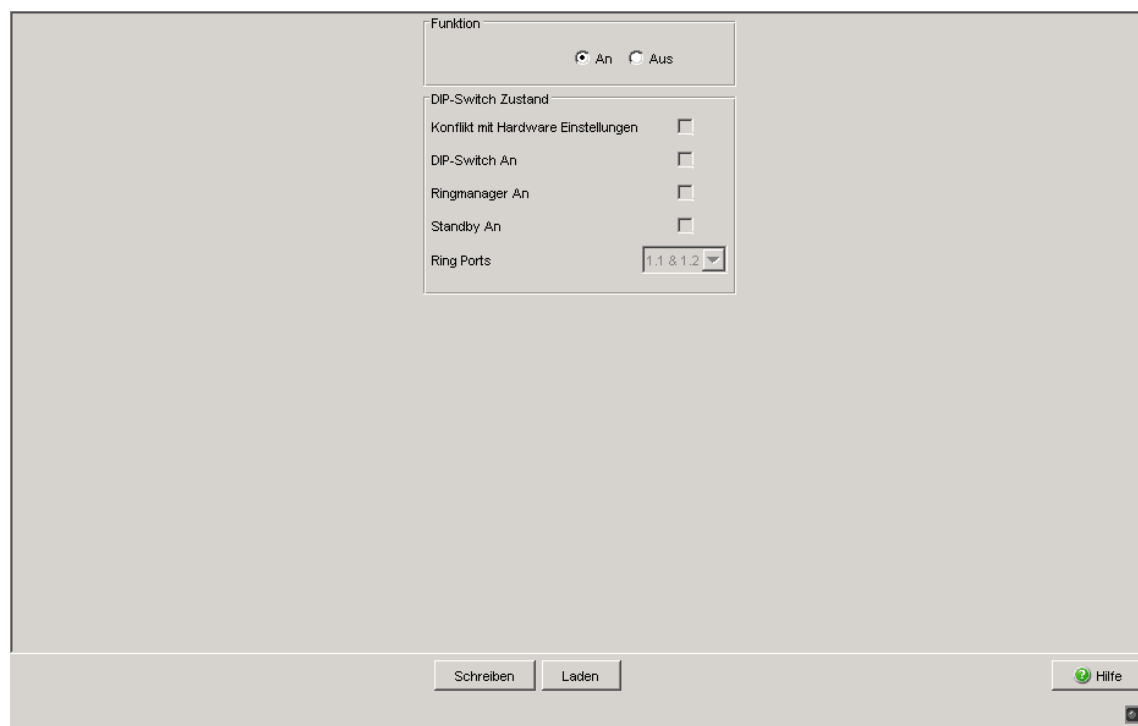


Abb. 111: Dialog *Erweitert:DIP-Switch*

■ 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 <i>Grundeinstellungen:Laden/Speichern</i> 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. 224: *Schaltflächen*

8.5 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. 225: 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	512 (RS20/RS30/RS40, RSR20/RSR30, MS20/MS30, OCTOPUS, MACH 100, MACH 1000) 1.000 (PowerMICE, MACH 104, MACH 1040, MACH 4000)
Max. Länge überlanger Pakete	<ul style="list-style-type: none"> – 1.632 Bytes (RS20/RS30/RS40, RSR20/RSR30, MS20/MS30, OCTOPUS, MACH 100, MACH 1000) – 1.552 Bytes (PowerMICE) – 9.022 Bytes (MACH 104, MACH 1040, MACH 4000)

VLAN	
VLAN-ID	1 bis 4.042
Anzahl VLANs	max. 255 gleichzeitig pro Gerät (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 gleichzeitig pro Gerät) max. 255 gleichzeitig pro Port (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 gleichzeitig pro Port)
Anzahl VLANs im GMRP in VLAN 1	max. 255 gleichzeitig pro Gerät (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 gleichzeitig pro Gerät) max. 255 gleichzeitig pro Port (PowerMICE, MACH 104, MACH 1040, MACH 4000: 256 gleichzeitig pro Port)

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	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lesbarkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verständlichkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Beispiele	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Aufbau	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vollständigkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Grafiken	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Zeichnungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tabellen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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	220		
802.1X	98		
802.1X-Authentifizierung (Voice-VLAN)	205		
A			
ACA (AutoConfiguration Adapter)	52, 344		
Acceptable Frame Types	199		
Address Conflict Detection (ACD)	351		
AF	223		
Aging Time	164		
Alarm	343		
Anforderungsintervall (SNTP)	136		
Assured Forwarding	223		
AutoConfiguration Adapter (ACA)	344		
B			
Bedienhinweise (GUI)	18		
Bericht	346		
BPDU-Guard	266		
Broadcast-Limiter	173, 175		
C			
Cable-Crossing	38		
CLI	401		
Class Selector	223		
Command Line Interface	401		
D			
DHCP-Relay-Agent	366		
DHCP-Server	371		
DHCP-Server (Lease-Tabelle)	379		
DHCP-Server-Pool	374		
DIP-Schalter	233		
Diagnose	291		
DiffServ	209		
DSCP	209		
E			
EF	223		
Eingeschränkter Management-Zugriff	85		
Ein-Switch-Kopplung	256		
Empfangsleistungs-Status	344		
Ereignis-Log	296		
Erweitert	365		
EtherNet/IP	385		
Expedited Forwarding	223		
F			
FAQ	419		
Fast HIPER-Ring konfigurieren	244		
Fast HIPER-Ring (Port-VLAN-ID)	201		
Filter für MAC-Adressen	168		
Forward Delay	265, 267		
G			
Grafische Benutzeroberfläche starten	15		
Grafische Benutzeroberfläche (GUI)	15		
Grandmaster	152		
Grundeinstellungen	21		
H			
Hardware-Uhr (gepuffert)	132		
Hello Time	264, 267		
HIPER-Ring	198, 233		
HIPER-Ring konfigurieren	233		
HIPER-Ring (Quelle für Alarme)	344		
HiView	15		
I			
IGMP-Einstellungen	178		
IGMP-Querier	178		
IGMP-Snooping	178		
Independent VLAN	191		
Industrial HiVision	12		
Industrieprotokolle	11, 382		
Ingress Filtering	199		
IP-DSCP Wert	210		
IP-DSCP-Mapping	209, 222		
J			
Java Runtime Environment	21		
K			
Kaltstart	68		
Kaltstart (nach dem Software-Update)	34, 35		
Konfigurationsprofil speichern (GUI)	19		
Konfigurations-Check	322		
L			
LACP Link Aggregation Control Protocol	226		
Lastbegrenzer Einstellungen	173, 175		
Lieferzustand wiederherstellen	52		
Link Aggregation	225, 228		
LLDP	322, 325		
LLDP-MED (Voice-VLAN)	204		

Login-Banner	125	Restricted Management Access	85
Login-Fenster	17	RFC	405
M		Ring	230
Max Age	265, 267	Ringmanager	230
Medienmodul (bei modularen Geräten)	23	Ringport	233
Meldekontakt	337	Ringstruktur	230
Meldekontakt (Quelle für Alarm)	344	Ring-Redundanz	225
MRP-Domäne	250, 251	Ring-/Netzkopplung	198, 225, 254, 336
MRP-Ring	198, 226, 237	Ring-/Netzkopplung (Quelle für Alarme)	344
MRP-Ring konfigurieren	237	RMON-Probe	331
Multicasts	177	RM-Funktion	230
Multiple Spanning Tree (MSTP)	260	Root-Bridge	261
N		S	
Netzlast	260, 300	Schulungsangebote	419
Netzmanagementstation	325	Selbsttest	357
Neustart	68	Service-Mode	359
P		SFP-Modul	302
Passwort	72, 74	SFP-Zustandsanzeige	302
Per-Hop-Behavior (PHB)	223	Shared VLAN	191
PHY Fast Startup pro Port	384	Sicherheit	71
Portkonfiguration	37	SNMPv1/v2-Zugriffs-Einstellungen	76
Portkonfiguration (QoS/Priorität)	214	SNMP-Logging	292
Ports	298	SNTP-Broadcasts	136
Portsicherheit (802.1X-basiert)	98	SNTP-Server	369
Portsicherheit (IP-/MAC-basiert)	89	Software-Update	32
Portsicherheit (Quelle für Alarme)	92, 96	Spanning Tree (STP)	260
Portstatistiken	298	SSH-Zugriff	80
Port-Mirroring	331	Statistiktafel	298
Port-Monitor	306	Statusleiste über Menü	18
Port-Priorität	214, 216	Sub-Ring konfigurieren	247, 248, 251
Port-VLAN-ID	199	Switching	163
Port-Zustand (Link)	37	Symbol	13
Power over ETHERNET	40	Syslog	292
PROFINET IO	11, 382	Systemvoraussetzungen (GUI)	15
Precedence	223	Systemzeit	136
Precision Time Protocol	139	T	
Pre-Login-Banner	125	Technische Fragen	419
Prioritäts-Queue	211	Telnet-Zugriff	80
PTP	139	Temperatur (Gerät)	23
Q		Temperatur (SFPs)	302
QoS/Priorität	209	Topologie	325
R		Topologie-Erkennung	322
RADIUS	117	ToS	209
RAM-Test	357	TP-Kabeldiagnose	303
Rapid Spanning Tree (RSTP)	260, 277	Trap	343
Reboot	68	Trunk	226
Redundanz	11, 225, 260	TrustDot1p (globaler Trust-Modus)	211, 218
Redundanzmanager	230	TrustIpDscp	211, 218
Referenzuhr	152	Trust Modus	214, 218
		TX Hold Count	265
		Type-of-Service	209

U

Uhr	139
Untrusted Traffic Class	214, 218
Untrusted (globaler Trust-Modus)	211, 218

V

Verbindungs-Zustand (Link)	37
Versorgungsspannung	344
VLAN	188
VLAN Aktuell Dialog	194
VLAN Global-Dialog	188
VLAN Modus	191
VLAN Port Dialog	199
VLAN Priorität	210
VLAN Statisch Dialog	196
VLAN und GOOSE Protokoll	190
VLAN und GVRP	200
VLAN und Redundanzringe	201
VLAN (HIPER-Ring)	235
VLAN-ID (Netzparameter)	29
VLAN-Mapping	209
Voice-VLAN	204
Voreinstellungen wiederherstellen	52

W

Web-Zugriff	80
-------------	----

Z

Zeit	131, 132
Zeitmanagement	139
Zeitstempelinheit	140
Zwei-Switch-Kopplung	256

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

**RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE,
RSR20/RSR30, MACH 100, MACH 1000, MACH 4000**

L2P Rel. 9.0

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

Content

Content	3
About this Manual	21
Maintenance	23
Service Shell	25
Permanently disabling the Service Shell	25
1 Command Structure	27
1.1 Format	28
1.1.1 Command	29
1.1.2 Parameters	29
1.1.3 Values	29
1.1.4 Conventions	31
1.1.5 Annotations	32
1.1.6 Special keys	33
1.1.7 Special characters in scripts	34
1.1.8 Secrets in scripts	36
2 Quick Start up	39
2.1 Quick Starting the Switch	40
2.2 System Info and System Setup	41
3 Mode-based CLI	47
3.1 Mode-based Topology	48
3.2 Mode-based Command Hierarchy	49
3.3 Flow of Operation	51
3.4 “No” Form of a Command	53
3.4.1 Support for “No” Form	53
3.4.2 Behavior of Command Help (“?”)	53

4	CLI Commands: Base	55
4.1	System Information and Statistics	56
4.1.1	show	56
4.1.2	show address-conflict	56
4.1.3	show arp switch	57
4.1.4	show bridge address-learning	57
4.1.5	show bridge address-relearn-detect	58
4.1.6	show bridge aging-time	58
4.1.7	show bridge duplex-mismatch-detect	59
4.1.8	show bridge fast-link-detection	59
4.1.9	show bridge framesize	59
4.1.10	show bridge vlan-learning	60
4.1.11	bridge framesize	60
4.1.12	show config-watchdog	61
4.1.13	show device-status	61
4.1.14	show authentication	62
4.1.15	show eventlog	63
4.1.16	show interface	64
4.1.17	show interface ethernet	66
4.1.18	show interface switchport	73
4.1.19	show interface utilization	74
4.1.20	show logging	75
4.1.21	show mac-address-conflict	76
4.1.22	show mac-addr-table	77
4.1.23	show signal-contact	78
4.1.24	show slot	80
4.1.25	show running-config	81
4.1.26	show sysinfo	82
4.1.27	show temperature	85
4.1.28	utilization alarm-threshold	85
4.2	Debug Commands	86
4.2.1	debug tcpdump help	86
4.2.2	debug tcpdump start cpu	86
4.2.3	debug tcpdump start cpu filter	87
4.2.4	debug tcpdump stop	87
4.2.5	debug tcpdump filter show	88
4.2.6	debug tcpdump filter list	88
4.2.7	debug tcpdump filter delete	89
4.3	Management VLAN Commands	90

4.3.1	network mgmt_vlan	90
4.4	Class of Service (CoS) Commands	91
4.4.1	classofservice dot1p-mapping	92
4.4.2	classofservice ip-dscp-mapping	93
4.4.3	classofservice trust	94
4.4.4	show classofservice dot1p-mapping	95
4.4.5	show classofservice ip-dscp-mapping	96
4.4.6	show classofservice trust	97
4.4.7	vlan port priority all	97
4.4.8	vlan priority	98
4.4.9	dvlan-tunnel ethertype	98
4.4.10	mode dvlan-tunnel	100
4.4.11	show dvlan-tunnel	101
4.5	Link Aggregation(802.3ad) Commands	102
4.5.1	link-aggregation staticcapability	102
4.5.2	show link-aggregation brief	103
4.6	Management Commands	104
4.6.1	telnet	104
4.6.2	transport input telnet	105
4.6.3	transport output telnet	106
4.6.4	session-limit	107
4.6.5	session-timeout	108
4.6.6	bridge address-learning	108
4.6.7	bridge address-relearn detect operation	109
4.6.8	bridge address-relearn detect threshold	109
4.6.9	bridge aging-time	110
4.6.10	bridge fast-link-detection	111
4.6.11	bridge duplex-mismatch-detect operation	111
4.6.12	bridge vlan-learning	112
4.6.13	digital-input	112
4.6.14	digital-output	114
4.6.15	show digital-input	117
4.6.16	show digital-input config	118
4.6.17	show digital-input all	119
4.6.18	show digital-input <slot/input>	120
4.6.19	show digital-output	121
4.6.20	show digital-output config	122
4.6.21	show digital-output all	123
4.6.22	show digital-output <slot/output>	124

4.6.23	ethernet-ip	125
4.6.24	iec61850-mms	126
4.6.25	show iec61850-mms	127
4.6.26	network mgmt-access add	128
4.6.27	network mgmt-access delete	128
4.6.28	network mgmt-access modify	129
4.6.29	network mgmt-access operation	130
4.6.30	network mgmt-access status	131
4.6.31	network parms	131
4.6.32	network protocol	132
4.6.33	network priority	133
4.6.34	profinetio	134
4.6.35	serial timeout	135
4.6.36	set prompt	135
4.6.37	show ethernet-ip	136
4.6.38	show network	136
4.6.39	show network mgmt-access	138
4.6.40	show profinetio	139
4.6.41	show serial	139
4.6.42	show snmp-access	140
4.6.43	show snmpcommunity	141
4.6.44	show snmp sync	142
4.6.45	show snmptrap	143
4.6.46	show telnet	144
4.6.47	show telnetcon	145
4.6.48	show trapflags	146
4.6.49	snmp-access global	147
4.6.50	snmp-access version	148
4.6.51	snmp-access version v3-encryption	149
4.6.52	snmp-server	150
4.6.53	snmp-server community	151
4.6.54	snmp-server contact	152
4.6.55	snmp-server community ipaddr	153
4.6.56	snmp-server community ipmask	154
4.6.57	snmp-server community mode	155
4.6.58	snmp-server community ro	156
4.6.59	snmp-server community rw	156
4.6.60	snmp-server location	156
4.6.61	snmp-server sysname	157
4.6.62	snmp-server enable traps	157
4.6.63	snmp-server enable traps chassis	158

4.6.64	snmp-server enable traps l2redundancy	159
4.6.65	snmp-server enable traps linkmode	160
4.6.66	snmp-server enable traps multiusers	161
4.6.67	snmp-server enable traps port-sec	162
4.6.68	snmp-server enable traps stpmode	163
4.6.69	snmptrap	164
4.6.70	snmptrap ipaddr	165
4.6.71	snmptrap mode	166
4.6.72	snmptrap snmpversion	167
4.6.73	telnetcon maxsessions	168
4.6.74	telnetcon timeout	169
4.7	Syslog Commands	170
4.7.1	logging buffered	170
4.7.2	logging buffered wrap	171
4.7.3	logging cli-command	172
4.7.4	logging console	173
4.7.5	logging host	174
4.7.6	logging host reconfigure	175
4.7.7	logging host remove	175
4.7.8	logging snmp-requests get operation	175
4.7.9	logging snmp-requests set operation	176
4.7.10	logging snmp-requests get severity	176
4.7.11	logging snmp-requests set severity	177
4.7.12	logging syslog	178
4.7.13	logging syslog port	178
4.8	Scripting Commands	179
4.8.1	script apply	179
4.8.2	script delete	180
4.8.3	script list	180
4.8.4	script show	181
4.8.5	script validate	181
4.9	Device Configuration Commands	183
4.9.1	addport	183
4.9.2	adminmode	184
4.9.3	auto-disable reason	185
4.9.4	auto-disable reset	187
4.9.5	auto-disable timer	187
4.9.6	auto-negotiate	188
4.9.7	auto-negotiate all	189

4.9.8	cable-crossing	190
4.9.9	media-module	191
4.9.10	deletport	192
4.9.11	deletport all	192
4.9.12	dip-switch operation	193
4.9.13	macfilter	194
4.9.14	macfilter adddest	195
4.9.15	macfilter adddest all	196
4.9.16	mac notification (Global Config)	197
4.9.17	mac notification (Interface Config)	198
4.9.18	monitor session <session-id>	199
4.9.19	monitor session <session-id> mode	201
4.9.20	monitor session <session-id> source/destination	202
4.9.21	link-aggregation	203
4.9.22	link-aggregation adminmode	204
4.9.23	link-aggregation linktrap	205
4.9.24	link-aggregation name	206
4.9.25	rmon-alarm add	206
4.9.26	rmon-alarm delete	207
4.9.27	rmon-alarm enable	207
4.9.28	rmon-alarm disable	208
4.9.29	rmon-alarm modify mib-variable	208
4.9.30	rmon-alarm modify thresholds	209
4.9.31	rmon-alarm modify interval	209
4.9.32	rmon-alarm modify sample-type	210
4.9.33	rmon-alarm modify startup-alarm	210
4.9.34	rmon-alarm modify rising-event	211
4.9.35	rmon-alarm modify falling-event	211
4.9.36	set garp timer join	212
4.9.37	set garp timer leave	213
4.9.38	set garp timer leaveall	214
4.9.39	set gmrp adminmode	215
4.9.40	set gmrp interfacemode	216
4.9.41	set gmrp interfacemode	217
4.9.42	set gmrp forward-all-groups	218
4.9.43	set gmrp forward-unknown	219
4.9.44	set igmp	220
4.9.45	set igmp	221
4.9.46	set igmp aging-time-unknown	221
4.9.47	set igmp automatic-mode	222
4.9.48	set igmp forward-all	223

4.9.49	set igmp forward-unknown	224
4.9.50	set igmp static-query-port	225
4.9.51	set igmp groupmembershipinterval	226
4.9.52	set igmp interfacemode	227
4.9.53	set igmp lookup-interval-unknown	228
4.9.54	set igmp lookup-resp-time-unknown	228
4.9.55	set igmp maxresponse	229
4.9.56	set igmp querier max-response-time	230
4.9.57	set igmp querier protocol-version	230
4.9.58	set igmp querier status	231
4.9.59	set igmp querier tx-interval	231
4.9.60	set igmp query-ports-to-filter	232
4.9.61	selftest ramtest	232
4.9.62	selftest reboot-on-hdxerror	233
4.9.63	selftest reboot-on-error	234
4.9.64	serviceshell	235
4.9.65	update module-configuration	235
4.9.66	show auto-disable brief	236
4.9.67	show auto-disable reasons	237
4.9.68	show dip-switch	238
4.9.69	show garp	239
4.9.70	show gmrp configuration	239
4.9.71	show igmpsnooping	240
4.9.72	show mac-filter-table gmrp	242
4.9.73	show mac-filter-table igmpsnooping	243
4.9.74	show mac-filter-table multicast	244
4.9.75	show mac-filter-table static	245
4.9.76	show mac-filter-table staticfiltering	246
4.9.77	show mac-filter-table stats	247
4.9.78	show mac notification	247
4.9.79	show monitor session	249
4.9.80	show port	250
4.9.81	show link-aggregation	251
4.9.82	show rmon-alarm	252
4.9.83	show selftest	253
4.9.84	show serviceshell	253
4.9.85	show storm-control	254
4.9.86	show storm-control limiters port	254
4.9.87	show vlan	255
4.9.88	show vlan brief	257
4.9.89	show vlan port	258

4.9.90	show voice vlan	259
4.9.91	show voice vlan interface	260
4.9.92	shutdown	261
4.9.93	shutdown all	262
4.9.94	snmp sync community-to-v3	263
4.9.95	snmp sync v3-to-community	264
4.9.96	snmp trap link-status	264
4.9.97	snmp trap link-status all	265
4.9.98	spanning-tree bpdumigrationcheck	266
4.9.99	speed	267
4.9.100	storm-control broadcast	268
4.9.101	storm-control egress-limiting	268
4.9.102	storm-control ingress-limiting	269
4.9.103	storm-control ingress-mode	269
4.9.104	storm-control broadcast (port-related)	270
4.9.105	storm-control egress-limit	270
4.9.106	storm-control ingress-limit	271
4.9.107	storm-control ingress-mode	271
4.9.108	storm-control flowcontrol	272
4.9.109	storm-control flowcontrol per port	273
4.9.110	vlan	274
4.9.111	vlan0-transparent-mode	275
4.9.112	vlan acceptframe	276
4.9.113	vlan database	277
4.9.114	vlan ingressfilter	278
4.9.115	vlan name	279
4.9.116	vlan participation	280
4.9.117	vlan participation all	281
4.9.118	vlan port acceptframe all	282
4.9.119	vlan port ingressfilter all	283
4.9.120	vlan port pvid all	284
4.9.121	vlan port tagging all	285
4.9.122	vlan pvid	286
4.9.123	vlan tagging	287
4.9.124	voice vlan (Global Config Mode)	288
4.9.125	voice vlan <id>	289
4.9.126	voice vlan dot1p	290
4.9.127	voice vlan none	290
4.9.128	voice vlan untagged	291
4.9.129	voice vlan auth	291

4.10	User Account Management Commands	292
4.10.1	disconnect	292
4.10.2	show loginsession	293
4.10.3	show users	294
4.10.4	users defaultlogin	295
4.10.5	users login <user>	296
4.10.6	users access	297
4.10.7	users name	298
4.10.8	users passwd	299
4.10.9	users snmpv3 accessmode	300
4.10.10	users snmpv3 authentication	301
4.10.11	users snmpv3 encryption	302
4.11	System Utilities	303
4.11.1	address-conflict	303
4.11.2	boot skip-aca-on-boot	304
4.11.3	show boot skip-aca-on-boot	304
4.11.4	cablestatus	305
4.11.5	clear eventlog	305
4.11.6	traceroute	306
4.11.7	clear arp-table-switch	306
4.11.8	clear config	307
4.11.9	clear config factory	307
4.11.10	clear counters	307
4.11.11	clear hiper-ring	308
4.11.12	clear igmpsnooping	308
4.11.13	clear mac-addr-table	309
4.11.14	clear pass	309
4.11.15	clear link-aggregation	310
4.11.16	clear signal-contact	310
4.11.17	clear traplog	311
4.11.18	clear ring-coupling	311
4.11.19	clear vlan	311
4.11.20	config-watchdog	312
4.11.21	copy	312
4.11.22	device-status connection-error	321
4.11.23	device-status monitor	322
4.11.24	logout	323
4.11.25	mac-address conflict operation	323
4.11.26	ping	324
4.11.27	signal-contact connection-error	324

4.11.28	signal-contact	325
4.11.29	temperature	326
4.11.30	reboot	327
4.11.31	show reboot	328
4.11.32	reload	329
4.11.33	show reload	330
4.11.34	set clibanner	331
4.11.35	set pre-login-banner	333
4.12	LLDP - Link Layer Discovery Protocol	335
4.12.1	show lldp	335
4.12.2	show lldp config	335
4.12.3	show lldp config chassis	336
4.12.4	show lldp config chassis admin-state	336
4.12.5	show lldp config chassis notification-interval	336
4.12.6	show lldp config chassis re-init-delay	337
4.12.7	show lldp config chassis tx-delay	337
4.12.8	show lldp config chassis tx-hold-mult	337
4.12.9	show lldp config chassis tx-interval	338
4.12.10	show lldp config port	339
4.12.11	show lldp config port tlv	340
4.12.12	show lldp med	341
4.12.13	show lldp med interface	342
4.12.14	show lldp med local-device detail	343
4.12.15	show lldp med remote-device	344
4.12.16	show lldp med remote-device detail	345
4.12.17	show lldp remote-data	345
4.12.18	lldp	347
4.12.19	lldp config chassis admin-state	348
4.12.20	lldp config chassis notification-interval	348
4.12.21	lldp config chassis re-init-delay	349
4.12.22	lldp config chassis tx-delay	349
4.12.23	lldp config chassis tx-hold-mult	350
4.12.24	lldp chassis tx-interval	350
4.12.25	clear lldp config all	351
4.12.26	lldp admin-state	351
4.12.27	lldp fdb-mode	352
4.12.28	lldp hm-mode	352
4.12.29	lldp max-neighbors	353
4.12.30	lldp med	354
4.12.31	lldp med all	355

4.12.32	lldp med confignotification	355
4.12.33	lldp med confignotification all	356
4.12.34	lldp med faststartrepeatcount	357
4.12.35	lldp med transmit-tlv	358
4.12.36	lldp med transmit-tlv all	359
4.12.37	lldp notification	360
4.12.38	lldp tlv link-aggregation	360
4.12.39	lldp tlv mac-phy-config-state	360
4.12.40	lldp tlv max-frame-size	361
4.12.41	lldp tlv mgmt-addr	361
4.12.42	lldp tlv pnio	361
4.12.43	lldp tlv pnio-alias	362
4.12.44	lldp tlv pnio-mrp	362
4.12.45	lldp tlv port-desc	362
4.12.46	lldp tlv port-vlan	363
4.12.47	lldp tlv gmrp	363
4.12.48	lldp tlv igmp	363
4.12.49	lldp tlv portsec	364
4.12.50	lldp tlv ptp	364
4.12.51	lldp tlv protocol	364
4.12.52	lldp tlv sys-cap	365
4.12.53	lldp tlv sys-desc	365
4.12.54	lldp tlv sys-name	365
4.12.55	lldp tlv vlan-name	366
4.12.56	name	366
4.13	SNTP - Simple Network Time Protocol	367
4.13.1	show sntp	367
4.13.2	show sntp anycast	369
4.13.3	show sntp client	369
4.13.4	show sntp operation	370
4.13.5	show sntp server	371
4.13.6	show sntp status	371
4.13.7	show sntp time	372
4.13.8	no sntp	372
4.13.9	sntp anycast address	373
4.13.10	sntp anycast transmit-interval	373
4.13.11	sntp anycast vlan	374
4.13.12	sntp client accept-broadcast	374
4.13.13	sntp client disable-after-sync	375
4.13.14	sntp client offset	375

4.13.15	sntp client request-interval	376
4.13.16	no sntp client server	376
4.13.17	sntp client server primary	377
4.13.18	sntp client server secondary	378
4.13.19	sntp client threshold	379
4.13.20	sntp operation	380
4.13.21	sntp server disable-if-local	381
4.13.22	sntp time system	381
4.14	PTP - Precision Time Protocol	382
4.14.1	show ptp	382
4.14.2	show ptp configuration	385
4.14.3	show ptp operation	385
4.14.4	show ptp port	386
4.14.5	show ptp status	387
4.14.6	ptp clock-mode	388
4.14.7	ptp operation	389
4.14.8	ptp sync-lower-bound	389
4.14.9	ptp sync-upper-bound	390
4.14.10	ptp v1 preferred-master	390
4.14.11	ptp v1 re-initialize	391
4.14.12	ptp v1 subdomain-name	391
4.14.13	ptp v1 sync-interval	392
4.14.14	ptp v2bc priority1	393
4.14.15	ptp v2bc priority2	393
4.14.16	ptp v2bc domain	394
4.14.17	ptp v2bc utc-offset	394
4.14.18	ptp v2bc utc-offset-valid	394
4.14.19	ptp v2bc vlan	395
4.14.20	ptp v2bc vlan-priority	395
4.14.21	ptp v1 burst	396
4.14.22	ptp v1 operation	396
4.14.23	ptp v2bc operation	397
4.14.24	ptp v2bc announce-interval	397
4.14.25	ptp v2bc announce-timeout	398
4.14.26	ptp v2bc sync-interval	398
4.14.27	ptp v2bc delay-mechanism	398
4.14.28	ptp v2bc pdelay-interval	399
4.14.29	ptp v2bc network-protocol	399
4.14.30	ptp v2bc v1-compatibility-mode	399
4.14.31	ptp v2bc asymmetry	400

4.14.32	ptp v2tc asymmetry	400
4.14.33	ptp v2tc delay-mechanism	400
4.14.34	ptp v2tc management	401
4.14.35	ptp v2tc multi-domain-mode	401
4.14.36	ptp v2tc network-protocol	402
4.14.37	ptp v2tc operation	402
4.14.38	ptp v2tc pdelay-interval	403
4.14.39	ptp v2tc primary-domain	403
4.14.40	ptp v2tc profile	404
4.14.41	ptp v2tc syntonization	404
4.14.42	ptp v2tc vlan	405
4.14.43	ptp v2tc power-tlv-check	405
4.14.44	ptp v2tc vlan-priority	406
4.14.45	ptp v2tc sync-local-clock	406
4.15	PoE - Power over Ethernet	407
4.15.1	show inlinepower	407
4.15.2	show inlinepower port	408
4.15.3	inlinepower (Global Config)	411
4.15.4	inlinepower (Interface Config)	412
4.15.5	clear inlinepower	413
4.16	PoE+ - Power over Ethernet Plus	414
4.16.1	show inlinepower slot	414
4.16.2	inlinepower budget slot	415
4.16.3	inlinepower threshold slot	416
4.16.4	inlinepower trap slot	416
4.17	Port monitor	417
4.17.1	show port-monitor	418
4.17.2	show port-monitor <slot/port>	419
4.17.3	show port-monitor brief	420
4.17.4	show port-monitor crc-fragment	421
4.17.5	show port-monitor link-flap	421
4.17.6	show port-monitor overload-detection	422
4.17.7	show port-monitor speed-duplex	423
4.17.8	port-monitor (Global Config)	424
4.17.9	port-monitor (Interface Config)	424
4.17.10	port-monitor action	425
4.17.11	port-monitor condition overload-detection polling-interval (Global Config)	426

4.17.12	port-monitor condition overload-detection (Interface Config)	426
4.17.13	show port-monitor overload-detection	428
4.17.14	port-monitor condition link-flap (Global Config)	429
4.17.15	port-monitor condition link-flap (Interface Config)	429
4.17.16	port-monitor condition crc-fragment (Global Config)	430
4.17.17	port-monitor condition crc-fragment (Interface Config)	431
4.17.18	port-monitor condition speed-duplex-monitor (Interface Config)	431
4.17.19	port-monitor condition speed-duplex-monitor speed (Interface Config)	432
4.17.20	port-monitor condition speed-duplex-monitor clear (Interface Config)	432
5	CLI Commands: Switching	433
5.1	Spanning Tree Commands	435
5.1.1	show spanning-tree	435
5.1.2	show spanning-tree interface	438
5.1.3	show spanning-tree mst detailed	439
5.1.4	show spanning-tree mst port detailed	440
5.1.5	show spanning-tree mst port summary	443
5.1.6	show spanning-tree mst summary	444
5.1.7	show spanning-tree summary	445
5.1.8	show spanning-tree vlan	446
5.1.9	spanning-tree	447
5.1.10	spanning-tree auto-edgeport	448
5.1.11	spanning-tree bpduguard	449
5.1.12	spanning-tree configuration name	450
5.1.13	spanning-tree configuration revision	451
5.1.14	spanning-tree edgeport	452
5.1.15	spanning-tree forceversion	453
5.1.16	spanning-tree forward-time	454
5.1.17	spanning-tree guard loop	455
5.1.18	spanning-tree guard none	456
5.1.19	spanning-tree guard root	457
5.1.20	spanning-tree hello-time	458
5.1.21	spanning-tree hold-count	458
5.1.22	spanning-tree max-age	459
5.1.23	spanning-tree max-hops	460
5.1.24	spanning-tree mst	461

5.1.25	spanning-tree mst priority	463
5.1.26	spanning-tree mst vlan	464
5.1.27	spanning-tree mst instance	465
5.1.28	spanning-tree port mode	466
5.1.29	spanning-tree port mode all	467
5.1.30	spanning-tree stp-mrp-mode	468
5.1.31	spanning-tree tcnguard	469
5.2	MRP	470
5.2.1	show mrp	470
5.2.2	show mrp current-domain	471
5.2.3	mrp current-domain	472
5.2.4	mrp delete-domain	474
5.2.5	mrp new-domain	474
5.2.6	arc	475
5.2.7	show arc	476
5.3	HIPER-Ring	478
5.3.1	show hiper-ring	479
5.3.2	hiper-ring	480
5.3.3	hiper-ring mode	480
5.3.4	hiper-ring port primary	481
5.3.5	hiper-ring port secondary	481
5.3.6	hiper-ring recovery-delay	482
5.4	Fast-HIPER-Ring	483
5.4.1	show fast-hiper-ring (MACH1000, RSR20/RSR30)	484
5.4.2	show fast-hiper-ring current-id (MACH1000, RSR20/RSR30)	485
5.4.3	fast-hiper-ring	486
5.5	Redundant Coupling	488
5.5.1	show ring-coupling	489
5.5.2	ring-coupling	491
5.5.3	ring-coupling config	492
5.5.4	ring-coupling net-coupling	493
5.5.5	ring-coupling operation	493
5.5.6	ring-coupling port	494
5.5.7	ring-coupling redundancy-mode	494
5.6	Port Security	495
5.6.1	show port-sec dynamic	495
5.6.2	show port-sec mode	496
5.6.3	show port-sec port	497

5.6.4	port-sec mode	497
5.6.5	port-sec action	498
5.6.6	port-sec allowed-ip	499
5.6.7	port-sec allowed-ip add	499
5.6.8	port-sec allowed-ip remove	500
5.6.9	port-sec allowed-mac	500
5.6.10	port-sec allowed-mac add	501
5.6.11	port-sec allowed-mac remove	501
5.6.12	port-sec dynamic	502
5.6.13	clear port-sec	502
5.7	DHCP Relay Commands	503
5.7.1	dhcp-relay	504
5.7.2	dhcp-relay	505
5.7.3	show dhcp-relay	506
5.8	DHCP Server Commands	508
5.8.1	DHCP server configuration example	508
5.8.2	show dhcp-server	510
5.8.3	show dhcp-server operation	511
5.8.4	show dhcp-server port	511
5.8.5	show dhcp-server pool	512
5.8.6	dhcp-server addr-probe	512
5.8.7	dhcp-server operation	513
5.8.8	dhcp-server pool add <id>	513
5.8.9	dhcp-server pool modify <id> mode	514
5.8.10	dhcp-server pool modify <id> option	516
5.8.11	dhcp-server pool modify leasetime	517
5.8.12	dhcp-server pool modify <id> hirschmann-device	517
5.8.13	dhcp-server pool enable	518
5.8.14	dhcp-server pool disable	518
5.8.15	dhcp-server pool delete	518
5.9	Sub-Ring Commands	519
5.9.1	show sub-ring	519
5.9.2	sub-ring <id> mode	521
5.9.3	sub-ring <id> operation	522
5.9.4	sub-ring <id> protocol	522
5.9.5	sub-ring <id> port	523
5.9.6	sub-ring <id> ring-name	523
5.9.7	sub-ring <id> vlan	524
5.9.8	sub-ring <id> mrp-domainID	525

5.9.9	sub-ring delete-ring	526
5.9.10	sub-ring new-ring	526
6	CLI Commands: Security	527
6.1	Security Commands	529
6.1.1	authentication login	529
6.1.2	authorization network radius	531
6.1.3	clear dot1x statistics	531
6.1.4	clear radius statistics	532
6.1.5	dot1x defaultlogin	532
6.1.6	dot1x dynamic-vlan enable	533
6.1.7	dot1x guest-vlan	534
6.1.8	dot1x initialize	535
6.1.9	dot1x login	535
6.1.10	dot1x mac-auth-bypass	536
6.1.11	dot1x max-req	537
6.1.12	dot1x max-users	538
6.1.13	dot1x port-control	539
6.1.14	dot1x port-control all	540
6.1.15	dot1x re-authenticate	541
6.1.16	dot1x re-authentication	541
6.1.17	dot1x safe-vlan	542
6.1.18	dot1x system-auth-control	543
6.1.19	dot1x timeout	543
6.1.20	dot1x timeout guest-vlan-period	545
6.1.21	dot1x unauthenticated-vlan	546
6.1.22	dot1x user	547
6.1.23	ip ssh protocol	548
6.1.24	radius accounting mode	549
6.1.25	radius server host	549
6.1.26	radius server key	551
6.1.27	radius server msgauth	551
6.1.28	radius server primary	552
6.1.29	radius server retransmit	553
6.1.30	radius server timeout	554
6.1.31	show radius accounting	554
6.1.32	show authentication	557
6.1.33	show authentication users	558
6.1.34	show dot1x	558
6.1.35	show dot1x users	563

6.1.36	show dot1x clients	564
6.1.37	show ip ssh	565
6.1.38	show radius	566
6.1.39	show radius statistics	567
6.1.40	show users authentication	569
6.1.41	users login	570
6.2	HTTP Commands	571
6.2.1	ip http server	571
6.2.2	show ip http	572
6.2.3	ip https server	573
6.2.4	ip https port	574
6.2.5	ip https certgen	574
6.2.6	show ip https	575
7	Appendix- VLAN Example	577
7.1	SOLUTION 1	579
7.2	SOLUTION 2	581
8	Index	583
9	Glossary	593
10	Further support	609

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 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

Commands are followed by values, parameters, or both.

■ 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 text in courier font is to be typed exactly as shown.

1.1.2 Parameters

Parameters are order dependent.

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`. The `|` indicates that only one of the parameters should be entered.
- ▶ The `{}` curly braces indicate that a parameter must be chosen from the list of choices.

1.1.3 Values

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.

slot/port

Valid slot and port number separated by forward slashes. For example, 1/1 represents slot number 1 and port number 1.

logical slot/port

Logical slot and port number. This is applicable in the case of a link-aggregation (LAG) and vlan router interfaces (9/x). The operator can use the logical slot/port to configure the link-aggregation.

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

The following list of special keys may be helpful to enter command lines.

BS	delete previous character
Ctrl-A	go to beginning of line
Ctrl-E	go to end of line
Ctrl-F	go forward one character
Ctrl-B	go backward one character
Ctrl-D	delete current character
Ctrl-H	display command history or retrieve a command
Ctrl-U, X	delete to beginning of line
Ctrl-K	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-R	rewrites or pastes the line
Ctrl-N	go to next line in history buffer
Ctrl-Y	print last deleted character
Ctrl-Q	enables serial flow
Ctrl-S	disables serial flow
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
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

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

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
<code>show port all</code> (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 9: Quick Start up Physical Port Data

■ Quick Start up User Account Management

Command	Details
<code>show users</code> (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.
<code>show login session</code> (in User EXEC)	Displays all of the login session information

Table 10: Quick Start up User Account Management

Command	Details
<pre>users passwd <user- name></pre> (in Global Config)	<p>Allows the user to set passwords or change passwords needed to login</p> <p>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.</p> <p>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.</p> <p>User password should not be more than eight characters in length.</p> <p>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.</p>
<pre>copy system:running- config nvram:startup-config</pre> (in Privileged EXEC)	<p>This will save passwords and all other changes to the device.</p> <p>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.</p>
<pre>logout</pre> (in User EXEC and Privileged EXEC)	<p>Logs the user out of the switch</p>

Table 10: Quick Start up User Account Management

■ Quick Start up IP Address

To view the network parameters the operator can access the device by the following three methods.

- ▶ Simple Network Management Protocol - SNMP
- ▶ Telnet
- ▶ 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)	<p>Displays the Network Configurations</p> <p>IP Address - IP Address of the switch Default IP is 0.0.0.0</p> <p>Subnet Mask - IP Subnet Mask for the switch Default is 0.0.0.0</p> <p>Default Gateway - The default Gateway for this switch Default value is 0.0.0.0</p> <p>Burned in MAC Address - The Burned in MAC Address used for in-band connectivity</p> <p>Network Configurations Protocol (BOOTP/DHCP) - Indicates which network protocol is being used Default is DHCP</p> <p>Network Configurations Protocol HiDiscovery - Indicates the status of the HiDiscovery protocol. Default is read-write</p> <p>Management VLAN Id - Specifies VLAN id</p> <p>Web Mode - Indicates whether HTTP/Web is enabled.</p> <p>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.</p>
network parms <ipaddr> <net-mask> [gateway] (in Privileged EXEC)	<p>Sets the IP Address, subnet mask and gateway of the router. The IP Address and the gateway must be on the same subnet.</p> <p>IP Address range from 0.0.0.0 to 255.255.255.255</p>

Table 11: Quick Start up IP Address

Command	Details
	Subnet Mask range from 0.0.0.0 to 255.255.255.255
	Gateway Address range from 0.0.0.0 to 255.255.255.255

Table 11: 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
<code>copy <url> {nvram:startup-config system:image}</code>	Sets the destination (download) datatype to be an image (system:image) or a configuration file (nvram:startup-config). The URL must be specified as: ftp://ipAddr/filepath/fileName. The nvram:startup-config option downloads the configuration file using tftp and system:image option downloads the code file.

Table 12: Quick Start up Downloading from TFTP Server

■ Quick Start up Factory Defaults

Command	Details
<code>clear config</code> (in Privileged EXEC Mode)	Enter yes when the prompt pops up to clear all the configurations made to the switch.
<code>copy system:running-config nvram:startup-config</code>	Enter yes when the prompt pops up that asks if you want to save the configurations made to the switch.
<code>reboot</code> (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 13: 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

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.
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.

Table 14: 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.

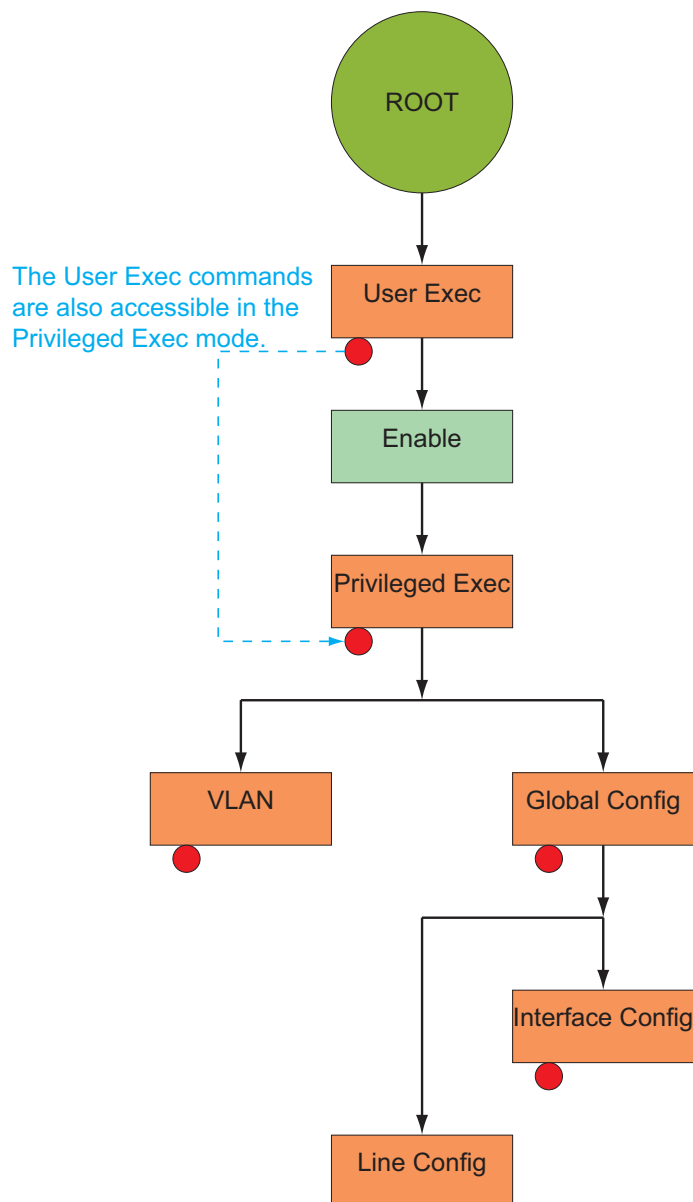


Fig. 1: Mode-based CLI

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 or enter 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) #
```

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 1632¹⁾ or 9022²⁾ as maximum size of frame (packet size).

Default

```
1522
```

Format

```
bridge framesize { 1522 | 16321) | 90222) }
```

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 multi-cast 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 multi-cast 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 242](#).

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 250](#)).

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 alphanumeric 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.
MAR1020-99TTTTMMMMTTTTTTTTTTTTTTTTTUC9HPHH

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 address.

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 iec61850-mms

Note: This command is available for the RSR20/RSR30 and MACH1000 devices.

This command is used to configure the IEC61850 MMS server functionality on this device.

Default

disable

Format

```
iec61850-mms { admin-state {enable | disable} |  
               write-access {enable | disable} }
```

Mode

Global Config

Admin-state

Disable: Disables the IEC61850 MMS Server functionality on this device. This is the default.

Note: The relevant MIB objects are still accessible.

Enable: Enables the IEC61850 MMS Server functionality on this device.

Write-access

Disable: Disables the write-access of the IEC61850 MMS Server on this device. This is the default.

Enable: Enables the write-access of the IEC61850 MMS Server on this device.

Note: Write-Access via the IEC61850 MMS Server will be non authenticated. This could be a possible security risk.

4.6.25 show iec61850-mms

Note: This command is available for the RSR20/RSR30 and MACH1000 devices.

This command is used to show the IEC61850 MMS server settings on this device.

Default

`disable`

Format

`show iec61850-mms`

Mode

Global Config

IEC61850 MMS Server Admin State

Display the IEC61850 MMS Server Admin State.

Possible values: `Enable`, `Disable`

IEC61850 MMS Server Write-Access State

Show the IEC61850 MMS Server Write-Access State.

Possible values: `Enable`, `Disable`

4.6.26 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.

4.6.27 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.

4.6.28 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.

4.6.29 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.

4.6.30 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.

4.6.31 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

4.6.32 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

4.6.33 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

4.6.34 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.

4.6.35 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

4.6.36 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

4.6.37 show ethernet-ip

This command displays the admin state of the EtherNet/IP function.

Format

```
show ethernet-ip
```

Mode

Privileged EXEC and User EXEC

4.6.38 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`.

4.6.39 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] | [].

4.6.40 show profinetio

This command displays the admin state of the PROFINET IO function.

Format

```
show profinetio
```

Mode

Privileged EXEC and User EXEC

4.6.41 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.

4.6.42 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
```

4.6.43 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.

4.6.44 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.

4.6.45 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.

4.6.46 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*.

4.6.47 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`.

4.6.48 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.

4.6.49 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.

4.6.50 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.

4.6.51 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 SNMPv3 protocol version.

readwrite

Enable SNMP read-write access to this switch (enable write access) by SNMPv3 protocol version.

4.6.52 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

4.6.53 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
```

4.6.54 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

4.6.55 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

4.6.56 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

4.6.57 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
```

4.6.58 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
```

4.6.59 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
```

4.6.60 snmp-server location

This command configures the system location.

Format

```
snmp-server location <system location>
```

Mode

```
Global Config
```

4.6.61 snmp-server sysname

This command configures the system name.

Format

```
snmp-server sysname <system name>
```

Mode

Global Config

4.6.62 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

4.6.63 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 SNMP 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

4.6.64 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

4.6.65 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

4.6.66 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

4.6.67 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

4.6.68 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

4.6.69 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

4.6.70 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.

4.6.71 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
```

4.6.72 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.

ipAddr

Enter the IP Address.

snmpv1

Use SNMP v1 to send traps.

snmpv2

Use SNMP v2 to send traps.

4.6.73 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

4.6.74 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 15

■ 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. 15: 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 port and 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 alphanumeric 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

This 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 forward-unknown

Note: This command is available for MS20/MS30.

This command defines how to handle unknown multicast frames.

Format

```
set igmp forward-unknown
                        { discard | flood | query-ports }
```

Mode

Global Config

discard

Unknown multicast frames will be discarded.

flood

Unknown multicast frames will be flooded.

query-ports

Unknown multicast frames will be forwarded only to query ports.

4.9.50 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

4.9.51 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

4.9.52 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
```

4.9.53 set igmp lookup-interval-unknown n

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).

4.9.54 set igmp lookup-resp-time-unknown n

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).

4.9.55 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

4.9.56 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.

4.9.57 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

4.9.58 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

4.9.59 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

4.9.60 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.

4.9.61 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.

4.9.62 selftest reboot-on-hdxerror

Enable or disable a restart when the device detects a half duplex mismatch error. Default value: `enabled`.

Format

```
selftest reboot-on-hdxerror {disable | enable}
```

Mode

```
Global Config
```

selftest reboot-on-hdxerror disable

Disable the reboot-on-hdxerror function.

selftest reboot-on-hdxerror enable

Enable the reboot-on-hdxerror function. This is the default.

4.9.63 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.

4.9.64 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.

4.9.65 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.

4.9.66 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.

4.9.67 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.

4.9.68 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`

4.9.69 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.

4.9.70 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.

4.9.71 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.

4.9.72 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:).

4.9.73 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:).

4.9.74 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.

4.9.75 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).

4.9.76 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:).

4.9.77 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.

4.9.78 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`.

4.9.79 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.

4.9.80 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.

4.9.81 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).

4.9.82 show rmon-alarm

This command displays switch configuration information.

Format

```
show rmon-alarm
```

Mode

Privileged EXEC and User EXEC

4.9.83 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.

4.9.84 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.

4.9.85 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.

4.9.86 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.

4.9.87 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.

4.9.88 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.

4.9.89 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.

4.9.90 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`

4.9.91 show voice vlan interface

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.

4.9.92 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

4.9.93 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

4.9.94 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
```

4.9.95 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
```

4.9.96 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
```

4.9.97 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
```


4.9.98 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

4.9.99 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.

4.9.100 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
```

4.9.101 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
```

4.9.102 storm-control ingress-limiting

This command enables or disables the ingress limiter globally.

Format

```
storm-control ingress-limiting {disable | enable}
```

Mode

```
Global Config
```

4.9.103 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
```

4.9.104 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
```

4.9.105 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
```

4.9.106 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
```

4.9.107 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
```

4.9.108 storm-control flow control

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 flow control

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

4.9.109 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

4.9.110 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
```

4.9.111 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
```

4.9.112 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
```

4.9.113 vlan database

This command switches into the global VLAN mode.

Default

```
Admit All
```

Format

```
vlan database
```

Mode

```
Privileged EXEC
```

4.9.114 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

4.9.115 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

4.9.116 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.

4.9.117 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.

4.9.118 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
```

4.9.119 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

4.9.120 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

4.9.121 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
```

4.9.122 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

4.9.123 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
```

4.9.124 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

4.9.125 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

4.9.126 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.

4.9.127 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
```

4.9.128 voice vlan untagged

Use this command to configure the phone to send untagged voice traffic.

Format

```
voice vlan untagged
```

Mode

```
Interface Config
```

4.9.129 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 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:https-cert
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. File-name 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:https-cert

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 exceed 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 331

■ **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 329. 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 scheduled), 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 327.](#)

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 348](#)).

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 (10⁹-1), 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 (10⁹), 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.

Condition overload-detection interval (seconds)

Note: This command is available for the MACH1040 and MACH104 devices.

Display the condition of the overload-detect interval in seconds.

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.

Overload detection

Note: This command is available for the MACH1040 and MACH104 devices.

Display the condition of the overload-detection state.

Possible values: Enabled, 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.

Overload detection

Note: This command is available for the MACH1040 and MACH104 devices.

Display the condition of the overload-detection state.

Possible values: Enabled, 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 overload-detection polling-interval (Global Config)

Note: This command is available for the MACH104 and MACH1040 devices. Use this command to configure the polling-interval in seconds for overload-detection condition.

Default

1

Format

```
port-monitor condition overload-detection
                polling-interval <interval value>
```

Mode

Global Config

<interval value>

Enter a polling-interval value for overload-detection.
Possible values: 1..20. Default: 1.

4.17.12 port-monitor condition overload-detection (Interface Config)

Note: This command is available for the MACH104 and MACH1040 devices. Use this command to configure the Port Monitor overload-detection settings.

Format

```
port-monitor condition overload-detection
{ [traffic-type bc | bc+mc | all] |
  [threshold-type pps | kbps | link-capacity ] |
  [lower-threshold <threshold value>] |
```

```
[upper-threshold <threshold value>] |  
{enable | disable}
```

Mode

Interface Config

traffic-type bc

Define traffic class for overload-detection: Broadcast traffic (`bc`).

traffic-type bc+mc

Define traffic class for overload-detection:
Broadcast and multicast traffic (`bc+mc`).

traffic-type all

Define traffic class for overload-detection: All traffic types (`all`).

threshold-type pps

Define threshold type for overload-detection condition:
Packets per second (`pps`).

threshold-type kbps

Define threshold type for overload-detection condition:
Kilobits per second (`kbps`).

threshold-type link-capacity

Define threshold type for overload-detection condition:
Link capacity percentage (% of the link capacity).

lower-threshold

Define the lower threshold value for overload-condition (packets per second, kbits or % of the link capacity) for different types of traffic.
<threshold value> Enter a lower-threshold value.
Possible values: 0..10000000.

upper-threshold

Define the upper threshold value for overload-condition (packets per second, kbits or % of the link capacity) for different types of traffic.
<threshold value> Enter a upper-threshold value.
Possible values: 0..10000000.

enable

Enable the overload-detection.

disable

Disable the overload-detection.

4.17.13 show port-monitor overload-detection

Note: This command is available for the MACH104 and MACH1040 devices. Use this command to display information about port-monitor overload-detection for a specific interface.

Default

1

Format

```
show port-monitor overload-detection <slot/port>
```

Mode

User EXEC and Privileged EXEC

<slot/port>

Valid slot and port number separated by forward slashes.

Overload-detection traffic type

Display the traffic type for the port monitor overload detection.

Possible values:

bc (broadcast traffic),

bc+mc (broadcast and multicast),

all (all traffic types).

Overload-detection threshold type

Display the threshold type for the port monitor overload detection.

Possible values:

pps (packets per second),

kbps (kilobits per second),

link-capacity (% of the link capacity).

Overload-detection lower threshold

Display the lower threshold for the port monitor overload detection.

Possible values: 0..10000000

Overload-detection upper threshold

Display the upper threshold for the port monitor overload detection.

Possible values: 0..10000000

4.17.14 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.

4.17.15 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

4.17.16 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.

4.17.17 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

4.17.18 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

4.17.19 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

4.17.20 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 $(\text{Bridge Max Age} / 2) + 1$.

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 to 127.

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".

5.4.1 **show fast-hiper-ring (MACH1000, RSR20/RSR30)**

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 the Fast-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.

5.4.2 show fast-hiper-ring current-id (MACH1000, RSR20/RSR30)

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.

5.4.3 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 Security 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 DHCP 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 DHCP 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 DHCP 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 Relay'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 DHCP server operation setting.

Possible values: *Enabled, Disabled*

DHCP Address Probe

Display the DHCP server address probe setting.

Possible values: *Enabled, Disabled*

DHCP, Port-Related Settings:

Port

Display the port number in <slot/port> notation.

