



HIRSCHMANN

A **BELDEN** BRAND

Hirschmann Automation and Control GmbH

EES HiOS-2E Rel. 07000

Referenz-Handbücher

Grafische Benutzeroberfläche

Command Line Interface

Anwender-Handbuch

Konfiguration



HIRSCHMANN

A **BELDEN** BRAND

Referenz-Handbuch

Grafische Benutzeroberfläche HiOS-2E EES (Embedded Ethernet Switch)

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.

© 2017 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.

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

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

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

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

Inhalt

Sicherheitshinweise	9
Über dieses Handbuch	11
Legende	13
Hinweise zur grafischen Benutzeroberfläche	15
1 Grundeinstellungen	21
1.1 System	22
1.2 Netz	25
Global	26
MAC-Konfiguration	29
1.3 Software	30
1.4 Laden/Speichern	32
1.5 Port	40
Konfiguration	41
Statistiken	45
Netzlast	47
1.6 Neustart	48
2 Zeit	49
2.1 Grundeinstellungen	50
Global	51
Sommerzeit	52
2.2 IRIG-B/PPS	55
IRIG-B	56
PPS	58
2.3 SNTP	59
2.3.1 SNTP Client	60
2.3.2 SNTP Server	63
2.4 PTP	65
2.4.1 PTP Global	66
2.4.2 PTP Boundary Clock	68
2.4.2.1 PTP Boundary Clock Global	69
2.4.2.2 PTP Boundary Clock Port	72
2.4.3 PTP Transparent Clock	75
2.4.3.1 PTP Transparent Clock Global	76
2.4.3.2 PTP Transparent Clock Port	79
3 Gerätesicherheit	81
3.1 Benutzerverwaltung	82

3.2	Authentifizierungs-Liste	86
3.3	Management-Zugriff	89
3.3.1	Server	90
	Information	91
	SNMP	93
	Telnet	95
	SSH	96
	HTTP	99
	HTTPS	100
3.3.2	IP-Zugriffsbeschränkung	103
3.3.3	Web	106
3.3.4	Command Line Interface	107
	Global	108
	Login-Banner	109
3.3.5	SNMPv1/v2 Community	110
3.4	Pre-Login-Banner	111
4	Netzsicherheit	113
4.1	Port-Sicherheit	114
	Wizard : Port-Sicherheit	117
4.2	802.1X Port-Authentifizierung	119
4.2.1	802.1X Global	120
4.2.2	802.1X Port-Konfiguration	122
4.2.3	802.1X Port-Clients	125
4.2.4	802.1X EAPOL-Portstatistiken	126
4.2.5	802.1X Port-Authentifizierung-Historie	127
4.2.6	802.1X Integrierter Authentifikations-Server	129
4.3	RADIUS	130
4.3.1	RADIUS Global	131
4.3.2	RADIUS Authentication-Server	132
4.3.3	RADIUS Accounting-Server	134
4.3.4	RADIUS Authentication Statistiken	135
4.3.5	RADIUS Accounting-Statistiken	136
4.4	DoS	137
4.4.1	DoS-Global	138
5	Switching	141
5.1	Switching Global	142
5.2	Lastbegrenzer	144
5.3	Filter für MAC-Adressen	146
5.4	IGMP-Snooping	148
5.4.1	IGMP-Snooping Global	149
5.4.2	IGMP-Snooping Konfiguration	150

VLAN-ID	151
Port	152
5.4.3 IGMP-Snooping Erweiterungen	154
Wizard : Selection VLAN/Port	156
5.4.4 IGMP Snooping-Querier	157
5.4.5 IGMP Snooping Multicasts	159
5.5 MRP-IEEE	160
5.5.1 MRP-IEEE Konfiguration	161
5.5.2 MRP-IEEE Multiple MAC Registration Protocol	162
Konfiguration	163
Service-Requirement	165
Statistiken	166
5.5.3 MRP-IEEE Multiple VLAN Registration Protocol	167
Konfiguration	168
Statistiken	170
5.6 QoS/Priorität	171
5.6.1 QoS/Priorität Global	172
5.6.2 QoS/Priorität Port-Konfiguration	173
5.6.3 802.1D/p Zuweisung	174
5.6.4 IP-DSCP-Zuweisung	175
5.6.5 Queue-Management	177
5.7 VLAN	178
5.7.1 VLAN Global	179
5.7.2 VLAN Konfiguration	180
5.7.3 VLAN Port	182
5.8 L2-Redundanz	183
5.8.1 MRP	184
5.8.2 PRP	187
5.8.2.1 PRP Konfiguration	188
5.8.2.2 DAN/VDAN-Tabelle	191
5.8.2.3 Proxy-Node-Tabelle	192
5.8.2.4 PRP Statistiken	193
5.8.3 HSR	194
5.8.3.1 HSR Konfiguration	195
5.8.3.2 DAN/VDAN-Tabelle	198
5.8.3.3 Proxy-Node-Tabelle	199
5.8.3.4 HSR Statistiken	200
5.8.4 Spanning Tree	201
5.8.4.1 Spanning Tree Global	202
5.8.4.2 Spanning Tree Port	207
CIST	208
Guards	212

5.8.5	Link-Aggregation	214
5.8.6	Link-Backup	219
6	Diagnose	223
6.1	Statuskonfiguration	224
6.1.1	Gerätestatus	225
	Global	226
	Port	228
	Status	229
6.1.2	Sicherheitsstatus	230
	Global	231
	Port	235
	Status	236
6.1.3	Alarmer (Traps)	237
6.2	System	238
6.2.1	Systeminformationen	239
6.2.2	Hardware-Zustand	240
6.2.3	Konfigurations-Check	241
6.2.4	IP-Adressen Konflikterkennung	243
6.2.5	ARP	246
6.2.6	Selbsttest	247
6.3	Syslog	249
6.4	Ports	251
6.4.1	SFP	252
6.4.2	Port-Monitor	253
	Global	254
	Auto-Disable	257
	Link-Änderungen	258
	CRC/Fragmente	259
	Überlast-Erkennung	260
	Link-Speed-/Duplex-Mode-Erkennung	261
6.4.3	Auto-Disable	263
	Port	263
	Status	265
6.4.4	Port-Mirroring	266
6.5	LLDP	269
6.5.1	LLDP Konfiguration	270
6.5.2	LLDP Topologie-Erkennung	273
6.6	Bericht	275
6.6.1	Bericht Global	276
6.6.2	System Log	280
6.6.3	Audit Trail	281

7	Erweitert	283
7.1	Industrie-Protokolle	284
7.1.1	IEC61850-MMS	285
7.1.2	Modbus TCP	287
7.1.3	PROFINET	289
7.1.4	EtherNet/IP	291
A	Index	293
B	Weitere Unterstützung	295
C	Leserkritik	296

Sicherheitshinweise

WARNUNG

UNKONTROLLIERTE MASCHINENBEWEGUNGEN

Um unkontrollierte Maschinenbewegungen aufgrund von Datenverlust zu vermeiden, konfigurieren Sie alle Geräte zur Datenübertragung individuell.

Nehmen Sie eine Maschine, die mittels Datenübertragung gesteuert wird, erst in Betrieb, wenn Sie alle Geräte zur Datenübertragung vollständig konfiguriert haben.

Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.

Über dieses Handbuch

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

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

Das Referenz-Handbuch „Grafische Benutzeroberfläche“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Geräts über die grafische Oberfläche.

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

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

- ▶ Autotopologie-Erkennung
- ▶ Browser-Interface
- ▶ Client/Server-Struktur
- ▶ Ereignisbehandlung
- ▶ Ereignisprotokoll
- ▶ Gleichzeitige Konfiguration mehrerer Geräte
- ▶ Grafische Benutzeroberfläche mit Netz-Layout
- ▶ SNMP/OPC-Gateway

Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
□	Arbeitsschritt
■	Zwischenüberschrift
Verweis	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
<code>Courier</code>	ASCII-Darstellung in der grafischen Benutzeroberfläche

Hinweise zur grafischen Benutzeroberfläche

Die grafische Benutzeroberfläche des Geräts ist wie folgt unterteilt:

- ▶ Navigationsbereich
- ▶ Dialogbereich
- ▶ Schaltflächen

Navigationsbereich

Der Navigationsbereich befindet sich auf der linken Seite der grafischen Benutzeroberfläche.

Der Navigationsbereich enthält die folgenden Elemente:





- ▶ Symbolleiste
- ▶ Filter
- ▶ Menü




Sie haben die Möglichkeit, den Navigationsbereich zuzuklappen, zum Beispiel wenn Sie die grafische Benutzeroberfläche auf kleinen Bildschirmen anzeigen. Zum Zu- oder Aufklappen klicken Sie den kleinen Pfeil am oberen Rand des Navigationsbereichs.

■ Symbolleiste

Die Symbolleiste am oberen Rand des Navigationsbereichs enthält mehrere Schaltflächen.

- Wenn Sie den Mauszeiger über einer Schaltfläche positionieren, zeigt ein Tooltip weitere Informationen.
- Wenn die Verbindung zum Gerät unterbrochen ist, dann ist die Symbolleiste ausgegraut.

Schaltfläche	Bedeutung
	Das Gerät aktualisiert die Informationen in der Symbolleiste automatisch alle 5 Sekunden. Klicken Sie die Schaltfläche, um die Symbolleiste manuell zu aktualisieren.
	Wenn Sie den Mauszeiger über der Schaltfläche positionieren, zeigt ein Tooltip die folgenden Informationen: <ul style="list-style-type: none"> ▶ <i>Benutzer:</i> Bezeichnung des angemeldeten Benutzers ▶ <i>Gerätename:</i> Bezeichnung des Geräts Klicken Sie die Schaltfläche, um den Dialog <i>Gerätesicherheit > Benutzerverwaltung</i> zu öffnen.
	Wenn Sie den Mauszeiger über der Schaltfläche positionieren, zeigt ein Tooltip die Zusammenfassung des Dialogs <i>Diagnose > System > Konfigurations-Check</i> . Klicken Sie die Schaltfläche, um den Dialog <i>Diagnose > System > Konfigurations-Check</i> zu öffnen.
	Klicken Sie die Schaltfläche, um den gegenwärtig angemeldeten Benutzer abzumelden und die Login-Seite anzuzeigen.

Schaltfläche	Bedeutung
	<p>Zeigt die verbleibende Zeit in Sekunden, bis das Gerät einen inaktiven Benutzer automatisch abmeldet.</p> <p>Klicken Sie die Schaltfläche, um den Dialog <i>Gerätesicherheit > Management-Zugriff > Web</i> zu öffnen. Dort können Sie das Timeout festlegen.</p>
	<p>Diese Schaltfläche ist sichtbar, wenn das Konfigurationsprofil im flüchtigen Speicher (RAM) und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (NVM) sich unterscheiden. Andernfalls ist die Schaltfläche unsichtbar.</p> <p>Klicken Sie die Schaltfläche, um den Dialog <i>Grundeinstellungen > Laden/Speichern</i> zu öffnen.</p> <p>Mit einem Rechtsklick auf die Schaltfläche können Sie die gegenwärtigen Einstellungen im permanenten Speicher (NVM) speichern.</p>
	<p>Wenn Sie den Mauszeiger über der Schaltfläche positionieren, zeigt ein Tooltip die folgenden Informationen:</p> <ul style="list-style-type: none"> ▶ Gerätestatus: Dieser Abschnitt zeigt eine komprimierte Ansicht des Rahmens <i>Gerätestatus</i> im Dialog <i>Grundeinstellungen > System</i>. Der Abschnitt zeigt den zeitlich zuerst aufgetretenen, gegenwärtig noch andauernden Alarm. ▶ Sicherheitsstatus: Dieser Abschnitt zeigt eine komprimierte Ansicht des Rahmens <i>Sicherheits-Status</i> im Dialog <i>Grundeinstellungen > System</i>. Der Abschnitt zeigt den zeitlich zuerst aufgetretenen, gegenwärtig noch andauernden Alarm. ▶ Boot-Parameter: Wenn Sie geänderte Einstellungen permanent speichern und sich mindestens ein Boot-Parameter von dem beim letzten Neustart verwendeten Konfigurationsprofil unterscheidet, dann zeigt dieser Abschnitt einen Hinweis. Folgende Einstellungen rufen eine Änderung der Boot-Parameter hervor: <ul style="list-style-type: none"> – Dialog <i>Grundeinstellungen > Netz</i>, Registerkarte <i>MAC-Konfiguration</i>, Parameter <i>Lokale Administrator-MAC-Adresse</i> – Dialog <i>Gerätesicherheit > Management-Zugriff > Server</i>, Registerkarte <i>SNMP</i>, Parameter <i>UDP-Port</i> – Dialog <i>Diagnose > System > Selbsttest</i>, Parameter <i>RAM test</i> – Dialog <i>Diagnose > System > Selbsttest</i>, Parameter <i>SysMon1 ist verfügbar</i> – Dialog <i>Diagnose > System > Selbsttest</i>, Parameter <i>Bei Fehler Default-Konfiguration laden</i> <p>Klicken Sie die Schaltfläche, um den Dialog <i>Diagnose > Statuskonfiguration > Gerätestatus</i> zu öffnen.</p>

Filter

Der Filter bietet Ihnen die Möglichkeit, die Anzahl der Menüpunkte im Menü zu reduzieren. Während des Filterns zeigt das Menü ausschließlich diejenigen Menüpunkte, die den im Filterfeld eingegebenen Suchbegriff enthalten.

■ Menü

Das Menü zeigt die Menüpunkte.

Sie haben die Möglichkeit, die Menüpunkte zu filtern. Siehe Abschnitt „[Filter](#)“.

Um den zugehörigen Dialog im Dialogbereich anzuzeigen, klicken Sie den gewünschten Menüpunkt. Wenn der ausgewählte Menüpunkt ein Knoten ist, der untergeordnete Menüpunkte enthält, dann klappt der Knoten beim Klicken auf oder zu. Der Dialogbereich zeigt weiterhin den zuvor angezeigten Dialog.

Sie haben die Möglichkeit, jeden Knoten im Menü gleichzeitig auf- oder zuzuklappen. Wenn Sie an beliebiger Stelle im Menü rechtsklicken, zeigt ein Kontextmenü die folgenden Einträge:

▶ **Aufklappen**

Klappt jeden Knoten im Menü gleichzeitig auf. Das Menü zeigt die Menüpunkte jeder Ebene.

▶ **Zuklappen**


Klappt jeden Knoten im Menü gleichzeitig zu. Das Menü zeigt die Menüpunkte der obersten Ebene.

Dialogbereich




Der Dialogbereich befindet sich auf der rechten Seite der grafischen Benutzeroberfläche. Wenn Sie im Navigationsbereich einen Menüpunkt klicken, zeigt der Dialogbereich den zugehörigen Dialog.

■ Anzeige aktualisieren

Wenn ein Dialog über längere Zeit geöffnet ist, dann kann es vorkommen, dass sich die Werte im Gerät inzwischen geändert haben.

- Um die Anzeige im Dialog zu aktualisieren, klicken Sie die Schaltfläche . Ungespeicherte Änderungen im Dialog gehen dabei verloren.

■ Einstellungen speichern

- Um geänderte Einstellungen in den flüchtigen Speicher (RAM) des Geräts zu übertragen, klicken Sie die Schaltfläche .
- Damit geänderte Einstellungen auch nach dem Neustart des Geräts erhalten bleiben, gehen Sie wie folgt vor:
 - Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
 - Markieren Sie in der Tabelle das gewünschte Konfigurationsprofil.
 - Wenn in Spalte *Ausgewählt* das Kontrollkästchen noch unmarkiert ist, klicken Sie die Schaltfläche  und dann den Eintrag *Auswählen*.
 - Klicken Sie die Schaltfläche  und dann den Eintrag *Speichern*.

Anmerkung: Unbeabsichtigte Änderungen an den Einstellungen führen möglicherweise zum Verbindungsabbruch zwischen Ihrem PC und dem Gerät. Damit das Gerät erreichbar bleibt, schalten Sie die Funktion *Konfigurationsänderungen rückgängig machen* im Dialog *Grundeinstellungen > Laden/Speichern* ein, bevor Sie Einstellungen ändern. Mit der Funktion prüft das Gerät kontinuierlich, ob es von der IP-Adresse dieses Benutzers erreichbar bleibt. Bricht die Verbindung ab, lädt das Gerät nach der festgelegten Zeit das im permanenten Speicher (*Grundeinstellungen > Laden/Speichern*) gespeicherte Konfigurationsprofil. Danach ist das Gerät wieder erreichbar.

■ Arbeiten mit Tabellen

Die Dialoge zeigen zahlreiche Einstellungen in tabellarischer Form.

Wenn Sie eine Tabellenzelle ändern, zeigt die Tabellenzelle eine rote Markierung in der linken oberen Ecke. Die rote Markierung weist darauf hin, dass Ihre Änderungen noch nicht in den flüchtigen Speicher (RAM) des Geräts übertragen sind.

Sie haben die Möglichkeit, das Erscheinungsbild der Tabellen an Ihre Bedürfnisse anzupassen. Wenn Sie den Mauszeiger über einer Spaltenüberschrift positionieren, zeigt die Spaltenüberschrift die Schaltfläche einer Dropdown-Liste. Wenn Sie diese Schaltfläche klicken, zeigt die Dropdown-Liste die folgenden Einträge:








- ▶ Aufsteigend sortieren
Sortiert die Tabelleneinträge in aufsteigender Reihenfolge basierend auf den Einträgen der ausgewählten Spalte.
Sortierte Tabelleneinträge erkennen Sie an einem Pfeil in der Spaltenüberschrift.
- ▶ Absteigend sortieren
Sortiert die Tabelleneinträge in absteigender Reihenfolge basierend auf den Einträgen der ausgewählten Spalte.
Sortierte Tabelleneinträge erkennen Sie an einem Pfeil in der Spaltenüberschrift.
- ▶ Spalten
Blendet Spalten ein oder aus.
Ausgeblendete Spalten erkennen Sie an einem unmarkierten Kontrollkästchen in der Dropdown-Liste.
- ▶ Filter
Die Tabelle zeigt ausschließlich die Einträge, deren Inhalt mit den festgelegten Filterkriterien der ausgewählten Spalte übereinstimmt.
Gefilterte Tabelleneinträge erkennen Sie an einer hervorgehobenen Spaltenüberschrift.

Sie haben die Möglichkeit, mehrere Tabelleneinträge gleichzeitig zu markieren, um anschließend eine Aktion darauf anzuwenden. Dies ist nützlich, wenn Sie mehrere Tabelleneinträge gleichzeitig entfernen möchten.

- ▶ Mehrere aufeinander folgende Tabelleneinträge auswählen:
 - Klicken Sie den ersten gewünschten Tabelleneintrag, um diesen zu markieren.
 - Drücken und halten Sie die <SHIFT>-Taste.
 - Klicken Sie den letzten gewünschten Tabelleneintrag, um jeden gewünschten Tabelleneintrag zu markieren.
- ▶ Mehrere einzelne Tabelleneinträge markieren:
 - Klicken Sie den ersten gewünschten Tabelleneintrag, um diesen zu markieren.
 - Drücken und halten Sie die <STRG>-Taste.
 - Klicken Sie den nächsten gewünschten Tabelleneintrag, um diesen zu markieren.
Wiederholen Sie, bis jeder gewünschte Tabelleneintrag markiert ist.

Schaltflächen

Hier finden Sie die Beschreibung der Standard-Schaltflächen. Spezielle, Dialog-spezifische Schaltflächen sind im Hilfetext des zugehörigen Dialogs beschrieben.

Schaltfläche	Bedeutung
	Überträgt die Änderungen in den flüchtigen Speicher (RAM) des Geräts und wendet diese an. Um die Änderungen im permanenten Speicher zu speichern, gehen Sie wie folgt vor: <ul style="list-style-type: none"> <input type="checkbox"/> Öffnen Sie den Dialog <i>Grundeinstellungen > Laden/Speichern</i>. <input type="checkbox"/> Markieren Sie in der Tabelle das gewünschte Konfigurationsprofil. <input type="checkbox"/> Wenn in Spalte <i>Ausgewählt</i> das Kontrollkästchen noch unmarkiert ist, klicken Sie die Schaltfläche  und dann den Eintrag <i>Auswählen</i>. <input type="checkbox"/> Klicken Sie die Schaltfläche  und dann den Eintrag <i>Speichern</i>.
	Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (RAM) des Geräts gespeichert sind.
	Fügt einen neuen Tabelleneintrag hinzu.
	Entfernt den markierten Tabelleneintrag.
	Öffnet die Online-Hilfe.

1 Grundeinstellungen

Das Menü enthält die folgenden Dialoge:

- ▶ System
- ▶ Netz
- ▶ Software
- ▶ Laden/Speichern
- ▶ Port
- ▶ Neustart


1.1 System

In diesem Dialog überwachen Sie einzelne Betriebszustände.

■ Geräte-Status

Die Felder in diesem Rahmen zeigen den Gerätstatus und informieren über aufgetretene Alarme. Der Rahmen ist hervorgehoben, wenn gegenwärtig ein Alarm vorhanden ist.


Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose* > Statuskonfiguration > Gerätestatus .

Parameter	Bedeutung
Anzahl Alarme	Zeigt die Anzahl der gegenwärtig vorhandenen Alarme.
	Das Symbol ist sichtbar, wenn mindestens ein Alarm gegenwärtig vorhanden ist. Wenn Sie den Mauszeiger über dem Symbol positionieren, zeigt ein Tooltip die Ursache der gegenwärtig vorhandenen Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat. Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht. Der Dialog <i>Diagnose</i> > <i>Statuskonfiguration</i> > <i>Gerätestatus</i> , Registerkarte <i>Status</i> zeigt die Alarme im Überblick.

■ Sicherheits-Status

Die Felder in diesem Rahmen zeigen den Sicherheitsstatus und informieren über aufgetretene Alarme. Der Rahmen ist hervorgehoben, wenn gegenwärtig ein Alarm vorhanden ist.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose* > Statuskonfiguration > Sicherheitsstatus .

Parameter	Bedeutung
Anzahl Alarme	Zeigt die Anzahl der gegenwärtig vorhandenen Alarme.
	Das Symbol ist sichtbar, wenn mindestens ein Alarm gegenwärtig vorhanden ist. Wenn Sie den Mauszeiger über dem Symbol positionieren, zeigt ein Tooltip die Ursache der gegenwärtig vorhandenen Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat. Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht. Der Dialog <i>Diagnose</i> > <i>Statuskonfiguration</i> > <i>Sicherheitsstatus</i> , Registerkarte <i>Status</i> zeigt die Alarme im Überblick.

■ Systemdaten








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

Parameter	Bedeutung
Systemname	<p>Legt den Namen fest, unter dem das Gerät im Netz bekannt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen Die folgenden Zeichen sind zulässig: <ul style="list-style-type: none"> - 0..9 - a..z - A..Z - !#\$%&'()*+,-./:;<=>?@[\\]^_`{ }~ - <Gerätename>-<MAC-Adresse> (Voreinstellung) <p>Beim Erzeugen von HTTPS-X.509-Zertifikaten verwendet die Applikation, die das Zertifikat generiert, den festgelegten Wert als Domain-Namen und als gemeinsamen Namen.</p> <p>Die folgenden Funktionen verwenden den festgelegten Wert als Hostnamen oder FQDN (Fully Qualified Domain Name). Für die Kompatibilität ist es empfehlenswert, nur Kleinbuchstaben zu verwenden, da nicht jedes System zwischen Groß- und Kleinschreibung im FQDN unterscheidet. Vergewissern Sie sich, dass dieser Name im gesamten Netz eindeutig ist.</p> <ul style="list-style-type: none"> ▶ DHCP-Client ▶ <i>Syslog</i> ▶ <i>IEC61850-MMS</i> ▶ <i>PROFINET</i> <p>Anmerkung: Für die Kompatibilität in PROFINET-Umgebungen legen Sie den PROFINET-Gerätenamen fest. In PROFINET ist der Name auf maximal 240 Zeichen begrenzt. Der Name darf nicht mit einer Ziffer beginnen. Programme lesen den Gerätenamen unter Verwendung von SNMP und PROFINET DCP.</p>
Standort	<p>Legt den Standort des Geräts fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
Ansprechpartner	<p>Legt den Ansprechpartner für dieses Gerät fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
Gerätetyp	Zeigt die Produktbezeichnung des Geräts.
Netzteil 1 Netzteil 2	<p>Zeigt den Status des Netzteils am betreffenden Spannungsversorgungs-Anschluss.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ vorhanden ▶ defekt ▶ nicht vorhanden ▶ unbekannt
Betriebszeit	<p>Zeigt die Zeit, die seit dem letzten Neustart dieses Geräts vergangen ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Zeit im Format Tag(e), ...h ...m ...s
Obere Temp.- Grenze [°C]	<p>Legt die obere Temperaturgrenze in °C fest.</p> <p>Das Anwender-Handbuch „Installation“ enthält ausführliche Informationen zum Festlegen der Temperaturgrenzen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ -99..99 (ganze Zahl) <p>Überschreitet die Temperatur im Gerät diesen Wert, generiert das Gerät einen Alarm.</p>
Untere Temp.- Grenze [°C]	<p>Legt die untere Temperaturgrenze in °C fest.</p> <p>Das Anwender-Handbuch „Installation“ enthält ausführliche Informationen zum Festlegen der Temperaturgrenzen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ -99..99 (ganze Zahl) <p>Unterschreitet die Temperatur im Gerät diesen Wert, generiert das Gerät einen Alarm.</p>

■ Status Port

Dieser Rahmen zeigt eine vereinfachte Ansicht der Ports des Geräts zum Zeitpunkt der letzten Aktualisierung.

Die Symbole stellen den Zustand der einzelnen Ports dar. In manchen Situationen überlagern sich die folgenden Symbole. Wenn Sie den Mauszeiger über dem entsprechenden Port-Symbol positionieren, zeigt ein Tooltip detaillierte Informationen zum Port-Status.

Parameter	Status	Bedeutung
<Port-Nummer>		Der Port ist inaktiv. Der Port sendet und empfängt keine Daten.
		Der Port ist inaktiv. Das Kabel ist verbunden. Aktiver Link.
		Der Port ist aktiv. Kein Kabel angesteckt oder kein aktiver Link.
		Der Port ist aktiv. Das Kabel ist verbunden. Verbindung in Ordnung. Aktiver Link. Vollduplex-Modus
		Die Halbduplex-Modus ist eingeschaltet. Prüfen Sie die Einstellungen im Dialog <i>Grundeinstellungen > Ports</i> , Registerkarte <i>Konfiguration</i> .
		Der Port ist aufgrund einer Redundanzfunktion im "blocking"-Zustand.
		Der Port arbeitet als Router-Interface.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

1.2 Netz

Dieser Dialog bietet Ihnen die Möglichkeit, die für den Zugriff über das Netz auf das Management des Geräts erforderlichen IP-, VLAN- und HiDiscovery-Einstellungen festzulegen.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [\[Global\]](#)
- ▶ [\[MAC-Konfiguration\]](#)

[Global]

Diese Registerkarte bietet Ihnen die Möglichkeit, die IP-, VLAN- und HiDiscovery-Einstellungen festzulegen.

