



HIRSCHMANN

A **BELDEN** BRAND

Referenz-Handbuch

Web-based Interface

Industrial ETHERNET Switch

RSB20, OCTOPUS OS20/OS24 Managed

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.

© 2012 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.

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).

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

Inhalt

Über dieses Handbuch	7
Legende	9
Öffnen des Web-based Interface	11
1 Grundeinstellungen	17
1.1 System	18
1.2 Netz	22
1.3 Software	25
1.3.1 Anzeige der im Gerät vorhandenen Software-Versionen	26
1.3.2 tftp-Software-Update	26
1.3.3 http-Software-Update	27
1.4 Portkonfiguration	28
1.5 Power over ETHERNET	31
1.6 Konfiguration laden/speichern	33
1.6.1 Konfiguration laden	34
1.6.2 Konfiguration speichern	34
1.6.3 URL	35
1.6.4 Konfiguration löschen	35
1.6.5 AutoConfiguration Adapter (ACA) verwenden	36
1.7 Neustart	38
2 Sicherheit	41
2.1 Passwort / SNMPv3-Zugriff	42
2.2 SNMPv1/v2-Zugriffs-Einstellungen	45
2.3 Web-Zugriff	48
2.3.1 Beschreibung Web-Zugriff (http)	48
3 Zeit	51
3.1 SNTP-Konfiguration	53
3.2 PTP (IEEE 1588)	57

4	Switching	59
4.1	Switching Global	60
4.2	Filter für MAC-Adressen	61
4.3	Multicasts	63
4.3.1	Globale Einstellung	64
4.3.2	IGMP-Querier- und IGMP-Einstellungen	64
4.3.3	Multicasts	66
4.3.4	Einstellungen pro Port (Tabelle)	69
5	QoS/Priorität	71
5.1	Global	72
5.2	Portkonfiguration	75
5.2.1	Port-Priorität eingeben	76
5.3	802.1D/p-Mapping	77
5.4	IP-DSCP-Mapping	80
6	Redundanz	83
6.1	Ring-Redundanz	84
6.1.1	HIPER-Ring konfigurieren	86
6.1.2	MRP-Ring konfigurieren	90
6.2	Rapid Spanning Tree	93
6.2.1	Global	95
6.2.2	Rapid-Spanning-Tree-Port	100
7	Diagnose	103
7.1	Ereignis-Log	104
7.2	Ports	105
7.2.1	Statistiktable	105
7.2.2	Auslastung (Netzlant)	106
7.2.3	SFP-Module	108
7.3	Topologie-Erkennung	110
7.4	Port-Mirroring	111
7.5	Gerätstatus	113
7.6	Meldekontakt	116
7.6.1	Manuelle Einstellung	116
7.6.2	Funktionsüberwachung	117

7.6.3	Gerätstatus	118
7.6.4	Trapeinstellung	119
7.7	Alarmer (Traps)	120
7.8	Bericht	122
7.9	Selbsttest	123
8	Erweitert	125
8.1	DHCP-Relay-Agent	126
8.2	Command Line Interface	128
A	Anhang	129
A.1	Technische Daten	130
A.2	Liste der RFCs	131
A.3	Zugrundeliegende IEEE-Normen	133
A.4	Zugrundeliegende IEC-Normen	134
A.5	Copyright integrierter Software	135
A.5.1	Bouncy Castle Crypto APIs (Java)	135
A.5.2	Broadcom Corporation	136
B	Leserkritik	137
C	Stichwortverzeichnis	139
D	Weitere Unterstützung	141

Über dieses Handbuch

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

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.

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

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

Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
□	Arbeitsschritt
■	Zwischenüberschrift
Link	Querverweis mit Verknüpfung
Hinweis:	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

Öffnen des Web-based Interface

Zum Öffnen des Web-based Interface benötigen Sie einen Web Browser (Programm, das das Lesen von Hypertext ermöglicht), zum Beispiel den Mozilla Firefox ab der Version 2 oder den Microsoft Internet Explorer ab der Version 6.

Hinweis: Das Web-based Interface verwendet die Java-Software 6 ("Java™ Runtime Environment Version 1.6.x").

Installieren Sie die Software von der beiliegenden CD-ROM. Hierzu wählen Sie unter „Zusatzsoftware“ `Java Runtime Environment` und klicken auf „Installation“.



Abb. 1: Java installieren

- Starten Sie Ihren Web-Browser.
- Stellen Sie sicher, dass Java in den Sicherheitseinstellungen Ihres Web-Browsers eingeschaltet ist.
- Zur Herstellung der Verbindung geben Sie im Adressfeld des Web-Browsers die IP-Adresse des Gerätes, das Sie mit dem Web-based Management administrieren möchten, in der folgenden Form ein:

`http://xxx.xxx.xxx.xxx`

Auf dem Bildschirm erscheint das Login-Fenster.

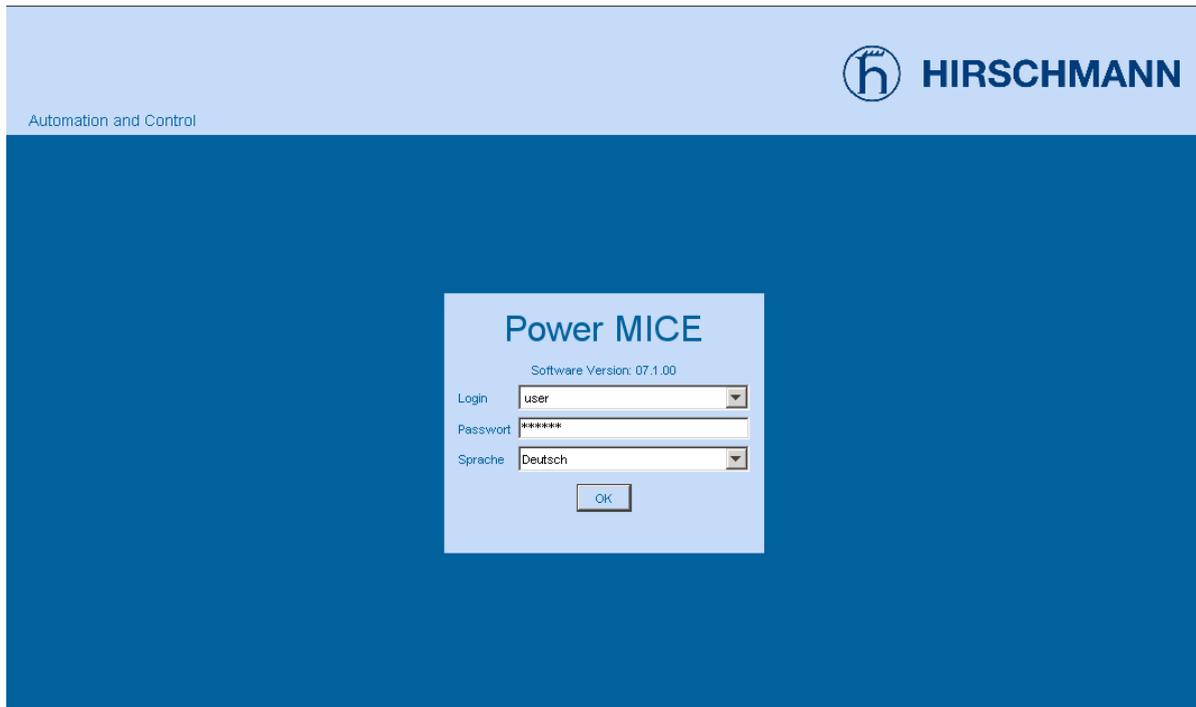


Abb. 2: Login-Fenster

- Wählen Sie die gewünschte Sprache aus.
- Wählen Sie im Login-Ausklappmenü
 - user, um mit Leserecht oder
 - admin, um mit Schreib- und Leserecht auf das Gerät zuzugreifen.
- Im Passwort-Feld ist das Passwort "public", mit dem Sie über Leserechte verfügen, vorgegeben. Wollen Sie mit Schreibrechten auf das Gerät zugreifen, dann markieren Sie den Inhalt des Passwortfeldes und überschreiben ihn mit dem Passwort "private" (Lieferzustand).
- Klicken Sie auf OK.

Am Bildschirm erscheint die Benutzeroberfläche (Web-based Interface) des Gerätes.

Hinweis: Änderungen, die Sie an den Dialogen vornehmen, übernimmt das Gerät in den flüchtigen Speicher (RAM), wenn Sie auf „Schreiben“ klicken. Klicken Sie auf „Laden“, um die Anzeige zu aktualisieren.

Um jegliche durchgeführten Änderungen so zu speichern, dass sie nach einem Wiedereinschalten oder Neustart des Gerätes erhalten bleiben, benutzen Sie „Sichern“ im Dialog „Laden/Speichern“ (siehe auf Seite 34 „Konfiguration speichern“).

Hinweis: Wenn Sie eine fehlerhafte Konfiguration eingeben, können Sie sich den Zugang zum Gerät versperren.

Die eingeschaltete Funktion „Konfigurationsänderung widerrufen“ im „Laden/Speichern“-Dialog ermöglicht Ihnen, nach Ablauf einer einstellbaren Zeitspanne automatisch wieder zur letzten Konfiguration zurückzukehren. Damit haben Sie wieder Zugriff auf das Gerät.

Am Bildschirm erscheint die Benutzeroberfläche (Web-based Interface) des Gerätes.

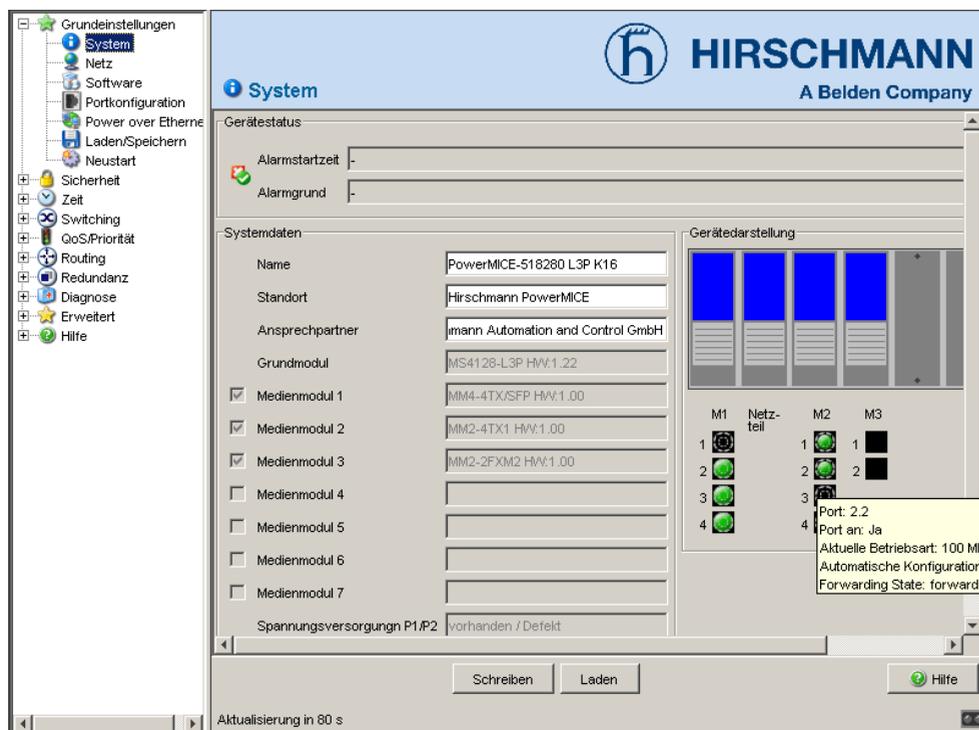


Abb. 3: Benutzeroberfläche (Web-based Interface) des Gerätes mit Sprechblanchenhilfe

Der Menüteil zeigt die Menüpunkte. Durch Platzieren des Mauszeigers im Menüteil und Drücken der rechten Maustaste können Sie mit „Zurück“ auf einen beliebigen, bereits schon vorher ausgewählten Menüpunkt zurückspringen und mit „Vor“ wieder auf einen beliebigen bereits schon vorher ausgewählten Menüpunkt vorspringen.