Mode

Display the DHCP server interface information.

Possible values: *enable, disable*

DHCP, Pools:

Display the DHCP 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 DHCP server pool information for all IDs.

show dhcp-server pool <id>

Display the DHCP server pool information for the specified ID only.

5.8.6 dhcp-server addr-probe

Use this command to 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)
    | vlan {none | <vlan id >} }
```

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.

dhcp-server pool modify <id> mode vlan <vlan id> ¹⁾

Enter valid VLAN ID.

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

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`, `Timeout`, `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 571.

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 workgroups. This logical segmentation is commonly referred to 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)

VLAN	Command
create VLAN 2	<pre>vlan database vlan 2 exit config interface 1/1 vlan participation include 2 exit interface 1/2 vlan participation include 2 exit</pre>

Table 16: Creating VLANs

VLAN	Command
create VLAN 3	<pre> vlan database vlan 3 exit config interface 0/3 vlan participation include 3 exit interface 0/4 vlan participation include 3 exit </pre>
create VLAN 4	<pre> vlan database vlan 4 exit config interface 0/5 vlan participation include 4 exit interface 0/6 vlan participation include 4 exit </pre>
create VLAN 9	<pre> vlan database vlan 9 exit config interface 0/1 vlan participation include 9 exit interface 0/2 vlan participation include 9 exit interface 0/3 vlan participation include 9 exit interface 0/4 vlan participation include 9 exit interface 0/5 vlan participation include 9 exit interface 0/6 vlan participation include 9 exit interface 0/7 vlan participation include 9 exit </pre>

Table 16: Creating VLANs

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 Index

- A**
- addport 183
 - address-conflict 303
 - adminmode 184
 - arc 475
 - areaid 29
 - authentication login 529
 - authorization network radius 531
 - auto-disable reason 185
 - auto-disable reset 187
 - auto-disable timer 187
 - auto-negotiate 188
 - auto-negotiate all 189
- B**
- boot skip-aca-on-boot 304, 304
 - bridge address-learning 108
 - bridge address-relearn detect operation 109
 - bridge address-relearn detect threshold 109
 - bridge aging-time 110
 - bridge duplex-mismatch-detect operation 111
 - bridge fast-link-detection 111
 - bridge framesize 60
 - bridge vlan-learning 112
 - broadcasts
 - broadcast storm recovery mode 268, 269, 271
- C**
- cable-crossing 190
 - cablestatus 305
 - classofservice dot1p mapping 92
 - classofservice ip-dscp-mapping 93
 - classofservice trus 94
 - clear arp-table-switch 306
 - clear commands
 - clear arp-table-switch 306
 - clear config 307
 - clear pass 309
 - clear traplog 310, 311
 - clear vlan 311
 - clear config 307
 - clear config factory 307
 - clear counters 307
 - clear dot1x statistics 531
 - clear eventlog 305
 - clear hiper-ring 308
 - clear igmpsnooping 308
 - clear inlinepower 413
 - clear link-aggregation 310
 - clear lldp config all 351
 - clear mac-addr-table 309
 - clear pass 309
 - clear port-sec 502
 - clear radius statistics 532
 - clear ring-coupling 311
 - clear sfp-white-list 320
 - clear signal-contact 310
 - clear traplog 311
 - clear vlan 311
 - Competence Center 611
 - config commands
 - config lags adminmode 204
 - config lags linktrap 205
 - config lags name 206
 - config loginsession 292
 - config port admin-mode 261, 262
 - config port linktrap 263, 264, 265
 - config port physical-mode 267
 - config switchconfig broadcast 268, 269, 271
 - config switchconfig flowcontrol 272, 273
 - config users add 297, 298
 - config users delete 296, 297, 298
 - config users passwd 299
 - config vlan add 274
 - config vlan delete 274
 - config vlan garp jointime 206, 207, 208, 209, 210, 211, 212
 - config vlan garp leavealltime 214
 - config vlan garp leavetime 213
 - config vlan interface acceptframe 276, 277, 282
 - config vlan name 279
 - config vlan participation 280, 281
 - config vlan ports ingressfilter 278, 283
 - config vlan ports pvid 284, 286
 - config vlan ports tagging 285, 287
 - config port autoneg 206
 - config switchconfig flowcontrol 272, 273
 - config users delete 296, 297, 298, 299
 - config users passwd 296, 297, 298, 299
 - config vlan delete 274
 - config vlan ports acceptframe 286
 - config vlan ports ingressfilter 277, 282, 283, 284

configuration reset	307	dot1x max-req	537
config-watchdog	312	dot1x max-users	538
copy	312	dot1x port-control	539
copy nvram clibanner	318	dot1x port-control all	540
copy nvram startup-config	320	dot1x re-authenticate	541
copy system bootcode	320	dot1x re-authentication	541
copy system image	320	dot1x safe-vlan	542
copy system running-config	320	dot1x system-auth-control	543
copy nvram capture	315	dot1x timeout	543
copy nvram capture aca		dot1x user	547
capture	315	duplex settings	267
copy nvram clibanner	315	dvlan-tunnel ethertype	98
copy nvram errorlog	316		
copy nvram script	316	E	
copy nvram traplog	317	ethernet-ip	125
copy system running-config	317		
copy tftp/// nvramhttpscert	315	F	
		fast-hiper-ring	486
D		flow control	272, 273
debug tcpdump filter delete	89	frame acceptance mode	276, 277, 282
debug tcpdump filter list	88		
debug tcpdump filter show	88	G	
debug tcpdump help	86	Global Config Mode	49
debug tcpdump start cpu	86	GVRP	
debug tcpdump start cpu filter	87	join time	206, 207, 208, 209, 210, 211,
debug tcpdump stop	87		212
deleteport	192	leave time	213
deleteport all	192		
device configuration commands	201	H	
device-status connection-error	321	hiper-ring	480
device-status monitor	322	hiper-ring mode	480
DHCP server configuration example	508	hiper-ring port primary	481
dhcp-relay	504, 505	hiper-ring port secondary	481
dhcp-server addr-probe	512	hiper-ring recovery-delay	482
dhcp-server operation	513		
dhcp-server pool add	513	I	
dhcp-server pool delete	518	iec61850-mms	126
dhcp-server pool disable	518	IEEE 802.1Q	276, 277, 282
dhcp-server pool enable	518	ingress filtering	278, 283
dhcp-server pool modify hirschmann-device	517	inlinepower (Global Config)	411
		inlinepower (Interface Config)	412
dhcp-server pool modify mode	514	inlinepower budget slot	415
dhcp-server pool modify option	516	inlinepower threshold slot	416
dhcp-server pool modify leasetime	517	inlinepower trap slot	416
digital-input	112	Interface Config Mode	50
digital-output	114	inventory	238, 239, 240, 242, 243, 244, 246,
dip-switch operation	193		247, 529
disconnect	292	ip http secure-port	571
dot1x defaultlogin	532	ip http secure-protocol	571
dot1x dynamic-vlan enable	533	ip http server	571
dot1x guest-vlan	534	ip https certgen	574
dot1x initialize	535	ip https port	574
dot1x login	535	ip https server	573
dot1x mac-auth-bypass	536	ip ssh protocol	548

J			
join time	206, 207, 208, 209, 210, 211, 212		
L			
LAGs			
enabling or disabling	204		
link traps	205		
name	206		
summary information	251		
leave time	213, 214		
Line Config Mode	50		
Link Aggregation(802.3ad) Commands	102		
link aggregations. See LAGs			
link traps			
interface	263, 264, 265		
LAG	205		
link-aggregation	203		
link-aggregation adminmode	204		
link-aggregation linktrap	205		
link-aggregation name	206		
link-aggregation staticcapability	102		
lldp	347		
LLDP - Link Layer Discovery Protocol	335		
lldp admin-state	351		
lldp chassis tx-interval	350		
lldp config chassis admin-state	348		
lldp config chassis notification-interval	348		
lldp config chassis re-init-delay	349		
lldp config chassis tx-delay	349		
lldp config chassis tx-hold-mult	350		
lldp fdb-mode	352		
lldp hm-mode	352		
lldp max-neighbors	353		
lldp med	354		
lldp med al	355		
lldp med confignotification	355		
lldp med confignotification all	356		
lldp med faststartrepeatcount	357		
lldp med transmit-tlv	358		
lldp med transmit-tlv all	359		
lldp notification	360		
lldp tlv gmrp	363		
lldp tlv igmp	363		
lldp tlv link-aggregation	360		
lldp tlv mac-phy-config-state	360		
lldp tlv max-frame-size	361		
lldp tlv mgmt-addr	361		
lldp tlv pnio	361		
lldp tlv pnio-alias	362		
lldp tlv pnio-mrp	362		
lldp tlv port-desc	362		
lldp tlv portsec	364		
lldp tlv port-vlan	363		
lldp tlv protocol	364		
lldp tlv ptp	364		
lldp tlv sys-cap	365		
lldp tlv sys-desc	365		
lldp tlv sys-name	365		
lldp tlv vlan-name	366		
logging buffered	170		
logging buffered wrap	171		
logging cli-command	172		
logging console	173		
logging host	174		
logging host reconfigure	175		
logging host remove	175		
logging snmp-requests get operation	175		
logging snmp-requests get severity	176		
logging snmp-requests set operation	176		
logging snmp-requests set severity	177		
logging syslog	178		
logging syslog port	178		
logical slot/port	30		
logout	323		
logout command	323		
M			
mac notification (Global Config)	197		
mac notification (Interface Config)	198		
macaddr	29		
mac-address conflict	323		
macfilter	194		
macfilter adddest	195		
macfilter adddest all	196		
media-module	191		
media-module remove	191		
mode dvlan-tunnel	100		
monitor session	199		
monitor session mode	201		
monitor session source/destination	202		
mrp current-domain	472		
mrp delete-domain	474		
mrp new-domain	474		
N			
name	366		
network javascriptmode	128		
network mgmt_vlan	90		
network mgmt-access add	128		
network mgmt-access delete	128		
network mgmt-access modify	129		
network mgmt-access operation	130		
network mgmt-access status	131		
network parms	131		
network priority	133		
network protocol	132		
no dhcp-relay	504		
no lldp	347		

-
- no snmp 372
 - no snmp anycast address 373, 374, 380
 - no snmp client server 376
 - no snmp client server primary 377, 378, 379
 - no storm-control broadcast 268
- P**
- passwords
 - changing user 299
 - resetting all 309
 - PDUUs 206, 207, 208, 209, 210, 211, 212, 214
 - ping 324
 - ping command 321, 322, 324
 - PoE - Power over Ethernet 407
 - Port monitor 417
 - port-monitor (Global Config) 424
 - port-monitor (Interface Config) 424
 - port-monitor action 425
 - port-monitor condition crc-fragment (Global Config) 430
 - port-monitor condition crc-fragment (Interface Config) 431
 - port-monitor condition link-flap (Global Config) 429
 - port-monitor condition link-flap (Interface Config) 429
 - port-monitor condition speed-duplex-monitor (Interface Config) 431
 - port-monitor condition speed-duplex-monitor clear (Interface Config) 432
 - port-monitor condition speed-duplex-monitor speed (Interface Config) 432
 - port-monitor overload-detection (Global Config) 426
 - port-monitor overload-detection (Interface Config) 426
 - ports
 - administrative mode 261, 262
 - frame acceptance mode 276, 277, 282
 - information 250
 - ingress filtering 278, 283
 - link traps 263, 264, 265
 - physical mode 267
 - tagging 285, 287
 - VLAN IDs 284, 286
 - VLAN information 258
 - port-sec action 498
 - port-sec allowed-ip 499
 - port-sec allowed-ip add 499
 - port-sec allowed-ip remove 500
 - port-sec allowed-mac 500
 - port-sec allowed-mac add 501
 - port-sec allowed-mac remove 501
 - port-sec dynamic 502
 - port-sec mode 497
 - Privileged Exec Mode 49
 - profinetio 134
 - Protocol Data Units. See PDUs
 - PTP - Precision Time Protocol 382
 - ptp clock-mode 388
 - ptp operation 389
 - ptp sync-lower-bound 389
 - ptp sync-upper-bound 390
 - ptp v1 burst 396
 - ptp v1 operation 396
 - ptp v1 preferred-master 390
 - ptp v1 re-initialize 391
 - ptp v1 subdomain-name 391
 - ptp v1 sync-interval 392
 - ptp v2bc announce-interval 397
 - ptp v2bc announce-timeout 398
 - ptp v2bc asymmetry 400
 - ptp v2bc delay-mechanism 398
 - ptp v2bc domain 394
 - ptp v2bc network-protocol 399
 - ptp v2bc operation 397
 - ptp v2bc pdelay-interval 399
 - ptp v2bc priority1 393
 - ptp v2bc priority2 393
 - ptp v2bc sync-interval 398
 - ptp v2bc utc-offset 394
 - ptp v2bc utc-offset-valid 394
 - ptp v2bc v1-compatibility-mode 399
 - ptp v2bc vlan 395
 - ptp v2bc vlan-priority 395
 - ptp v2tc asymmetry 400
 - ptp v2tc delay-mechanism 400
 - ptp v2tc management 401
 - ptp v2tc multi-domain-mode 401
 - ptp v2tc network-protocol 402
 - ptp v2tc operation 402
 - ptp v2tc pdelay-interval 403
 - ptp v2tc power-tlv-check 405
 - ptp v2tc primary-domain 403
 - ptp v2tc profile 404
 - ptp v2tc sync-local-clock 406
 - ptp v2tc syntonization 404
 - ptp v2tc vlan 405
 - ptp v2tc vlan-priority 406
- R**
- radius accounting mode 549
 - radius server host 549
 - radius server key 551
 - radius server msgauth 551
 - radius server primary 552
 - radius server retransmit 553

radius server timeout	554	set igmp lookup-interval-unknown	228
reboot	327	set igmp lookup-resp-time-unknown	228
reload	329	set igmp maxresponse	229
reset system command	327, 329	set igmp querier max-response-time	230
ring-coupling	491	set igmp querier protocol-version	230
ring-coupling config	492	set igmp querier status	231
ring-coupling net-coupling	493	set igmp querier tx-interval	231
ring-coupling operation	493	set igmp query-ports-to-filter	232
ring-coupling port	494	set igmp static-query-port	225
ring-coupling redundancy-mode	494	set pre-login-banner text	232
rmon-alarm add	206	set pro-login-banner banner	333
rmon-alarm delete	207	set prompt	135
rmon-alarm disable	208	show	56
rmon-alarm enable	207	show address-conflict	56
rmon-alarm modify falling-event	211	show arc	476
rmon-alarm modify interval	209	show arp switch	57, 63
rmon-alarm modify mib-variable	208	show authentication	62, 557
rmon-alarm modify rising-event	211	show authentication users	558
rmon-alarm modify sample-type	210	show auto-disable brief	236
rmon-alarm modify startup-alarm	210	show auto-disable reasons	237
rmon-alarm modify thresholds	209	show boot skip-aca-on-boot	304, 304
		show bridge address-learning	57
		show bridge address-relearn-detect	58
		show bridge aging-time	58
		show bridge duplex-mismatch-detect	59
		show bridge fast-link-detection	59
		show bridge framesize	59
		show bridge vlan-learning	60
		show classofservice dot1pmapping	95
		show classofservice ip-dscp-mapping	96
		show classofservice trust	97
		show commands	
		show inventory	238, 239, 240, 242, 243, 244, 246, 247, 529
		show lags summary	251
		show loginsession	293
		show port	250
		show stats switch detailed	64, 66, 72
		show switchconfig	252, 253, 254
		show users	294
		show vlan detailed	255
		show vlan interface	258
		show vlan summary	257
		show config-watchdog	61
		show device-status	61
		show dhcp-relay	504, 506
		show dhcp-server	510
		show dhcp-server operation	511
		show dhcp-server pool	512
		show dhcp-server port	511
		show digital-input	117, 120
		show digital-input all	119
		show digital-input config	118
S			
Schulungsangebot	611		
script apply	179		
script delete	180		
script list	180		
script show	181		
script validate	181		
selftest ramtest	232		
selftest reboot-on-error	234		
selftest reboot-on-hdxerror	233		
serial timeout	135		
serviceshell	235		
session-limit	107		
sessions			
closing	292, 323		
displaying	293		
session-timeout	108		
set cli banner	331		
set garp timer join	212		
set garp timer leave	213		
set garp timer leaveall	214		
set gmrp adminmode	215		
set gmrp forward-all-groups	218		
set gmrp forward-unknown	219		
set gmrp interfacemode	216, 217		
set igmp	220, 221		
set igmp aging-time-unknown	221		
set igmp automatic-mode	222		
set igmp forward-all	223		
set igmp forward-unknown	224		
set igmp groupmembershipinterval	226		
set igmp interfacemode	227		

show digital-output	121, 124	show mac-filter-table gmrp	242
show digital-output all	123	show mac-filter-table igmpsnooping	243
show digital-output config	122	show mac-filter-table multicast	244
show dip-switch	238	show mac-filter-table static	245
show dot1x	558	show mac-filter-table staticfiltering	246
show dot1x clients	564	show mac-filter-table stats	247
show dot1x users	563	show monitor session	249
show dvlan-tunnel	101	show mrp	470
show ethernet-ip	136, 139	show mrp current domain	471
show eventlog	63	show network	110, 136
show fast-hiper-ring	484	show network mgmt-access	138
show fast-hiper-ring current-id	485	show port	250, 272, 273
show garp	239	show port-monitor	418, 419
show gmrp configuration	239	show port-monitor brief	420
show hiper-ring	479	show port-monitor crc-fragment	421
show hiper-ring info	480	show port-monitor link-flap	421
show iec61850-mms	127	show port-monitor speed-duplex	423
show igmpsnooping	240	show port-sec dynamic	495
show inlinepower	407	show port-sec mode	496
show inlinepower port	408	show port-sec port	497
show inlinepower slot	414	show ptp	382
show interface	64	show ptp configuration	385
show interface ethernet	66	show ptp operation	385
show interface switchport	73	show ptp port	386
show interface utilization	74	show ptp status	387
show inventory	278	show radius	566
show ip http	572	show radius accounting	554
show ip https	575	show radius statistics	567
show ip ssh	565	show reboot	328
show link-aggregation	251	show reload	330
show link-aggregation brief	103	show ring-coupling	489
show lldp	335	show rmon-alarm	252
show lldp chassis tx-interval	338	show running-config	81
show lldp config	335	show selftest	253
show lldp config chassis	336	show serial	139
show lldp config chassis admin-state	336	show serviceshell	253
show lldp config chassis notification-interval	336	show signal-contact	78
show lldp config chassis re-init-delay	337	show slot	80
show lldp config chassis tx-delay	337	show snmp sync	142
show lldp config chassis tx-hold-mult	337	show snmp-access	140
show lldp config port	339	show snmpcommunity	141
show lldp config port tlv	340	show snmptrap	143
show lldp med	341	show snmp	367
show lldp med interface	342	show snmp anycast	369
show lldp med local-device detail	343	show snmp client	369
show lldp med remote-device	344	show snmp operation	370
show lldp med remote-device detail	345	show snmp server	371
show lldp remote-data	345	show snmp status	371
show logging	75	show snmp time	372
show login session	293, 300	show spanning-tree	435
show mac notification	247	show spanning-tree brief	436
show mac-address-conflict	76	show spanning-tree interface	438
show mac-addr-table	77	show spanning-tree mst detailed	439
		show spanning-tree mst port detailed	440

Index

show spanning-tree mst port summary	443	sntp client disable-after-sync	375
show spanning-tree mst summary	444	sntp client offset	375
show spanning-tree summary	445	sntp client request-interval	376
show spanning-tree vlan	446	sntp client server primary	377
show storm-control	254	sntp client server secondary	378
show storm-control limiters port	254	sntp client threshold	379
show sub-ring	519	sntp operation	380
show switchconfig	110	sntp server disable-if-local	381
show sysinfo	82, 97, 98	sntp time system	381
show telnet	144	spanning-tree	447
show telnetcon	145	spanning-tree auto-edgeport	448
show temperature	85	spanning-tree bpduguard	449
show trapflags	146	spanning-tree bpdumigrationcheck	266
show users	294	spanning-tree configuration name	450
show users authentication	569	spanning-tree configuration revision	451
show vlan	255	spanning-tree edgeport	452
show vlan brief	257	spanning-tree forceversion	453
show vlan port	258	spanning-tree forward-time	454, 456
show voice vlan	259	spanning-tree guard loop	455
show voice vlan interface	260	spanning-tree guard none	456
shutdown	261	spanning-tree guard root	457
shutdown all	262	spanning-tree hello-time	458
signal-contact	325	spanning-tree hold-count	458
signal-contact connection-error	324	spanning-tree max-age	459
slot/port	30	spanning-tree max-hops	460
snmp sync community-to-v3	263	spanning-tree mst	461
snmp trap link-status	264	spanning-tree mst instance	465
snmp trap link-status all	265	spanning-tree mst priority	463
snmp-access global	147, 148	spanning-tree mst vlan	464
snmp-access version v3-encryption	148	spanning-tree port mode	466
snmp-server	86, 150	spanning-tree port mode all	467
snmp-server community	151	spanning-tree stp-mrp-mode	468
snmp-server community ipaddr	153	spanning-tree tcnguard	469
snmp-server community ipmask	154	speed	267
snmp-server community mode	155	speeds	267
snmp-server community ro	156	statistics	
snmp-server community rw	156	switch, related commands	64, 66, 72
snmp-server contact	152	storm-control broadcast	268
snmp-server enable traps	157	storm-control broadcast (port-related)	270
snmp-server enable traps linkmode	160	storm-control egress-limit	270
snmp-server enable traps multiusers	161	storm-control egress-limiting	268
snmp-server enable traps port-sec	162	storm-control flowcontrol	272
snmp-server enable traps stpmode	163	storm-control flowcontrol per port	273
snmp-server location	156	storm-control ingress-limit	271
snmp-server sysname	157	storm-control ingress-limiting	269
snmptrap	164	storm-control ingress-mode	269, 271
snmptrap ipaddr	165	sub-ring mode	521
snmptrap mode	166	sub-ring mrp-domainID	525
snmptrap snmpversion	167	sub-ring operation	522
SNTP - Simple Network Time Protocol	367	sub-ring port	523
sntp anycast address	373	sub-ring protocol	522
sntp anycast transmit-interval	373	sub-ring ring-name	523
sntp anycast vlan	374	sub-ring vlan	524
sntp client accept-broadcast	374	Sub-Ring Commands	519

- sub-ring delete-ring 526
- sub-ring new-ring 526
- switch
 - information, related commands 252, 253, 254
 - inventory 238, 239, 240, 242, 243, 244, 246, 247, 529
 - resetting 327, 329
 - statistics, related commands 64, 66, 72
- System Information and Statistics Commands 90
- System Utilities 303, 529
- system utilities 303–324

- T**
- tagging 285, 287
- telnet 104
 - sessions, closing 292, 323
 - sessions, displaying 293
- telnetcon maxsessions 168
- telnetcon timeout 169
- temperature 326
- traceroute 306
- transport input telnet 105
- transport output telnet 106
- trap log
 - clearing 310, 311
- trunks. See LAGs

- U**
- update module-configuration 235
- User Account Management Commands 292
- user account management commands 292
- User Exec Mode 49
- users
 - adding 297, 298
 - deleting 296, 297, 298
 - displaying 294
 - passwords 299, 309
- users access 297
- users defaultlogin 295
- users login 296, 570
- users name 298
- users passwd 299
- users snmpv3 accessmode 300
- users snmpv3 authentication 301
- users snmpv3 encryption 302
- utilization alarm-threshold 85

- V**
- vlan 274
- vlan acceptframe 276, 277
- vlan ingressfilter 278
- VLAN Mode 49
- vlan name 279
- vlan participation 280
- vlan participation all 281
- vlan port acceptframe all 282
- vlan port ingressfilter all 283
- vlan port priority all 97
- vlan port pvid all 284
- vlan port tagging all 285
- vlan priority 98
- vlan pvid 286
- vlan tagging 287
- vlan0-transparent-mode 275
- VLANs
 - adding 274
 - changing the name of 279
 - deleting 274
 - details 255
 - frame acceptance mode 276, 277, 282
 - IDs 284, 286
 - ingress filtering 278, 283
 - jointime 206, 207, 208, 209, 210, 211, 212
 - leave all time 214
 - leave time 213
 - participation in 280, 281
 - port information 258
 - resetting parameters 311
 - summary information 257
 - tagging 285, 287
 - voice vlan (Global Config Mode) 288
 - voice vlan (Interface Config Mode) 289
 - voice vlan auth 291

- W**
- Web connections, displaying 293

9 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 606 for more information.

A

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.

Application Programming Interface. An API is an interface used by a programmer to interface with functions provided by an application.

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 594.

BootP. See “Bootstrap Protocol.” on page 594.

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.

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 examining 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

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 594.

Command Line Interface. CLI is a line-item interface for configuring systems.

Complex Programmable Logic Device. CPLD is a programmable circuit on which a logic network can be programmed after its construction.

CPLD. See “Complex Programmable Logic Device.” on page 595.

D

DAPI. See “Device Application Programming Interface” on page 595.

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 595.

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 595..

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 596.

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 605 for more information.

FIFO. First In First Out.

Flash Memory. See “EEPROM” on page 596.

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 597.

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 597.

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 596.

GMRP. See “GARP Multicast Registration Protocol” on page 597.

GPCM. See “General Purpose Chip-select Machine” on page 597.

GVD. GARP VLAN Database.

GVRP. See “GARP VLAN Registration Protocol.” on page 597.

H

.h file. Header file in C code. Contains function and coding definitions.

HAPI. See “Hardware Abstraction Programming Interface” on page 597.

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 598.

IGMP. See “Internet Group Management Protocol” on page 598.

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 598 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 598.

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 599.

L

LAN. See “Local Area Network” on page 600.

LDAP. See “Lightweight Directory Access Protocol” on page 599.

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 determining 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 601.

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 600.

MOSPF. See “Multicast OSPF” on page 601.

MPLS. See “Multi-Protocol Label Switching” on page 601.

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 “mrouterd” 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 “P” on page 603 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 601.

N

NM. Network Module.

nm. Nanometer (1×10^9) meters.

NP. Network Processor.

O

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 602.

OSI. See “Open Systems Interconnection” on page 602.

P

PDU. See “Protocol Data Unit” on page 603.

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.

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.

Q

QoS. See “Quality of Service” on page 603.

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.

RFC. Request For Comment.

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.

RTOS. See “Real-Time Operating System” on page 604.

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 defining 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 defining 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 604.

SODIMM. Small Outline Dual Inline Memory Module.

SRAM. Static Random Access Memory.

STP. Spanning Tree Protocol. See "802.1D" on page 593 for more information.

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 605.

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 combining 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.

VLAN. See "Virtual Local Area Network" on page 606.

vMAN. Virtual Metropolitan Area Network.

W

WAN. See "Wide Area Network" on page 606.

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

RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE,

RSR20/RSR30, MACH 100, MACH 1000, 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

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 DHCP-Server Pools pro VLAN	50
2.7.1 Anwendungsbeispiel	51
2.8 System-Konfiguration via DHCP-Option 82	54
2.9 IP-Konfiguration via grafische Benutzeroberfläche	55
2.10 Defekte Geräte ersetzen	58

3	Einstellungen laden/speichern	59
3.1	Einstellungen laden	60
3.1.1	Laden aus lokalem nicht-flüchtigen Speicher	61
3.1.2	Laden aus einer Datei	62
3.1.3	Die aktuelle Konfiguration in den Lieferzustand zurückzusetzen.	64
3.1.4	Laden vom AutoConfiguration Adapter	65
3.1.5	Den Offline-Konfigurator verwenden	67
3.2	Einstellungen speichern	69
3.2.1	Lokal (und auf den ACA) speichern	69
3.2.2	Speichern in eine Binär- oder Skript-Datei auf einem URL	71
3.2.3	Speichern in eine Binär-Datei auf den PC	72
3.2.4	Speichern als Skript auf den PC	72
3.2.5	Speichern als Offline-Konfigurations-Datei auf den PC	73
3.3	Konfigurations-Signatur	74
4	Neueste Software laden	75
4.1	Software manuell vom ACA laden	77
4.1.1	Auswahl der zu ladenden Software	78
4.1.2	Starten der Software	79
4.1.3	Kaltstart durchführen	80
4.2	Automatischer Software-Update vom ACA	81
4.3	Software vom TFTP-Server laden	83
4.4	Software über Datei-Auswahl laden	85
4.5	Bootcode-Update via TFTP	86
4.5.1	Aktualisieren der Bootcode-Datei	86
4.6	Software-Update OCTOPUS	88
5	Ports konfigurieren	91
6	Unterstützung beim Schutz vor unberechtigtem Zugriff	99
6.1	Das Gerät schützen	100
6.2	Passwort für SNMP-Zugriff	101
6.2.1	Beschreibung Passwort für SNMP-Zugriff	101
6.2.2	Passwort für SNMP-Zugriff eingeben	102

6.3	Telnet-/Web-/SSH-Zugriff	106
6.3.1	Beschreibung Telnet-Zugriff	106
6.3.2	Beschreibung Web-Zugriff (http)	106
6.3.3	Beschreibung SSH-Zugriff	107
6.3.4	Telnet-/Web-/SSH-Zugriff aus-/einschalten	108
6.3.5	Web-Zugriff über HTTPS	109
6.4	Restricted Management Access	112
6.5	HiDiscovery-Zugriff aus-/einschalten	115
6.5.1	Beschreibung HiDiscovery-Protokoll	115
6.5.2	HiDiscovery-Funktion aus-/einschalten	115
6.6	Portzugangskontrolle	117
6.6.1	Beschreibung der Portzugangskontrolle	117
6.6.2	Anwendungsbeispiel für Portzugangskontrolle	118
6.7	Port-Authentifizierung nach IEEE 802.1X	120
6.7.1	Beschreibung Port-Authentifizierung nach IEEE 802.1X	120
6.7.2	Authentifizierungsablauf nach IEEE 802.1X	121
6.7.3	Vorbereitung des Gerätes für die IEEE 802.1X-Port-Authentifizierung	121
6.7.4	IEEE 802.1X-Einstellungen	122
6.8	Login-Banner	124
6.9	CLI-Banner	125
7	Die Systemzeit im Netz synchronisieren	127
7.1	Uhrzeit einstellen	128
7.2	SNTP	130
7.2.1	Beschreibung SNTP	130
7.2.2	Vorbereitung der SNTP-Konfiguration	131
7.2.3	Konfiguration SNTP	132
7.3	Precision Time Protocol	135
7.3.1	Funktionsbeschreibung PTP	135
7.3.2	PTP-Konfiguration vorbereiten	141
7.3.3	Anwendungsbeispiel	143
7.4	Interaktion von PTP und SNTP	148
8	Netzlaststeuerung	151
8.1	Gezielte Paketvermittlung	152
8.1.1	Store and Forward	152
8.1.2	Multiadress-Fähigkeit	152
8.1.3	Aging gelernter MAC-Adressen	153

8.1.4	Statische Adresseinträge eingeben	154
8.1.5	Gezielte Paketvermittlung ausschalten	156
8.2	Multicast-Anwendung	157
8.2.1	Beschreibung Multicast-Anwendung	157
8.2.2	Beispiel für eine Multicast-Anwendung	158
8.2.3	Beschreibung IGMP-Snooping	159
8.2.4	IGMP-Snooping einstellen	160
8.2.5	Beschreibung von GMRP	165
8.2.6	GMRP einstellen	167
8.3	Lastbegrenzer	169
8.3.1	Beschreibung Lastbegrenzer	169
8.3.2	Lastbegrenzer-Einstellungen	170
8.3.3	Lastbegrenzer-Einstellungen für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS	171
8.4	QoS/Priorität	173
8.4.1	Beschreibung Priorisierung	173
8.4.2	VLAN-Tagging	174
8.4.3	IP ToS / DiffServ	177
8.4.4	Management-Priorisierung	180
8.4.5	Behandlung empfangener Prioritätsinformationen	181
8.4.6	Handhabung der Verkehrsklassen	182
8.4.7	Priorisierung einstellen	183
8.5	Flusskontrolle	188
8.5.1	Beschreibung Flusskontrolle	188
8.5.2	Flusskontrolle einstellen	190
8.6	VLANs	191
8.6.1	Beschreibung VLAN	191
8.6.2	Beispiele für ein VLAN	192
9	Funktionsdiagnose	207
9.1	Alarmmeldungen versenden	208
9.1.1	Auflistung der SNMP-Traps	209
9.1.2	SNMP-Traps beim Booten	210
9.1.3	Trapeinstellung	211
9.2	Gerätestatus überwachen	213
9.2.1	Gerätestatus konfigurieren	214
9.2.2	Gerätestatus anzeigen	215
9.3	Out-of-band-Signalisierung	216
9.3.1	Meldekontakt steuern	217
9.3.2	Gerätestatus mit Meldekontakt überwachen	218
9.3.3	Gerätestatus mit Meldekontakt überwachen	218
9.3.4	Lüfter überwachen	220

9.4	Port-Zustandsanzeige	222
9.5	Ereigniszähler auf Portebene	224
9.5.1	Erkennen der Nichtübereinstimmung der Duplex- Modi	225
9.5.2	TP-Kabeldiagnose	227
9.5.3	Port-Monitor	229
9.5.4	Auto-Disable	232
9.6	SFP-Zustandsanzeige	234
9.7	Topologie-Erkennung	235
9.7.1	Beschreibung Topologie-Erkennung	235
9.7.2	Anzeige der Topologie-Erkennung	236
9.8	IP-Adresskonflikte erkennen	238
9.8.1	Beschreibung von IP-Adresskonflikten	238
9.8.2	ACD konfigurieren	239
9.8.3	ACD anzeigen	239
9.9	Erkennen von Loops (Schleifen)	240
9.10	Berichte	242
9.11	Datenverkehr von Ports beobachten (Port-Mirroring)	244
9.12	Syslog	248
9.13	Trap-Log	251
9.14	MAC-Benachrichtigung	252
A	Konfigurationsumgebung einrichten	255
A.1	DHCP/BOOTP-Server einrichten	256
A.2	DHCP-Server Option 82 einrichten	262
A.3	TFTP-Server für SW-Updates	266
A.3.1	tftp-Prozess einrichten	267
A.3.2	Software-Zugriffsrechte	270
A.4	SSH-Zugriff vorbereiten	271
A.4.1	Schlüssel erzeugen	271
A.4.2	Schlüssel auf das Gerät laden	273
A.4.3	Zugriff mittels SSH	273
A.5	HTTPS-Zertifikat	276
A.6	Service-Shell	277

B	Allgemeine Informationen	279
B.1	Management Information BASE (MIB)	280
B.2	Verwendete Abkürzungen	283
B.3	Technische Daten	284
B.4	Leserkritik	285
C	Stichwortverzeichnis	287
D	Weitere Unterstützung	291

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 „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
<input type="checkbox"/>	Arbeitsschritt
	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Anmerkung	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
<code>Courier</code>	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

Legende



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
Stopbit	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.

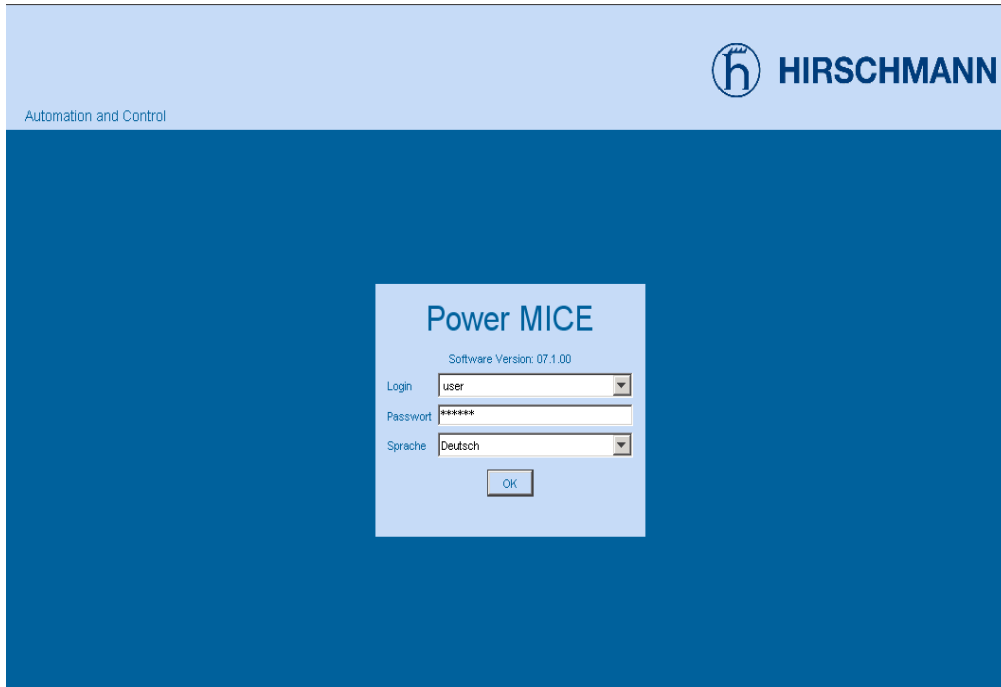


Abb. 5: Login-Fenster

- 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 54 „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

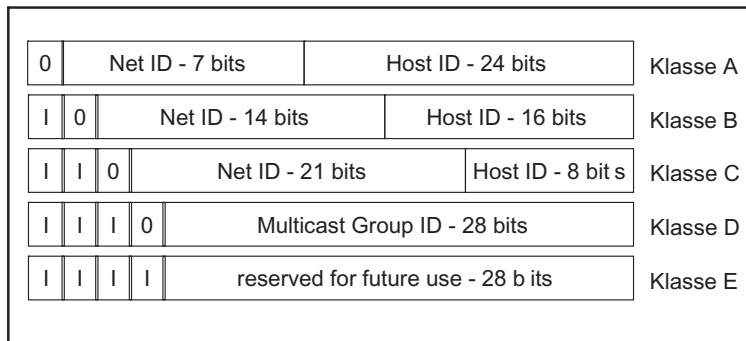


Abb. 6: Bitdarstellung der IP-Adresse

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.

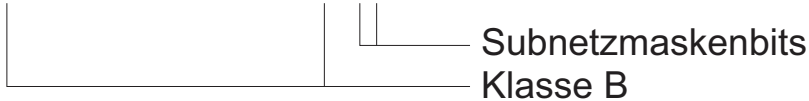
Die Einteilung in Subnetze mit Hilfe der Netzmaske geschieht analog zu der Einteilung in die Klassen A bis C der Netzadresse (net id).

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:

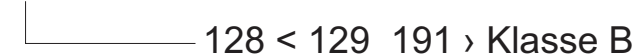
Dezimale Darstellung  
255.255.192.0

Binäre Darstellung  
11111111.11111111.11000000.00000000

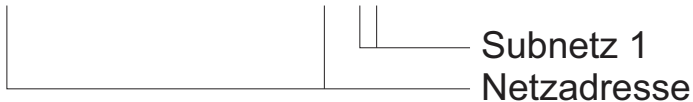


Beispiel für IP-Adressen mit Subnetzzuordnung nach der Netzmaske aus dem obigen Beispiel:

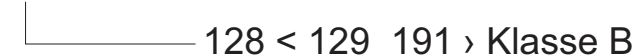
Dezimale Darstellung  
129.218.65.17




Binäre Darstellung  
10000001.11011010.01000001.00010001



Dezimale Darstellung  
129.218.129.17



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?

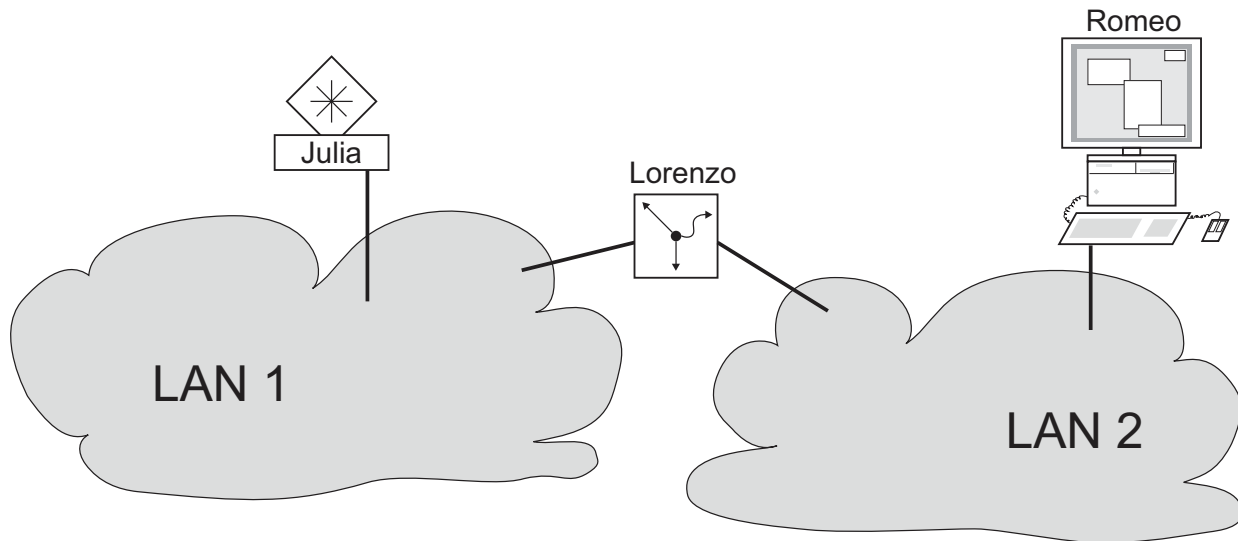


Abb. 7: Management-Agent durch Router von der Managementstation getrennt

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 Umschlages 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 Adressbereich, 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.

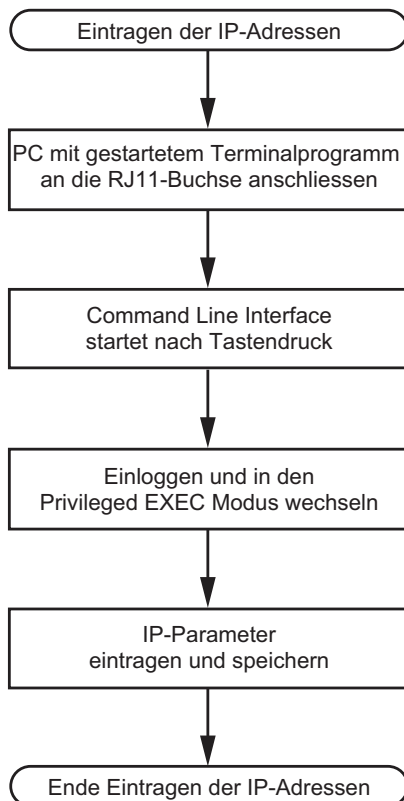


Abb. 8: Ablaufdiagramm Eintragen der IP-Adressen

---

**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
network protocol none
network parms 10.0.1.23
 255.255.255.0

copy system:running-config
nvram:startup-config
```

Wechsel in den Privileged-EXEC-Modus.

DHCP ausschalten.

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.

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 Gerätenamen und die IP-Parameter eintragen können.

**Anmerkung:** Mit dem Eintragen der IP-Adresse übernimmt das Gerät die lokalen Konfigurationseinstellungen ([siehe auf Seite 59 „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 55 „IP-Konfiguration via grafische Benutzeroberfläche“](#)).

**Anmerkung:** Speichern Sie die Einstellungen, damit Sie die Eingaben nach einem Neustart noch verfügbar haben ([siehe auf Seite 59 „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 69 „Lokal \(und auf den ACA\) speichern“](#).

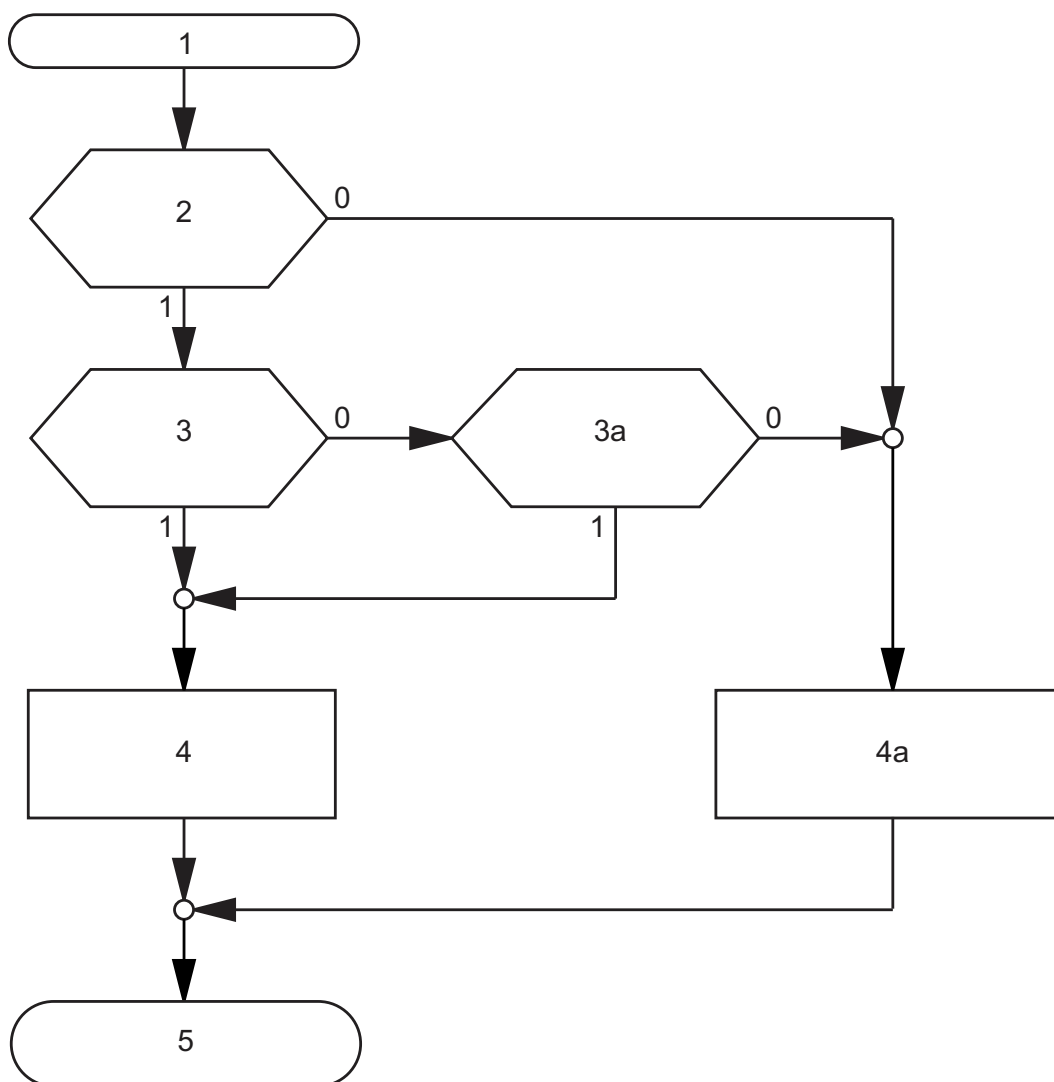


Abb. 9: Ablaufdiagramm Konfigurationsdaten vom ACA laden

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 55 „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<br>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 256.](#)

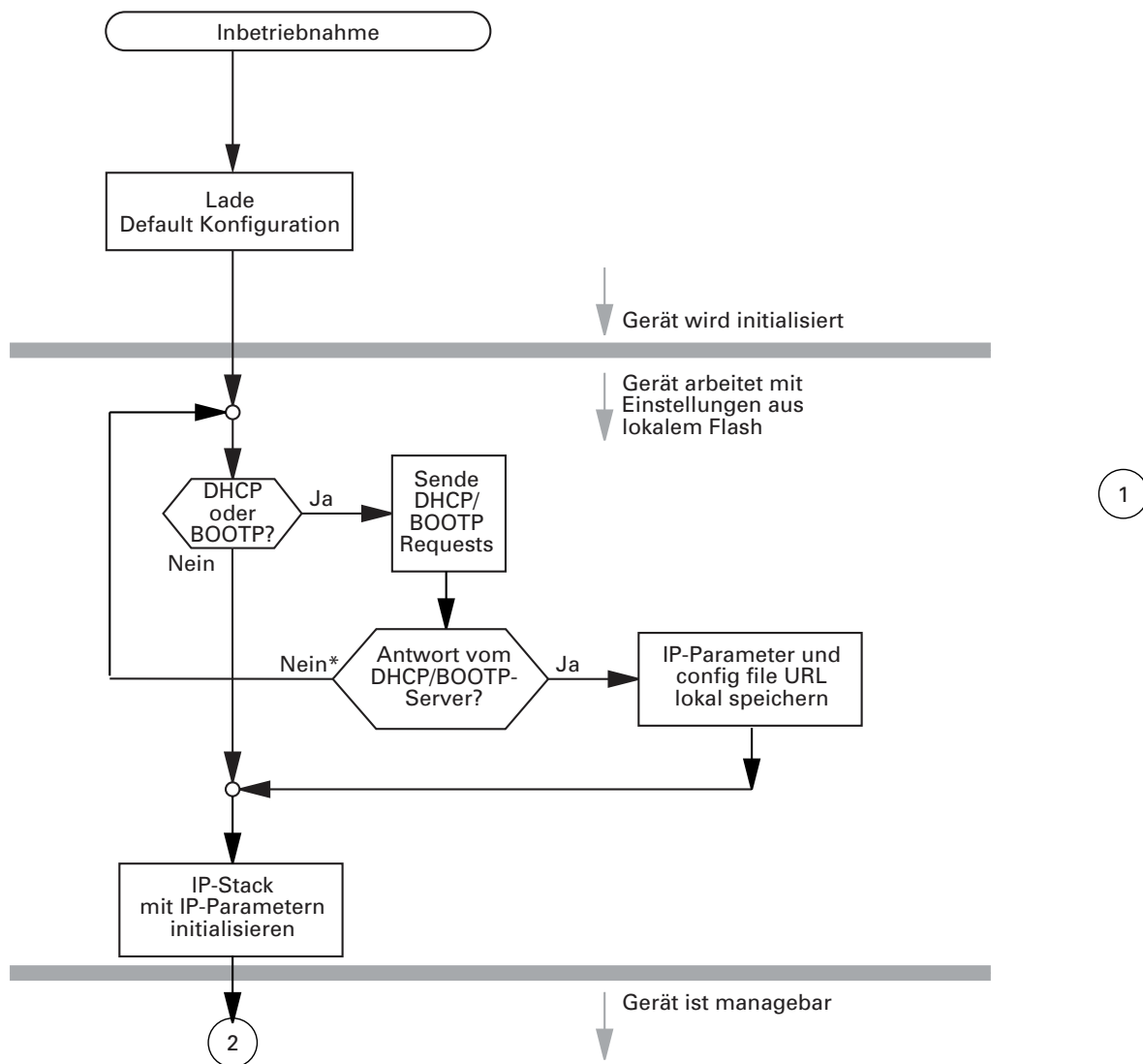


Abb. 10: Ablaufdiagramm BOOTP/DHCP-Prozess, Teil 1  
\* siehe Hinweis [Abbildung 11](#)

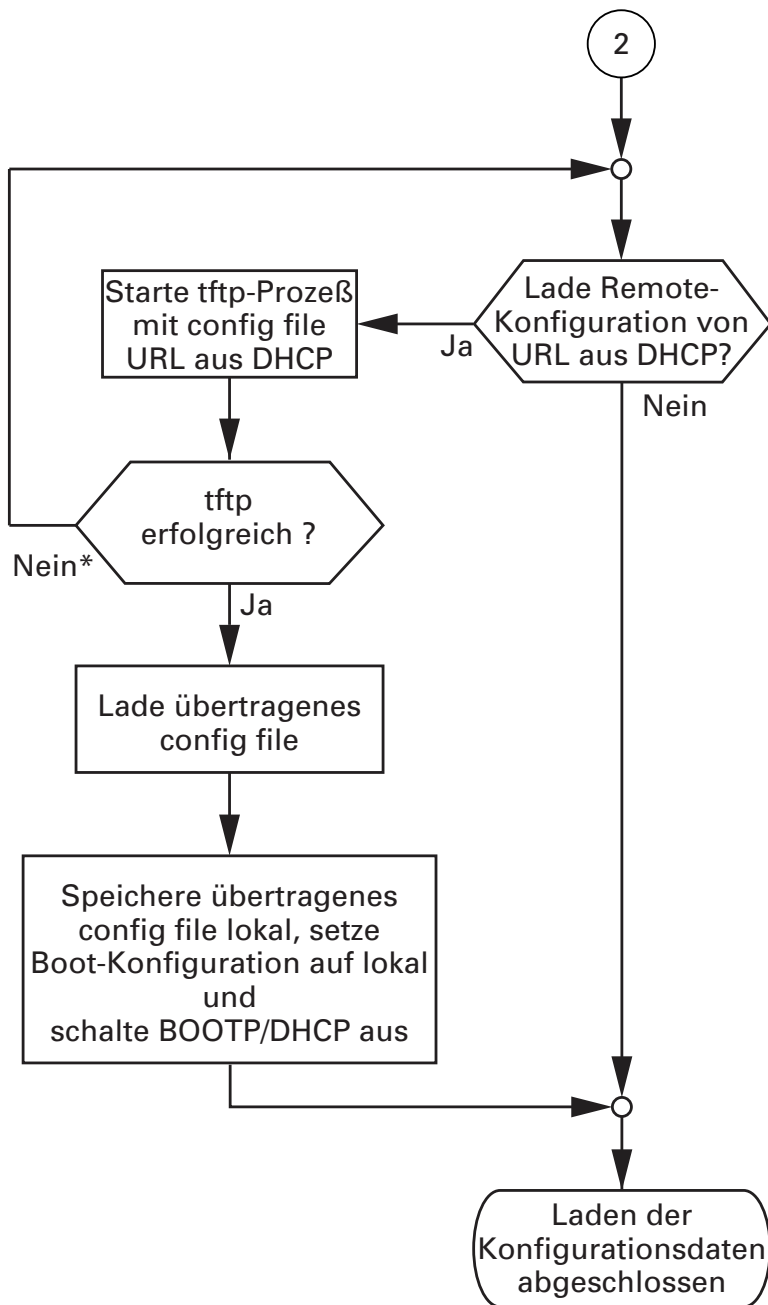


Abb. 11: Ablaufdiagramm BOOTP/DHCP-Prozess, Teil 2

**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 55](#) „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 Adressvergabe) 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 256 „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 DHCP-Server Pools pro VLAN

Die Geräte der OCTOPUS-, MS20/MS30-, RS20/RS30/RS40-, RSR20/RSR30-, MACH100- und MACH1020/1030-Familie bieten Ihnen die Möglichkeit, einen oder mehrere IP-Adress-Pools (kurz „Pools“) pro VLAN zu konfigurieren und ein- bzw. auszuschalten. Der DHCP-Server beantwortet die Anfragen der Clients aus den VLANs und vergibt die IP-Adressen aus einem Pool. 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 IP-Adress Vergabe.

- ▶ Bei der dynamischen IP-Adress Vergabe definieren Sie einen dynamischen Adressbereich pro VLAN. Meldet sich ein Client aus einem VLAN, dann weist der DHCP-Server eine noch freie IP-Adresse aus einem Pool-Eintrag zu.
- ▶ Bei der statischen IP-Adress Vergabe weist der DHCP-Server stets dieselbe IP-Adresse an einen Client aus einem VLAN 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 VLANs oder für ein bestimmtes VLAN gelten.