■ Management-Schnittstelle

Dieser Rahmen bietet Ihnen die Möglichkeit, die folgenden Einstellungen festzulegen:

- ▶ Quelle, aus der das Management des Geräts seine IP-Parameter erhält
- ▶ VLAN, in dem das Management erreichbar ist

Parameter	Bedeutung
Zuweisung IP-Adresse	<p>Legt fest, aus welcher Quelle das Gerät nach dem Starten seine IP-Parameter erhält.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ Lokal (Voreinstellung) Das Gerät verwendet die IP-Parameter aus dem internen Speicher. Die Einstellungen dafür legen Sie im Rahmen <i>IP-Parameter</i> fest.▶ BOOTP Das Gerät erhält seine IP-Parameter von einem BOOTP- oder DHCP-Server. Der Server wertet die MAC-Adresse des Geräts aus und weist daraufhin die IP-Parameter zu.▶ DHCP Das Gerät erhält seine IP-Parameter von einem DHCP-Server. Der Server wertet die MAC-Adresse, den DHCP-Namen oder andere Parameter des Geräts aus und weist daraufhin die IP-Parameter zu. <p>Anmerkung: Bleibt die Antwort des BOOTP- oder DHCP-Servers aus, setzt das Gerät die IP-Adresse auf 0.0.0.0 und versucht erneut, eine gültige IP-Adresse zu erhalten.</p>
VLAN-ID	<p>Legt das VLAN fest, in dem das Management des Geräts über das Netz erreichbar ist. Das Management ist ausschließlich über Ports erreichbar, die Mitglied dieses VLANs sind.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 1..4042 (Voreinstellung: 1) Voraussetzung ist, dass das VLAN bereits eingerichtet ist. Siehe Dialog <i>Switching > VLAN > Konfiguration</i>. <p>Wenn Sie nach Ändern des Werts die Schaltfläche <input checked="" type="checkbox"/> klicken, öffnet sich der Dialog <i>Information</i>. Wählen Sie den Port aus, über den Sie die Verbindung zum Gerät zukünftig herstellen. Nach Klicken der Schaltfläche <i>Ok</i> sind die Einstellungen des neuen Management-VLANs dem Port zugewiesen.</p> <ul style="list-style-type: none">– Der Port wird Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag (untagged). Siehe Dialog <i>Switching > VLAN > Konfiguration</i>.– Das Gerät weist dem Port die Port-VLAN-ID des neuen Management-VLANs zu. Siehe Dialog <i>Switching > VLAN > Port</i>. <p>Nach kurzer Wartezeit ist das Gerät über den neuen Port im neuen Management-VLAN erreichbar.</p>
MAC-Adresse	<p>Zeigt die MAC-Adresse des Geräts. Mit der MAC-Adresse ist das Management des Geräts über das Netz erreichbar.</p>

■ BOOTP/DHCP

Parameter	Bedeutung
Client-ID	<p>Zeigt die DHCP-Client-ID, die das Gerät an den BOOTP- oder DHCP-Server sendet. Eine entsprechende Konfiguration des Servers vorausgesetzt, reserviert der Server eine IP-Adresse für diese DHCP-Client-ID. Demzufolge erhält das Gerät bei jeder Anfrage dieselbe IP-Adresse vom Server.</p> <p>Das Gerät sendet als DHCP-Client-ID den Gerätenamen, der im Feld <i>Systemname</i> im Dialog <i>Grundeinstellungen > System</i> festgelegt ist.</p>

■ HiDiscovery Protokoll v1/v2

Dieser Rahmen bietet Ihnen die Möglichkeit, Einstellungen für den Zugriff auf das Gerät per HiDiscovery-Protokoll festzulegen.

Auf einem PC zeigt Ihnen die HiDiscovery-Software im Netz erreichbare Hirschmann-Geräte, auf denen die HiDiscovery-Funktion eingeschaltet ist. Sie erreichen die Geräte sogar dann, wenn ihnen ungültige oder keine IP-Parameter zugewiesen sind. Die HiDiscovery-Software bietet Ihnen die Möglichkeit, die IP-Parameter im Gerät zuzuweisen oder zu ändern.

Parameter	Bedeutung
Funktion	<p>Schaltet die HiDiscovery-Funktion im Gerät ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An (Voreinstellung) HiDiscovery ist eingeschaltet. Sie haben die Möglichkeit, das Gerät mit der HiDiscovery-Software von Ihrem PC aus zu erreichen. ▶ Aus HiDiscovery ist ausgeschaltet.
Zugriff	<p>Schaltet den Schreibzugriff auf das Gerät per HiDiscovery ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ readWrite (Voreinstellung) Die HiDiscovery-Software erhält Schreibzugriff auf das Gerät. Mit dieser Einstellung haben Sie die Möglichkeit, die IP-Parameter im Gerät zu ändern. ▶ readOnly Die HiDiscovery-Software erhält ausschließlich Lesezugriff auf das Gerät. Mit dieser Einstellung haben Sie die Möglichkeit, die IP-Parameter im Gerät anzusehen. <p>Empfehlung: Ändern Sie erst nach Inbetriebnahme des Geräts die Einstellung auf <code>readOnly</code>.</p>
Signal	<p>Aktiviert/deaktiviert das Blinken der Port-LEDs wie die gleichnamige Funktion in der HiDiscovery-Software. Diese Funktion bietet Ihnen die Möglichkeit, das Gerät im Feld zu identifizieren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Das Blinken der Port-LEDs ist aktiv. Die Port-LEDs blinken solange, bis Sie die Funktion wieder ausschalten. ▶ unmarkiert (Voreinstellung) Das Blinken der Port-LEDs ist inaktiv.

Anmerkung: Mit der HiDiscovery-Software erreichen Sie das Gerät ausschließlich über Ports, die Mitglied desselben VLANs sind wie das Management des Geräts. Welchem Port welches VLAN zugewiesen ist, legen Sie fest im Dialog *Switching > VLAN > Konfiguration*.

■ IP-Parameter

Dieser Rahmen bietet Ihnen die Möglichkeit, die IP-Parameter manuell zuzuweisen. Die Felder sind editierbar, wenn Sie im Rahmen *Zuweisung IP-Adresse*, Optionsliste *Zuweisung IP-Adresse* das Optionsfeld `Lokal` auswählen.

Parameter	Bedeutung
IP-Adresse	Legt die IP-Adresse fest, unter der das Management des Geräts über das Netz erreichbar ist. Mögliche Werte: ▶ Gültige IPv4-Adresse (Voreinstellung: 192.168.1.1)
Netzmaske	Legt die Netzmaske fest. Die Netzmaske kennzeichnet in der IP-Adresse das Netzpräfix und die Host-Adresse des Geräts. Mögliche Werte: ▶ Gültige IPv4-Netzmaske (Voreinstellung: 255.255.255.0)
Gateway-Adresse	Legt die IP-Adresse eines Routers fest, über den das Gerät andere Geräte außerhalb des eigenen Netzes erreicht. Mögliche Werte: ▶ Gültige IPv4-Adresse

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[MAC-Konfiguration]

Mit den voreingestellten Werten ist der Management-Zugriff über jeden Port möglich. Diese Registerkarte bietet Ihnen die Möglichkeit, den Management-Zugriff auf über ausschließlich einen Port zu beschränken. Außerdem haben Sie die Möglichkeit, dem Management eine benutzerdefinierte MAC-Adresse zuzuweisen.

■ Konfiguration

Parameter	Bedeutung
Lokale Administrator-MAC-Adresse	<p>Legt eine benutzerdefinierte MAC-Adresse fest, mit der das Management des Geräts erreichbar ist. Wenn der hier eingefügte Wert von der Voreinstellung abweicht, verwendet das Gerät diese MAC-Adresse nach einem Neustart.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Gültige Unicast-MAC-Adresse (Voreinstellung: 00:00:00:00:00:00) Geben Sie den Wert in einem der folgenden Formate ein: <ul style="list-style-type: none"> – ohne Trennzeichen, zum Beispiel 001122334455 – Trennung mit Leerzeichen, zum Beispiel 00 11 22 33 44 55 – Trennung mit Doppelpunkt, zum Beispiel 00:11:22:33:44:55 – Trennung mit Bindestrich, zum Beispiel 00-11-22-33-44-55 – Trennung mit Punkt, zum Beispiel 00.11.22.33.44.55 – Trennung mit Punkt nach jedem 4. Zeichen, zum Beispiel 0011.2233.4455 <p>Anmerkung: Speichern Sie die Änderungen in diesem Feld im permanenten Speicher, bevor Sie das Gerät neu starten.</p>
Management-Port	<p>Legt den Port fest, über den das Management des Geräts über das Netz erreichbar ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alle (Voreinstellung) Das Management des Geräts ist über jedenPort erreichbar. ▶ <Port-Nummer> Das Management des Geräts ist ausschließlich über den ausgewählten Port erreichbar.

■ Information

Parameter	Bedeutung
Burned-In MAC-Adresse	Zeigt die durch den Hersteller vorgegebene MAC-Adresse des Geräts.
MAC-Adress-Typ	<p>Zeigt, mit welcher MAC-Adresse das Gerät erreichbar ist:</p> <ul style="list-style-type: none"> ▶ burned-in Das Management des Geräts ist mit der durch den Hersteller vorgegebenen MAC-Adresse erreichbar. ▶ lokal Das Management des Geräts ist mit der im Rahmen <i>Konfiguration</i> festgelegten, benutzerdefinierten MAC-Adresse erreichbar.
Momentan genutzte MAC-Adresse	Zeigt die MAC-Adresse, mit der das Management des Geräts erreichbar ist.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

1.3 Software

Dieser Dialog bietet Ihnen die Möglichkeit, die Geräte-Software zu aktualisieren und Informationen über die Geräte-Software anzuzeigen.

Anmerkung: Beachten Sie vor dem Aktualisieren der Geräte-Software die versionsspezifischen Hinweise in der `Liesmich`-Textdatei.

■ Version

Parameter	Bedeutung
Stored version	Zeigt Versionsnummer und Erstellungsdatum der im Flash gespeicherten Geräte-Software. Das Gerät lädt die Geräte-Software beim nächsten Neustart.
Running version	Zeigt Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Neustart geladen hat und gegenwärtig ausführt.
Bootcode	Zeigt Versionsnummer und Erstellungsdatum des Bootcodes.

■ Software-Update

Parameter	Bedeutung
URL	<p>Legt Pfad und Dateiname der Image-Datei fest, mit der Sie die Geräte-Software aktualisieren.</p> <p>Das Gerät bietet Ihnen folgende Möglichkeiten, die Geräte-Software zu aktualisieren:</p> <ul style="list-style-type: none">▶ Software-Update vom PC Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie die Datei in den -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.▶ Software-Update von einem FTP-Server Befindet sich die Datei auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest: <code>ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname></code>▶ Software-Update von einem TFTP-Server Befindet sich die Datei auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest: <code>tftp://<IP-Adresse>/<Pfad>/<Dateiname></code>▶ Software-Update von einem SCP- oder SFTP-Server Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in einer der folgenden Formen fest:<ul style="list-style-type: none">– <code>scp://</code> oder <code>sftp://<IP-Adresse>/<Pfad>/<Dateiname></code> Nach Klicken der Schaltfläche <i>Start</i> zeigt das Gerät das Fenster <i>Anmeldeinformationen</i>. Geben Sie dort <i>Benutzername</i> und <i>Passwort</i> ein, um sich am Server anzumelden.– <code>scp://</code> oder <code>sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname></code>
Start	<p>Aktualisiert die Geräte-Software.</p> <p>Das Gerät installiert die ausgewählte Datei im Flash-Speicher und ersetzt die bisher dort gespeicherte Geräte-Software. Beim nächsten Neustart lädt das Gerät die installierte Geräte-Software.</p> <p>Um während des Software-Updates im Gerät angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ legen Sie vor dem Software-Update im Dialog <i>Gerätesicherheit</i> > Management-Zugriff > Web, Feld <i>Web-Interface Session-Timeout [min]</i> einen ausreichend hohen Wert fest.</p>

■ Tabelle

Parameter	Bedeutung
Datei Ort	Zeigt den Speicherort der Geräte-Software. Mögliche Werte: <ul style="list-style-type: none">▶ ram Flüchtiger Speicher des Geräts▶ flash Permanenter Speicher (NVM) des Geräts
Index	Zeigt den Index der Geräte-Software.
Dateiname	Zeigt den geräteinternen Dateinamen der Geräte-Software.
Firmware	Zeigt Versionsnummer und Erstellungsdatum der Geräte-Software.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

1.4 Laden/Speichern

Dieser Dialog bietet Ihnen die Möglichkeit, die Einstellungen des Geräts permanent in einem Konfigurationsprofil zu speichern.

Im Gerät können mehrere Konfigurationsprofile gespeichert sein. Wenn Sie ein alternatives Konfigurationsprofil aktivieren, schalten Sie das Gerät auf andere Einstellungen um. Sie haben die Möglichkeit, die Konfigurationsprofile auf Ihren PC oder auf einen Server zu exportieren. Außerdem haben Sie die Möglichkeit, Konfigurationsprofile von Ihrem PC oder von einem Server in das Gerät zu importieren.

In der Voreinstellung speichert das Gerät die Konfigurationsprofile unverschlüsselt. Wenn Sie ein Passwort im Rahmen *Konfigurations-Verschlüsselung* vergeben, speichert das Gerät sowohl das gegenwärtige als auch die zukünftigen Konfigurationsprofile in einem verschlüsselten Format.

Unbeabsichtigte Änderungen an den Einstellungen führen möglicherweise zum Verbindungsabbruch zwischen Ihrem PC und dem Gerät. Damit das Gerät erreichbar bleibt, schalten Sie vor dem Ändern von Einstellungen die Funktion *Konfigurationsänderungen rückgängig machen* ein. Bricht die Verbindung ab, lädt das Gerät nach der festgelegten Zeit das im permanenten Speicher (NVM) gespeicherte Konfigurationsprofil.

■ Konfigurations-Verschlüsselung

Parameter	Bedeutung
Aktiv	<p>Zeigt, ob die Konfigurations-Verschlüsselung im Gerät aktiv/inaktiv ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Die Konfigurations-Verschlüsselung ist aktiv. Das Gerät lädt ein Konfigurationsprofil aus dem permanenten Speicher (NVM) ausschließlich dann, wenn dieses verschlüsselt ist und das Passwort mit dem im Gerät gespeicherten Passwort übereinstimmt.▶ <i>unmarkiert</i> Die Konfigurations-Verschlüsselung ist inaktiv. Das Gerät lädt ein Konfigurationsprofil aus dem permanenten Speicher (NVM) ausschließlich dann, wenn dieses unverschlüsselt ist.
Passwort setzen	<p>Öffnet das <i>Passwort setzen</i>-Fenster, das Ihnen beim Festlegen des Passworts hilft, das für die Verschlüsselung des Konfigurationsprofils erforderlich ist. Das Verschlüsseln des Konfigurationsprofils erschwert den unberechtigten Zugriff.</p> <ul style="list-style-type: none"><input type="checkbox"/> Wenn Sie ein vorhandenes Passwort ändern, geben Sie in das Feld <i>Altes Passwort</i> das bisherige Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen <i>Passwort anzeigen</i>.<input type="checkbox"/> Geben Sie im Feld <i>Neues Passwort</i> das Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen <i>Passwort anzeigen</i>.<input type="checkbox"/> Markieren Sie das Kontrollkästchen <i>Konfiguration danach speichern</i>, um die Verschlüsselung auf das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (NVM) anzuwenden.

Anmerkung: Wenden Sie diese Funktion ausschließlich dann an, wenn maximal 1 Konfigurationsprofil im permanenten Speicher (NVM) des Geräts gespeichert ist. Entscheiden Sie sich vor dem Anlegen zusätzlicher Konfigurationsprofile für oder gegen eine dauerhaft eingeschaltete Konfigurations-Verschlüsselung im Gerät. Speichern Sie zusätzliche Konfigurationsprofile entweder unverschlüsselt oder mit demselben Passwort verschlüsselt.

Parameter	Bedeutung
Löschen	<p>Öffnet das <i>Löschen</i>-Fenster, das Ihnen beim Aufheben der Konfigurations-Verschlüsselung im Gerät hilft.</p> <ul style="list-style-type: none"> <input type="checkbox"/> Geben Sie im Feld <i>Altes Passwort</i> das bisherige Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen <i>Passwort anzeigen</i>. <input type="checkbox"/> Markieren Sie das Kontrollkästchen <i>Konfiguration danach speichern</i>, um die Verschlüsselung auch im „ausgewählten“ Konfigurationsprofil im permanenten Speicher (NVM) aufzuheben. <p>Anmerkung: Wenn Sie weitere Konfigurationsprofile verschlüsselt im Speicher vorhalten, hindert das Gerät Sie anschließend daran, diese Konfigurationsprofile zu aktivieren oder als „ausgewählt“ zu kennzeichnen.</p>

■ Information

Parameter	Bedeutung
NVM synchron mit running-config	<p>Zeigt, ob das Konfigurationsprofil im flüchtigen Speicher (RAM) und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (NVM) übereinstimmen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>markiert</i> Die Konfigurationsprofile stimmen überein. ▶ <i>unmarkiert</i> Die Konfigurationsprofile unterscheiden sich.

■ Sichere Konfiguration auf Remote-Server beim Speichern






Parameter	Bedeutung
Funktion	<p>Schaltet die <i>Sichere Konfiguration auf Remote-Server beim Speichern</i>-Funktion ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>Eingeschaltet</i> Die <i>Sichere Konfiguration auf Remote-Server beim Speichern</i>-Funktion ist eingeschaltet. Wenn Sie das Konfigurationsprofil im permanenten Speicher (NVM) speichern, sichert das Gerät das Konfigurationsprofil automatisch auf dem im Feld <i>URL</i> festgelegten Remote-Server. ▶ <i>Ausgeschaltet</i> (Voreinstellung) Die <i>Sichere Konfiguration auf Remote-Server beim Speichern</i>-Funktion ist ausgeschaltet.
URL	<p>Legt Pfad und Dateiname des zu sichernden Konfigurationsprofils auf dem Remote-Server fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen Beispiel: <code>tftp://192.9.200.1/cfg/config.xml</code> <p>Das Gerät unterstützt die folgenden Platzhalter:</p> <ul style="list-style-type: none"> – %d Systemdatum im Format YYYY-mm-dd – %t Systemzeit im Format HH_MM_SS – %i IP-Adresse des Geräts – %m MAC-Adresse des Geräts im Format AA-BB-CC-DD-EE-FF – %p Produktbezeichnung des Geräts

Parameter	Bedeutung
Zugangsdaten setzen	<p>Öffnet das <i>Anmeldeinformationen</i>-Fenster, das Ihnen beim Festlegen des Passworts hilft, das für die Anmeldung auf dem Remote-Server erforderlich ist.</p> <p><input type="checkbox"/> Geben Sie im Feld <i>Benutzername</i> den Benutzernamen ein. Um anstelle von ***** (Sternchen) den Benutzernamen im Klartext anzuzeigen, markieren Sie das Kontrollkästchen <i>Passwort anzeigen</i>. Mögliche Werte: – Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen</p> <p><input type="checkbox"/> Geben Sie im Feld <i>Passwort</i> das Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen <i>Passwort anzeigen</i>. Mögliche Werte: ► Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen Die folgenden Zeichen sind zulässig: a..z A..Z 0..9 # \$ % & ' () * + , - . / : ; < = > ? @ _ `</p>

■ Konfigurationsänderungen rückgängig machen

Parameter	Bedeutung
Funktion	<p>Schaltet die <i>Konfigurationsänderungen rückgängig machen</i>-Funktion ein/aus. Mit der Funktion prüft das Gerät kontinuierlich, ob es von der IP-Adresse dieses Benutzers erreichbar bleibt. Bricht die Verbindung ab, lädt das Gerät nach einer festgelegten Zeitspanne das „ausgewählte“ Konfigurationsprofil aus dem permanenten Speicher (NVM). Danach ist das Gerät wieder erreichbar.</p> <p>Mögliche Werte:</p> <p>► An Die Funktion ist eingeschaltet. – Die Zeitspanne zwischen Verbindungsabbruch und Laden des Konfigurationsprofils legen Sie fest im Feld <i>Timeout [s] für Wiederherstellung nach Verbindungsabbruch</i>. – Enthält der permanente Speicher (NVM) mehrere Konfigurationsprofile, lädt das Gerät das als „ausgewählt“ gekennzeichnete Konfigurationsprofil.</p> <p>► Aus (Voreinstellung) Die Funktion ist ausgeschaltet. Schalten Sie die Funktion wieder aus, bevor Sie die grafische Benutzeroberfläche schließen. So vermeiden Sie, dass das Gerät das als „ausgewählt“ gekennzeichnete Konfigurationsprofil wiederherstellt.</p> <p>Anmerkung: Bevor Sie die Funktion einschalten, speichern Sie die Einstellungen im Konfigurationsprofil. Gegenwärtige Änderungen, die lediglich flüchtig im Gerät gespeichert sind, bleiben somit erhalten.</p>
Timeout [s] für Wiederherstellung nach Verbindungsabbruch	<p>Legt die Zeit in Sekunden fest, nach der das Gerät das „ausgewählte“ Konfigurationsprofil aus dem permanenten Speicher (NVM) lädt, wenn die Verbindung abbricht.</p> <p>Mögliche Werte: ► 30..600 (Voreinstellung: 600)</p> <p>Legen Sie den Wert ausreichend groß fest. Berücksichtigen Sie die Zeit, in der Sie die Dialoge der grafischen Oberfläche lediglich ansehen, ohne sie zu ändern oder zu aktualisieren.</p>
Watchdog IP-Adresse	<p>Zeigt die IP-Adresse des PCs, auf dem Sie die Funktion eingeschaltet haben.</p> <p>Mögliche Werte: ► IPv4-Adresse (Voreinstellung: 0.0.0.0)</p>



■ **Tabelle**


Parameter	Bedeutung
Speicher-Typ	<p>Zeigt den Speicherort des Konfigurationsprofils.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ RAM (flüchtiger Speicher des Geräts) Im flüchtigen Speicher speichert das Gerät die Einstellungen für den laufenden Betrieb. ▶ NVM (permanenter Speicher des Geräts) Aus dem permanenten Speicher lädt das Gerät das „ausgewählte“ Konfigurationsprofil beim Neustart oder beim Anwenden der Funktion <i>Konfigurationsänderungen rückgängig machen</i>. Der permanente Speicher bietet Platz für mehrere Konfigurationsprofile, abhängig von der Anzahl der im Konfigurationsprofil gespeicherten Einstellungen. Das Gerät verwaltet im permanenten Speicher maximal 20 Konfigurationsprofile. Sie können ein Konfigurationsprofil in den flüchtigen Speicher (RAM) laden: <input type="checkbox"/> Markieren Sie in der Tabelle das Konfigurationsprofil. <input type="checkbox"/> Klicken Sie die Schaltfläche  und dann den Eintrag <i>Aktivieren</i>.
Profilname	<p>Zeigt die Bezeichnung des Konfigurationsprofils.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ running-config Bezeichnung des Konfigurationsprofils im flüchtigen Speicher (RAM). ▶ config Bezeichnung des werksseitig vorhandenen Konfigurationsprofils im permanenten Speicher (NVM). ▶ benutzerdefinierter Name Das Gerät bietet Ihnen die Möglichkeit, ein Konfigurationsprofil mit benutzerdefiniertem Namen zu speichern, wenn Sie ein vorhandenes Konfigurationsprofil in der Tabelle markieren, die Schaltfläche  und dann den Eintrag <i>Speichern unter...</i> klicken. Um das Konfigurationsprofil als XML-Datei auf Ihren PC zu exportieren, klicken Sie den Link. Dann wählen Sie den Speicherort und legen den Dateinamen fest. Um die Datei auf einem Remote-Server zu speichern, klicken Sie die Schaltfläche  und dann den Eintrag <i>Exportieren...</i>
Datum der letzten Änderung (UTC)	Zeigt den Zeitpunkt (UTC), zu dem ein Benutzer das Konfigurationsprofil zuletzt gespeichert hat.
Ausgewählt	<p>Zeigt, ob das Konfigurationsprofil als „ausgewählt“ gekennzeichnet ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Das Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet. <ul style="list-style-type: none"> – Das Gerät lädt die das Konfigurationsprofil beim Neustart oder beim Anwenden der Funktion in den flüchtigen Speicher (RAM). – Wenn Sie die Schaltfläche  klicken, speichert das Gerät die zwischengespeicherten Einstellungen in diesem Konfigurationsprofil. ▶ unmarkiert Ein anderes Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet. Um ein anderes Konfigurationsprofil als „ausgewählt“ zu kennzeichnen, markieren Sie das gewünschte Konfigurationsprofil in der Tabelle, klicken die Schaltfläche  und dann den Eintrag <i>Aktivieren</i>.
Verschlüsselt	<p>Zeigt, ob das Konfigurationsprofil verschlüsselt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Das Konfigurationsprofil ist verschlüsselt. ▶ unmarkiert Das Konfigurationsprofil ist unverschlüsselt. <p>Die Verschlüsselung des Konfigurationsprofils schalten Sie im Rahmen <i>Konfigurations-Verschlüsselung</i> ein und aus.</p>


Parameter	Bedeutung
Verschlüsselung verifiziert	<p>Zeigt, ob das Passwort des verschlüsselten Konfigurationsprofils mit dem im Gerät gespeicherten Passwort übereinstimmt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die Passwörter stimmen überein. Das Gerät ist imstande, das Konfigurationsprofil zu entschlüsseln. ▶ unmarkiert Die Passwörter unterscheiden sich. Das Gerät ist außerstande, das Konfigurationsprofil zu entschlüsseln.
Software-Version	<p>Zeigt die Versionsnummer der Geräte-Software, die das Gerät beim Speichern des Konfigurationsprofils ausgeführt hat.</p>
Fingerprint	<p>Zeigt die im Konfigurationsprofil gespeicherte Prüfsumme. Das Gerät berechnet die Prüfsumme beim Speichern der Einstellungen und fügt sie in das Konfigurationsprofil ein.</p>
Fingerprint verifiziert	<p>Zeigt, ob die im Konfigurationsprofil gespeicherte Prüfsumme gültig ist.</p> <p>Das Gerät berechnet die Prüfsumme des als „ausgewählt“ gekennzeichneten Konfigurationsprofils und vergleicht diese mit der Prüfsumme, die in diesem Konfigurationsprofil gespeichert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Berechnete und gespeicherte Prüfsumme stimmen überein. Die gespeicherten Einstellungen sind konsistent. ▶ unmarkiert Für das als „ausgewählt“ gekennzeichnete Konfigurationsprofil gilt: Berechnete und gespeicherte Prüfsumme unterscheiden sich. Das Konfigurationsprofil enthält geänderte Einstellungen. Mögliche Ursachen: <ul style="list-style-type: none"> – Die Datei ist beschädigt. – Ein Benutzer hat das Konfigurationsprofil exportiert und die XML-Datei außerhalb des Geräts verändert. Für die anderen Konfigurationsprofile hat das Gerät die Prüfsumme nicht berechnet. <p>Das Gerät verifiziert die Prüfsumme ausschließlich dann korrekt, wenn das Konfigurationsprofil zuvor wie folgt gespeichert wurde:</p> <ul style="list-style-type: none"> – auf einem baugleichen Gerät – mit derselben Software-Version, welche das Gerät derzeit ausführt <p>Anmerkung: Diese Funktion kennzeichnet Änderungen an den Einstellungen des Konfigurationsprofils. Die Funktion bietet keinen Schutz davor, das Gerät mit geänderten Einstellungen zu betreiben.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	<p>Entfernt das in der Tabelle markierte Konfigurationsprofil aus dem permanenten Speicher (NVM).</p> <p>Wenn das Konfigurationsprofil als „ausgewählt“ gekennzeichnet ist, hindert das Gerät Sie daran, das Konfigurationsprofil zu entfernen.</p>
	<p>Überträgt die Einstellungen aus dem flüchtigen Speicher (RAM) in das als „ausgewählt“ gekennzeichnete Konfigurationsprofil im permanenten Speicher (NVM).</p>