1 Grundeinstellungen

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

- ▶ System
- ▶ Netz
- ▶ Software
- ▶ Portkonfiguration
- ▶ Power over Ethernet (PoE)
- ▶ Laden/Speichern
- ▶ Neustart

1.1 System

Das Untermenü „System“ im Grundeinstellungsmenü ist untergliedert in:

- ▶ Gerätestatus
- ▶ Systemdaten
- ▶ Gerätedarstellung
- ▶ Aktualisierung

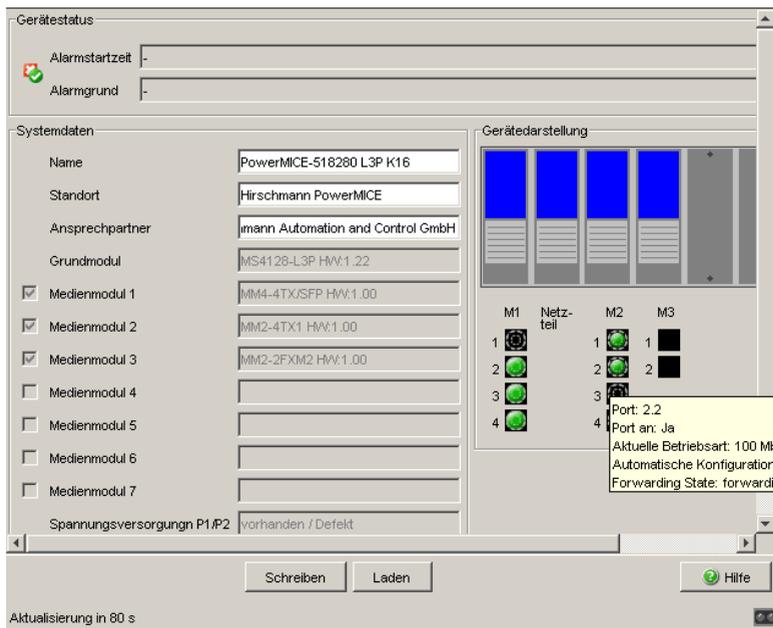


Abb. 4: Untermenü „System“

■ Gerätestatus

Dieser Bereich der Benutzeroberfläche (Web-based Interface) gibt Auskunft über den Gerätestatus und Alarmzustand des Gerätes.

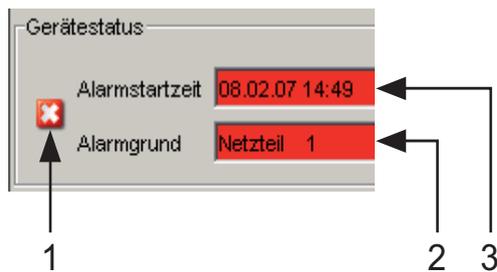


Abb. 5: Gerätestatus- und Alarm-Anzeige
 1 - Das Symbol zeigt den Gerätestatus an
 2 - Ursache des ältesten, bestehenden Alarms
 3 - Beginn des ältesten, bestehenden Alarms

■ Systemdaten

Dieser Bereich der grafischen Benutzeroberfläche zeigt die Systemparameter des Gerätes an. In den weiß unterlegten Feldern haben Sie die Möglichkeit, die Einstellungen zu ändern.

- den Systemnamen,
- die Standortbezeichnung,
- den Namen des Ansprechpartners für dieses Gerät

Bezeichnung	Bedeutung
Name	Systemname dieses Gerätes
Standort	Standort dieses Gerätes
Ansprechpartner	Ansprechpartner für dieses Gerät
Grundmodul	Hardware-Version des Geräts
Spannungsversorgung (P1/P2)	Status der Netzteile (P1/P2)
Betriebszeit	Zeigt die Zeit, die seit dem letzten Neustart dieses Gerätes vergangen ist.

Tab. 1: 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.

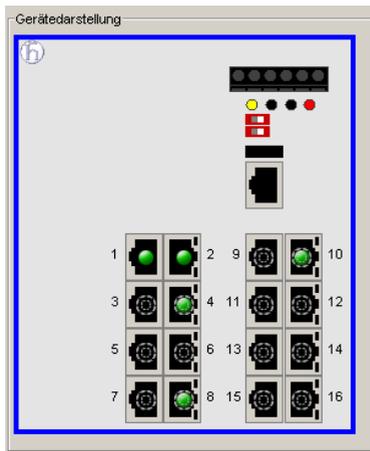


Abb. 6: Gerätedarstellung

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

Dieser Bereich der grafischen Benutzeroberfläche links unten zeigt an, nach welcher Zeit das Applet die aktuellen Daten dieses Dialogs wieder abrufen. Das Klicken auf die „Laden“-Taste bewirkt ein sofortiges Abrufen der aktuellen Daten des Dialogs. Das Applet ruft automatisch alle 100 Sekunden die aktuellen Daten des Gerätes ab.

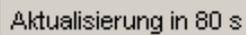
A screenshot of a user interface element, likely a status bar or a notification box, showing the text "Aktualisierung in 80 s" (Update in 80 s) in a grey rectangular box.

Abb. 7: Zeit bis zur Aktualisierung

1.2 Netz

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

The screenshot shows a configuration dialog box for network parameters. On the left, under the heading 'Modus', there are three radio buttons: 'BOOTP', 'DHCP', and 'Lokal'. The 'Lokal' radio button is selected. To the right of the 'Modus' section, there are several input fields: 'MAC-Adresse' (00:80:63:4A:A7:B3), 'Name' (RS-4AA7B3), 'IP-Adresse' (10.0.1.10), 'Netzmaske' (255.255.255.0), and 'Gateway-Adresse' (0.0.0.0). Below these fields is a section for 'HiDiscovery Protokoll' with radio buttons for 'Funktion' (selected), 'An', and 'Aus', and a dropdown menu for 'Zugriff' set to 'read-write'. At the bottom of the dialog, there are buttons for 'Schreiben', 'Laden', and 'Hilfe'.

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 33 „Konfiguration 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 33 „Konfiguration 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 im System-Dialog des Web-based Interface in der Zeile „Name“ ein.

- Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät an Hand seiner MAC-Adresse 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“).

Hinweis: 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.

1.3 Software

Der Dialog Software bietet Ihnen die Möglichkeit, die im Gerät vorhandenen Software-Versionen anzuzeigen und ein Software-Update des Gerätes via Datei-Auswahl durchzuführen.

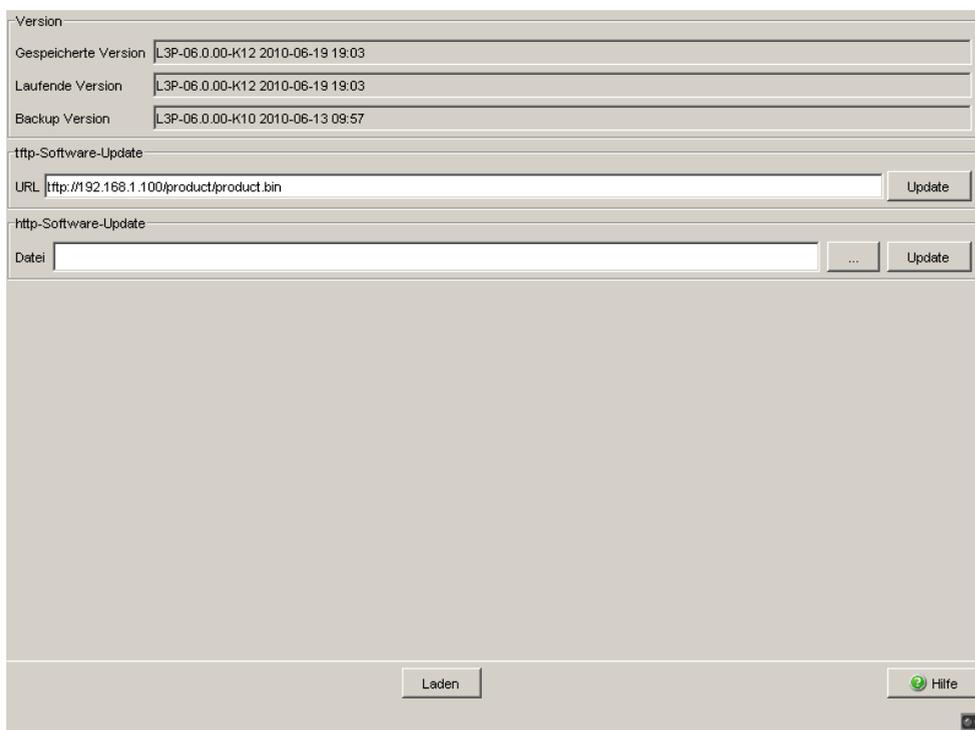


Abb. 9: Dialog Software

1.3.1 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.

1.3.2 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).

Mit "tftp-Update" lädt das Gerät die Software vom tftp-Server.

Um die neue Software nach dem Laden zu starten, führen Sie einen Kaltstart des Gerätes durch ([siehe auf Seite 38 „Neustart“](#)).

1.3.3 http-Software-Update

Für ein http-Software-Update (über ein Datei-Auswahl-Fenster), kopieren Sie die Geräte-Software auf einem Datenträger, den Sie von Ihrer Workstation aus erreichen.

- 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 abgeschlossen.
 - ▶ Update abgebrochen, Ursache: Falsche Datei.
 - ▶ Update abgebrochen, Ursache: Abspeichern erfolglos.
 - ▶ Datei nicht gefunden (Ursache: Dateiname nicht gefunden oder nicht vorhanden).
 - ▶ Einen unterbrochenen Link (Ursache: Pfad ohne Dateiname).
- Nach erfolgreichem Update aktivieren Sie die neue Software:
Wählen Sie den Dialog `Grundeinstellungen: Neustart` und führen Sie einen Kaltstart durch.
Bei einem Kaltstart lädt das Gerät die Software neu aus dem nichtflüchtigen Speicher, startet neu und führt einen Selbsttest durch.
 - Klicken Sie in Ihrem Browser auf „Neu laden“, um nach dem Booten des Gerätes wieder auf das Gerät zugreifen zu können.

1.4 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).

- ▶ In der Spalte „Name“ haben Sie die Möglichkeit, für jeden Port einen beliebigen Namen aus bis zu 20 Zeichen 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 Gerätzustand 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 vertauscht das Sende- und Empfangs-Leitungspaar des TP-Kabels für diesen Port (MDIX).
 - disable: Das Gerät vertauscht das Sende- und Empfangs-Leitungspaar des TP-Kabels für diesen Port nicht (MDI).
 - nicht unterstützt: Der Port unterstützt diese Funktion nicht (optischer Port).

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

Hinweis: 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	100 Mbit/s Vollduplex (FDX)
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)

Tab. 2: 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.

Port	Name	Port an	Verbindungsfehler weitermelden	Automatische Konfiguration	Manuelle Konfiguration	Link/ Aktuelle Betriebsart	Manuelles Cable-Crossing (Auto. Konfig. aus)	Flussskontrolle
1.1		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000 Mbit/s FDX	-	disable	<input checked="" type="checkbox"/>
1.2		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000 Mbit/s FDX	1000 Mbit/s FDX	disable	<input checked="" type="checkbox"/>
1.3		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000 Mbit/s FDX	1000 Mbit/s FDX	disable	<input checked="" type="checkbox"/>
1.4		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	1000 Mbit/s FDX	1000 Mbit/s FDX	disable	<input checked="" type="checkbox"/>
2.1		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	100 Mbit/s FDX	disable	<input checked="" type="checkbox"/>
2.2		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	100 Mbit/s FDX	disable	<input checked="" type="checkbox"/>
2.3		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	-	disable	<input checked="" type="checkbox"/>
2.4		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	100 Mbit/s FDX	100 Mbit/s FDX	disable	<input checked="" type="checkbox"/>
3.1		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>
3.2		<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	100 Mbit/s FDX	-	unsupported	<input checked="" type="checkbox"/>

Schreiben Laden Hilfe

Abb. 10: Dialog Portkonfigurations-Tabelle

1.5 Power over ETHERNET

Für die Geräte

- ▶ OS24-080900T5T5TFFBHH
- ▶ OS24-080900T5T5TNEBHH

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.

Das Gerät bietet eine nominale Leistung von 61,6 W für die Summe aller PoE-Ports. Benötigen die angeschlossenen Geräte mehr PoE-Leistung als die angebotene PoE-Leistung, dann schaltet das Gerät PoE an den Ports aus. Das Gerät schaltet PoE zuerst an den Ports mit der höheren Portnummer aus.

- Mit „Funktion An/Aus“ schalten Sie PoE ein/aus.
- „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.
- In „Threshold“ (Leistungsschwelle) geben Sie die Leistungsschwelle an, bei deren Überschreiten/Unterschreiten das Gerät ein Trap sendet, sofern „Verschicke Trap“ eingeschaltet ist. Die Leistungsschwelle geben Sie in Prozent der abgegebenen Leistung zur nominalen Leistung ein.
- "Nominale Leistung" zeigt die Leistung an, die das Gerät nominal für alle PoE-Ports zusammen zur Verfügung stellt.
- „Reservierte Leistung“ zeigt an, wieviel Leistung das Gerät allen angeschlossenen PoE-Geräten zusammen auf Grund ihrer Klassifizierung maximal zur Verfügung stellt.
- "Abgegebene Leistung" zeigt an, wie groß der momentane Leistungsbedarf an allen PoE-Ports ist.