## 2.7.1 Anwendungsbeispiel

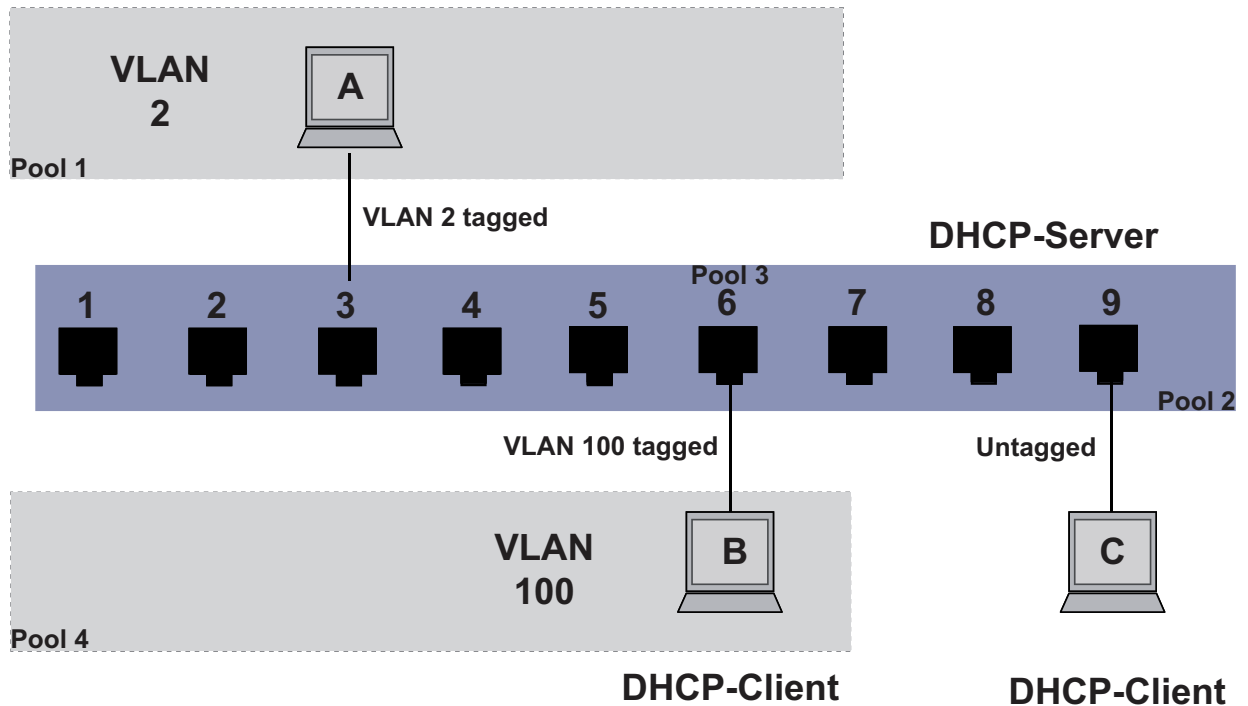


Abb. 12: Anwendungsbeispiel DHCP-Server: IP Adress Pools pro VLAN

Das Anwendungsbeispiel zeigt, wie Sie DHCP-Server Pools pro VLAN oder pro Interface einrichten können.

- Konfigurieren Sie die VLANs (siehe Kapitel „VLANs“ auf Seite 191).
- Definieren Sie die gewünschten IP-Adressbereiche und schalten Sie den DHCP-Server für die gewünschten VLANs ein.

Öffnen Sie den Dialog `Erweitert:DHCP-Server:Pool`.

Klicken Sie die Schaltfläche `Erzeugen`, um die gewünschten Pool-Einträge zu erstellen.

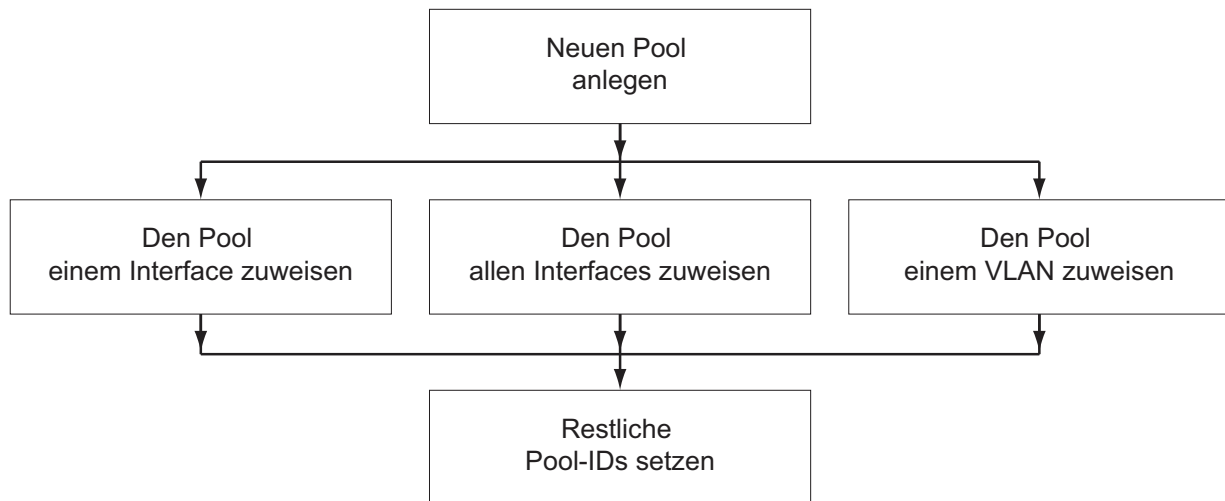


Abb. 13: DHCP-Server: Pool pro VLAN oder für ein/alle Interface(s) anlegen

- Definieren Sie die DHCP Server Pools wie folgt:
  - ▶ Pool 1: Dynamisch. Weisen Sie Pool 1 dem VLAN 2 zu.
  - ▶ Pool 2: Dynamisch. Weisen Sie Pool 2 global zu.
  - ▶ Pool 3: Statisch. Weisen Sie Pool 3 dem Interface 6 zu.
- Konfigurieren Sie die Interfaces für die Clients A und B wie folgt:
  - ▶ Ordnen Sie Interface 3 dem VLAN 2 zu.
  - ▶ Ordnen Sie Interface 6 dem VLAN 100 zu.

DHCP-Anfragen von Client A werden von Pool 1 beantwortet. Falls der Pool aufgebraucht ist, werden weitere Anfragen erst dann beantwortet, wenn Sie einen neuen Pool angelegt haben.

DHCP-Anfragen von Client B werden zunächst ignoriert, da VLAN 100 noch keinen Zugriff auf den DHCP-Server hat.

- Um DHCP-Zugriff zu ermöglichen, fügen Sie Pool 4 hinzu:
  - ▶ Pool 4: Dynamisch. Weisen Sie Pool 4 dem VLAN 100 zu.

Die erste Anfrage wird nun von Pool 3 beantwortet. Die folgenden Anfragen werden von Pool 4 beantwortet.

Die Anfragen von Client C werden von Pool 2 beantwortet.

**Anmerkung:** Wenn Client A (oder B) eine untagged DHCP-Anfrage versendet, antwortet der DHCP-Server ausschließlich, wenn Sie die PVID (Port VLAN Identifier) von Interface 3 (oder 6) auf 2 (oder 100) gesetzt haben. Wenn Sie die PVID eines Interfaces dem Management-VLAN zugeordnet haben, erreichen die Anfragen den DHCP-Server, aber der Client erhält keine Antwort aus dem VLAN-Pool.

**Anmerkung:** Abhängig von den Interface-Einstellungen ist die Antwort vom DHCP-Server tagged or untagged, auch wenn die DHCP-Anfrage tagged ist.

Mit dem CLI konfigurieren Sie Pools pro VLAN wie folgt (Detaillierte Informationen finden Sie im Kapitel „VLANs“ auf Seite 191):

- Wechseln Sie in den "VLAN Database" -Modus.  
Legen Sie ein VLAN an, falls es noch nicht existiert.
- Wechseln Sie in den "Interface"-Modus.  
Definieren Sie die dem VLAN zugehörigen Ports.
- Wechseln Sie in den "Configure"-Modus.  
Legen Sie einen neuen Pool an, falls er noch nicht existiert.  

```
dhcp-server pool add <pool_id> dynamic <startIP> <endIP>
```

  
Das Gerät weist dem Pool zunächst "Alle Interfaces" und „Management-VLAN" zu.
- Ordnen Sie den Pool einer bestimmten VLAN ID zu  

```
dhcp-server pool modify <pool_id> mode vlan <vlan_id>
```
- Schalten Sie den Pool ein.  

```
dhcp-server pool enable <pool_id>
```
- Um das VLAN eines Pools zurückzusetzen (d.h. "Alle Interfaces" und „Management-VLAN" zuweisen):  

```
dhcp-server pool modify <pool_id> mode vlan none
```

**Anmerkung:** Beachten Sie beim Anlegen von Pools pro VLAN:

- ▶ VLAN unterstützt ausschließlich dynamische Pools.
- ▶ Pro VLAN ist ein dynamischer Pool möglich.
- ▶ Schalten Sie einen Pool aus, bevor Sie ihn modifizieren.

## 2.8 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 262](#).

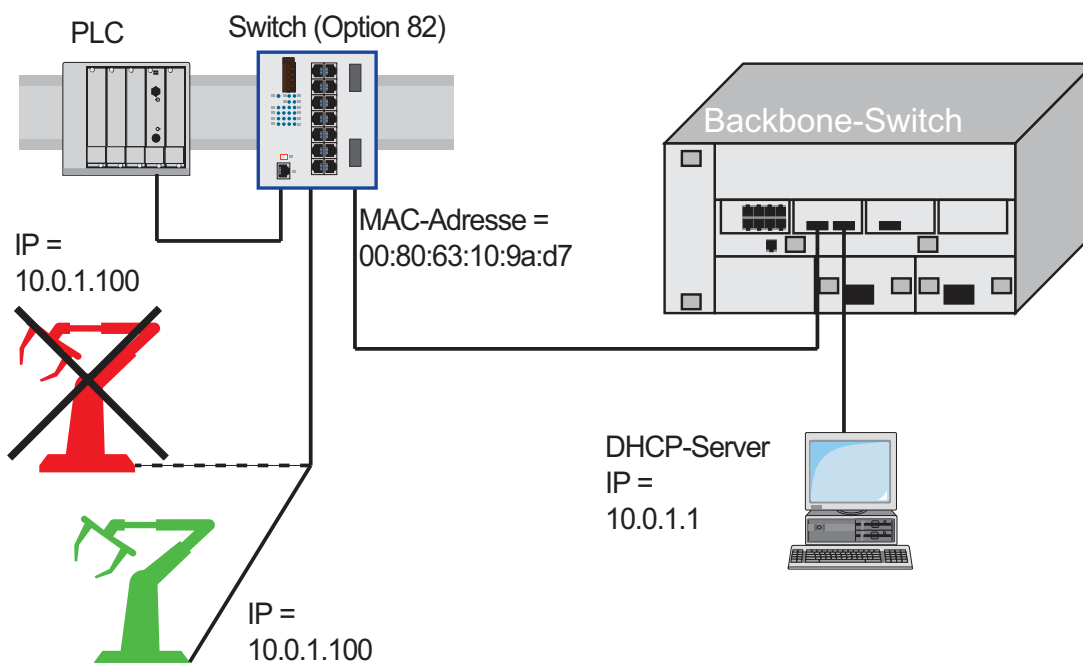


Abb. 14: Anwendungsbeispiel für den Einsatz von Option 82

## 2.9 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.

The screenshot shows a configuration dialog box for network parameters. On the left, under 'Modus', the 'Lokal' radio button is selected. The 'BOOTP / DHCP' section has a 'MAC-Adresse' field with the value '00:80:63:40:77:00'. The 'DHCP' section has a 'Name' field with the value 'MACH4002-407700'. The 'Lokal' section has three fields: 'IP-Adresse' (10.0.1.112), 'Netzmaske' (255.255.255.0), and 'Gateway-Adresse' (0.0.0.0). The 'VLAN' section has an 'ID' field with the value '1'. The 'HIDiscovery Protokoll' section has 'Funktion' set to 'An' and 'Zugriff' set to 'read-write'. At the bottom, there are buttons for 'Schreiben', 'Laden', and 'Hilfe'.

Abb. 15: 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 256.](#)
  - ▶ 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 262.](#)
  - ▶ 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 59 „Einstellungen laden/speichern“](#)).



---

## 2.10 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 262 „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 273 „Schlüssel auf das Gerät laden“](#)).
- Andernfalls erzeugen Sie einen neuen SSH-Schlüssel und laden ihn auf das neue Gerät ([siehe auf Seite 271 „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 65 „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 Skriptdatei 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 Skriptdatei wiederherstellen. Die Skriptdatei kann eine Offline-Konfigurations-Datei (\*.ocf) oder eine CLI-Skriptdatei (\*.cli) sein. Das Gerät ermittelt den Dateityp automatisch.
- ▶ Wenn Sie die Konfiguration aus einer Skriptdatei wiederherstellen, löschen Sie zuerst die Gerätekonfiguration, so dass die Voreinstellungen richtig überschrieben werden. Für weitere Informationen ([siehe auf Seite 64 „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 71 „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. 16: 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 69 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 Skriptdatei 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 211 „Trapeinstellung“](#)),
- ▶ den Gerätestatus zu aktualisieren ([siehe auf Seite 214 „Gerätestatus konfigurieren“](#)),
- ▶ den Zustand der Meldekontakte zu aktualisieren ([siehe auf Seite 217 „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](http://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 211 „Trapeinstellung“](#)),
- ▶ den Gerätestatus zu aktualisieren ([siehe auf Seite 214 „Gerätestatus konfigurieren“](#)),
- ▶ den Zustand der Meldekontakte zu aktualisieren ([siehe auf Seite 217 „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.

|                                             |                                                                                        |
|---------------------------------------------|----------------------------------------------------------------------------------------|
| <code>enable</code>                         | Wechsel in den Privileged-EXEC-Modus.                                                  |
| <code>configure</code>                      | Wechsel in den Global-Configure-Modus.                                                 |
| <code>#boot skip-aca-on-boot enable</code>  | Den ACA21 in der Bootphase überspringen. (Lieferzustand: ausgeschaltet).               |
| <code>#boot skip-aca-on-boot disable</code> | Den ACA21 in der Bootphase berücksichtigen.                                            |
| <code>#show boot skip-aca-on-boot</code>    | 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 lesbare 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
copy nvram:startup-config
 tftp://10.1.112.159/
 switch/config.dat
copy nvram:script
 tftp://10.0.1.159/switch/
 config.txt
```

Wechsel in den Privileged-EXEC-Modus.

Das Gerät speichert die Konfigurationsdaten in eine Binärdatei auf einen tftp-Server im angeschlossenen Netz

Das Gerät speichert die Konfigurationsdaten in eine Skript-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 editier- 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](http://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
show sysinfo
```

Wechsel in den Privileged-EXEC-Modus.  
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. 17: 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 77.](#)

- 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 passenden 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 266 „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.

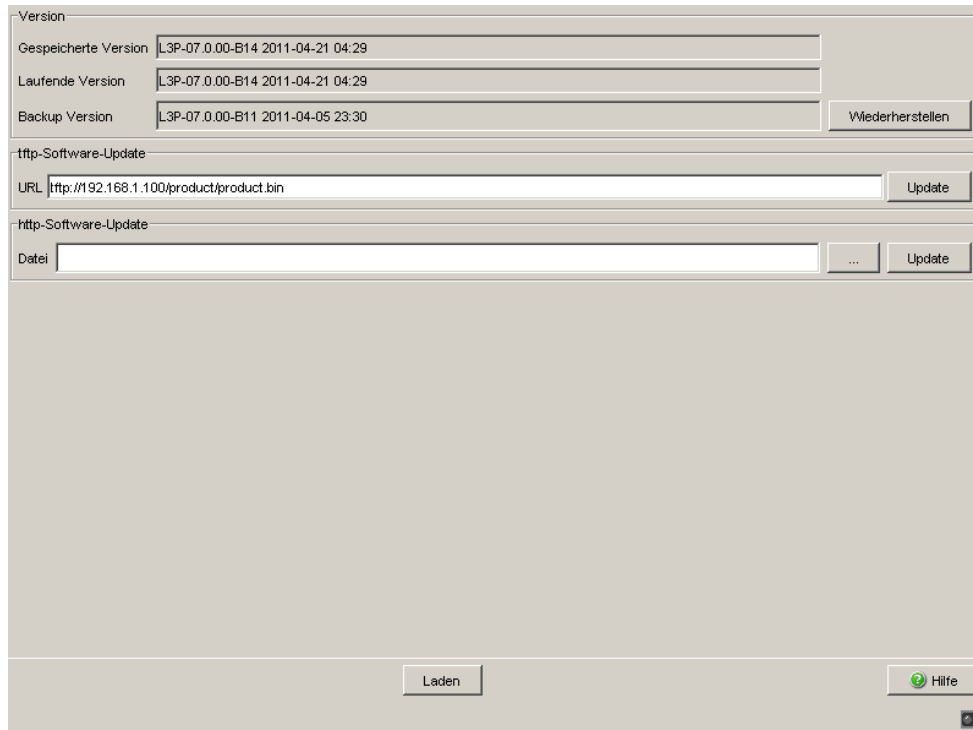


Abb. 18: Dialog Software-Update

- 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
copy
tftp://10.0.1.159/product.b
in system:image
```

Wechsel in den Privileged-EXEC-Modus.  
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 nicht-flüchtigen 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
configure
copy <url> system:bootcode
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Kopieren Sie die Bootcode-Datei vom TFTP-Server auf das Gerät an.

---

## 4.6 Software-Update OCTOPUS

### ■ Bezeichnung der Software-Images für Geräte der OCTOPUS-Familie

| Gerät                                      | Bezeichnung Rel. 7.0 | Bezeichnung Rel. 7.1 |
|--------------------------------------------|----------------------|----------------------|
| OCTOPUS 8M,<br>OCTOPUS 16M,<br>OCTOPUS 24M | omL2P.bin            | octL2P.bin           |
| OCTOPUS OS 20,<br>OCTOPUS OS 30            | orL2P.bin            | osL2P.bin            |
| OCTOPUS OS 32                              | omL2P.bin            | -                    |

Tab. 4: Bezeichnung der Software-Images für Geräte der OCTOPUS-Familie

## ■ Update-Anleitung für die Geräte OCTOPUS 8M, OCTOPUS 16M und OCTOPUS 24M

**Anmerkung:** Voraussetzung für den Software-Update:

Auf dem Gerät ist die Geräte-Software Version 07.0.03 (oder höher) und die Boot-Software Version 05.0.00 (oder höher) installiert.

- Die Version der installierten Geräte-Software und Boot-Software erfahren Sie im CLI mit dem Befehl "show sysinfo".

Beispiel:

```
show sysinfo.....
```

```
...
```

```
Boot Software Release..... L2P-06.0.03
```

```
...
```

```
Running Software Release..... L2P-07.0.03
```

```
...
```

### ▶ Schritt 1:

- Geräte-Software aktualisieren auf Version 07.0.03.
- Gerät neu starten.

### ▶ Schritt 2:

- Boot-Software aktualisieren. Verwenden Sie ausschließlich das CLI mit folgendem Befehl:

```
copy tftp://<server IP>/<path>/octL2P_boot.img
system:bootcode
```

- Gerät neu starten.

### ▶ Schritt 3:

- Geräte-Software aktualisieren auf Version 07.1.00. Achten Sie auf die Bezeichnung der Software-Images.





## 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**

Geräte mit Power over ETHERNET- (PoE-) Medienmodulen oder PoE-Ports bieten Ihnen die Möglichkeit, Endgeräte wie z.B. IP-Telefone über das Twisted-Pair-Kabel mit Strom zu versorgen. PoE-Medienmodule und PoE-Ports unterstützen Power over ETHERNET nach IEEE 802.3af. Die Funktion Power over Ethernet ist global aktiv. Die PoE-fähigen Ports sind aktiv, sobald eine Auslieferung an sie erfolgt.

### **Für die Geräte MACH 102 und MACH 104:**

Das Gerät unterstützt Power over ETHERNET nach IEEE 802.3at (PoE+) und bietet Ihnen die Möglichkeit, Endgeräte wie z.B. IP-Telefone über das Twisted-Pair-Kabel mit Strom zu versorgen.

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 OCTOPUS 8M-PoE:

Das Gerät bietet die nominale Leistung für die Summe aller PoE-Ports zuzüglich einer Reserve. Da das Gerät 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 15 Watt pro PoE-Port an.

### Nominale Leistung für MACH 102 mit Modulen M1-8TP-RJ45-PoE:

Das Gerät kann 2 PoE+-Module M1-8TP-RJ45 PoE aufnehmen und bietet pro Modul eine nominale Leistung von 124 W 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.

### Nominale Leistung für MACH 104 16TX-PoEP:

Das Gerät bietet eine nominale Leistung von 248 W 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.

### Nominale Leistung für MACH 104 20TX-F-4PoE:

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.

### 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
- Für die Geräte MACH 102 und MACH 104:**  
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: 30,0 W
- 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.

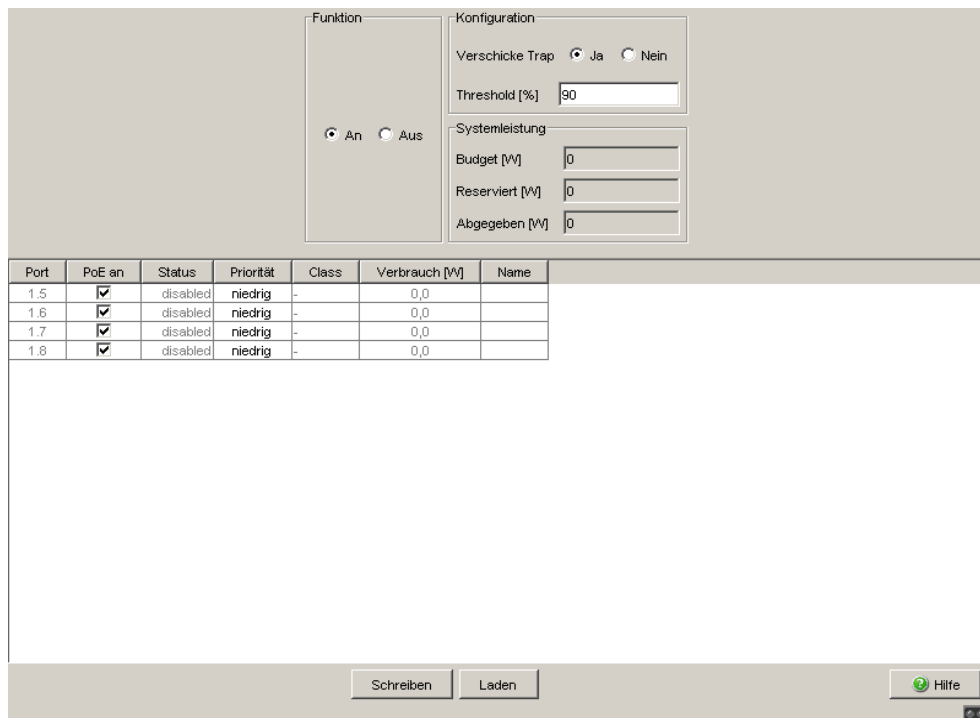


Abb. 19: Dialog Power over Ethernet

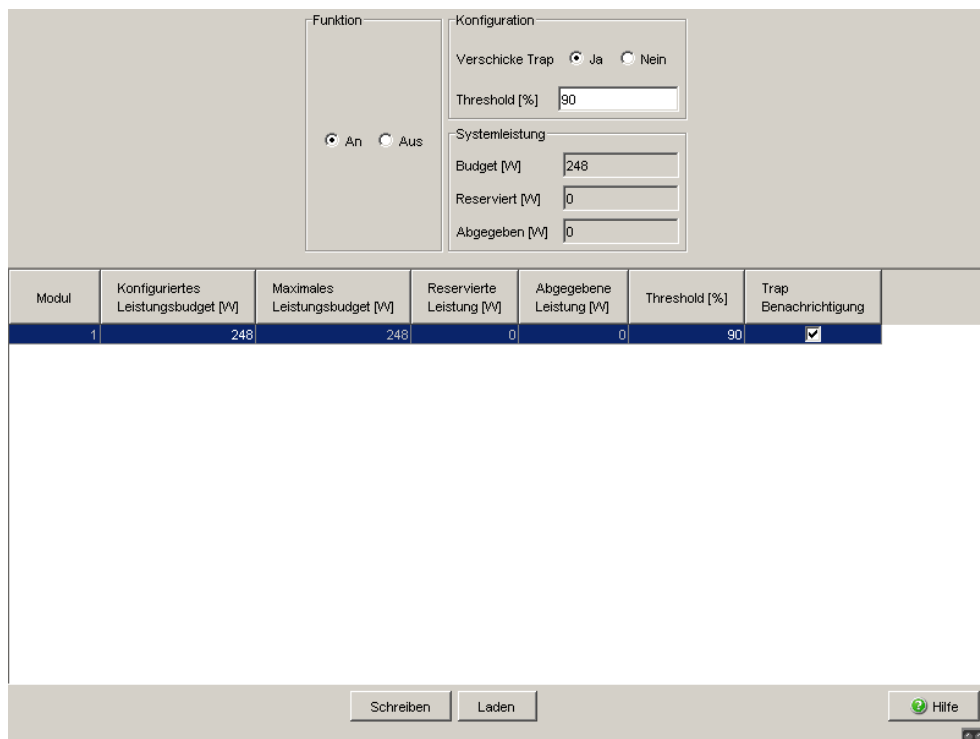


Abb. 20: Dialog Power over Ethernet Plus, Global (MACH 102 und MACH 104)

| Port | PoE an                              | Status    | Priorität | Class | Verbrauch [W] | Name |
|------|-------------------------------------|-----------|-----------|-------|---------------|------|
| 1.5  | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.6  | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.7  | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.8  | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.9  | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.10 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.11 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.12 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.13 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.14 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.15 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.16 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.17 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.18 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.19 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |
| 1.20 | <input checked="" type="checkbox"/> | searching | niedrig   | -     | 0,0           |      |

Buttons: Schreiben, Laden, Hilfe

Abb. 21: Dialog Power over Ethernet Plus, Port (MACH 102 und MACH 104)

## ■ 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
configure
#inlinepower fast-startup
enable
#inlinepower fast-startup
disable
#show inlinepower
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Global-Configure-Modus.

Inline Power Fast Startup einschalten (Lieferzustand: ausgeschaltet).

Inline Power Fast Startup ausschalten.

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 208 „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
configure
#selftest reboot-on-error
enable
#selftest reboot-on-error
seriousOnly
#selftest reboot-on-error
disable
#show selftest
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Global-Configure-Modus.

Die Funktion „Kaltstart bei erkanntem Fehler“ einschalten.

Die Funktion „Kaltstart ausschließlich bei erkanntem schwerwiegenden Fehler“ einschalten.

Die Funktion „Kaltstart bei erkanntem Fehler“ ausschalten (Lieferzustand: eingeschaltet).

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
- ▶ 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 102 „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 108.](#)
- 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 Lese Passwort und das Schreib-/Lese Passwort 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 „Lese Passwort ändern (user)“, um das Lese Passwort einzugeben.
- Geben Sie das neue Lese Passwort in der Zeile „Neues Passwort“ ein und wiederholen Sie die Eingabe in der Zeile „Bitte nochmals eingeben“.
- Wählen Sie „Schreib-/Lese Passwort ändern (admin)“, um das Schreib-/Lese Passwort einzugeben.
- Geben Sie das Schreib-/Lese Passwort 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/Lese Passwort 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. 22: 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.

Die Tabelle lässt bis zu 8 Einträge zu.

Aus Sicherheitsgründen können Lese Passwort und Schreib-/Lese Passwort 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.                                                                                                                                                                                                                                                                           |

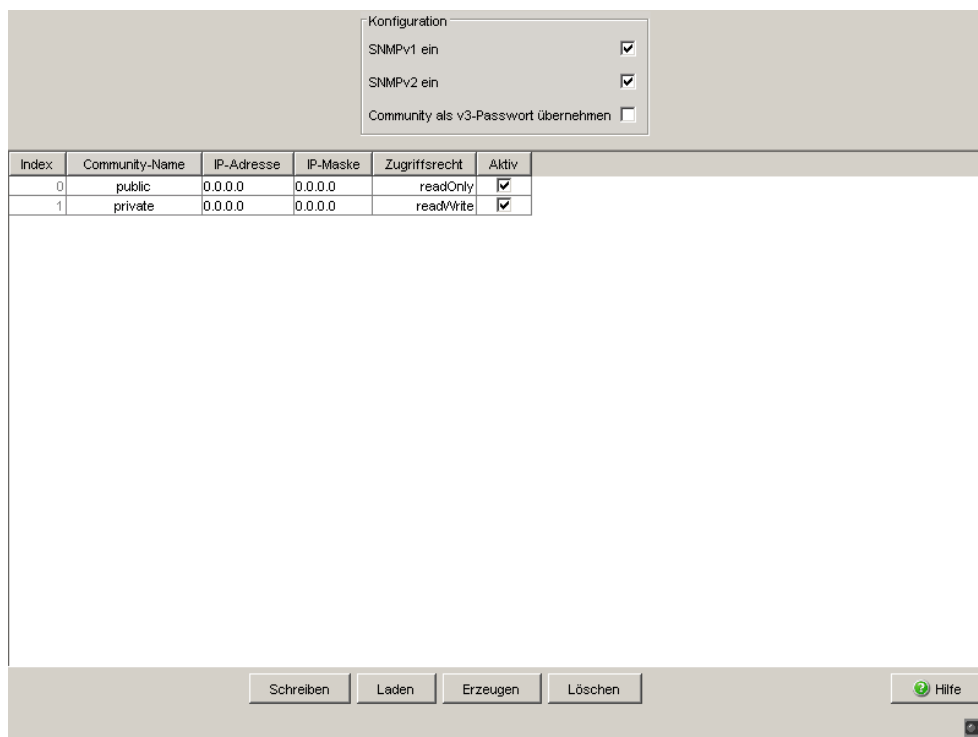


Abb. 23: Dialog SNMPv1/v2-Zugriff

- 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 271.](#)

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 lädt 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>`  
`nvrn: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
ip https server
ip https port <port_no>

no ip https server
ip https server

show ip https

ip https certgen
copy
tftp://<server_ip>/<path_to_
pem> nvram:httpscert
no ip https server
ip https server
```

Wechsel in den Privileged-EXEC-Modus.

HTTPS-Server einschalten.

Die HTTPS-Portnummer für eine gesicherte HTTP-Verbindung setzen.

- Lieferzustand: 443.

- Wertebereich: 1-65535

Nach dem Ändern HTTPS-Portnummer den HTTPS-Server aus- und wieder einschalten, damit die Änderung wirksam wird.

Optional: Den Status des HTTPS-Servers und die HTTPS-Portnummer anzeigen lassen.

X509/PEM-Zertifikat erzeugen.

Ein X509/PEM-Zertifikat für HTTPS über TFTP hoch laden.

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-Adressbereich 109.237.176.0 - 109.237.176.255.

Das Gerät sei bereits auf den SSH-Zugriff vorbereitet ([siehe auf Seite 271 „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. 5: 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.



|                                                                     |                                                                                             |
|---------------------------------------------------------------------|---------------------------------------------------------------------------------------------|
| <code>enable</code>                                                 | Wechsel in den Privileged-EXEC-Modus.                                                       |
| <code>show network mgmt-access</code>                               | Zeigt die momentane Konfiguration an.                                                       |
| <code>network mgmt-access add</code>                                | Legt einen Eintrag für das IT-Netz an. Dieser bekommt die kleinste freie ID, im Beispiel 2. |
| <code>network mgmt-access modify 2<br/>ip 192.168.1.0</code>        | Setzt die IP-Adresse des Eintrags für das IT-Netz.                                          |
| <code>network mgmt-access modify 2<br/>netmask 255.255.255.0</code> | Setzt die Netzmaske des Eintrags für das IT-Netz.                                           |
| <code>network mgmt-access modify 2<br/>telnet disable</code>        | Schaltet Telnet für den Eintrag des IT-Netzes ab.                                           |
| <code>network mgmt-access modify 2<br/>ssh disable</code>           | Schaltet SSH für den Eintrag des IT-Netzes ab.                                              |
| <code>network mgmt-access add</code>                                | Legt einen Eintrag für das Mobilfunk-Netz an. Dieser bekommt im Beispiel die ID 3.          |
| <code>network mgmt-access modify 3<br/>ip 109.237.176.0</code>      | Setzt die IP-Adresse des Eintrags für das Mobilfunk-Netz.                                   |
| <code>network mgmt-access modify 3<br/>netmask 255.255.255.0</code> | Setzt die Netzmaske des Eintrags für das Mobilfunk-Netz.                                    |
| <code>network mgmt-access modify 3<br/>http disable</code>          | Schaltet http für den Eintrag des Mobilfunk-Netzes ab.                                      |
| <code>network mgmt-access modify 3<br/>snmp disable</code>          | Schaltet snmp für den Eintrag des Mobilfunk-Netzes ab.                                      |
| <code>network mgmt-access modify 3<br/>telnet disable</code>        | Schaltet Telnet für den Eintrag des Mobilfunk-Netzes ab.                                    |
| <code>network mgmt-access status 1<br/>disable</code>               | Schaltet den <b>voreingestellten</b> Eintrag ab.                                            |
| <code>network mgmt-access<br/>operation enable</code>               | Schaltet die Funktion <b>sofort</b> ein.                                                    |
| <code>show network mgmt-access</code>                               | Zeigt die momentane Konfiguration der Funktion an.                                          |
| <code>copy system:running-config<br/>nvram:startup-config</code>    | Speichert die gesamte Konfiguration nicht-flüchtig.                                         |

## 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.

|                                                          |                                                                                 |
|----------------------------------------------------------|---------------------------------------------------------------------------------|
| <code>network protocol hidiscovery<br/>off</code>        | HiDiscovery-Funktion ausschalten.                                               |
| <code>network protocol hidiscovery<br/>read-only</code>  | HiDiscovery-Funktion mit dem Zugriffsrecht<br>„lesen“ einschalten               |
| <code>network protocol hidiscovery<br/>read-write</code> | HiDiscovery-Funktion mit dem Zugriffsrecht<br>„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-Adressen 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 Portzugangskontrolle

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<br>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 ( <a href="#">siehe auf Seite 91 „Ports konfigurieren“</a> ) abschalten und einen Alarm verschicken |

Voraussetzungen für die weitere Konfiguration:

- ▶ Der Port für den LAN-Anschluss ist eingeschaltet und richtig konfiguriert ([siehe auf Seite 91 „Ports konfigurieren“](#))
- ▶ Voraussetzungen damit das Gerät einen Alarm (Trap) senden kann ([siehe auf Seite 211 „Trapeinstellung“](#)):
  - Sie haben mindestens einen Empfänger eingetragen,
  - Sie haben für mindestens einen Empfänger in der Spalte „Aktiv“ ein Kreuz gesetzt,
  - 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`.

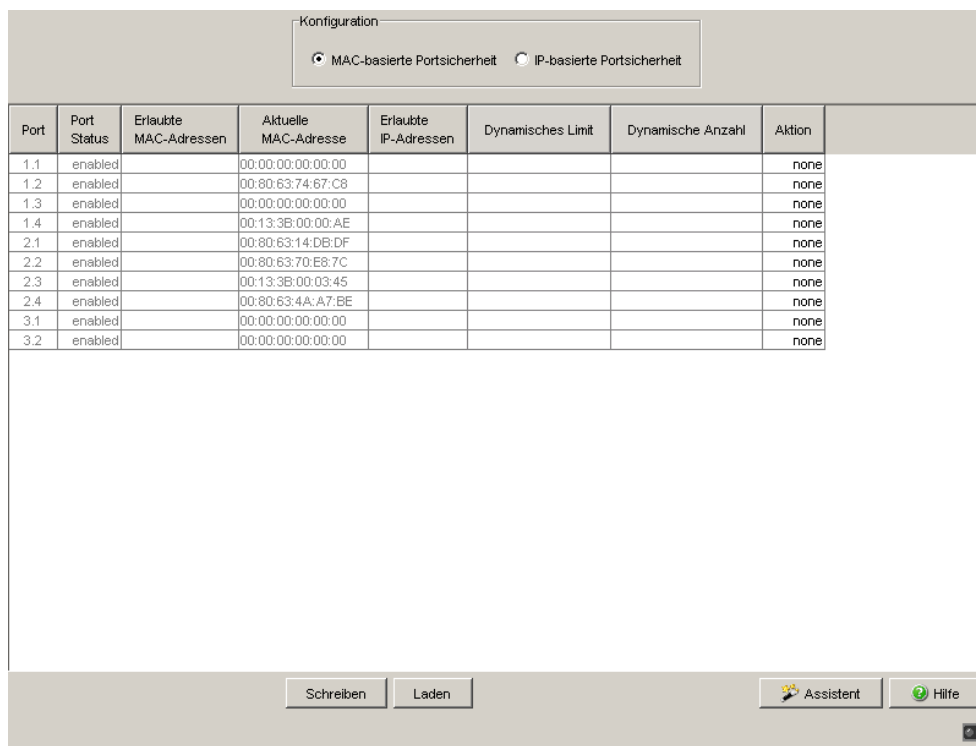


Abb. 24: Dialog Portsicherheit

- 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.

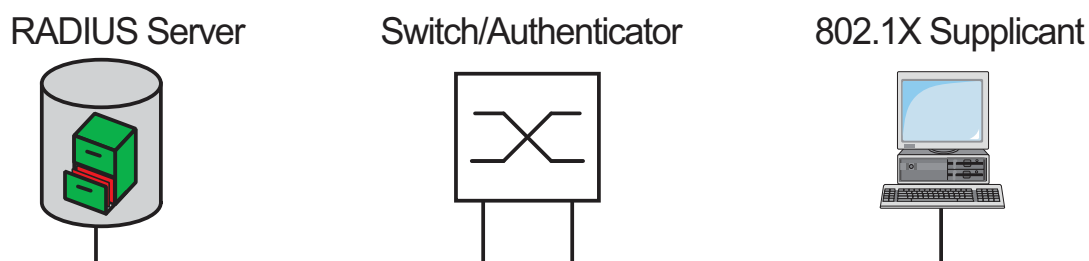


Abb. 25: Radius-Server-Anbindung

## 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.
- ▶ Das Gerät 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 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
set pre-login-banner text
"<string>"
```

```
set pre-login-banner
operation
logout
```

Wechsel in den Privileged-EXEC-Modus.

Weist den Begrüßungstext zu:

- Den Text in Anführungszeichen setzen.
- Max. 255 Zeichen sind zulässig.
- Tabulator durch Zeichenfolge `\\t` einfügen.
- Zeilenumbruch durch Zeichenfolge `\\n` einfügen.

Funktion einschalten.

Vom Gerät abmelden.

Vor dem erneuten Anmelden ist der Text sichtbar.

## 6.9 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
set clibanner text
 "<string>"

set clibanner operation
logout
```

Wechsel in den Privileged-EXEC-Modus.

Weist den Text zu:

- Den Text in Anführungszeichen setzen.
- Max. 2048 Zeichen sind zulässig.
- Tabulator durch Zeichenfolge `\\t` einfügen.
- Zeilenumbruch durch Zeichenfolge `\\n` einfügen.

Funktion einschalten.

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 132 „Konfiguration SNTP“](#)), ([siehe auf Seite 143 „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
configure
sntp time <YYYY-MM-DD
 HH:MM:SS>
sntp client offset
 <-1000 to 1000>
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Einstellen der Systemzeit des Gerätes.

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.

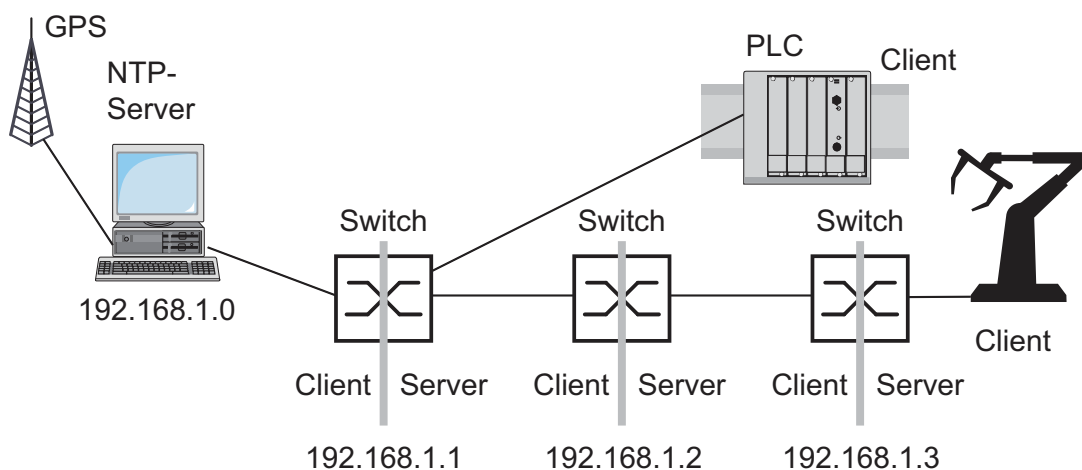


Abb. 26: SNTP-Kaskade

## 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.

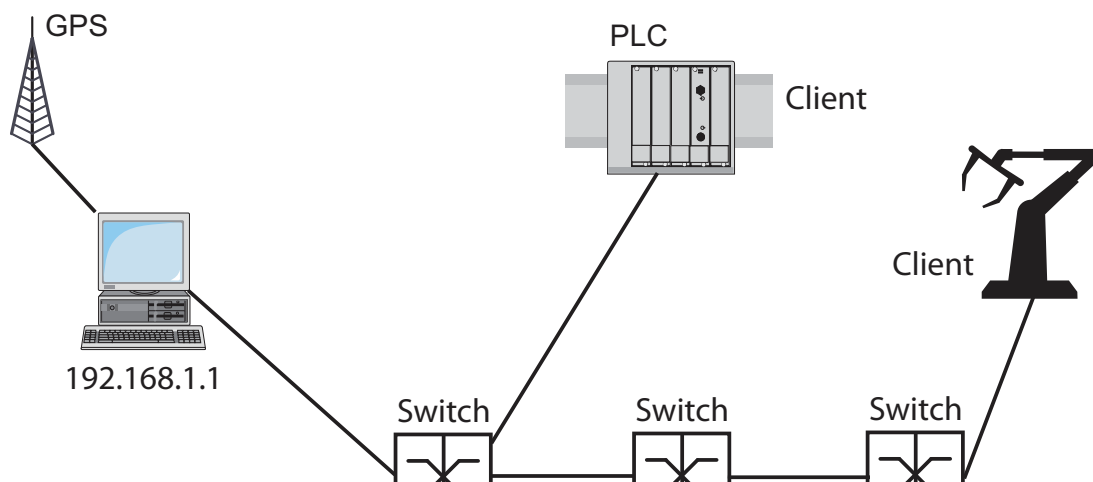


Abb. 27: Beispiel SNTP-Kaskade

- 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 erfolgreicher 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. 28: 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 27)

## **7.3 Precision 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.

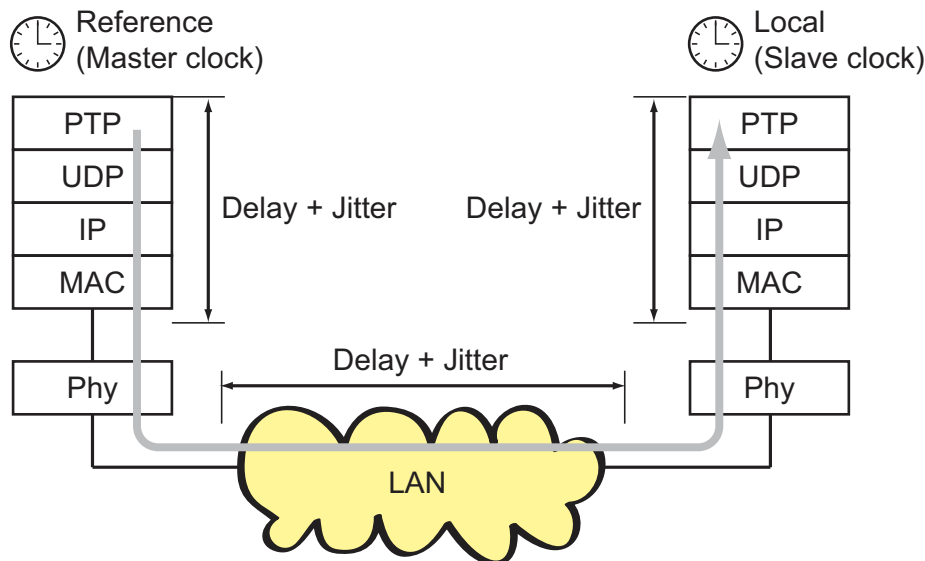
Einfluß auf die Präzision haben:

- ▶ 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 Standard-einstellung 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

- ▶ Kabelllaufzeiten; 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 Datagram Protocol (Transport Layer)  
 IP Internet Protocol (Network Layer)  
 MAC Media Access Control  
 Phy Physical Layer

Abb. 29: Delay- und Jitter beim Uhrenabgleich

Um die Reduktion der Laufzeit und des Jitters im Protokollstapel zu umgehen, empfiehlt IEEE 1588, eine spezielle Hardware-Zeitstempereinheit (Time Stamp Unit) zwischen MAC und Phy einzusetzen. Geräte/Module mit der Namensergänzung „-RT“ besitzen diese Zeitstempereinheit 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“.

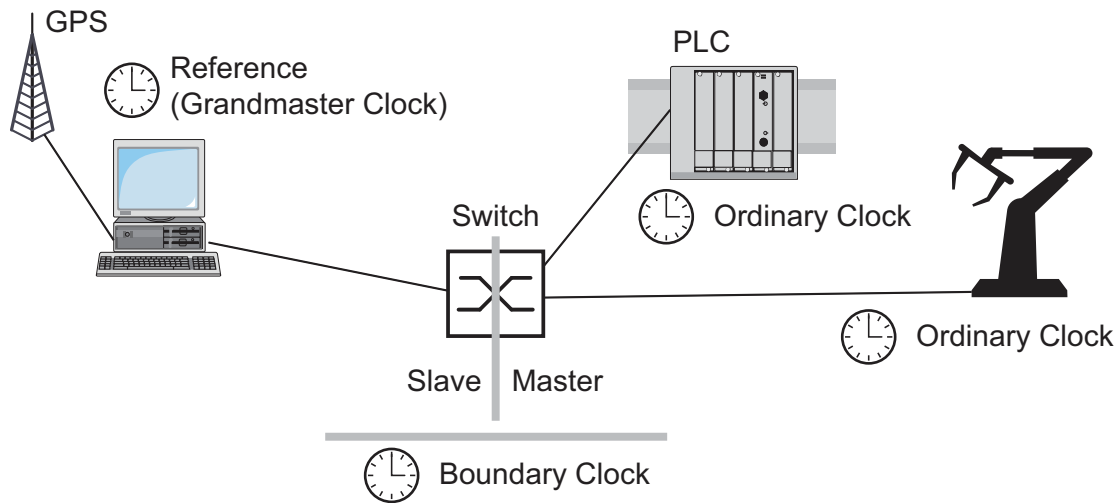


Abb. 30: Position der Boundary-Clock in einem Netz

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.

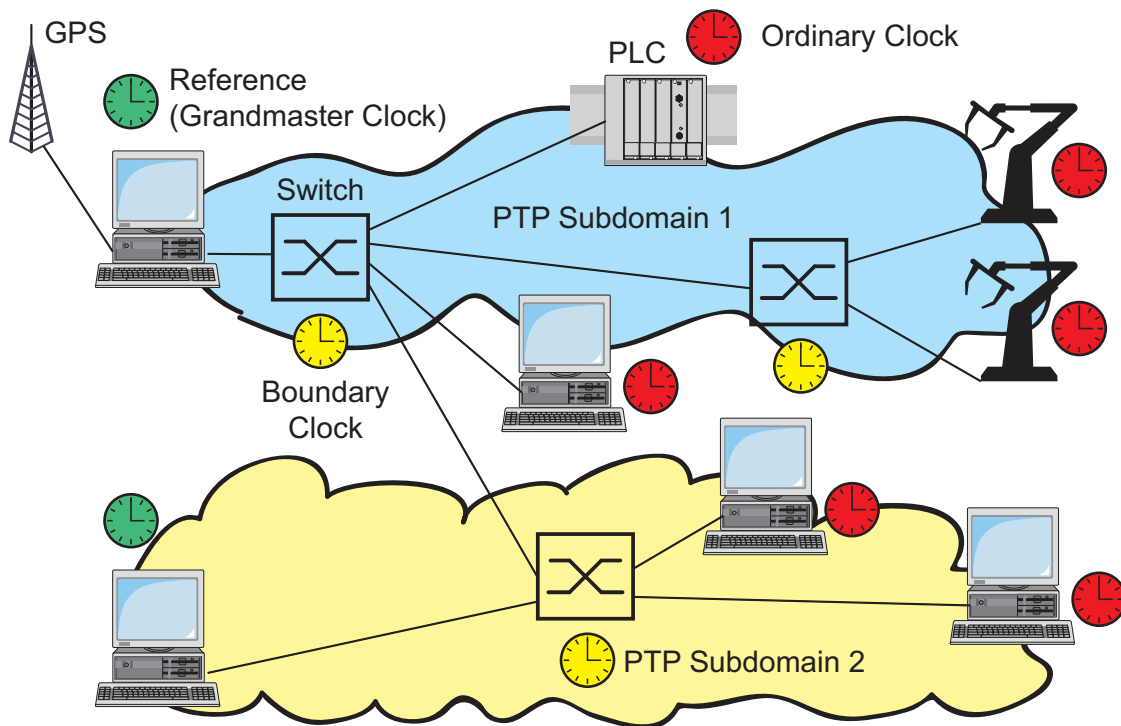


Abb. 31: PTP-Subdomänen

### 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 Zeitstempereinheit (RT-Module) an.

Geräte ohne Zeitstempereinheit 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 Zeitstempereinheit (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 Zeitstempelinheit (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 32](#)) 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“.

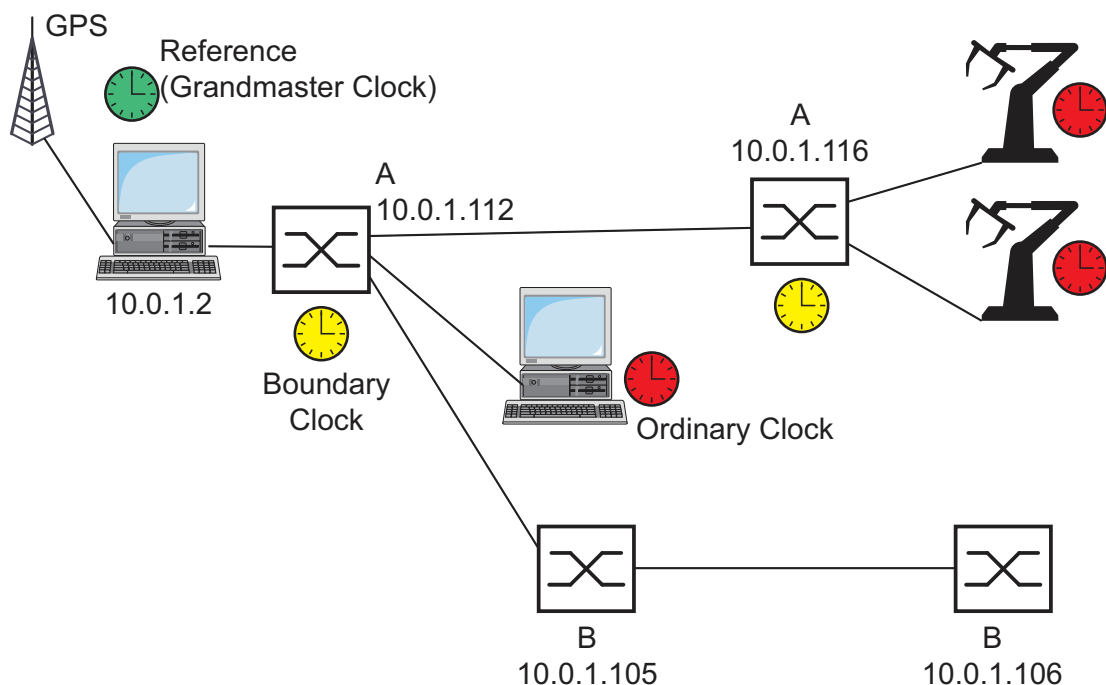


Abb. 32: Beispiel für PTP-Synchronisation .  
A: Gerät mit RT-Modul  
B: Gerät ohne RT-Modul

| 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 32)

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“.

|                                                      |                                                                              |
|------------------------------------------------------|------------------------------------------------------------------------------|
| <code>enable</code>                                  | Wechsel in den Privileged-EXEC-Modus.                                        |
| <code>configure</code>                               | Wechsel in den Konfigurationsmodus.                                          |
| <code>sntp operation on</code>                       | SNTP global einschalten.                                                     |
| <code>sntp operation client on</code>                | SNTP-Client einschalten.                                                     |
| <code>sntp client server primary<br/>10.0.1.2</code> | Die IP-Adresse des externen SNTP-Servers<br>10.0.1.2 eingeben.               |
| <code>sntp client request-interval<br/>30</code>     | Den Wert 30 Sekunden für das SNTP-Server-<br>Anforderungsintervall eingeben. |
| <code>sntp client accept-broadcast<br/>off</code>    | „SNTP-Broadcasts akzeptieren“ ausschalten.                                   |
| <code>sntp operation server on</code>                | SNTP-Server einschalten.                                                     |
| <code>sntp anycast address 0.0.0.0</code>            | Die SNTP-Server-Anycast-Zieladresse 0.0.0.0<br>eingeben.                     |
| <code>sntp anycast vlan 1</code>                     | 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“.

|                                                   |                                     |
|---------------------------------------------------|-------------------------------------|
| <code>ptp operation enable</code>                 | PTP global einschalten.             |
| <code>ptp clock-mode<br/>v1-boundary-clock</code> | 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 „Bevorzugten 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 nichtflüchtig 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 33](#)) zeigt eine solche Anwendung.

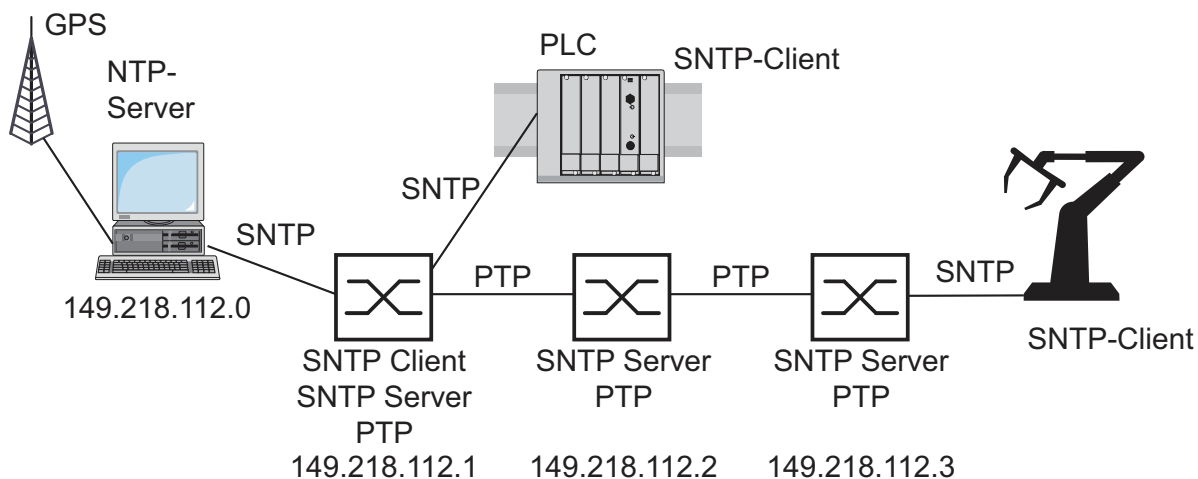


Abb. 33: Beispiel für die Koexistenz von PTP und SNTP

### ■ Anwendungsbeispiel

Die Anforderungen an die Genauigkeit der Uhrzeit im Netz sei recht hoch, die Endgeräte unterstützen jedoch ausschließlich SNTP (siehe [Abbildung 33](#)).

| 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-Anforderungsintervall | 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 Endgeräte 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

- ▶ unbekanntem 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 154 „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 unbekanntem 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  $\geq 30$  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 152 „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 69 „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 angeschlossen 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.