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Speichern unter...	<p>Kopiert das in der Tabelle markierte Konfigurationsprofil und speichert es mit benutzerdefiniertem Namen im permanenten Speicher (NVM). Das Gerät kennzeichnet das neue Konfigurationsprofil als „ausgewählt“.</p> <p>Anmerkung: Entscheiden Sie sich vor dem Anlegen zusätzlicher Konfigurationsprofile für oder gegen eine dauerhaft eingeschaltete Konfigurations-Verschlüsselung im Gerät. Speichern Sie zusätzliche Konfigurationsprofile entweder unverschlüsselt oder mit demselben Passwort verschlüsselt.</p>
Aktivieren	<p>Lädt die Einstellungen des in der Tabelle markierten Konfigurationsprofils in den flüchtigen Speicher (RAM).</p> <ul style="list-style-type: none"> ▶ Das Gerät trennt die Verbindung zur grafischen Benutzeroberfläche. <ul style="list-style-type: none"> <input type="checkbox"/> Laden Sie die grafische Benutzeroberfläche neu. <input type="checkbox"/> Melden Sie sich erneut an. ▶ Das Gerät verwendet die Einstellungen des Konfigurationsprofils ab sofort im laufenden Betrieb. <p>Schalten Sie die Funktion <i>Konfigurationsänderungen rückgängig machen</i> ein, bevor Sie ein anderes Konfigurationsprofil aktivieren. Bricht danach die Verbindung ab, lädt das Gerät das zuletzt als „ausgewählt“ gekennzeichnete Konfigurationsprofil aus dem permanenten Speicher (NVM). Das Gerät ist dann wieder erreichbar.</p> <p>Ist die Konfigurations-Verschlüsselung inaktiv, lädt das Gerät das Konfigurationsprofil ausschließlich dann, wenn dieses unverschlüsselt ist. Ist die Konfigurations-Verschlüsselung aktiv, lädt das Gerät das Konfigurationsprofil ausschließlich dann, wenn dieses verschlüsselt ist und das Passwort mit dem im Gerät gespeicherten Passwort übereinstimmt.</p> <p>Wenn Sie ein älteres Konfigurationsprofil aktivieren, übernimmt das Gerät die Einstellungen der in dieser Software-Version vorhandenen Funktionen. Das Gerät setzt die Werte der neuen Funktionen auf ihren voreingestellten Wert.</p>
Auswählen	<p>Kennzeichnet das in der Tabelle markierte Konfigurationsprofil als „ausgewählt“. Anschließend ist in Spalte <i>Ausgewählt</i> das Kontrollkästchen <i>markiert</i>.</p> <p>Das Gerät lädt die Einstellungen dieses Konfigurationsprofils beim Neustart oder beim Anwenden der Funktion <i>Konfigurationsänderungen rückgängig machen</i> in den flüchtigen Speicher (RAM).</p> <ul style="list-style-type: none"> ▶ Kennzeichnen Sie ein unverschlüsseltes Konfigurationsprofil ausschließlich dann als „ausgewählt“, wenn die Konfigurations-Verschlüsselung im Gerät ausgeschaltet ist. ▶ Kennzeichnen Sie ein verschlüsseltes Konfigurationsprofil ausschließlich dann als „ausgewählt“, wenn folgende Voraussetzungen erfüllt sind: <ul style="list-style-type: none"> – Die Konfigurations-Verschlüsselung im Gerät ist eingeschaltet. – Das Passwort des Konfigurationsprofils stimmt mit dem im Gerät gespeicherten Passwort überein. <p>Andernfalls ist das Gerät außerstande, beim nächsten Neustart die Einstellungen des Konfigurationsprofils zu laden und zu entschlüsseln. Für diesen Fall legen Sie im Dialog <i>Diagnose > System > Selbsttest</i> fest, ob das Gerät mit Werkseinstellungen startet oder den Neustart abbricht und anhält.</p> <p>Anmerkung: Als „ausgewählt“ lassen sich ausschließlich Konfigurationsprofile kennzeichnen, die im permanenten Speicher (NVM) gespeichert sind.</p>

Schaltfläche	Bedeutung
Importieren...	<p>Öffnet den Dialog <i>Importieren...</i>, um ein Konfigurationsprofil zu importieren. Voraussetzung ist, dass Sie das Konfigurationsprofil zuvor mit der Schaltfläche <i>Exportieren...</i> oder mit dem Link in Spalte <i>Profilname</i> exportiert haben.</p> <ul style="list-style-type: none"><input type="checkbox"/> Wählen Sie in der Dropdown-Liste <i>Select source</i> aus, woher das Gerät das Konfigurationsprofil importiert.<ul style="list-style-type: none">▶ PC/URL Das Gerät importiert das Konfigurationsprofil vom lokalen PC oder von einem Remote-Server.<input type="checkbox"/> Wenn oben <i>PC/URL</i> ausgewählt ist, dann legen Sie im Rahmen <i>Import profile from PC/URL</i> die Datei des zu importierenden Konfigurationsprofils fest.<ul style="list-style-type: none">– Import vom PC Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie die Datei in den -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.– Import von einem FTP-Server Befindet sich die Datei auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest: <code>ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname></code>– Import von einem TFTP-Server Befindet sich die Datei auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest: <code>tftp://<IP-Adresse>/<Pfad>/<Dateiname></code>– Import von einem SCP- oder SFTP-Server Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in einer der folgenden Formen fest: <code>scp://</code> oder <code>sftp://<IP-Adresse>/<Pfad>/<Dateiname></code> Nach Klicken der Schaltfläche <i>Start</i> zeigt das Gerät das Fenster <i>Anmeldeinformationen</i>. Geben Sie dort <i>Benutzername</i> und <i>Passwort</i> ein, um sich am Server anzumelden. <code>scp://</code> oder <code>sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname></code><input type="checkbox"/> Wenn oben <i>Externer Speicher</i> ausgewählt ist, dann legen Sie im Rahmen <i>Import profile from external memory</i> die Datei des zu importierenden Konfigurationsprofils fest. Wählen Sie in der Dropdown-Liste <i>Profilname</i> den Namen des zu importierenden Konfigurationsprofils.<input type="checkbox"/> Im Rahmen <i>Ziel</i> legen Sie fest, wo das Gerät das importierte Konfigurationsprofil speichert. Im Feld <i>Profilname</i> legen Sie den Namen fest, unter dem das Gerät das Konfigurationsprofil speichert. Im Feld <i>Speicher-Typ</i> legen Sie den Speicherort für das Konfigurationsprofil fest. Voraussetzung ist, dass Sie in der Dropdown-Liste <i>Select source</i> den Wert <i>PC/URL</i> ausgewählt haben.<ul style="list-style-type: none">▶ RAM Das Gerät speichert das Konfigurationsprofil im flüchtigen Speicher (RAM) des Geräts. Dies ersetzt die <i>running-config</i>, das Gerät verwendet sofort die Einstellungen des importierten Konfigurationsprofils. Das Gerät trennt die Verbindung zur grafischen Benutzeroberfläche. Laden Sie die grafische Benutzeroberfläche neu. Melden Sie sich erneut an.▶ NVM Das Gerät speichert das Konfigurationsprofil im permanenten Speicher (NVM) des Geräts. <p>Beim Importieren eines Konfigurationsprofils übernimmt das Gerät die Einstellungen wie folgt:</p> <ul style="list-style-type: none">– Wenn das Konfigurationsprofil von demselben Gerät oder von einem identisch ausgestatteten Gerät des gleichen Typs exportiert wurde: Das Gerät übernimmt die Einstellungen komplett.– Wenn das Konfigurationsprofil von einem anderen Gerät exportiert wurde: Das Gerät übernimmt die Einstellungen, die es mit seiner Hardware-Ausstattung und seinem Software-Level interpretieren kann. Die übrigen Einstellungen übernimmt das Gerät aus seinem <i>running-config</i>-Konfigurationsprofil. <p>Bezüglich Verschlüsselung des Konfigurationsprofil lesen Sie auch den Hilfetext zum Rahmen <i>Konfigurations-Verschlüsselung</i>. Das Gerät importiert das Konfigurationsprofil unter den folgenden Bedingungen:</p> <ul style="list-style-type: none">– Die Konfigurations-Verschlüsselung des Geräts ist inaktiv. Das Konfigurationsprofil ist unverschlüsselt.– Die Konfigurations-Verschlüsselung des Geräts ist aktiv. Das Konfigurationsprofil ist mit dem gleichen Passwort verschlüsselt, welches das Gerät gegenwärtig verwendet.

Schaltfläche	Bedeutung
Exportieren...	<p>Exportiert das in der Tabelle markierte Konfigurationsprofil und speichert es als XML-Datei auf einem Remote-Server.</p> <p>Um die Datei auf Ihrem PC zu speichern, klicken Sie den Link in Spalte <i>Profilname</i>, um den Speicherort zu wählen und den Dateinamen festzulegen.</p> <p>Das Gerät bietet Ihnen folgende Möglichkeiten, ein Konfigurationsprofil zu exportieren:</p> <ul style="list-style-type: none"> ▶ Export auf einen FTP-Server Um die Datei auf einem FTP-Server zu speichern, legen Sie den URL zur Datei in der folgenden Form fest: ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname> ▶ Export auf einen TFTP-Server Um die Datei auf einem TFTP-Server zu speichern, legen Sie den URL zur Datei in der folgenden Form fest: tftp://<IP-Adresse>/<Pfad>/<Dateiname> ▶ Export auf einen SCP- oder SFTP-Server Um die Datei auf einem SCP- oder SFTP-Server zu speichern, legen Sie den URL zur Datei in einer der folgenden Formen fest: <ul style="list-style-type: none"> – scp:// oder sftp://<IP-Adresse>/<Pfad>/<Dateiname> Nach Klicken der Schaltfläche <i>Ok</i> zeigt das Gerät das Fenster <i>Anmeldeinformationen</i>. Geben Sie dort <i>Benutzername</i> und <i>Passwort</i> ein, um sich am Server anzumelden. – scp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>
Auf Lieferzustand zurücksetzen...	<p>Setzt die Einstellungen im Gerät auf die voreingestellten Werte zurück.</p> <ul style="list-style-type: none"> ▶ Das Gerät löscht die gespeicherten Konfigurationsprofile aus dem flüchtigen Speicher (RAM) und aus dem permanenten Speicher (NVM). ▶ Das Gerät löscht das vom Webserver im Gerät verwendete HTTPS-Zertifikat. ▶ Das Gerät löscht den vom SSH-Server im Gerät verwendeten DSA-/RSA-Schlüssel (Host Key). ▶ Nach kurzer Zeit startet das Gerät neu mit den im Lieferzustand voreingestellten Werten.
Auf Default-Zustand zurücksetzen	<p>Löscht die gegenwärtigen Betriebseinstellungen (<i>running config</i>) aus dem flüchtigen Speicher (RAM).</p>

1.5 Port

Dieser Dialog bietet Ihnen die Möglichkeit, Einstellungen für die einzelnen Ports festzulegen. Der Dialog zeigt außerdem Betriebsmodus, Verbindungszustand, Bitrate und Duplex-Modus für jeden Port.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [Konfiguration]
- ▶ [Statistiken]
- ▶ [Netzlast]

[Konfiguration]

■ Tabelle


Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Name	<p>Bezeichnung des Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen Die folgenden Zeichen sind zulässig: <ul style="list-style-type: none"> - <space> - 0..9 - a..z - A..Z - !#\$%&'()*+,-./:;<=>?@[\\]^_`{ }~
Port an	<p>Aktiviert/deaktiviert den Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der Port ist aktiv. ▶ <code>unmarkiert</code> Der Port ist inaktiv. Der Port sendet und empfängt keine Daten.
Zustand	<p>Zeigt, ob der Port gegenwärtig physikalisch eingeschaltet oder ausgeschaltet ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Der Port ist physikalisch eingeschaltet. ▶ <code>unmarkiert</code> Der Port ist physikalisch ausgeschaltet. Wenn die Funktion <i>Port an</i> aktiv ist, hat die <i>Auto-Disable</i>-Funktion den Port ausgeschaltet. Die Einstellungen der Funktion <i>Auto-Disable</i> legen Sie im Dialog <i>Diagnose > Ports > Auto-Disable</i> fest.
Power-State (Port aus)	<p>Legt fest, ob der Port physikalisch eingeschaltet oder ausgeschaltet ist, wenn Sie den Port mit der Funktion <i>Port an</i> deaktivieren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Der Port bleibt physikalisch eingeschaltet. Ein angeschlossenes Gerät empfängt einen aktiven Link. ▶ <code>unmarkiert</code> (Voreinstellung) Der Port ist physikalisch ausgeschaltet.
Auto power down	<p>Legt fest, wie sich der Port verhält, wenn kein Kabel angeschlossen ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>no-power-save</code> (Voreinstellung) Der Port bleibt aktiviert. ▶ <code>auto-power-down</code> Der Port schaltet in den Energiesparmodus. ▶ <code>unsupported</code> Der Port unterstützt diese Funktion nicht und bleibt aktiviert.

Parameter	Bedeutung
Automatische Konfiguration	<p>Aktiviert/deaktiviert die automatische Auswahl des Betriebsmodus für den Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert (Voreinstellung) Die automatische Auswahl des Betriebsmodus ist aktiv. Der Port handelt den Betriebsmodus per Autonegotiation selbständig aus und erkennt die Belegung der Anschlüsse des TP-Ports automatisch (Auto Cable-Crossing). Diese Einstellung hat Vorrang vor der manuellen Einstellung des Betriebsmodus. Bis der Port den Betriebsmodus eingestellt hat, vergehen einige Sekunden.▶ unmarkiert Die automatische Auswahl des Betriebsmodus ist inaktiv. Der Port arbeitet mit den Werten, die Sie in Spalte <i>Manuelle Konfiguration</i> und in Spalte <i>Manuelles Cable-Crossing (Auto. Konfig. aus)</i> festlegen.▶ Ausgegraute Darstellung Keine automatische Auswahl des Betriebsmodus.
Manuelle Konfiguration	<p>Legt den Betriebsmodus des Ports fest, wenn die <i>Automatische Konfiguration</i>-Funktion ausgeschaltet ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 10 Mbit/s HDX Halbduplex-Verbindung▶ 10 Mbit/s FDX Vollduplex-Verbindung▶ 100 Mbit/s HDX Halbduplex-Verbindung▶ 100 Mbit/s FDX Vollduplex-Verbindung▶ 1000 Mbit/s FDX Vollduplex-Verbindung▶ 2500 Mbit/s FDX Vollduplex-Verbindung <p>Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts.</p>
Link/ Aktuelle Betriebsart	<p>Zeigt, welchen Betriebsmodus der Port gegenwärtig verwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ - Kein Kabel angesteckt, keine Verbindung.▶ 10 Mbit/s HDX Halbduplex-Verbindung▶ 10 Mbit/s FDX Vollduplex-Verbindung▶ 100 Mbit/s HDX Halbduplex-Verbindung▶ 100 Mbit/s FDX Vollduplex-Verbindung▶ 1000 Mbit/s FDX Vollduplex-Verbindung▶ 2500 Mbit/s FDX Vollduplex-Verbindung <p>Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts.</p>

Parameter	Bedeutung
Manuelles Cable-Crossing (Auto. Konfig. aus)	<p>Legt die Belegung der Anschlüsse eines TP-Ports fest. Voraussetzung ist, dass die <i>Automatische Konfiguration</i>-Funktion ausgeschaltet ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ mdi Das Gerät vertauscht das Sende- und Empfangsleitungspaar auf dem Port. ▶ mdix (Voreinstellung auf TP-Ports) Das Gerät vertauscht keine Leitungspaare auf dem Port. ▶ auto-mdix Das Gerät erkennt das Sende- und Empfangsleitungspaar des angeschlossenen Geräts und stellt sich automatisch darauf ein. Beispiel: Wenn Sie ein Endgerät mit gekreuztem Kabel anschließen, stellt das Gerät den Port automatisch von mdix auf mdi. ▶ unsupported (Voreinstellung auf optischen Ports oder TP-SFP-Ports) Der Port unterstützt diese Funktion nicht.
Flusskontrolle	<p>Aktiviert/deaktiviert die Flusskontrolle auf dem Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Die Flusskontrolle auf dem Port ist aktiv. Auf dem Port ist das Senden und Auswerten von Pause-Paketen (Voll duplex-Betrieb) oder Kollisionen (Halbduplex-Betrieb) aktiviert. <ul style="list-style-type: none"> <input type="checkbox"/> Um die Flusskontrolle im Gerät einzuschalten, aktivieren Sie zusätzlich die Funktion <i>Flusskontrolle</i> im Dialog <i>Switching > Global</i>. <input type="checkbox"/> Aktivieren Sie die Flusskontrolle außerdem auf dem Port des mit diesem Port verbundenen Geräts. Auf einem Uplink-Port führt das Aktivieren der Flusskontrolle möglicherweise zu unerwünschten Sendepausen im übergeordneten Netzsegment („Wandering Backpressure“). ▶ unmarkiert Die Flusskontrolle auf dem Port ist inaktiv. <p>Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Ports. Sind Flusskontrolle und Redundanzfunktion gleichzeitig aktiv, arbeitet die Redundanzfunktion möglicherweise nicht wie beabsichtigt.</p>
Trap senden (Link-Up/Down)	<p>Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Link-Status-Änderungen auf dem Port erkennt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Das Senden von SNMP-Traps ist aktiv. Das Gerät sendet einen SNMP-Trap, wenn es eine Link-Status-Änderung erkennt. ▶ unmarkiert Das Senden von SNMP-Traps ist inaktiv. <p>Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose > Statuskonfiguration > Alarme (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen.</p>
Signal	<p>Aktiviert/deaktiviert das Blinken der Port-LED. Diese Funktion bietet Ihnen die Möglichkeit, den Port im Feld zu identifizieren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Das Blinken der Port-LED ist aktiv. Die Port-LED blinkt solange, bis Sie die Funktion wieder ausschalten. ▶ unmarkiert (Voreinstellung) Das Blinken der Port-LED ist inaktiv.
Link-Überwachung	<p>Aktiviert/deaktiviert die <i>Link-Überwachung</i>-Funktion auf dem Interface. Verwenden Sie die <i>Link-Überwachung</i>-Funktion für Endgeräte, die kein Far End Fault Indication (FEFI) auf optischen Links unterstützen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die <i>Link-Überwachung</i>-Funktion ist aktiv. Wenn das Gerät einen vorhandenen Link erkennt, leuchtet die Port-LED. Wenn das Gerät erkennt, dass der Link unterbrochen ist, erlischt die Port-LED. ▶ unmarkiert (Voreinstellung) Die <i>Link-Überwachung</i>-Funktion ist inaktiv.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Port-Statistiken leeren	Setzt die Zähler der Portstatistik auf 0.

[Statistiken]


Diese Registerkarte zeigt pro Port folgenden Überblick:

- ▶ Anzahl der vom Gerät empfangenen Datenpakete/Bytes
 - *Empfangene Pakete*
 - *Empfangene Oktets*
 - *Empfangene Unicast-Pakete*
 - *Empfangene Multicast-Pakete*
 - *Empfangene Broadcast-Pakete*
- ▶ Anzahl der vom Gerät gesendeten Datenpakete/Bytes
 - *Gesendete Pakete*
 - *Gesendete Oktets*
 - *Gesendete Unicast-Pakete*
 - *Gesendete Multicast-Pakete*
 - *Gesendete Broadcast-Pakete*
- ▶ Anzahl der vom Gerät erkannten Fehler
 - *Empfangene Fragmente*
 - *Erkannte CRC-Fehler*
 - *Erkannte Kollisionen*
- ▶ Anzahl der vom Gerät empfangenen und gesendeten Datenpakete pro Größenkategorie
 - *Pakete 64 Byte*
 - *Pakete 65 bis 127 Byte*
 - *Pakete 128 bis 255 Byte*
 - *Pakete 256 bis 511 Byte*
 - *Pakete 512 bis 1023 Byte*
 - *Pakete 1024 bis 1518 Byte*
- ▶ Anzahl der vom Gerät verworfenen Datenpakete
 - *Empfangsseitig verworfene Pakete*
 - *Sendeseitig verworfene Pakete*

Um die Tabelle nach einem bestimmten Kriterium zu sortieren, klicken Sie die Überschrift der entsprechenden Spalte.


Um die Tabelle beispielsweise nach der Anzahl der empfangenen Bytes in aufsteigender Reihenfolge zu sortieren, klicken Sie 1 Mal die Überschrift der Spalte *Empfangene Oktets*. Um absteigend zu sortieren, klicken Sie die Überschrift erneut.

Um die Portstatistik-Zähler in der Tabelle auf 0 zurückzusetzen, gehen Sie wie folgt vor:

- ▶ Klicken Sie im Dialog *Grundeinstellungen > Port* die Schaltfläche  und dann den Eintrag *Port-Statistiken leeren*.
oder
- ▶ Klicken Sie im Dialog *Grundeinstellungen > Neustart* die Schaltfläche *Port-Statistiken leeren*.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Port-Statistiken leeren	Setzt die Zähler der Portstatistik auf 0.

[Netzlust]


Diese Registerkarte zeigt Ihnen die Auslastung (Netzlust) der einzelnen Ports an.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Netzlust [%]	Zeigt die gegenwärtige Netzlust in Prozent, bezogen auf die in Spalte <i>Kontroll-Intervall [s]</i> festgelegte Zeitspanne. Die Netzlust ist das Verhältnis der empfangen Datenmenge zur maximal möglichen Datenmenge bei der gegenwärtig konfigurierten Datenrate.
Unterer Grenzwert [%]	Legt einen unteren Grenzwert für die Netzlust fest. Unterschreitet die Netzlust des Ports diesen Wert, zeigt Spalte <i>Alarm</i> einen Alarm. Mögliche Werte: ▶ 0.00..100.00 (Voreinstellung: 0.00) Der Wert 0 deaktiviert den unteren Grenzwert.
Oberer Grenzwert [%]	Legt einen oberen Grenzwert für die Netzlust fest. Überschreitet die Netzlust des Ports diesen Wert, zeigt Spalte <i>Alarm</i> einen Alarm. Mögliche Werte: ▶ 0.00..100.00 (Voreinstellung: 0.00) Der Wert 0 deaktiviert den oberen Grenzwert.
Kontroll-Intervall [s]	Legt die Zeitspanne in Sekunden fest. Mögliche Werte: ▶ 1..3600 (Voreinstellung: 30)
Alarm	Kennzeichnet den Alarmzustand für die Netzlust. Mögliche Werte: ▶ markiert Die Netzlust des Ports liegt unter dem in Spalte <i>Unterer Grenzwert [%]</i> oder über dem in Spalte <i>Oberer Grenzwert [%]</i> festgelegten Wert. Das Gerät sendet einen SNMP-Trap. ▶ unmarkiert Die Netzlust des Ports liegt über dem in Spalte <i>Unterer Grenzwert [%]</i> und unter dem in Spalte <i>Oberer Grenzwert [%]</i> festgelegten Wert. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose > Statuskonfiguration > Alarme (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen.

■ Schaltflächen


Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Port-Statistiken leeren	Setzt die Zähler der Portstatistik auf 0.

1.6 Neustart

Dieser Dialog bietet Ihnen die Möglichkeit, das Gerät neu zu starten, Portzähler und Adresstabellen zurückzusetzen sowie Log-Dateien zu löschen.

■ Neustart

Parameter	Bedeutung
Neustart in	Zeigt die verbleibende Zeit bis das Gerät neu startet. Um die Anzeige der verbleibenden Zeit zu aktualisieren, klicken Sie die Schaltfläche  .
Abbrechen	Bricht den verzögerten Neustart ab.
Kaltstart...	Öffnet den Dialog <i>Neustart</i> , um einen sofortigen oder einen verzögerten Neustart des Geräts auszulösen. Wenn sich das Konfigurationsprofil im flüchtigen Speicher (<i>Warnung</i> RAM) und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (NVM) unterscheiden, zeigt das Gerät den Dialog <i>Warnung</i> . <input type="checkbox"/> Um die Änderungen permanent zu speichern, klicken Sie im Dialog <i>Warnung</i> die Schaltfläche <i>Ja</i> . <input type="checkbox"/> Um die Änderungen zu verwerfen, klicken Sie im Dialog <i>Warnung</i> die Schaltfläche <i>Nein</i> . ▶ Im Feld <i>Neustart in</i> legen Sie die Verzögerungszeit für den verzögerten Neustart fest. Mögliche Werte: – 00:00:00..596:31:23 (Voreinstellung: 00:00:00) Nach Ablauf der Verzögerungszeit startet das Gerät neu und durchläuft folgende Phasen: ▶ Das Gerät führt einen RAM-Test durch, sofern diese Funktion im Dialog <i>Diagnose</i> > System > <i>Selbsttest</i> aktiviert ist. ▶ Das Gerät startet die Geräte-Software, die das Feld <i>Stored version</i> im Dialog <i>Grundeinstellungen</i> > <i>Software</i> anzeigt. ▶ Das Gerät lädt die Einstellungen aus dem „ausgewählten“ Konfigurationsprofil. Siehe Dialog <i>Grundeinstellungen</i> > <i>Laden/Speichern</i> . Anmerkung: Während des Neustarts überträgt das Gerät keine Daten. Das Gerät ist während dieser Zeit für die grafische Benutzeroberfläche und andere Managementsysteme unerreichbar.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
MAC-Adresstabelle zurücksetzen	Entfernt aus der Forwarding-Tabelle (FDB) die MAC-Adressen, die im Dialog <i>Switching</i> > Filter für MAC-Adressen in Spalte <i>Status</i> den Wert <i>learned</i> haben.
ARP-Tabelle zurücksetzen	Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen. Siehe Dialog <i>Diagnose</i> > System > <i>ARP</i> .
Port-Statistiken leeren	Setzt die Zähler der Portstatistik auf 0. Siehe Dialog <i>Grundeinstellungen</i> > Port, Registerkarte <i>Statistiken</i> .
IGMP-Snooping-Daten zurücksetzen	Entfernt die IGMP-Snooping-Einträge und setzt den Zähler im Rahmen <i>Information</i> auf 0. Siehe Dialog <i>Switching</i> > <i>IGMP-Snooping</i> > <i>Global</i> .
Log-Datei löschen	Entfernt die protokollierten Einträge aus der Log-Datei. Siehe Dialog <i>Diagnose</i> > Bericht > System Log.

2 Zeit

Das Menü enthält die folgenden Dialoge:

- ▶ Grundeinstellungen
- ▶ IRIG-B/PPS
- ▶ Sntp
- ▶ PTP

2.1 Grundeinstellungen

Nach einem Neustart initialisiert das Gerät seine Uhr auf den 1. Januar, 0.00 Uhr. Stellen Sie die Uhrzeit neu ein, wenn Sie das Gerät von der Stromversorgung trennen oder es neu starten. Alternativ legen Sie fest, dass das Gerät die gegenwärtige Uhrzeit automatisch von einem SNTP-Server oder von einer PTP-Uhr bezieht.

In diesem Dialog legen Sie, unabhängig vom gewählten Zeitsynchronisationsprotokoll, zeitbezogene Einstellungen fest.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [\[Global \]](#)
- ▶ [\[Sommerzeit \]](#)

[Global]

In dieser Registerkarte legen Sie die Systemzeit im Gerät und die Zeitzone fest.