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

- 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.

- Die Spalte "Class" 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
- 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.

Funktion An Aus

Verschicke Trap Ja Nein

Threshold [%]

Nominale Leistung [W]

Reservierte Leistung [W]

Abgegebene Leistung [W]

Modul	Port	POE an	Status	Class	Verbrauch [W]	Name
1	1	<input checked="" type="checkbox"/>	disabled	-	0,0	
1	2	<input checked="" type="checkbox"/>	searching	-	0,0	
1	3	<input checked="" type="checkbox"/>	searching	-	0,0	
1	4	<input checked="" type="checkbox"/>	searching	-	0,0	
1	5	<input checked="" type="checkbox"/>	searching	-	0,0	
1	6	<input checked="" type="checkbox"/>	searching	-	0,0	
1	7	<input checked="" type="checkbox"/>	searching	-	0,0	
1	8	<input checked="" type="checkbox"/>	searching	-	0,0	
1	9	<input checked="" type="checkbox"/>	searching	-	0,0	

Abb. 11: Dialog Power over Ethernet

1.6 Konfiguration laden/ speichern

Dieser Dialog bietet Ihnen die Möglichkeit,

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

The dialog box contains the following elements:

- Laden:** Radio buttons for 'vom Gerät', 'vom URL', 'vom URL & auf dem Gerät speichern', and 'via PC'. A 'Wiederherstellen' button is located to the right.
- Speichern:** Radio buttons for 'auf dem Gerät', 'auf URL (binär)', and 'auf dem PC (binär)'. A 'Sichern' button is located to the right.
- URL:** A text input field containing 'http://192.168.1.100/product/product.cfg'.
- Löschen:** Radio buttons for 'aktuelle Konfiguration' and 'aktuelle Konfiguration und vom Gerät'. A 'Konfiguration löschen' button is located to the right.
- AutoConfiguration Adapter:** A dropdown menu labeled 'Status' with the value 'notPresent'.
- Bottom:** Buttons for 'Schreiben', 'Laden', and 'Hilfe'.

Abb. 12: Dialog Laden/Speichern

1.6.1 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 im Binärformat gespeicherte Konfiguration zu laden.

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

1.6.2 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 zu speichern,
- ▶ die aktuelle Konfiguration im Binärformat auf dem PC zu speichern.

Hinweis: Den von DHCP/BOOTP (siehe „[Netz](#)“ auf [Seite 22](#)) 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 das Web-based Interface das „Laden/Speichern“-Symbol im Navigationsbaum von einem Diskettensymbol in ein gelbes Dreieck. Nach dem Speichern der Konfiguration zeigt das Web-based Interface das „Laden/Speichern“-Symbol wieder als Diskette an.

1.6.3 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`).

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

1.6.4 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. Dabei löscht das Gerät seine Konfiguration sowohl im flüchtigen als auch im nichtflüchtigen Speicher. Dies schließt die IP-Adresse ein. Das Gerät ist wieder über das Netz erreichbar, sobald es eine neue IP-Adresse erhalten hat, z.B. über DHCP oder die V.24-Schnittstelle.

1.6.5 AutoConfiguration Adapter (ACA) verwenden

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

Hinweis: Die beschriebenen Geräte verwenden den folgenden AutoConfiguration Adapter: ACA 11.

■ **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.

You have the option of transferring the current device configuration, including the SNMP password, to the ACA and the flash memory by using the "to device" option in the "Save" frame .

■ **Konfigurationsdaten vom ACA übernehmen:**

Bei einem Neustart mit angeschlossenem ACA übernimmt das Gerät die Konfigurationsdaten des ACA und speichert sie nicht-flüchtig im Flash-Speicher. Enthält der angeschlossene ACA keine gültigen Daten, z.B. wenn er im Lieferzustand ist, dann lädt das Gerät die Daten aus dem Flash-Speicher.

Hinweis: 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 ACA stammen von einem anderen Gerätetyp und können nicht gelesen oder konvertiert werden.
checksumErr	Die Konfigurationsdaten sind beschädigt.

Tab. 3: 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.

1.7 Neustart

Dieser Dialog bietet Ihnen folgende Funktionen:

- ▶ einen Kaltstart des Gerätes auslösen. Hierbei lädt das Gerät die Software neu aus dem nichtflüchtigen Speicher, startet neu und führt einen Selbsttest durch.
Laden Sie die Webseite in Ihrem Browser neu, um nach dem Neustart wieder auf das Gerät zuzugreifen.
- ▶ einen Warmstart des Gerätes auslösen. Hierbei prüft das Gerät die Software im flüchtigen Speicher und startet neu. Ist ein Warmstart nicht möglich, führt das Gerät automatisch einen Kaltstart aus.
- ▶ 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 Port-Zähler zurücksetzen,
- ▶ die Log-Datei löschen.

Hinweis: Während des Neustarts überträgt das Gerät kurzfristig keine Daten und ist nicht durch das Web-based-Interface oder andere Managementsysteme wie z.B. Industrial HiVision erreichbar.



Abb. 13: Dialog Neustart

2 Sicherheit

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

- ▶ Passwort/SNMPv3-Zugriff
- ▶ SNMPv1/v2-Zugriff
- ▶ Web-Zugriff

2.1 Passwort / SNMPv3-Zugriff

Dieser Dialog bietet Ihnen die Möglichkeit, das Lese- und das Schreib/Lese-Passwort für den Zugriff mit dem Web-based Interface, über das CLI und per SNMPv3 (SNMP-Version 3) auf dem Gerät zu ändern.

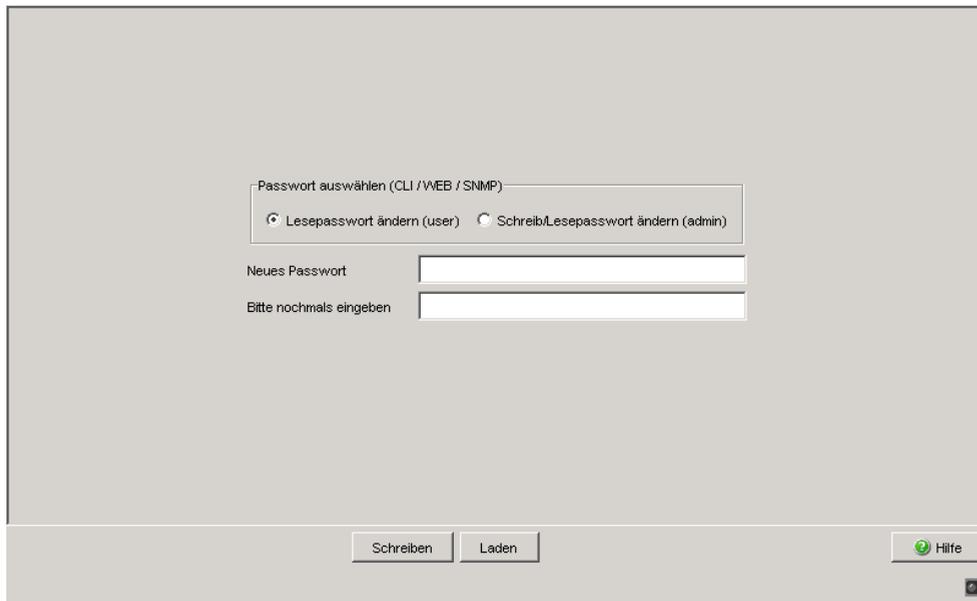
Stellen Sie für das Lese Passwort und das Schreib-/Lese Passwort unterschiedliche Passwörter ein, damit ein Benutzer, der nur Lesezugriff hat (Benutzername „user“), das Passwort für den Schreib-/Lesezugriff (Benutzername „admin“) nicht kennen oder erraten kann.

Wenn Sie identische Passwörter setzen, meldet das Gerät beim Versuch, diese Daten zu schreiben, einen allgemeinen Fehler.

Das Web-based Interface und das User Interface (CLI) verwenden für die Benutzer „admin“ und „user“ die selben Passwörter wie SNMPv3.

Hinweis: 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.



Passwort auswählen (CLI / WEB / SNMP)

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

Neues Passwort

Bitte nochmals eingeben

Schreiben Laden Hilfe

Abb. 14: Dialog Passwort/SNMP-Zugriff

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

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

Hinweis: 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.

Hinweis: 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 nehmen Sie in einem eigenen Dialog vor ([siehe auf Seite 48 „Web-Zugriff“](#)).

Den Zugriff auf IP-Adressebene können Sie in einem eigenen Dialog beschränken ([siehe auf Seite 45 „SNMPv1/v2-Zugriffs-Einstellungen“](#)).

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 HiVision verwalten und mit früheren Versionen von SNMP kommunizieren.

Hinweis: Damit Sie die Daten dieses Dialogs lesen und/oder ändern können, melden Sie sich im Web-based Interface mit dem Benutzernamen „admin“ und dem dazu passenden Passwort an.

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

Hinweis: Passwörter unterscheiden Groß- und Kleinschreibung.

- ▶ 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.

Hinweis: 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 ([siehe auf Seite 42 „Passwort / SNMPv3-Zugriff“](#)). So erreichen Sie, dass Sie auch per SNMPv3 mit dem selben Passwort zugreifen können.

- ▶ In der Spalte "Aktiv" aktivieren/deaktivieren Sie diesen Tabelleneintrag.

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

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

Hinweis: Das Gerät verhindert das Löschen oder Ändern der Zeile mit dem aktuell benutzten Passwort.

SNMPv1 ein

SNMPv2 ein

Index	Passwort	IP-Adresse	IP-Maske	Zugriffsrecht	Aktiv
0	public	0.0.0.0	0.0.0.0	readOnly	<input checked="" type="checkbox"/>
1	private	0.0.0.0	0.0.0.0	readWrite	<input checked="" type="checkbox"/>

Schreiben Laden Eintrag erzeugen Eintrag löschen Hilfe

Abb. 15: Dialog SNMPv1/v2-Zugriff

2.3 Web-Zugriff

Dieser Dialog bietet Ihnen die Möglichkeit, den Web-Server auf dem Gerät abzuschalten.

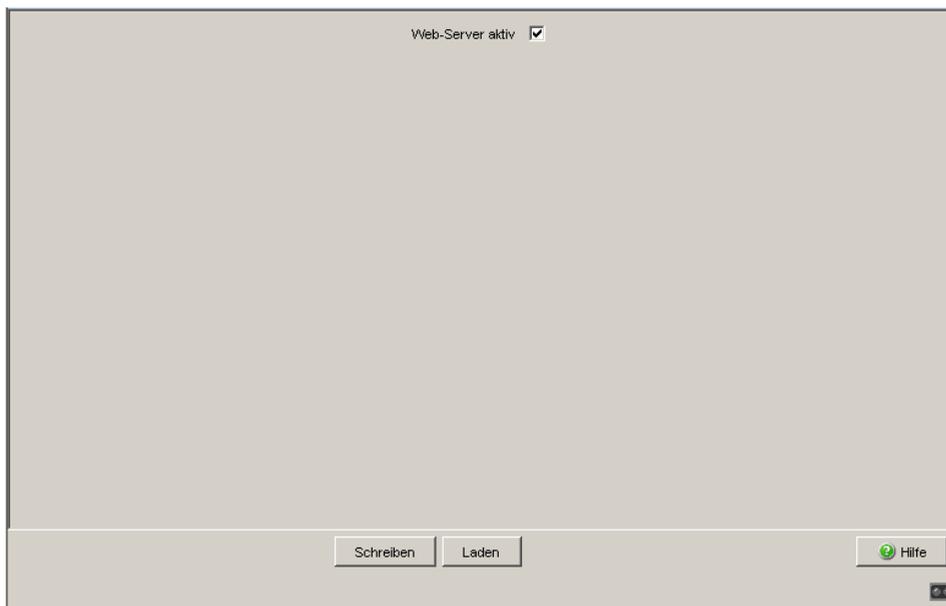


Abb. 16: Dialog Web-Zugriff

2.3.1 Beschreibung Web-Zugriff (http)

Der Web-Server des Gerätes bietet Ihnen die Möglichkeit, das Gerät mit Hilfe des Web-based Interfaces 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 Web-Servers ist ein erneutes Anmelden über einen Web-Browser nicht mehr möglich. Die Anmeldung im offenen Browserfenster bleibt aktiv.

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

3 Zeit

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.

Hinweis: 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.