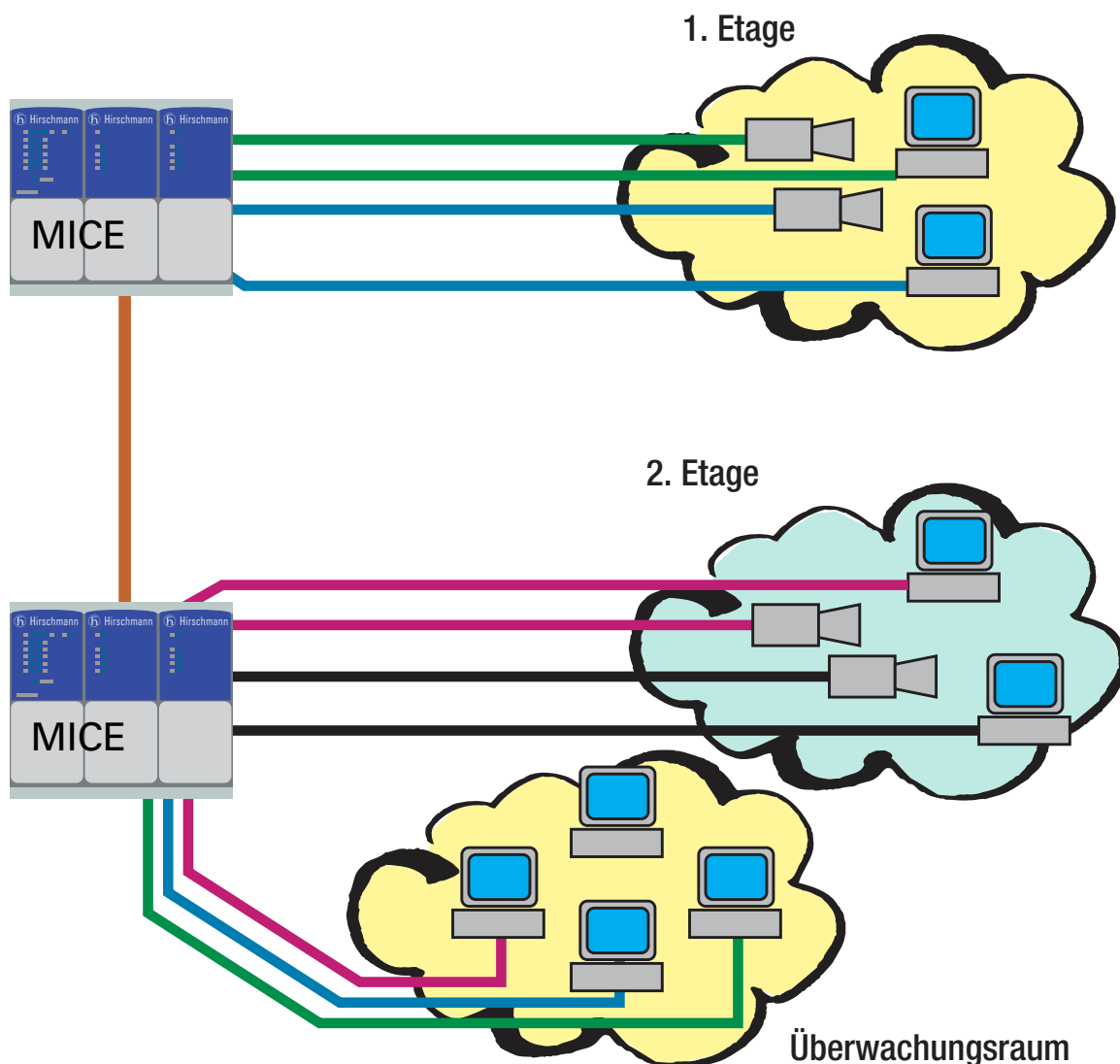


Abb. 34: Beispiel: Video-Überwachung in Maschinenräumen

### 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 162 „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 162 „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 162 „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<br>3         | 1-25 Sekunden<br>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 unbekanntem - nicht mit IGMP-Snooping gelernten - MAC/IP-Multicast-Adressen vermittelt.

„Unbekannte Multicasts“ bietet Ihnen die Möglichkeit, zu bestimmen, wie das Gerät unbekanntem 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 ungelerten 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 Porteeinstellungen.  
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.

| Port | IGMP an                             | IGMP Forw. All           | IGMP Automatic Query Port | Statischer Query Port | Gelernter Query Port     |
|------|-------------------------------------|--------------------------|---------------------------|-----------------------|--------------------------|
| 1.1  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 1.2  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 1.3  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 1.4  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 2.1  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 2.2  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 2.3  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 2.4  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 3.1  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |
| 3.2  | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/>  | disable               | <input type="checkbox"/> |

Abb. 35: 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-Adressen oder leitet die Datenpakete mit unbekanntem Multicast-Adressen 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.

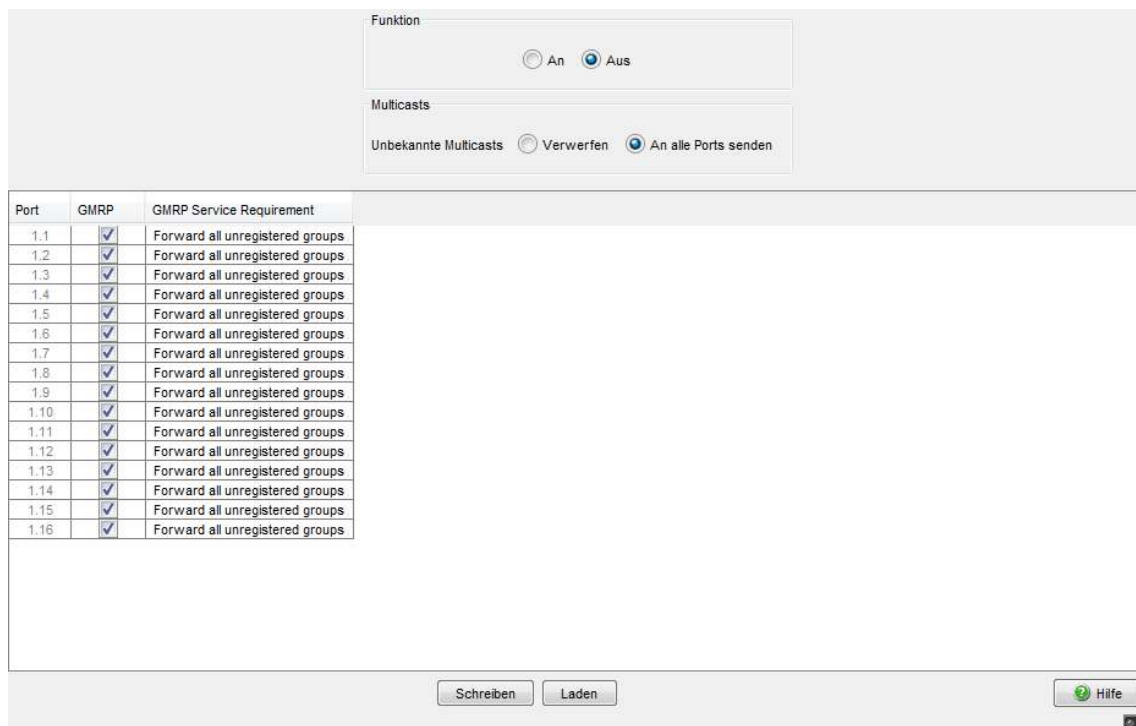


Abb. 36: Dialog GMRP

---

## 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.

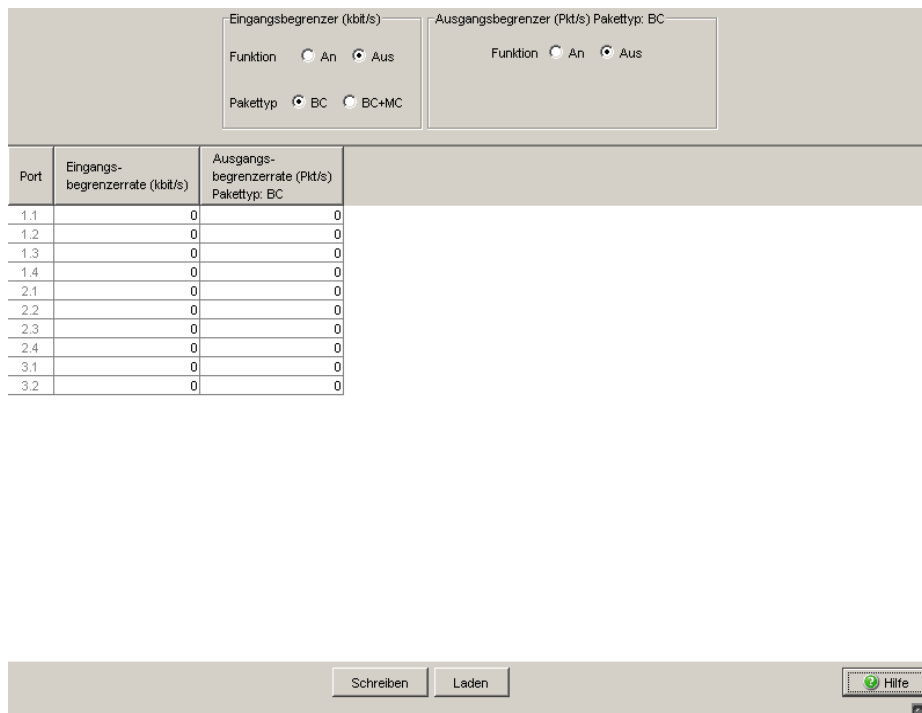


Abb. 37: Dialog Lastbegrenzer

### 8.3.3 Lastbegrenzer-Einstellungen für RS20/RS30/RS40, MS20/MS30, RSR20/RSR30, MACH 100, MACH 1000 und OCTOPUS

- Wählen Sie den Dialog `Switching:Lastbegrenzer`.
- ▶ „Eingangsbegrenzer (kbit/s)“ bietet Ihnen die Möglichkeit, die Eingangsbegrenzerfunktion für alle Ports ein-/auszuschalten.
- ▶ „Ausgangsbegrenzer (Pkt/s)“ bietet Ihnen die Möglichkeit, die Broadcast-Ausgangsbegrenzung an allen Ports ein-/auszuschalten.
- ▶ „Ausgangsbegrenzer (kbit/s)“ bietet Ihnen die Möglichkeit, die Ausgangsbegrenzung für alle Pakettypen an allen Ports ein/auszuschalten.

Einstellmöglichkeiten pro Port:

- ▶ „Eingangspakettypen“ bietet Ihnen die Möglichkeit, den Pakettyp auszuwählen, für den die Begrenzung gelten soll:
  - ▶ All, Begrenzung des gesamten eingangsseitigen Datenvolumens an diesem Port.
  - ▶ BC, Begrenzung des eingangsseitigen Broadcast-Volumens an diesem Port.
  - ▶ BC + MC, Begrenzung des eingangsseitigen Broadcast- und Multicast-Volumens an diesem Port.
  - ▶ BC + MC + uUC, Begrenzung des eingangsseitigen Broadcast-, Multicast- und unbekanntes Unicast-Volumens an diesem Port.
- ▶ Eingangsbegrenzerrate (kbit/s) für den gewählten Eingangspakettyp:
  - ▶ = 0, keine Begrenzung eingangsseitig an diesem Port.
  - ▶ > 0, maximale Übertragungsrate in kbit/s, die an diesem Port empfangen werden darf.
- ▶ Ausgangsbegrenzerrate (Pkt/s) 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.
- ▶ Ausgangsbegrenzerrate (kbit/s) für den gesamten Datenstrom:
  - ▶ = 0, keine Begrenzung des Datenstroms ausgangsseitig an diesem Port.
  - ▶ > 0, maximale Übertragungsrate in kbit/s, die ausgangsseitig an diesem Port gesendet wird.

Eingangsbegrenzer (kbit/s)  
 An  Aus

Ausgangsbegrenzer (Pkt/s) Pakettyp: BC  
 An  Aus

Ausgangsbegrenzer (kbit/s) Pakettypen: alle  
 An  Aus

| Port | Eingangs Pakettypen | Eingangs-<br>begrenzzrate (kbit/s) | Ausgangs-<br>begrenzzrate (Pkt/s)<br>Pakettyp: BC | Ausgangs-<br>begrenzzrate (kbit/s)<br>Pakettypen: alle |
|------|---------------------|------------------------------------|---------------------------------------------------|--------------------------------------------------------|
| 1.1  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.2  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.3  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.4  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.5  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.6  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.7  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.8  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.9  | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.10 | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.11 | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.12 | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.13 | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.14 | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.15 | BC                  | 0                                  | 0                                                 | 0                                                      |
| 1.16 | BC                  | 0                                  | 0                                                 | 0                                                      |

Abb. 38: 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 4 (8 bei MACH 4000, MACH 104, MACH 1040 und PowerMICE) Priority Queues (Traffic Classes nach IEEE 802.1D). Die Zuordnung von empfangenen Datenpaketen zu diesen Klassen erfolgt durch

- ▶ 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 91 „Ports konfigurieren“](#)) und wenn der Port auf „trust dot1p“ konfiguriert wurde.  
Voreinstellung: „trust dot1p“.

Das Gerät berücksichtigt die Klassifizierungsmechanismen in der oben dargestellten Reihenfolge.

Datenpakete können Priorisierungs/QoS-Informationen enthalten:

- ▶ VLAN-Priorität nach IEEE 802.1Q/ 802.1D (Layer 2)

### 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 für RS20/RS30/RS4 0, MACH 1000, MS20/MS30, OCTOPUS (Voreinstellung) | Traffic Class für PowerMICE, MACH 104/MACH H 1040 und MACH 4000 (Voreinstellung) | IEEE 802.1D-Verkehrstyp                                 |
|------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------|---------------------------------------------------------|
| 0                      | 1                                                                                 | 2                                                                                | Best Effort (default)                                   |
| 1                      | 0                                                                                 | 0                                                                                | Background                                              |
| 2                      | 0                                                                                 | 1                                                                                | Standard                                                |
| 3                      | 1                                                                                 | 3                                                                                | Excellent Effort (business critical)                    |
| 4                      | 2                                                                                 | 4                                                                                | Controlled load (streaming multimedia)                  |
| 5                      | 2                                                                                 | 5                                                                                | Video, less than 100 milliseconds of latency and jitter |

Tab. 13: Zuordnung der im Tag eingetragenen Priorität zu den Traffic Classes

| Eingetragene Priorität | Traffic Class für RS20/RS30/RS4 0, MACH 1000, MS20/MS30, OCTOPUS (Voreinstellung) | Traffic Class für PowerMICE, MACH 104/MACH H 1040 und MACH 4000 (Voreinstellung) | IEEE 802.1D-Verkehrstyp                                |
|------------------------|-----------------------------------------------------------------------------------|----------------------------------------------------------------------------------|--------------------------------------------------------|
| 6                      | 3                                                                                 | 6                                                                                | Voice; less than 10 milliseconds of latency and jitter |
| 7                      | 3                                                                                 | 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 3 (RS20/30/40, MS20/30, RSR20/RSR30, MACH 1000, OCTOPUS) bzw. 7 (PowerMICE, MACH 104/MACH 1040, MACH 4000). Wählen Sie deshalb andere Traffic Classes für Anwendungsdaten.

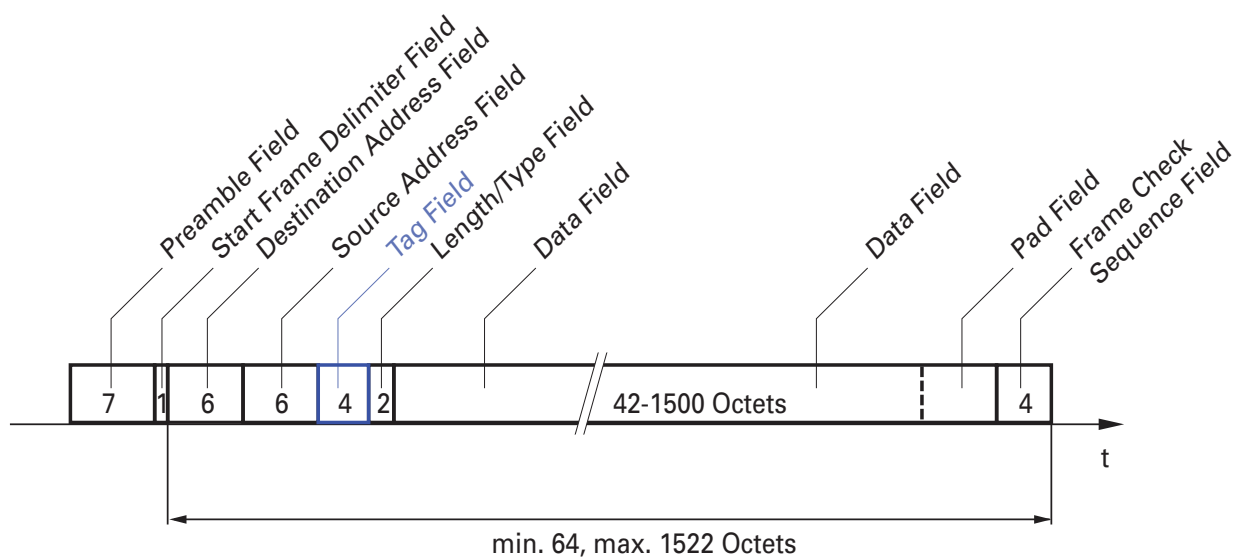


Abb. 39: Ethernet-Datenpaket mit Tag

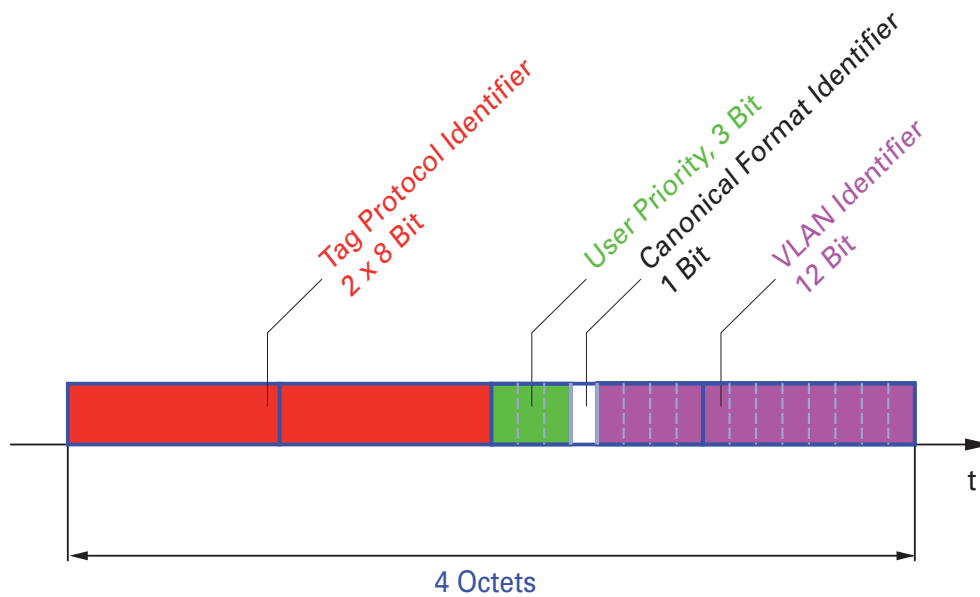


Abb. 40: Tag-Format

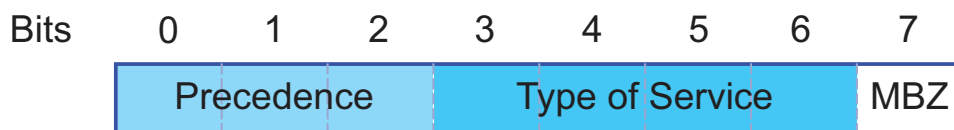
Beim Einsatz der VLAN-Priorisierung beachten Sie folgende Besonderheiten:

- ▶ 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 Dienstgütern 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 Dienstgütern. 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 - Immediat                    |                                     |                  |
| 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 41) - 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.

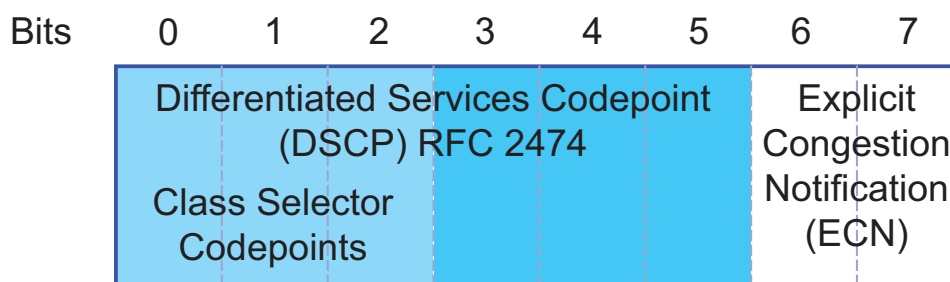


Abb. 41: Differentiated-Services-Feld im IP-Header

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)      |
| Immmediate           | 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 für<br>MACH 4000,<br>MACH 104,<br>MACH 1040, Power-<br>MICE<br>(Voreinstellung) | Traffic Class für<br>RS20/RS30/RS40,<br>RSR20/RSR30,<br>MS20/MS30,<br>OCTOPUS,<br>MACH 1000<br>(Voreinstellung) |
|-------------------|------------------|-----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------|
| 0                 | Best Effort /CS0 | 2                                                                                             | 1                                                                                                               |
| 1-7               |                  | 2                                                                                             | 1                                                                                                               |
| 8                 | CS1              | 0                                                                                             | 0                                                                                                               |
| 9,11,13,15        |                  | 0                                                                                             | 0                                                                                                               |
| 10,12,14          | AF11,AF12,AF13   | 0                                                                                             | 0                                                                                                               |
| 16                | CS2              | 1                                                                                             | 0                                                                                                               |
| 17,19,21,23       |                  | 1                                                                                             | 0                                                                                                               |
| 18,20,22          | AF21,AF22,AF23   | 1                                                                                             | 0                                                                                                               |
| 24                | CS3              | 3                                                                                             | 1                                                                                                               |
| 25,27,29,31       |                  | 3                                                                                             | 1                                                                                                               |
| 26,28,30          | AF31,AF32,AF33   | 3                                                                                             | 1                                                                                                               |
| 32                | CS4              | 4                                                                                             | 2                                                                                                               |
| 33,35,37,39       |                  | 4                                                                                             | 2                                                                                                               |
| 34,36,38          | AF41,AF42,AF43   | 4                                                                                             | 2                                                                                                               |
| 40                | CS5              | 5                                                                                             | 2                                                                                                               |
| 41,42,43,44,45,47 |                  | 5                                                                                             | 2                                                                                                               |
| 46                | EF               | 5                                                                                             | 2                                                                                                               |
| 48                | CS6              | 6                                                                                             | 3                                                                                                               |
| 49-55             |                  | 6                                                                                             | 3                                                                                                               |
| 56                | CS7              | 7                                                                                             | 3                                                                                                               |
| 57-63             |                  | 7                                                                                             | 3                                                                                                               |

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 Ihnen 3 Möglichkeiten, global für alle Ports (je Port beim PowerMICE, MACH 104, MACH 1040 und MACH 4000) zu wählen, wie es empfangene Datenpakete behandelt, die eine Prioritätsinformation enthalten.

- ▶ **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 174 „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

### ■ 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 höherprioritem Verkehr zum Senden ansteht.

Bei verzögerungsempfindlichen Anwendungen wie VoIP oder Video ermöglicht Strict-Priority das unmittelbare Senden hochpriorer Daten.

## 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 173 „Beschreibung Priorisierung“).

**Anmerkung:** Falls Sie VLANs eingerichtet haben, beachten Sie den „VLAN 0-Transparent Modus“ (siehe `Switching:VLAN:Global`).

```
enable
configure
interface 1/1

vlan priority 3
exit
```

Wechsel in den Privileged-EXEC-Modus.  
Wechsel in den Konfigurationsmodus.  
Wechsel in den Interface-Konfigurationsmodus von Port 1.1.  
Weist dem Interface 1/1 die Port-Priorität 3 zu.  
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
configure
classofservice dot1p-
mapping 0 2
classofservice dot1p-
mapping 1 2
exit
show classofservice dot1p-
mapping
```

Wechsel in den Privileged-EXEC-Modus.  
Wechsel in den Konfigurationsmodus.  
Weist der VLAN-Priorität 0 die Traffic Class 2 zu.  
Weist der VLAN-Priorität 1 auch die Traffic Class 2 zu.  
Wechsel in den Privileged-EXEC-Modus.  
Zeigt die Zuordnung an.

| User Priority<br>----- | Traffic Class<br>----- |
|------------------------|------------------------|
| 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<br>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<br>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<br>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 |                                            |



### ■ 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 192 „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 Der Management-Priorität den Wert 7 zuweisen,
 7 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 Der Management-Priorität den Wert cs7 zuweisen,
 cs7 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 42](#)) 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 Sendewarteschlange 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.

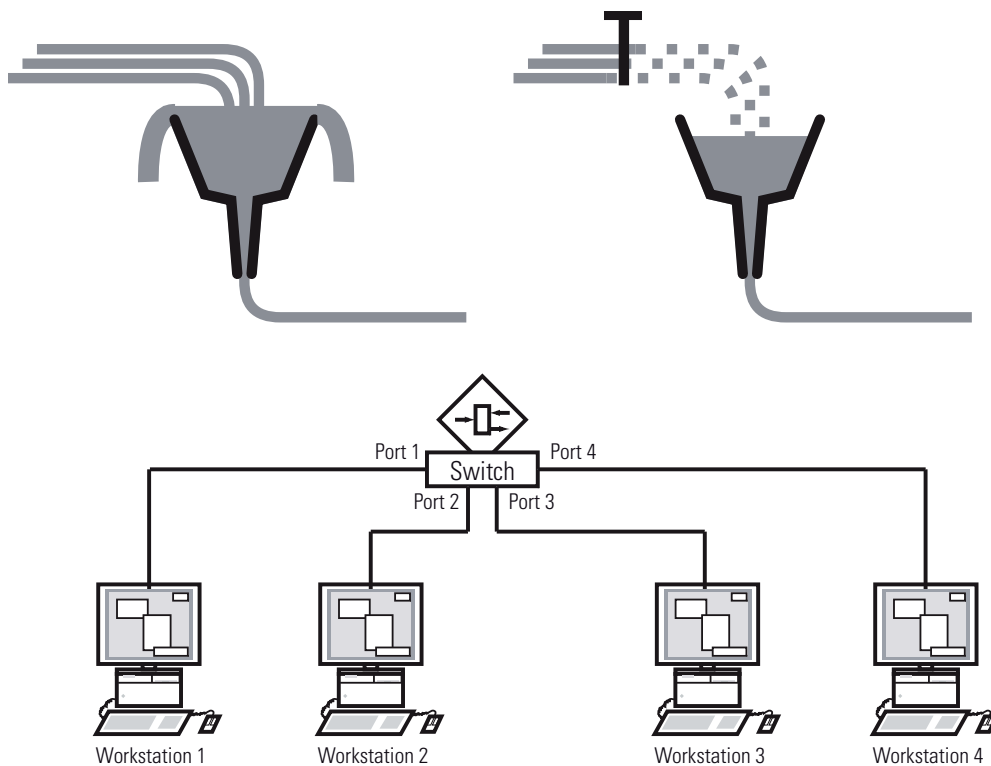


Abb. 42: Beispiel für Flusskontrolle

### ■ Flusskontrolle bei Vollduplex-Verbindung

Im Beispiel (siehe [Abbildung 42](#)) sei zwischen der Workstation 2 und dem Gerät eine Vollduplex-Verbindung.

Bevor die Sendewarteschlange 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 42](#)) 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 „Flusskontrolle 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 unbekanntem (nicht gelerntem) Zieladressen ausschließlich innerhalb des virtuellen LANs vermitteln. Der Rest des Datennetzes übermitteln 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

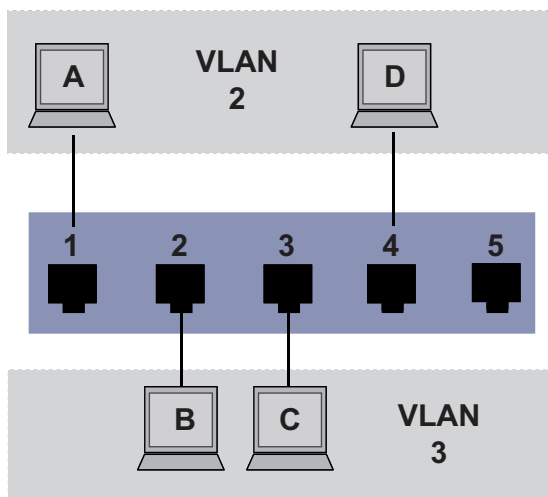


Abb. 43: Beispiel für ein einfaches portbasiertes VLAN

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 Identifier (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`.



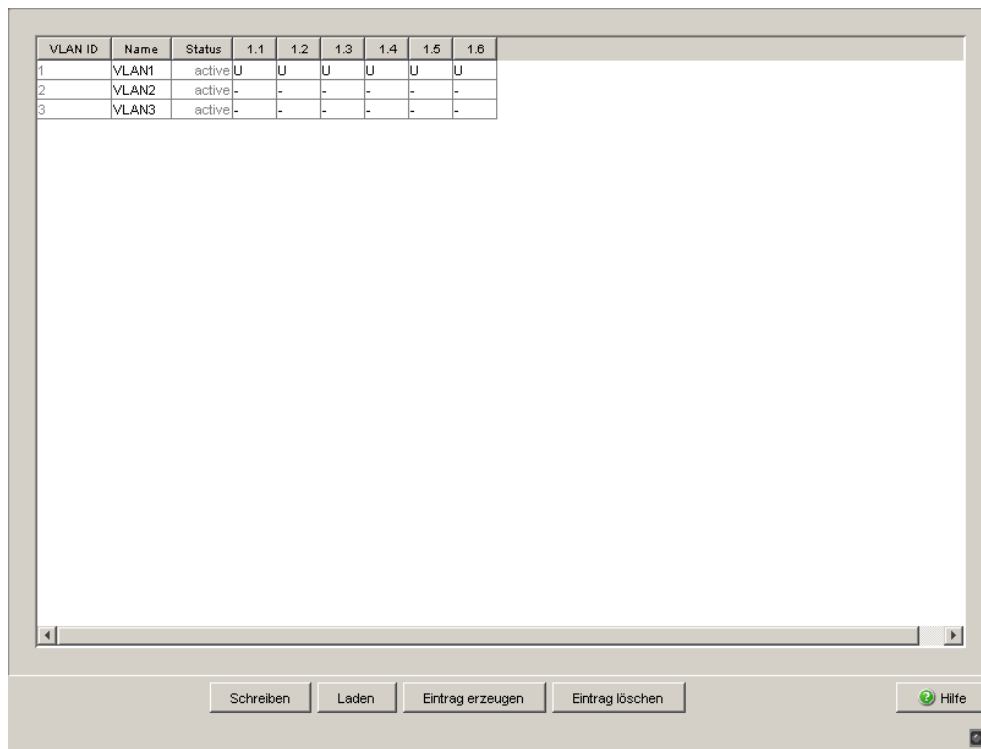


Abb. 44: Neue VLANs erzeugen und benennen

- 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
vlan database
vlan 2
vlan name 2 VLAN2

vlan 3
vlan name 3 VLAN3

vlan name 1 VLAN1

exit
```

Wechsel in den Privileged-EXEC-Modus.  
 Wechsel in den VLAN-Konfigurationsmodus.  
 Erzeugt ein neues VLAN mit der VLAN-ID 2.  
 Benennt das VLAN mit der VLAN-ID 2 mit dem Namen VLAN2.  
 Erzeugt ein neues VLAN mit der VLAN-ID 3.  
 Benennt das VLAN mit der VLAN-ID 3 mit dem Namen VLAN3.  
 Benennt das VLAN mit der VLAN-ID 1 mit dem Namen VLAN1.  
 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

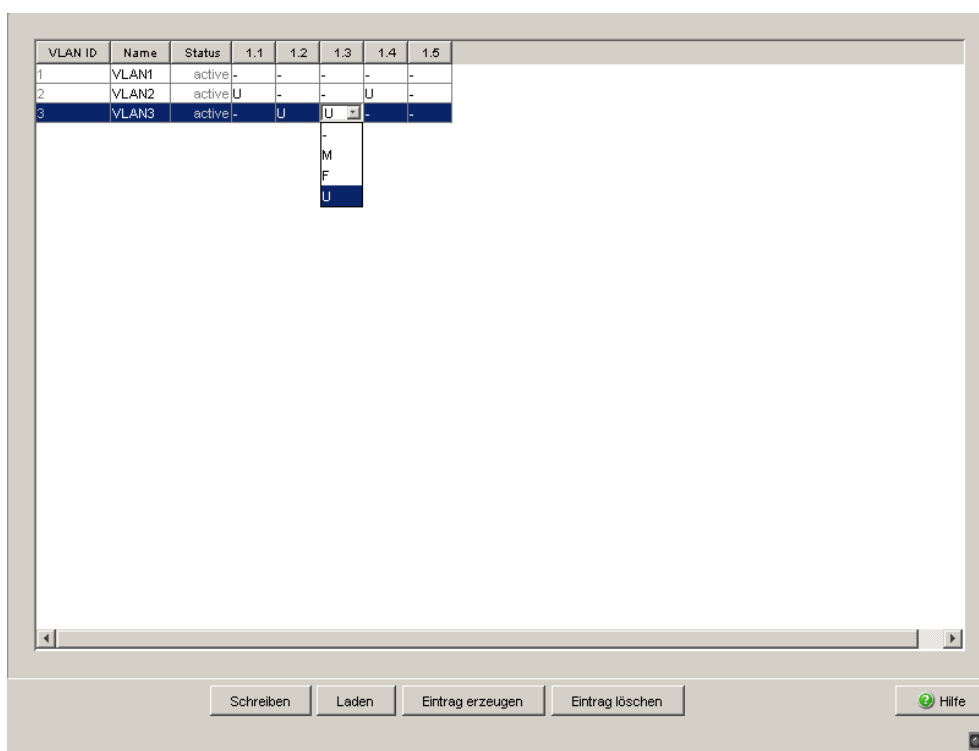


Abb. 45: VLAN-Zugehörigkeit der Ports definieren.

- Weisen Sie die Ports des Gerätes den entsprechenden VLANs zu, indem Sie durch einen Klick in die zugehörigen Tabellenzellen das Auswahlmengü 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`.

| Port | Port-VLAN-ID | Acceptable Frame Types | Ingress Filtering        | GVRP                                |
|------|--------------|------------------------|--------------------------|-------------------------------------|
| 1.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.2  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.3  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.4  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.2  | 1            | admitOnlyVlanTag       | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.3  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.4  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.2  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Abb. 46: „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.

|                                           |                                                            |
|-------------------------------------------|------------------------------------------------------------|
| <code>enable</code>                       | Wechsel in den Privileged-EXEC-Modus.                      |
| <code>configure</code>                    | Wechsel in den Konfigurationsmodus.                        |
| <code>interface 1/1</code>                | Wechsel in den Interface-Konfigurationsmodus von Port 1.1. |
| <code>vlan participation include 2</code> | Port 1/1 wird member untagged in VLAN 2.                   |

```

vlan pvid 2
exit
interface 1/2

vlan participation include 3
vlan pvid 3
exit
interface 1/3

vlan participation include 3
vlan pvid 3
exit
interface 1/4

vlan participation include 2
vlan pvid 2
exit
exit
show vlan 3
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

```

Port 1/1 wird die Port-VLAN-ID 2 zugewiesen.  
 Wechsel in den Konfigurationsmodus.  
 Wechsel in den Interface-Konfigurationsmodus des Ports 1.2.  
 Port 1/2 wird member untagged in VLAN 3.  
 Port 1/2 wird die Port-VLAN-ID 3 zugewiesen.  
 Wechsel in den Konfigurationsmodus.  
 Wechsel in den Interface-Konfigurationsmodus von Interface 1.3.  
 Port 1/3 wird member untagged in VLAN 3.  
 Port 1/3 wird die Port-VLAN-ID 3 zugewiesen.  
 Wechsel in den Konfigurationsmodus.  
 Wechsel in den Interface-Konfigurationsmodus von Port 1/4.  
 Port 1/4 wird member untagged in VLAN 2.  
 Port 1/4 wird die Port-VLAN-ID 2 zugewiesen.  
 Wechsel in den Konfigurationsmodus.  
 Wechsel in den Privileged-EXEC-Modus.  
 Zeigt Details zum VLAN 3 an.

■ **Beispiel 2**

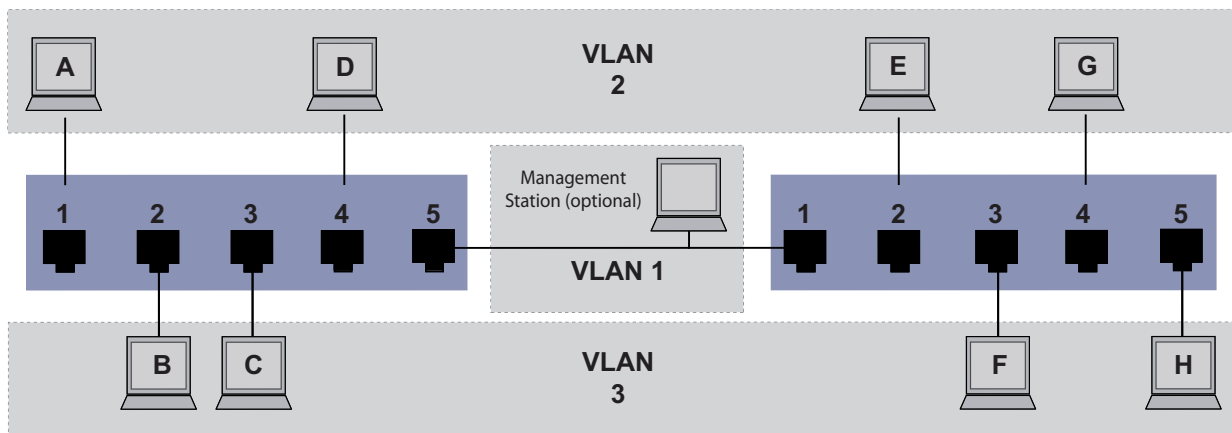


Abb. 47: Beispiel für eine komplexere VLAN-Konfiguration

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 Identifier (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 Identifier (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.

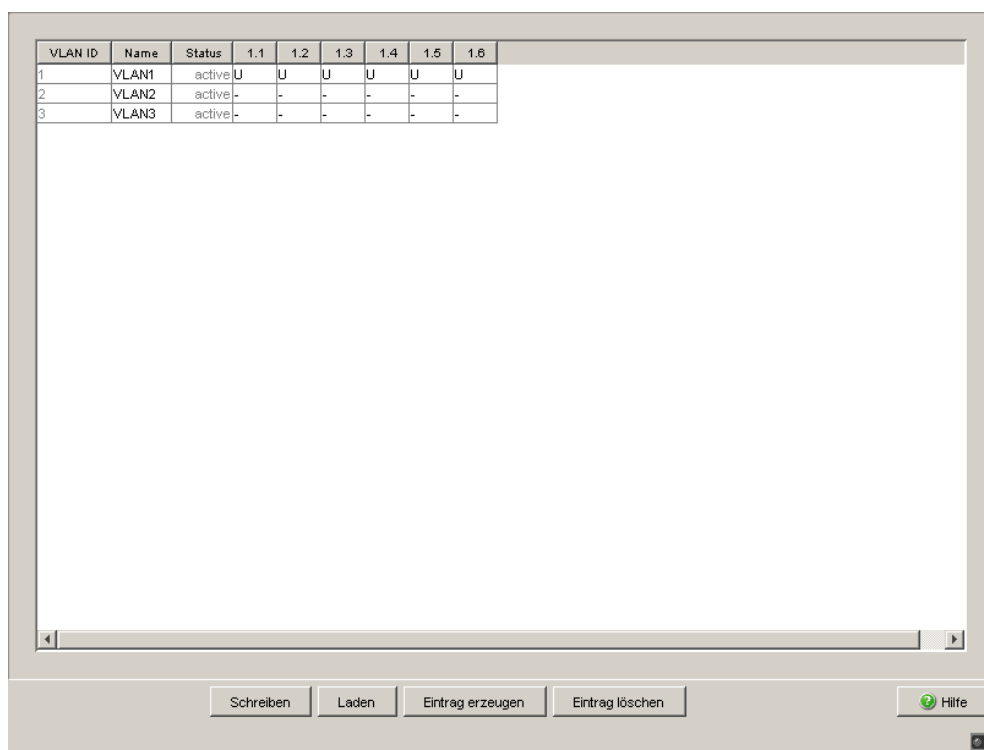
Dabei kommt innerhalb des VLANs mit der ID 1 (Uplink) das VLAN-Tagging (IEEE 801.1Q) zum Einsatz. Dies erkennen Sie am Buchstaben  $\mathbb{T}$  in der Egress-Tabelle der Ports.

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`.



| VLAN ID | Name  | Status | 1.1 | 1.2 | 1.3 | 1.4 | 1.5 | 1.6 |
|---------|-------|--------|-----|-----|-----|-----|-----|-----|
| 1       | VLAN1 | active | U   | U   | U   | U   | U   | U   |
| 2       | VLAN2 | active | -   | -   | -   | -   | -   | -   |
| 3       | VLAN3 | active | -   | -   | -   | -   | -   | -   |

Abb. 48: 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
vlan database
vlan 2
vlan name 2 VLAN2

vlan 3
vlan name 3 VLAN3

vlan name 1 VLAN1

exit
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den VLAN-Konfigurationsmodus.

Erzeugt ein neues VLAN mit der VLAN-ID 2.

Benennt das VLAN mit der VLAN-ID 2 mit dem Namen VLAN2.

Erzeugt ein neues VLAN mit der VLAN-ID 3.

Benennt das VLAN mit der VLAN-ID 3 mit dem Namen VLAN3.

Benennt das VLAN mit der VLAN-ID 1 mit dem Namen VLAN1.

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

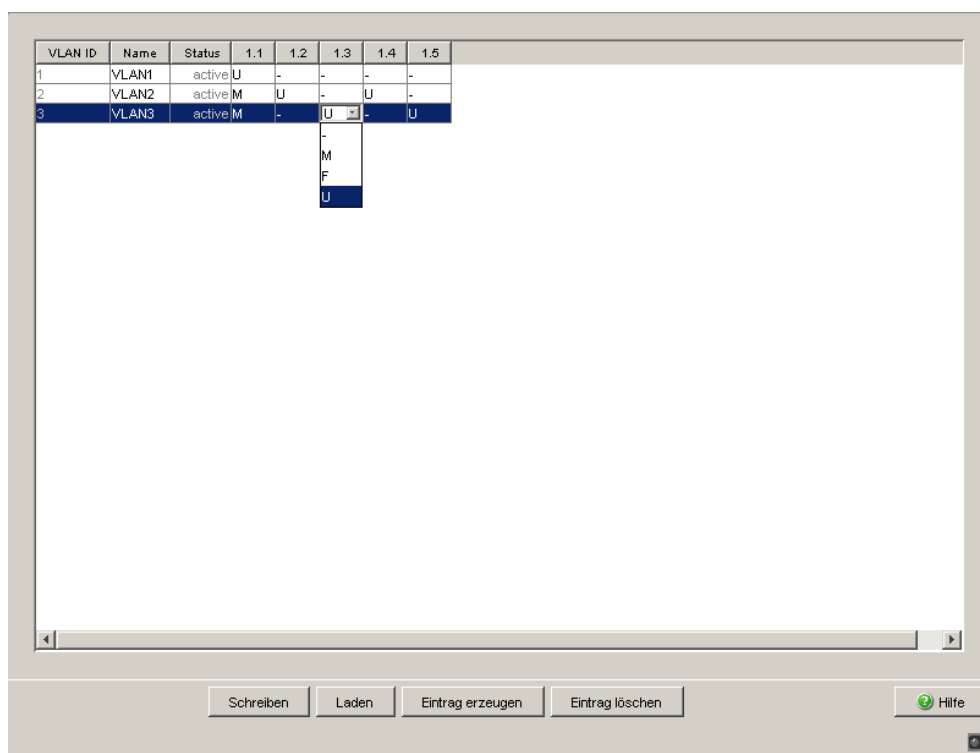


Abb. 49: VLAN-Zugehörigkeit der Ports definieren.

- Weisen Sie die Ports des Gerätes den entsprechenden VLANs zu, indem Sie durch einen Klick in die zugehörigen Tabellenzellen das Auswahlmengü 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`.

| Port | Port-VLAN-ID | Acceptable Frame Types | Ingress Filtering        | GVRP                                |
|------|--------------|------------------------|--------------------------|-------------------------------------|
| 1.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.2  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.3  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 1.4  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.2  | 1            | admitOnlyVlanTag       | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.3  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2.4  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.1  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3.2  | 1            | admitAll               | <input type="checkbox"/> | <input checked="" type="checkbox"/> |

Abb. 50: „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.



## 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<br>– hmPortSecPermission entspricht und<br>– 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. 23: 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.                                                                                                                                                                                |
| 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.                                                                                                                                                          |
| hmAddressRelearnDetectTrap  | 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 gesendet, 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. 23: 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:Alarmer (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.

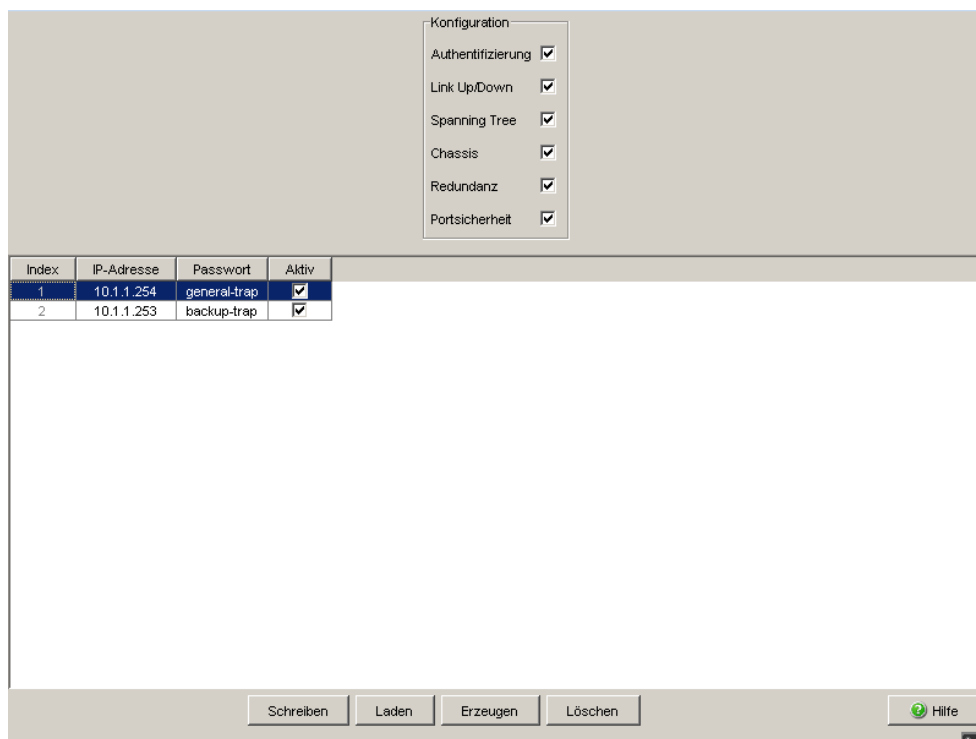


Abb. 51: Dialog Alarmer

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           | <p>Fasst die folgenden Ereignisse zusammen:</p> <ul style="list-style-type: none"> <li>– Der Status einer Versorgungsspannung hat sich geändert (siehe Dialog System).</li> <li>– Der Status des Meldekontakts hat sich geändert.</li> </ul> <p>Um dieses Ereignis zu berücksichtigen, aktivieren Sie „Trap bei Statuswechsel erzeugen“ im Dialog <code>Diagnose:Meldekontakt 1/2</code>.</p> <ul style="list-style-type: none"> <li>– Der AutoConfiguration Adapter (ACA) wurde hinzugefügt oder entfernt.</li> <li>– Die Konfiguration auf dem AutoConfiguration Adapter (ACA) unterscheidet sich von der im Gerät.</li> <li>– Die Temperaturschwellen wurden unter- oder überschritten.</li> <li>– Ein Medienmodul wurde hinzugefügt oder entfernt (nur bei modularen Geräten).</li> <li>– Der Empfangsleistungs-Status eines Ports mit SFP-Modul hat sich geändert (siehe Dialog <code>Diagnose:Ports:SFP-Module</code>).</li> </ul> <p>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.</p> |
| Portsicherheit    | An einem Port wurde ein Datenpaket von einem nicht erlaubten Endgerät empfangen (siehe Dialog Portsicherheit).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |

Tab. 24: 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 218 „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 92 „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 218 „Gerätfunktionen 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
configure
device-status monitor all
error
device-status trap enable
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

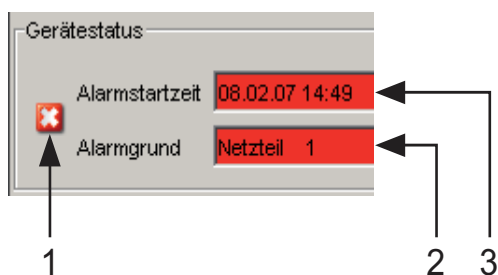
Bezieht alle möglichen Ereignisse zur Gerätestatusermittlung mit ein.

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

```
exit
show device-status
```

Wechsel in den Privileged-EXEC-Modus.  
 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 externen 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 92 „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 218](#) „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`

`configure`

`signal-contact 1 mode manual`

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

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 213 „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 `Grundeinstellungen:System` am Ende der Systemdaten die Temperaturschwellen ein.

enable Wechsel in den Privileged-EXEC-Modus.  
configure Wechsel in den Konfigurationsmodus.

|  |                                           |                                                                                             |
|--|-------------------------------------------|---------------------------------------------------------------------------------------------|
|  | <code>signal-contact 1 monitor all</code> | Bezieht alle möglichen Ereignisse zur Funktionsüberwachung mit ein.                         |
|  | <code>signal-contact 1 trap enable</code> | 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.

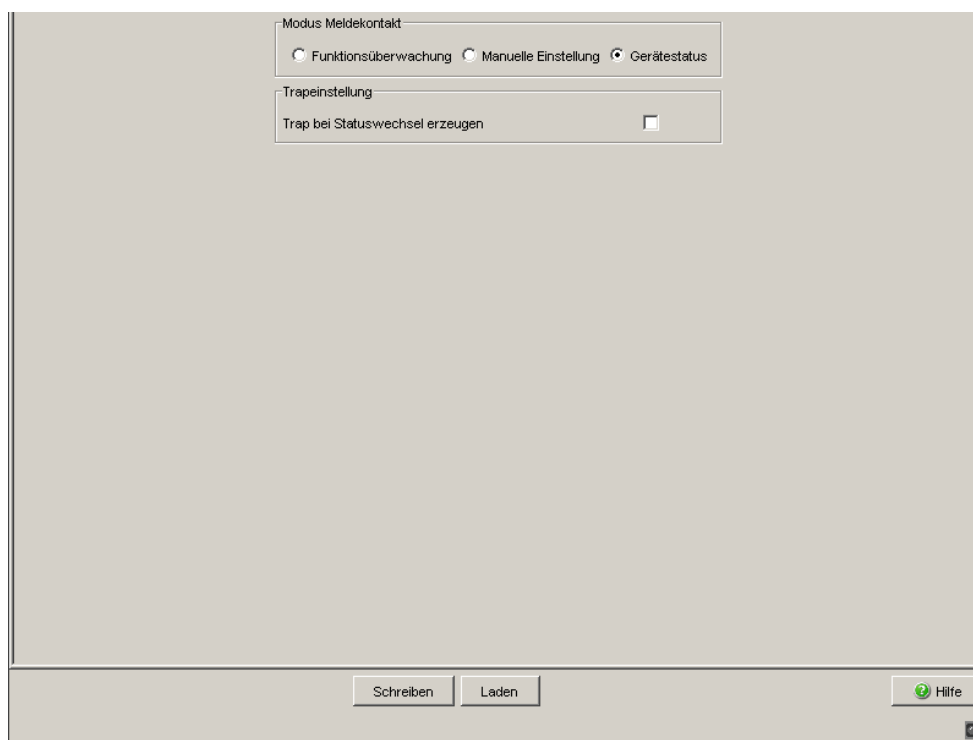


Abb. 53: Dialog Meldekontakt

|  |                                    |                                                                                         |
|--|------------------------------------|-----------------------------------------------------------------------------------------|
|  | <code>exit</code>                  | Wechsel in den Privileged-EXEC-Modus.                                                   |
|  | <code>show signal-contact 1</code> | 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 218 „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 Signalisierung 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 nicht-flüchtig in der aktiven Konfiguration zu speichern.

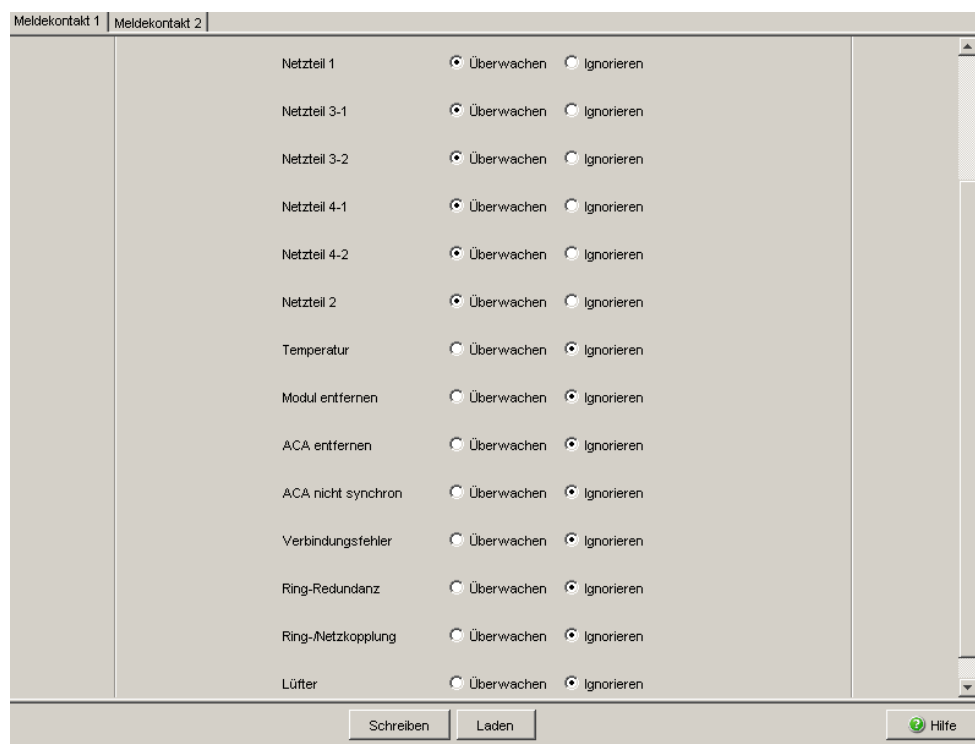


Abb. 54: Lüfter mit Meldekontakt und Trap überwachen

## 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.

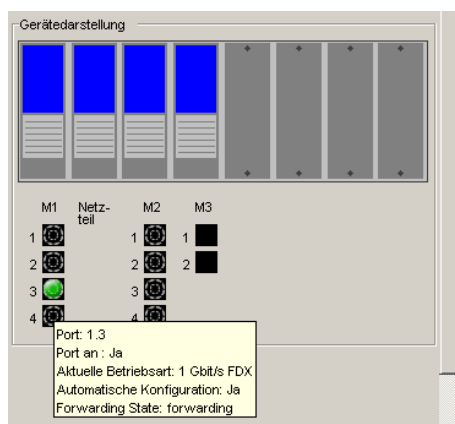









Abb. 55: Gerätedarstellung

**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-Statistiktablett 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<br>– Elektromagnetische Einkoppelung im Übertragungsmedium                                               |
| CRC-Fehler           | – Nicht funktionierender Controller des verbundenen Gerätes<br>– Elektromagnetische Einkoppelung im Übertragungsmedium<br>– Nicht betriebsbereite Komponente im Netz |
| Kollisionen          | – Nicht funktionierender Controller des verbundenen Gerätes<br>– Netzausdehnung zu groß/Zeilen zu lang<br>– Kollision oder Fehler beim Datenpaket ermittelt          |

Tab. 25: 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            | 47098                    | 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. 56: 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 ( $\geq 10$ 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. 26: 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 | Duplex-Problem, EMI erkannt |

Tab. 26: 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
```

```
configure
```

```
bridge duplex-mismatch-detect
operation enable
```

```
bridge duplex-mismatch-detect
operation disable
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Schaltet die Erkennung und Meldung der Nichtübereinstimmung der Duplex-Modi ein.