■ Konfiguration

Parameter	Bedeutung
Systemzeit (UTC)	Zeigt das gegenwärtige Datum und die gegenwärtige Uhrzeit bezogen auf die koordinierte Weltzeit UTC an.
Setze Zeit vom PC	Das Gerät verwendet die Uhrzeit des PCs als Systemzeit.
Systemzeit	Zeigt das gegenwärtige Datum und die gegenwärtige Uhrzeit bezogen auf die lokale Zeit an: $Systemzeit = Systemzeit (UTC) + Lokaler Offset [min] + Sommerzeit$
Quelle der Zeit	Zeigt die Zeitquelle, aus der das Gerät die Zeitinformation bezieht. Das Gerät wählt automatisch die verfügbare Zeitquelle mit der höchsten Genauigkeit. Mögliche Werte: <ul style="list-style-type: none"> ▶ lokal Systemuhr des Geräts. ▶ sntp Der SNTP-Client ist aktiviert und das Gerät ist durch einen SNTP-Server synchronisiert. ▶ ptp PTP ist aktiviert und die Uhr des Geräts ist auf eine PTP-Master-Uhr synchronisiert.
Lokaler Offset [min]	Legt die Differenz zwischen lokaler Zeit und $Systemzeit (UTC)$ in Minuten fest: $Lokaler Offset [min] = Systemzeit - Systemzeit (UTC)$ Mögliche Werte: <ul style="list-style-type: none"> ▶ -780..840 (Voreinstellung: 60)

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

[Sommerzeit]

In dieser Registerkarte aktivieren Sie die automatische Sommerzeit-Umschaltung. Beginn und Ende der Sommerzeit wählen Sie anhand eines vordefinierten Profils oder Sie legen diese Einstellungen individuell fest. Während der Sommerzeit stellt das Gerät die lokale Zeit um 1 Stunde vor.

■ Funktion

Parameter	Bedeutung
Sommerzeit	Schaltet die <i>Sommerzeit</i> -Modus ein/aus. Mögliche Werte: ▶ An Die <i>Sommerzeit</i> -Modus ist eingeschaltet. Das Gerät wechselt automatisch zwischen Sommerzeit und Winterzeit. ▶ Aus (Voreinstellung) Die <i>Sommerzeit</i> -Modus ist ausgeschaltet. Die Zeitpunkte, zu denen das Gerät zwischen Sommer- und Winterzeit umschaltet, sind in den Rahmen <i>Sommerzeit Beginn</i> und <i>Sommerzeit Ende</i> festgelegt.
Profil...	Öffnet den Dialog <i>Profil...</i> . Dort wählen Sie ein vordefiniertes Profil für Beginn und Ende der Sommerzeit aus. Dieses Profil überschreibt die Einstellungen in den Rahmen <i>Sommerzeit Beginn</i> und <i>Sommerzeit Ende</i> .

■ Sommerzeit Beginn

In den ersten 3 Feldern legen Sie den Tag für den Beginn der Sommerzeit fest, im letzten Feld die Uhrzeit.

Das Gerät schaltet auf Sommerzeit, wenn die Uhrzeit im Feld *Systemzeit* den hier festgelegten Wert erreicht.

Parameter	Bedeutung
Woche	Legt die Woche im gegenwärtigen Monat fest. Mögliche Werte: ▶ kein (Voreinstellung) ▶ first ▶ second ▶ third ▶ fourth ▶ last
Tag	Legt den Wochentag fest. Mögliche Werte: ▶ kein (Voreinstellung) ▶ Sunday ▶ Monday ▶ Tuesday ▶ Wednesday ▶ Thursday ▶ Friday ▶ Saturday

Parameter	Bedeutung
Monat	Legt den Monat fest. Mögliche Werte: ▶ kein (Voreinstellung) ▶ January ▶ February ▶ March ▶ April ▶ May ▶ June ▶ July ▶ August ▶ September ▶ October ▶ November ▶ December
Systemzeit	Legt die Uhrzeit fest. Mögliche Werte: ▶ <HH:MM> (Voreinstellung: 00:00)

■ Sommerzeit Ende

In den ersten 3 Feldern legen Sie den Tag für das Ende der Sommerzeit fest, im letzten Feld die Uhrzeit.

Das Gerät schaltet auf Normalzeit, wenn die Uhrzeit im Feld *Systemzeit* den hier festgelegten Wert erreicht.

Parameter	Bedeutung
Woche	Legt die Woche im gegenwärtigen Monat fest. Mögliche Werte: ▶ kein (Voreinstellung) ▶ first ▶ second ▶ third ▶ fourth ▶ last
Tag	Legt den Wochentag fest. Mögliche Werte: ▶ kein (Voreinstellung) ▶ Sunday ▶ Monday ▶ Tuesday ▶ Wednesday ▶ Thursday ▶ Friday ▶ Saturday

Parameter	Bedeutung
Monat	Legt den Monat fest. Mögliche Werte: <ul style="list-style-type: none">▶ kein (Voreinstellung)▶ January▶ February▶ March▶ April▶ May▶ June▶ July▶ August▶ September▶ October▶ November▶ December
Systemzeit	Legt die Uhrzeit fest. Mögliche Werte: <ul style="list-style-type: none">▶ <HH:MM> (Voreinstellung: 00:00)

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

2.2 IRIG-B/PPS

Das Gerät bietet Ihnen die Möglichkeit, binär codierte Zeitsignale extern auszugeben. Die Zeitsignale ermöglichen die Synchronisierung anderer Geräte.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [IRIG-B]
- ▶ [PPS]

[IRIG-B]

In dieser Registerkarte konfigurieren Sie den IRIG-B-Ausgang des Geräts.

Am IRIG-B-Ausgang stellt das Gerät ein pulsweiten-moduliertes Zeitsignal mit 100 Pulsen pro Sekunde bereit. Voraussetzung ist, dass die PTP-Slave-Uhr des Geräts synchronisiert ist.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet den <i>IRIG-B</i> -Ausgang des Geräts ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Der <i>IRIG-B</i>-Ausgang ist eingeschaltet. Der Rahmen <i>Konfiguration</i> zeigt, ob das Zeitsignal anliegt.▶ Aus (Voreinstellung) Der <i>IRIG-B</i>-Ausgang ist ausgeschaltet.

■ Konfiguration

Parameter	Bedeutung
Modus	Legt den Code des Zeitsignals fest. Jeder Code enthält eine spezifische Zeitinformation. Mögliche Werte: <ul style="list-style-type: none">▶ <i>irig-b000</i> enthält BCDtoy, CF, SBS▶ <i>irig-b001</i> enthält BCDtoy, CF▶ <i>irig-b002</i> enthält BCDtoy▶ <i>irig-b003</i> (Voreinstellung) enthält BCDtoy, SBS▶ <i>irig-b004</i> enthält BCDtoy, BCDyear, CF, SBS▶ <i>irig-b005</i> enthält BCDtoy, BCDyear, CF▶ <i>irig-b006</i> enthält BCDtoy, BCDyear▶ <i>irig-b007</i> enthält BCDtoy, BCDyear, SBS Erläuterung: <ul style="list-style-type: none">– BCDtoy = binary coded decimal time of year– BCDyear = binary coded decimal year– CF = control functions (according to IEEE 1344)– SBS = straight binary seconds of day
Zeit-Modus	Legt fest, welche Zeitinformation der internen Uhr das Gerät überträgt. Mögliche Werte: <ul style="list-style-type: none">▶ <i>lokal</i> Das Gerät überträgt die Zeitinformation bezogen auf die lokale Zeit.▶ <i>utc</i> (Voreinstellung) Das Gerät überträgt die Zeitinformation bezogen auf die koordinierte Weltzeit UTC.
Qualität	Zeigt, welche Genauigkeit das Zeitsignal hat („time quality“ gemäß IEEE 1344): <ul style="list-style-type: none">▶ Fehler Keine Zeitquelle vorhanden oder Zeitquelle unzuverlässig.▶ <i>locked</i> Zeitquelle vorhanden.

■ Information

Parameter	Bedeutung
Ausgang aktiv	Zeigt, ob das Zeitsignal am IRIG-B-Ausgang anliegt. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Am IRIG-B-Ausgang liegt das Zeitsignal an. Die PTP-Slave-Uhr des Geräts ist auf einen PTP-Master-Uhr synchronisiert.▶ unmarkiert Am IRIG-B-Ausgang liegt kein Zeitsignal an. Die PTP-Slave-Uhr des Geräts ist nicht synchronisiert.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[PPS]

In dieser Registerkarte konfigurieren Sie den PPS-Ausgang des Geräts.

Am PPS-Ausgang stellt das Gerät das Zeitsignal als PPS (1 Puls pro Sekunde) bereit.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet den <i>PPS</i> -Ausgang des Geräts ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Der <i>PPS</i>-Ausgang ist eingeschaltet. Das Zeitsignal liegt am PPS-Ausgang an. Die Periodendauer des Pulses beträgt 1 Sekunde (200 ms High, 800 ms Low).▶ Aus (Voreinstellung) Der <i>PPS</i>-Ausgang ist ausgeschaltet.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

2.3 SNTP

Das Simple Network Time Protocol (SNTP) ist ein im RFC 4330 beschriebenes Verfahren für die Zeitsynchronisation im Netz.

Das Gerät bietet Ihnen die Möglichkeit, als SNTP-Client die Systemzeit im Gerät zu synchronisieren. Als SNTP-Server stellt das Gerät die Zeitinformation anderen Geräten zur Verfügung.

Das Menü enthält die folgenden Dialoge:

- ▶ [SNTP Client](#)
- ▶ [SNTP Server](#)

2.3.1 SNTP Client

In diesem Dialog legen Sie die Einstellungen fest, mit denen das Gerät als SNTP-Client arbeitet.

Als SNTP-Client bezieht das Gerät die Zeitinformationen sowohl von SNTP-Servern als auch von NTP-Servern und synchronisiert die lokale Uhr auf die Zeit des Zeit-Servers.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>SNTP Client</i> -Funktion des Geräts ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>SNTP Client</i>-Funktion ist eingeschaltet. Das Gerät arbeitet als SNTP-Client.▶ Aus (Voreinstellung) Die <i>SNTP Client</i>-Funktion ist ausgeschaltet.

■ Konfiguration

Parameter	Bedeutung
Modus	Legt fest, ob das Gerät die Zeitinformation aktiv bei einem im Netz bekannten und konfigurierten SNTP-Server anfragt (Unicast-Modus) oder passiv auf die Zeitinformation eines beliebigen SNTP-Servers wartet (Broadcast-Modus). Mögliche Werte: <ul style="list-style-type: none">▶ unicast (Voreinstellung) Das Gerät bezieht die Zeitinformation ausschließlich vom konfigurierten SNTP-Server. Das Gerät sendet Unicast-Anfragen an den SNTP-Server und wertet dessen Antworten aus.▶ broadcast Das Gerät bezieht die Zeitinformation von einem oder mehreren SNTP- oder NTP-Servern. Das Gerät wertet ausschließlich die Broadcasts oder Multicasts dieser Server aus.
Request-Intervall [s]	Legt das Intervall in Sekunden fest, in dem das Gerät Zeitinformationen beim SNTP-Server anfordert. Mögliche Werte: <ul style="list-style-type: none">▶ 5..3600 (Voreinstellung: 30)
Broadcast-Recv-Timeout [s]	Legt die Zeit in Sekunden fest, die ein Client im Broadcast-Client-Modus wartet, bevor er den Wert im Feld von <code>syncToRemoteServer</code> zu <code>notSynchronized</code> ändert, wenn der Client keine Broadcast-Pakete empfängt. Mögliche Werte: <ul style="list-style-type: none">▶ 128..2048 (Voreinstellung: 320)
Deaktiviere Client nach erfolgreicher Synchronisierung	Aktiviert/deaktiviert das Ausschalten des SNTP-Clients, wenn das Gerät die Zeit erfolgreich synchronisiert hat. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Das Ausschalten des SNTP-Clients ist aktiv. Das Gerät deaktiviert den SNTP-Client nach erfolgreicher Synchronisation der Zeit.▶ unmarkiert (Voreinstellung) Das Ausschalten des SNTP-Clients ist inaktiv. Der SNTP-Client bleibt nach erfolgreicher Synchronisation der Zeit aktiv.

■ Zustand

Parameter	Bedeutung
Zustand	<p>Zeigt den Zustand des SNTP-Clients.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ disabled Der SNTP-Client ist deaktiviert. ▶ notSynchronized Der SNTP-Client ist auf keinen SNTP- oder NTP-Server synchronisiert. ▶ synchronizedToRemoteServer Der SNTP-Client ist auf einen SNTP- oder NTP-Server synchronisiert.

■ Tabelle

In der Tabelle legen Sie die Einstellungen für bis zu 4 SNTP-Server fest.

Parameter	Bedeutung
Index	<p>Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..4 <p>Das Gerät legt diese Nummer automatisch fest. Wenn Sie einen Tabelleneintrag löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie einen neuen Tabelleneintrag erzeugen, schließt das Gerät die 1. Lücke.</p> <p>Das Gerät sendet nach dem Starten Anfragen an den SNTP-Server, der im 1. Tabelleneintrag konfiguriert ist. Bleibt die Antwort des Servers aus, sendet das Gerät seine Anfragen an den SNTP-Server, der im nächsten Tabelleneintrag konfiguriert ist.</p> <p>Antwortet vorübergehend keiner der konfigurierten SNTP-Server, verliert der SNTP-Client seine Synchronisation. Das Gerät fragt solange zyklisch nacheinander bei jedem SNTP-Server an, bis ein Server eine gültige Zeit liefert. Das Gerät synchronisiert sich auf diesen SNTP-Server, auch wenn die anderen Server später wieder erreichbar sind.</p>
Name	<p>Legt die Bezeichnung des SNTP-Servers fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
Adresse	<p>Legt die IP-Adresse des SNTP-Servers fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)
Ziel-UDP-Port	<p>Legt den UDP-Port fest, auf dem der SNTP-Server die Zeitinformationen erwartet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..65535 (Voreinstellung: 123) Ausnahme: Port 2222 ist für interne Funktionen reserviert.

Parameter	Bedeutung
Status	<p>Zeigt den Verbindungsstatus zwischen SNTP-Client und SNTP-Server.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>erfolgreich</code> Das Gerät hat die Zeit erfolgreich mit dem SNTP-Server synchronisiert.▶ <code>badDateEncoded</code> Die empfangene Zeitinformation enthält Protokollfehler, Synchronisation fehlgeschlagen.▶ <code>other</code><ul style="list-style-type: none">– Für die IP-Adresse des SNTP-Servers ist der Wert <code>0.0.0.0</code> eingetragen, Synchronisation fehlgeschlagen.oder– Der SNTP-Client verwendet einen anderen SNTP-Server.▶ <code>requestTimedOut</code> Das Gerät hat keine Antwort vom SNTP-Server erhalten, Synchronisation fehlgeschlagen.▶ <code>serverKissOfDeath</code> Der SNTP-Server ist überlastet. Das Gerät ist aufgefordert, sich mit einem anderen SNTP-Server zu synchronisieren. Steht kein anderer SNTP-Server zur Verfügung, fragt das Gerät in Abständen größer als im Feld <i>Request-Intervall [s]</i> eingestellt nach, ob der Server noch überlastet ist.▶ <code>serverUnsynchronized</code> Der SNTP-Server ist weder auf eine lokale noch auf eine externe Referenzzeitquelle synchronisiert, Synchronisation fehlgeschlagen.▶ <code>versionNotSupported</code> Die SNTP-Versionen auf Client und Server sind zueinander inkompatibel, Synchronisation fehlgeschlagen.
Aktiv	<p>Aktiviert/deaktiviert die Verbindung zum SNTP-Server.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Die Verbindung zum SNTP-Server ist aktiviert. Der SNTP-Client hat Zugriff auf den SNTP-Server.▶ <code>unmarkiert (Voreinstellung)</code> Die Verbindung zum SNTP-Server ist deaktiviert. Der SNTP-Client hat keinen Zugriff auf den SNTP-Server.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

2.3.2 SNTP Server

In diesem Dialog legen Sie die Einstellungen fest, mit denen das Gerät als SNTP-Server arbeitet.

Der SNTP-Server stellt die koordinierte Weltzeit (UTC) zur Verfügung, ohne lokale Zeitverschiebungen zu berücksichtigen.

Bei entsprechender Einstellung arbeitet der SNTP-Server im Broadcast-Modus: Der SNTP-Server sendet im Broadcast-Modus automatisch Broadcast-Nachrichten oder Multicast-Nachrichten im Broadcast-Sendeintervall.

■ Funktion

Parameter	Bedeutung
Funktion	<p>Schaltet die <i>SNTP Server</i>-Funktion des Geräts ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An Die <i>SNTP Server</i>-Funktion ist eingeschaltet. Das Gerät arbeitet als SNTP-Server. ▶ Aus (Voreinstellung) Die <i>SNTP Server</i>-Funktion ist ausgeschaltet. <p>Beachten Sie die Einstellung des Kontrollkästchens <i>Server deaktivieren bei lokaler Zeitquelle</i> im Rahmen <i>Konfiguration</i>.</p>

■ Konfiguration

Parameter	Bedeutung
UDP-Port	<p>Legt die Nummer des UDP-Ports fest, auf dem der SNTP-Server des Geräts Anfragen anderer Clients entgegennimmt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..65535 (Voreinstellung: 123) Ausnahme: Port 2222 ist für interne Funktionen reserviert.
Broadcast-Admin-Modus	<p>Aktiviert/deaktiviert den Broadcast-Modus:</p> <ul style="list-style-type: none"> ▶ markiert Der SNTP-Server beantwortet Anfragen von SNTP-Clients im Unicast-Modus und sendet zusätzlich SNTP-Pakete im Broadcast-Modus als Broadcast oder Multicast. ▶ unmarkiert (Voreinstellung) Der SNTP-Server beantwortet Anfragen von SNTP-Clients im Unicast-Modus.
Broadcast-Ziel-Adresse	<p>Legt die IP-Adresse fest, an die der SNTP-Server des Geräts die SNTP-Pakete im Broadcast-Modus sendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0) <p>Broadcast- und Multicast-Adressen sind zulässig.</p>
Broadcast-UDP-Port	<p>Legt die Nummer des UDP-Ports fest, auf dem der SNTP-Server die SNTP-Pakete im Broadcast-Modus sendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..65535 (Voreinstellung: 123) Ausnahme: Port 2222 ist für interne Funktionen reserviert.

Parameter	Bedeutung
Broadcast VLAN-ID	Legt die ID des VLANs fest, in welchem der SNTP-Server des Geräts die SNTP-Pakete im Broadcast-Modus sendet. Mögliche Werte: <ul style="list-style-type: none">▶ 0 Der SNTP-Server sendet die SNTP-Pakete im selben VLAN, in dem der Management-Zugriff auf das Gerät möglich ist. Siehe Dialog <i>Grundeinstellungen</i> > <i>Netz</i>.▶ 1..4042 (Voreinstellung: 1)
Broadcast-Sende-Intervall [s]	Legt den Zeitabstand fest, in dem der SNTP-Server des Geräts SNTP-Broadcast Pakete sendet. Mögliche Werte: <ul style="list-style-type: none">▶ 64..1024 (Voreinstellung: 128)
Server deaktivieren bei lokaler Zeitquelle	Aktiviert/deaktiviert das Ausschalten des SNTP-Broadcast-Servers, wenn sich das Gerät auf die lokale Uhr synchronisiert hat. Mögliche Werte: <ul style="list-style-type: none">▶ <code>markiert</code> Das Ausschalten des SNTP-Broadcast-Servers ist aktiv. Das Gerät deaktiviert den SNTP-Broadcast-Server, wenn das Gerät auf die lokale Uhr synchronisiert ist. Anfragen von SNTP-Clients beantwortet der SNTP-Server weiterhin. Im SNTP-Paket teilt der SNTP-Server den Clients mit, dass er lokal synchronisiert ist.▶ <code>unmarkiert</code> (Voreinstellung) Das Ausschalten des SNTP-Broadcast-Servers ist inaktiv. Der SNTP-Broadcast-Server bleibt aktiv, wenn das Gerät auf die lokale Uhr synchronisiert ist.

■ Zustand

Parameter	Bedeutung
Zustand	Zeigt den Zustand des SNTP-Servers. Mögliche Werte: <ul style="list-style-type: none">▶ <code>disabled</code> Der SNTP-Server ist deaktiviert.▶ <code>notSynchronized</code> Der SNTP-Server ist weder auf eine lokale noch auf eine externe Referenzzeitquelle synchronisiert.▶ <code>syncToLocal</code> Der SNTP-Server ist synchronisiert auf die Hardware-Uhr des Geräts.▶ <code>syncToRefclock</code> Der SNTP-Server ist synchronisiert auf eine externe Referenzzeitquelle, zum Beispiel PTP.▶ <code>syncToRemoteServer</code> Der SNTP-Server ist synchronisiert auf einen SNTP-Server, der in einer Kaskade dem Gerät übergeordnet ist.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

2.4 PTP

Das Menü enthält die folgenden Dialoge:

- ▶ PTP Global
- ▶ PTP Boundary Clock
- ▶ PTP Transparent Clock

2.4.1 PTP Global

Das Precision Time Protocol (PTP) ist ein in der Norm IEEE 1588-2008 beschriebenes Verfahren, das die Geräte im Netz mit einer exakten Uhrzeit versorgt. Das Verfahren erlaubt, die Uhren im Netz mit Genauigkeiten von wenigen 100 ns zu synchronisieren. Das Protokoll verwendet Multicast-Kommunikation, weshalb die PTP-Synchronisationsnachrichten das Netz kaum belasten.

PTP ist erheblich genauer als SNTP. Sind im Gerät beide Protokolle eingeschaltet, dann hat PTP Vorrang.

Anhand des „Best Master Clock“-Algorithmus bestimmen die Geräte im Netz das Gerät mit der genauesten Zeit zur Referenzzeitquelle (Grandmaster). Anschließend synchronisieren sich die beteiligten Geräte auf diese Referenzzeitquelle.

Möchten Sie die PTP-Zeit präzise durch Ihr Netz transportieren, verwenden Sie in den Transportpfaden ausschließlich Geräte mit PTP-Hardware-Unterstützung.

Das Protokoll unterscheidet zwischen den folgenden Uhren:

- ▶ **Boundary Clock (BC)**
Diese Uhr besitzt beliebig viele PTP-Ports und arbeitet zugleich als PTP-Master und als PTP-Slave. Im jeweiligen Netzsegment verhält sich die Uhr wie eine Ordinary Clock.
 - Als PTP-Slave synchronisiert sich die Uhr auf einen PTP-Master, der in der Kaskade dem Gerät übergeordnet ist.
 - Als PTP-Master gibt die Uhr die Zeitinformation über das Netz an PTP-Slaves weiter, die in der Kaskade dem Gerät untergeordnet sind.
- ▶ **Transparent Clock (TC)**
Diese Uhr besitzt beliebig viele PTP-Ports. Im Gegensatz zur Boundary Clock korrigiert die Uhr ausschließlich die Zeitinformation vor Weitergabe, ohne sich selbst zu synchronisieren.

In diesem Dialog legen Sie grundlegende Einstellungen für PTP fest

■ Funktion IEEE1588/PTP

Parameter	Bedeutung
Funktion IEEE1588/ PTP	Schaltet die <i>PTP</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>PTP</i>-Funktion ist eingeschaltet. Das Gerät synchronisiert seine Uhr mit PTP. Wenn gleichzeitig SNTP im Gerät eingeschaltet ist, dann hat PTP Vorrang.▶ Aus (Voreinstellung) Die <i>PTP</i>-Funktion ist ausgeschaltet. Das Gerät vermittelt PTP-Synchronisationsnachrichten ohne Korrektur an jeden Port.

■ Konfiguration IEEE1588/PTP

Parameter	Bedeutung
PTP-Modus	Legt die PTP-Version und den Modus der lokalen Uhr fest. Mögliche Werte: <ul style="list-style-type: none">▶ v2-transparent-clock (Voreinstellung)▶ v2-boundary-clock

Parameter	Bedeutung
Untere Synchronisations-Schwelle [ns]	<p>Legt den unteren Schwellwert in Nanosekunden fest für den Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (Grandmaster). Unterschreitet der Gangunterschied einmalig diesen Wert, dann gilt die lokale Uhr als synchronisiert.</p> <p>Mögliche Werte: ▶ 0..999999999 (Voreinstellung: 30)</p>
Obere Synchronisations-Schwelle [ns]	<p>Legt den oberen Grenzwert in Nanosekunden fest für den Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (Grandmaster). Überschreitet der Gangunterschied einmalig diesen Wert, dann gilt die lokale Uhr als unsynchronisiert.</p> <p>Mögliche Werte: ▶ 31..1000000000 (Voreinstellung: 5000)</p>
PTP-Management	<p>Aktiviert/deaktiviert das in der PTP-Norm definierte PTP-Management.</p> <p>Mögliche Werte: ▶ <code>markiert</code> PTP-Management ist aktiviert. ▶ <code>unmarkiert</code> (Voreinstellung) PTP-Management ist deaktiviert.</p>

■ Status

Parameter	Bedeutung
Ist synchronisiert	<p>Zeigt, ob die lokale Uhr mit der Referenzzeitquelle (Grandmaster) synchronisiert ist. Die lokale Uhr ist synchronisiert, sobald der Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (Grandmaster) einmalig den unteren Synchronisations-Grenzwert unterschreitet. Dieser Zustand bleibt so lange erhalten, bis der Gangunterschied den oberen Synchronisations-Grenzwert einmalig überschreitet. Die Synchronisations-Grenzwerte legen Sie fest im Rahmen <i>Konfiguration IEEE1588/PTP</i>.</p>
Max. Offset absolut [ns]	<p>Zeigt den maximalen Gangunterschied in Nanosekunden, der aufgetreten ist, seitdem die lokale Uhr mit der Referenzzeitquelle (Grandmaster) synchronisiert ist.</p>
PTP-Zeit	<p>Zeigt Datum und Zeit der PTP-Zeitskala, wenn die lokale Uhr mit der Referenzzeitquelle (Grandmaster) synchronisiert ist. Format: <code>TT.MM.JJJJ hh:mm:ss</code></p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

2.4.2 PTP Boundary Clock

Dieses Menü bietet Ihnen die Möglichkeit, die Einstellungen für den Boundary-Clock-Modus der lokalen Uhr festzulegen.

Das Menü enthält die folgenden Dialoge:

- ▶ [PTP Boundary Clock Global](#)
- ▶ [PTP Boundary Clock Port](#)

2.4.2.1 PTP Boundary Clock Global

In diesem Dialog legen Sie allgemeine, portübergreifende Einstellungen für den Boundary-Clock-Modus der lokalen Uhr fest. Die Boundary Clock (BC) arbeitet gemäß PTP Version 2 (IEEE 1588-2008).

Die Einstellungen sind wirksam, wenn die lokale Uhr als Boundary Clock (BC) arbeitet. Wählen Sie dazu im Dialog *Zeit > PTP > Global* im Feld *PTP-Modus* den Wert *v2-boundary-clock*.