Konfiguration	
Systemzeit (UTC)	02.01.2011 18:58:14
Systemzeit	02.01.2011 19:58:11
Quelle der Zeit	local
Lokaler Offset [min]	60

Schreiben Laden Hilfe

Abb. 17: Dialog Zeit, Grundeinstellungen

3.1 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.

Hinweis: 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
Funktion	Ein-/Ausschalten der SNTP-Funktion In diesem Rahmen schalten Sie die SNTP-Funktion ein/aus. Im ausgeschalteten Zustand sendet der SNTP-Server keine SNTP-Pakete und beantwortet keine SNTP-Anfragen. Der SNTP-Client sendet keine SNTP-Anforderungen und wertet keine SNTP-Broadcast-/Multicast-Pakete aus.

Tab. 4: Konfiguration SNTP Client und Server

Parameter	Bedeutung	Wertebereich	Voreinstellung
SNTP-Status	Anzeige von Zuständen, wie z.B. „Server nicht erreichbar“.	-	-

Tab. 5: SNTP-Status

Parameter	Bedeutung	Wertebereich	Voreinstellung
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 Tab. 7).	Gültige IPv4-Adresse	0.0.0.0
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. 6: Konfiguration SNTP-Server

IP-Zieladresse	Zyklisch SNTP-Paket versenden an
0.0.0.0	niemanden
Unicast	Unicast
224.0.1.1	Multicast
255.255.255.255	Broadcast

Tab. 7: Zyklisches Versenden von SNTP-Paketen

Parameter	Bedeutung	Wertebereich	Voreinstellung
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. 8: Konfiguration SNTP-Client

Hinweis: 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.

Hinweis: 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.

Funktion <input type="radio"/> An <input checked="" type="radio"/> Aus		SNTP Status <input type="text"/>	
Konfiguration SNTP Client Client Status <input checked="" type="radio"/> An <input type="radio"/> Aus		Konfiguration SNTP Server Server Status <input checked="" type="radio"/> An <input type="radio"/> Aus	
Externe Server-Adresse	<input type="text" value="0.0.0.0"/>	Anycast Zieladresse	<input type="text" value="0.0.0.0"/>
Redundante Server-Adresse	<input type="text" value="0.0.0.0"/>	VLAN ID	<input type="text" value="1"/>
Server Anforderungsintervall [s]	<input type="text" value="30"/>	Anycast Sendeintervall [s]	<input type="text" value="120"/>
SNTP Broadcasts akzeptieren	<input checked="" type="checkbox"/>	Server deaktivieren bei lokaler Zeitquelle	<input type="checkbox"/>
Schwellwert für den Bezug der UTC [ms]	<input type="text" value="0"/>		
Client deaktivieren nach erfolgter Synchronisation	<input type="checkbox"/>		
<input type="button" value="Schreiben"/> <input type="button" value="Laden"/>		<input type="button" value="Hilfe"/>	

Abb. 18: Dialog SNTP

3.2 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.

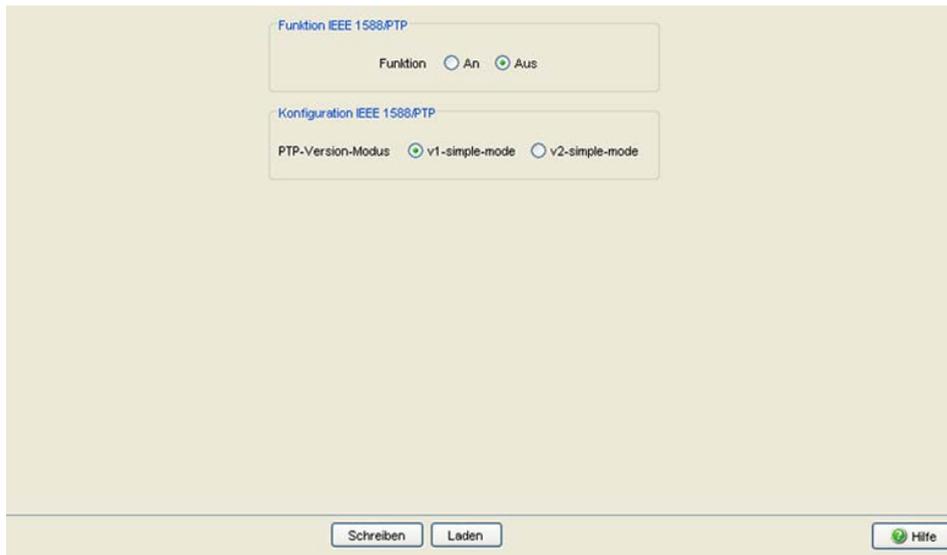
Geräte ohne PTP-Hardware-Unterstützung, die ausschließlich Ports ohne Zeitstempelinheit aufweisen, unterstützen den Simple-Modus von PTP. Dieser Modus bietet eine geringere Genauigkeit der Zeitverteilung.

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.

Hinweis: 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.



The image shows a configuration dialog box for IEEE 1588 PTP. It has a light beige background and a thin border. At the top, there is a section titled "Funktion IEEE 1588:PTP" containing a label "Funktion" followed by two radio buttons: "An" (unselected) and "Aus" (selected). Below this is another section titled "Konfiguration IEEE 1588:PTP" containing a label "PTP-Version-Modus" followed by two radio buttons: "v1-simple-mode" (selected) and "v2-simple-mode" (unselected). At the bottom of the dialog, there are three buttons: "Schreiben" (left), "Laden" (middle), and "Hilfe" (right, with a green question mark icon).

Abb. 19: Dialog PTP

4 Switching

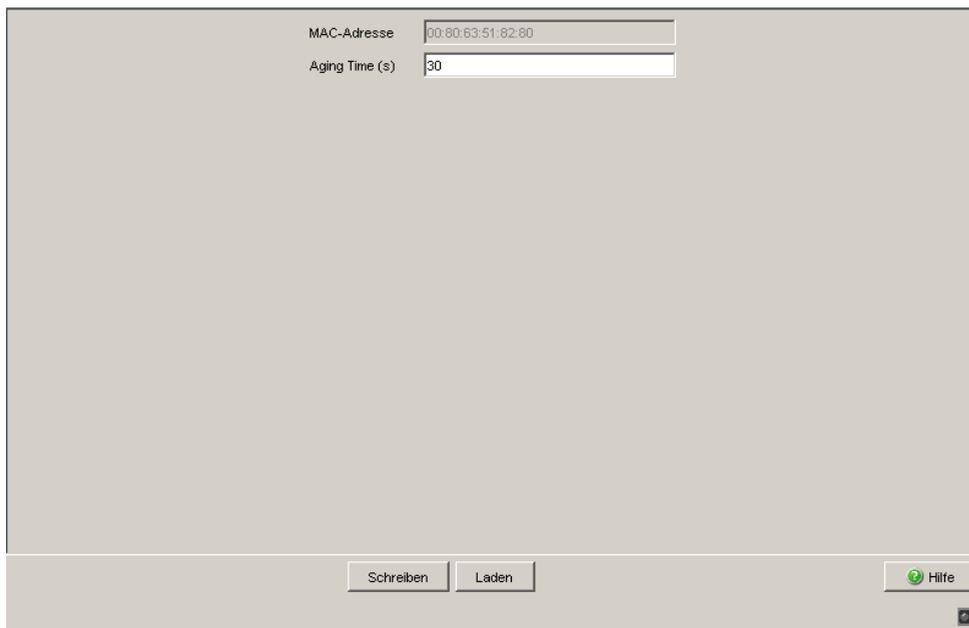
Das Switching-Menü enthält die Dialoge, Anzeigen und Tabellen zur Konfiguration der Switching-Einstellungen:

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

4.1 Switching Global

Variable	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.	15-3.825	30

Tab. 9: *Switching:Global-Dialog*



The screenshot shows a dialog box with a light gray background. At the top, there are two input fields. The first is labeled 'MAC-Adresse' and contains the text '00:80:63:51:82:80'. The second is labeled 'Aging Time (s)' and contains the text '30'. Below these fields, there are three buttons: 'Schreiben', 'Laden', and 'Hilfe'. The 'Hilfe' button has a small green icon to its left. In the bottom right corner, there are three small window control icons (minimize, maximize, close).

Abb. 20: *Dialog Switching Global*

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 33 „Konfiguration laden/speichern“).
- ▶ igmp: Das Filter wurde durch IGMP-Snooping angelegt.

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

Adresse	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 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 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. 21: Dialog Filtertabelle

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

4.3 Multicasts

Dieser Dialog bietet Ihnen die Möglichkeit,

- ▶ die IGMP-Funktion global ein- oder auszuschalten,
- ▶ das IGMP global und pro Port zu konfigurieren.

Modul	Port	IGMP an	IGMP Fow. All	Statischer Query Port	Geleerter Query Port
1	1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1	2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1	3	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>
1	4	<input checked="" type="checkbox"/>	<input type="checkbox"/>	disable	<input type="checkbox"/>

Abb. 22: Dialog GMRP

4.3.1 Globale Einstellung

Dieser Rahmen bietet Ihnen die Möglichkeit,

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

Parameter	Bedeutung	Voreinstellung
IGMP-Snooping	IGMP-Snooping für das gesamte Gerät global einschalten.	abgewählt
inaktiv	IGMP-Snooping für das gesamte Gerät global 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. 	angewählt

Tab. 10: Globale Einstellung

4.3.2 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	Wertebereich	Voreinstellung
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.		
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. 11: IGMP-Querier- und IGMP-Einstellungen

- a. Beachten Sie den Parameter-Zusammenhang zwischen Max.-Response-Time, Sende-Intervall und Group-Membership-Intervall (siehe Tab. 12.)

Die Parameter

- Max. Response-Time,
- Sende-Intervall und
- Group-Membership-Intervall

stehen in Beziehung zueinander:

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

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

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

Tab. 12: Wertebereich für
 - *Max. Response-Time*
 - *Sende-Intervall*
 - *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.

4.3.3 Multicasts

In diesem Rahmen bestimmen Sie, wie das Gerät Pakete mit

- ▶ unbekanntem - nicht mit IGMP-Snooping gelernten- MAC-/IP-Multicast-Adressen
- ▶ bekanntem - mit IGMP-Snooping gelernten- MAC-/IP-Multicast-Adressen vermittelt.

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

Parameter	Bedeutung	Wertebereich	Voreinstellung
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 Porteinstellungen. Anwendung: Routing-Protokoll PIM-SM. 	An Query- und registrierte Ports senden, An registrierte Ports senden	An registrierte Ports senden

Tab. 13: Bekannte und unbekannt Multicasts

Hinweis: 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.

4.3.4 Einstellungen pro Port (Tabelle)

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

► IGMP

Parameter	Bedeutung	Wertebereich	Voreinstellung
Modul	Modulnummer bei modularen Geräten, sonst 1.		
Port	Modul- und Port-Nummer, für die dieser Eintrag gilt.	-	-
IGMP an	IGMP je Port ein-/ausschalten. Das Ausschalten von IGMP an einem Port verhindert Registrierungen für diesen Port. Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.	An Aus	An
IGMP Forward all	Die IGMP-Snooping-Funktion Forward All ein-/ausschalten. Mit der Einstellung IGMP Forward All vermittelt das Gerät an diesem Port alle Datenpakete mit einer Multicast-Adresse im Zieladressfeld. Voraussetzung: Die IGMP-Snooping-Funktion ist global eingeschaltet.	An Aus	Aus

Hinweis: Sind mehrere Router an ein Subnetz angeschlossen, dann verwenden Sie IGMP-Version 1, damit alle Router alle IGMP-Reports erhalten.

Hinweis: Wenn Sie IGMP-Version 1 in einem Subnetz verwenden, dann verwenden Sie IGMP-Version 1 auch im gesamten Netz.

Tab. 14: IGMP-Einstellungen pro Port

Parameter	Bedeutung	Wertebereich	Voreinstellung
IGMP Automatic Query Port	Anzeige, welche Ports das Gerät als Query Ports gelernt hat, wenn in „Statischer Query Port“ „automatic“ gewählt ist. Voraussetzung: Im Dialog Switching:Multicasts:Globale Einstellung ist der Modus IGMP-Snooping ausgewählt.	ja, nein	-
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: Im Dialog Switching:Multicasts:Globale Einstellung ist der Modus IGMP-Snooping ausgewählt.	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. 14: IGMP-Einstellungen pro Port

Hinweis: Ist das Gerät in einen HIPER-Ring eingebunden, dann erreichen Sie für Datenpakete mit registrierten Multicast-Zieladressen eine schnelle Rekonfiguration des Netzes nach einer Ringschaltung 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.