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. 27: 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.

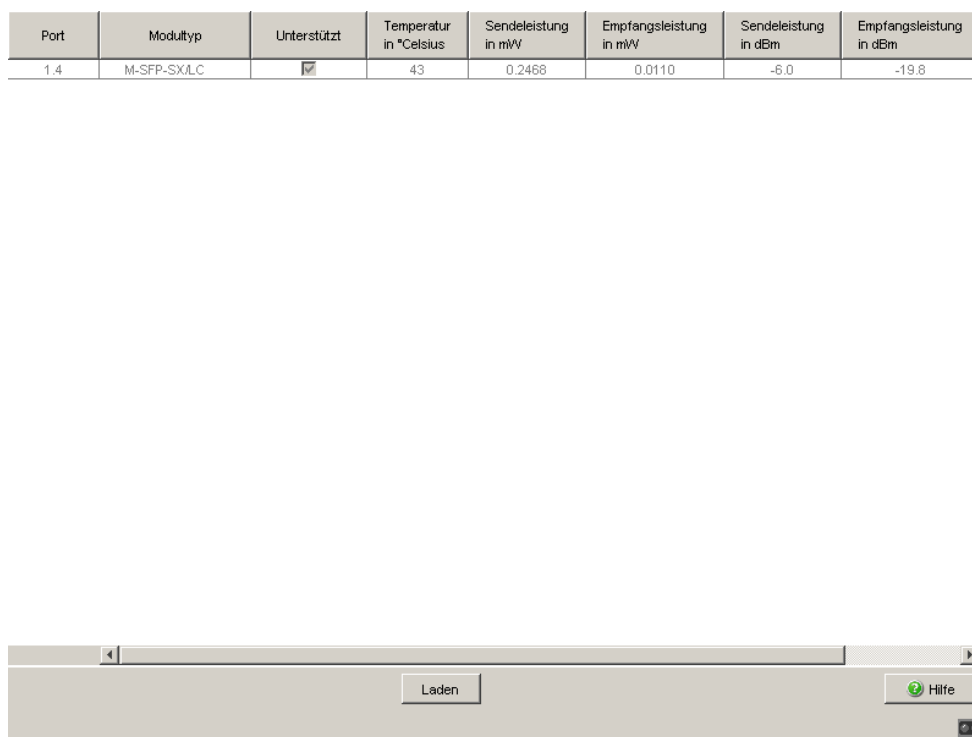


## 9.6 SFP-Zustandsanzeige

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`.



| Port | Modultyp   | Unterstützt                         | Temperatur in °Celsius | Sendeleistung in mW | Empfangsleistung in mW | Sendeleistung in dBm | Empfangsleistung in dBm |
|------|------------|-------------------------------------|------------------------|---------------------|------------------------|----------------------|-------------------------|
| 1.4  | M-SFP-SXLC | <input checked="" type="checkbox"/> | 43                     | 0.2468              | 0.0110                 | -6.0                 | -19.8                   |

Abb. 57: 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 Netzmanagementstation 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-Informationsaustausch 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. Hirschmann-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 154 „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 Gratuitous 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. 28: 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 28](#)).

## 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.

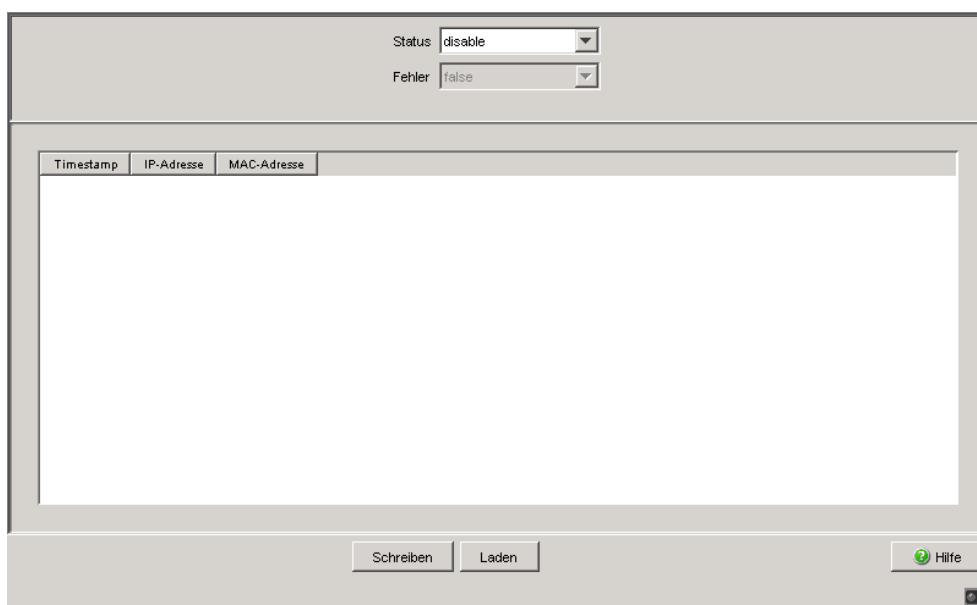


Abb. 58: Dialog IP-Adressen Konflikterkennung

## 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 eingeht, 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.

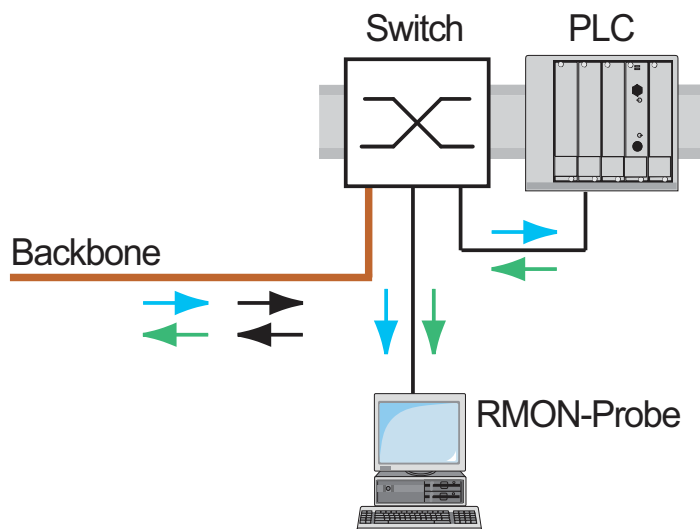


Abb. 59: Port-Mirroring

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 zurückzusetzen.

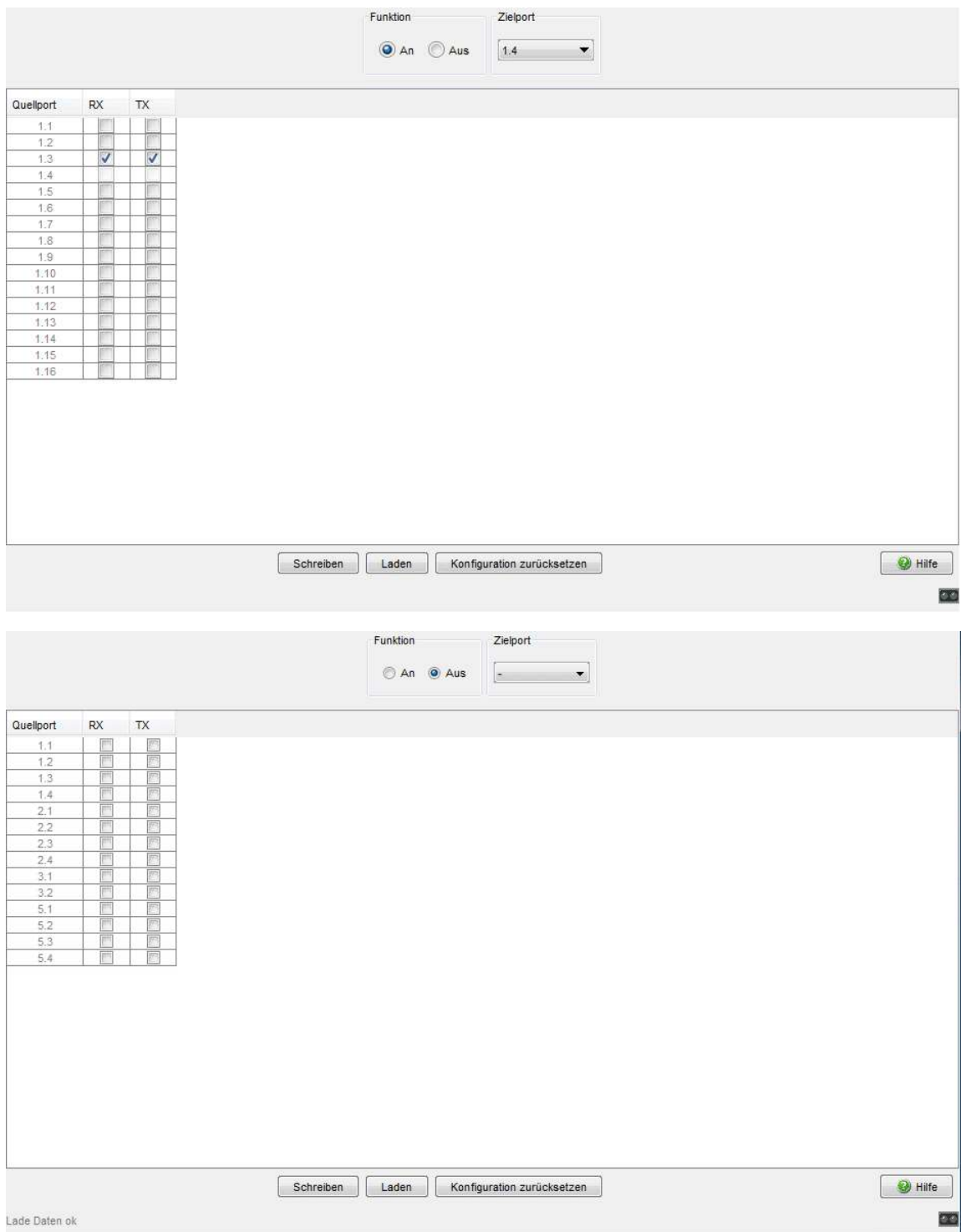


Abb. 60: Dialog Port-Mirroring

## 9.12 Syslog

Das Gerät bietet Ihnen die Möglichkeit, Meldungen über wichtige Geräteinterne 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 251 „Trap-Log“](#)) und in der Log-Datei ([siehe auf Seite 242 „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“.

|                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure logging host 10.0.1.159 514 3  logging syslog exit show logging hosts Index      IP Address      Severity  Port      Status -----  - 1         10.0.1.159     error     514      Active</pre> | <p>Wechsel in den Privileged-EXEC-Modus.<br/>Wechsel in den Konfigurationsmodus.<br/>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“.<br/>Schaltet die Syslog-Funktion ein.<br/>Wechsel in den Privileged-EXEC-Modus.<br/>Zeigt die Syslog-Host-Einstellungen.</p>                                                                                                            |
| <pre>enable configure logging snmp-requests get operation enable logging snmp-requests get severity 5  logging snmp-requests set operation enable logging snmp-requests set severity 5</pre>                        | <p>Wechsel in den Privileged-EXEC-Modus.<br/>Wechsel in den Konfigurationsmodus.<br/>Erzeugt aus lesenden SNMP-Anfragen Log-Ereignisse.<br/>Die „5“ gibt den Schweregrad der Meldung an, die das Gerät Meldungen aus lesenden SNMP-Anfragen zuordnet. „5“ bedeutet „Hinweis“.<br/>Erzeugt aus schreibenden SNMP-Anfragen Log-Ereignisse.<br/>Die „5“ gibt den Schweregrad der Meldung an, die das Gerät Meldungen aus schreibenden SNMP-Anfragen zuordnet. „5“ bedeutet „Hinweis“.</p> |



---

```
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 248 „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“.

|                                           |                                                                                 |
|-------------------------------------------|---------------------------------------------------------------------------------|
| <code>enable</code>                       | Wechsel in den Privileged-EXEC-Modus.                                           |
| <code>configure</code>                    | Wechsel in den Konfigurationsmodus.                                             |
| <code>mac notification interval 20</code> | Setzen Sie das Intervall für die MAC-Benachrichtigung auf 20 Sekunden.          |
| <code>interface 1/1</code>                | Wechsel in den Interface-Konfigurationsmodus von Port 1/1.                      |
| <code>mac notification mode</code>        | Setzen Sie den Modus, für den das Gerät eine MAC-Benachrichtigung versendet.    |
| <code>mac notification operation</code>   | Aktivieren Sie das Versenden von MAC-Benachrichtigungs-Alarmen für diesen Port. |



```
exit
mac notification operation
```

Wechsel in den Konfigurationsmodus.

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. 61: 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`.

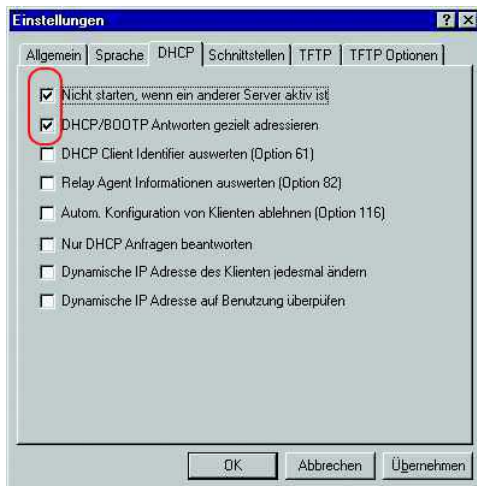


Abb. 62: DHCP-Einstellung

- 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. 63: Konfigurationsprofile hinzufügen

- Geben Sie die Netzmaske ein und klicken Sie auf Übernehmen.

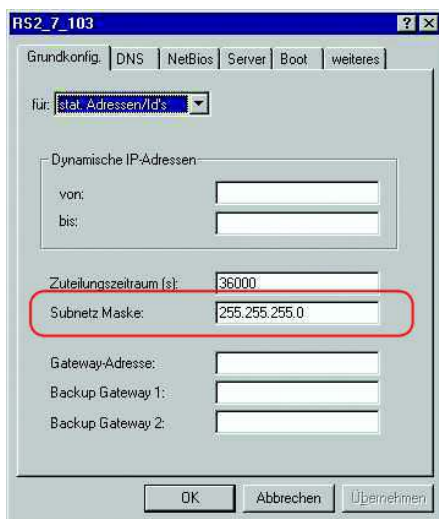


Abb. 64: Netzmaske im Konfigurationsprofil

- 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`.

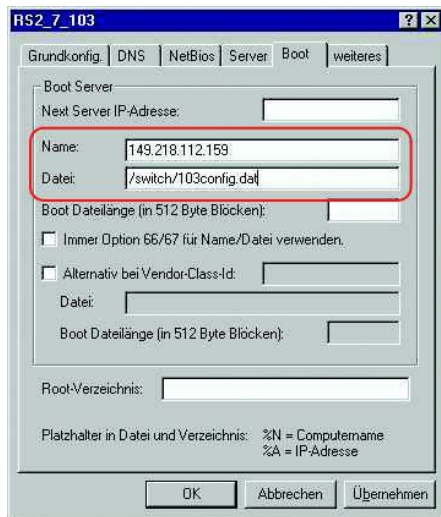


Abb. 65: Konfigurationsdatei auf dem tftp-Server

- 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.

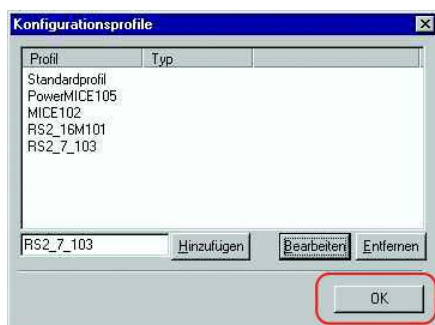


Abb. 66: Konfigurationsprofile verwalten

- Zur Eingabe der statischen Adressen klicken Sie im Hauptfenster auf Statisch.



Abb. 67: Statische Adresseingabe

- Klicken Sie auf Hinzufügen.

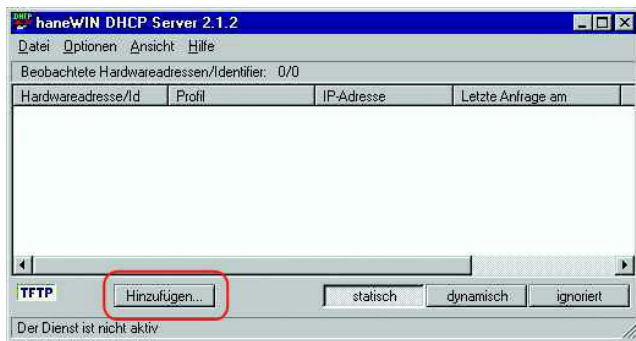


Abb. 68: Statische Adressen hinzufügen

- 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.

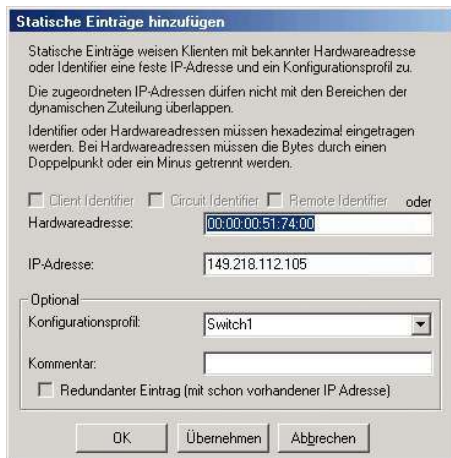


Abb. 69: Einträge für statische Adressen

- Fügen Sie für jedes Gerät, das vom DHCP-Server seine Parameter erhalten soll, einen Eintrag hinzu.

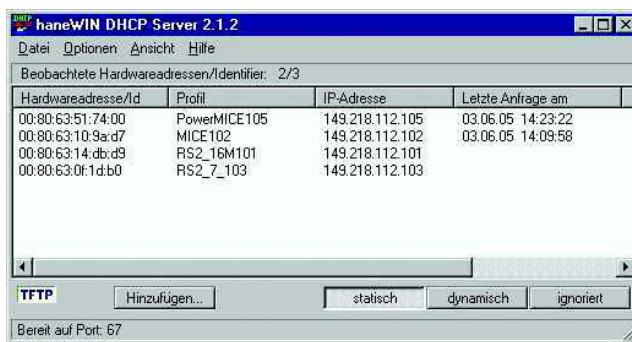


Abb. 70: DHCP-Server mit Einträgen

## 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. 71: 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.

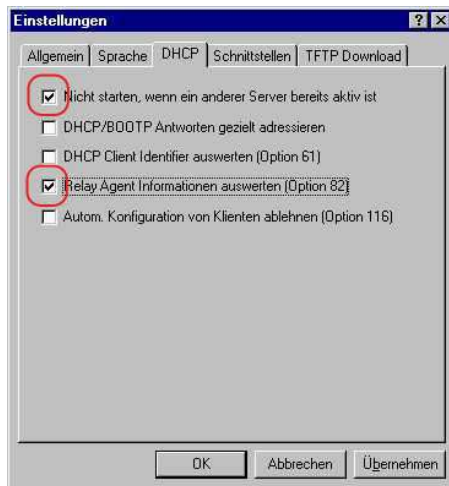


Abb. 72: DHCP-Einstellung

- Zur Eingabe der statischen Adressen klicken Sie auf **Hinzufügen**.

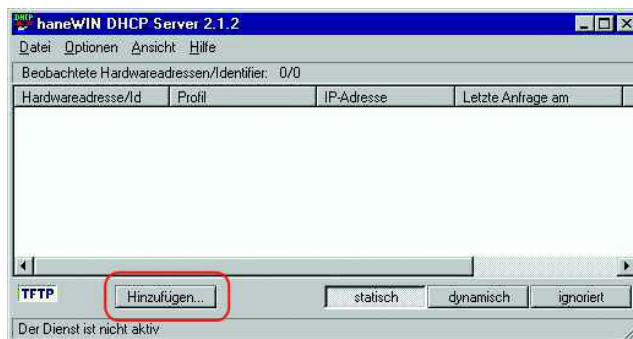


Abb. 73: Statische Adressen hinzufügen

- Wählen Sie **Circuit Identifizier** und **Remote Identifizier**.

Abb. 74: 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:

ciclhhvvvssmmpprirlxxxxxxxxxxxx

- ▶ ci: Subidentifizier für Typ des Circuit-ID
- ▶ cl: Länge des Circuit-ID
- ▶ hh: Hirschmann-Identifizier: 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: Subidentifizier 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.

**feste Adresszuweisungen**

Mit statischen Einträgen können Klienten mit bekannter Hardwareadresse oder Identifier eine feste IP-Adresse und ein Konfigurationsprofil zugeordnet werden. Die zugeordneten IP-Adressen dürfen nicht mit den Bereichen der dynamischen Zuteilung überlappen.

Identifier oder Hardwareadressen müssen hexadezimal eingetragen werden. Bei Hardwareadressen müssen die Bytes durch einen Doppelpunkt oder ein Minus getrennt werden.

Client Identifier  Circuit Identifier  Remote Identifier oder

Hardwareadresse:

IP-Adresse:

Optional

Konfigurationsprofil:

Kommentar:

OK Abbrechen Übernehmen

Abb. 75: Eintragen der Adressen

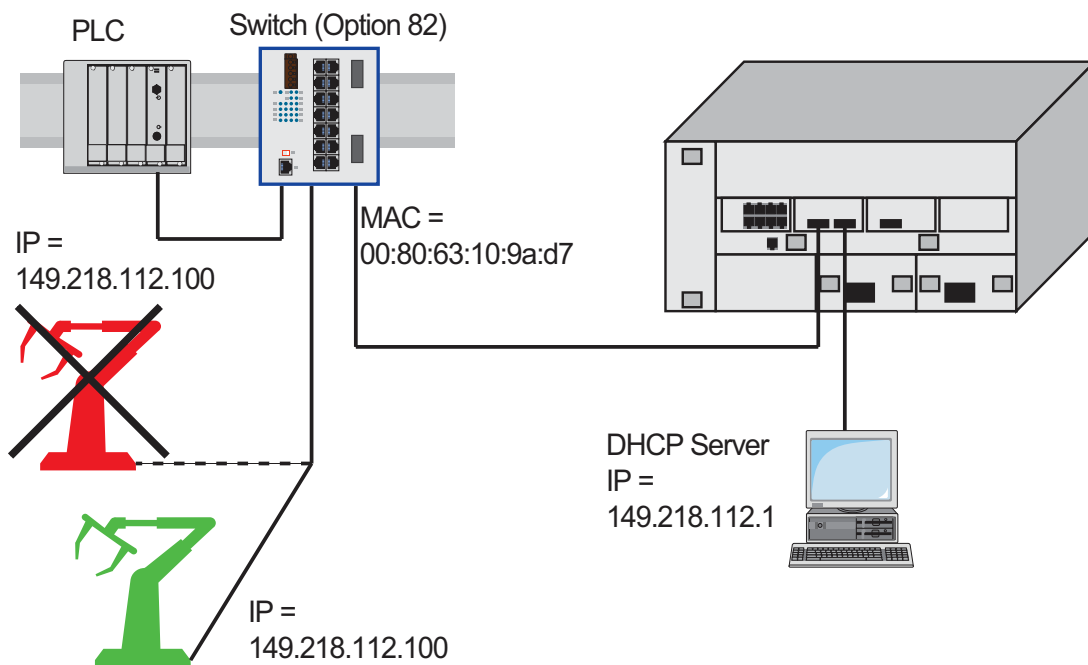


Abb. 76: Anwendungsbeispiel für den Einsatz von Option 82



## 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 ein 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 77](#)) 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.

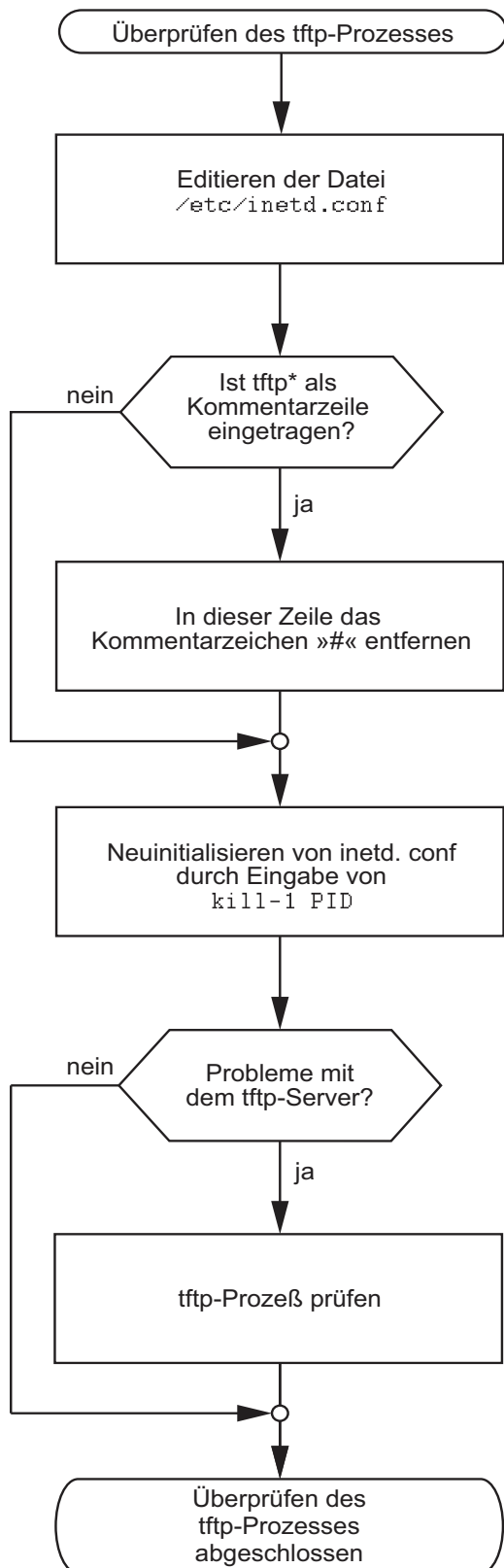
Zum Beispiel:

```
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. 77: 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. 29: 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.

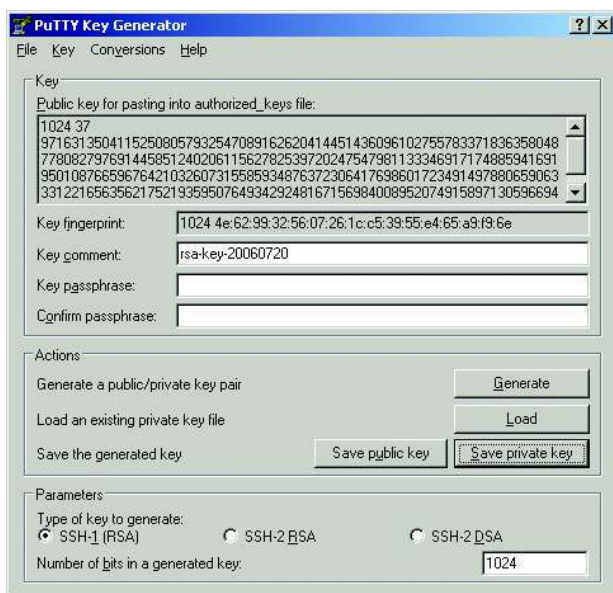


Abb. 78: PuTTY Schlüsselgenerator

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
no ip ssh
copy tftp://ip/filepath/key
 nvram:sshkey-rsa2

copy tftp://ip/filepath/key
 nvram:sshkey-dsa

copy tftp://ip/filepath/key
 nvram:sshkey-rsa1

ip ssh
```

Wechsel in den Privileged-EXEC-Modus.

SSH-Server ausschalten.

Lädt den Schlüssel in den nicht-flüchtigen Speicher des Gerätes.

▶ nvram:sshkey-rsa2 ist der Speicherort des RSA-Schlüssels für SSH-Version 2.

▶ nvram:sshkey-dsa ist der Speicherort des DSA-Schlüssels für SSH-Version 2.

▶ nvram:sshkey-rsa1 ist der Speicherort des RSA-Schlüssels für SSH-Version 1.

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. 79: 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. 80: Sicherheitsabfrage zur eingestellten Warnschwelle

- Klicken Sie auf „Ja“ dieser Sicherheitsalarmmeldung.

Um für zukünftige Verbindungsaufbauten 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 -c des
```

- ▶ `admin` stellt den Benutzernamen dar.
- ▶ `10.0.112.53` stellt die IP-Adresse Ihres Gerätes dar.
- ▶ `-c des` 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
```