■ Funktion IEEE1588/PTPv2 BC

Parameter	Bedeutung
Priorität 1	<p>Legt die Priorität 1 des Geräts fest.</p> <p>Mögliche Werte: ▶ 0..255 (Voreinstellung: 128)</p> <p>Der „Best Master Clock“-Algorithmus bewertet zuerst die Priorität 1 der beteiligten Geräte, um die Referenzzeitquelle (Grandmaster) zu bestimmen. Je niedriger Sie den Wert einstellen, desto wahrscheinlicher wird das Gerät Referenzzeitquelle (Grandmaster). Siehe Rahmen <i>Grandmaster</i>.</p>
Priorität 2	<p>Legt die Priorität 2 des Geräts fest.</p> <p>Mögliche Werte: ▶ 0..255 (Voreinstellung: 128)</p> <p>Der „Best Master Clock“-Algorithmus bewertet die Priorität 2 der beteiligten Geräte, wenn die zuvor bewerteten Kriterien bei mehreren Geräten gleich sind. Je niedriger Sie den Wert einstellen, desto wahrscheinlicher wird das Gerät Referenzzeitquelle (Grandmaster). Siehe Rahmen <i>Grandmaster</i>.</p>
Domänen-Nummer	<p>Weist das Gerät einer PTP-Domäne zu.</p> <p>Mögliche Werte: ▶ 0..255 (Voreinstellung: 0)</p> <p>Das Gerät überträgt Zeitinformationen ausschließlich von und zu Geräten in derselben Domäne.</p>

■ Status IEEE1588/PTPv2 BC

Parameter	Bedeutung
Two step	Zeigt, dass die Uhr im Two-Step-Modus arbeitet.
Steps removed	<p>Zeigt die Anzahl der durchlaufenen Kommunikationspfade zwischen der lokalen Uhr des Geräts und der Referenzzeitquelle (Grandmaster). Für einen PTP-Slave bedeutet der Wert 1, dass die Uhr direkt über 1 Kommunikationspfad mit der Referenzzeitquelle (Grandmaster) verbunden ist.</p>
Offset zum Master [ns]	<p>Zeigt die gemessene Differenz (Offset) zwischen lokaler Uhr und Referenzzeitquelle (Grandmaster) in Nanosekunden. Der PTP-Slave berechnet die Differenz aus den empfangenen Zeitinformationen.</p> <p>Im Two-Step-Modus besteht die Zeitinformation aus je 2 PTP-Synchronisationsnachrichten, die der PTP-Master zyklisch sendet:</p> <ul style="list-style-type: none"> ▶ Die 1. Synchronisationsnachricht (Sync Message) enthält einen geschätzten Wert des exakten Sendezeitpunktes der Nachricht. ▶ Die 2. Synchronisationsnachricht (Follow-Up Message) enthält den exakten Sendezeitpunkt der 1. Nachricht. <p>Der PTP-Slave berechnet aus beiden PTP-Synchronisationsnachrichten die Differenz (Offset) zum Master und korrigiert seine Uhr um diesen Differenz. Dabei berücksichtigt der PTP-Slave die <i>Laufzeit zum Master [ns]</i>.</p>

Parameter	Bedeutung
Laufzeit zum Master [ns]	Zeigt die Laufzeit (Delay) beim Übertragen der PTP-Synchronisationsnachrichten vom PTP-Master zum PTP-Slave in Nanosekunden. Der PTP-Slave sendet ein „Delay Request“-Paket an den PTP-Master und ermittelt dabei die exakte Sendezeit des Pakets. Der PTP-Master generiert bei Empfang des Pakets einen Zeitstempel und sendet diesen in einem „Delay Response“-Paket an den PTP-Slave zurück. Der PTP-Slave berechnet aus beiden Paketen die Laufzeit (Delay) und berücksichtigt sie ab der nächsten Offset-Messung. Voraussetzung ist, dass für den Laufzeitmess-Mechanismus des Slave-Ports der Wert <code>e2e</code> festgelegt ist.

■ Grandmaster

Der Rahmen zeigt die Kriterien, die der „Best Master Clock“-Algorithmus beim Bestimmen der Referenzzeitquelle (Grandmaster) bewertet.

Der Algorithmus bewertet zuerst die Priorität 1 der beteiligten Geräte. Das Gerät mit dem kleinsten Wert für die Priorität 1 wird Referenzzeitquelle (Grandmaster). Ist der Wert bei mehreren Geräten gleich, zieht der Algorithmus das nächste Kriterium heran, bei erneuter Übereinstimmung das jeweils nächste Kriterium. Wenn jeder Wert bei mehreren Geräten gleich ist, entscheidet der kleinste Wert im Feld *Uhr-Kennung*, welches Gerät Referenzzeitquelle (Grandmaster) wird.

Das Gerät bietet Ihnen die Möglichkeit, selbst Einfluss darauf zu nehmen, welches Gerät im Netz Referenzzeitquelle (Grandmaster) wird. Passen Sie dazu im Rahmen *Funktion IEEE1588/PTPv2 BC* den Wert im Feld *Priorität 1* oder im Feld *Priorität 2* an.

Parameter	Bedeutung
Priorität 1	Zeigt die Priorität 1 des Geräts, das gegenwärtig Referenzzeitquelle (Grandmaster) ist.
Uhren-Klasse	Klasse der Referenzzeitquelle (Grandmaster), auch bezeichnet als ‚Clock class‘. Kenngröße für den Best-Master-Clock-Algorithmus.
Präzision	Geschätzte Ganggenauigkeit der Referenzzeitquelle (Grandmaster), auch bezeichnet als ‚Clock accuracy‘. Kenngröße für den Best-Master-Clock-Algorithmus.
Uhren-Varianz	Varianz der Referenzzeitquelle, auch bezeichnet als ‚Offset scaled log variance‘. Kenngröße für den Best-Master-Clock-Algorithmus.
Priorität 2	Zeigt die Priorität 2 des Geräts, das gegenwärtig Referenzzeitquelle (Grandmaster) ist.

■ Lokale Zeit-Eigenschaften

Parameter	Bedeutung
Quelle der Zeit	Legt fest, von welcher Zeitquelle die lokale Uhr ihre Zeitinformation bezieht. Mögliche Werte: <ul style="list-style-type: none"> ▶ atomicClock ▶ gps ▶ terrestrialRadio ▶ ptp ▶ ntp ▶ handSet ▶ other ▶ internalOscillator (Voreinstellung)

Parameter	Bedeutung
UTC-Offset [s]	<p>Legt die Differenz der PTP-Zeitskala zur UTC fest. Siehe Kontrollkästchen <i>PTP-Zeitskala</i>.</p> <p>Mögliche Werte: ▶ -32768..32767</p> <p>Anmerkung: Voreingestellt ist der zum Zeitpunkt der Erstellung der Geräte-Software gültige Wert. Weitere Informationen finden Sie im „Bulletin C“ des International Earth Rotation and Reference Systems Service (IERS): http://www.iers.org/iers/EN/Publications/Bulletins/bulletins.html</p>
UTC-Offset gültig	<p>Legt fest, ob der im Feld <i>UTC-Offset [s]</i> festgelegte Wert korrekt ist.</p> <p>Mögliche Werte: ▶ markiert ▶ unmarkiert (Voreinstellung)</p>
Zeit nachvollziehbar	<p>Zeigt, ob das Gerät die Zeit von einer primären UTC-Referenz bezieht, zum Beispiel von einem NTP-Server.</p> <p>Mögliche Werte: ▶ markiert ▶ unmarkiert</p>
Frequenz nachvollziehbar	<p>Zeigt, ob das Gerät die Frequenz von einer primären UTC-Referenz bezieht, zum Beispiel von einem NTP-Server.</p> <p>Mögliche Werte: ▶ markiert ▶ unmarkiert</p>
PTP-Zeitskala	<p>Zeigt, ob das Gerät die PTP-Zeitskala verwendet.</p> <p>Mögliche Werte: ▶ markiert ▶ unmarkiert</p> <p>Die PTP-Zeitskala ist laut IEEE 1588 die Atomzeit TAI mit dem Startzeitpunkt 01.01.1970. Im Gegensatz zu UTC kennt TAI keine Schaltsekunden. Die Differenz zwischen TAI und UTC betrug am 01.01.2011 +34 Sekunden.</p>

■ Kennungen

Parameter	Bedeutung
Uhr-Kennung	Zeigt die eigene Identifikationsnummer (UUID) des Geräts.
Port-Kennung Parent	Zeigt die Port-Identifikationsnummer (UUID) des direkt übergeordneten Master-Geräts.
Grandmaster-Kennung	Zeigt die Identifikationsnummer (UUID) des Referenzzeitquellen-Geräts.

Das Gerät zeigt die Kennungen als Byte-Folge in Hexadezimalnotation.

Die Identifikationsnummern (UUID) setzen sich wie folgt zusammen:

- ▶ Die Geräte-Identifikationsnummer besteht aus der MAC-Adresse des Geräts, erweitert um die Werte *ff* und *fe* zwischen Byte 3 und Byte 4.
- ▶ Die Port-UUID besteht aus der Geräte-Identifikationsnummer, gefolgt von einer 16-bit-Port-ID.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

2.4.2.2 PTP Boundary Clock Port

In diesem Dialog legen Sie für jeden einzelnen Port die Einstellungen der Boundary Clock (BC) fest. Die Einstellungen sind wirksam, wenn die lokale Uhr als Boundary Clock (BC) arbeitet. Wählen Sie dazu im Dialog *Zeit > PTP > Global* im Feld *PTP-Modus* den Wert `v2-boundary-clock`.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
PTP an	Aktiviert/deaktiviert die Übertragung von PTP-Synchronisationsnachrichten auf dem Port. Mögliche Werte: <ul style="list-style-type: none">▶ <code>markiert</code> (Voreinstellung) Die Übertragung ist aktiviert. Der Port sendet und empfängt PTP-Synchronisationsnachrichten.▶ <code>unmarkiert</code> Die Übertragung ist deaktiviert. Der Port blockiert PTP-Synchronisationsnachrichten.
PTP-Status	Zeigt den gegenwärtigen Zustand des Ports. Mögliche Werte: <ul style="list-style-type: none">▶ <code>initializing</code> Initialisierungsphase▶ <code>faulty</code> Faulty Modus: Fehler im PTP-Protokoll.▶ <code>disabled</code> PTP ist auf dem Port ausgeschaltet.▶ <code>listening</code> Port wartet auf PTP-Synchronisationsnachrichten.▶ <code>pre-master</code> PTP-Pre-Master-Modus▶ <code>master</code> PTP-Master-Modus▶ <code>passiv</code> PTP-Passiv-Modus▶ <code>uncalibrated</code> PTP-Unkalibriert-Modus▶ <code>slave</code> PTP-Slave-Modus
Sync-Intervall [s]	Legt das Intervall in Sekunden fest, in welchem der Port PTP-Synchronisationsnachrichten überträgt. Mögliche Werte: <ul style="list-style-type: none">▶ 0.25▶ 0.5▶ 1 (Voreinstellung)▶ 2

Parameter	Bedeutung
Laufzeitmess-Mechanismus	<p>Legt den Mechanismus fest, mit dem das Gerät die Laufzeit (Delay) beim Übertragen der PTP-Synchronisationsnachrichten misst.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ disabled Die Messung der Laufzeit (Delay) der PTP-Synchronisationsnachrichten zu den angeschlossenen PTP-Geräten ist deaktiviert. ▶ e2e (Voreinstellung) End-to-End: Als PTP-Slave misst der Port die Laufzeit der PTP-Synchronisationsnachrichten zum PTP-Master. Das Gerät zeigt den Messwert im Dialog <i>Zeit > PTP > Boundary Clock > Global</i> an. ▶ p2p Peer-to-Peer: Das Gerät misst die Laufzeit (Delay) der PTP-Synchronisationsnachrichten zu allen angeschlossenen PTP-Geräten, vorausgesetzt, diese Geräte unterstützen P2P. Dieser Mechanismus erspart dem Gerät im Fall einer Rekonfiguration, die Laufzeit erneut zu ermitteln. Wenn Sie diesen Wert festlegen, ist in Spalte <i>Netz-Protokoll</i> ausschließlich der Wert IEEE 802.3 verfügbar.
P2P-Laufzeit	<p>Zeigt die gemessene Peer-to-Peer-Laufzeit der PTP-Synchronisationsnachrichten. Voraussetzung ist, dass Sie in Spalte <i>Laufzeitmess-Mechanismus</i> den Wert p2p festlegen.</p>
P2P-Laufzeitmess-Intervall [s]	<p>Legt das Intervall in Sekunden fest, in welchem der Port die Peer-to-Peer-Laufzeit misst. Voraussetzung ist, dass Sie den Wert p2p an diesem Port und am Port der Gegenstelle eingestellt haben.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1 (Voreinstellung) ▶ 2 ▶ 4 ▶ 8 ▶ 16 ▶ 32
Netz-Protokoll	<p>Legt fest, welches Protokoll der Port für das Übertragen der PTP-Synchronisationsnachrichten verwendet.</p> <p>Wenn Sie den Wert für einen Port ändern, ändert das Gerät nach Klicken der Schaltfläche <input checked="" type="checkbox"/> jeden Port auf diesen Wert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ IEEE 802.3 (Voreinstellung) ▶ UDP/IPv4 Dieser Wert ist ausschließlich dann verfügbar, wenn in Spalte <i>Laufzeitmess-Mechanismus</i> ein anderer Wert als P2P festgelegt ist.
Announce-Intervall [s]	<p>Legt das Intervall in Sekunden fest, in welchem der Port Nachrichten für die PTP-Topologieerkennung überträgt. Weisen Sie jedem Gerät einer PTP-Domäne denselben Wert zu.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1 ▶ 2 (Voreinstellung) ▶ 4 ▶ 8 ▶ 16
Announce-Timeout	<p>Legt die Anzahl der Announce-Intervalle fest.</p> <p>Beispiel: In der Voreinstellung (<i>Announce-Intervall [s]</i> = 2 und <i>Announce-Timeout</i> = 3) beträgt das Timeout 3 x 2 s = 6 s.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 2..10 (Voreinstellung: 3) Weisen Sie jedem Gerät einer PTP-Domäne denselben Wert zu.
E2E-Laufzeitmess-Intervall [s]	<p>Zeigt das Intervall in Sekunden an, in welchem der Port die End-to-End-Laufzeit misst:</p> <ul style="list-style-type: none"> ▶ Arbeitet der Port als PTP-Master, weist das Gerät dem Port den Wert 8 zu. ▶ Arbeitet der Port als PTP-Slave, legt der mit dem Port verbundene PTP-Master den Wert fest.

Parameter	Bedeutung
V1-Hardware-Kompatibilität	<p>Legt fest, ob der Port die Länge der PTP-Synchronisationsnachrichten anpasst, wenn Sie in Spalte <i>Netz-Protokoll</i> den Wert <code>udpIpv4</code> eingestellt haben.</p> <p>Unter Umständen erwarten andere Geräte im Netz die PTP-Synchronisationsnachrichten in der Länge von PTPv1-Nachrichten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>auto</code> (Voreinstellung) Das Gerät erkennt automatisch, ob andere Geräte im Netz PTP-Synchronisationsnachrichten in der Länge von PTPv1-Nachrichten erwarten. Ist das der Fall, erweitert das Gerät die Länge der PTP-Synchronisationsnachrichten vor dem Übertragen. ▶ <code>on</code> Das Gerät erweitert die Länge der PTP-Synchronisationsnachrichten vor dem Übertragen. ▶ <code>off</code> Das Gerät überträgt PTP-Synchronisationsnachrichten und behält die Länge bei.
Asymmetrie	<p>Korrigiert den durch asymmetrische Übertragungswege verfälschten Laufzeitmesswert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>-2000000000..2000000000</code> (Voreinstellung: 0) <p>Der Wert repräsentiert die Laufzeitasymmetrie in Nanosekunden. Ein Laufzeitmesswert von x ns entspricht einer Asymmetrie von x·2 ns. Der Wert ist positiv, wenn die Laufzeit vom PTP-Master zum PTP-Slave länger ist als in umgekehrter Richtung.</p>
VLAN	<p>Legt die VLAN-ID fest, mit der das Gerät die PTP-Synchronisationsnachrichten an diesem Port markiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>kein</code> (Voreinstellung) Das Gerät überträgt PTP-Synchronisationsnachrichten ohne VLAN-Tag. ▶ <code>0..4042</code> VLANs, die Sie im Gerät bereits eingerichtet haben, wählen Sie in der Liste aus. <p>Stellen Sie sicher, dass der Port Mitglied des VLANs ist. Siehe Dialog <i>Switching > VLAN > Konfiguration</i>.</p>
VLAN-Priorität	<p>Legt die Priorität fest, mit der das Gerät die mit VLAN-ID markierten PTP-Synchronisationsnachrichten überträgt (Schicht 2, IEEE 802.1D).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>0..7</code> (Voreinstellung: 4) <p>Haben Sie in Spalte <i>VLAN</i> den Wert <code>kein</code> festgelegt, ignoriert das Gerät die VLAN-Priorität.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

2.4.3 PTP Transparent Clock

Dieses Menü bietet Ihnen die Möglichkeit, die Einstellungen für den Transparent-Clock-Modus der lokalen Uhr festzulegen.

Das Menü enthält die folgenden Dialoge:

- ▶ [PTP Transparent Clock Global](#)
- ▶ [PTP Transparent Clock Port](#)

2.4.3.1 PTP Transparent Clock Global

In diesem Dialog legen Sie allgemeine, portübergreifende Einstellungen für den Transparent-Clock-Modus der lokalen Uhr fest. Die Transparent Clock (TC) arbeitet gemäß PTP Version 2 (IEEE 1588-2008).

Die Einstellungen sind wirksam, wenn die lokale Uhr als Transparent Clock (TC) arbeitet. Wählen Sie dazu im Dialog *Zeit > PTP > Global* im Feld *PTP-Modus* den Wert *v2-transparent-clock*.

■ Funktion IEEE1588/PTPv2 TC

Parameter	Bedeutung
Laufzeitmess-Mechanismus	<p>Legt den Mechanismus fest, mit dem das Gerät die Laufzeit (Delay) beim Übertragen der PTP-Synchronisationsnachrichten misst.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>e2e</i> (Voreinstellung) Als PTP-Slave misst der Port die Laufzeit der PTP-Synchronisationsnachrichten zum PTP-Master. Das Gerät zeigt den Messwert im Dialog <i>Zeit > PTP > Transparent Clock > Global</i> an.▶ <i>p2p</i> Das Gerät misst die Laufzeit (Delay) der PTP-Synchronisationsnachrichten zu allen angeschlossenen PTP-Geräten, vorausgesetzt, diese Geräte unterstützen P2P. Dieser Mechanismus erspart dem Gerät im Fall einer Rekonfiguration, die Laufzeit erneut zu ermitteln. Wenn Sie diesen Wert festlegen, ist im Feld <i>Netz-Protokoll</i> ausschließlich der Wert <i>IEEE 802.3</i> verfügbar.▶ <i>e2e-optimized</i> Wie <i>e2e</i>, mit folgenden Besonderheiten:<ul style="list-style-type: none">– Delay-Anfragen der PTP-Slaves vermittelt das Gerät ausschließlich an den PTP-Master, obwohl diese Anfragen Multicast-Nachrichten sind. Das Gerät entlastet damit die anderen Geräte von unnötigen Multicast-Anfragen.– Wenn sich die Master-Slave-Topologie ändert, lernt das Gerät den Port zum PTP-Master um, sobald es eine Synchronisationsnachricht von einem anderen PTP-Master empfängt.– Kennt das Gerät keinen PTP-Master, überträgt es Delay-Anfragen an allen Ports.▶ <i>disabled</i> Auf dem Port ist die Laufzeitmessung ausgeschaltet. Das Gerät verwirft Nachrichten für die Laufzeitmessung.
Primäre Domäne	<p>Weist das Gerät einer PTP-Domäne zu.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>0..255</i> (Voreinstellung: 0) <p>Das Gerät überträgt Zeitinformationen ausschließlich von und zu Geräten in derselben Domäne.</p>
Netz-Protokoll	<p>Legt fest, welches Protokoll der Port für das Übertragen der PTP-Synchronisationsnachrichten verwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>ieee8023</i> (Voreinstellung)▶ <i>udpIpv4</i> Ausschließlich dann verfügbar, wenn in der Optionsliste <i>Laufzeitmess-Mechanismus</i> ein anderes Optionsfeld als <i>p2p</i> ausgewählt ist.
Multi-Domain-Modus	<p>Aktiviert/deaktiviert in jeder PTP-Domäne die Korrektur von PTP-Synchronisationsnachrichten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Das Gerät korrigiert PTP-Synchronisationsnachrichten in allen PTP-Domänen.▶ <i>unmarkiert</i> (Voreinstellung) Das Gerät korrigiert PTP-Synchronisationsnachrichten ausschließlich in der primären PTP-Domäne. Siehe Feld <i>Primäre Domäne</i>.

Parameter	Bedeutung
VLAN-ID	<p>Legt die VLAN-ID fest, mit der das Gerät die PTP-Synchronisationsnachrichten an diesem Port markiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ kein (Voreinstellung) Das Gerät überträgt PTP-Synchronisationsnachrichten ohne VLAN-Tag. ▶ 0..4042 VLANs, die Sie im Gerät bereits eingerichtet haben, wählen Sie in der Liste aus.
VLAN-Priorität	<p>Legt die Priorität fest, mit der das Gerät die mit VLAN-ID markierten PTP-Synchronisationsnachrichten überträgt (Schicht 2, IEEE 802.1D).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..7 (Voreinstellung: 4) <p>Haben Sie im Feld <i>VLAN-ID</i> den Wert none festgelegt, ignoriert das Gerät den hier eingestellten Wert.</p>

■ Lokale Synchronisation

Parameter	Bedeutung
Syntonize	<p>Aktiviert/deaktiviert die Frequenz-Synchronisation der Transparent Clock mit dem PTP-Master.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Die Frequenz-Synchronisation ist aktiv. Das Gerät synchronisiert die Frequenz. ▶ unmarkiert Die Frequenz-Synchronisation ist inaktiv. Die Frequenz bleibt konstant.
Lokale Uhr synchronisieren	<p>Aktiviert/deaktiviert die Synchronisation der lokalen Systemzeit.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die Synchronisation ist aktiv. Das Gerät synchronisiert die lokale Systemzeit mit der per PTP empfangenen Uhrzeit. Voraussetzung ist, dass das Kontrollkästchen <i>Syntonize</i> markiert ist. ▶ unmarkiert (Voreinstellung) Die Synchronisation ist inaktiv. Die lokale Systemzeit bleibt konstant.
Aktueller Master	<p>Zeigt die Port-Identifikationsnummer (UUID) des Master-Geräts, auf welches das Gerät seine Frequenz synchronisiert.</p> <p>Enthält der Wert ausschließlich Nullen, hat das die folgende Ursache:</p> <ul style="list-style-type: none"> ▶ Die <i>Syntonize</i>-Funktion ist ausgeschaltet. oder ▶ Das Gerät findet keinen PTP-Master.
Offset zum Master [ns]	<p>Zeigt die gemessene Differenz (Offset) zwischen lokaler Uhr und dem PTP-Master in Nanosekunden. Das Gerät berechnet den die Differenz aus den empfangenen Zeitinformationen. Voraussetzung ist, dass die Funktion <i>Lokale Uhr synchronisieren</i> eingeschaltet ist.</p>
Laufzeit zum Master [ns]	<p>Zeigt die Laufzeit (Delay) beim Übertragen der PTP-Synchronisationsnachrichten vom PTP-Master zum PTP-Slave in Nanosekunden.</p> <p>Voraussetzung:</p> <ul style="list-style-type: none"> ▶ Die <i>Lokale Uhr synchronisieren</i>-Funktion ist eingeschaltet. ▶ Im Feld <i>Laufzeitmess-Mechanismus</i> ist der Wert <i>e2e</i> ausgewählt.

■ Status IEEE1588/PTPv2 TC

Parameter	Bedeutung
Uhr-Kennung	Zeigt die eigene Identifikationsnummer (UUID) des Geräts. Das Gerät zeigt die Kennungen als Byte-Folge in Hexadezimalnotation. Die Geräte-Identifikationsnummer besteht aus der MAC-Adresse des Geräts, erweitert um die Werte ff und fe zwischen Byte 3 und Byte 4.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

2.4.3.2 PTP Transparent Clock Port

In diesem Dialog legen Sie für jeden einzelnen Port die Einstellungen der Transparent Clock (TC) fest. Die Einstellungen sind wirksam, wenn die lokale Uhr als Transparent Clock (TC) arbeitet. Wählen Sie dazu im Dialog *Zeit > PTP > Global* im Feld *PTP-Modus* den Wert *v2-transparent-clock*.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
PTP an	Aktiviert/deaktiviert die Übertragung von PTP-Synchronisationsnachrichten auf dem Port. Mögliche Werte: ▶ <i>markiert</i> (Voreinstellung) Die Übertragung ist aktiv. Der Port sendet und empfängt PTP-Synchronisationsnachrichten. ▶ <i>unmarkiert</i> Die Übertragung ist inaktiv. Der Port blockiert PTP-Synchronisationsnachrichten.
P2P-Laufzeitmess-Intervall [s]	Legt das Intervall in Sekunden fest, in welchem der Port die Peer-to-Peer-Laufzeit misst. Voraussetzung ist, dass Sie den Wert <i>p2p</i> auf diesem Port und auf dem Port der Gegenstelle festlegen. Siehe Optionsliste <i>Laufzeitmess-Mechanismus</i> im Dialog <i>p2p</i> . Mögliche Werte: ▶ 1 (Voreinstellung) ▶ 2 ▶ 4 ▶ 8 ▶ 16 ▶ 32
P2P-Laufzeit	Zeigt die gemessene Peer-to-Peer-Laufzeit der PTP-Synchronisationsnachrichten. Voraussetzung ist, dass Sie in der Optionsliste <i>Laufzeitmess-Mechanismus</i> das Optionfeld <i>p2p</i> auswählen. Siehe Feld <i>Laufzeitmess-Mechanismus</i> im Dialog <i>p2p</i> .
Asymmetrie	Korrigiert den durch asymmetrische Übertragungswege verfälschten Laufzeitmesswert. Mögliche Werte: ▶ -2000000000..2000000000 (Voreinstellung: 0) Der Wert repräsentiert die Laufzeitasymmetrie in Nanosekunden. Ein Laufzeitmesswert von <i>x</i> ns entspricht einer Asymmetrie von <i>x</i> ·2 ns. Der Wert ist positiv, wenn die Laufzeit vom PTP-Master zum PTP-Slave länger ist als in umgekehrter Richtung.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

3 Gerätesicherheit

Das Menü enthält die folgenden Dialoge:

- ▶ [Benutzerverwaltung](#)
- ▶ [Authentifizierungs-Liste](#)
- ▶ [Management-Zugriff](#)
- ▶ [Pre-Login-Banner](#)

3.1 Benutzerverwaltung

Das Gerät gewährt Benutzern Zugriff auf das Management, wenn diese sich mit gültigen Zugangsdaten anmelden.

In diesem Dialog verwalten Sie die Benutzer der lokalen Benutzerverwaltung. Außerdem legen Sie hier die folgenden Einstellungen fest:

- ▶ Einstellungen für das Login
- ▶ Einstellungen für das Speichern der Passwörter
- ▶ Richtlinien für gültige Passwörter festlegen

Die Methoden, die das Gerät für die Authentifizierung der Benutzer verwendet, legen Sie fest im Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

■ Konfiguration

Dieser Rahmen bietet Ihnen die Möglichkeit, Einstellungen für das Login festzulegen.

Parameter	Bedeutung
Login-Versuche	Anzahl möglicher Versuche, sich anzumelden. Mögliche Werte: ▶ 0..5 (Voreinstellung: 0) Meldet sich der Benutzer ein weiteres Mal ohne Erfolg an, sperrt das Gerät für den Benutzer den Zugriff auf das Gerät. Das Gerät erlaubt ausschließlich Benutzern mit der Berechtigung <code>administrator</code> , die Sperre aufzuheben. Der Wert 0 deaktiviert die Sperre. Der Benutzer hat beliebig viele Versuche, sich anzumelden.
Min. Passwort-Länge	Das Gerät akzeptiert das Passwort, wenn es sich aus mindestens so vielen Zeichen zusammensetzt, wie hier angegeben. Das Gerät prüft das Passwort gemäß dieser Richtlinie, unabhängig von der Einstellung des Kontrollkästchens <i>Richtlinien überprüfen</i> . Mögliche Werte: ▶ 1..64 (Voreinstellung: 6)

■ Passwort-Richtlinien

Dieser Rahmen bietet Ihnen die Möglichkeit, Richtlinien für gültige Passwörter festzulegen. Das Gerät prüft jedes neue Passwort und Passwortänderungen gemäß dieser Richtlinien.