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:

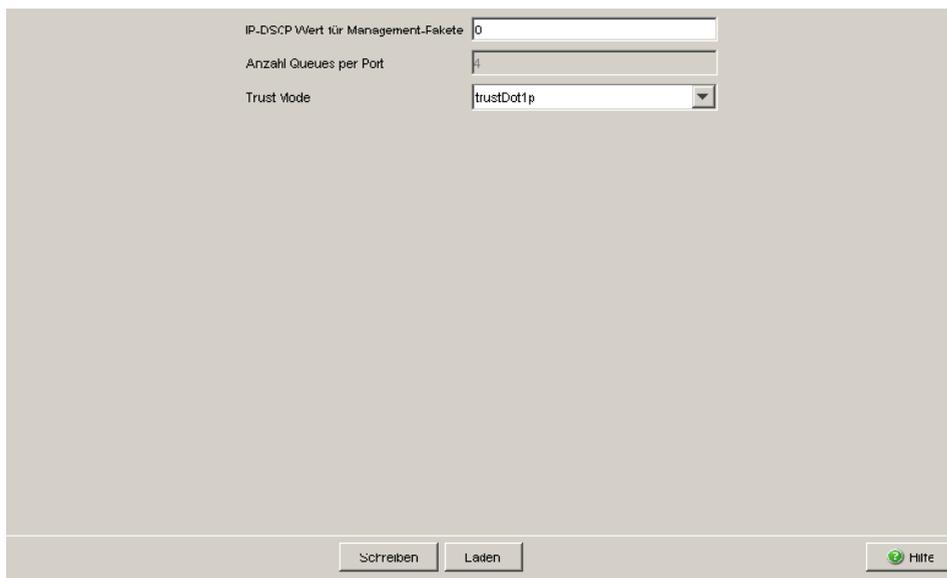
- ▶ den IP-DSCP-Wert für Management-Pakete im Bereich von 0 bis 63 einzugeben (Voreinstellung: 0 (be/cs0)).
Damit Sie in Situationen großer Netzlast immer vollen Zugriff auf die Verwaltung des Gerätes haben, bietet Ihnen das Gerät die Möglichkeit, Management-Pakete zu priorisieren.
Bei der Priorisierung 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 Tab. 19](#)).

Hinweis: 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. 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 IP-Pakete priorisiert (einer Traffic Class zuordnen, siehe „[IP-DSCP-Mapping](#)“) das Gerät entsprechend ihres DSCP-Wertes.
Empfangene Pakete, die keine IP-Pakete sind, priorisiert (einer Traffic Class zuordnen, siehe „[Port-Priorität eingeben](#)“) das Gerät entsprechend der Port-Priorität des Empfangsports.

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. 15: VLAN-Prio-Remarking



IP-DSCP Wert für Management-Fakete 0

Anzahl Queues per Port 4

Trust Mode trustDot1p

Schreiben Laden Hilfe

Abb. 23: Dialog Global

5.2 Portkonfiguration

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

- ▶ einem Port eine Port-Priorität zuweisen.

Parameter	Bedeutung
Modul	Modul des Gerätes, auf dem sich der Port befindet.
Port	Port, für den dieser Eintrag gilt.
Port Priorität	Eingeben der Portpriorität

Tab. 16: Portkonfiguration-Tabelle

Modul	Port	Port Priorität
1	1	0
1	2	0
1	3	0
1	4	0
1	5	0
1	6	0
1	7	0
1	8	0
1	9	0
1	10	0
1	11	0
1	12	0
1	13	0
1	14	0
1	15	0
1	16	0

Schreiben Laden Hilfe

Abb. 24: Dialog Portkonfiguration

5.2.1 Port-Priorität eingeben

- Doppelklicken Sie in der Spalte „Port Priorität“ in eine Zelle und tragen Sie die Priorität (0-7) ein.

Das Gerät ordnet Datenpakete, die es an diesem Port empfängt, entsprechend der eingetragenen Priorität einer Prioritätsklasse zu (siehe Tab. 17).

Voraussetzung:

Einstellung im Dialog `Global: Trust Modus: untrusted` (siehe auf Seite 72 „Global“) oder

Einstellung im Dialog `Global: Trust Modus: trustDot1p` (siehe auf Seite 72 „Global“) und die Datenpakete enthalten kein VLAN-Tag oder

Einstellung im Dialog `Global: Trust Modus: trustIpDscp` (siehe auf Seite 72 „Global“) und die Datenpakete sind keine IP-Pakete.

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

Tab. 17: Zuordnung der Port-Priorität zu den 4 Traffic Classes

5.3 802.1D/p-Mapping

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

VLAN Priorität	Traffic class
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Schreiben Laden Hilfe

Abb. 25: Dialog 802.1D/p-Mapping

- Tragen Sie für jede VLAN-Priorität im Feld Traffic Class den gewünschten Wert zwischen 0 und 3 ein.

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

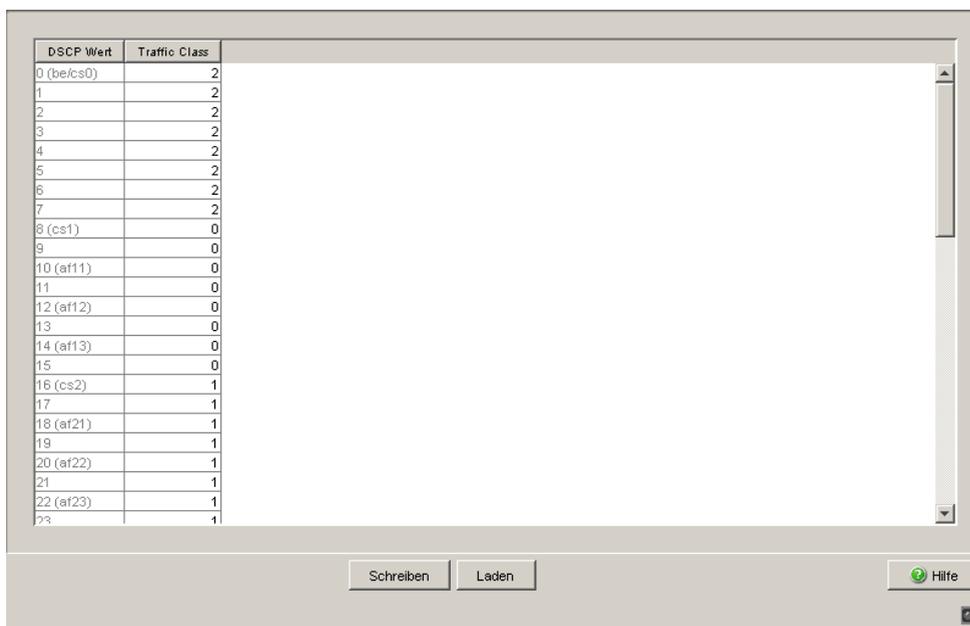
Tab. 18: Zuordnung der VLAN-Priorität zu den 4 Traffic Classes

Hinweis: Netzprotokolle und Redundanzmechanismen nutzen die höchste Traffic Class 3. Wählen Sie deshalb andere Traffic Classes für Anwendungsdaten.

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 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. 26: Tabelle IP DSCP Mapping

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

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

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

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

Tab. 19: Abbildung der DSCP-Werte auf die Traffic Classes

6 Redundanz

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

- ▶ Ring-Redundanz
- ▶ Sub-Ring
- ▶ Redundante Kopplung von Ringen und Netzsegmenten
- ▶ Rapid Spanning Tree Protokoll (RSTP)

6.1 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.

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
 - RSB20
 - 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.

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.

Hinweis: 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.

Parameter	Bedeutung
Version	Wählen Sie, welche Ring-Redundanz-Version Sie einsetzen: HIPER-Ring MRP Voreinstellung ist HIPER-Ring
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
Operation	Werte abhängig von gewählter Ring-Redundanz-Version. Beschreibung in den folgenden Abschnitten bei der entsprechenden Ring-Redundanz-Version.

Tab. 20: Ring-Redundanz Basiskonfiguration

6.1.1 HIPER-Ring konfigurieren

Für die Ring-Ports wählen Sie im Dialog `Grundeinstellungen:Port-konfiguration`) folgende Grundeinstellungen:

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

Tab. 21: *Port-Einstellungen für Ring-Ports*

Hinweis: 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.

Hinweis: Alternativ zur Konfiguration des HIPER-Rings per Software, können Sie bei den Geräten RS20/30/40 und MS20/30 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.

Tab. 22: HIPER-Ring-Konfiguration

Parameter	Bedeutung
Ringrekonfiguration	<p>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.</p> <ul style="list-style-type: none"> ▶ Standard: Testpakete-Timeout 480 ms ▶ Beschleunigt: Testpakete-Timeout 280 ms <p>Hinweis: 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	<p>Wenn das Gerät Ring-Manager ist: Die Anzeigen in diesem Rahmen bedeuten:</p> <p>„Redundanz vorhanden“: Wenn eine Komponente des Rings ausfällt, übernimmt die redundante Strecke deren Funktion.</p> <p>„Konfigurationsfehler“: Sie haben die Funktion falsch konfiguriert oder die Ringportverbindung ist nicht vorhanden.</p>

Tab. 22: HIPER-Ring-Konfiguration

The screenshot shows a web-based configuration interface for ring redundancy. It includes sections for selecting the version (HIPER-Ring or MRP), configuring two ring ports (Ring Port 1 and Ring Port 2) with module, port, and operation details, setting the redundancy manager (Advanced Mode), choosing the manager mode (An/Aus), selecting the function (An/Aus), and setting the ring reconfiguration time (500ms/200ms). There is also a VLAN ID field and an information section. At the bottom, there are buttons for 'Schreiben', 'Laden', 'Lösche Ringkonfiguration', and 'Hilfe'.

Abb. 27: Ring-Redundanz wählen, Ringports eingeben, Ring-Manager ein-/ausschalten und Ringrekonfiguration wählen.

Hinweis: Deaktivieren Sie das Spanning-Tree-Protokoll an den Ports, die an den redundanten Ring angeschlossen sind, da Spanning-Tree und Ring-Redundanz mit unterschiedlichen Reaktionszeiten arbeiten (Redundanz:Rapid Spanning Tree:Port).

Hinweis: 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.

6.1.2 MRP-Ring konfigurieren

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)
Optisch	100 Mbit/s	aus	an	100 Mbit/s Vollduplex (FDX)

Tab. 23: *Port-Einstellungen für Ring-Ports*

Hinweis: 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.

Parameter	Bedeutung
Ring-Port X.X	Anzeige im Feld „Operation“:
Operation	<p><code>forwarding</code>: Sie haben diesen Port eingeschaltet und er hat einen Link.</p> <p><code>blocked</code>: dieser Port ist blockiert und hat einen Link</p> <p><code>disabled</code>: Sie haben diesen Port ausgeschaltet</p> <p><code>not-connected</code>: dieser Port hat keinen Link.</p>
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.
Hinweis: 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	<p>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.</p> <p>Hinweis: Einstellungen im Rahmen „Ringrekonfiguration“ sind lediglich bei Geräten wirksam, die Ring-Manager sind.</p>
Information	<p>Wenn das Gerät Ring-Manager ist: Die Anzeigen in diesem Rahmen bedeuten:</p> <p>„Redundanz vorhanden“: Wenn eine Komponente des Rings ausfällt, übernimmt die redundante Strecke deren Funktion.</p> <p>„Konfigurationsfehler“: Sie haben die Funktion falsch konfiguriert oder die Ringportverbindung ist nicht vorhanden.</p>

Tab. 24: MRP-Ring Konfiguration

The screenshot shows a configuration window for a ring network. At the top, under 'Version', the 'MRP' radio button is selected. Below this, there are two columns for 'Ring Port 1' and 'Ring Port 2'. For Ring Port 1, 'Modul' is 1 and 'Port' is 1. For Ring Port 2, 'Modul' is 1 and 'Port' is 2. The 'Kongfiguration des Redundanzmanager' section has a checked box for 'Advanced Mode'. The 'Redundanzmanager' section has the 'An' radio button selected. The 'Funktion' section has the 'An' radio button selected. The 'Ringrekonfiguration' section has the '500ms' radio button selected. The 'VLAN' section has 'VLAN ID' set to 1. At the bottom, there are buttons for 'Schreiben', 'Laden', 'Lösche Ringkonfiguration', and 'Hilfe'.

Abb. 28: MRP-Ring-Version wählen, Ringports eingeben und Ring-Manager ein-/ausschalten.

Hinweis: 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.

Hinweis: 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.

6.2 Rapid Spanning Tree

Dieser Dialog bietet Ihnen die Möglichkeit:

- ▶ Das Rapid-Spanning-Tree-Protokoll ein-/auszuschalten,
- ▶ gerätespezifische Informationen zum Rapid-Spanning-Tree-Protokoll anzusehen,
- ▶ gerätespezifische Parameter des Rapid-Spanning-Tree-Protokolls zu konfigurieren, und
- ▶ portspezifische Parameter des Rapid-Spanning-Tree-Protokolls zu konfigurieren.