```
no ip https
```

```
copy tftp://ip/filepath/cert
nvram:httpscert
```

```
ip https
```

Wechsel in den Privileged-EXEC-Modus.

Vor dem Übertragen des Zertifikats auf das Gerät die HTTPS-Funktion ausschalten.

Lädt das Zertifikat in den nicht-flüchtigen Speicher des Gerätes.

`nvram:httpscert` ist der Speicherort des X.509-Zertifikats.

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 Subidentifizier (SID) werden sie instanziiert.

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 Subidentifiziers (2) wird diese abstrakte Information auf die Wirklichkeit abgebildet, instanziiert, 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<br>(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<br>(Nummer des Netzteils)                                                     |
| TimeTicks         | Stop-Uhr,<br>verronnene Zeit = Zahlenwert/100 in Sekunden<br>Zahlenwert = ganze Zahl im Bereich von $0-2^{32}-1$ |
| Timeout           | Zeitwert in hundertstel Sekunden<br>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.                   |



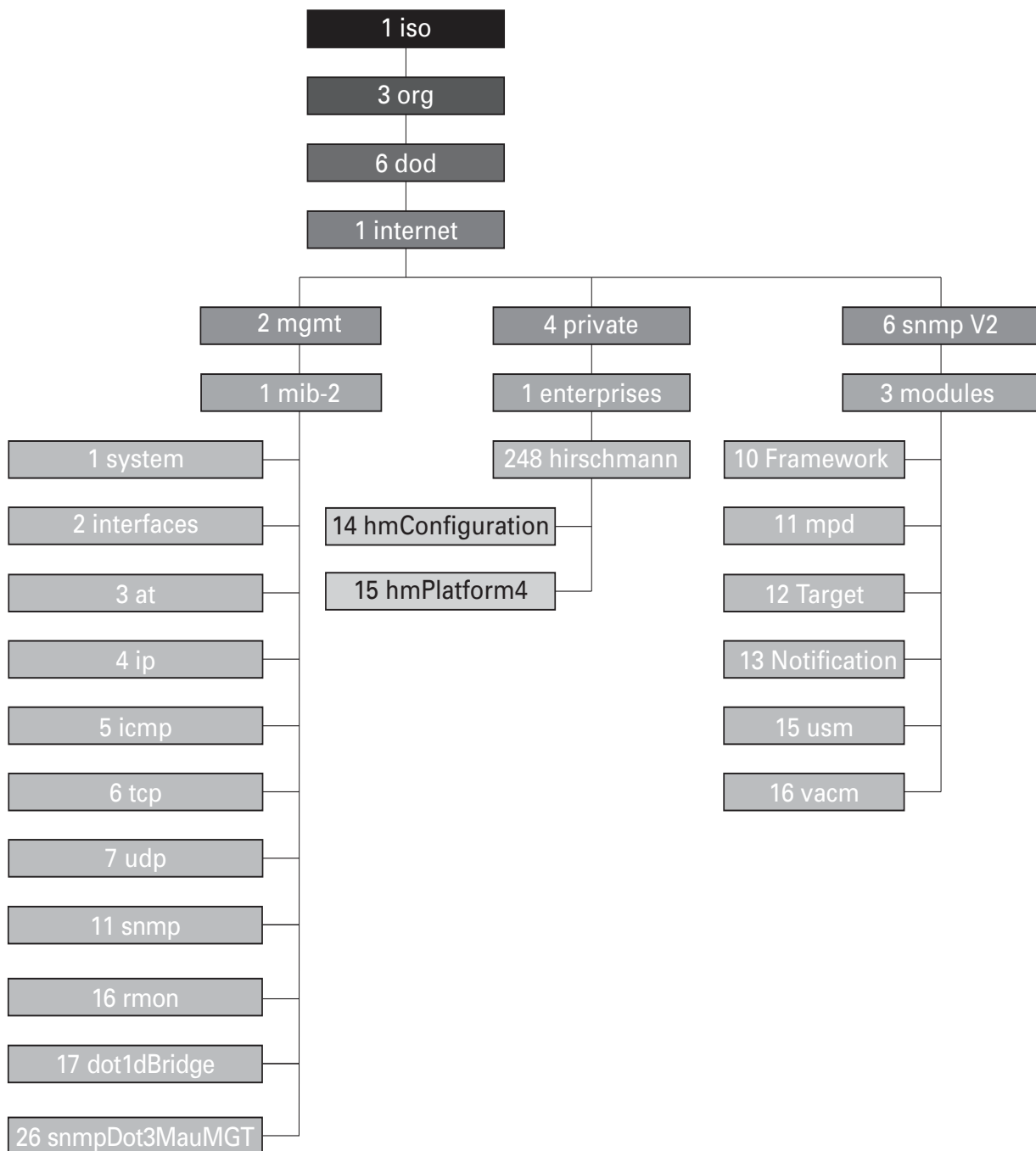


Abb. 81: Baumstruktur der Hirschmann-MIB

Die vollständige Beschreibung der MIB finden Sie auf der Produkt-CD, die zum Lieferumfang des Geräts gehört.

---

## B.2 Verwendete Abkürzungen

|       |                                         |
|-------|-----------------------------------------|
| ACA   | AutoConfiguration Adapter               |
| 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 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Lesbarkeit          | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Verständlichkeit    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Beispiele           | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Aufbau              | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Vollständigkeit     | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Grafiken            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Zeichnungen         | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Tabellen            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

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, 60, 60, 77, 79, 212 |
| ACD                          | 238                     |
| Address Conflict Detection   | 238                     |
| Adresstabelle                | 153                     |
| AF                           | 178                     |
| Aging Time                   | 153, 159, 159           |
| Alarm                        | 211                     |
| Alarmnachrichten             | 208                     |
| Anforderungsintervall (SNTP) | 132                     |
| APNIC                        | 29                      |
| ARIN                         | 29                      |
| ARP                          | 33                      |
| Assured Forwarding           | 178                     |
| Authentifizierung            | 212                     |
| AutoConfiguration Adapter    | 40, 212                 |
| Automatische Konfiguration   | 91                      |

## B

|                   |               |
|-------------------|---------------|
| Bandbreite        | 157, 188      |
| Benutzernamen     | 22            |
| Bericht           | 242           |
| BOOTP             | 27            |
| Booten            | 19            |
| Boundary Clock    | 138           |
| Broadcast         | 152, 154, 157 |
| Broadcast-Limiter | 171           |

## C

|                                |          |
|--------------------------------|----------|
| CDROM                          | 256, 262 |
| CIDR                           | 33       |
| CLI-Banner                     | 125      |
| Classless Inter Domain Routing | 33       |
| Class Selector                 | 178      |
| Command Line Interface         | 21       |

## D

|                                    |                    |
|------------------------------------|--------------------|
| Destination Address                | 154                |
| DHCP                               | 27, 47, 54         |
| DHCP Option 82                     | 54                 |
| DHCP-Client                        | 47                 |
| DHCP-Server                        | 128, 256, 262      |
| Differentiated Services            | 178                |
| Differenzierter Management-Zugriff | 112                |
| DiffServ                           | 173                |
| DiffServ-Codepoint                 | 178                |
| DSCP                               | 178, 181, 185, 185 |
| Dynamisch                          | 154                |

## E

|                                              |          |
|----------------------------------------------|----------|
| E2E                                          | 138      |
| Echtzeit                                     | 127, 173 |
| EF                                           | 178      |
| Empfangsleistungs-Status (Quelle für Alarme) | 212      |
| Empfangsport                                 | 155      |
| End-to-End                                   | 138      |
| Ereignis-Log                                 | 251      |
| Erstinstallation                             | 27       |
| Expedited Forwarding                         | 178      |

## F

|                           |          |
|---------------------------|----------|
| FAQ                       | 291      |
| Faulty Device Replacement | 58       |
| FDB                       | 154      |
| Ferndiagnose              | 216      |
| Filter                    | 154      |
| Filtertabelle             | 154, 166 |
| Flash-Speicher            | 65, 79   |
| Flow control              | 188      |
| Forwarding Database       | 154      |
| Funktionsüberwachung      | 216      |

## G

|                                      |          |
|--------------------------------------|----------|
| Gateway                              | 30, 37   |
| Generische Objektklassen             | 280      |
| Gerätestatus                         | 213      |
| GMRP                                 | 157, 165 |
| GMRP pro Port                        | 168      |
| Grafische Benutzeroberfläche         | 24       |
| Grafische Benutzeroberfläche starten | 25       |
| Grandmaster                          | 136      |

## H

|                                |          |
|--------------------------------|----------|
| HaneWin                        | 256, 262 |
| Hardware-Adresse               | 43       |
| Hardware-Reset                 | 208      |
| Hardware-Uhr (gepuffert)       | 128      |
| HIPER-Ring (Quelle für Alarme) | 212      |
| HiDiscovery                    | 38, 115  |
| HiView                         | 25       |
| Host-Adresse                   | 30       |

## I

|                |     |
|----------------|-----|
| IANA           | 29  |
| IEEE 1588-Zeit | 129 |
| IEEE 802.1 Q   | 174 |

|                                                     |                     |                         |                    |
|-----------------------------------------------------|---------------------|-------------------------|--------------------|
| IGMP                                                | 159                 | Netzmaske               | 30, 37             |
| IGMP Querier                                        | 161                 | Netztopologie           | 54                 |
| IGMP-Snooping                                       | 157, 159            | Neustart                | 80                 |
| Industrial HiVision                                 | 12, 48              |                         |                    |
| Industrieprotokolle                                 | 11                  | <b>O</b>                |                    |
| Instanziierung                                      | 280                 | Object Description      | 280                |
| Internet Assigned Numbers Authority                 | 29                  | Object-ID               | 280                |
| Internet-Service-Provider                           | 29                  | Objektklassen           | 280                |
| In-band                                             | 21                  | Offline-Konfiguration   | 67                 |
| IP-Adresse                                          | 29, 36, 43, 47, 238 | Option 82               | 28, 54, 262        |
| IP-Header                                           | 173, 177, 178       | Ordinary Clock          | 138                |
| IP-Parameter                                        | 27                  | Out-of-band             | 21                 |
| ISO/OSI-Schichtenmodell                             | 33                  |                         |                    |
|                                                     |                     | <b>P</b>                |                    |
| <b>J</b>                                            |                     | P2P                     | 138                |
| Java Runtime Environment                            | 68                  | Passwort                | 22, 71, 102, 104   |
| JRE                                                 | 68                  | Peer-to-Peer            | 138                |
|                                                     |                     | PHB                     | 178                |
| <b>K</b>                                            |                     | Phy                     | 137                |
| Kaltstart                                           | 80                  | Polling                 | 208                |
| Konfiguration                                       | 65                  | Portauthentifizierung   | 120                |
| Konfigurationsänderungen                            | 208                 | Portkonfiguration       | 91                 |
| Konfigurationsdatei                                 | 47, 65, 66          | Port-Mirroring          | 244                |
| Konfigurationsdaten                                 | 42, 54, 62, 69      | Port-Priorität          | 181, 184           |
|                                                     |                     | Power over ETHERNET     | 92                 |
| <b>L</b>                                            |                     | PROFINET IO             | 11                 |
| LACNIC                                              | 29                  | Precedence              | 178                |
| Lastbegrenzer Einstellungen                         | 170, 171            | Precision Time Protocol | 135                |
| Leave                                               | 159                 | Priorität               | 174, 181           |
| Lieferzustand                                       | 64, 65, 101         | Prioritätsklasse        | 184                |
| Login-Banner                                        | 124                 | Priority Queues         | 173                |
| Login-Fenster                                       | 26                  | Priority Tagged Frames  | 174                |
| Lokale Uhr                                          | 136                 | Protokollstapel         | 137                |
| Lüfter                                              | 220                 | PTP                     | 127, 129, 135      |
|                                                     |                     | PTP-Subdomäne           | 139                |
| <b>M</b>                                            |                     | <b>Q</b>                |                    |
| MAC                                                 | 137                 | QoS                     | 174                |
| MAC-Adresse                                         | 236                 | Quelladresse            | 152                |
| MAC-Zieladresse                                     | 33                  | Query                   | 159                |
| Medienmodul für modulare Geräte (Quelle für Alarme) | 212                 | Query-Funktion          | 161                |
| Meldekontakt                                        | 92, 216             |                         |                    |
| Meldekontakt (Quelle für Alarm)                     | 212                 | <b>R</b>                |                    |
| Modus                                               | 91                  | Reboot                  | 80                 |
| Multicast                                           | 132, 154, 157, 159  | Redundanz               | 11                 |
| Multicast-Adresse                                   | 166                 | Redundanz Manager       | 154                |
|                                                     |                     | Referenzuhr             | 128, 131, 136, 142 |
| <b>N</b>                                            |                     | Relaiskontakt           | 216                |
| Nachricht                                           | 208                 | Release                 | 75                 |
| Netzadresse                                         | 29                  | Report                  | 159                |
| Netzmanagement                                      | 48                  | Reset                   | 80                 |
| Netzmanagementstation                               | 237                 | RIPE NCC                | 29                 |

|                                        |               |                                   |                    |
|----------------------------------------|---------------|-----------------------------------|--------------------|
| Ring-/Netzkopplung (Quelle für Alarme) | 212           | <b>U</b>                          |                    |
| RMON-Probe                             | 244           | Uhr                               | 135                |
| Router                                 | 30            | Uhrenabgleich                     | 137                |
| Ruhestromschaltung                     | 216           | Unicast                           | 157                |
|                                        |               | Untrusted                         | 181                |
| <b>S</b>                               |               | Update                            | 18                 |
| Schulungsangebote                      | 291           | USB-Stick                         | 77                 |
| Segmentierung                          | 208           | UTC                               | 129                |
| Service                                | 242           | Überlastschutz                    | 188                |
| Service-Provider                       | 29            | Übertragungsparameter             | 18                 |
| Service-Shell-Funktion reaktivieren    | 277           | Übertragungssicherheit            | 208                |
| SFP-Modul                              | 234           | <b>V</b>                          |                    |
| SFP-Modul (Quelle für Alarme)          | 212           | Verbindungsfehler                 | 92                 |
| SFP-Zustandsanzeige                    | 234           | Verbindungsüberwachung            | 213, 216           |
| Signallaufzeit                         | 131           | Versorgungsspannung               | 212                |
| Skriptdatei vom ACA laden              | 65            | Video                             | 182                |
| SNMP                                   | 24, 101, 208  | VLAN                              | 174, 181, 191      |
| SNTP                                   | 127, 132      | VLAN-ID (Netzparameter)           | 55                 |
| SNTP-Client                            | 132           | VLAN-Priorität                    | 183                |
| SNTP-Server                            | 148           | VLAN-Tag                          | 174, 191           |
| Software                               | 270           | VoIP                              | 182                |
| Software-Release                       | 75            | V.24                              | 21                 |
| Sommerzeit                             | 128           | <b>W</b>                          |                    |
| SSH                                    | 21            | Warteschlange                     | 182                |
| Statisch                               | 154           | Winterzeit                        | 128                |
| Strict-Priority                        | 182           | <b>X</b>                          |                    |
| Subdomäne                              | 139           | XML (Offline Configurator Format) | 67                 |
| Subidentifizier                        | 280           | <b>Z</b>                          |                    |
| Subnetz                                | 37, 153       | Zeitmanagement                    | 135                |
| Symbol                                 | 13            | Zeitstempereinheit                | 137, 141           |
| Systemname                             | 47            | Zeitverschiebung                  | 129                |
| Systemvoraussetzungen (GUI)            | 25            | Zeitzone                          | 128                |
| Systemzeit                             | 131, 132      | Zieladresse                       | 153, 154, 155, 166 |
| System-Monitor                         | 18            | Zieltabelle                       | 208                |
| <b>T</b>                               |               | Zugangsschutz                     | 91                 |
| TAI                                    | 129           | Zugriff                           | 212                |
| TCP/IP-Stack                           | 267           | Zugriffsrecht                     | 71, 101            |
| Technische Fragen                      | 291           |                                   |                    |
| Telnet                                 | 21            |                                   |                    |
| TFTP                                   | 266           |                                   |                    |
| TFTP-Update                            | 83            |                                   |                    |
| Time Stamp Unit                        | 137           |                                   |                    |
| Topologie                              | 54            |                                   |                    |
| ToS                                    | 173, 177, 178 |                                   |                    |
| TP-Kabeldiagnose                       | 227           |                                   |                    |
| Traffic Classes                        | 173, 182      |                                   |                    |
| Transparent Clock                      | 138           |                                   |                    |
| Trap                                   | 208, 211      |                                   |                    |
| Trap-Zieltabelle                       | 208           |                                   |                    |
| Trivial File Transfer Protocol         | 266           |                                   |                    |
| Trust dot1p                            | 181           |                                   |                    |
| Trust ip-dscp                          | 181           |                                   |                    |
| Type of Service                        | 177           |                                   |                    |
| Typfeld                                | 174           |                                   |                    |





## 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](mailto:hac.support@belden.com)

in der Region Amerika unter

- ▶ Tel.: +1 (717) 217-2270
- ▶ E-Mail: [inet-support.us@belden.com](mailto:inet-support.us@belden.com)

in der Region Asien-Pazifik unter

- ▶ Tel.: +65 6854 9860
- ▶ E-Mail: [inet-ap@belden.com](mailto: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](http://www.hirschmann.com)).

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

# Inhalt

|          |                                              |           |
|----------|----------------------------------------------|-----------|
|          | <b>Sicherheitshinweise</b>                   | <b>5</b>  |
|          | <b>Über dieses Handbuch</b>                  | <b>7</b>  |
|          | <b>Legende</b>                               | <b>9</b>  |
| <b>1</b> | <b>Industrie-Protokolle</b>                  | <b>11</b> |
| <b>2</b> | <b>EtherNet/IP</b>                           | <b>15</b> |
| 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        |
| <b>3</b> | <b>PROFINET IO</b>                           | <b>33</b> |
| 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    | Alarmer                                      | 56        |
| 3.2.2    | Record-Parameter                             | 56        |
| 3.2.3    | I/O-Daten                                    | 60        |
| <b>4</b> | <b>IEC 61850/MMS (RSR20/RSR30/MACH1000)</b>  | <b>63</b> |
| 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        |



|          |                              |           |
|----------|------------------------------|-----------|
| <b>A</b> | <b>GSD-Datei-Generator</b>   | <b>69</b> |
| <b>B</b> | <b>Leserkritik</b>           | <b>70</b> |
| <b>C</b> | <b>Stichwortverzeichnis</b>  | <b>73</b> |
| <b>D</b> | <b>Weitere Unterstützung</b> | <b>75</b> |

# 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                                                                                      |
| <input type="checkbox"/>                                                          | Arbeitsschritt                                                                                  |
|  | Zwischenüberschrift                                                                             |
| <a href="#">Link</a>                                                              | Querverweis mit Verknüpfung                                                                     |
| <b>Anmerkung</b>                                                                  | Ein Hinweis betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit. |
| <code>Courier</code>                                                              | ASCII-Darstellung in Bedienoberfläche                                                           |

Verwendete Symbole:

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

# Legende

---



Hub



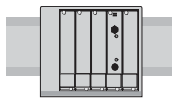
Beliebiger Computer



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. Verschmutzte, 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.



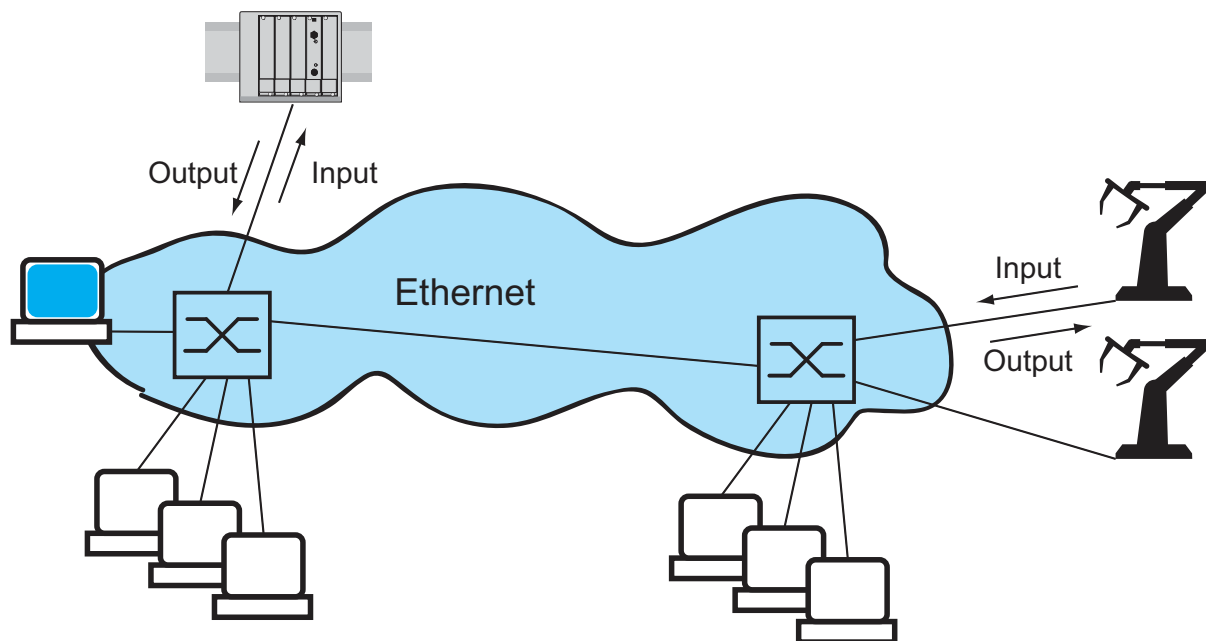


Abb. 1: Beispiel für die Kommunikation.

Hirschmann Switches 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<br>+ 3 Byte MAC | Product name<br>+ 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-<br>Protokolle:PROFINET          | PROFINET IO einschalten.                                     |
| Boot-Modus               | Grundeinstel-<br>lungen:Netz/Modus                   | „Lokal“ wählen.                                              |
| IP-Adresse               | Grundeinstel-<br>lungen:Netz/Lokal                   | Die „IP-Adresse“ 0.0.0.0 eingeben                            |
| Netzmaske                | Grundeinstel-<br>lungen:Netz/Lokal                   | Die „Netzmaske“ 0.0.0.0 eingeben.                            |
| Gateway-Adresse          | Grundeinstel-<br>lungen:Netz/Lokal                   | Die „Gateway-Adresse“ 0.0.0.0 eingeben.                      |
| VLAN 0-Transparent-Modus | Switching:VLAN:Global                                | Den „VLAN 0-Transparent-Modus“ einschalten.                  |
| HiDiscovery              | Grundeinstel-<br>lungen:Netz/HiDiscovery<br>Protocol | Die Funktion einschalten und den Zugriff „Read-only“ wählen. |
| Systemname               | Grundeinstellungen:<br>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.

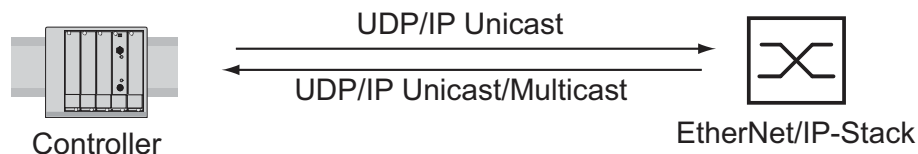


Abb. 2: Kommunikation zwischen Controller (SPS) und Switch

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.

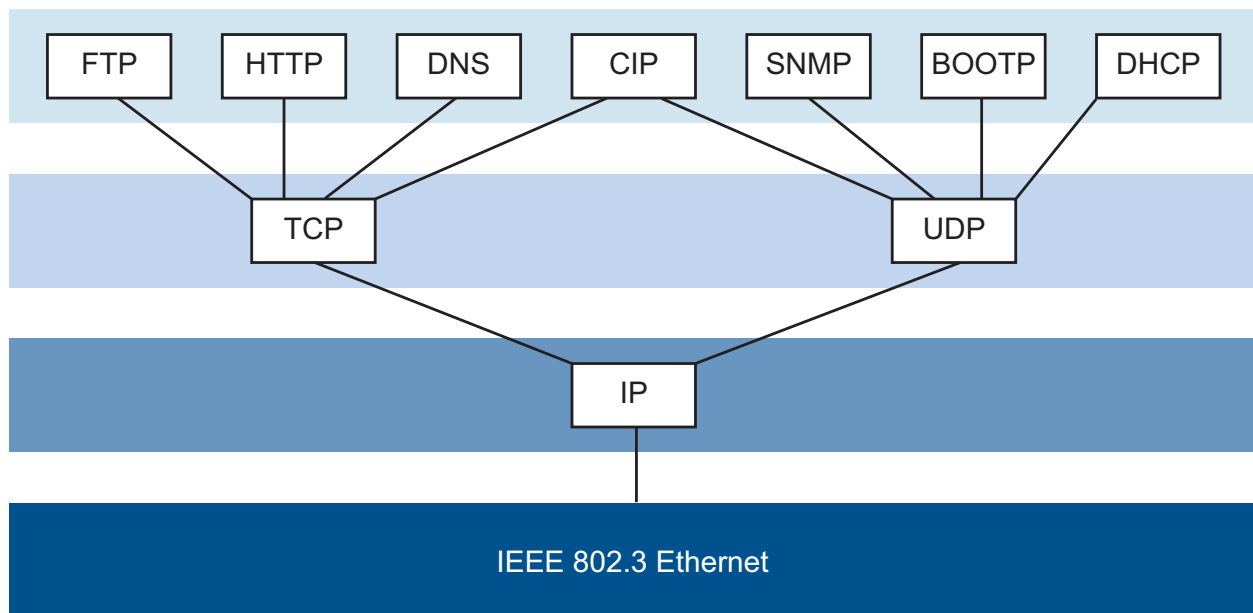


Abb. 3: EtherNet/IP (CIP) im ISO/OSI-Referenzmodell

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](http://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<br>(MACH 4000: 11)  | 7<br>(MACH 4000: 11)  | 7<br>(MACH 4000: 11)            |
| Output Assembly Instance        | 1                     | 254                   | 255                             |
| Output Size                     | 1<br>(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

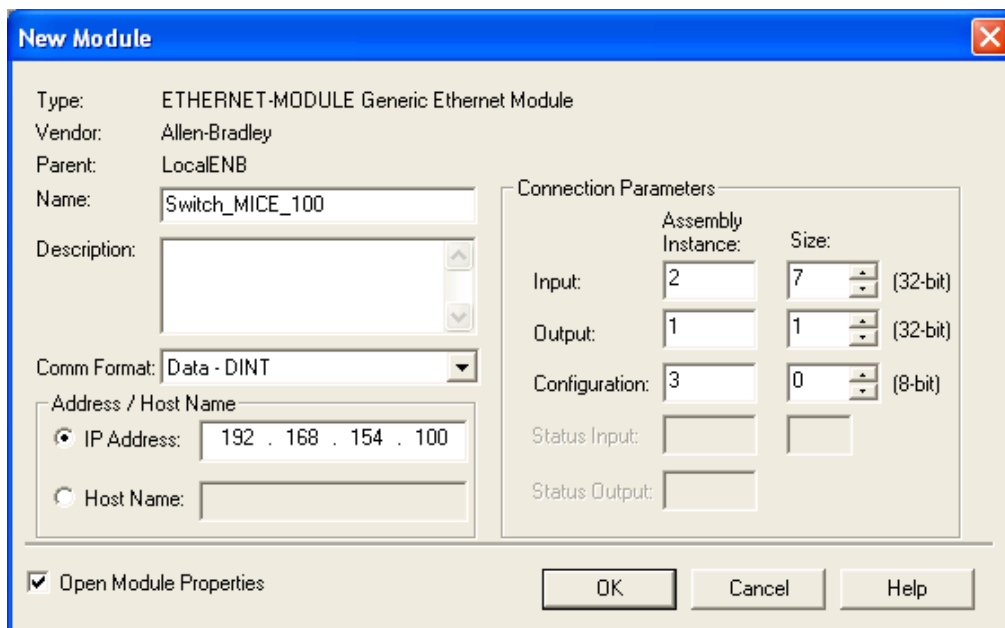


Abb. 4: Neues Modul in Logix 5000 einbinden

- Geben Sie in den Moduleigenschaften für das Request Packet Intervall (RPI) einen Wert von mindestens 100 ms ein.

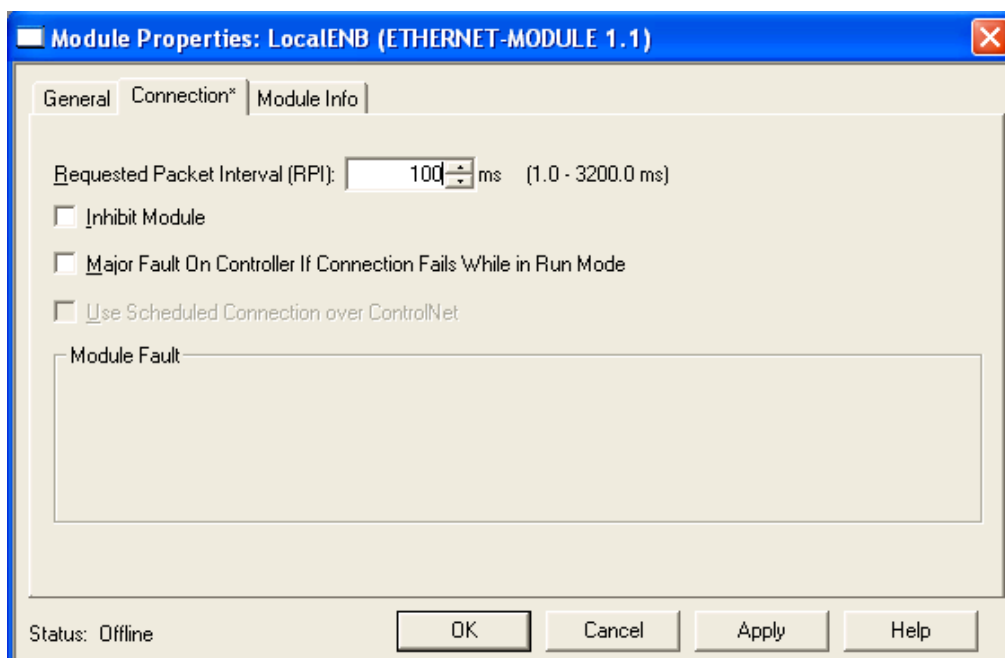


Abb. 5: Moduleigenschaften für das Request Packet Intervall (RPI)



**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 hersteller-spezifische ID 149 (95<sub>H</sub>) 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<br>USINT Major<br>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<br>(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<sub>H</sub>, 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,<br>Bit 1: DNS Client,<br>Bit 2: DHCP Client,<br>Bit 3: DHCP-DNS Update,<br>Bit 4: Configuration settable (within CIP).<br>Other bits reserved (0).                                         |
| 3  | Config Control             | Set/Get     | DWORD                                      | Bits 0 through 3:<br>Value 0: using stored config,<br>Value 1: using BOOTP,<br>Value 2: using DHCP.<br>Bit 4: 1 device uses DNS for name lookup<br>(always 0 because not supported)<br>Other bits reserved (0). |
| 4  | Physical Link Object       | Get         | Structure: UINT<br>Path size<br>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

| <b>Id</b> | <b>Attribute</b>        | <b>Access rule</b> | <b>Data type</b>                                                                                                                             | <b>Description</b>                                                                                             |
|-----------|-------------------------|--------------------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| 5         | Interface Configuration | Set/Get            | Structure:<br>UDINT IP address<br>UDINT Netmask<br>UDINT Gateway address<br>UDINT Name server 1<br>UDINT Name server 2<br>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<sub>H</sub>, 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:<br>Bit 0: Link State (1: Link up),<br>Bit 1: 0: Half-Duplex, 1: FullDuplex1,<br>Bits 2 through 4: Autoneg Status (0: Autoneg in Progress, 1: Autoneg unsuccessful, 2: unsuccessful but Speed detected, 3: Autoneg success, 4: No Autoneg),<br>Bit 5: manual configuration requires reset (always 0 because not needed),<br>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<br>Jewels UDINT              | InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors.                                                                                                                                                                                                                            |
| 5  | Media Counters     | Get         | Struct Ethernet MIB Counters<br>Jewels 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<br>Forced Iface Speed UINT | Control Bits:<br>Bit 0: Autoneg enable/disable (1: enable),<br>Bit 1: Duplex mode (1: full duplex, if Autoneg is disabled).<br>Interface speed in MBits/s: 10, 100,..., if Autoneg is disabled.                                                                                                                                                                                    |
| 7  | Interface Type     | Get         | USINT                                               | Value 0: Unknown interface type,<br>Value 1: The interface is internal,<br>Value 2: Twisted-pair,<br>Value 3: Optical fiber.                                                                                                                                                                                                                                                       |

Tab. 5: Ethernet Link-Objekt

| <b>Id</b> | <b>Attribute</b> | <b>Access rule</b> | <b>Data type</b> | <b>Description</b>                                                                                                                                   |
|-----------|------------------|--------------------|------------------|------------------------------------------------------------------------------------------------------------------------------------------------------|
| 8         | Interface State  | Get                | USINT            | Value 0: Unknown interface state,<br>Value 1: The interface is enabled,<br>Value 2: The interface is disabled,<br>Value 3: The interface is testing, |
| 9         | Admin State      | Set                | USINT            | Value 1: Enable the interface,<br>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.

| <b>Id</b>     | <b>Attribute</b>                            | <b>Access rule</b> | <b>Data type</b> | <b>Description</b>                                                                                                                                                                  |
|---------------|---------------------------------------------|--------------------|------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 100<br>(64 H) | Ethernet Interface Index                    | Get                | UDINT            | Interface/Port Index (ifIndex from MIB II)                                                                                                                                          |
| 101<br>(65 H) | Port Control                                | Get/Set            | DWORD            | Bit 0 (RO): Link state (0: link down, 1: link up)<br>Bit 1 (R/W): Link admin state (0: disabled, 1: enabled)<br>Bit 8 (RO): Access violation alarm<br>Bit 9 (RO): Utilization alarm |
| 102<br>(66 H) | Interface Utilization                       | Get                | UDINT            | The existing Counter from the private MIB hmlfaceUtilization is used. Utilization in percentage <sup>a</sup> . RX Interface Utilization.                                            |
| 103<br>(67 H) | Interface Utilization Alarm Upper Threshold | Get/Set            | UDINT            | Within this parameter the variable hmlfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage <sup>a</sup> . RX Interface Utilization Upper Limit.            |
| 104<br>(68 H) | Interface Utilization Alarm Lower Threshold | Get/Set            | UDINT            | Within this parameter the variable hmlfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage <sup>a</sup> . RX Interface Utilization Lower Limit.            |

Tab. 6: *Hirschmann-Erweiterungen des Ethernet Link-Objekts*

| Id               | Attribute                            | Access rule | Data type                                            | Description                                                                                                                                  |
|------------------|--------------------------------------|-------------|------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| 105<br>(69<br>H) | Broadcast Limit                      | Get/Set     | UDINT                                                | Broadcast limiter Service (Egress BC-Frames limitation, 0: disabled), Frames/second                                                          |
| 106<br>(6A<br>H) | Ethernet<br>Interface<br>Description | Get         | STRING<br>[max. 64 Bytes]<br>even number of<br>Bytes | Interface/Port Description<br>(from MIB II ifDescr), e.g. "Unit: 1 Slot: 2 Port:<br>1 - 10/100 Mbit TX", or "unavailable",<br>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<sub>H</sub>, 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 <sup>a</sup> 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 <sup>a</sup> 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<sub>H</sub> 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<br>0: No link, 1: Link up                                                                                                       | Input, DWORD <sup>a</sup>  |
| Output Links Admin State applied | Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, e.g. for controller access port.<br>0: Port enabled, 1: Port disabled. | Input DWORD <sup>a</sup>   |
| Utilization Alarm                | Bitmask, 1 Bit per port<br>0: No alarm, 1: Alarm on port                                                                                                | Input, DWORD <sup>a</sup>  |
| Access Violation Alarm           | Bitmask, 1 Bit per port<br>0: No alarm, 1: Alarm on port                                                                                                | Input, DWORD <sup>a</sup>  |
| 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<br>0: Port enabled, 1: Port disabled                                                                                          | Output, DWORD <sup>a</sup> |

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<br>RSR20/RSR30,<br>OCTOPUS,<br>MACH 1000 | MS20/MS30,<br>PowerMICE,<br>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)<br>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.

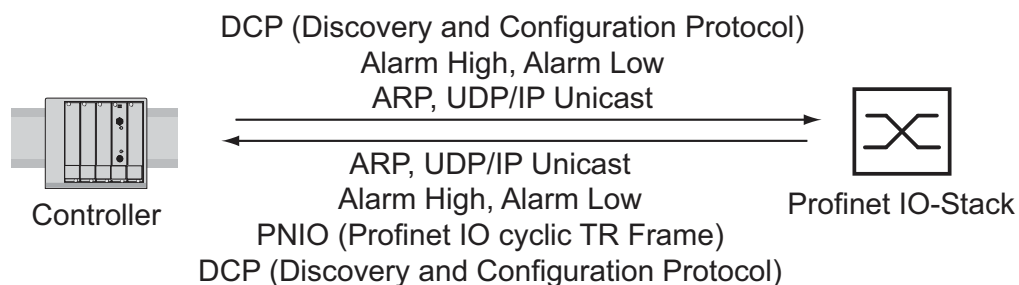


Abb. 6: Kommunikation zwischen Controller und Switch

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.

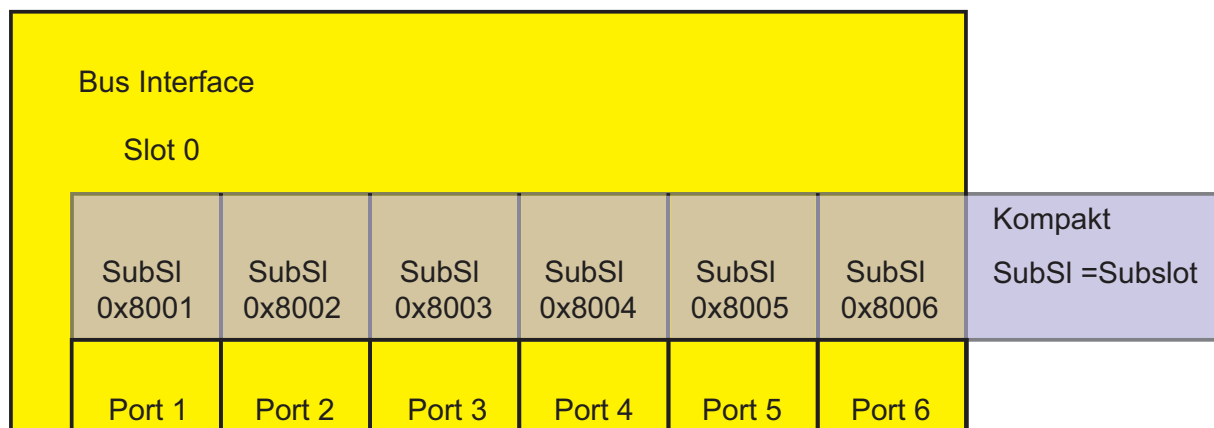


Abb. 7: Kompakter Switch

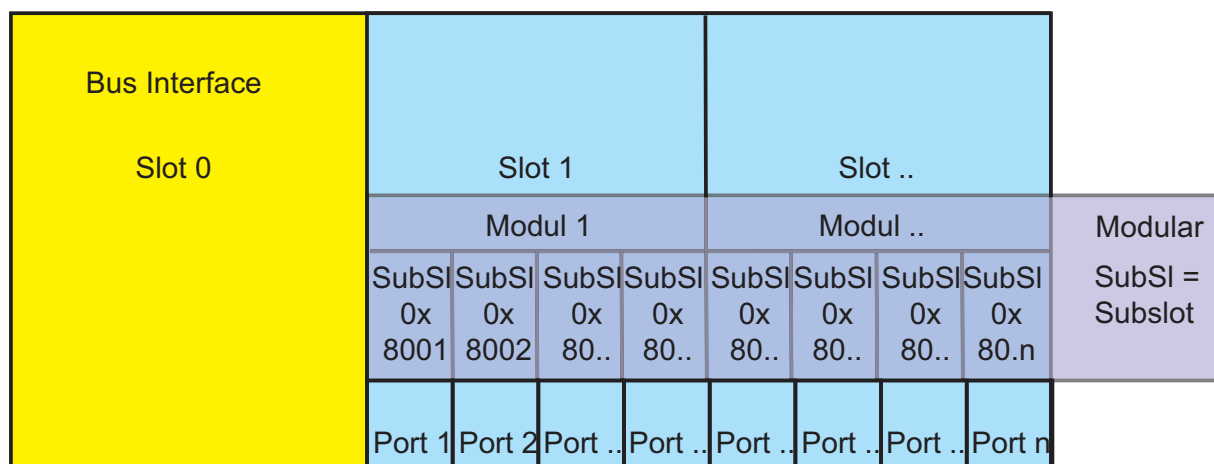


Abb. 8: Modularer Switch

## ■ 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  
Alarmer, 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 Phoenix.

**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-programmtechnische 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.

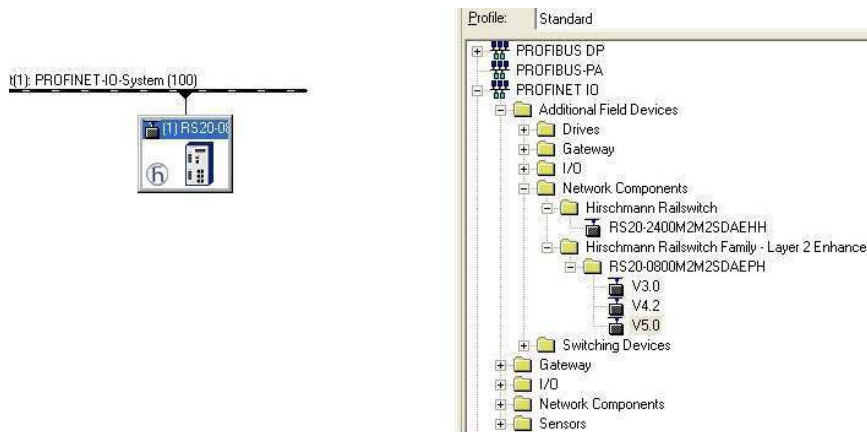


Abb. 9: Einfügen eines Switch aus der Simatic S7-Bibliothek

- 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`.

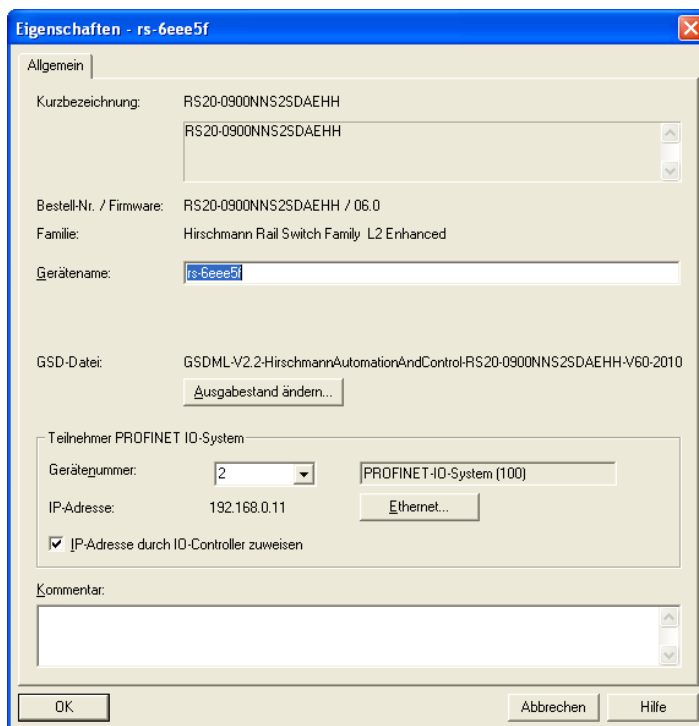


Abb. 11: Dialog zur Eingabe des Objektnamens (= Name des Switch) und der IP-Parameter

- 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**.

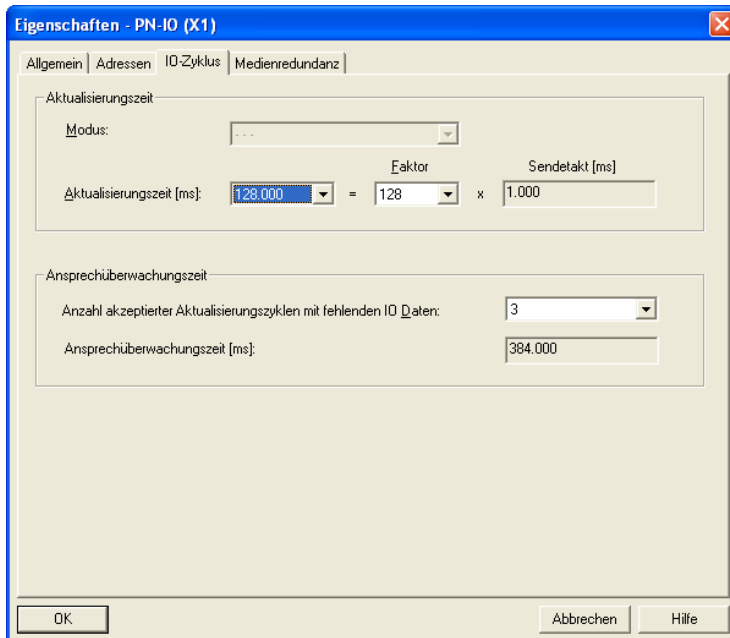


Abb. 12: Dialog zur Eingabe des IO-Zyklus

- 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 Anspruchüberwachungszeit/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**.

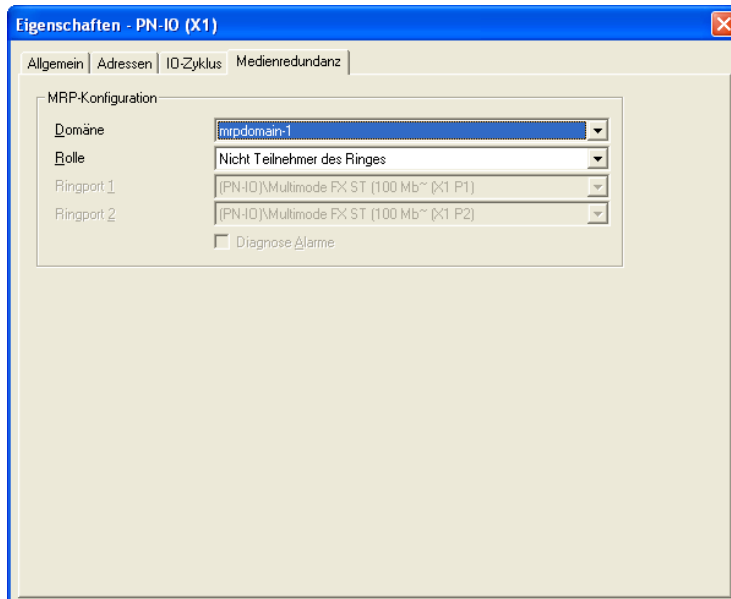


Abb. 13: Dialog zur Eingabe der Medienredundanz

- 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".

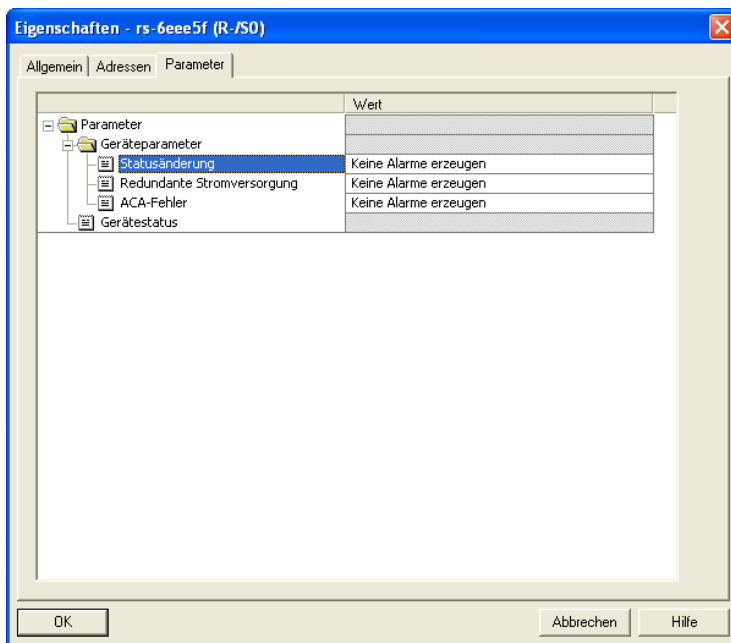


Abb. 14: Geräte-Alarme für z.B. RS20/RS30 konfigurieren.

## ■ 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.

### Alarmer 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 Alarmer aus und schließen Sie das Fenster (siehe [Abbildung 15](#)).

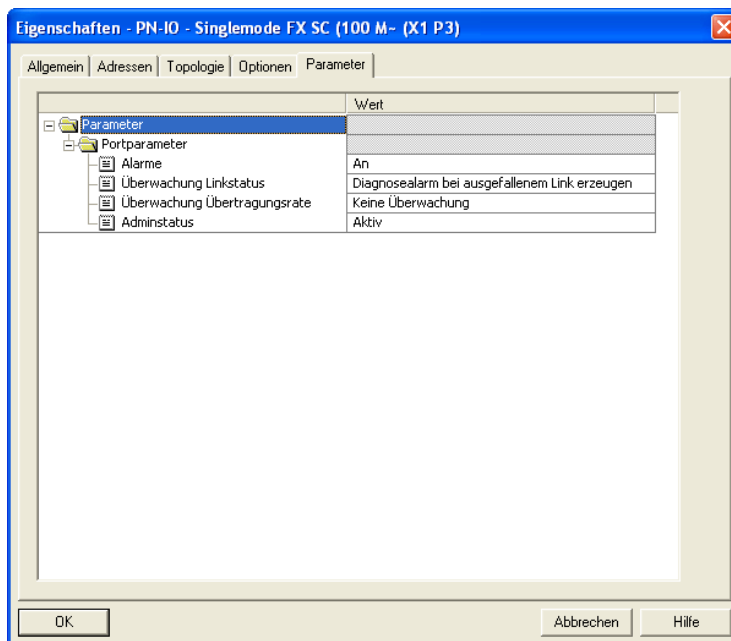


Abb. 15: Port-Eigenschaften

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-Alarm:**

- Wählen Sie unter **Objekteigenschaften** die Karteikarte **Parameter** (Hirschmann-spezifisch).  
Schalten Sie „**Alar**me“ 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**.

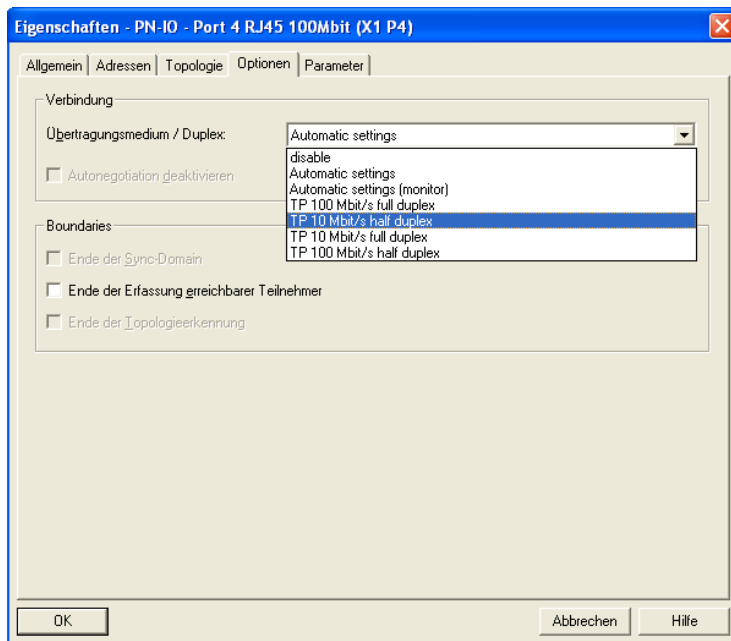


Abb. 16: Dialog zur Eingabe der Verbindungs-Optionen

- 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.

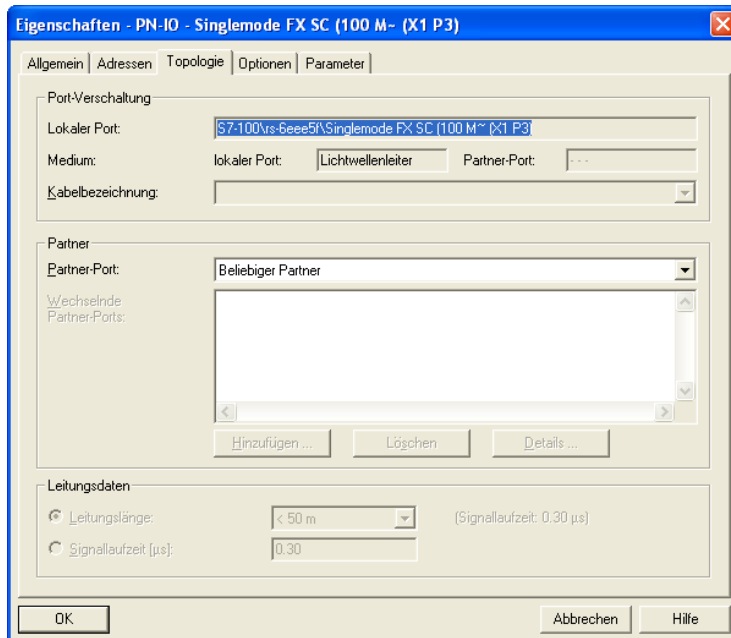


Abb. 17: Dialog zur Eingabe der Topologie

- 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.

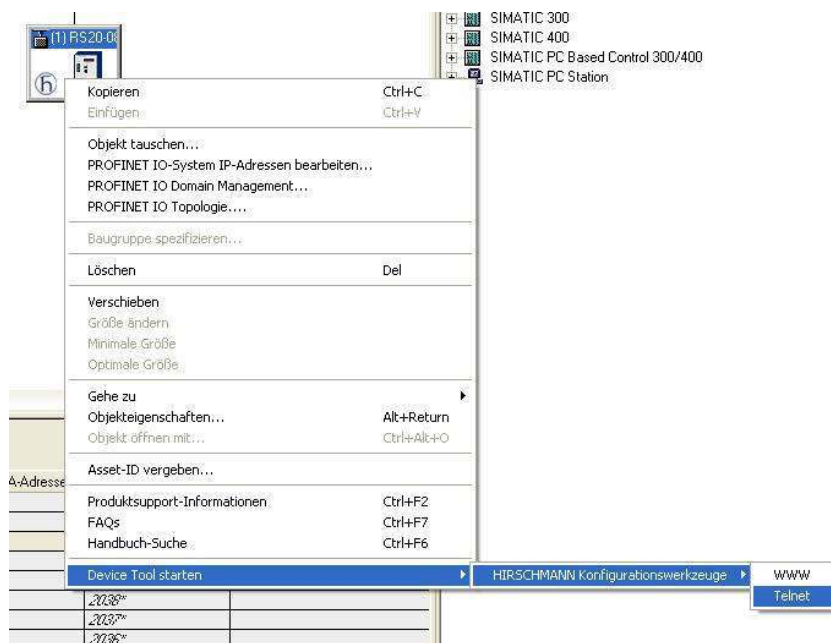


Abb. 18: Hirschmann-Bedienprogramm aufrufen

### 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.

Setzen 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.

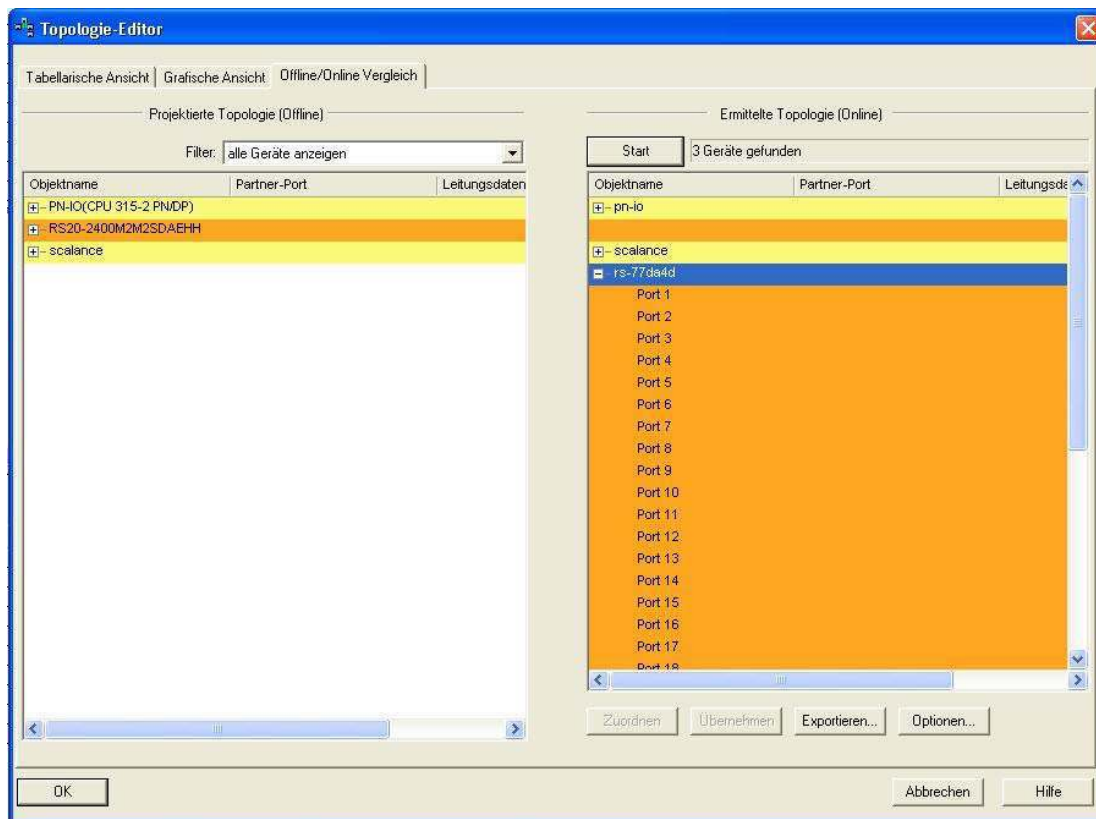


Abb. 19: Topologie-Erkennung

### ■ 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.

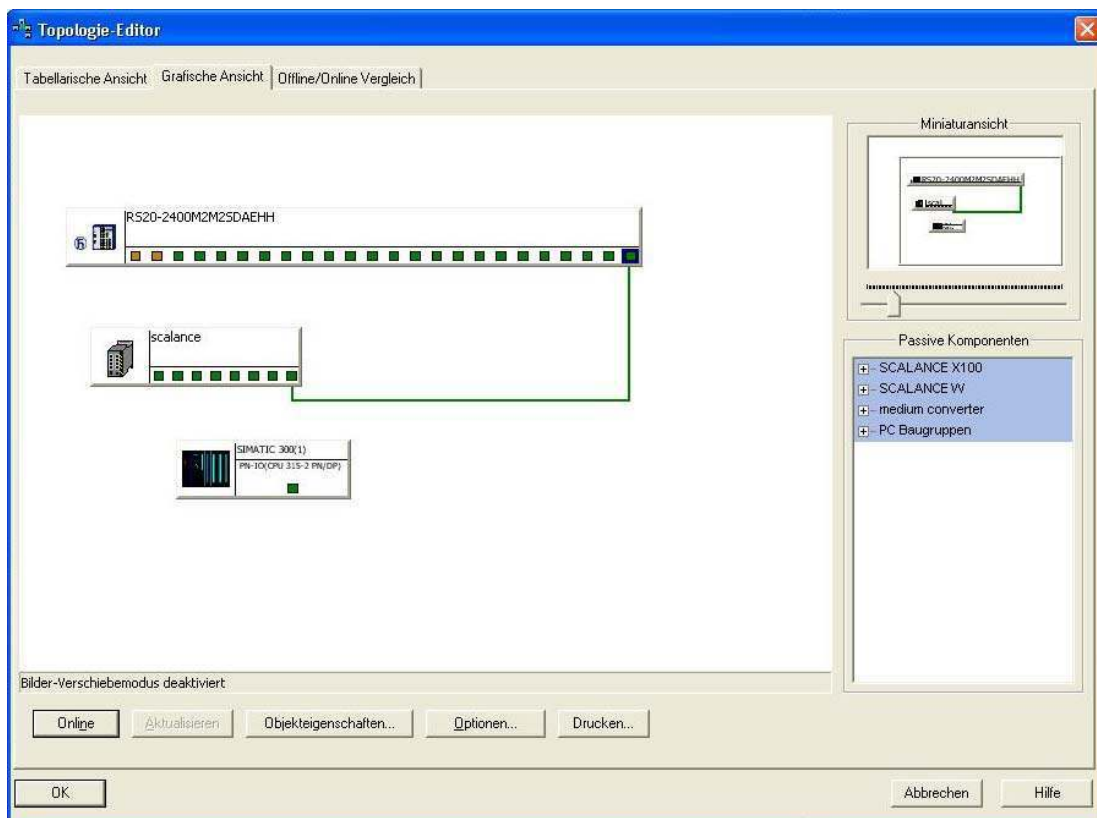


Abb. 20: Projektierung der Topologie

## ■ Kommunikationsdiagnose

Simatic S7 überwacht die Kommunikationsqualität und gibt Meldungen bezüglich Kommunikationsproblemen aus.

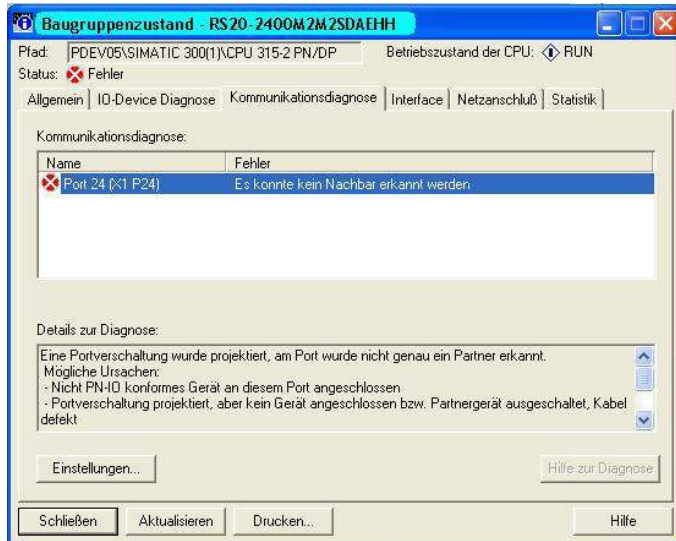


Abb. 21: Diagnosemeldungen zur Kommunikation zwischen den Switches und IO-Geräten

### ■ Portstatistiken ausgeben

Simatic S7 zählt je Port die Anzahl empfangener und gesendeter Datenpakete, Kollisionen, usw. Diese Zählerstände können Sie in Form von Statistiktabelle in Simatic S7 einsehen.

| Port             | Statistikwert                           | aktuell |
|------------------|-----------------------------------------|---------|
| Port 18 (x1 P18) | Dropped received packets - no resources | 0       |
| Port 18 (x1 P18) | Bad received packets                    | 0       |
| Port 18 (x1 P18) | Received octets                         | 337557  |
| Port 18 (x1 P18) | Dropped send packets - no resources     | 0       |
| Port 18 (x1 P18) | Bad send packets - transmit collisions  | 0       |
| Port 18 (x1 P18) | Send octets                             | 469518  |

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<br>- Ausfall der redundanten Spannungsversorgung<br>- Ausfall/Entfernen des ACA |
| Alarme auf Port-Ebene   | - Änderung des Linkstatus,<br>- 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 Statuswechsel 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 Spannungsversorgung 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 Modulbestückung 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<br>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                |
| Input                               | 1             | 7   | nicht benutzt                |
|                                     |               |     | Netzteil-Zustand             |
|                                     |               | 0   | Netzteil 1                   |
|                                     |               | 1   | Netzteil 2                   |
|                                     |               | 2   | Netzteil 3                   |
|                                     |               | 3   | Netzteil 4                   |
|                                     |               | 4   | Netzteil 5                   |
|                                     |               | 5   | Netzteil 6                   |
| Input                               | 2             | 6   | Netzteil 7                   |
|                                     |               | 7   | Netzteil 8                   |
|                                     |               |     | Versorgungsspannungs-Zustand |
|                                     |               | 0   | HIPER-Ring                   |
|                                     |               | 1   | Ring-/Netzkopplung           |
|                                     |               | 2   | VVerbindungsfehler           |
|                                     |               | 3   | nicht benutzt                |
|                                     |               | 4   | nicht benutzt                |
| 5                                   | nicht benutzt |     |                              |
| Output                              |               | 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-Bitinhalt: |      |     |                                                                     |
| - 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-Bitinhalt: |      |     |                                                                        |
| - 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.

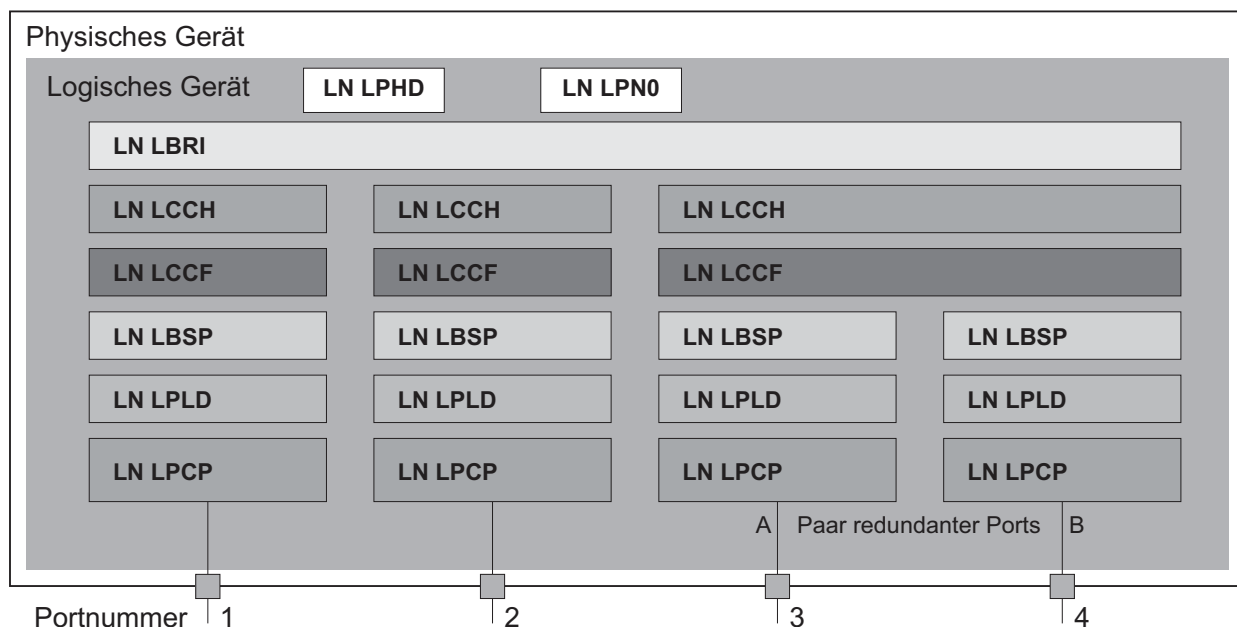


Abb. 23: Bridge-Modell nach Technical Report IEC 61850 90-4

| Klasse  | Beschreibung                                                                                               |
|---------|------------------------------------------------------------------------------------------------------------|
| LN LLN0 | Logischer Knoten „Zero“ des IED „Bridge“:<br>Definiert die logischen Eigenschaften des Geräts.             |
| LN LPHD | Logischer Knoten „Physical Device“ des IED „Bridge“:<br>Definiert die physischen Eigenschaften des Geräts. |
| LN LBRI | Logischer Knoten „Bridge“:<br>Bildet generelle Einstellungen der Bridge-Funktionen des Gerätes ab.         |

Tab. 17: Klassen des Bridge-Modells nach TR IEC61850 90-4

| <b>Klasse</b> | <b>Beschreibung</b>                                                                                                                                       |
|---------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|
| LN LCCH       | Logischer Knoten „Communication Channel“:<br>Definiert den logischen „Communication Channel“, der aus einem oder mehreren physischen Geräteports besteht. |
| LN LCCF       | Logischer Knoten „Channel Communication Filtering“:<br>Definiert die VLAN- und Multicast-Einstellungen für den übergeordneten „Communication Channel“.    |
| LN LBSP       | Logischer Knoten „Port Spanning Tree Protocol“:<br>Definiert die Spanning-Tree-Zustände und -Einstellungen für den jeweiligen physischen Geräteport.      |
| LN LPLD       | Logischer Knoten „Port Layer Discovery“:<br>Definiert die LLDP-Zustände und -Einstellungen für den jeweiligen physischen Geräteport.                      |
| LN LPCP       | Logischer Knoten „Physical Communication Port“:<br>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.

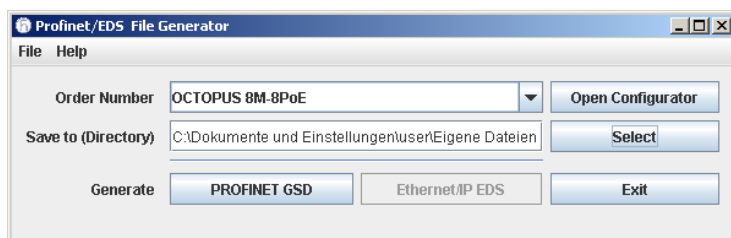


Abb. 24: Standalone GSD-Datei-Generator

## 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 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Lesbarkeit          | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Verständlichkeit    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Beispiele           | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Aufbau              | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Vollständigkeit     | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Grafiken            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Zeichnungen         | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Tabellen            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

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

|                            |            |                               |        |
|----------------------------|------------|-------------------------------|--------|
| <b>A</b>                   |            | <b>R</b>                      |        |
| Alarm                      | 56         | Record                        | 45, 56 |
| Alarmeinrichtung           | 37         | Redundanz                     | 7      |
| <b>C</b>                   |            | Request Packet Intervall      | 19     |
| CIP                        | 15         | Router-Funktion               | 17     |
| Common Industrial Protocol | 15         | RPI                           | 19     |
| <b>E</b>                   |            | RS Who                        | 17     |
| EDS                        | 17, 69     | <b>S</b>                      |        |
| Engineering-Station        | 50, 51     | Schulungsangebote             | 75     |
| Engineering-System         | 38         | Schwellwert                   | 37     |
| EtherNet/IP-Web-Site       | 16         | Simatic S7                    | 38     |
| <b>F</b>                   |            | Standalone GSD File Generator | 38     |
| FAQ                        | 75         | Symbol                        | 9      |
| <b>G</b>                   |            | <b>T</b>                      |        |
| Generic Ethernet Module    | 18         | TCP/IP                        | 15, 33 |
| Gerätebeschreibungssprache | 33         | Technische Fragen             | 75     |
| GSD                        | 36, 69     | <b>U</b>                      |        |
| GSDML                      | 33         | UDP/IP                        | 15, 33 |
| GSDML file Generator       | 37         |                               |        |
| GSDML-Datei                | 39         |                               |        |
| <b>I</b>                   |            |                               |        |
| Icon                       | 17, 36, 39 |                               |        |
| IEC 61850                  | 63         |                               |        |
| IGMP-Snooping              | 17         |                               |        |
| Industrial HiVision        | 8          |                               |        |
| Industrieprotokolle        | 7          |                               |        |
| <b>K</b>                   |            |                               |        |
| Konformitätsklasse         | 33         |                               |        |
| <b>M</b>                   |            |                               |        |
| MMS                        | 63         |                               |        |
| Modul-Eigenschaften        | 43         |                               |        |
| <b>O</b>                   |            |                               |        |
| ODVA                       | 15         |                               |        |
| ODVA-Web-Site              | 16         |                               |        |
| <b>P</b>                   |            |                               |        |
| PC Worx                    | 38         |                               |        |
| PROFIBUS-Organisation      | 33         |                               |        |
| PROFINET IO                | 7          |                               |        |



## 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](mailto:hac.support@belden.com)

in der Region Amerika unter

- ▶ Tel.: +1 (717) 217-2270
- ▶ E-Mail: [inet-support.us@belden.com](mailto:inet-support.us@belden.com)

in der Region Asien-Pazifik unter

- ▶ Tel.: +65 6854 9860
- ▶ E-Mail: [inet-ap@belden.com](mailto: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**

**RS20/RS30/RS40, MS20/MS30, OCTOPUS, PowerMICE,**

**RSR20/RSR30, MACH 100, MACH 1000, 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](http://www.hirschmann.com)).

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

# Inhalt

|          |                                                           |           |
|----------|-----------------------------------------------------------|-----------|
|          | <b>Sicherheitshinweise</b>                                | <b>5</b>  |
|          | <b>Über dieses Handbuch</b>                               | <b>7</b>  |
|          | <b>Legende</b>                                            | <b>9</b>  |
| <b>1</b> | <b>Einleitung</b>                                         | <b>11</b> |
| 1.1      | Übersicht Redundanz-Topologien                            | 12        |
| 1.2      | Übersicht Redundanzverfahren                              | 14        |
| <b>2</b> | <b>Link-Aggregation</b>                                   | <b>17</b> |
| 2.1      | Beispiel für Link-Aggregation                             | 18        |
| 2.1.1    | Link-Aggregation anlegen und konfigurieren                | 19        |
| 2.2      | HIPER-Ring und Link-Aggregation (PowerMICE und MACH 4000) | 24        |
| <b>3</b> | <b>Ring-Redundanz</b>                                     | <b>27</b> |
| 3.1      | Beispiel für HIPER-Ring                                   | 30        |
| 3.1.1    | HIPER-Ring einrichten und konfigurieren                   | 32        |
| 3.2      | Beispiel für MRP-Ring                                     | 36        |
| 3.3      | Beispiel für Fast HIPER-Ring                              | 42        |
| <b>4</b> | <b>Multiple Ringe</b>                                     | <b>47</b> |
| 4.1      | Sub-Ring                                                  | 48        |
| 4.1.1    | Sub-Ring-Beschreibung                                     | 48        |
| 4.1.2    | Sub-Ring-Beispiel                                         | 52        |
| 4.1.3    | Konfiguration des Sub-Ring-Beispiels                      | 55        |
| <b>5</b> | <b>Ring-/Netzkopplung</b>                                 | <b>61</b> |
| 5.1      | Die Varianten der Ring-/Netzkopplung                      | 62        |
| 5.2      | Ring-/Netzkopplung vorbereiten                            | 64        |
| 5.2.1    | STAND-BY-Schalter                                         | 64        |
| 5.2.2    | Ein-Switch-Kopplung                                       | 68        |
| 5.2.3    | Zwei-Switch-Kopplung                                      | 74        |
| 5.2.4    | Zwei-Switch-Kopplung mit Steuerleitung                    | 83        |

|          |                                                            |            |
|----------|------------------------------------------------------------|------------|
| <b>6</b> | <b>Spanning Tree</b>                                       | <b>93</b>  |
| 6.1      | Das Spanning Tree Protokoll                                | 95         |
| 6.1.1    | Die Aufgaben des STP                                       | 95         |
| 6.1.2    | Die Bridge-Parameter                                       | 96         |
| 6.1.3    | Bridge-Identifikation (Bridge-Identifizier)                | 96         |
| 6.1.4    | Root-Pfadkosten                                            | 97         |
| 6.1.5    | Portidentifikation                                         | 99         |
| 6.2      | Regeln für die Erstellung der Baumstruktur                 | 100        |
| 6.2.1    | Bridge-Information                                         | 100        |
| 6.2.2    | Aufbauen der Baumstruktur                                  | 100        |
| 6.3      | Beispiel für die Bestimmung des Root-Pfads                 | 103        |
| 6.4      | Beispiel für die Manipulation des Root-Pfads               | 105        |
| 6.5      | Beispiel für die Manipulation der Baumstruktur             | 107        |
| 6.6      | Das Rapid Spanning Tree Protokoll                          | 108        |
| 6.6.1    | Port-Rollen                                                | 108        |
| 6.6.2    | Port-Stati                                                 | 111        |
| 6.6.3    | Spanning Tree Priority Vector                              | 112        |
| 6.6.4    | Schnelle Rekonfiguration                                   | 112        |
| 6.6.5    | Rapid Spanning Tree konfigurieren                          | 113        |
| 6.7      | Kombinieren von RSTP und MRP                               | 124        |
| 6.7.1    | Anwendungsbeispiel für die Kombination von RSTP<br>und MRP | 126        |
| <b>A</b> | <b>Leserkritik</b>                                         | <b>129</b> |
| <b>B</b> | <b>Stichwortverzeichnis</b>                                | <b>131</b> |
| <b>C</b> | <b>Weitere Unterstützung</b>                               | <b>133</b> |

# 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 „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                                                                                         |
| <input type="checkbox"/>                                                           | Arbeitsschritt                                                                                     |
|   | Zwischenüberschrift                                                                                |
| <a href="#">Link</a>                                                               | Querverweis mit Verknüpfung                                                                        |
| <b>Anmerkung</b>                                                                   | Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit. |
| <code>Courier</code>                                                               | 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              |

# Legende

---



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
- ▶ Fast HIPER-Ring (RSR20, RSR30 und MACH 1000)
- ▶ Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 und MACH 4000)
- ▶ Ring-/Netzkopplung
- ▶ Rapid Spanning Tree Algorithmus (RSTP)

# 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<br>Ring-Redundanz                                                                                | Ring-Redundanz-Verfahren (HIPER-Ring, Fast HIPER-Ring oder MRP) bieten kürzere Umschaltzeiten als RSTP.                                                                                                                |
| Topologie mit 2 Schleifen                       | RSTP<br>Ring-Redundanz<br>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<br>Ring-Redundanz<br>Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 und MACH 4000)<br>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<br>Sub-Ring (RSR20, RSR30, PowerMICE, MACH 1000 und MACH 4000)<br>Ringkopplung                   | Die Ringkopplung koppelt ausschließlich nicht-verschachtelte 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 48 „Sub-Ring“](#)).
- ▶ Sie haben die Möglichkeit, an MRP-Ringe weitere Ringstrukturen anzukoppeln, die mit RSTP arbeiten ([siehe auf Seite 124 „Kombinieren von RSTP und MRP“](#)).



# 1.2 Übersicht

## Redundanzverfahren

| Redundanzverfahren                                                                                                                                                                                                                                                          | Netz-Topologie                                                                                                 | Umschaltzeit                                                                                       |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------|
| RSTP                                                                                                                                                                                                                                                                        | beliebige Struktur                                                                                             | typ. < 1 s (STP < 30 s) bis zu < 30 s - stark abhängig von der Anzahl der Geräte                   |
| <p><b>Anmerkung:</b> Bis zu 79 Geräte je nach Topologie und Konfiguration möglich. Bei Verwendung der Vorgabewerte (Fabrikeinstellungen) je nach Topologie bis zu 39 Geräte möglich (<a href="#">siehe auf Seite 93 „Spanning Tree“</a>).</p>                               |                                                                                                                |                                                                                                    |
| 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. |
| <p><b>Anmerkung:</b> Bei Kombination mit RSTP im MRP-Kompatibilität-Modus je nach Konfiguration bis zu 39 Geräte möglich. Bei Verwendung der Vorgabewerte (Fabrikeinstellungen) für RSTP bis zu 19 Geräte möglich (<a href="#">siehe auf Seite 93 „Spanning Tree“</a>).</p> |                                                                                                                |                                                                                                    |
| Fast HIPER-Ring (RSR20, RSR30 und MACH 1000)                                                                                                                                                                                                                                | Ring                                                                                                           | < 10 ms bei 5 Geräten im Ring.<br>Bei mehr als 5 Geräten erhöht sich die Umschaltzeit.             |
| 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-Aggregation                                                                                                                                                                                                                                                            | Kopplung von Netzsegmenten über parallele aktive Strecken mit dynamischer Lastverteilung und Streckenredundanz |                                                                                                    |

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 zusammenfassen. 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.

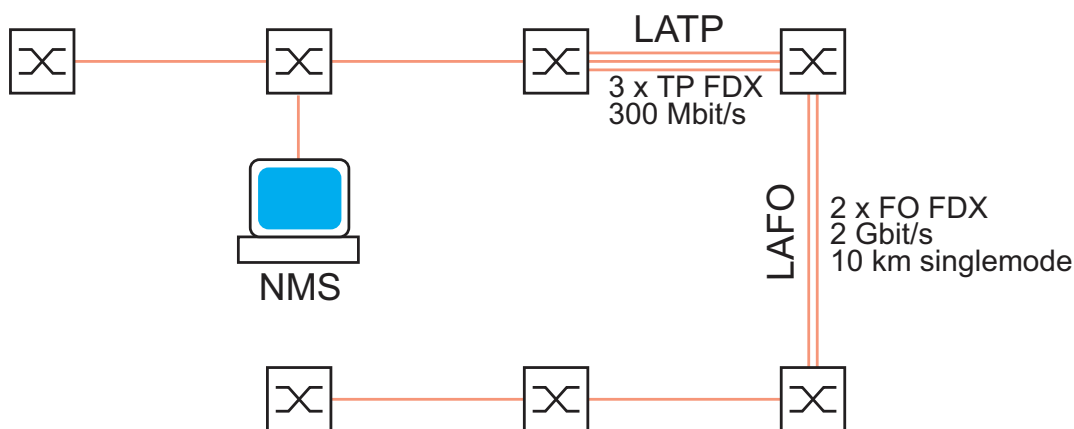


Abb. 1: *Beispiel für Link-Aggregation*  
NMS = Netz-Management-Station  
LATP = Link-Aggregation Twisted Pair  
LAFO = Link-Aggregation Fiber Optic

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 Beispiel 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.

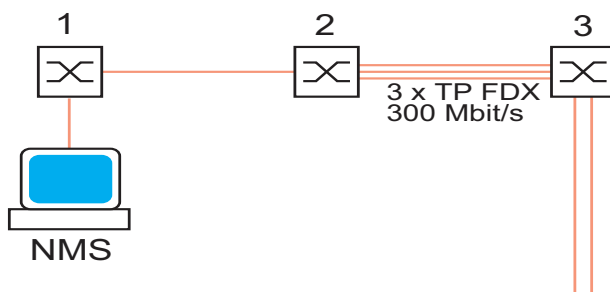


Abb. 2: Beispiel „erstes Gerät bestimmen“  
NMS = Netzmanagementstation

- 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](#)).

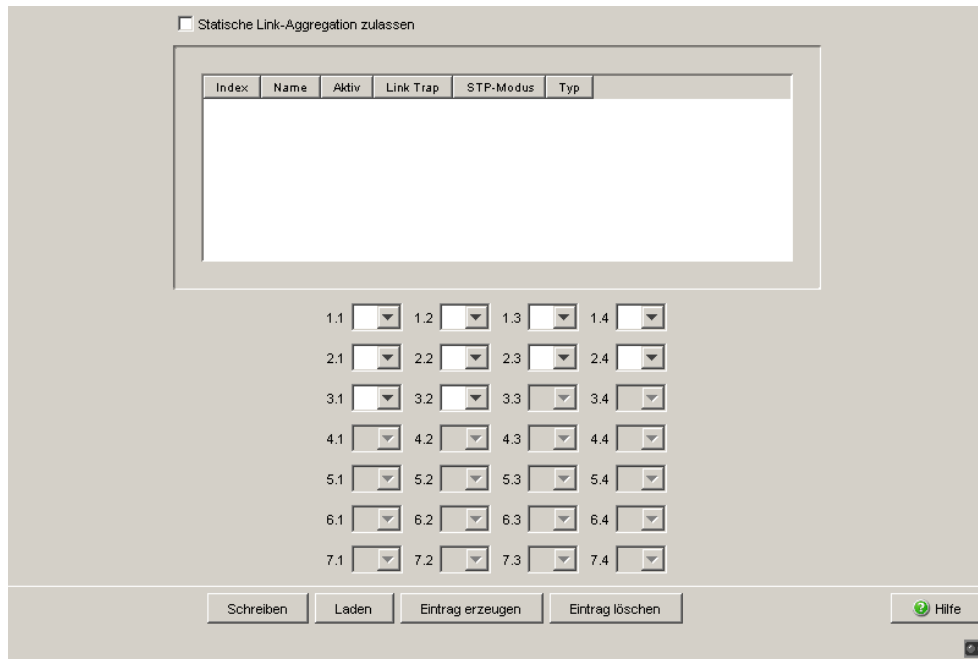


Abb. 3: Link Aggregation anlegen

- 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.

Statische Link-Aggregation zulassen

| Index | Name | Aktiv                               | Link Trap                           | STP-Modus | Typ     |
|-------|------|-------------------------------------|-------------------------------------|-----------|---------|
| 6.1   | LATP | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | on        | dynamic |

1.1  1.2  1.3  1.4

2.1  2.2  2.3  2.4

3.1  3.2  3.3  3.4

4.1  4.2  4.3  4.4

5.1  5.2  5.3  5.4

6.1  6.2  6.3  6.4

7.1  7.2  7.3  7.4

Schreiben    Laden    Eintrag erzeugen    Eintrag löschen    Hilfe

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).



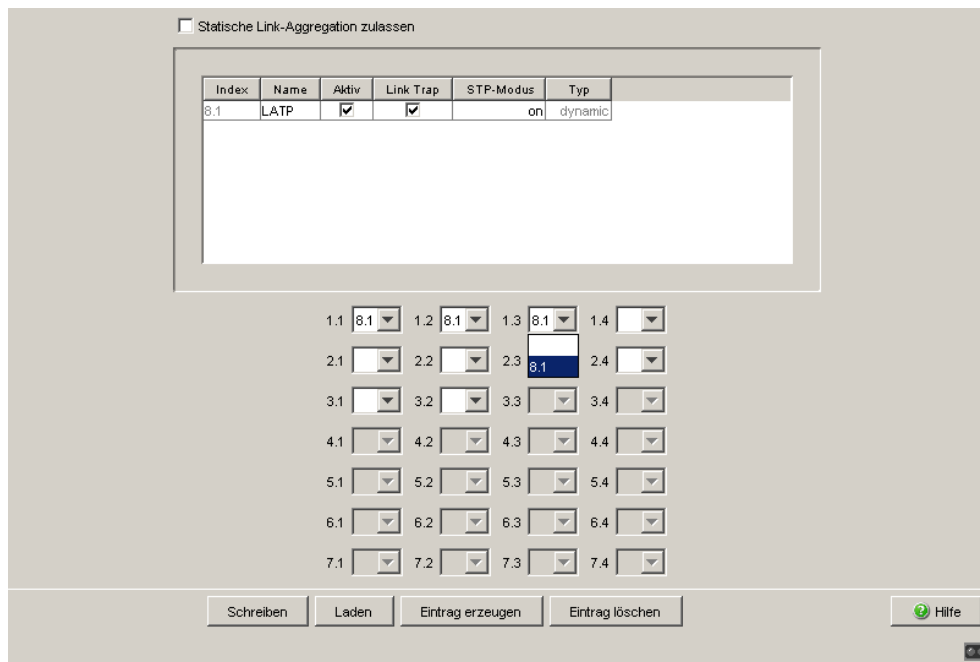


Abb. 5: Ports der Link Aggregation zuweisen

```
enable
configure
link-aggregation LATP
```

```
New Link-Aggregation created. Slot/port is 8.1.
```

```
Interface 1/1
```

```
addport 8/1
```

```
Interface 1/2
```

```
addport 8/1
```

```
Interface 1/3
```

```
addport 8/1
```

```
exit
```

```
show link-aggregation brief
```

```
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
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Legt eine neue Link Aggregation mit dem Namen LATP an.