Die Einstellungen wirken auf Spalte *Passwort*. Voraussetzung ist, dass das Kontrollkästchen in Spalte *Richtlinien überprüfen* markiert ist.


Parameter	Bedeutung
Großbuchstaben (min.)	Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Großbuchstaben enthält, wie hier angegeben. Mögliche Werte: ▶ 0..16 (Voreinstellung: 1) Der Wert 0 deaktiviert diese Richtlinie.

Parameter	Bedeutung
Kleinbuchstaben (min.)	Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Kleinbuchstaben enthält, wie hier angegeben. Mögliche Werte: ▶ 0..16 (Voreinstellung: 1) Der Wert 0 deaktiviert diese Richtlinie.
Ziffern (min.)	Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Ziffern enthält, wie hier angegeben. Mögliche Werte: ▶ 0..16 (Voreinstellung: 1) Der Wert 0 deaktiviert diese Richtlinie.
Sonderzeichen (min.)	Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Sonderzeichen enthält, wie hier angegeben. Mögliche Werte: ▶ 0..16 (Voreinstellung: 1) Der Wert 0 deaktiviert diese Richtlinie.

■ Tabelle

Jeder Benutzer benötigt ein aktives Benutzerkonto, um Management-Zugriff auf das Geräts zu erhalten. Die Tabelle bietet Ihnen die Möglichkeit, Benutzerkonten einzurichten und zu verwalten.


Um Einstellungen zu ändern, klicken Sie in der Tabelle den gewünschten Parameter und modifizieren den Wert.

Parameter	Bedeutung
Benutzername	Zeigt die Bezeichnung des Benutzerkontos. Um ein neues Benutzerkonto anzulegen, klicken Sie die Schaltfläche  .
Aktiv	Aktiviert/deaktiviert das Benutzerkonto. Mögliche Werte: ▶ <code>markiert</code> Das Benutzerkonto ist aktiv. Das Gerät akzeptiert die Anmeldung eines Benutzers mit dem Benutzernamen. ▶ <code>unmarkiert</code> (Voreinstellung) Das Benutzerkonto ist inaktiv. Das Gerät verweigert die Anmeldung eines Benutzers mit dem Benutzernamen. Wenn ausschließlich 1 Benutzerkonto mit der Berechtigung <code>administrator</code> existiert, ist dieses Benutzerkonto immer aktiv.
Passwort	Zeigt ***** (Sternchen) anstelle des Passworts, mit dem sich der Benutzer anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen Die folgenden Zeichen sind zulässig: - <code>a..z</code> - <code>A..Z</code> - <code>0..9</code> - <code>#\$%&'()*+,-./:;<=>?@_`</code> Die Mindestlänge des Passworts ist im Rahmen <i>Konfiguration</i> festgelegt. Das Gerät unterscheidet zwischen Groß- und Kleinschreibung. Wenn das Kontrollkästchen in Spalte <i>Richtlinien überprüfen</i> markiert ist, prüft das Gerät das Passwort gemäß der im Rahmen <i>Passwort-Richtlinien</i> festgelegten Richtlinien. Die Mindestlänge des Passwortes prüft das Gerät immer, auch wenn das Kontrollkästchen in Spalte <i>Richtlinien überprüfen</i> unmarkiert ist.

Parameter	Bedeutung
Rolle	<p>Legt die Benutzer-Rolle fest, die den Zugriff des Benutzers auf die einzelnen Funktionen des Geräts regelt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>unauthorized</code> Der Benutzer ist gesperrt, das Gerät verweigert die Anmeldung des Benutzers. Weisen Sie diesen Wert zu, um das Benutzerkonto vorübergehend zu sperren. Wenn beim Zuweisen einer anderen Rolle ein Fehler auftritt, weist das Gerät dem Benutzerkonto diese Rolle zu. ▶ <code>guest</code> (Voreinstellung) Der Benutzer ist berechtigt, das Gerät zu überwachen. ▶ <code>auditor</code> Der Benutzer ist berechtigt, das Gerät zu überwachen und im Dialog <i>Diagnose > Bericht > Audit Trail</i> die Protokoll-Datei zu speichern. ▶ <code>operator</code> Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern – mit Ausnahme der Sicherheitseinstellungen für den Zugriff auf das Gerät. ▶ <code>administrator</code> Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern. <p>Den in der Antwort eines RADIUS-Servers übertragenen Service-Type weist das Gerät wie folgt einer Benutzer-Rolle zu:</p> <ul style="list-style-type: none"> - Administrative-User: administrator - Login-User: operator - NAS-Prompt-User: guest
Benutzer gesperrt	<p>Entsperrt das Benutzerkonto.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Das Benutzerkonto ist gesperrt. Der Benutzer hat keinen Management-Zugriff auf das Gerät. Das Gerät sperrt einen Benutzer automatisch, wenn dieser zu oft erfolglos versucht, sich anzumelden. ▶ <code>unmarkiert</code> (ausgegraut) (Voreinstellung) Das Benutzerkonto ist entsperrt. Der Benutzer hat Management-Zugriff auf das Gerät.
Richtlinien überprüfen	<p>Aktiviert/deaktiviert das Prüfen des Passworts.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Das Prüfen des Passworts ist aktiviert. Beim Einrichten oder Ändern des Passworts prüft das Gerät das Passwort gemäß der im Rahmen <i>Passwort-Richtlinien</i> festgelegten Richtlinien. ▶ <code>unmarkiert</code> (Voreinstellung) Das Prüfen des Passworts ist deaktiviert.
SNMP-Authentifizierung	<p>Legt das Authentifizierungsprotokoll fest, welches das Gerät beim Zugriff des Benutzers per SNMPv3 anwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>hmacmd5</code> (Voreinstellung) Das Gerät verwendet für dieses Benutzerkonto das Protokoll HMAC-MD5. ▶ <code>hmacsha</code> Das Gerät verwendet für dieses Benutzerkonto das Protokoll HMAC-SHA.
SNMP-Verschlüsselung	<p>Legt das Verschlüsselungsprotokoll fest, welches das Gerät beim Zugriff des Benutzers per SNMPv3 anwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>kein</code> keine Verschlüsselung ▶ <code>des</code> (Voreinstellung) DES-Verschlüsselung ▶ <code>aesCfb128</code> AES-128-Verschlüsselung

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Öffnet das Fenster <i>Erzeugen</i> , um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld <i>Benutzername</i> legen Sie die Bezeichnung des Benutzerkontos fest. Mögliche Werte: – Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

3.2 Authentifizierungs-Liste

In diesem Dialog verwalten Sie die Authentifizierungs-Listen. In einer Authentifizierungsliste legen Sie fest, welche Methode das Gerät für die Authentifizierung verwendet. Sie haben außerdem die Möglichkeit, den Authentifizierungslisten vordefinierte Anwendungen zuzuweisen.

Das Gerät gewährt Benutzern Zugriff auf das Management, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Benutzer mit folgenden Methoden:

- ▶ Benutzerverwaltung des Geräts
- ▶ RADIUS


Mit der portbasierten Zugriffskontrolle gemäß IEEE 802.1X gewährt das Gerät angeschlossenen Endgeräten ausschließlich dann Zugriff auf das Netz, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Endgeräte mit folgenden Methoden:


- ▶ RADIUS
- ▶ IAS (Integrated Authentication Server)

In der Voreinstellung sind die folgende Authentifizierungslisten verfügbar:

- defaultDot1x8021AuthList
- defaultLoginAuthList
- defaultV24AuthList

■ Tabelle






Parameter	Bedeutung
Name	Zeigt die Bezeichnung der Liste. Um eine neue Liste anzulegen, klicken Sie die Schaltfläche  . Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Parameter	Bedeutung
Richtlinie 1 Richtlinie 2 Richtlinie 3 Richtlinie 4 Richtlinie 5	<p>Legt die Authentifizierungsrichtlinie fest, die das Gerät beim Zugriff über die in Spalte <i>Zugeordnete Anwendungen</i> festgelegte Anwendung anwendet.</p> <p>Das Gerät bietet Ihnen die Möglichkeit einer Fall-Back-Lösung. Legen Sie hierfür in den Richtlinien-Feldern jeweils eine andere Richtlinie fest. Abhängig von der Reihenfolge der in den einzelnen Richtlinien eingetragenen Werte kann das Gerät die nächste Richtlinie verwenden, wenn die Authentifizierung mit der festgelegten Richtlinie fehlschlägt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>lokal</code> (Voreinstellung) Das Gerät authentifiziert die Benutzer mittels der lokalen Benutzerverwaltung. Siehe Dialog <i>Gerätesicherheit > Benutzerverwaltung</i>. Der Authentifizierungsliste <code>defaultDot1x8021AuthList</code> können Sie diesen Wert nicht zuweisen. ▶ <code>radius</code> Das Gerät authentifiziert die Benutzer mit einem RADIUS-Server im Netz. Den RADIUS-Server legen Sie im Dialog <i>Netzsicherheit > RADIUS > Authentication-Server</i> fest. ▶ <code>reject</code> Abhängig von der Richtlinie, die Sie zuerst anwenden, akzeptiert das Gerät die Authentifizierung oder lehnt die Authentifizierung ab. Mögliche Authentifizierungsszenarios sind: <ul style="list-style-type: none"> – Wenn die erste Richtlinie in der Authentifizierungsliste <code>lokal</code> ist und das Gerät die Anmeldeinformationen des Benutzers akzeptiert, meldet das Gerät den Benutzer an, ohne die anderen Authentifizierungsrichtlinien anzuwenden. – Wenn die erste Richtlinie in der Authentifizierungsliste <code>lokal</code> ist und das Gerät die Anmeldeinformationen des Benutzers ablehnt, versucht das Gerät, den Benutzer mithilfe der anderen Richtlinien in der festgelegten Reihenfolge anzumelden. – Wenn die erste Richtlinie in der Authentifizierungsliste <code>radius</code> ist und das Gerät die Anmeldung ablehnt, wird die Anmeldung sofort verweigert, ohne dass das Gerät versucht, den Benutzer über eine andere Richtlinie anzumelden. Bleibt die Antwort des RADIUS-Servers aus, versucht das Gerät die Authentifizierung des Benutzers mit der nächsten Richtlinie. – Wenn die erste Richtlinie in der Authentifizierungsliste <code>reject</code> ist, lehnen die Geräte die Benutzeranmeldung sofort ab, ohne eine andere Richtlinie anzuwenden. – Vergewissern Sie sich, dass die Authentifizierungsliste <code>defaultV24AuthList</code> mindestens eine Richtlinie enthält, die vom Wert <code>reject</code> abweicht. ▶ <code>ias</code> Das Gerät authentifiziert die sich per 802.1X anmeldenden Endgeräte mit dem Integrierten Authentifizierungs-Server (IAS). Der Integrierte Authentifizierungs-Server verwaltet die Zugangsdaten in einer eigenständigen Datenbank. Siehe Dialog <i>Netzsicherheit > 802.1X Port-Authentifizierung > Integrierter Authentifikations-Server</i>. Der Authentifizierungsliste <code>defaultDot1x8021AuthList</code> können Sie ausschließlich diesen Wert zuweisen.
Zugeordnete Anwendungen	<p>Zeigt die zugeordneten Anwendungen. Wenn Benutzer mit der betreffenden Anwendung auf das Gerät zugreifen, wendet das Gerät die festgelegten Richtlinien für die Authentifizierung an.</p> <p>Um der Liste eine andere Anwendung zuzuordnen oder die Zuordnung aufzuheben, klicken Sie die Schaltfläche  und dann den Eintrag <i>Anwendungen zuordnen</i>. Jede Anwendung lässt sich immer genau einer Liste zuordnen.</p>
Aktiv	<p>Aktiviert/deaktiviert die Liste.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Die Liste ist aktiviert. Das Gerät wendet die Richtlinien dieser Liste an, wenn Benutzer mit der betreffenden Anwendung auf das Gerät zugreifen. ▶ <code>unmarkiert</code> (Voreinstellung) Die Liste ist deaktiviert.

Anmerkung: Wenn die Tabelle keine Liste enthält, ist der Management-Zugriff ausschließlich per CLI über die V.24-Schnittstelle des Geräts möglich. In diesem Fall authentifiziert das Gerät den Benutzer anhand der lokalen Benutzerverwaltung. Siehe Dialog *Gerätesicherheit > Benutzerverwaltung*.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Anwendungen zuordnen	<p>Öffnet das Fenster <i>Anwendungen zuordnen</i>.</p> <ul style="list-style-type: none">▶ Das linke Feld zeigt die Anwendungen, die sich der ausgewählten Liste zuordnen lassen.▶ Das rechte Feld zeigt die Anwendungen, die der ausgewählten Liste zugeordnet sind.▶ Schaltflächen:<ul style="list-style-type: none"> : Verschiebt jeden Eintrag in das rechte Feld. : Verschiebt die markierten Einträge aus dem linken Feld in das rechte Feld. : Verschiebt die markierten Einträge aus dem rechten Feld in das linke Feld. : Verschiebt jeden Eintrag in das linke Feld. <p>Verschieben Sie keinesfalls den Eintrag <code>WebInterface</code> in das linke Feld. Andernfalls bricht die Verbindung zum Gerät ab, sobald Sie die Schaltfläche <i>Ok</i> klicken.</p>

3.3 Management-Zugriff

Das Menü enthält die folgenden Dialoge:

- ▶ [Server](#)
- ▶ [IP-Zugriffsbeschränkung](#)
- ▶ [Web](#)
- ▶ [Command Line Interface](#)
- ▶ [SNMPv1/v2 Community](#)

3.3.1 Server

Dieser Dialog bietet Ihnen die Möglichkeit, die Server-Dienste einzurichten, mit denen Benutzer oder Anwendungen Management-Zugriff auf das Gerät erhalten.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [Information]
- ▶ [SNMP]
- ▶ [Telnet]
- ▶ [SSH]
- ▶ [HTTP]
- ▶ [HTTPS]

[Information]

Diese Registerkarte zeigt im Überblick, welche Server-Dienste eingeschaltet sind.

■ Tabelle

Parameter	Bedeutung
SNMPv1	<p>Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 1 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte <i>SNMP</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert Server-Dienst ist aktiv.▶ unmarkiert Server-Dienst ist inaktiv.
SNMPv2	<p>Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 2 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte <i>SNMP</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert Server-Dienst ist aktiv.▶ unmarkiert Server-Dienst ist inaktiv.
SNMPv3	<p>Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 3 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte <i>SNMP</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert Server-Dienst ist aktiv.▶ unmarkiert Server-Dienst ist inaktiv.
Telnet server	<p>Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit Telnet ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte <i>Telnet</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert Server-Dienst ist aktiv.▶ unmarkiert Server-Dienst ist inaktiv.
SSH server	<p>Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit Secure Shell ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte <i>SSH</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert Server-Dienst ist aktiv.▶ unmarkiert Server-Dienst ist inaktiv.
HTTP server	<p>Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit der grafischen Bedienoberfläche über HTTP ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte <i>HTTP</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert Server-Dienst ist aktiv.▶ unmarkiert Server-Dienst ist inaktiv.
HTTPS server	<p>Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit der grafischen Bedienoberfläche über HTTPS ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte <i>HTTP</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert Server-Dienst ist aktiv.▶ unmarkiert Server-Dienst ist inaktiv.

■ Schaltflächen



Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

[SNMP]

Diese Registerkarte bietet Ihnen die Möglichkeit, Einstellungen für den SNMP-Agenten des Geräts festzulegen und den Zugriff auf das Gerät mit unterschiedlichen SNMP-Versionen ein-/auszuschalten.

Der SNMP-Agent ermöglicht den Management-Zugriff auf das Gerät mit SNMP-basierten Anwendungen.

■ Konfiguration

Parameter	Bedeutung
SNMPv1	<p>Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 1.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Zugriff ist aktiviert. ▶ <code>unmarkiert</code> Zugriff ist deaktiviert. <p>Die Community-Namen legen Sie fest im Dialog <i>Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community</i>.</p>
SNMPv2	<p>Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 2.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Zugriff ist aktiviert. ▶ <code>unmarkiert</code> Zugriff ist deaktiviert. <p>Die Community-Namen legen Sie fest im Dialog <i>Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community</i>.</p>
SNMPv3	<p>Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 3.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Zugriff ist aktiviert. ▶ <code>unmarkiert</code> Zugriff ist deaktiviert. <p>Netzmanagementsysteme wie Industrial HiVision verwenden dieses Protokoll, um mit dem Gerät zu kommunizieren.</p>
UDP-Port	<p>Legt die Nummer des UDP-Ports fest, auf dem der SNMP-Agent Anfragen von Clients entgegennimmt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>1..65535</code> (Voreinstellung: 161) Ausnahme: Port 2222 ist für interne Funktionen reserviert. <p>Damit der SNMP-Agent nach einer Änderung den neuen Port verwendet, gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Klicken Sie die Schaltfläche . <input type="checkbox"/> Wählen Sie im Dialog <i>Grundeinstellungen > Laden/Speichern</i> das aktive Konfigurationsprofil. <input type="checkbox"/> Klicken Sie die Schaltfläche  und dann den Eintrag <i>Speichern</i>. <input type="checkbox"/> Starten Sie das Gerät neu.
SNMPover802	<p>Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP über IEEE-802.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Zugriff ist aktiviert. ▶ <code>unmarkiert</code> (Voreinstellung) Zugriff ist deaktiviert. <p>Die HiDiscovery-Software verwendet SNMP über IEEE-802, um Geräte ohne IP-Adresse zu erreichen.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Telnet]

Diese Registerkarte bietet Ihnen die Möglichkeit, den Telnet-Server im Gerät ein-/auszuschalten und die für Telnet erforderlichen Einstellungen festzulegen.

Der Telnet-Server ermöglicht den Management-Zugriff auf das Gerät per Fernzugriff mit dem Command Line Interface. Telnet-Verbindungen sind unverschlüsselt.

■ Funktion

Parameter	Bedeutung
Funktion	<p>Schaltet den Telnet-Server ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An (Voreinstellung) Der Telnet-Server ist eingeschaltet. Der Management-Zugriff auf das Gerät ist möglich mit dem Command Line Interface über eine unverschlüsselte Telnet-Verbindung erreichbar. ▶ Aus Der Telnet-Server ist ausgeschaltet. <p>Anmerkung: Wenn der SSH-Server ausgeschaltet ist und Sie auch Telnet ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die V.24-Schnittstelle des Geräts möglich.</p>

■ Konfiguration

Parameter	Bedeutung
TCP-Port	<p>Legt die Nummer des TCP-Ports fest, auf dem das Gerät Telnet-Anfragen von den Clients entgegennimmt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..65535 (Voreinstellung: 23) Ausnahme: Port 2222 ist für interne Funktionen reserviert. <p>Nach Ändern des Ports startet der Server automatisch neu. Bestehende Verbindungen bleiben aufgebaut.</p>
Verbindungen	Zeigt, wie viele Telnet-Verbindungen gegenwärtig zum Gerät aufgebaut sind.
Verbindungen (max.)	<p>Legt fest, wie viele gleichzeitige Telnet-Verbindungen zum Gerät maximal möglich sind.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..2 (Voreinstellung: 2)
Session-Timeout [min]	<p>Legt die Timeout-Zeit in Minuten fest. Bei Inaktivität beendet das Gerät nach dieser Zeit die Sitzung des angemeldeten Benutzers.</p> <p>Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers wirksam.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0 Deaktiviert die Funktion. Die Verbindung bleibt bei Inaktivität aufgebaut. ▶ 1..160 (Voreinstellung: 5)

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[SSH]

Diese Registerkarte bietet Ihnen die Möglichkeit, den SSH-Server im Gerät ein-/auszuschalten und die für SSH erforderlichen Einstellungen festzulegen. Der Server arbeitet mit SSH-Version 2.

Der SSH-Server ermöglicht den Management-Zugriff auf das Gerät per Fernzugriff mit dem Command Line Interface. SSH-Verbindungen sind verschlüsselt.

Der SSH-Server identifiziert sich gegenüber den Clients mit seinem öffentlichen RSA- oder DSA-Schlüssel. Beim 1. Verbindungsaufbau zeigt das Client-Programm dem Benutzer den Fingerprint dieses Schlüssels an. Der Fingerprint enthält eine einfach zu prüfende, hexadezimale Ziffernfolge. Wenn Sie den Benutzern diese Ziffernfolge über einen vertrauenswürdigen Kanal zur Verfügung stellen, haben diese die Möglichkeit, beide Fingerprints zu vergleichen. Stimmen die Ziffernfolgen überein, ist der Client mit dem korrekten Server verbunden.

Das Gerät bietet Ihnen die Möglichkeit, die für RSA und DSA erforderlichen privaten und öffentlichen Schlüssel (Host Keys) direkt auf dem Gerät zu erzeugen. Andernfalls haben Sie die Möglichkeit, eigene Schlüssel im PEM-Format auf das Gerät zu kopieren.

■ Funktion

Parameter	Bedeutung
Funktion	<p>Schaltet den SSH-Server ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ An (Voreinstellung) Der SSH-Server ist eingeschaltet. Der Management-Zugriff auf das Gerät ist möglich mit dem Command Line Interface über eine verschlüsselte SSH-Verbindung erreichbar. Der Server lässt sich ausschließlich dann starten, wenn eine RSA- oder DSA-Signatur im Gerät vorhanden ist.▶ Aus Der SSH-Server ist ausgeschaltet. Wenn Sie den SSH-Server ausschalten, bleiben bestehende Verbindungen aufgebaut. Den Aufbau neuer Verbindungen verweigert das Gerät jedoch. <p>Anmerkung: Wenn der Telnet-Server ausgeschaltet ist und Sie auch SSH ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die V.24-Schnittstelle des Geräts möglich.</p>

■ Konfiguration

Parameter	Bedeutung
TCP-Port	<p>Legt die Nummer des TCP-Ports fest, auf dem das Gerät SSH-Anfragen von den Clients entgegennimmt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 1..65535 (Voreinstellung: 22) Ausnahme: Port 2222 ist für interne Funktionen reserviert. <p>Nach Ändern des Ports startet der Server automatisch neu. Bestehende Verbindungen bleiben aufgebaut.</p>
Sessions	Zeigt, wie viele SSH-Verbindungen gegenwärtig zum Gerät aufgebaut sind.
Sessions (max.)	<p>Legt fest, wie viele gleichzeitige SSH-Verbindungen zum Gerät maximal möglich sind.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 1..2 (Voreinstellung: 2)

Parameter	Bedeutung
Session-Timeout [min]	<p>Legt die Timeout-Zeit in Minuten fest. Bei Inaktivität des angemeldeten Benutzers trennt das Gerät nach dieser Zeit die Verbindung. Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers wirksam.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0 Deaktiviert die Funktion. Die Verbindung bleibt bei Inaktivität aufgebaut. ▶ 1..160 (Voreinstellung: 5)

■ Fingerprint

Der Fingerprint ist eine einfach zu prüfende Zeichenfolge, die den RSA- oder DSA-Host-Key des SSH-Servers eindeutig identifiziert.

Parameter	Bedeutung
DSA	Fingerprint des öffentlichen DSA-Host-Keys des Servers.
RSA	Fingerprint des öffentlichen RSA-Host-Keys des Servers.


Nach Importieren eines neuen RSA- oder DSA-Host-Keys zeigt das Gerät den bisherigen Fingerprint so lange an, bis Sie den Server neu starten.

■ Signatur

Parameter	Bedeutung
DSA vorhanden	<p>Zeigt, ob ein DSA-Host-Key im Gerät vorhanden ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Schlüssel vorhanden. ▶ unmarkiert Kein Schlüssel vorhanden.
RSA vorhanden	<p>Zeigt, ob ein RSA-Host-Key im Gerät vorhanden ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Schlüssel vorhanden. ▶ unmarkiert Kein Schlüssel vorhanden.
Erzeugen	<p>Erzeugt einen Host-Key auf dem Gerät. Voraussetzung ist, dass der <i>SSH</i>-Server ausgeschaltet ist.</p> <p>Länge des erzeugten Schlüssels:</p> <ul style="list-style-type: none"> ▶ 2048 Bit (RSA) ▶ 1024 Bit (DSA) <p>Damit der Server den generierten Host-Key verwendet, starten Sie den Server neu.</p> <p>Alternativ haben Sie die Möglichkeit, einen eigenen Schlüssel im PEM-Format auf das Gerät zu kopieren. Siehe Rahmen <i>Key-Import</i>.</p>
Löschen	Entfernt den Host-Key aus dem Gerät. Voraussetzung ist, dass der SSH-Server ausgeschaltet ist.

Parameter	Bedeutung
Betriebszustand	<p>Zeigt, ob das Gerät gegenwärtig einen Host-Key erzeugt. Möglicherweise hat ein anderer Benutzer diese Aktion ausgelöst.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ dsa Das Gerät erzeugt gegenwärtig einen DSA-Host-Key. ▶ rsa Das Gerät erzeugt gegenwärtig einen RSA-Host-Key. ▶ beide Das Gerät erzeugt derzeit gleichzeitig einen DSA- und einen RSA-Host-Key. ▶ kein Das Gerät generiert keinen Host-Key.

■ Key-Import

Parameter	Bedeutung
URL	<p>Legt Pfad und Dateiname Ihres DSA-/RSA-Host-Keys fest.</p> <p>Das Gerät akzeptiert den DSA-/RSA-Schlüssel, wenn dieser die folgende Schlüssellänge aufweist:</p> <ul style="list-style-type: none"> – 2048 bit (RSA) – 1024 bit (DSA) <p>Das Gerät bietet Ihnen folgende Möglichkeiten, den Schlüssel in das Gerät zu kopieren:</p> <ul style="list-style-type: none"> ▶ Import vom PC Befindet sich der Host-Key auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie die Datei, die den Host-Key enthält, in den -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen. ▶ Import von einem FTP-Server Befindet sich der Schlüssel auf einem FTP-Server, legen Sie den URL zur Datei in folgender Form fest: <code>ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname></code> ▶ Import von einem TFTP-Server Befindet sich der Schlüssel auf einem TFTP-Server, legen Sie den URL zur Datei in folgender Form fest: <code>tftp://<IP-Adresse>/<Pfad>/<Dateiname></code> ▶ Import von einem SCP- oder SFTP-Server Befindet sich der Schlüssel auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in folgender Form fest: <ul style="list-style-type: none"> – <code>scp://</code> oder <code>sftp://<IP-Adresse>/<Pfad>/<Dateiname></code> Nach Klicken der Schaltfläche <i>Start</i> zeigt das Gerät das Fenster <i>Anmeldeinformationen</i>. Geben Sie dort <i>Benutzername</i> und <i>Passwort</i> ein, um sich am Server anzumelden. – <code>scp://</code> oder <code>sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname></code>
Start	Kopiert den im Feld <i>URL</i> festgelegten Key in das Gerät.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

[HTTP]

Diese Registerkarte bietet Ihnen die Möglichkeit, für den Webserver das Protokoll HTTP ein-/ auszuschalten und die für HTTP erforderlichen Einstellungen festzulegen.

Der Webserver liefert die grafische Benutzeroberfläche über eine unverschlüsselte HTTP-Verbindung aus. Deaktivieren Sie aus Sicherheitsgründen das HTTP-Protokoll, verwenden Sie stattdessen das HTTPS-Protokoll.