Hinweis: Das Spanning-Tree-Protokoll ist ein Protokoll für MAC-Brücken. Daher wird in der folgenden Beschreibung der Begriff Brücke für Switch verwendet.

Lokale Netze werden immer größer. Dies gilt sowohl für die geographische Ausdehnung als auch für die Anzahl der Netzteilnehmer. Deshalb ist der Einsatz mehrerer Bridges vorteilhaft, z.B. um:

- ▶ die Netzlast in Teilbereichen zu verringern,
- ▶ redundante Verbindungen aufzubauen und
- ▶ Entfernungseinschränkungen zu überwinden.

Der Einsatz mehrerer Bridges mit mehrfachen, redundanten Verbindungen zwischen den Teilnetzen kann jedoch zu Schleifen/Loops und zum Verlust der Kommunikation durch das Netz führen. Als Hilfe, um dies zu verhindern, haben Sie die Möglichkeit, Spanning Tree einzusetzen. Spanning Tree erzielt Schleifenfreiheit durch das gezielte Deaktivieren von redundanten Verbindungen. Das gezielte Wieder-Aktivieren einzelner Verbindungen bei Bedarf ermöglicht die Redundanz.

RSTP ist eine Weiterentwicklung des Spanning-Tree-Protokolls (STP) und ist zu diesem kompatibel. Das STP benötigte bei Betriebsunfähigkeit einer Verbindung oder einer Bridge eine Rekonfigurationszeit von max. 30 s. Dies ist für zeitkritische Anwendungen nicht mehr akzeptabel. RSTP erreicht durchschnittliche Rekonfigurationszeiten von unter einer Sekunde. Wenn Sie RSTP in einer Ringtopologie mit 10 bis 20 Geräten einsetzen, können Sie auch Rekonfigurationszeiten im Millisekundenbereich erreichen.

Hinweis: 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.

Hinweis: 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.

Hinweis: 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.

Hinweis: 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.

6.2.1 Global

Hinweis: 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.

Parameter	Bedeutung	Wertebereich	Voreinstellung
Funktion	Schalten Sie die RSTP-Funktion für dieses Gerät „An“ oder „Aus“. Wird RSTP für ein Gerät global ausgeschaltet, so flutet das Gerät die RSTP Pakete wie normale Multicast Pakete. Das Gerät verhält sich transparent gegenüber RSTP-Paketen.	An, Aus	
MRP-Kompatibilität	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. 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.	An, Aus	Aus
Root Information	In jeder RSTP-Umgebung existiert ein Root Gerät, welches die Auflösung der Topologie und das Verhalten von RSTP steuert. Hier werden die Parameter des aktuellen Root Gerätes angezeigt. – Root-ID: zeigt die Brückenidentifikation des Root Gerätes an. Diese setzt sich aus dem Wert für die Priorität und der MAC Adresse des Gerätes zusammen. „Dieses Gerät ist Root“: ein Häkchen zeigt, dass das Gerät zur Zeit Wurzelswitch ist. – Root-Port: zeigt den Port an, der zum Wurzelswitch führt. Haben Sie das Gerät selbst als Root Gerät konfiguriert, so wird 0.0 angezeigt. – Root-Kosten: zeigt die Rootkosten bis zum Root-Gerät an. Haben Sie das Gerät selbst als Root konfiguriert, so werden Kosten von 0 angezeigt.		

Tab. 25: Globale Spanning-Tree-Einstellungen, Grundfunktionen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Priorität	Stellt die lokale Bridge-Priorität ein. Die Bridge-Priorität und die eigene MAC-Adresse zusammen bilden die eigene Bridge-ID. Das Gerät mit dem besten, also numerisch niedrigsten Prioritätswert übernimmt die Rolle der Root-Bridge. Bestimmen Sie das Root-Gerät, indem Sie dem Gerät die beste Priorität in der Bridge-ID unter allen Geräten im Netz zuweisen. Geben Sie den Wert als Vielfaches von 4.096 ein.	$0 \leq n \cdot 4.096 \leq 61.440$	32.768
Hello Time	Stellt die Hello-Time ein. Die lokale Hello Time gibt die Zeit zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Pakete) in Sekunden an. Hat das lokale Gerät die Root-Funktion, übernehmen die anderen Geräte im gesamten Netz diesen Wert. Ansonsten benutzt das lokale Gerät den Wert der Root-Bridge in der rechten Spalte „Root“.	1 - 2	2
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	15 s

Tab. 25: Globale Spanning-Tree-Einstellungen, Grundfunktionen

Parameter	Bedeutung	Wertebereich	Voreinstellung
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).</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>	6 - 40 s	20 s
Bridge-ID (Read-Only)	<p>Die lokale Bridge-ID, zusammengesetzt aus der lokalen Priorität und der eigenen MAC-Adresse.</p> <p>Das Format ist ppppp / mm mm mm mm mm mm, mit: ppppp: Priorität (dezimal) und mm: das jeweilige Byte der MAC-Adresse (hexadezimal).</p>		
Topologie Änderungen	Dieses Feld zeigt die Anzahl der Änderungen seit dem Start von RSTP an.		
Dauer seit letzter Änderung	Dieses Feld zeigt die verstrichene Zeit seit der letzten Rekonfiguration des Netzes an.		
Information	<p>Dieser Rahmen zeigt an, ob ein Konfigurationskonflikt vorliegt.</p> <p>In diesem Fall liegt außerhalb des MRP-Rings das Gerät mit der angezeigten MAC-Adresse. Die angezeigte Priorität dieses Gerätes ist besser (numerisch kleiner), als die Priorität der Root-Brücke im MRP-Ring.</p> <p>Um den Konflikt zu beseitigen, stellen Sie auf dem angezeigten Gerät eine schlechtere Priorität (numerisch größer) ein, als die Priorität der Root-Brücke im MRP-Ring.</p>		

Tab. 25: Globale Spanning-Tree-Einstellungen, Grundfunktionen

Hinweis: 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.

The screenshot shows the RSTP Global-Dialog configuration window. It is divided into several sections:

- Funktion:** Radio buttons for 'An' and 'Aus'.
- MRP-Kompatibilität:** Radio buttons for 'An' and 'Aus'.
- Root-Information:**
 - Root-ID: 20480
 - Root-Port: 1.4
 - Root-Kosten: 220000
 - Priority: 32768
 - MAC-Adresse: 00 80 63 0f 1d b0
 - Checkbox: Dieses Gerät ist Root
- Protokoll-Konfiguration-Information:**
 - Priority: 32768
 - MAC-Adresse: 00 80 63 51 82 80
 - Hello Time [s]: 2
 - Topologie-Änderungen: 5
 - Forward Delay [s]: 15
 - Dauer seit letzter Änderung: 0 Tag(e), 4:05:28
 - Max Age [s]: 20
- Information:** Empty text field.
- Buttons:** 'Schreiben', 'Laden', and 'Hilfe'.

Abb. 29: RSTP Global-Dialog

6.2.2 Rapid-Spanning-Tree-Port

Parameter	Bedeutung	Wertebereich	Voreinstellung
STP-Status	Hier können Sie RSTP für diesen Port ein- oder ausschalten. Ist RSTP global eingeschaltet und an einem Port ausgeschaltet, so werden an diesem Port empfangene RSTP-Pakete verworfen.	an, aus	an
Port-Status	Zeigt den RSTP-Port-Status an.	disabled, forwarding, discarding, blocking, learning	-
Port-Priorität	Hier geben Sie das 1. Byte der Port-Identifikation ein.	$16 \leq n \cdot 16 \leq 240$	128
Port-Pfadkosten	Eingabe der Pfadkosten zur Bevorzugung redundanter Pfade. Beim Wert 0 ermittelt der Switch automatisch die Pfadkosten abhängig von der Übertragungsrate.	0 - 200.000.000	0
Soll-Edge-Port	Beim Wert „true“ schaltet der Port in den Forwarding Status. Empfängt der Port trotzdem ein RSTP-Paket, wird der Port geblockt und die Portrolle geklärt. Beim Wert „false“ bleibt der Port solange geblockt, bis seine Rolle geklärt ist. Erst danach schaltet der Port in seinen endgültigen Status.	true, false	false
Ist-Edge-Port	Ist „true“ wenn keine RSTP-Pakete empfangen wurden, also ein Endgerät angeschlossen ist. Ist „false“ wenn RSTP-Pakete empfangen wurden, also kein Endgerät, sondern eine Bridge angeschlossen ist.	true, false	-

Tab. 26: Port-bezogene RSTP-Einstellungen und -Anzeigen

Parameter	Bedeutung	Wertebereich	Voreinstellung
Auto-Edge-Port	Die Einstellung Auto-Edge-Port wird nur berücksichtigt, wenn der Parameter Soll-Edge-Port auf „false“ steht. Ist Auto-Edge-Port „true“, vermittelt der Port innerhalb von 1,5 x Hello Time (3 Sekunden). Ist Auto-Edge-Port „false“, dann dauert es 30 Sekunden, bis ein Endgeräteport Datenpakete vermittelt.	true, false	true
Ist PointToPoint	Wenn an diesem Port eine Voll duplex-Verbindung zwischen zwei RSTP-Geräten besteht, wird Ist PointToPoint „true“; anderenfalls wird „false“ angezeigt (z.B. wenn ein Hub angeschlossen ist). Die Punkt-zu-Punkt-Verbindung ist eine direkte Verbindung zwischen zwei RSTP-Geräten. Die direkte, dezentrale Kommunikation zwischen den beiden Switches bewirkt eine schnelle Rekonfigurationszeit.	true, false	auto (wird aus Duplex-Modus bestimmt: FDX: true HDX: false)
Designierte Root	Zeigt für diesen Port die Brückenidentifikation der designierten Root-Bridge an.	Brückenidentifikation (hexadezimal)	-
Designierte Kosten	Anzeige der Kosten des Pfades von diesem Port zur Root-Bridge.	Kosten	-
Designierter Port	Anzeige der Port-Identifikation des Ports, der für den lokalen Port- (auf dem designated Switch) die Verbindung zur Root-Bridge herstellt.	Port-Identifikation (hexadezimal) und Portnummer	-

Tab. 26: Port-bezogene RSTP-Einstellungen und -Anzeigen

CIST Guards MSTI 2													
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 type="checkbox"/>	<input 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	

Schreiben Laden Erzeugen Löschen Hilfe

Abb. 30: RSTP-Port-Dialog

7 Diagnose

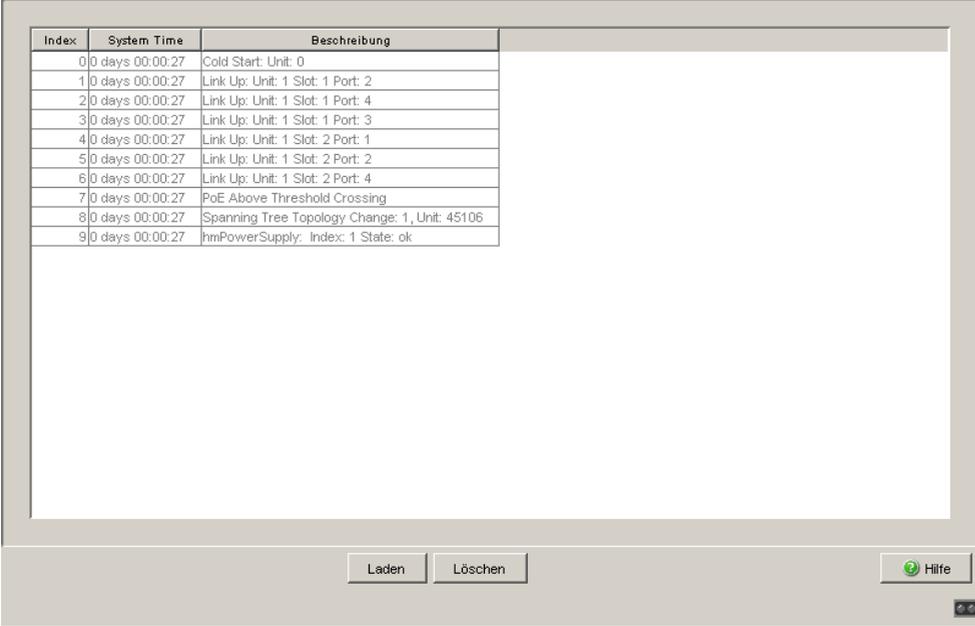
Das Diagnose-Menü enthält folgende Tabellen und Dialoge:

- ▶ Trap-Log
- ▶ Ports (Statistiken, Netzlast, SFP-Module)
- ▶ Topologie-Erkennung
- ▶ Port-Mirroring
- ▶ Gerätestatus
- ▶ Meldekontakt
- ▶ Alarme (Traps)
- ▶ Bericht (Log-Datei, Systeminformation)
- ▶ IP-Adressen Konflikterkennung
- ▶ Selbsttest

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

7.1 Ereignis-Log

Die Tabelle listet die geloggtten Ereignisse mit Zeitstempel auf. Die „Laden“-Bedientaste bietet Ihnen die Möglichkeit, den Inhalt des Ereignis-Logs zu aktualisieren, mit der „Löschen“-Bedientaste löschen Sie den Inhalt des Ereignis-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	hmPowerSupply: Index: 1 State: ok

Abb. 31: Ereignis-Log Tabelle

7.2 Ports

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

- ▶ Statistiktabelle
- ▶ Netzlast
- ▶ SFP-Module

7.2.1 Statistiktabelle

Diese Tabelle zeigt Ihnen die Inhalte verschiedener Ereigniszähler an. Im Menüpunkt Neustart können Sie mit „Warmstart“, „Kaltstart“ oder „Port-Zähler 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	0
1.2	4133	137	3996	14461	3815040	0	0	0	0	0
1.3	7031	2719	4312	17061	4325761	0	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	0
2.2	196124	135	195989	11854	3279565	0	0	0	0	0
2.3	0	0	0	0	0	0	0	0	0	0
2.4	197631	1653	195978	13322	3072287	0	0	0	0	0
3.1	0	0	0	0	0	0	0	0	0	0
3.2	0	0	0	0	0	0	0	0	0	0

Abb. 32: Portstatistiken, Tabelle

7.2.2 Auslastung (Netzlust)

Diese Tabelle zeigt Ihnen die Auslastung (Netzlust) 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.