Konfiguration für Port 1.1

Zuweisung Port 1.1 zu Link Aggregation 8.1.

Konfiguration für Port 1.2

Zuweisung Port 1.2 zu Link Aggregation 8.1.

Konfiguration für Port 1.3

Zuweisung Port 1.3 zu Link Aggregation 8.1.

Wechsel in den Privileged-EXEC-Modus.

Zeigt die Parameter aller auf dem Gerät angelegten Link Aggregationen an.

- 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
- ▶ Fast HIPER-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 27 „Ring-Redundanz“) und Link-Aggregation kombinieren.

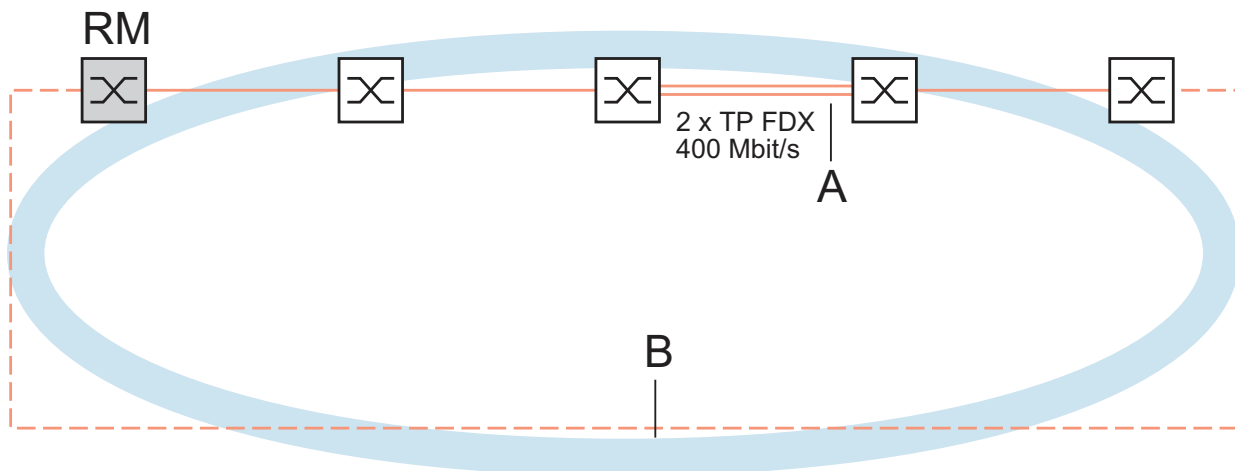


Abb. 6: *Beispiel für HIPER-Ring / Link Aggregation Kombination*  
RM = Ring-Manager  
A = Link-Aggregation  
B = HIPER-Ring

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.

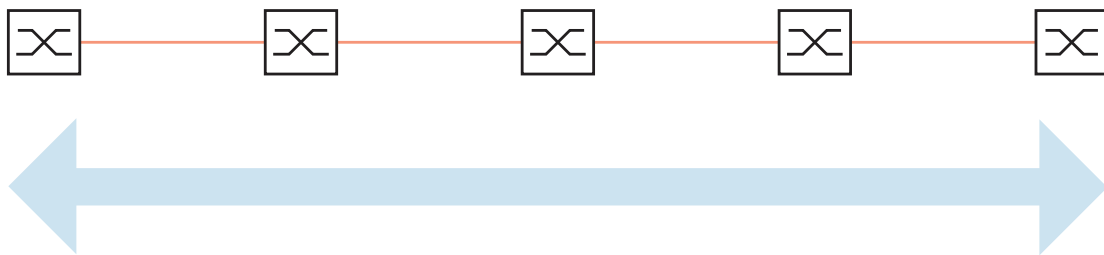


Abb. 7: *Linienstruktur*

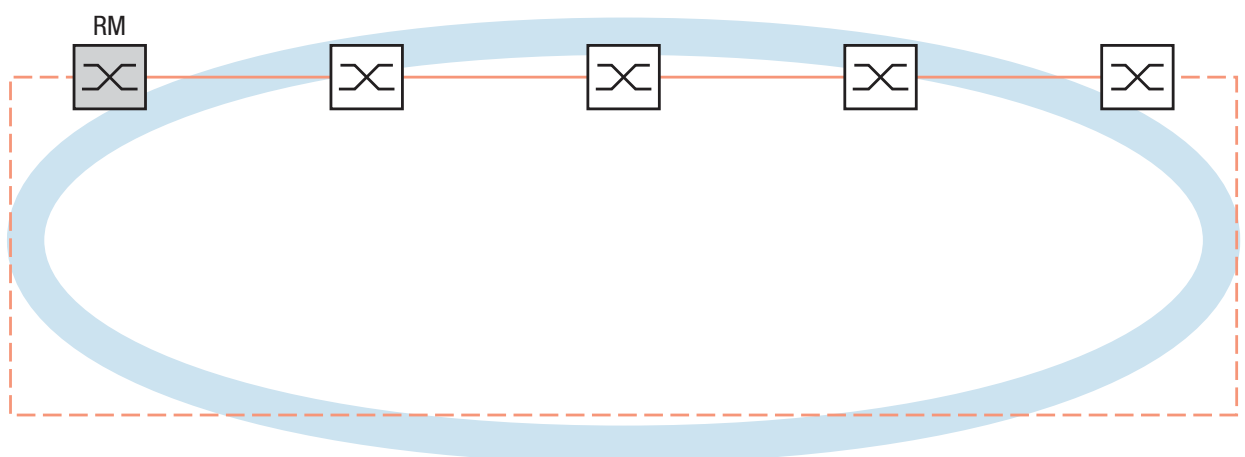


Abb. 8: *Redundante Ringstruktur*  
RM = Ring-Manager  
— Hauptleitung  
- - - Redundante Leitung

Beim Ausfall einer Teilstrecke wandelt sich die Ringstruktur eines

- ▶ **HIPER-(HIGH PERFORMANCE REDUNDANCY)** Rings mit bis zu 50 Geräten im typischen Fall innerhalb von 80 ms (einstellbar: Standard/Beschleunigt) wieder in eine Linienstruktur zurück.
- ▶ **MRP (Media Redundancy Protocol)**-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.
- ▶ **Fast HIPER**-Rings bei bis zu 5 Geräten im typischen Fall innerhalb von 5 ms (maximal 10 ms) wieder in eine Linienstruktur zurück. Beim Einsatz einer größeren Anzahl von Geräten erhöht sich die Rekonfigurationszeit.

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-Protokoll nach IEC 62439 unterstützen.
- ▶ Innerhalb eines Fast HIPER-Ringes können Sie eine beliebige Mischung der folgenden Geräte einsetzen:
  - RSR20/RSR30
  - MACH 1000
  - MACH 1040

**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<sup>1</sup>.

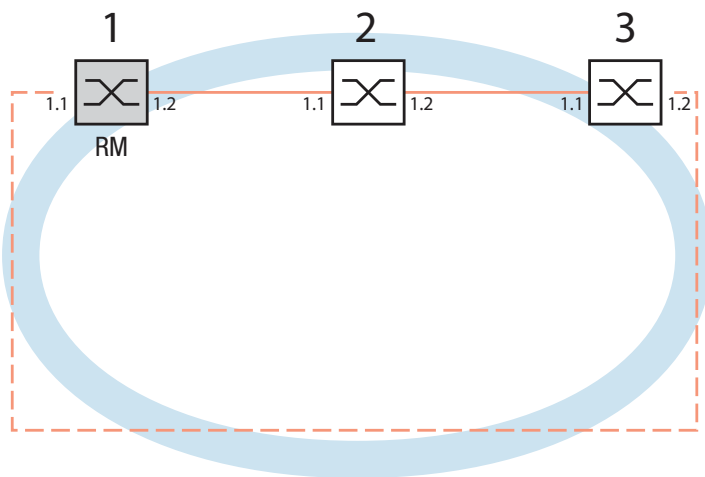


Abb. 9: *Beispiel für HIPER-Ring*  
*RM = Ring-Manager*  
*— Hauptleitung*  
*- - - Redundante Leitung*

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<br>(Automatische<br>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 (RSR20, RSR30, MACH 1000)

- 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“.

|                                                                                     |                                                                                                                                                                       |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure hiper-ring mode ring-manager</pre>                            | <p>Wechsel in den Privileged-EXEC-Modus.<br/>Wechsel in den Konfigurationsmodus.<br/>Wählt die HIPER-Ring Ring-Redundanz und bestimmt das Gerät zum Ring-Manager.</p> |
| <pre>Switch's HIPER Ring mode set to ring-manager hiper-ring port primary 1/1</pre> | <p>Definiert den Port 1 im Modul 1 als Ring Port 1.</p>                                                                                                               |
| <pre>HIPER Ring primary port set to 1/1 hiper-ring port secondary 1/2</pre>         | <p>Definiert den Port 2 im Modul 1 als Ring Port 2.</p>                                                                                                               |
| <pre>HIPER Ring secondary port set to 1/2 exit</pre>                                | <p>Wechsel in den Privileged-EXEC-Modus.</p>                                                                                                                          |

```

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.

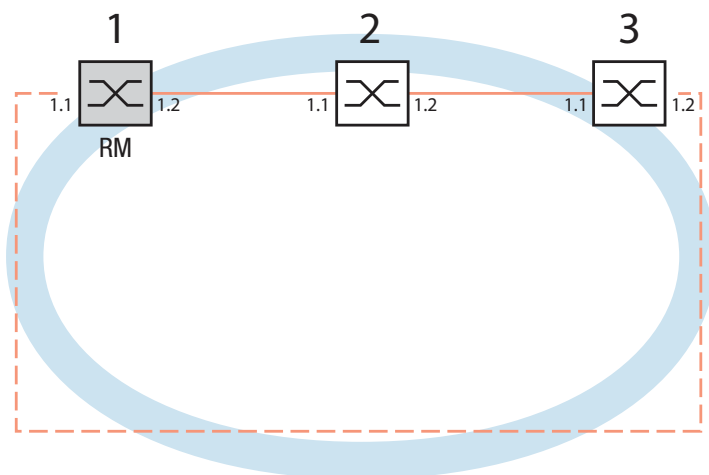


Abb. 11: *Beispiel für MRP-Ring*  
*RM = Ring Manager*  
*— Hauptleitung*  
*- - - Redundante Leitung*

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<br>(Automatische<br>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 (RSR20, RSR30, MACH 1000)

- 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 Redundanzmanagers“ 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  $\cup$  (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 ( $\mathbb{T}$ ) in der statischen VLAN-Tabelle.

**Anmerkung:** Wenn Sie in einem MRP-Ring das Redundanzprotokoll RSTP (siehe auf Seite 93 „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.

|                                                                                                                    |                                                                                                                                                                                                                |
|--------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure mrp new-domain   default-domain</pre>                                                        | <p>Wechsel in den Privileged-EXEC-Modus.<br/>Wechsel in den Konfigurationsmodus.<br/>Legt einen neuen MRP-Ring mit der Default-Domänen-ID<br/>255.255.255.255.255.255.255.255.255.<br/>255.255.255.255 an.</p> |
| <pre>MRP domain created: Domain ID: 255.255.255.255.255.255.255.255.255.255.255.255.255 (Default MRP domain)</pre> |                                                                                                                                                                                                                |
| <pre>mrp current-domain   port primary 1/1 Primary Port set to 1/1</pre>                                           | <p>Definiert den Port 1 im Modul 1 als Ring Port 1 (primary).</p>                                                                                                                                              |
| <pre>mrp current-domain   port secondary 1/2 Secondary Port set to 1/2</pre>                                       | <p>Definiert den Port 2 im Modul 1 als Ring Port 2. (secondary)</p>                                                                                                                                            |
| <pre>mrp current-domain mode manager Mode of Switch set to manager</pre>                                           | <p>Definiert dieses Gerät als Ring-Manager.</p>                                                                                                                                                                |
| <pre>mrp current-domain recovery- delay 200ms Recovery delay set to 200ms</pre>                                    | <p>Definiert 200ms als Wert für „Ringrekonfiguration“.</p>                                                                                                                                                     |
| <pre>mrp current-domain advanced- mode enable Advanced Mode (react on link change) set to Enabled</pre>            | <p>Schaltet den „MRP-Advanced Mode“ ein.</p>                                                                                                                                                                   |
| <pre>mrp current-domain   operation enable Operation set to Enabled</pre>                                          | <p>Schaltet den MRP Ring ein.</p>                                                                                                                                                                              |
| <pre>exit</pre>                                                                                                    | <p>Eine Ebene zurück.</p>                                                                                                                                                                                      |

```
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
(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.

## 3.3 Beispiel für Fast HIPER-Ring

Dieses Beispiel können Sie mit den Modellen RSR20, RSR30 und MACH 1000 realisieren.

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 eine Ring Redundanz zu überführen. Im Unterschied zum vorherigen Beispiel kommt es auf eine sehr kurze Umschaltzeit im Redundanzfall an (etwa 10 ms).

Als Geräte kommen ausschließlich RSR20/RSR30 und MACH 1000 zum Einsatz, deshalb entscheiden Sie sich für Fast HIPER-Ring als Ring-Redundanz-Protokoll. Als Ports für den Anschluss der Verbindungsstrecken nutzen Sie jeweils die Ports 1.1 und 1.2 der Geräte.

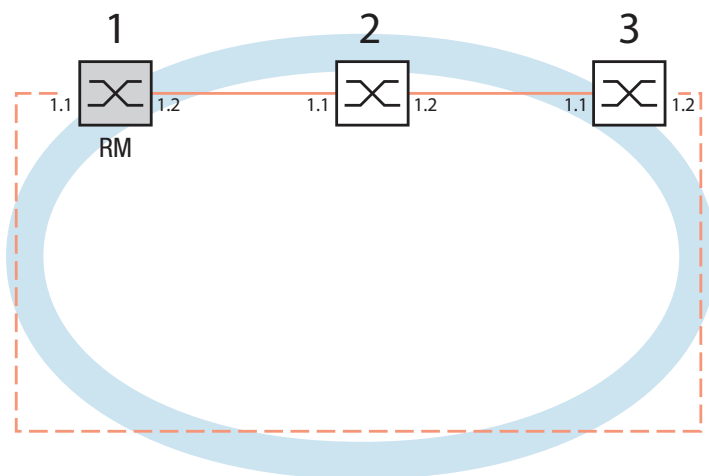


Abb. 13: *Beispiel für Fast HIPER-Ring*  
RM = Ring Manager  
— Hauptleitung  
- - - Redundante Leitung

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. Für dieses Beispiel wird kein VLAN genutzt.

**Anmerkung:** Konfigurieren Sie alle Geräte des Fast HIPER-Rings individuell. Warten Sie mit dem Anschließen der redundanten Strecke, bis Sie die Konfiguration aller Geräte des Fast HIPER-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 Duplex-einstellungen der Strecken der folgenden Tabelle entsprechen:

| Bitrate                                         | 100 Mbit/s | 1000 Mbit/s |
|-------------------------------------------------|------------|-------------|
| Autonegotiation<br>(Automatische Konfiguration) | aus        | an          |
| Port                                            | an         | an          |
| Duplex                                          | voll       | –           |

Tab. 5: Porteinstellungen für Ring-Ports

- Wählen Sie den Dialog `Redundanz: Ring-Redundanz`.
- Wählen Sie unter „Version“ `Fast 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“:

- ▶ `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. 14: Ring-Redundanz Dialog (RSR20, RSR30, MACH 1000)

- Schalten Sie bei diesem Gerät den Ring Manager ein. Schalten Sie bei keinem anderen Gerät im Fast HIPER-Ring den Ring-Manager ein.
- Schalten sie im Rahmen „Funktion“ die Funktion an.
- Belassen Sie im Feld VLAN die VLAN-ID bei 0.
- Geben Sie im Rahmen „Switche“ unter „Anzahl“ die Anzahl der Switche im Ring an. Dieser Eintrag dient der Optimierung der Rekonfigurationszeit und der Stabilität des Rings.
- Um die Änderungen flüchtig zu speichern, klicken Sie „Schreiben“.

Die Anzeige im Rahmen „Ringinformation“ bedeutet:

- Ringumlaufzeit: Vom Ring-Manager gemessene Ringumlaufzeit der Prüfpakete in  $\mu\text{s}$ .

Anzeige beginnend mit 100  $\mu\text{s}$ , in Schritten von 100  $\mu\text{s}$ . Werte um 1000  $\mu\text{s}$  und größer signalisieren, dass der Ring instabil werden kann. Überprüfen Sie in diesem Fall den korrekten Eintrag der Anzahl der Switche im Rahmen „Switche“.

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 Ringports sind inkorrekt konfiguriert (z.B. nicht an den Ringsports eingesteckt).

Der Rahmen "VLAN" bietet Ihnen die Möglichkeit, den Fast HIPER-Ring einem VLAN zuzuordnen:

- Sind VLANs konfiguriert, dann wählen Sie im Rahmen "VLAN":
  - die VLAN-ID 0, wenn die Fast HIPER-Ring-Konfiguration wie in diesem Beispiel keinem VLAN zugeordnet sein soll.  
Wählen Sie für die Ringports die VLAN ID 1 und die VLAN-Zugehörigkeit  $\cup$  (Untagged) in der statischen VLAN-Tabelle.
  - eine VLAN-ID > 0, wenn die Fast HIPER-Ring-Konfiguration diesem VLAN zugeordnet sein soll.  
Tragen Sie bei allen Geräten in diesem Fast HIPER-Ring diese VLAN-ID in der Fast HIPER-Ring-Konfiguration ein und wählen Sie für alle Ringports in diesem Fast HIPER-Ring dann diese VLAN-ID und die VLAN-Zugehörigkeit  $\mathbb{T}$  (Tagged) in der statischen VLAN-Tabelle.

**Anmerkung:** Wenn Sie einen Fast HIPER-Ring über das **Command Line Interface (CLI)** konfigurieren möchten, ist ein zusätzlicher Parameter zu definieren. Bei Konfiguration über das CLI wird ein Fast HIPER-Ring über seine Fast HIPER-Ring-ID angesprochen. Dies ist eine Ziffer im Wertebereich 1 - 2.147.483.647 ( $2^{31} - 1$ ). Die Voreinstellung ist 1. Diesen Wert benutzt das Grät auch intern bei einer Konfiguration über das Web based Interface. Konfigurieren Sie alle Geräte innerhalb eines Fast HIPER-Rings mit der gleichen Fast HIPER-Ring-ID.

```
enable
configure
fast-hiper-ring new-id
default-id
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Legt einen neuen Fast HIPER-Ring mit der „default id“ (1) an. Hierbei werden die Ports 1/1 und 1/2 als Ringports definiert. Behalten Sie diese Vorgabewerte bei.

```
Fast HIPER-Ring ID created:ID: 1 (Default Fast HIPER-Ring ID)
```

```
fast-hiper-ring current-id
mode ring-manager
```

Definiert dieses Gerät als Ring-Manager.

```
Mode of Switch set to Ring Manager
```



```

fast-hiper-ring current-id Definiert die Anzahl der Geräte im HFast HIPER-
nodes 3 Ring auf 3.
Number of nodes set to 3
fast-hiper-ring current-id Schaltet den Fast HIPER-Ring ein.
operation enable
Operation set to Enabled
exit Wechsel in den Konfigurationsmodus.
show fast-hiper-ring Zeigt die aktuellen Parameter des Fast HIPER-
 Rings an.

Ring ID: 1
 (Default Fast HIPER-Ring ID)
Mode of Switch (administrative setting). Ring Manager
Mode of Switch (real operating state)... Ring Manager
Ring Name.....<empty>
Number of nodes in the ring..... 3
Port Number, Primary..... 1/1, State: Not Connected
Port Number, Secondary..... 1/2, State: Not Connected
VLAN ID..... 0 (No VLAN)
Operation..... Enabled

General Operating States:
FHR Setup Info (Config. Failure)..... Ring Port Link Error

Manager-related Operating States:
Ring State..... Open
Redundancy Guaranteed..... No
Round Trip Delay..... 0

```

**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).

- 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 48 „Sub-Ring“](#)).
- ▶ Sie haben die Möglichkeit, an MRP-Ringe weitere Ringstrukturen anzukoppeln, die mit RSTP arbeiten ([siehe auf Seite 124 „Kombinieren von RSTP und MRP“](#)).

## 4.1 Sub-Ring

### 4.1.1 Sub-Ring-Beschreibung

Für die Geräte RSR20, RSR30, PowerMICE, MACH 1000, 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 angekopfelt wird, heißen Sub-Ring-Manager (SRM).

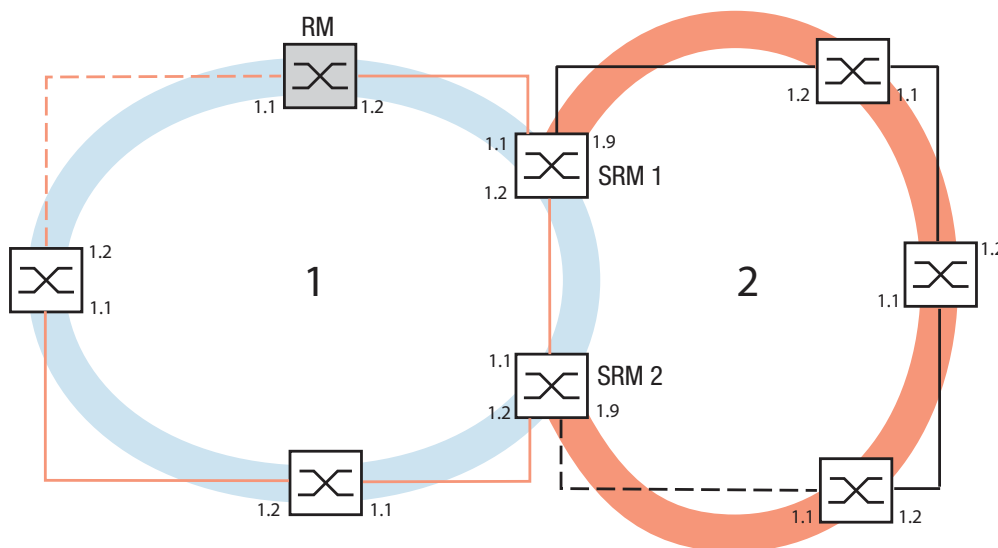


Abb. 15: *Beispiel für Sub-Ring-Struktur*  
 1 blauer Ring = Basis-Ring  
 2 orangefarbener Ring = Sub-Ring  
 SRM = Sub-Ring-Manager  
 RM = Ring-Manager

---

**Anmerkung:** Folgende Geräte unterstützen die Sub-Ring-Manager-Funktion:

- RSR20/RSR30
- MACH 1000
- 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:

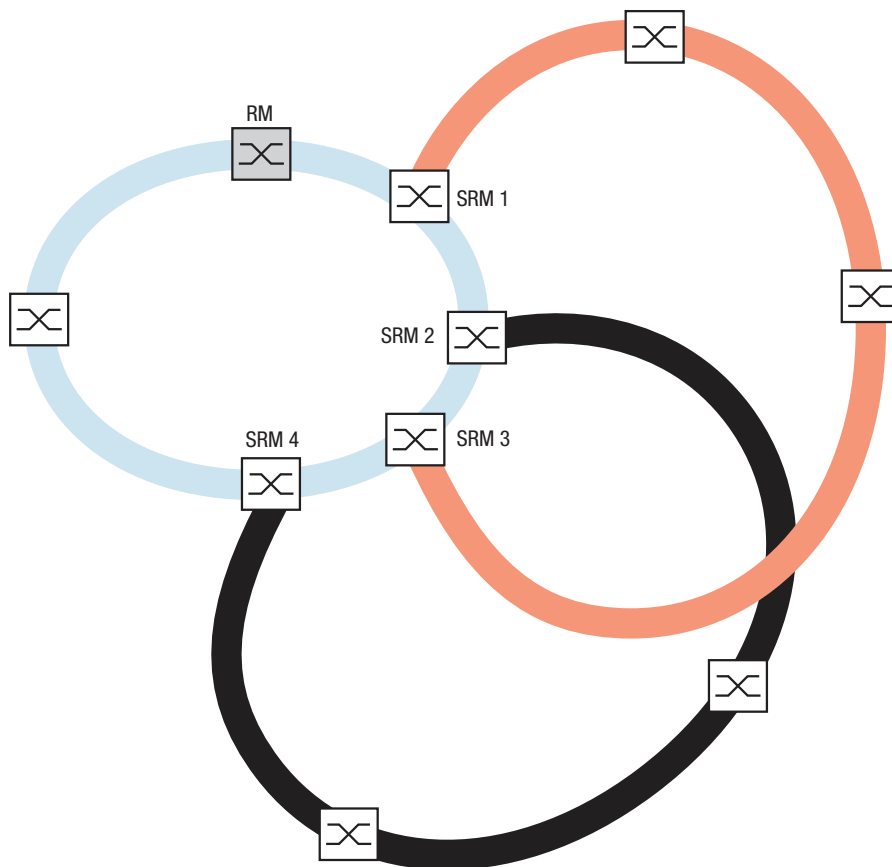


Abb. 16: Beispiel für überlappende Sub-Ring-Struktur

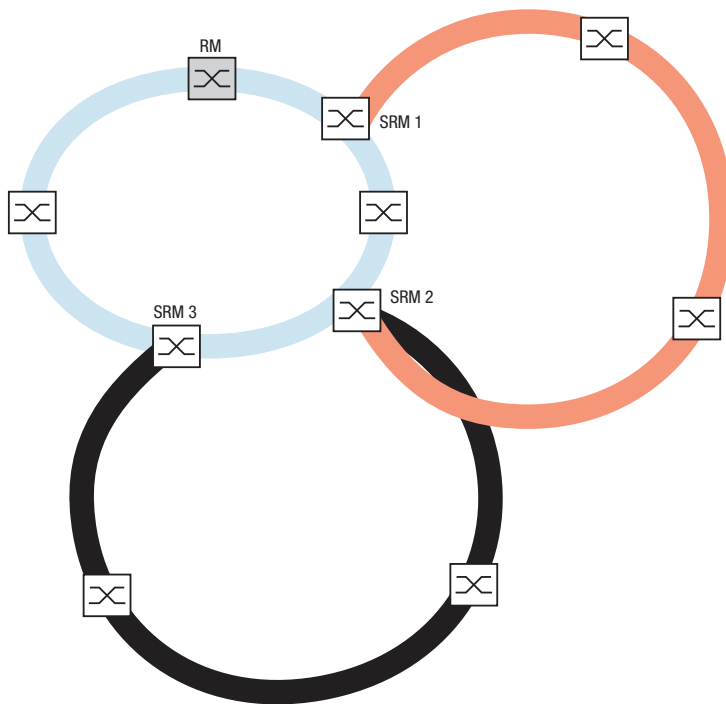


Abb. 17: Sonderfall: ein Sub-Ring-Manager verwaltet 2 Sub-Ringe (2 Instanzen), Je nach Gerätetyp können Sie weitere Instanzen konfigurieren.

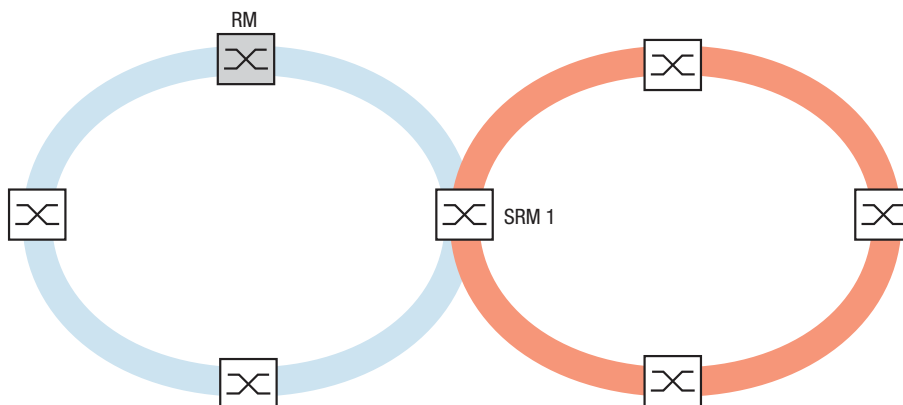


Abb. 18: Sonderfall: ein Sub-Ring-Manager verwaltet beide Enden eines Sub-Rings an unterschiedlichen Ports (Single-Sub-Ring-Manager)

**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

- RSR20/RSR30
- MACH 1000
- MACH 1040
- MACH 4000
- PowerMICE

Konfigurieren Sie diese Geräte zu Sub-Ring-Managern.

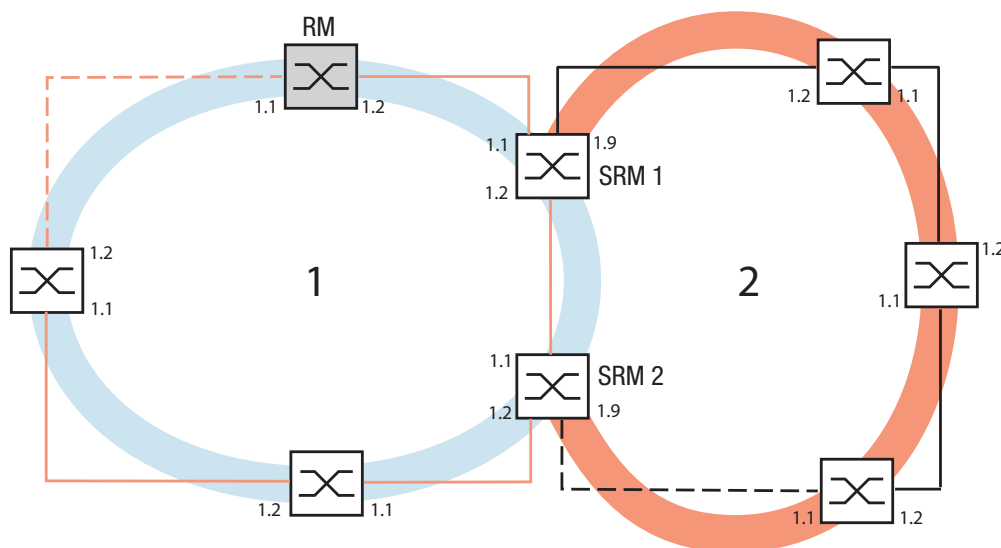


Abb. 19: Beispiel für Sub-Ring-Struktur  
 1 blauer Ring = Basis-Ring  
 2 orangefarbener Ring = Sub-Ring  
 SRM = Sub-Ring-Manager  
 RM = Ring-Manager

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<br>(Automatische<br>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. 6: 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.
  - 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:** 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. 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
configure
mrp delete-domain
current-domain
```

Wechsel in den Privileged-EXEC-Modus.  
 Wechsel in den Konfigurationsmodus.  
 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
 (Default MRP domain)

mrp new-domain
0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99
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

**Anmerkung:** Vermeiden Sie Schleifen während der Konfigurationsphase. Konfigurieren Sie alle Geräte des Sub-Rings individuell. Warten Sie mit dem Anschließen der redundanten Strecke (Schließen des Sub-Rings), bis Sie die Konfiguration aller Geräte des Sub-Rings abgeschlossen haben.

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“.

Neuer Eintrag

Sub-Ring-ID: 2

Port: 1.3

Name: Test

SRM-Modus: manager

VLAN: 0

MRP-Domäne: 255.255.255.255.255.255.255

Schreiben Zurück Hilfe

Abb. 20: 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 Verbindungspport 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) 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.

|                                                                                                                                                                                                                                  |                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <pre>enable configure sub-ring new-ring 1  Sub-Ring ID created:ID: 1 sub-ring 1 port 1/9 Port set to 1/9 sub-ring 1 ring-name Test Sub-Ring Ring name set to "Test" sub-ring 1 mode manager  Mode of Switch set to manager</pre> | <p>Wechsel in den Privileged-EXEC-Modus.<br/>Wechsel in den Konfigurationsmodus.<br/>Legt einen neuen Sub-Ring mit der Sub-Ring-ID 1 an.</p> <p>Definiert den Port 9 im Modul 1 als Sub Ring Port.</p> <p>Vergibt den Namen „Test“ für den Sub-Ring 1</p> <p>Konfiguriert den Modus dieses Sub-Ring-Manager als „manager“.</p> |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

- Klicken Sie auf „Laden“, um die Sub-Ring-Übersicht zu aktualisieren und überprüfen Sie alle Einträge.

| Sub-Ring-ID | Funktion an/aus                     | Konfigurationsstatus | Redundanz vorhanden | Modul. Port | Name | SRM-Modus | SRM-Status | Port-Status | VLAN | Partner-MAC       |
|-------------|-------------------------------------|----------------------|---------------------|-------------|------|-----------|------------|-------------|------|-------------------|
| 1           | <input checked="" type="checkbox"/> |                      |                     | 1.9         | Test | manager   | manager    | 0           | 0    | 00:00:00:00:00:01 |

Abb. 21: 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 nicht-flüchtig in der aktiven Konfiguration zu speichern.

```
enable
configure
sub-ring 1 operation enable
Operation set to Enabled
exit
show sub-ring
```

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Schaltet den Sub-Ring mit der Sub-Ring-ID 1 ein.

Wechsel in den Privileged-EXEC-Modus.

Zeigt den Status für alle Sub-Ringe auf diesem Gerät an.





## 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 23](#)). 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 29](#)).

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 7](#)).

|           | 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. 7: Auswahlkriterien für die Typen der redundanten Kopplungskonfiguration

**Anmerkung:** Wählen sie eine Konfiguration nach den bestehenden topologischen Umständen und dem Maß an Verfügbarkeit, das Sie benötigen, aus (siehe Tabelle 7).

## 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. 8: 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<br>- am DIP-Schalter „STAND-BY“ oder im<br>- Dialog Redundanz : Ring-/Netzkopplung durch Wahl in „Konfiguration auswählen“.<br><b>Hinweis:</b> 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. 9: 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 22](#)).

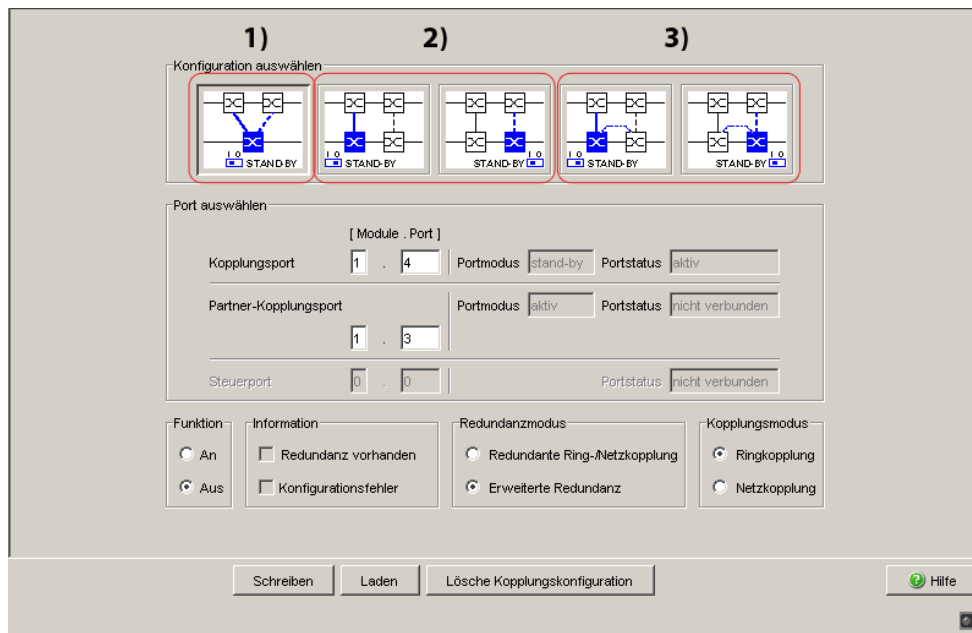


Abb. 22: Ringkopplungs-Konfiguration auswählen (bei deaktivierten DIP-Schaltern oder bei Geräten ohne DIP-Schalter)

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

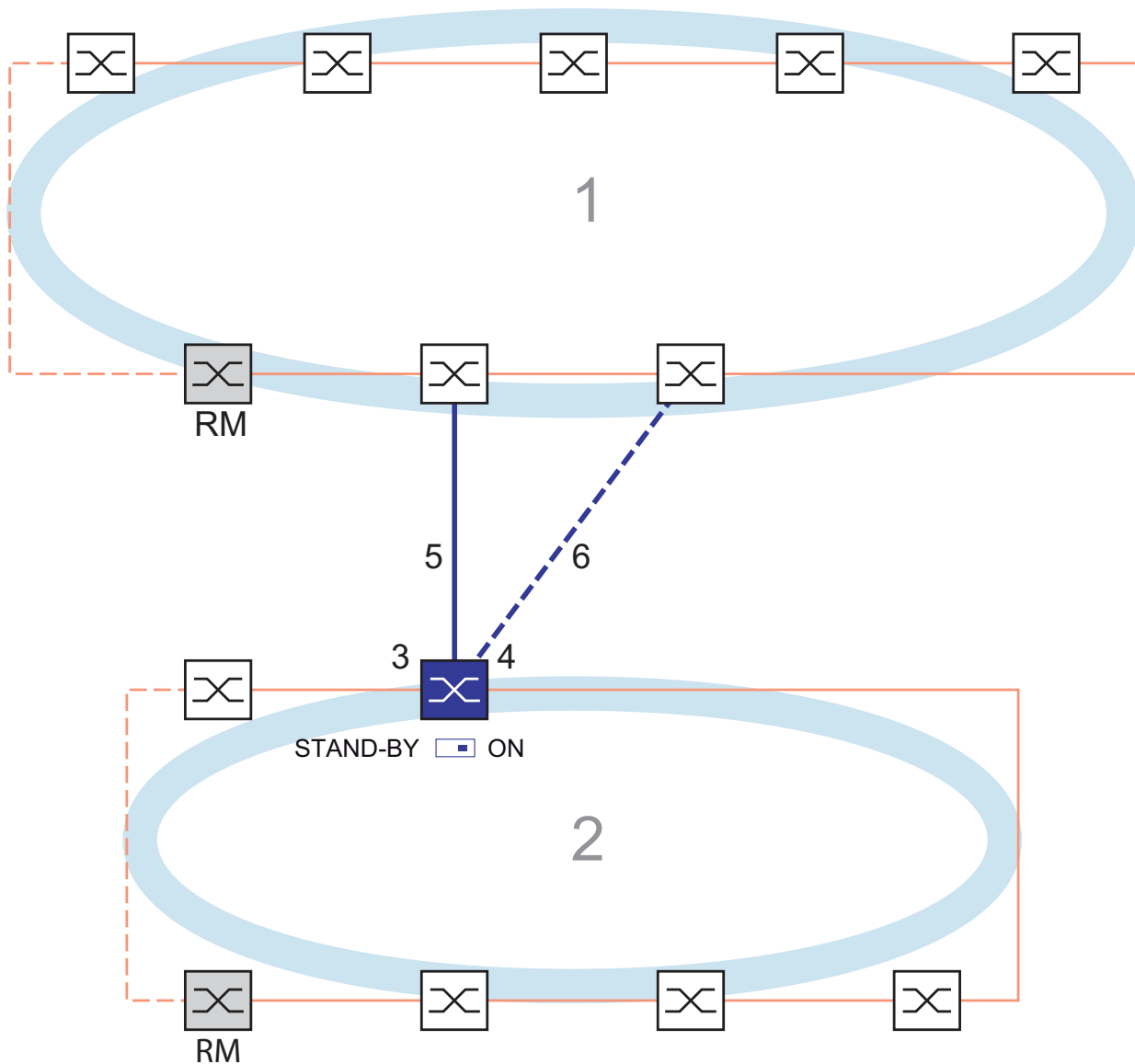


Abb. 23: Beispiel Ein-Switch-Kopplung

1: Backbone

2: Ring

3: Partner-Kopplungsport

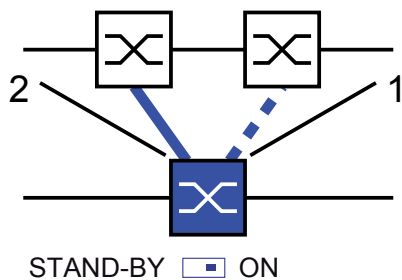
4: Kopplungsport

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 Linie), 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 24](#)).



*Abb. 24: 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 25](#)). Mit „Partner-Kopplungsport“ legen Sie fest, an welchen Port Sie die Hauptleitung anschließen. Die Portzuordnung für die redundante Kopplung finden Sie in [Tabelle 10](#).

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. 10: 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. 10: 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 25](#)).  
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](#).

**Anmerkung:** Konfigurieren Sie den Kopplungsport und die Redundanz-Ring-Ports auf verschiedenen Ports.

- Schalten Sie im Rahmen „Funktion“ die Funktion an (siehe [Abbildung 25](#)).

- 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.

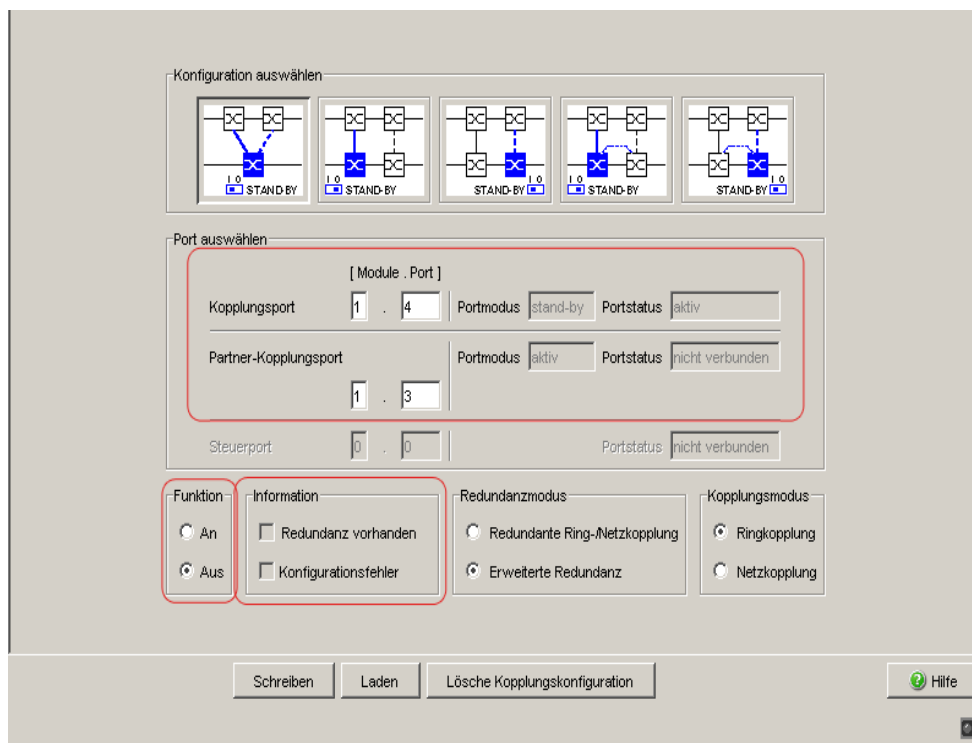


Abb. 25: Ein-Switch-Kopplung: Port auswählen und Funktion ein-/ausschalten

**Anmerkung:** Für die Kopplungsports sind folgende Einstellungen erforderlich (Wählen Sie hierzu den Dialog Grundeinstellungen: Portkonfiguration):

Siehe Tabelle 3 auf Seite 32.

**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  $\mathbb{T}$  (Tagged)  
Das Gerät sendet die Redundanzpakete in VLAN 1 mit höchster Priorität.

### Redundanzmodus

- Wählen Sie im Rahmen „Redundanzmodus“ (siehe Abbildung 26)
  - „Redundante Ring-/Netzkopplung“ oder
  - „Erweiterte Redundanz“.

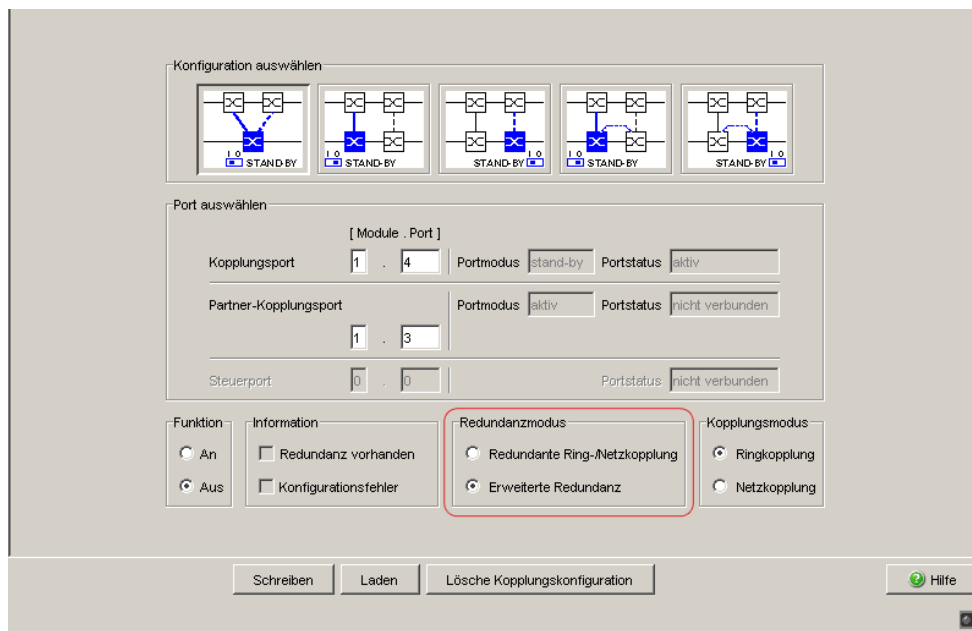


Abb. 26: Ein-Switch-Kopplung: Redundanzmodus auswählen

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 27).

Während der Rekonfigurationszeit kann es zu Paketdoppelungen kommen. Wählen Sie daher diese Einstellung ausschließlich dann, wenn Ihre Anwendung Paketdoppelungen erkennt.

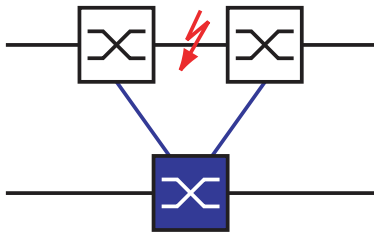


Abb. 27: Erweiterte Redundanz

### Kopplungsmodus

Der Kopplungsmodus bezeichnet die Art des angekoppelten Netzes.

- Wählen Sie im Rahmen „Kopplungsmodus“ (siehe Abbildung 28)
  - „Ringkopplung“ oder
  - „Netzkopplung“

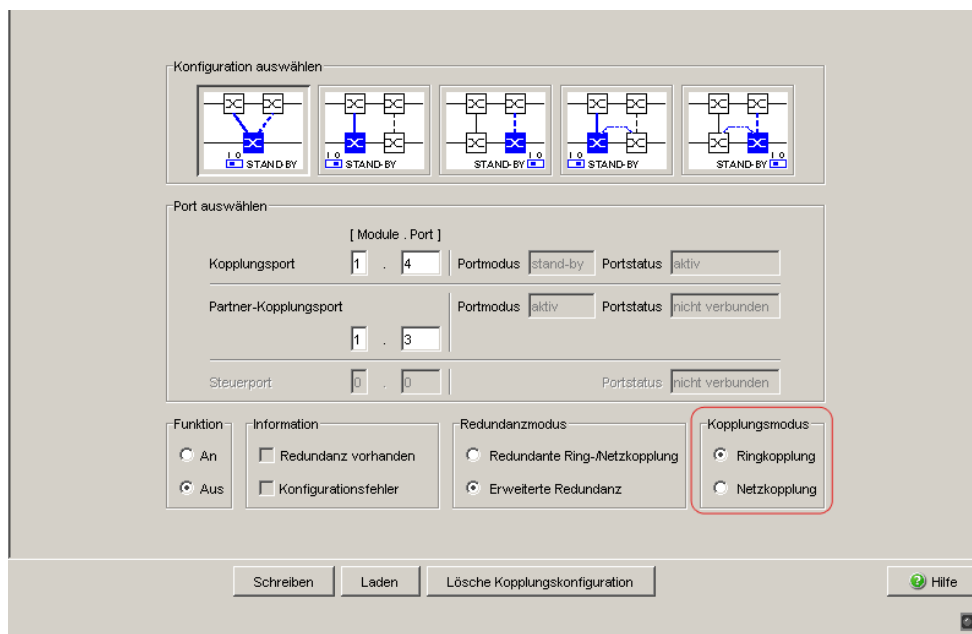


Abb. 28: Ein-Switch-Kopplung: Kopplungsmodus auswählen

- 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

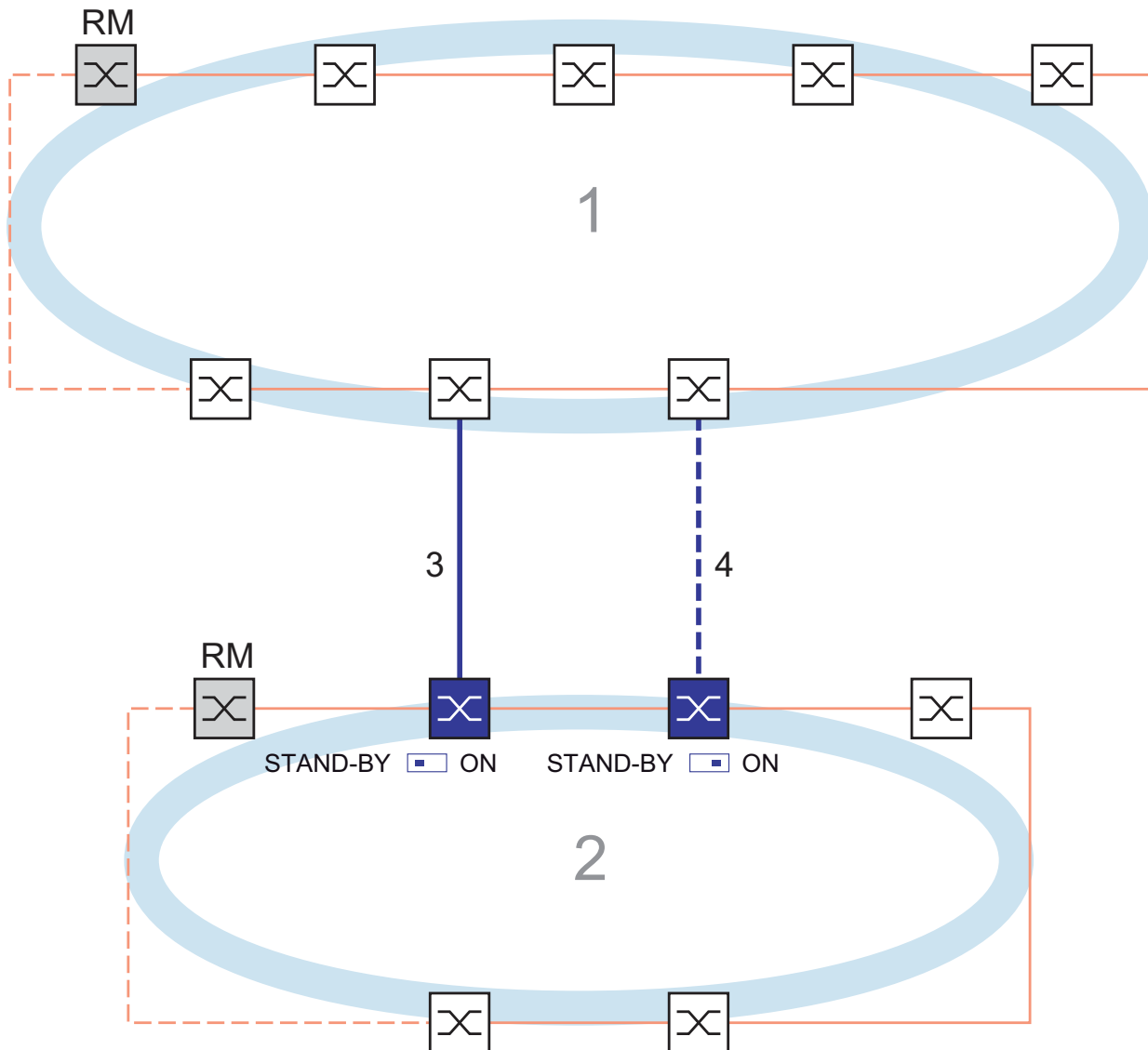


Abb. 29: *Beispiel Zwei-Switch-Kopplung*  
1: Backbone  
2: Ring  
3: Hauptleitung  
4: Redundante Leitung

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.