Das Gerät unterstützt bis zu 10 gleichzeitige Verbindungen per HTTP oder HTTPS.

Anmerkung: Wenn Sie Einstellungen in dieser Registerkarte ändern und die Schaltfläche klicken, beendet das Gerät die Sitzung und trennt jede geöffnete Verbindung. Um wieder mit der grafischen Benutzeroberfläche zu arbeiten, melden Sie sich erneut an.

■ Funktion

Parameter	Bedeutung
Funktion	<p>Schaltet für den Webserver das Protokoll <i>HTTP</i> ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An (Voreinstellung) Das Protokoll <i>HTTP</i> ist eingeschaltet. Der Management-Zugriff auf das Gerät ist möglich über eine unverschlüsselte <i>HTTP</i>-Verbindung. Wenn das Protokoll <i>HTTPS</i> ebenfalls eingeschaltet ist, leitet das Gerät die Anfrage für eine <i>HTTP</i>-Verbindung automatisch auf eine verschlüsselte <i>HTTPS</i>-Verbindung um. ▶ Aus Das Protokoll <i>HTTP</i> ist ausgeschaltet. Wenn das Protokoll <i>HTTPS</i> eingeschaltet ist, ist der Management-Zugriff auf das Gerät möglich über eine verschlüsselte <i>HTTPS</i>-Verbindung. <p>Anmerkung: Wenn die Protokolle <i>HTTP</i> und <i>HTTPS</i> ausgeschaltet sind, können Sie das Protokoll <i>HTTP</i> mit dem CLI-Kommando <code>http server</code> einschalten, um die grafische Benutzeroberfläche zu erreichen.</p>

■ Konfiguration

Parameter	Bedeutung
TCP-Port	<p>Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTP-Anfragen von den Clients entgegennimmt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..65535 (Voreinstellung: 80) Ausnahme: Port 2222 ist für interne Funktionen reserviert.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[HTTPS]

Diese Registerkarte bietet Ihnen die Möglichkeit, für den Webserver das Protokoll HTTPS ein-/ auszuschalten und die für HTTPS erforderlichen Einstellungen festzulegen.

Der Webserver liefert die grafische Benutzeroberfläche über eine verschlüsselte HTTP-Verbindung aus.

Für die Verschlüsselung der HTTP-Verbindung ist ein digitales Zertifikat notwendig. Das Gerät bietet Ihnen die Möglichkeit, dieses Zertifikat selbst zu erzeugen oder ein vorhandenes Zertifikat auf das Gerät zu laden.

Das Gerät unterstützt bis zu 10 gleichzeitige Verbindungen per HTTP oder HTTPS.

Anmerkung: Wenn Sie Einstellungen in dieser Registerkarte ändern und die Schaltfläche klicken, beendet das Gerät die Sitzung und trennt jede geöffnete Verbindung. Um wieder mit der grafischen Benutzeroberfläche zu arbeiten, melden Sie sich erneut an.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet für den Webserver das Protokoll <i>HTTPS</i> ein/aus. Mögliche Werte: ▶ An (Voreinstellung) Das Protokoll <i>HTTPS</i> ist eingeschaltet. Der Management-Zugriff auf das Gerät ist möglich über eine verschlüsselte <i>HTTPS</i> -Verbindung. Wenn kein digitales Zertifikat vorhanden ist, erzeugt das Gerät ein digitales Zertifikat, bevor es das <i>HTTPS</i> -Protokoll einschaltet. ▶ Aus Das Protokoll <i>HTTPS</i> ist ausgeschaltet. Wenn das Protokoll <i>HTTP</i> eingeschaltet ist, ist der Management-Zugriff auf das Gerät möglich über eine unverschlüsselte <i>HTTP</i> -Verbindung. Anmerkung: Wenn die Protokolle <i>HTTP</i> und <i>HTTPS</i> ausgeschaltet sind, können Sie das Protokoll <i>HTTPS</i> mit dem CLI-Kommando <code>https server</code> einschalten, um die grafische Benutzeroberfläche zu erreichen.


■ Konfiguration

Parameter	Bedeutung
TCP-Port	Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTPS-Anfragen von den Clients entgegennimmt. Mögliche Werte: ▶ 1..65535 (Voreinstellung: 443) Ausnahme: Port 2222 ist für interne Funktionen reserviert.

■ Fingerprint

Der Fingerprint ist eine einfach zu prüfende, hexadezimale Ziffernfolge, die das digitale Zertifikat des HTTPS-Servers eindeutig identifiziert.

Nach dem Importieren oder Erzeugen eines neuen digitalen Zertifikats zeigt das Gerät den gegenwärtig gültigen Fingerprint so lange an, bis Sie den Server neu starten.


Parameter	Bedeutung
Fingerprint-Typ	Legt fest, welchen Fingerprint das Feld <i>Fingerprint</i> anzeigt. Mögliche Werte: ▶ sha1 Das Feld <i>Fingerprint</i> zeigt den SHA1-Fingerprint des Zertifikats. ▶ sha256 Das Feld <i>Fingerprint</i> zeigt den SHA256-Fingerprint des Zertifikats.
Fingerprint	Zeichenfolge des digitalen Zertifikats, das der Server verwendet. Wenn Sie die Einstellung im Feld <i>Fingerprint-Typ</i> ändern, klicken Sie anschließend die Schaltflächen <input checked="" type="checkbox"/> und  , um die Anzeige zu aktualisieren.

■ Zertifikat

Parameter	Bedeutung
Vorhanden	Zeigt, ob das digitale Zertifikat im Gerät vorhanden ist. Mögliche Werte: ▶ markiert Das Zertifikat ist vorhanden. ▶ unmarkiert Das Zertifikat wurde entfernt.
Erzeugen	Generiert ein digitales Zertifikat auf dem Gerät. Bis zum Neustart verwendet der Webserver das vorherige Zertifikat. Damit der Webserver das neu generierte Zertifikat verwendet, starten Sie den Webserver neu. Der Neustart des Webserver ist ausschließlich über das Command Line Interface (CLI) möglich. Alternativ haben Sie die Möglichkeit, ein eigenes Zertifikat in das Gerät zu kopieren. Siehe Rahmen <i>Zertifikat-Import</i> .
Löschen	Entfernt das digitale Zertifikat. Bis zum Neustart verwendet der Webserver das vorherige Zertifikat.
Betriebszustand	Zeigt, ob das Gerät gegenwärtig ein digitales Zertifikat generiert oder löscht. Möglicherweise hat ein anderer Benutzer die Aktion ausgelöst. Mögliche Werte: ▶ kein Das Gerät generiert oder löscht gegenwärtig kein Zertifikat. ▶ delete Das Gerät löscht gegenwärtig ein Zertifikat. ▶ generate Das Gerät generiert gegenwärtig ein Zertifikat.

Anmerkung: Beim Laden der grafischen Benutzeroberfläche zeigt der Web-Browser eine Warnung, wenn das Gerät ein Zertifikat verwendet, das nicht von einer Zertifizierungsstelle signiert wurde. Um fortzufahren, fügen Sie im Web-Browser eine Ausnahmeregel für das Zertifikat hinzu.

■ Zertifikat-Import

Parameter	Bedeutung
URL	<p>Legt Pfad und Dateiname des Zertifikats fest.</p> <p>Zulässig sind Zertifikate mit folgenden Eigenschaften:</p> <ul style="list-style-type: none">– X.509-Format– .PEMDateinamenserweiterung– Base64-kodiert, umschlossen von<ul style="list-style-type: none">• -----BEGIN PRIVATE KEY----- und -----END PRIVATE KEY-----• -----BEGIN CERTIFICATE----- und -----END CERTIFICATE-----– RSA-Schlüssel mit 2048 bit Länge <p>Das Gerät bietet Ihnen folgende Möglichkeiten, das Zertifikat in das Gerät zu kopieren:</p> <ul style="list-style-type: none">▶ Import vom PC Befindet sich das Zertifikat auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie das Zertifikat in den -Bereich. Alternativ klicken Sie in den Bereich, um das Zertifikat auszuwählen.▶ Import von einem FTP-Server Befindet sich das Zertifikat auf einem FTP-Server, legen Sie den URL zur Datei in folgender Form fest: ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Pfad>/<Dateiname>▶ Import von einem TFTP-Server Befindet sich das Zertifikat auf einem TFTP-Server, legen Sie den URL zur Datei in folgender Form fest: tftp://<IP-Adresse>/<Pfad>/<Dateiname>▶ Import von einem SCP- oder SFTP-Server Befindet sich das Zertifikat auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in folgender Form fest:<ul style="list-style-type: none">– scp:// oder sftp://<IP-Adresse>/<Pfad>/<Dateiname> Nach Klicken der Schaltfläche Start zeigt das Gerät das Fenster Anmeldeinformationen. Geben Sie dort Benutzername und Passwort ein, um sich am Server anzumelden.– scp:// oder sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>
Start	Kopiert das im Feld <i>URL</i> festgelegte Zertifikat in das Gerät.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

3.3.2 IP-Zugriffsbeschränkung

Dieser Dialog bietet Ihnen die Möglichkeit, den Management-Zugriff auf das Gerät auf gewisse IP-Adressbereiche und ausgewählte IP-basierte Anwendungen zu beschränken.

- ▶ Bei ausgeschalteter Funktion ist der Management-Zugriff auf das Gerät von jeder beliebigen IP-Adresse und mit jeder Anwendung möglich.
- ▶ Bei eingeschalteter Funktion ist der Zugriff beschränkt. Ausschließlich unter den folgenden Voraussetzungen haben Sie Management-Zugriff:
 - Mindestens ein Tabelleneintrag ist aktiviert.
 - und
 - Sie verbinden sich mit einer erlaubten Anwendung aus einem zugelassenen IP-Adressbereich mit dem Gerät.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>IP-Zugriffsbeschränkung</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ An Die <i>IP-Zugriffsbeschränkung</i>-Funktion ist eingeschaltet. Der Management-Zugriff auf das Gerät ist beschränkt. ▶ Aus (Voreinstellung) Die <i>IP-Zugriffsbeschränkung</i>-Funktion ist ausgeschaltet.

Anmerkung: Bevor Sie die Funktion einschalten, vergewissern Sie sich, dass mindestens ein aktiver Eintrag in der Tabelle Ihnen den Zugriff ermöglicht. Andernfalls bricht die Verbindung zum Gerät ab, sobald Sie die Einstellungen ändern. Der Management-Zugriff auf das Gerät ist ausschließlich mit dem CLI über die V.24-Schnittstelle möglich.

■ Tabelle

Sie haben die Möglichkeit, bis zu 16 Tabelleneinträge zu definieren und separat zu aktivieren.

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht. Wenn Sie einen Tabelleneintrag löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie einen neuen Tabelleneintrag erzeugen, schließt das Gerät die 1. Lücke. Mögliche Werte: <ul style="list-style-type: none"> ▶ 1..16
Adresse	Legt die IP-Adresse des Netzes fest, von dem aus Sie den Management-Zugriff auf das Gerät erlauben. Den Netz-Bereich legen Sie fest in Spalte <i>Netzmaske</i> . Mögliche Werte: <ul style="list-style-type: none"> ▶ Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)
Netzmaske	Legt den Bereich des in Spalte <i>Adresse</i> festgelegten Netzes fest. Mögliche Werte: <ul style="list-style-type: none"> ▶ Gültige Netzmaske (Voreinstellung: 0.0.0.0)

Parameter	Bedeutung
HTTP	Aktiviert/deaktiviert den HTTP-Zugriff. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.
HTTPS	Aktiviert/deaktiviert den HTTPS-Zugriff. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.
SNMP	Aktiviert/deaktiviert den SNMP-Zugriff. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.
Telnet	Aktiviert/deaktiviert den Telnet-Zugriff. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.
SSH	Aktiviert/deaktiviert den SSH-Zugriff. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.
IEC61850-MMS	Aktiviert/deaktiviert den Zugriff auf den MMS-Server. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.
Modbus TCP	Aktiviert/deaktiviert den Zugriff auf den <i>Modbus TCP</i> -Server. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.
EtherNet/IP	Aktiviert/deaktiviert den Zugriff auf den <i>EtherNet/IP</i> -Server. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.
PROFINET	Aktiviert/deaktiviert den Zugriff auf den <i>PROFINET</i> -Server. Mögliche Werte: ▶ markiert (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ unmarkiert Zugriff ist deaktiviert.

Parameter	Bedeutung
Aktiv	Aktiviert/deaktiviert den Tabelleneintrag. Mögliche Werte: <ul style="list-style-type: none">▶ markiert (Voreinstellung) Tabelleneintrag ist aktiviert. Das Gerät beschränkt den Management-Zugriff auf den nebenstehenden IP-Adressbereich und die ausgewählten IP-basierten Anwendungen.▶ unmarkiert Tabelleneintrag ist deaktiviert.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

3.3.3 Web

In diesem Dialog legen Sie Einstellungen für die grafische Benutzeroberfläche fest.

■ Konfiguration

Parameter	Bedeutung
Web-Interface Session-Timeout [min]	Legt die Timeout-Zeit in Minuten fest. Bei Inaktivität beendet das Gerät nach dieser Zeit die Sitzung des angemeldeten Benutzers. Mögliche Werte: ▶ 0..160 (Voreinstellung: 5) Der Wert 0 deaktiviert die Funktion, der Benutzer bleibt bei Inaktivität angemeldet.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

3.3.4 Command Line Interface

In diesem Dialog legen Sie Einstellungen für das Command Line Interface (CLI) fest. Detaillierte Informationen zum Command Line Interface finden Sie im Referenzhandbuch „Command Line Interface“.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [\[Global\]](#)
- ▶ [\[Login-Banner\]](#)

[Global]

Diese Registerkarte bietet Ihnen die Möglichkeit, den CLI-Prompt zu ändern und das automatische Beenden bei Inaktivität der CLI-Sitzung über die V.24-Schnittstelle festzulegen.

■ Konfiguration

Parameter	Bedeutung
Login-Prompt	<p>Legt die Zeichenfolge fest, die das Gerät im Command Line Interface (CLI) am Beginn jeder Kommandozeile anzeigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen (0x20..0x7E) inklusive Leerzeichen <p>Wildcards</p> <ul style="list-style-type: none"> – %d Datum – %i IP-Adresse – %m MAC-Adresse – %p Produktname – %t Uhrzeit <p>Voreinstellung: ((EES))</p> <p>Änderungen an dieser Einstellung sind in aktiven CLI-Sitzungen sofort wirksam.</p>
V.24-Timeout [min]	<p>Legt die Zeit in Minuten fest, nach der das Gerät bei Inaktivität des angemeldeten Benutzers die CLI-Sitzung über die V.24-Schnittstelle automatisch beendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..160 (Voreinstellung: 5) <p>Der Wert 0 deaktiviert die Funktion, der Benutzer bleibt bei Inaktivität angemeldet.</p> <p>Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers wirksam.</p> <p>Für Telnet und SSH legen Sie das Timeout fest im Dialog <i>Gerätesicherheit > Management-Zugriff > Server</i>.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

[Login-Banner]

In dieser Registerkarte ersetzen Sie den CLI-Startbildschirm durch einen individuellen Text.

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

Um vor der Anmeldung einen individuellen Text im CLI und in der grafischen Benutzeroberfläche anzuzeigen, verwenden Sie den Dialog *Gerätesicherheit > Pre-Login-Banner*.

■ Funktion

Parameter	Bedeutung
Funktion	<p>Schaltet die <i>Login-Banner</i>-Funktion ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An Die <i>Login-Banner</i>-Funktion ist eingeschaltet. Das Gerät zeigt die im Feld <i>Banner-Text</i> festgelegte Textinformation den Benutzern, die sich mit dem Command Line Interface (CLI) auf dem Gerät anmelden. ▶ Aus (Voreinstellung) Die <i>Login-Banner</i>-Funktion ist ausgeschaltet. Der CLI-Startbildschirm zeigt Informationen über das Gerät. Die Textinformation im Feld <i>Banner-Text</i> bleibt erhalten.

■ Banner-Text

Parameter	Bedeutung
Banner-Text	<p>Legt die Textinformation fest, die das Gerät zu Beginn jeder Sitzung im Command Line Interface anzeigt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..1024 Zeichen (0x20..0x7E) inklusive Leerzeichen ▶ <Tabulator> ▶ <Zeilenumbruch>
Verbleibende Zeichen	<p>Zeigt, wie viele Zeichen im Feld <i>Banner-Text</i> noch für die Textinformation zur Verfügung stehen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1024..0

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

3.3.5 SNMPv1/v2 Community

In diesem Dialog legen Sie die Community-Namen für SNMPv1/v2-Anwendungen fest.

Anwendungen senden Anfragen per SNMPv1/v2 mit einem Community-Namen im SNMP-Datenpaket-Header. Abhängig vom Community-Namen erhält die Anwendung Leserechte oder Lese- und Schreibrechte auf dem Gerät.

Den Zugriff auf das Gerät per SNMPv1/v2 aktivieren Sie im Dialog *Gerätesicherheit > Management-Zugriff > Server*.

■ Tabelle

Parameter	Bedeutung
Community	Zeigt die Berechtigung für SNMPv1/v2-Anwendungen auf dem Gerät: <ul style="list-style-type: none">▶ <code>Write</code> Bei Anfragen mit dem nebenstehenden Community-Namen erhält die Anwendung Lese- und Schreibrechte auf dem Gerät.▶ <code>Read</code> Bei Anfragen mit dem nebenstehenden Community-Namen erhält die Anwendung Leserechte auf dem Gerät.
Name	Legt den Community-Namen für die nebenstehende Berechtigung fest. Mögliche Werte: <ul style="list-style-type: none">▶ Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen <code>private</code> (Voreinstellung für Lese- und Schreibrechte) <code>public</code> (Voreinstellung für Leserechte)

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

3.4 Pre-Login-Banner

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

Die Benutzer sehen den Text im Login-Dialog der grafischen Benutzeroberfläche (GUI) und des Command Line Interfaces (CLI). Benutzer, die sich mit SSH anmelden, sehen den Text – abhängig vom verwendeten Client – vor oder während der Anmeldung.

Um den Text ausschließlich im Command Line Interface (CLI) anzuzeigen, verwenden Sie die Einstellungen im Dialog *Gerätesicherheit > Management-Zugriff > CLI*.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>Pre-Login-Banner</i> -Funktion ein/aus. Mit der <i>Pre-Login-Banner</i> -Funktion zeigt das Gerät im Login-Dialog der grafischen Benutzeroberfläche und des Command Line Interfaces eine Begrüßung oder einen Hinweis. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>Pre-Login-Banner</i>-Funktion ist eingeschaltet. Das Gerät zeigt im Login-Dialog den im Feld <i>Banner-Text</i> festgelegten Text.▶ Aus (Voreinstellung) Die <i>Pre-Login-Banner</i>-Funktion ist ausgeschaltet. Das Gerät zeigt im Login-Dialog keinen Text. Haben Sie im Feld <i>Banner-Text</i> einen Text eingegeben, bleibt dieser erhalten.

■ Banner-Text

Parameter	Bedeutung
Banner-Text	Legt den Begrüßungs- oder Hinweistext fest, den das Gerät im Login-Dialog der grafischen Benutzeroberfläche (GUI) und des Command Line Interfaces (CLI) anzeigt. Mögliche Werte: <ul style="list-style-type: none">▶ Alphanumerische ASCII-Zeichenfolge mit 0..512 Zeichen (0x20..0x7E) inklusive Leerzeichen▶ <Tabulator>▶ <Zeilenumbruch>
Verbleibende Zeichen	Zeigt, wie viele Zeichen im Feld <i>Banner-Text</i> noch zur Verfügung stehen. Mögliche Werte: <ul style="list-style-type: none">▶ 512..0

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

4 Netzsicherheit

Das Menü enthält die folgenden Dialoge:

- ▶ Port-Sicherheit
- ▶ 802.1X Port-Authentifizierung
- ▶ RADIUS
- ▶ DoS

4.1 Port-Sicherheit

Das Gerät bietet Ihnen die Möglichkeit, ausschließlich Datenpakete von erwünschten Absendern auf einem Port zu vermitteln. Bei eingeschalteter Funktion prüft das Gerät VLAN-ID und MAC-Adresse des Absenders, bevor es ein Datenpaket vermittelt. Die Datenpakete anderer Absender verwirft das Gerät und protokolliert dieses Ereignis. Wenn die *Auto-Disable*-Funktion aktiviert ist, schaltet das Gerät den Port aus. Diese Begrenzung erschwert MAC-Spoofing-Attacken. Die *Auto-Disable*-Funktion schaltet den betreffenden Port automatisch wieder ein, sofern die Überschreitung der Parameter aufgehoben ist.

In diesem Dialog unterstützt Sie ein *Wizard*-Fenster, die Ports mit einem oder mehreren erwünschten Absendern zu verknüpfen. Im Gerät heißen diese Adressen *Statische Einträge (/)*. Zum Ansehen der festgelegten statischen Adressen markieren Sie den betreffenden Port und klicken die Schaltfläche



Um den Einrichtungsaufwand gering zu halten, bietet Ihnen das Gerät die Möglichkeit, die erwünschten Absender automatisch zu erfassen. Das Gerät „lernt“ die Absender durch das Auswerten der empfangenen Datenpakete. Im Gerät heißen diese Adressen *Dynamische Einträge*. Sobald eine benutzerdefinierte Obergrenze (*Dynamisches Limit*) erreicht ist, beendet das Gerät das „Lernen“ auf dem betreffenden Port und vermittelt ausschließlich die Datenpakete der bereits erfassten Absender. Wenn Sie die Obergrenze an die Anzahl der zu erwartenden Absender anpassen, erschweren Sie damit MAC-Flooding-Attacken.

Anmerkung: Beim automatischen Erfassen der *Dynamische Einträge* verwirft das Gerät immer das 1. Datenpaket von unbekanntem Absender. Anhand dieses 1. Datenpakets prüft das Gerät, ob die Obergrenze erreicht ist. Bis zum Erreichen der Obergrenze erfasst das Gerät den Absender. Anschließend vermittelt das Gerät Datenpakete, die es auf dem betreffenden Port von diesem Absender empfängt.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>Port-Sicherheit</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>Port-Sicherheit</i>-Funktion ist eingeschaltet. Das Gerät prüft VLAN-ID und MAC-Adresse des Absenders, bevor es ein Datenpaket vermittelt. Das Gerät vermittelt ein empfangenes Datenpaket ausschließlich dann, wenn dessen Absender auf dem betreffenden Port erwünscht ist. Aktivieren Sie das Prüfen des Absenders zusätzlich auf den betreffenden Ports.▶ Aus (Voreinstellung) Die <i>Port-Sicherheit</i>-Funktion ist ausgeschaltet. Das Gerät vermittelt jedes empfangene Datenpaket, ohne den Absender zu prüfen.

■ Konfiguration

Parameter	Bedeutung
Auto-Disable	<p>Aktiviert/deaktiviert die <i>Auto-Disable</i>-Funktion für <i>Port-Sicherheit</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die <i>Auto-Disable</i>-Funktion für <i>Port-Sicherheit</i> ist aktiv. Markieren Sie zusätzlich das Kontrollkästchen in Spalte <i>Auto-Disable</i> für die gewünschten Ports. ▶ unmarkiert (Voreinstellung) Die <i>Auto-Disable</i>-Funktion für <i>Port-Sicherheit</i> ist inaktiv.


■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Aktiv	<p>Aktiviert/deaktiviert auf dem Port das Prüfen des Absenders.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Das Gerät prüft jedes auf dem Port empfangene Datenpaket, und vermittelt es, wenn dessen Absender erwünscht ist. Schalten Sie zusätzlich die Funktion im Rahmen <i>Funktion</i> ein. ▶ unmarkiert (Voreinstellung) Das Gerät vermittelt jedes auf dem Port empfangene Datenpaket, ohne den Absender zu prüfen. <p>Anmerkung: Wenn Sie das Gerät als aktiven Teilnehmer innerhalb eines MRP-Rings betreiben, empfehlen wir, die Markierung des Kontrollkästchens aufzuheben.</p>
Auto-Disable	<p>Aktiviert/deaktiviert die <i>Auto-Disable</i>-Funktion für die Parameter, deren Einhaltung die <i>Port-Sicherheit</i>-Funktion auf dem Port überwacht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Die <i>Auto-Disable</i>-Funktion ist auf dem Port aktiv. Voraussetzung ist, dass im Rahmen <i>Konfiguration</i> das Kontrollkästchen <i>Auto-Disable</i> markiert ist. <ul style="list-style-type: none"> – Das Gerät schaltet den Port aus, wenn der Port unerwünschte Absender oder mehr Absender erfasst als in Spalte <i>Dynamisches Limit</i> festgelegt ist. Die „Link-Status“-LED des Ports blinkt 3 × pro Periode. – Der Dialog <i>Diagnose > Ports > Auto-Disable</i> zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind. – Die <i>Auto-Disable</i>-Funktion schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog <i>Diagnose > Ports > Auto-Disable</i> in Spalte <i>Reset-Timer [s]</i> eine Wartezeit für den betreffenden Port fest. ▶ unmarkiert Die <i>Auto-Disable</i>-Funktion auf dem Port ist inaktiv.
Trap senden	<p>Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät auf dem Port Datenpakete von einem unerwünschten Absender verwirft.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Das Gerät sendet einen SNMP-Trap, wenn es auf dem Port Datenpakete von einem unerwünschten Absender verwirft. ▶ unmarkiert (Voreinstellung) Das Senden von SNMP-Traps ist deaktiviert. <p>Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose > Statuskonfiguration > Alarme (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen.</p>

Parameter	Bedeutung
Trap-Intervall [s]	<p>Legt die Wartezeit in Sekunden fest, die das Gerät nach Senden eines SNMP-Traps einhält, bis es den nächsten SNMP-Trap sendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..3600 (Voreinstellung: 0) <p>Der Wert 0 deaktiviert die Wartezeit.</p>
Dynamisches Limit	<p>Legt die Obergrenze fest für die Anzahl automatisch erfasster Absender (<i>Dynamische Einträge</i>). Sobald die Obergrenze erreicht ist, beendet das Gerät das „Lernen“ auf diesem Port.</p> <p>Passen Sie den Wert an die Anzahl der zu erwartenden Absender an.</p> <p>Wenn der Port mehr Absender erfasst als hier festgelegt ist, schaltet die Funktion <i>Auto-Disable</i> den Port aus. Voraussetzung ist, dass in Spalte <i>Auto-Disable</i> das Kontrollkästchen markiert ist und im Rahmen <i>Konfiguration</i> das Kontrollkästchen <i>Auto-Disable</i> markiert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0 Deaktiviert das automatische Erfassen der Absender auf diesem Port. ▶ 1..600 (Voreinstellung: 600)
Statisches Limit	<p>Legt die Obergrenze fest für die Anzahl der mit dem Port verknüpften Absender (<i>Statische Einträge (/)</i>). Das <i>Wizard</i>-Fenster unterstützt Sie dabei, den Port mit einem oder mehreren erwünschten Absendern zu verknüpfen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..64 (Voreinstellung: 64) <p>Der Wert 0 verhindert, dass Sie einen Absender mit dem Port verknüpfen.</p>
Dynamische Einträge	<p>Zeigt, wie viele Absender das Gerät automatisch ermittelt hat. Siehe Dialog <i>Wizard</i>, Feld <i>Dynamische Einträge</i>.</p>
Statische Einträge	<p>Zeigt, wie viele Absender mit dem Port verknüpft sind. Siehe Dialog <i>Wizard</i>, Feld <i>Statische Einträge (/)</i>.</p>
Last violating VLAN ID/MAC	<p>Zeigt VLAN-ID und MAC-Adresse eines unerwünschten Absenders, dessen Datenpakete das Gerät an diesem Port zuletzt verworfen hat.</p>
Gesendete Traps	<p>Zeigt die Anzahl der auf diesem Port verworfenen Datenpakete, die das Gerät zum Senden eines SNMP-Traps veranlasst haben.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	<p>Öffnet den Dialog <i>Wizard</i>. Im Dialog <i>Wizard</i> weisen Sie einem Port die zulässigen MAC-Adressen zu.</p>

[Wizard : Port-Sicherheit]

■ Port auswählen


Das *Wizard*-Fenster unterstützt Sie dabei, die Ports mit einem oder mehreren erwünschten Absendern zu verknüpfen.