In der Spalte „Oberer Grenzwert [%]“ geben Sie den oberen Grenzwert für die Auslastung ein. Bei Überschreiten dieses Grenzwertes setzt das Gerät im Feld „Alarm“ eine Markierung.

In der Spalte „Unterer Grenzwert [%]“ geben Sie den unteren Grenzwert für die Auslastung ein. Bei Unterschreiten dieses Grenzwertes hebt das Gerät eine zuvor gesetzte Markierung wieder auf.

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. 33: Dialog Auslastung (Netzlast)

7.2.3 SFP-Module

Die SFP-Zustandsanzeige bietet Ihnen die Möglichkeit, die aktuelle Bestückung der SFP-Module und deren Eigenschaften einzusehen. Zu den Eigenschaften zählen:

Parameter	Bedeutung
Modul.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.
Empfangsleistungs-Status	Anzeige des Leistungsgrades des empfangenen Signals: - gute Empfangsleistung - eingeschränkte Empfangsleistung - unzureichende Empfangsleistung

Tab. 27: Dialog SFP-Module

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

Abb. 34: Dialog SFP-Module

7.3 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 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 61 „Filter für MAC-Adressen“](#)).

7.4 Port-Mirroring

Die Funktion Port-Mirroring bietet Ihnen die Möglichkeit, den Datenverkehr von bis zu 8 Ports des Geräts zu Diagnosezwecken zu untersuchen. Dabei leitet das Gerät die Daten dieser Ports zusätzlich an einen anderen Port weiter (spiegelt sie). Dieses Verfahren heißt auch Port-Mirroring.

Die zu untersuchenden Ports werden Quellports genannt. Der Port, zu dem das Gerät die zu untersuchenden Daten kopiert, heißt Zielport. Sie können ausschließlich physikalische Ports als Quell- oder Zielports verwenden.

Beim Port-Mirroring kopiert das Gerät gültige, ein- **und** ausgehende Datenpakete der Quellports zum Zielport. Den Datenverkehr an den Quellports lässt das Gerät beim Port-Mirroring unbeeinflusst.

Ein am Zielport angeschlossenes Management-Werkzeug, wie z.B. eine RMON-Probe, kann so den Datenverkehr der Quellports in Sende- und Empfangsrichtung beobachten.

Der Zielport leitet zu sendende Daten weiter.

Bei den Geräten PowerMICE, MACH 104, MACH 1040 und MACH 4000 blockiert der Zielport empfangene Daten, bei allen anderen Geräten leitet der Zielport auch empfangene Daten weiter.

- Wählen Sie die Quellports, deren Datenverkehr sie beobachten möchten, aus der Liste der physikalischen Ports aus, indem Sie die entsprechenden Kästchen markieren.
Sie können maximal 8 Quellports auswählen. Nicht auswählbare Ports stellt das Gerät inaktiv dar, z.B. den momentan als Zielport verwendeten Port, oder wenn Sie bereits 8 Ports ausgewählt haben. Voreinstellung: keine Quellports.
- Wählen Sie den Zielport, an dem Sie Ihr Management-Werkzeug angeschlossen haben, aus dem Listenelement im Rahmen „Zielport“ aus. Nicht auswählbare Ports zeigt das Gerät nicht in der Liste an, z.B. die momentan als Quellports verwendeten Ports. Voreinstellung: Port 0.0 (kein Zielport).
- Wählen Sie „An“ im Rahmen „Funktion“, um die Funktion einzuschalten. Voreinstellung: „Aus“.

Die Bedientaste „Konfiguration zurücksetzen“ im Dialog bietet Ihnen die Möglichkeit, alle Port-Mirroring-Einstellungen des Gerätes in den Lieferzustand zurückzusetzen.

Hinweis: Bei aktivem Port-Mirroring dient der festgelegte Zielport ausschließlich zur Beobachtung, er nimmt nicht am normalen Datenverkehr teil.

Quellport	Aktiv
1.1	<input checked="" type="checkbox"/>
1.2	<input type="checkbox"/>
1.3	<input type="checkbox"/>
1.4	<input type="checkbox"/>
2.1	<input checked="" type="checkbox"/>
2.2	<input type="checkbox"/>
2.3	<input type="checkbox"/>
2.4	<input type="checkbox"/>
3.1	<input type="checkbox"/>
3.2	<input type="checkbox"/>

Abb. 35: Dialog Port-Mirroring

7.5 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.

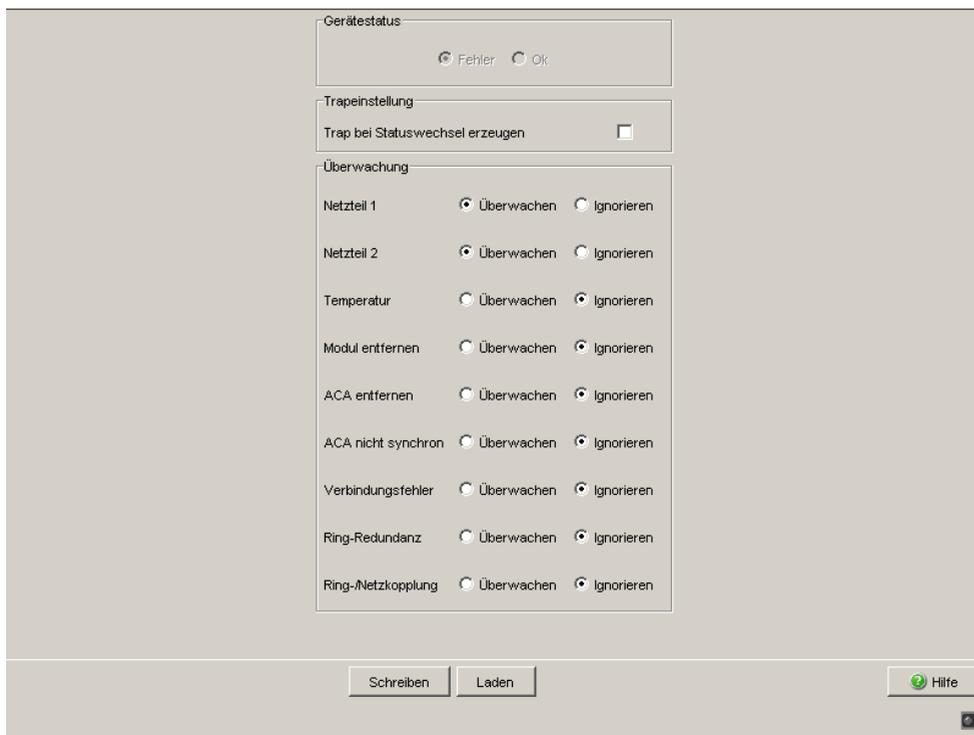


Abb. 36: Dialog Gerätestatus (bei PowerMICE)

- Wählen Sie im Feld „Überwachung“ die Ereignisse, die Sie überwachen möchten.

Die auswählbaren Ereignisse haben folgende Bedeutung:

Name	Bedeutung
Netzteil ...	Versorgungsspannung(en) überwachen/ignorieren
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 28 „Portkonfiguration“). Im Lieferzustand erfolgt keine Verbindungsüberwachung.

Tab. 28: Gerätestatus

Name	Bedeutung
Ring-Redundanz	<p>Ring-Redundanz überwachen/ignorieren (bei HIPER-Ring nur im Ring-Manager-Betrieb). Im Lieferzustand erfolgt keine Überwachung der Ring-Redundanz.</p> <p>Ist das Gerät normaler Ring-Teilnehmer und nicht Ring-Manager, meldet es folgendes:</p> <ul style="list-style-type: none"> ▶ nichts (beim HIPER-Ring) ▶ erkannte Fehler in der lokalen Konfiguration (beim Fast HIPER-Ring und bei MRP)
Ring-/Netzkopplung	<p>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:</p> <ul style="list-style-type: none"> – fehlerhafter Linkstatus der Steuerleitung – Partnergerät ist ebenfalls Slave (im Stand-by-Modus).

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

Tab. 28: Gerätestatus

- a. Die Konfigurationen stimmen dann nicht überein, wenn nur eine Datei existiert oder die 2 Dateien nicht den gleichen Inhalt haben.

- Wählen Sie im Feld „Trapeinstellung“ „Trap bei Statuswechsel erzeugen“, um das Versenden eines Traps zu aktivieren, wenn sich der Gerätestatus ändert.

Hinweis: 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 116 „Meldekontakt“](#)).

7.6 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.

7.6.1 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.

7.6.2 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.
 - ▶ Das Entfernen eines Moduls. Wählen Sie Modul entfernen „überwachen“, wenn der Meldekontakt das Entfernen eines Moduls melden soll (bei modularen Geräten).
 - ▶ 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 84 „Ring-Redundanz“](#)). Wählen Sie Ring-Redundanz „überwachen“, wenn der Meldekontakt den Entfall der Redundanz-Reserve im redundanten Ring melden soll.
Lieferzustand: keine Überwachung.

Hinweis: Ist das Gerät normaler Ring-Teilnehmer und nicht Ring-Manager, meldet es beim HIPER-Ring nichts und bei MRP nur erkannte Fehler in der lokalen Konfiguration.

7.6.3 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 113 „Gerätestatus“](#)) und ermöglicht damit eine Ferndiagnose.
Über den potentialfreien Meldekontakt (Relaiskontakt, Ruhestromschaltung) wird durch Kontaktunterbrechung der Gerätestatus „Fehler detektiert“ ([siehe auf Seite 113 „Gerätestatus“](#)) gemeldet.

7.6.4 Trapeinstellung

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

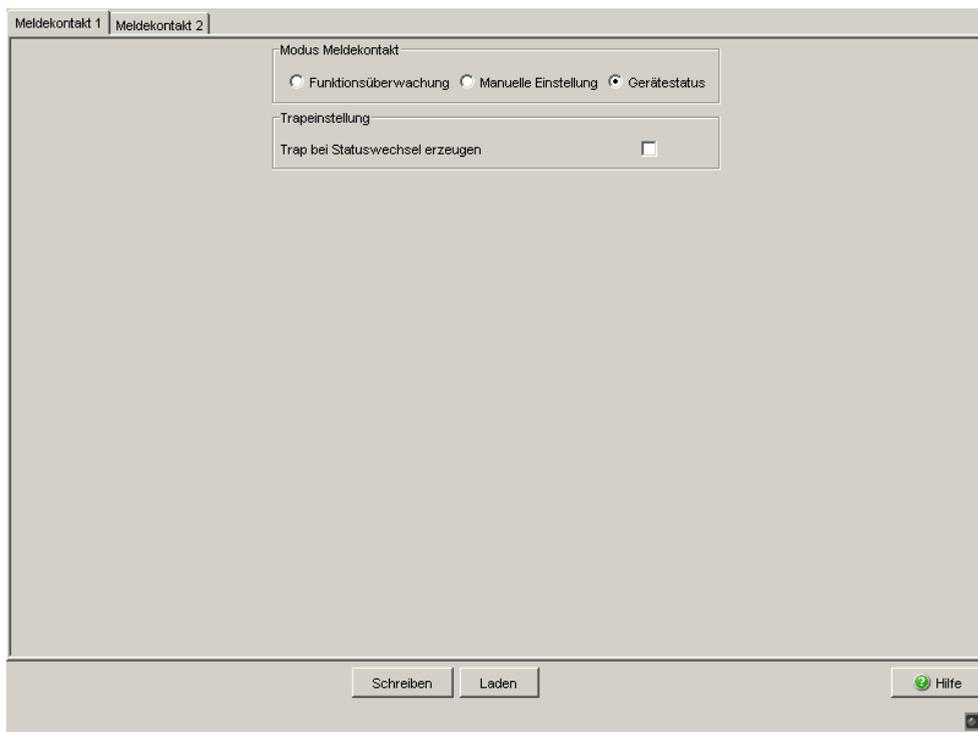


Abb. 37: Dialog Meldekontakt

7.7 Alarme (Traps)

Dieser Dialog bietet Ihnen die Möglichkeit festzulegen, welche Ereignisse einen Alarm (Trap) auslösen und an wen diese Alarme gesendet werden sollen.