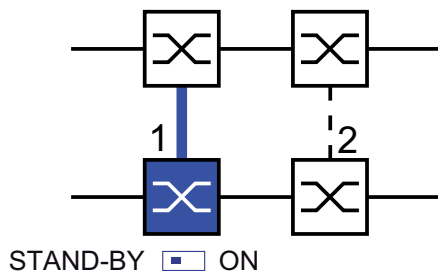
Die Kopplung erfolgt über zwei Switche.

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 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 31](#)).  
 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.

| 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. 11: 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 31](#)).
- 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.

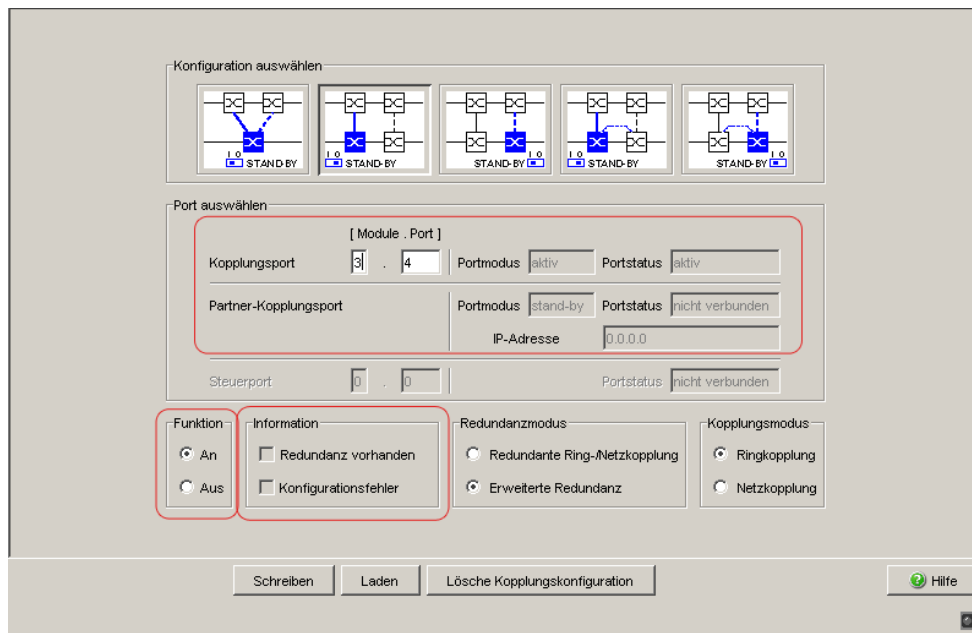


Abb. 31: Zwei-Switch-Kopplung: Port auswählen und Funktion ein-/ausschalten

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 32.](#)

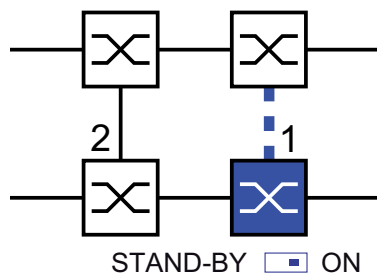
**Anmerkung:** Wenn VLANs konfiguriert sind, stellen Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports wie folgt ein:

- 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 32](#)).



*Abb. 32: 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 31](#)).  
 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.

**Anmerkung:** Konfigurieren Sie den Kopplungsport und die Redundanz-Ring-Ports auf verschiedenen Ports.

- Schalten Sie im Rahmen „Funktion“ die Funktion an (siehe [Abbildung 31](#)).

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 32.](#)

**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 33](#))
  - „Redundante Ring-/Netzkopplung“ oder
  - „Erweiterte Redundanz“.

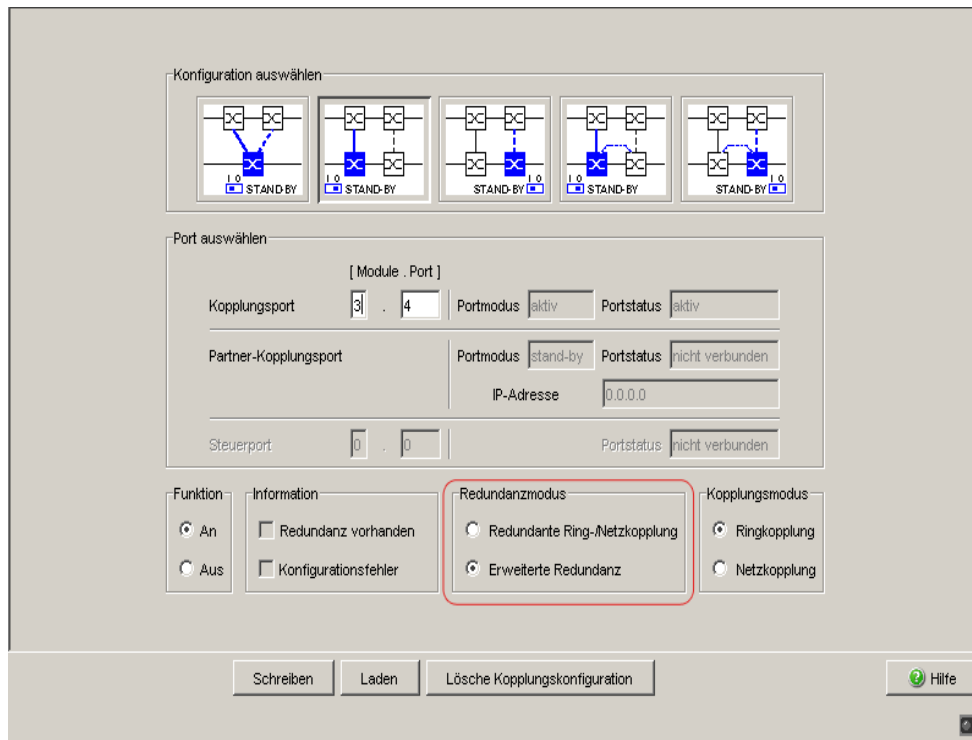


Abb. 33: Zwei-Switch-Kopplung: Redundanzmodus auswählen

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 27](#)).

Während der Rekonfigurationszeit kann es zu Paketdoppelungen kommen. Wählen Sie daher diese Einstellung ausschließlich dann, wenn Ihre Anwendung Paketdoppelungen erkennt.

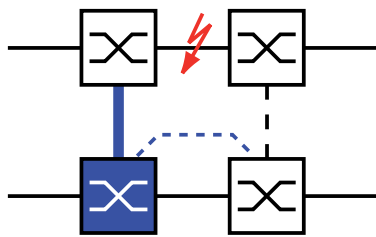


Abb. 34: Erweiterte Redundanz

### Kopplungsmodus

Der Kopplungsmodus bezeichnet die Art des angekoppelten Netzes.

- Wählen Sie im Rahmen „Kopplungsmodus“ (siehe Abbildung 35)
  - „Ringkopplung“ oder
  - „Netzkopplung“

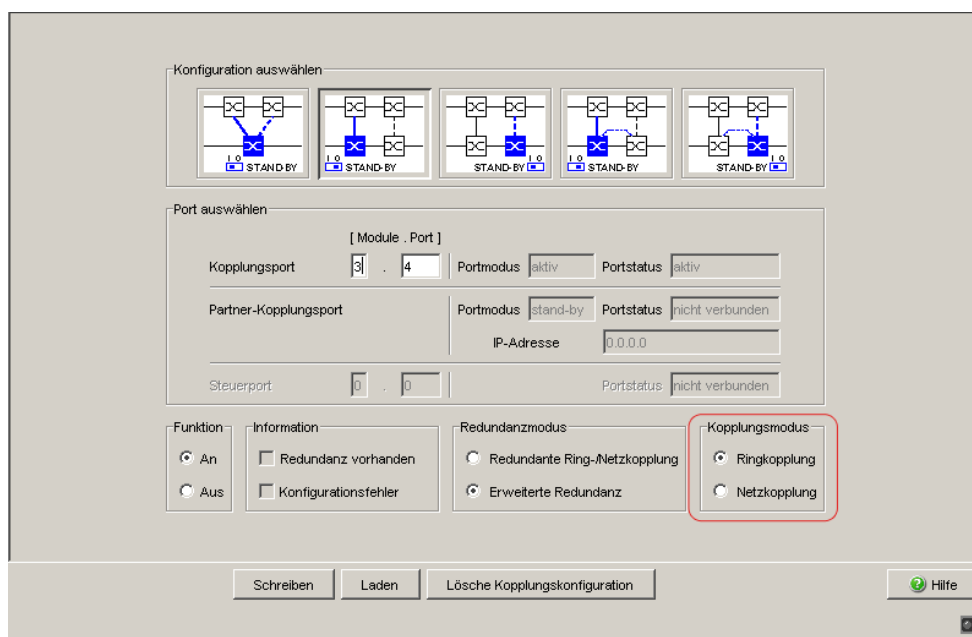


Abb. 35: Zwei-Switch-Kopplung: Kopplungsmodus auswählen

- 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

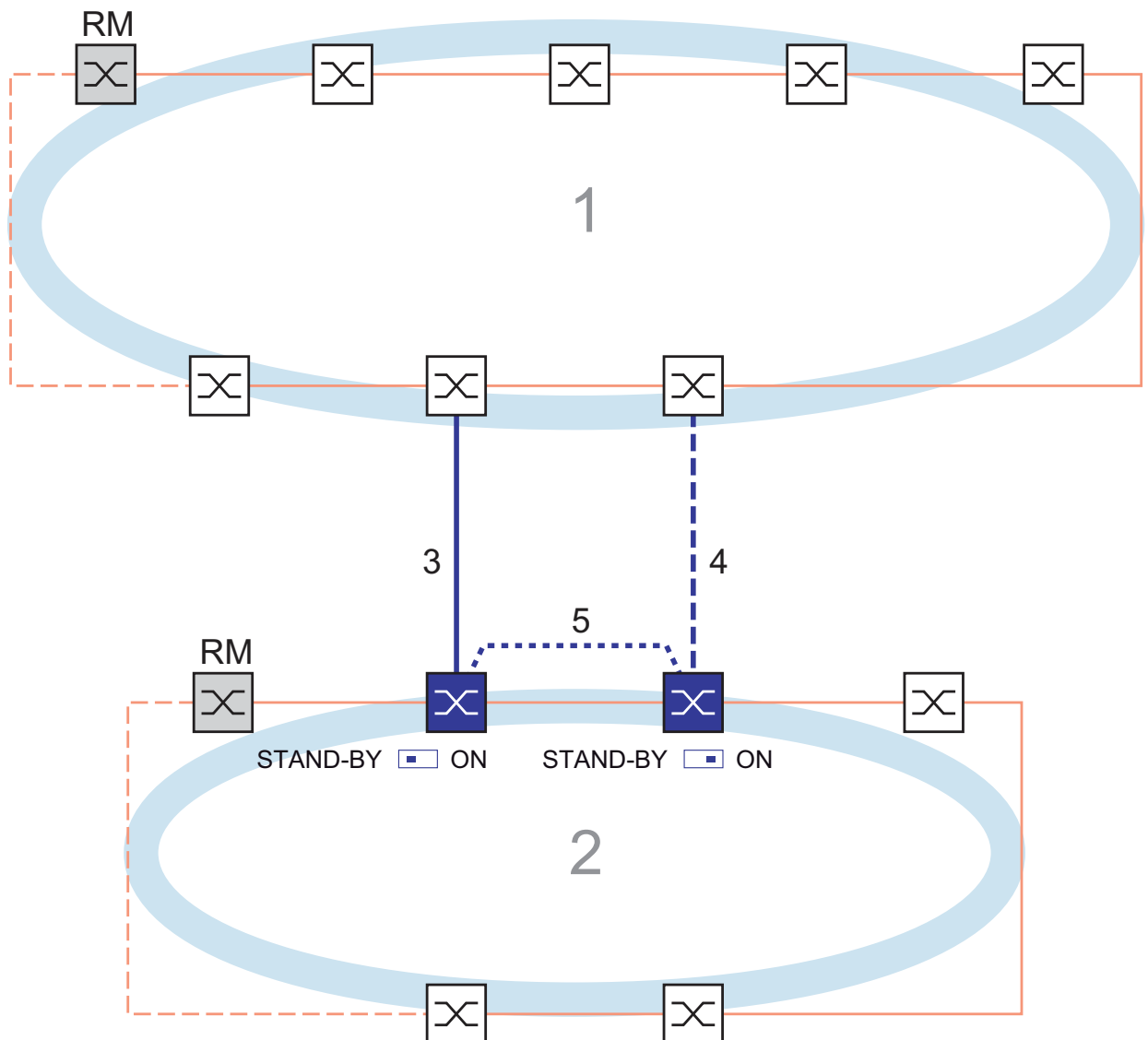


Abb. 36: *Beispiel Zwei-Switch-Kopplung mit Steuerleitung*  
1: Backbone  
2: Ring  
3: Hauptleitung  
4: Redundante Leitung  
5: Steuerleitung

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.

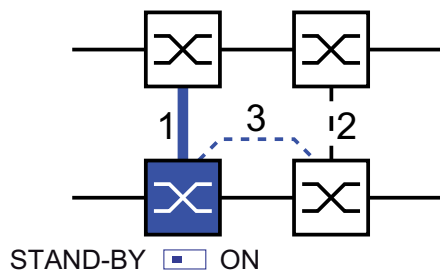
Die Kopplung erfolgt über zwei Switche.

Die Switche übermitteln ihre Kontrollpakete über eine Steuerleitung (punktierete 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 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 38](#)).  
 Mit „Kopplungsport“ legen Sie fest, an welchen Port Sie die Verbindung der Netzsegmente anschließen.  
 Die Portzuordnung für die redundante Kopplung finden Sie in [Tabelle 12](#).
- 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 38](#)).  
 Mit „Steuerport“ legen Sie fest, an welchen Port Sie die Steuerleitung anschließen.  
 Die Portzuordnung für die redundante Kopplung finden Sie in [Tabelle 12](#).

| Gerät               | Kopplungsport                                           | Steuerport                                               |
|---------------------|---------------------------------------------------------|----------------------------------------------------------|
| RS2-./.             | Port 1                                                  | Stand-by-Port (ausschließlich mit RS2-./.. kombinierbar) |
| RS2-16M             | Einstellbar für alle Ports<br>(Lieferzustand: Port 1)   | Einstellbar für alle Ports<br>(Lieferzustand: Port 2)    |
| RS20, RS30,<br>RS40 | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.3)  |
| OCTOPUS             | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.3)  |
| MICE                | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.3)  |
| PowerMICE           | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.3)  |
| MS20                | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.3)  |
| MS30                | Einstellbar für alle Ports<br>(Lieferzustand: Port 2.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 2.3)  |
| RSR20/RSR30         | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.3)  |
| MACH 100            | Einstellbar für alle Ports<br>(Lieferzustand: Port 2.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 2.3)  |
| MACH 1000           | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.3)  |
| MACH 3000           | Einstellbar für alle Ports                              | Einstellbar für alle Ports                               |
| MACH 4000           | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.4) | Einstellbar für alle Ports<br>(Lieferzustand: Port 1.3)  |

Tab. 12: 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 38](#)).
- 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.

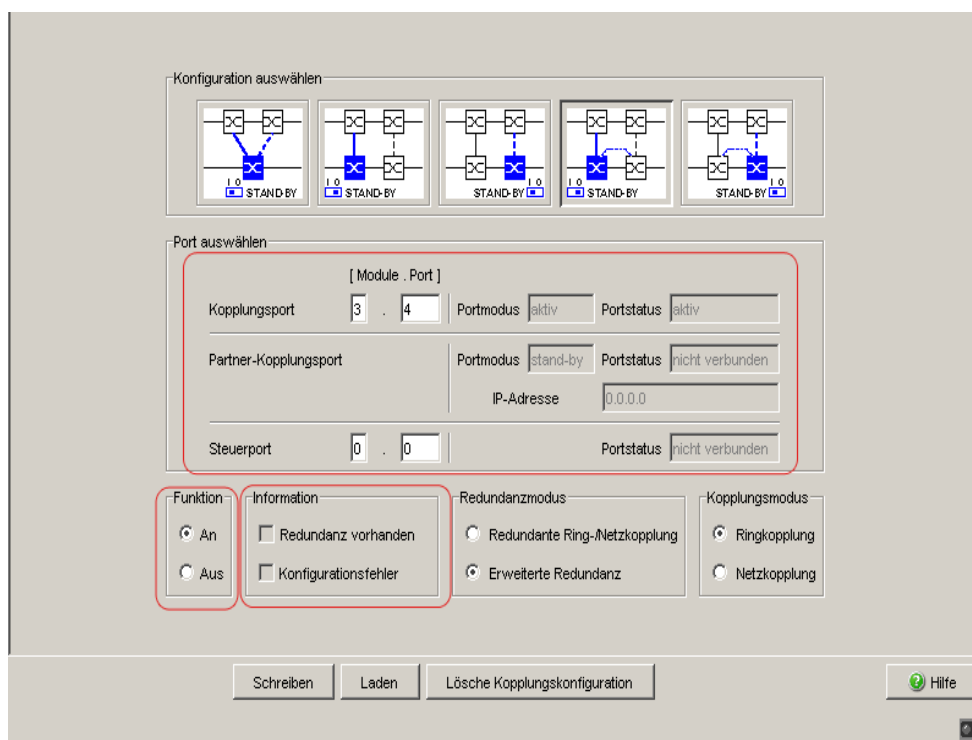


Abb. 38: Zwei-Switch-Kopplung mit Steuerleitung: Port auswählen und Funktion ein-/ausschalten

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 32](#).

**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  $\top$  (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 39](#)).

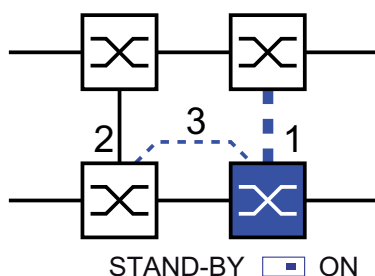


Abb. 39: Zwei-Switch-Kopplung mit Steuerleitung

- 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 38](#)). Mit „Kopplungsport“ legen Sie fest, an welchen Port Sie die Verbindung der Netzsegmente anschließen. Die Portzuordnung für die redundante Kopplung finden Sie in [Tabelle 12](#).

- 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 38](#)).  
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 38](#)).
- 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:

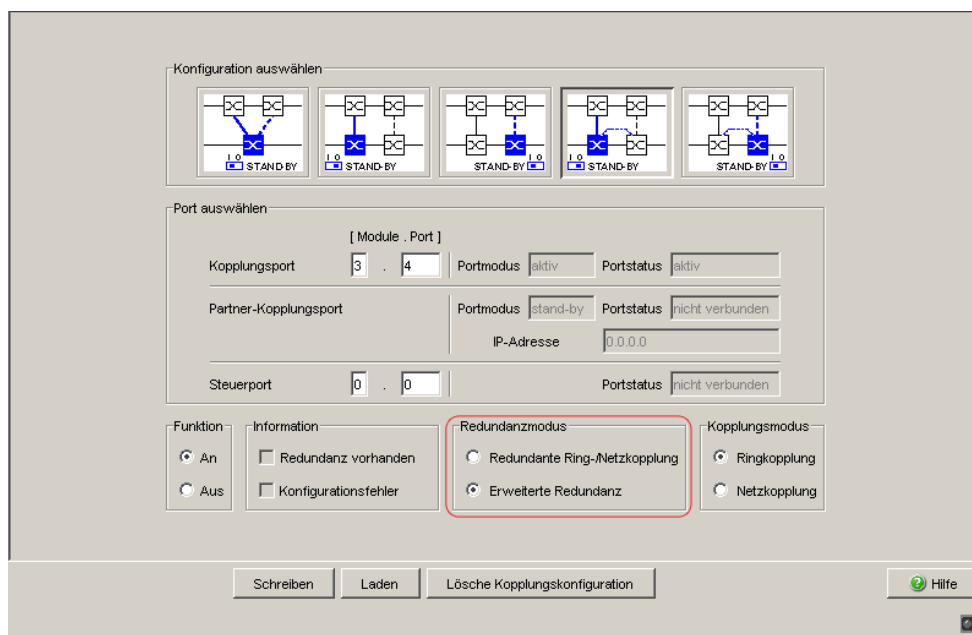
- die Funktion ausschalten oder
- die Konfiguration wechseln

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  $\mathbb{T}$  (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. 40:** 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 27).

Während der Rekonfigurationszeit kann es zu Paketdoppelungen kommen. Wählen Sie daher diese Einstellung ausschließlich dann, wenn Ihre Anwendung Paketdoppelungen erkennt.

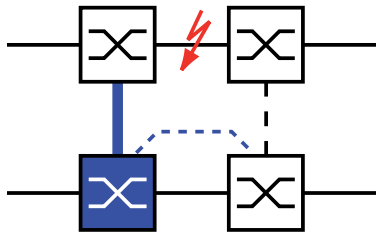


Abb. 41: Erweiterte Redundanz

### Kopplungsmodus

Der Kopplungsmodus bezeichnet die Art des angekoppelten Netzes.

- Wählen Sie im Rahmen „Kopplungsmodus“:
  - „Ringkopplung“  
oder
  - „Netzkopplung“

Konfiguration auswählen

Port auswählen

[ Module . Port ]

Kopplungsport 3 . 4 Portmodus aktiv Portstatus aktiv

Partner-Kopplungsport Portmodus stand-by Portstatus nicht verbunden

IP-Adresse 0.0.0.0

Steuerport 0 . 0 Portstatus nicht verbunden

Funktion Information Redundanzmodus Kopplungsmodus

An  Redundanz vorhanden  Redundante Ring-/Netzkopplung  Ringkopplung

Aus  Konfigurationsfehler  Erweiterte Redundanz  Netzkopplung

Schreiben Laden Lösche Kopplungskonfiguration Hilfe

Abb. 42: 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 benötigt 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`, [\(siehe Tabelle 15\)](#))
- ▶ 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-Identifizier),
- ▶ Root-Pfadkosten der Bridge-Ports,
- ▶ Port-Identifikation (Port-Identifizier).

## 6.1.3 Bridge-Identifikation (Bridge-Identifizier)

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. 43: 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 13). 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.

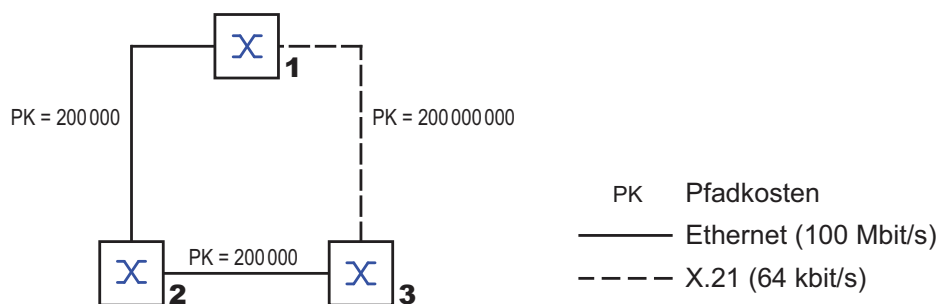


Abb. 44: Pfadkosten

| Datenrate   | Empfohlener Wert         | Empfohlener Bereich    | Möglicher Bereich |
|-------------|--------------------------|------------------------|-------------------|
| ≤100 Kbit/s | 200.000.000 <sup>a</sup> | 20.000.000-200.000.000 | 1-200.000.000     |
| 1 Mbit/s    | 20.000.000 <sup>a</sup>  | 2.000.000-200.000.000  | 1-200.000.000     |
| 10 Mbit/s   | 2.000.000 <sup>a</sup>   | 200.000-20.000.000     | 1-200.000.000     |
| 100 Mbit/s  | 200.000 <sup>a</sup>     | 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. 13: 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. 13: *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 17 „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.

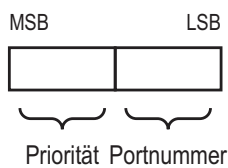


Abb. 45: *Portidentifikation*

## 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 45](#)). 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.



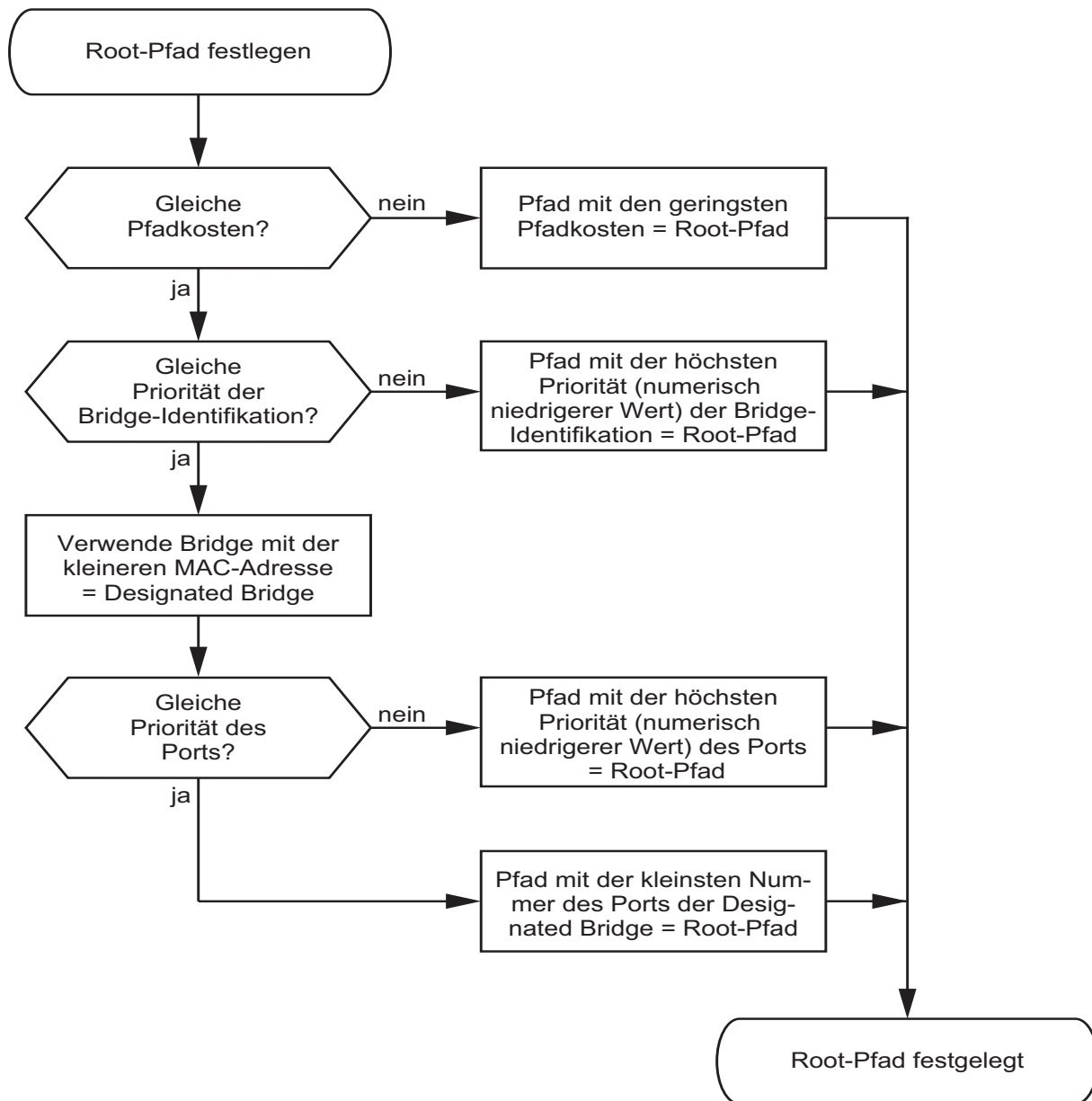


Abb. 46: Flussdiagramm Root-Pfad festlegen

## 6.3 Beispiel für die Bestimmung des Root-Pfads

Anhand des Netzplanes (siehe [Abbildung 47](#)) kann man das Flussdiagramm (siehe [Abbildung 46](#)) 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).

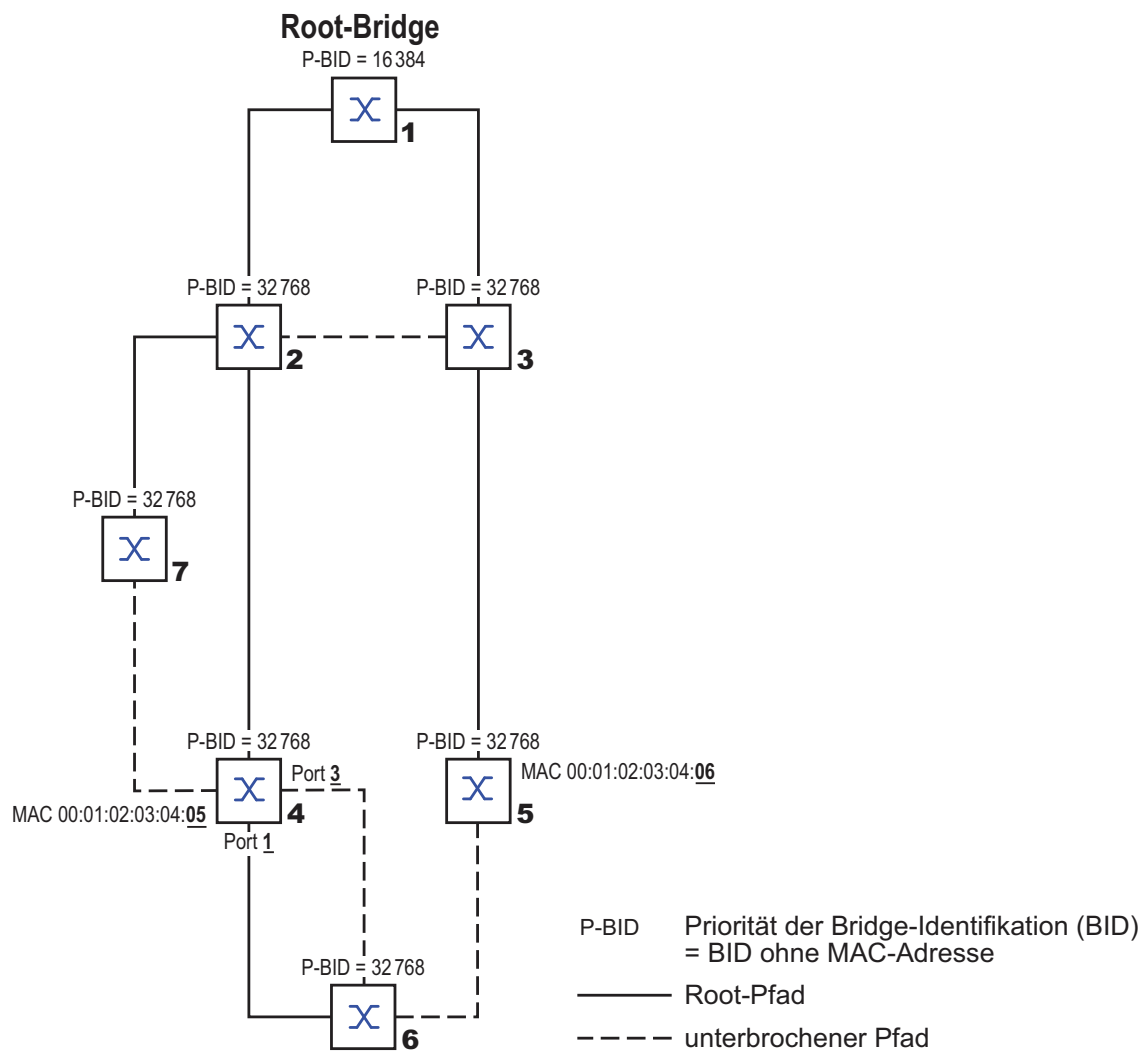


Abb. 47: Beispiel für die Bestimmung des Root-Pfads

## 6.4 Beispiel für die Manipulation des Root-Pfads

Anhand des Netzplanes (siehe [Abbildung 47](#)) kann man das Flussdiagramm (siehe [Abbildung 46](#)) 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:

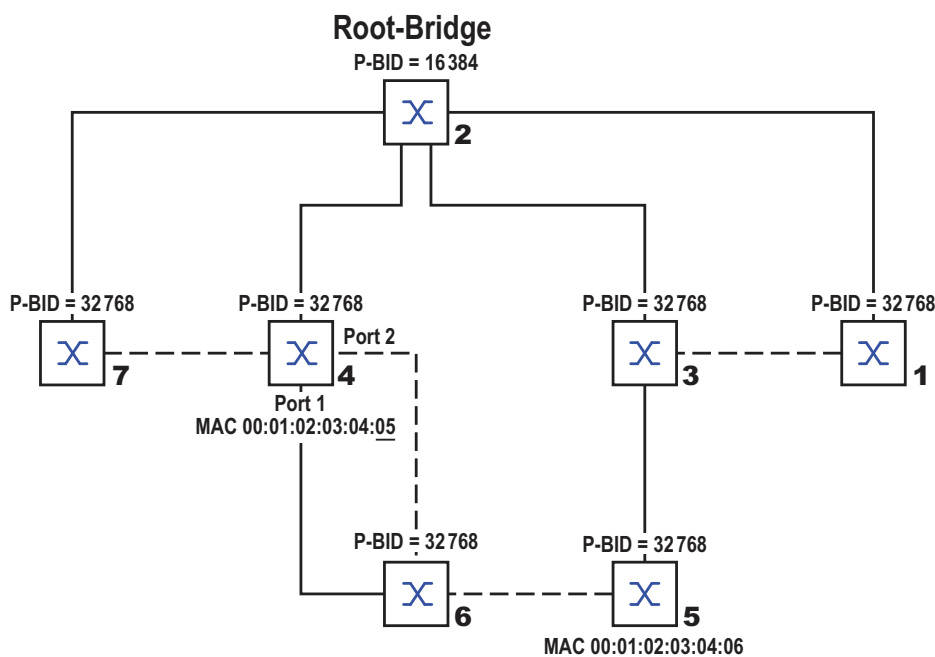
- ▶ Der Pfad über Bridge 5 und Bridge 3 verursacht die gleichen Root-Pfadkosten wie der Pfad über Bridge 4 und Bridge 2.
- ▶ STP wählt den Pfad über die Bridge, die in der Bridge-Identifikation die niedrigere MAC-Adresse hat (im Bild dargestellt Bridge 4).
- ▶ Zwischen Bridge 6 und Bridge 4 gibt es auch 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.



## 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 103 „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 49). Die Pfadkosten der meisten Bridges zur Root-Bridge sind kleiner geworden.



P-BID    Priorität der Bridge-Identifikation (BID)  
           = P-BID ohne MAC-Adresse

———— Root-Pfad

----- unterbrochener Pfad

Abb. 49: 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 50](#)):

- ▶ **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 46](#)).  
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<sup>1</sup>:  
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 geschichteten Netzes.



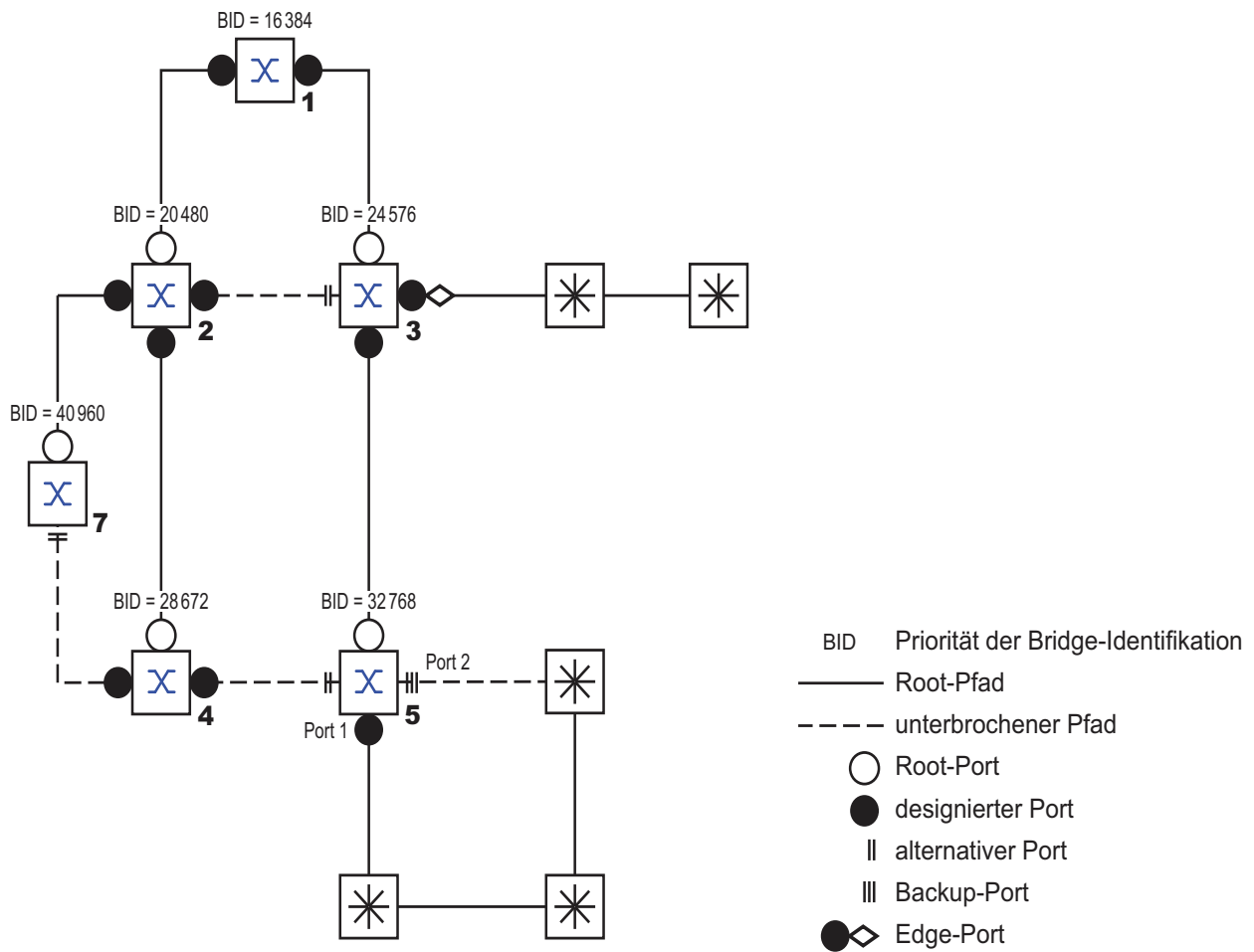


Abb. 50: Port-Rollen-Zuordnung

## 6.6.2 Port-Status

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 <sup>a</sup> | Excluded (Disabled)          |
| DISABLED        | Enabled                           | FALSE           | Discarding <sup>a</sup> | Excluded (Disabled)          |
| BLOCKING        | Enabled                           | TRUE            | Discarding <sup>b</sup> | Excluded (Alternate, Backup) |
| LISTENING       | Enabled                           | TRUE            | Discarding <sup>b</sup> | Included (Root, Designated)  |
| LEARNING        | Enabled                           | TRUE            | Learning                | Included (Root, Designated)  |
| FORWARDING      | Enabled                           | TRUE            | Forwarding              | Included (Root, Designated)  |

Tab. 14: 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-Status:

- ▶ Disabled: Port gehört nicht zur aktiven Topologie
- ▶ Discarding: kein Address 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 15](#)) ab, um sich zu vergewissern, dass keine BPDUsendende 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

The screenshot shows a configuration window for RSTP. At the top, there are two sections: 'Funktion' with radio buttons for 'An' (selected) and 'Aus', and 'Protokoll-Version' with a dropdown menu set to 'RSTP'. Below this is the 'Protokoll-Konfiguration / Information' section, which is divided into three columns: 'Bridge', 'Root', and 'Topologie'. The 'Bridge' column contains fields for Bridge-ID (32768 / 00 80 63 97 50 00), Priorität (32768), Hello Time [s] (2), Forward Delay [s] (15), Max Age (20), and Tx Hold Count (10). The 'Root' column contains fields for Root (20480 / 00 80 63 0f 1d b0), Root-Port (2), and Max Age (6). The 'Topologie' column contains a checkbox for 'Bridge ist Root' (checked), Root-Port (1.4), Root-Pfadkosten (440000), Anzahl Topologieänderungen (3), and Zeit seit letzter Änderung (0 Tag(e), 2:22:14). At the bottom of the window, there are three buttons: 'Schreiben', 'Laden', and 'Hilfe'.

Abb. 51: Funktion ein-/ausschalten

- Bestimmen Sie den gewünschten 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) eingeben können (siehe Tabelle 15). 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 15](#).

Abb. 52: 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.                                                                                                                                                                                                                                                                                 | $0 < n \cdot 4.096 (1000H) < 61.440 (F000H)$ | 32.768 (8000H) |
| Hello Time | Stellt die Hello-Time ein.<br>Die lokale Hello Time gibt die Zeit zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Pakete) in Sekunden an.<br>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. 15: Globale RSTP-Einstellungen

| Parameter     | Bedeutung                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  | Wertebereich                                                                  | Voreinstellung |
|---------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------|----------------|
| Forward Delay | <p>Stellt den Parameter Forward Delay ein.</p> <p>Beim Vorgängerprotokoll STP wurde der Parameter Forward Delay dazu verwendet, um den Zustandswechsel zwischen den Zuständen <code>disabled</code>, <code>discarding</code>, <code>learning</code>, <code>forwarding</code> zu verzögern. Seit der Einführung von RSTP hat dieser Parameter eine untergeordnete Bedeutung, weil die RSTP-Bridges den Zustandswechsel ohne vorgegebene Verzögerung aushandeln.</p> <p>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“.</p> | <p>4 - 30 s</p> <p>Beachten Sie den Hinweis, der auf diese Tabelle folgt.</p> | 15 s           |
| Max Age       | <p>Stellt den Parameter Max. Age ein.</p> <p>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“.</p>                                                                                                                                                                                              | <p>6 - 40 s</p> <p>Beachten Sie den Hinweis, der auf diese Tabelle folgt.</p> | 20 s           |

Tab. 15: Globale RSTP-Einstellungen



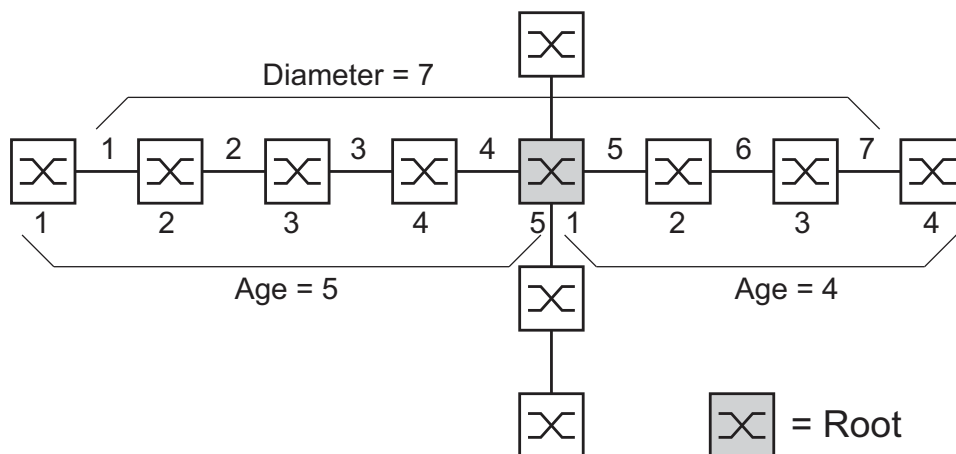


Abb. 53: Definition „Diameter“ und „Age“

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:

$$\text{Forward Delay} \geq (\text{Max Age}/2) + 1$$

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).

| Modul | Port | STP Status an                       | Port Status | Priorität | Port Pfadkosten | Soll Edge Port | Ist Edge Port | Auto Edge Port | Ist Punkt zu Punkt | Designierter Root (Priorität/MAC-Adresse) |
|-------|------|-------------------------------------|-------------|-----------|-----------------|----------------|---------------|----------------|--------------------|-------------------------------------------|
| 1     | 1    | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 2    | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 3    | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 4    | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 5    | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 6    | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 7    | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 8    | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 9    | <input checked="" type="checkbox"/> | manualFwd   | 128       | 0               | false          | false         | true           | true               | 80 00 00 80 63 74 67 c8                   |
| 1     | 10   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 11   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 12   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 13   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 14   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 15   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 16   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 17   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 18   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 19   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 20   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 21   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |
| 1     | 22   | <input checked="" type="checkbox"/> | disabled    | 128       | 0               | false          | false         | true           | false              | 80 00 00 80 63 74 67 c8                   |

Schreiben    Laden    Hilfe

Abb. 54: 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.                                                                                                                                                                 | An, Aus                                                                      | An             |
|                         | <p><b>Anmerkung:</b> 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.</p> |                                                                              |                |
| 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.                                                                                                                                                                                                      | $16 \leq n \cdot 16 \leq 240$                                                | 128            |

Tab. 16: 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. <code>forwarding</code> , <code>discarding</code> , <code>learning</code> .<br>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 <code>forwarding</code> geht. Diese Einstellung gilt für alle MSTIs. | aktiv (Kästchen markiert),<br>inaktiv (Kästchen leer) | inaktiv         |
| Oper-Edge-Port  | Das Gerät setzt den Zustand „Oper-Edge-Port“ (Operational: in Betrieb) auf <code>true</code> , wenn es keine STP-BPDUs empfangen hat, also ein Endgerät angeschlossen ist. Es setzt den Zustand auf <code>false</code> , wenn es eine STP-BPDUs empfangen hat, also eine Bridge angeschlossen ist.<br>Dieser Zustand gilt für alle MSTIs.                                                                                                                                                                                                                                                                                                                                                                                                                                            | <code>true</code> , <code>false</code>                | -               |

Tab. 16: 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 $1,5 \cdot \text{Hello Time}$ (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),<br>inaktiv (Kästchen leer)                                                                                        | aktiv          |
| Ist Punkt-zu-Punkt                | Das Gerät setzt den Zustand „Operational: in Betrieb“ auf <code>true</code> , wenn dieser Port eine Vollduplex-Verbindung zu einem STP-Gerät hat. Ansonsten setzt es den Zustand auf <code>false</code> (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 bewirkt eine kurze Rekonfigurationszeit. Dieser Zustand gilt für alle MSTIs. | <code>true, false</code><br><br>Das Gerät bestimmt diesen Zustand aus dem Duplex-Modus:<br>FDX: <code>true</code><br>HDX: <code>false</code> |                |
| Empfangene Bridge-ID (read-only)  | Zeigt die entfernte Bridge-ID an, von der dieser Port zuletzt eine STP-BPDU empfangen hat. <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                                          | Bridge-Identifikation (Format ppppp / mm 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. <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                              | 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. <sup>a</sup>                                                                                                                                                                                                                                                                                                                                                            | Port-Identifikation, Format pn nn, mit p: Port-Priorität / 16, nnn: Port-Nr., (beide hexadezimal)                                            | -              |

Tab. 16: Port-bezogene RSTP-Einstellungen und -Anzeigen

- <sup>a</sup> 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 53](#)) ist abhängig von  $\text{Max Age}$ . 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.

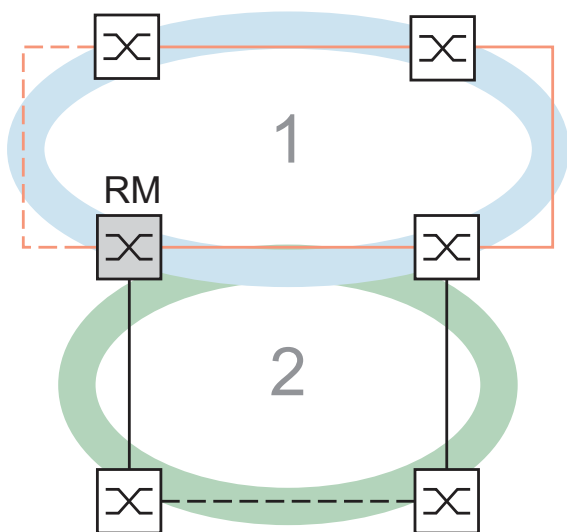


Abb. 55: Kombination von RSTP und MRP  
1: MRP-Ring  
2: RSTP-Ring  
RM: Ring-Manager

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 56](#)) zeigt ein Beispiel für die Kombination von RSTP und MRP.

| Parameter                                                  | S1    | S2  | S3     | S4     | S5     | S6     |
|------------------------------------------------------------|-------|-----|--------|--------|--------|--------|
| <b>MRP-Einstellungen</b>                                   |       |     |        |        |        |        |
| 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     |
| <b>RSTP-Einstellungen</b>                                  |       |     |        |        |        |        |
| 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. 17: 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.

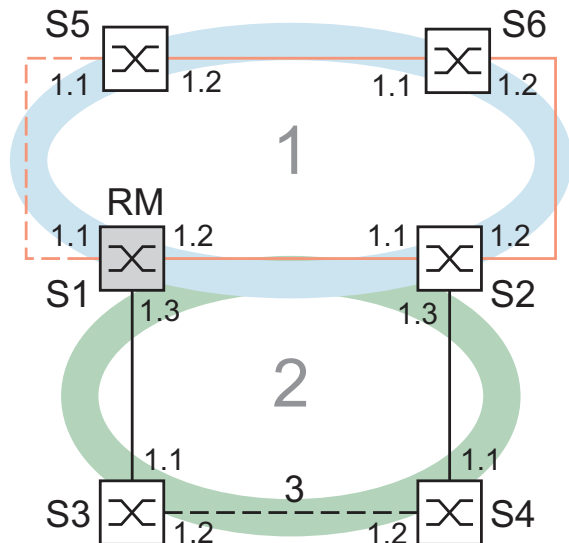


Abb. 56: Anwendungsbeispiel für die Kombination von RSTP und MRP  
 1: MRP-Ring, 2: RSTP-Ring, 3: redundante RSTP-Verbindung  
 RM: Ring-Manager  
 S2 ist RSTP-Root-Bridge  
 S1 ist RSTP-Ersatz-Root-Bridge

- Aktivieren Sie RSTP an den Ports, am Beispiel von S1 (siehe Tabelle 17).

```
enable
configure
interface 1/1

spanning-tree port mode
exit
interface 1/2

spanning-tree port mode
```

Wechsel in den Privileged-EXEC-Modus.  
 Wechsel in den Konfigurationsmodus.  
 Wechsel in den Interface-Konfigurationsmodus von Port 1/1.  
 RSTP am Port aktivieren.  
 Wechsel in den Konfigurationsmodus.  
 Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.  
 RSTP am Port aktivieren.

|                                    |                                                                 |
|------------------------------------|-----------------------------------------------------------------|
| <pre>exit</pre>                    | Wechsel in den Konfigurationsmodus.                             |
| <pre>interface 1/3</pre>           | Wechsel in den Interface-Konfigurationsmodus von Interface 1/3. |
| <pre>spanning-tree port mode</pre> | RSTP am Port aktivieren.                                        |
| <pre>exit</pre>                    | Wechsel in den Konfigurationsmodus.                             |

- Konfigurieren Sie die globalen Einstellungen, am Beispiel von S1:
  - die RSTP-Priorität
  - die globale Funktion
  - den MRP-Kompatibilitätsmodus

|                                                  |                                                                                                                |
|--------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| <pre>spanning-tree mst priority 0<br/>4096</pre> | Die RSTP-Priorität für MST-Instanz 0 auf den Wert 4.096 einstellen. Die MST-Instanz 0 ist die Default-Instanz. |
| <pre>spanning-tree</pre>                         | RSTP-Funktion global einschalten.                                                                              |
| <pre>spanning-tree stp-mrp-mode</pre>            | MRP-Kompatibilität einschalten.                                                                                |

- Konfigurieren Sie die anderen Switches S2 - S6 mit ihren jeweiligen Werten ([siehe Tabelle 17](#)).
- Schließen Sie die redundante RSTP-Verbindung an.

# 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 | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Lesbarkeit          | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Verständlichkeit    | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Beispiele           | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Aufbau              | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Vollständigkeit     | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Grafiken            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Zeichnungen         | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |
| Tabellen            | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> | <input type="radio"/> |

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

|                                        |                |                                |                |
|----------------------------------------|----------------|--------------------------------|----------------|
| <b>A</b>                               |                | <b>N</b>                       |                |
| Advanced Mode                          | 36             | Netzlast                       | 93, 95         |
| Age                                    | 118            | <b>P</b>                       |                |
| Alternate-Port                         | 109            | Pfadkosten                     | 97, 100        |
| <b>B</b>                               |                | Portnummer                     | 99             |
| Backup-Port                            | 109            | Port-Identifikation            | 96, 99         |
| Baumstruktur (Spanning Tree)           | 100, 107       | Port-Priorität (Spanning Tree) | 99             |
| BPDU                                   | 100            | Port-Rollen (RSTP)             | 108            |
| Bridge Identifier                      | 96             | Port-Status                    | 111            |
| Bridge Protocol Data Unit              | 100            | PROFINET IO                    | 7              |
| <b>D</b>                               |                | <b>R</b>                       |                |
| Deaktivierter Port (Spanning Tree)     | 109            | Rapid Spanning Tree            | 11, 108        |
| Designated Bridge                      | 108            | Redundanz                      | 7, 93          |
| Designated Port                        | 109, 109       | Redundanzfunktionen            | 11             |
| DIP-Schalter                           | 31             | Redundanzmanager               | 29             |
| Diameter                               | 118            | Redundanz vorhanden            | 35, 39, 45     |
| Disabled-Port                          | 109            | Rekonfiguration                | 95             |
| <b>E</b>                               |                | Ring                           | 27             |
| Edge-Port                              | 109            | Ringstruktur                   | 28             |
| Ersatzport                             | 109            | Ring-Manager                   | 27, 29         |
| <b>F</b>                               |                | Ring-Redundanz                 | 12, 12, 12     |
| FAQ                                    | 133            | Ring-/Netzkopplung             | 11             |
| Fast HIPER-Ring (Port-VLAN-ID)         | 11             | RM-Funktion                    | 27             |
| Forward Delay                          | 117            | Root Bridge                    | 100            |
| <b>H</b>                               |                | Root-Pfad                      | 103, 105       |
| Hello Time                             | 116            | Root-Pfadkosten                | 96             |
| HIPER Ring konfigurieren               | 43             | Root-Port                      | 108            |
| HIPER-Ring                             | 11, 14, 24     | RSTP                           | 11             |
| HIPER-Ring konfigurieren               | 31             | RST BPDU                       | 109, 112       |
| <b>I</b>                               |                | <b>S</b>                       |                |
| Industrial HiVision                    | 8              | Schleifen                      | 77, 79, 87, 88 |
| Industrieprotokolle                    | 7              | Schulungsangebote              | 133            |
| <b>K</b>                               |                | STP-BPDU                       | 100            |
| Konfigurationsfehler                   | 35, 39, 45     | Sub-Ring                       | 11, 48         |
| <b>L</b>                               |                | Symbol                         | 9              |
| LACP Link Aggregation Control Protocol | 17             | <b>T</b>                       |                |
| Link Aggregation                       | 11, 14, 24     | Technische Fragen              | 133            |
| Loops                                  | 77, 79, 87, 88 | Trunk                          | 17             |
| <b>M</b>                               |                | <b>V</b>                       |                |
| Max Age                                | 117            | VLAN (HIPER-Ring)              | 34             |
| MRP-Ring                               | 11, 14, 23     |                                |                |



## 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](mailto:hac.support@belden.com)

in der Region Amerika unter

- ▶ Tel.: +1 (717) 217-2270
- ▶ E-Mail: [inet-support.us@belden.com](mailto:inet-support.us@belden.com)

in der Region Asien-Pazifik unter

- ▶ Tel.: +65 6854 9860
- ▶ E-Mail: [inet-ap@belden.com](mailto: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