- Wählen 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.
- Im Rahmen „Konfiguration“ wählen Sie die Trap-Kategorien aus, von denen Sie Traps versenden wollen. Voreinstellung: alle Trap-Kategorien sind aktiv.

Die auswählbaren Ereignisse haben folgende Bedeutung:

Name	Bedeutung
Authentifizierung	Das Gerät hat einen unerlaubten Zugriff zurückgewiesen (siehe auf Seite 45 „SNMPv1/v2-Zugriffs-Einstellungen“).
Link Up/Down	An einem Port des Gerätes wurde die Verbindung zu einem anderen Gerät hergestellt/unterbrochen.
Spanning Tree	Die Topologie des Rapid Spanning Tree hat sich geändert
Chassis	Fasst die folgenden Ereignisse zusammen: <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> . <ul style="list-style-type: none"> – Ein Medienmodul wurde hinzugefügt oder entfernt (nur bei modularen Geräten). – 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>).
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.

Tab. 29: Trap-Kategorien

Konfiguration

- Authentifizierung
- Link Up/Down
- Spanning Tree
- Chassis
- Redundanz
- Portsicherheit

Index	IP-Adresse	Passwort	Aktiv
1	10.1.1.254	general-trap	<input checked="" type="checkbox"/>
2	10.1.1.253	backup-trap	<input checked="" type="checkbox"/>

Schreiben Laden Erzeugen Löschen Hilfe

Abb. 38: Dialog Alarme

7.8 Bericht

Folgende Berichte stehen zur Diagnose zur Verfügung:

- ▶ [Log-Datei](#).
Die Log-Datei ist eine HTML-Datei, in die das Gerät wichtige geräteinterne Ereignisse schreibt.
- ▶ [Systeminformation](#).
Die Systeminformation ist eine HTML-Datei mit systemrelevanten Daten.

7.9 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.



Abb. 39: Dialog Selbsttest

8 Erweitert

Das Menü enthält Dialoge, Anzeigen und Tabellen zu:

- ▶ DHCP-Relay-Agent

8.1 DHCP-Relay-Agent

Dieser Dialog ermöglicht Ihnen, den DHCP-Relay-Agenten zu konfigurieren.

- Geben Sie die DHCP-Server-IP-Adressen ein.
Sollte ein DHCP-Server nicht erreichbar sein, dann ermöglicht die Eingabe von bis zu 3 weiteren DHCP-Server-IP-Adressen dem Gerät das Ausweichen auf einen anderen DHCP-Server.

- Mit der Option 82 fügt der DHCP-Relay-Agent, der eine DHCP-Anforderung empfängt, der Anforderung ein „Option 82“-Feld an, sofern die empfangene Anforderung noch kein solches Feld besitzt.
Bei ausgeschalteter Funktion leitet das Gerät angehängte „Option 82“-Felder weiter, fügt jedoch keine an. Geben Sie in „Typ“ an, in welchem Format der DHCP-Relay-Agent die Geräteerkennung dieses Gerätes in das „Option 82“-Feld einfügen soll.

Zur Auswahl stehen:

- IP-Adresse
- MAC-Adresse (Lieferzustand)
- Systemname (Client-ID)
- other (frei definierbare ID, die Sie in der folgenden Zeile eingeben können).

„Remote ID-Eintrag für DHCP-Server“ zeigt Ihnen den Wert an, den Sie bei der Konfiguration Ihres DHCP-Servers eintragen. „Typanzeige“ zeigt die Geräteerkennung in der ausgewählten Form an.

- ▶ 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.

Hinweis: 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, so kann die Circuit-ID, die es an den DHCP-Server sendet, von der angezeigten abweichen.

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 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.

Server IP Address

DHCP Option 82

Funktion An Aus

Typ

konfigurierbarer Wert (Typ other)

RemotelD-Eintrag für DHCP-Server

Typanzeige

DHCP Relay nicht aktiv

Modul	Port	Circuit-ID	Option 82 ein	Hirschmann Gerät
1	1	B7 06 00 00 01 01 01 01	<input checked="" type="checkbox"/>	<input type="checkbox"/>
1	2	B7 06 00 00 01 01 01 02	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	1	B7 06 00 00 01 01 02 01	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	2	B7 06 00 00 01 01 02 02	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	3	B7 06 00 00 01 01 02 03	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	4	B7 06 00 00 01 01 02 04	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	1	B7 06 00 00 01 01 03 01	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	2	B7 06 00 00 01 01 03 02	<input checked="" type="checkbox"/>	<input type="checkbox"/>
3	3	B7 06 00 00 01 01 03 03	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Schreiben Laden Hilfe

Abb. 40: Dialog DHCP-Relay-Agent

8.2 Command Line Interface

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“.

A Anhang

A.1 Technische Daten

Switching	
Größe MAC-Adresstabelle (inkl. statische Filter)	2.048
Max. Anzahl statisch konfigurierter Multicast- MAC-Adressfilter	64
Max. Anzahl statisch konfigurierter Unicast- MAC-Adressfilter	100
Max. Länge überlanger Pakete (ab Rel. 03.0.00)	1.552 Bytes

A.2 Liste der RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
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 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2271	SNMP Framework MIB
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped Boundaries
RFC 2570	Introduction to SNMP v3
RFC 2571	Architecture for Describing SNMP Management Frameworks
RFC 2572	Message Processing and Dispatching for SNMP
RFC 2573	SNMP v3 Applications

RFC 2574	User Based Security Model for SNMP v3
RFC 2575	View Based Access Control Model for SNMP
RFC 2576	Coexistence between SNMP v1, v2 & v3
RFC 2578	SMI v2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting
RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol
RFC 3376	IGMPv3

A.3 Zugrundeliegende IEEE-Normen

IEEE 802.1AB	Topology Discovery (LLDP)
IEEE 802.1af	Power over Ethernet
IEEE 802.1D	Switching, GARP, GMRP, Spanning Tree (supported via IEEE 802.1Q-2005 implementation)
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-2005	Spanning Tree (STP), Rapid Spanning Tree (RSTP), Multiple Spanning Tree (MSTP)
IEEE 802.1X	Port Authentication
IEEE 802.3-2002	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3at-2009	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 Copyright integrierter Software

A.5.1 Bouncy Castle Crypto APIs (Java)

The Legion Of The Bouncy Castle
Copyright (c) 2000 - 2004 The Legion Of The Bouncy Castle
(<http://www.bouncycastle.org>)

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A.5.2 Broadcom Corporation

(c) Copyright 1999-2012 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"/>				
Lesbarkeit	<input type="radio"/>				
Verständlichkeit	<input type="radio"/>				
Beispiele	<input type="radio"/>				
Aufbau	<input type="radio"/>				
Vollständigkeit	<input type="radio"/>				
Grafiken	<input type="radio"/>				
Zeichnungen	<input type="radio"/>				
Tabellen	<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

8			
802.1D/p-Mapping	77		
A			
ACA	120		
AF	81		
Aging Time	60		
Alarm	120		
Anforderungsintervall (SNTP)	55, 55		
Assured Forwarding	81		
AutoConfiguration Adapter	120		
B			
Bericht	122		
C			
CLI	128		
CLI-Zugriff, Passwort	42		
Cable-Crossing	28		
Class Selector	80		
Command Line Interface	128		
D			
DHCP Option 82	126		
DHCP-Relay-Agent	126		
DIP-Schalter	87		
DSCP	71		
Diagnose	103		
DiffServ	71		
E			
EF	80		
Empfangsleistungs-Status	108		
Empfangsleistungs-Status (Quelle für Alarme)	120		
Ereignis-Log	104		
Erweitert	125		
Expedited Forwarding	80		
F			
FAQ	141		
Filter für MAC-Adressen	61		
Firmware-Update	25		
Forward Delay	97		
G			
General	17		
Gerätstatus	18, 18, 113		
H			
HIPER-Ring (Quelle für Alarme)	120		
HIPER-Ring konfigurieren	86		
Hello Time	97		
HiVision	7		
I			
IGMP-Einstellungen	64		
IGMP-Querier	64		
IGMP-Snooping	64		
IP-DSCP Wert	72		
IP-DSCP-Mapping	71, 80		
J			
Java Runtime Environment	11		
K			
Kaltstart	38		
Kaltstart (nach Software-Update)	26		
L			
Leserecht	13		
Lieferzustand wiederherstellen	33		
Login	12		
M			
MRP-Ring konfigurieren	90		
Max Age	98		
Medienmodul (bei modularen Geräten), Quelle für Alarme	120		
Meldekontakt	116		
Meldekontakt (Quelle für Alarm)	120		
Message URL http://myHostName/base/ system/event_log.html	122		
Message URL http://myHostName/base/ system/systemInfo.html	122		
N			
Netzlast	93, 106		
Neustart	38		
O			
Option 82	126		
P			
PTP	57		
Passwort	13, 43		
Passwort für CLI-Zugriff	42		
Passwort für SNMPv3-Zugriff	42		

Passwort für Zugriff mit Web-based Interface		Schulungsangebote	141
	42	Selbsttest	123
Per-Hop-Behavior (PHB)	80	Sicherheit	41
Port-Mirroring	111	Software-Update	25
Port-Priorität	75, 76	Statistiktafel	105
Port-Statistiken	105	Switching	59
Port-Zustand (Link)	28	Switching Global Dialog	60
Portkonfiguration	28	Symbol	9
Portkonfiguration (QoS/Priorität)	75	Systemzeit	55
Ports	105		
Precedence	80	T	
Precision Time Protocol	57	Technische Fragen	141
Prioritäts-Queue	73	Temperatur (SFPs)	108
		ToS	71
Q		Trap	120
QoS/Priorität	71	Trust Modus	73
		TrustDot1p (globaler Trust-Modus)	73
R		TrustIpDscp (globaler Trust-Modus)	73
RAM-Test	123	Type-of-Service	71
RFC	131		
RMON-Probe	111	U	
RSTP	93	Uhr	57
Rapid Spanning Tree	93	Untrusted (globaler Trust-Modus)	73
Rapid Spanning Tree Dialog	93		
Rapid-Spanning-Tree Port Protokoll	100	V	
Reboot	38	VLAN-Mapping	71
Redundante Kopplung	83, 115	VLAN-Priorität	71
Redundante Verbindungen	93	Verbindungs-Zustand (Link)	28
Redundanz	83	Versorgungsspannung	120
Redundanzfunktion	83	Voreinstellungen wiederherstellen	33
Redundanzmanager	84		
Ring	84	W	
Ring-/Netzkopplung	115	Web Site	13, 14
Ring-/Netzkopplung (Quelle für Alarmer)	120	Web-Zugriff	48
Ring-Redundanz	83	Web-based Interface	11
Ring-Redundanz Basiskonfiguration	85	Web-based Management	12
Ringmanager	84		
Ringport	86	Z	
Ringstruktur	84	Zeit	51, 51
Root-Bridge	94	Zeitmanagement	57
		Zugriff mit Web-based Interface, Passwort	42
S			
SFP-Modul	108		
SFP-Modul (Quelle für Alarmer)	120		
SFP-Zustandsanzeige	108		
SNMPv1/v2 Zugriffs-Einstellungen	45		
SNMPv3-Zugriff, Passwort	42		
SNTP	53		
SNTP-Anfrage	53		
SNTP-Broadcast akzeptieren	55		
SNTP-Broadcasts	55		
SNTP-Client	53, 53		
SNTP-Server	53, 53		
Schreibrecht	13		

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