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

■ Adressen

Das *Wizard*-Fenster unterstützt Sie dabei, die Ports mit einem oder mehreren erwünschten Absendern zu verknüpfen. Wenn Sie die Einstellungen festgelegt haben, klicken Sie die Schaltfläche *Fertig*.

Nach Schließen des *Wizard*-Fensters klicken Sie die Schaltfläche , um Ihre Einstellungen zu speichern.

Parameter	Bedeutung
VLAN-ID	Legt die VLAN-ID des erwünschten Absenders fest. Mögliche Werte: ▶ 1..4042 Um VLAN-ID und MAC-Adresse in das Feld <i>Statische Einträge (/)</i> zu übernehmen, klicken Sie die Schaltfläche <i>Hinzufügen</i> .
MAC-Adresse	Legt die MAC-Adresse des erwünschten Absenders fest. Mögliche Werte: ▶ Gültige Unicast-MAC-Adresse Legen Sie den Wert in einem der folgenden Formate fest: – ohne Trennzeichen, zum Beispiel 001122334455 – Trennung mit Leerzeichen, zum Beispiel 00 11 22 33 44 55 – Trennung mit Doppelpunkt, zum Beispiel 00:11:22:33:44:55 – Trennung mit Bindestrich, zum Beispiel 00-11-22-33-44-55 – Trennung mit Punkt, zum Beispiel 00.11.22.33.44.55 – Trennung mit Punkt nach jedem 4. Zeichen, zum Beispiel 0011.2233.4455 Um VLAN-ID und MAC-Adresse in das Feld <i>Statische Einträge (/)</i> zu übernehmen, klicken Sie die Schaltfläche <i>Hinzufügen</i> .
Hinzufügen	Übernimmt die in den Feldern <i>VLAN-ID</i> und <i>MAC-Adresse</i> festgelegten Werte in das Feld <i>Statische Einträge (/)</i> .
Statische Einträge (/)	Zeigt VLAN-ID und MAC-Adresse der mit dem Port verknüpften, erwünschten Absender. Über dem Feld zeigt das Gerät die Anzahl der mit dem Port verknüpften Absender sowie die Obergrenze. Die Obergrenze für die Anzahl der Einträge legen Sie fest in der Tabelle, Feld <i>Statisches Limit</i> . Anmerkung: Eine MAC-Adresse, die sie diesem Port zuweisen, können Sie keinem weiteren Port zuweisen.
Entfernen	Entfernt die im Feld <i>Statische Einträge (/)</i> markierten Einträge.
	Verschiebt die im Feld <i>Dynamische Einträge</i> markierten Einträge in das Feld <i>Statische Einträge (/)</i> .

Parameter	Bedeutung
◀	<p>Verschiebt jeden Eintrag aus dem Feld <i>Dynamische Einträge</i> in das Feld <i>Statische Einträge (/)</i>.</p> <p>Enthält das Feld <i>Dynamische Einträge</i> mehr Einträge als im Feld <i>Statische Einträge (/)</i> erlaubt sind, verschiebt das Gerät die vorderen Einträge, solange bis die Obergrenze erreicht ist.</p>
Dynamische Einträge	<p>Zeigt in aufsteigender Reihenfolge VLAN-ID und MAC-Adresse der auf diesem Port automatisch erfassten Absender. Das Gerät vermittelt Datenpakete von diesen Absendern, wenn es die Datenpakete auf diesem Port empfängt.</p> <p>Die Obergrenze für die Anzahl der Einträge legen Sie fest in der Tabelle, Feld <i>Dynamisches Limit</i>.</p> <p>Die Schaltflächen + und ◀ bieten Ihnen die Möglichkeit, Einträge aus diesem Feld in das Feld <i>Statische Einträge (/)</i> zu übernehmen. Damit verknüpfen Sie die betreffenden Absender mit dem Port.</p>

Anmerkung: Das Gerät speichert die mit dem Port verknüpften Absender so lange, bis Sie das Prüfen der Absender auf dem betreffenden Port oder im Rahmen *Funktion* deaktivieren.

4.2 802.1X Port-Authentifizierung

Mit der portbasierten Zugriffskontrolle gemäß IEEE 802.1X kontrolliert das Gerät den Zugriff angeschlossener Endgeräte auf das Netz. Das Gerät (Authenticator) gewährt einem Endgerät (Supplicant) ausschließlich dann Zugriff auf das Netz, wenn dieses sich mit gültigen Zugangsdaten anmeldet. Authenticator und Endgeräte kommunizieren über das Authentisierungsprotokoll EAPoL (Extensible Authentication Protocol over LANs).

Das Gerät unterstützt die folgenden Methoden, um Endgeräte zu authentifizieren:

- ▶ radius
Ein RADIUS-Server im Netz authentifiziert die Endgeräte.
- ▶ ias
Der im Gerät eingebaute Integrierte Authentifikationsserver (IAS) authentifiziert die Endgeräte. Im Vergleich zu RADIUS bietet der IAS lediglich grundlegende Funktionen.

Das Menü enthält die folgenden Dialoge:

- ▶ [802.1X Global](#)
- ▶ [802.1X Port-Konfiguration](#)
- ▶ [802.1X Port-Clients](#)
- ▶ [802.1X EAPoL-Portstatistiken](#)
- ▶ [802.1X Port-Authentifizierung-Historie](#)
- ▶ [802.1X Integrierter Authentifikations-Server](#)

4.2.1 802.1X Global

Dieser Dialog bietet Ihnen die Möglichkeit, grundlegende Einstellungen für die portbasierte Zugriffskontrolle festzulegen.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>802.1X Port-Authentifizierung</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>802.1X Port-Authentifizierung</i>-Funktion ist eingeschaltet. Das Gerät prüft den Zugriff angeschlossener Endgeräte auf das Netz. Die portbasierte Zugriffskontrolle ist eingeschaltet.▶ Aus (Voreinstellung) Die <i>802.1X Port-Authentifizierung</i>-Funktion ist ausgeschaltet. Die portbasierte Zugriffskontrolle ist ausgeschaltet.

■ Konfiguration

Parameter	Bedeutung
VLAN zuweisen	Aktiviert/deaktiviert die Zuweisung des betreffenden Ports zu einem VLAN. Diese Funktion bietet Ihnen die Möglichkeit, dem angeschlossenen Endgerät in diesem VLAN ausgewählte Dienste bereitzustellen. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Das Zuweisen ist aktiv. Wenn sich das Endgerät erfolgreich authentifiziert, weist das Gerät dem betreffenden Port die vom RADIUS-Authentication-Server übermittelte VLAN-ID zu.▶ unmarkiert (Voreinstellung) Die Zuweisen ist inaktiv. Der betreffende Port ist dem im Dialog <i>Netzicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration</i>, Spalte <i>Zugewiesene VLAN-ID</i> festgelegten VLAN zugewiesen.
VLAN dynamisch erzeugen	Aktiviert/deaktiviert das automatische Einrichten des vom RADIUS-Authentication-Server zugewiesenen VLANs, falls dieses nicht existiert. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Das automatische Einrichten von VLANs ist aktiv. Das Gerät erzeugt das VLAN, falls es nicht existiert.▶ unmarkiert (Voreinstellung) Das automatische Einrichten von VLANs ist inaktiv. Existiert das zugewiesene VLAN nicht, bleibt der Port dem ursprünglichen VLAN zugewiesen.
Monitor-Mode	Aktiviert/deaktiviert den Monitor-Modus. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Der Monitor-Modus ist eingeschaltet. Das Gerät überwacht die Authentifizierung und hilft bei der Fehlerdiagnose. Wenn sich ein Endgerät erfolglos anmeldet, gewährt das Gerät dem Endgerät Zugriff auf das Netz.▶ unmarkiert (Voreinstellung) Der Monitor-Modus ist ausgeschaltet.

■ Information

Parameter	Bedeutung
Monitor-Mode-Clients	Zeigt, wie vielen Endgeräten das Gerät trotz erfolgloser Anmeldung Zugriff auf das Netz gewährt hat. Voraussetzung ist, dass die Funktion <i>Monitor-Mode</i> im Gerät aktiviert ist. Siehe Rahmen <i>Konfiguration</i> .
Non-Monitor-Mode-Clients	Zeigt, wie vielen Endgeräten das Gerät nach erfolgreicher Anmeldung Zugriff auf das Netz gewährt hat.
Richtlinie 1	Zeigt die Methode, die das Gerät zum Authentifizieren der Endgeräte per IEEE 802.1X gegenwärtig anwendet. Die anzuwendende Methode legen Sie im Dialog <i>Gerätesicherheit > Authentifizierungsliste</i> fest. <ul style="list-style-type: none"> <input type="checkbox"/> Um die Endgeräte über einen RADIUS-Server zu authentifizieren, weisen Sie der Liste <i>radius</i> die Richtlinie <i>8021x</i> zu. <input type="checkbox"/> Um die Endgeräte über den Integrierten Authentifikationsserver (IAS) zu authentifizieren, weisen Sie der Liste <i>ias</i> die Richtlinie <i>8021x</i> zu.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

4.2.2 802.1X Port-Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, die Zugriffseinstellungen für jeden Port festzulegen.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Port-Initialisierung	<p>Aktiviert/deaktiviert das Initialisieren des Ports, um die Zugriffskontrolle auf dem Port zu aktivieren oder in den Initialzustand zurückzusetzen. Wenden Sie diese Funktion ausschließlich dann an, wenn für den Port in Spalte <i>Port-Kontrolle</i> der Wert <code>auto</code> festgelegt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Das Initialisieren des Ports ist aktiv. Sobald die Initialisierung abgeschlossen ist, ändert das Gerät den Wert wieder auf <code>unmarkiert</code>. ▶ <code>unmarkiert</code> (Voreinstellung) Das Initialisieren des Ports ist inaktiv. Das Gerät behält den gegenwärtigen Port-Status bei.
Port-Reauthentifizierung	<p>Aktiviert/deaktiviert die einmalige Authentifizierungsanforderung. Wenden Sie diese Funktion ausschließlich dann an, wenn für den Port in Spalte <i>Port-Kontrolle</i> der Wert <code>auto</code> festgelegt ist. Das Gerät bietet Ihnen außerdem die Möglichkeit, das Endgerät periodisch aufzufordern, sich erneut anzumelden. Siehe Spalte <i>Periodische Reauthentifizierung</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Die einmalige Authentifizierungsanforderung ist aktiv. Das Gerät fordert das Endgerät auf, sich erneut anzumelden. Anschließend ändert das Gerät den Wert wieder auf <code>unmarkiert</code>. ▶ <code>unmarkiert</code> (Voreinstellung) Die einmalige Authentifizierungsanforderung ist inaktiv. Das Gerät behält die Anmeldung des Endgeräts bei.
Authentifizierungsvorgang	<p>Zeigt den gegenwärtigen Zustand des Authenticators (<code>Authenticator PAE state</code>).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>initialize</code> ▶ <code>disconnected</code> ▶ <code>connecting</code> ▶ <code>authenticating</code> ▶ <code>authenticated</code> ▶ <code>aborting</code> ▶ <code>held</code> ▶ <code>forceAuth</code> ▶ <code>forceUnauth</code>
Authentifizierungszustand Backend	<p>Zeigt den gegenwärtigen Zustand der Verbindung zum Authentifizierungs-Server (<code>Backend Authentication state</code>).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>request</code> ▶ <code>response</code> ▶ <code>erfolgreich</code> ▶ <code>fail</code> ▶ <code>timeout</code> ▶ <code>idle</code> ▶ <code>initialize</code>

Parameter	Bedeutung
Authentifizierungs-Zustand	<p>Zeigt den gegenwärtigen Zustand der Authentifizierung auf dem Port (<code>Controlled Port Status</code>).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>authorized</code> Das Endgerät ist erfolgreich angemeldet. ▶ <code>unauthorized</code> Das Endgerät ist nicht angemeldet.
Port-Kontrolle	<p>Legt fest, wie das Gerät den Zugriff auf das Netz gewährt (<code>Port control mode</code>).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>forceUnauthorized</code> Das Gerät sperrt den Zugriff auf das Netz. Verwenden Sie diese Einstellung, wenn am Port ein Endgerät angeschlossen ist, das keinen Zugriff auf das Netz erhält. ▶ <code>auto</code> Das Gerät gewährt den Zugriff auf das Netz, wenn sich das Endgerät erfolgreich angemeldet hat. Verwenden Sie diese Einstellung, wenn am Port ein Endgerät angeschlossen ist, das sich beim Authenticator anmeldet. Wenn über denselben Port weitere Endgeräte angeschlossen sind, erhalten diese ohne zusätzliche Authentifizierung Zugriff auf das Netz. ▶ <code>forceAuthorized</code> (Voreinstellung) Das Gerät gewährt den Zugriff auf das Netz. Verwenden Sie diese Einstellung, wenn am Port ein Endgerät angeschlossen ist, das ohne Anmeldung Zugriff auf das Netz erhält.
Ruheperiode [s]	<p>Legt die Zeitspanne in Sekunden fest, in welcher der Authenticator nach einem erfolglosen Anmeldeversuch keine erneute Anmeldung des Endgeräts akzeptiert (<code>Ruheperiode [s]</code>).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>0..65535</code> (Voreinstellung: 60)
Sendeperiode [s]	<p>Legt die Zeit in Sekunden fest, nach welcher der Authenticator das Endgerät auffordert, sich erneut anzumelden. Nach dieser Wartezeit sendet das Gerät ein EAP-Request/Identity-Datenpaket an das Endgerät.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>1..65535</code> (Voreinstellung: 30)
Supplikant-Timeout [s]	<p>Legt die Zeitspanne in Sekunden fest, innerhalb welcher der Authenticator auf die Anmeldung des Endgeräts wartet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>1..65535</code> (Voreinstellung: 30)
Server-Timeout [s]	<p>Legt die Zeitspanne in Sekunden fest, innerhalb welcher der Authenticator auf die Antwort des Authentication-Servers (RADIUS oder IAS) wartet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>1..65535</code> (Voreinstellung: 30)
Requests (max.)	<p>Legt fest, wie viele Male der Authenticator das Endgerät auffordert, sich anzumelden, bis die in Spalte <i>Supplikant-Timeout [s]</i> festgelegte Zeit erreicht ist. Das Gerät sendet sooft wie hier festgelegt ein EAP-Request/Identity-Datenpaket an das Endgerät.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>0..10</code> (Voreinstellung: 2)
Zugewiesene VLAN-ID	<p>Zeigt die ID des VLANs, die der Authenticator dem Port zugewiesen hat. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte <i>Port-Kontrolle</i> der Wert <code>auto</code> festgelegt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>0..4042</code> (Voreinstellung: 0) <p>Die VLAN-ID, die der Authenticator den Ports zugewiesen hat, finden Sie im Dialog <i>Netzicherheit > 802.1X Port-Authentifizierung > Port-Clients</i>.</p> <p>Wenn für den Port in Spalte <i>Port-Kontrolle</i> der Wert <code>multiClient</code> festgelegt ist: Das Gerät weist das VLAN-Tag anhand der MAC-Adresse des Endgeräts zu, wenn es Datenpakete ohne VLAN-Tag empfängt.</p>

Parameter	Bedeutung
Zuweisungsgrund	<p>Zeigt den Grund für die Zuweisung der VLAN-ID. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte <i>Port-Kontrolle</i> der Wert <code>auto</code> festgelegt ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>notAssigned</code> (Voreinstellung) ▶ <code>radius</code> ▶ <code>guestVlan</code> ▶ <code>unauthenticatedVlan</code> <p>Die VLAN-ID, die der Authenticator den Ports zugewiesen hat, finden Sie im Dialog <i>Netzsicherheit > 802.1X Port-Authentifizierung > Port-Clients</i>.</p>
Reauthentifizierungs-Periode [s]	<p>Legt die Zeitspanne in Sekunden fest, nach welcher der Authenticator periodisch das Endgerät auffordert, sich erneut anzumelden.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>1..65535</code> (Voreinstellung: 3600)
Periodische Reauthentifizierung	<p>Aktiviert/deaktiviert periodische Authentifizierungsanforderungen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Periodische Authentifizierungsanforderungen sind aktiv. Das Gerät fordert das Endgerät periodisch auf, sich erneut anzumelden. Die Zeitspanne legen Sie fest in Spalte <i>Reauthentifizierungs-Periode [s]</i>. Diese Einstellung ist außer Kraft gesetzt, wenn der Authenticator dem Endgerät die ID eines Voice-, Unauthenticated- oder Gast-VLANs zugewiesen hat. ▶ <code>unmarkiert</code> (Voreinstellung) Periodische Authentifizierungsanforderungen sind inaktiv. Das Gerät behält die Anmeldung des Endgeräts bei.
Gast VLAN-ID	<p>Legt die ID des VLANs fest, die der Authenticator dem Port zuweist, wenn sich das Endgerät während der in Spalte <i>Gast-VLAN-Intervall</i> festgelegten Zeit nicht anmeldet. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte <i>Port-Kontrolle</i> der Wert <code>auto</code> festgelegt ist.</p> <p>Diese Funktion bietet Ihnen die Möglichkeit, Endgeräten ohne 802.1X-Unterstützung Zugriff auf ausgewählte Dienste im Netz zu gewähren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>0</code> (Voreinstellung) Der Authenticator weist dem Port kein Gast-VLAN zu. ▶ <code>1..4042</code> <p>Anmerkung: Weisen Sie dem Port ausschließlich ein im Gerät statisch eingerichtetes VLAN zu.</p>
Gast-VLAN-Intervall	<p>Legt die Zeitspanne in Sekunden fest, in welcher der Authenticator nach Anschließen des Endgeräts auf EAPOL-Datenpakete wartet. Läuft diese Zeit ab, gewährt der Authenticator dem Endgerät Zugriff auf das Netz und weist den Port dem in Spalte <i>Gast VLAN-ID</i> festgelegten Gast-VLAN zu.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>1..300</code> (Voreinstellung: 90)
Unauthenticated-VLAN-ID	<p>Legt die ID des VLANs fest, die der Authenticator dem Port zuweist, wenn sich das Endgerät ohne Erfolg anmeldet. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte <i>Port-Kontrolle</i> der Wert <code>auto</code> festgelegt ist.</p> <p>Diese Funktion bietet Ihnen die Möglichkeit, Endgeräten ohne gültige Zugangsdaten Zugriff auf ausgewählte Dienste im Netz zu gewähren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>0..4042</code> (Voreinstellung: 0) <p>Der Wert <code>0</code> bewirkt, dass der Authenticator dem Port kein Unauthenticated-VLAN zuweist.</p> <p>Anmerkung: Weisen Sie dem Port ausschließlich ein im Gerät statisch eingerichtetes VLAN zu.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

4.2.3 802.1X Port-Clients

Dieser Dialog zeigt Informationen über die angeschlossenen Endgeräte.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Benutzername	Zeigt den Benutzernamen, mit dem sich das Endgerät angemeldet hat.
MAC-Adresse	Zeigt die MAC-Adresse des Endgeräts.
Zugewiesene VLAN-ID	Zeigt die VLAN-ID, die der Authenticator dem Port nach erfolgreicher Authentifizierung des Endgeräts zugewiesen hat.
Zuweisungsgrund	<p>Zeigt den Grund für die Zuweisung des VLANs.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ default ▶ radius ▶ unauthenticatedVlan ▶ guestVlan ▶ monitorVlan ▶ invalid <p>Das Feld zeigt ausschließlich dann einen gültigen Wert, solange der Client authentifiziert ist.</p>
Session-Timeout	<p>Zeigt die verbleibende Zeit in Sekunden, bis die Anmeldung des Endgeräts abläuft. Dieser Wert gilt ausschließlich dann, wenn für den Port im Dialog <i>Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration</i>, Spalte <i>Port-Kontrolle</i> der Wert <code>auto</code> festgelegt ist.</p> <p>Der Authentication-Server weist dem Gerät die Timeout-Zeit per RADIUS zu. Der Wert <code>0</code> bedeutet, dass der Authentication-Server kein Timeout zugewiesen hat.</p>
Termination action	<p>Zeigt die Aktion, die das Gerät bei Ablauf der Anmeldung ausführt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ default ▶ reauthenticate

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

4.2.4 802.1X EAPOL-Portstatistiken

Dieser Dialog zeigt, welche EAPoL-Datenpakete das Gerät für die Authentifizierung der Endgeräte gesendet und empfangen hat.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Empfangene Pakete	Zeigt, wie viele EAPOL-Datenpakete insgesamt das Gerät auf dem Port empfangen hat.
Gesendete Pakete	Zeigt, wie viele EAPOL-Datenpakete insgesamt das Gerät auf dem Port gesendet hat.
Start-Pakete	Zeigt, wie viele EAPOL-Start-Datenpakete das Gerät auf dem Port empfangen hat.
Abmelde-Pakete	Zeigt, wie viele EAPOL-Logoff-Datenpakete das Gerät auf dem Port empfangen hat.
Response/ID packets	Zeigt, wie viele EAP-Response/Identity-Datenpakete das Gerät auf dem Port empfangen hat.
Antwort-Pakete	Zeigt, wie viele gültige EAP-Response-Datenpakete das Gerät auf dem Port empfangen hat (ohne EAP-Response/Identity-Datenpakete).
Request/ID-Pakete	Zeigt, wie viele EAP-Request/Identity-Datenpakete das Gerät auf dem Port empfangen hat.
Request-Pakete	Zeigt, wie viele gültige EAP-Request-Datenpakete das Gerät auf dem Port empfangen hat (ohne EAP-Request/Identity-Datenpakete).
Ungültige Pakete	Zeigt, wie viele EAPOL-Datenpakete mit unbekanntem Frame-Typ das Gerät auf dem Port empfangen hat.
Empfangene Error-Pakete	Zeigt, wie viele EAPOL-Datenpakete mit ungültigem Packet-Body-Length-Feld das Gerät auf dem Port empfangen hat.
Paket-Version	Zeigt die Protokoll-Versionsnummer des EAPOL-Datenpakets, welches das Gerät auf dem Port zuletzt empfangen hat.
Quelle des zuletzt empfangenen Pakets	Zeigt die Absender-MAC-Adresse des EAPOL-Datenpakets, welches das Gerät auf dem Port zuletzt empfangen hat. Der Wert 00:00:00:00:00:00 bedeutet, dass der Port noch kein EAPOL-Datenpaket empfangen hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

4.2.5 802.1X Port-Authentifizierung-Historie

Das Gerät protokolliert den Authentifizierungsvorgang der Endgeräte, die an seinen Ports angeschlossen sind. Dieser Dialog zeigt die bei der Authentifizierung erfassten Informationen.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Authentifizierungs-Zeitpunkt	Zeigt den Zeitpunkt, zu dem der Authenticator das Endgerät authentifiziert hat.
Eintrag vorhanden seit	Zeigt, seit wann dieser Eintrag in der Tabelle eingetragen ist.
MAC-Adresse	Zeigt die MAC-Adresse des Endgeräts.
VLAN-ID	Zeigt die ID des VLAN, das dem Endgerät vor der Anmeldung zugewiesen war.
Authentifizierungs-Status	<p>Zeigt den Zustand der Authentifizierung auf dem Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ erfolgreich Die Authentifizierung war erfolgreich. ▶ Fehler Die Authentifizierung war fehlerhaft.
Zugriffs-Status	<p>Zeigt, ob das Gerät dem Endgerät Zugriff auf das Netz gewährt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ granted Das Gerät gewährt dem Endgerät den Zugriff auf das Netz. ▶ denied Das Gerät sperrt dem Endgerät den Zugriff auf das Netz.
Zugewiesene VLAN-ID	Zeigt die ID des VLANs, die der Authenticator dem Port zugewiesen hat.
Zuweisungs-Typ	<p>Zeigt die Art des VLAN, das der Authenticator dem Port zugewiesen hat.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ default ▶ radius ▶ unauthenticatedVlan ▶ guestVlan ▶ monitorVlan ▶ notAssigned
Zuweisungsgrund	Zeigt den Grund für die Zuweisung der VLAN-ID und des VLAN-Typs.

■ 802.1X Port-Authentifizierung-Historie

Parameter	Bedeutung
Port	<p>Vereinfacht die Anzeige und zeigt in der Tabelle ausschließlich die Einträge, die den hier ausgewählten Port betreffen. Dies erleichtert Ihnen, die Tabelle zu erfassen und nach Ihren Wünschen zu sortieren.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ all Die Tabelle zeigt die Einträge für jeden Port.▶ <Port-Nummer> Die Tabelle zeigt die Einträge, die ausschließlich den hier ausgewählten Port betreffen.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.


4.2.6 802.1X Integrierter Authentifikations-Server

Der Integrierte Authentifikationsserver (IAS) bietet Ihnen die Möglichkeit, Endgeräte per IEEE 802.1X zu authentifizieren. Im Vergleich zu RADIUS hat der IAS einen sehr eingeschränkten Funktionsumfang. Die Authentifizierung erfolgt ausschließlich anhand von Benutzername und Passwort.

In diesem Dialog verwalten Sie die Zugangsdaten der Endgeräte. Das Gerät bietet Ihnen die Möglichkeit, bis zu 100 Zugangsdaten einzurichten.


Um die Endgeräte über den Integrierten Authentifikationsserver zu authentifizieren, weisen Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* der Liste *ias* die Richtlinie *ias* zu.

■ Tabelle

Parameter	Bedeutung
Benutzername	Zeigt den Benutzernamen des Endgeräts. Um einen neuen Benutzer anzulegen, klicken Sie die Schaltfläche  .
Passwort	Legt das Passwort fest, mit dem sich der Benutzer authentifiziert. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
Aktiv	Aktiviert/deaktiviert die Zugangsdaten. Mögliche Werte: ▶ <i>markiert</i> Die Zugangsdaten sind aktiv. Ein Endgerät hat die Möglichkeit, sich mit diesen Zugangsdaten per 802.1x anzumelden. ▶ <i>unmarkiert</i> (Voreinstellung) Die Zugangsdaten sind inaktiv.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Öffnet das Fenster <i>Erzeugen</i> , um der Tabelle einen neuen Eintrag hinzuzufügen. Im Feld <i>Benutzername</i> legen Sie den Benutzernamen des Endgeräts fest.

4.3 RADIUS

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

RADIUS (Remote Authentication Dial-In User Service) bietet Ihnen die Möglichkeit, die Benutzer gegen eine zentrale Stelle im Netz zu authentifizieren und zu autorisieren. Ein RADIUS-Server erledigt dabei folgende Aufgaben:

- ▶ **Authentifizierung**
Der Authentication-Server authentifiziert die Benutzer, wenn der RADIUS-Client im Zugangspunkt die Zugangsdaten der Benutzer an ihn weiterleitet.
- ▶ **Autorisierung**
Der Authentication-Server autorisiert angemeldete Benutzer für ausgewählte Dienste, indem er dem RADIUS-Client im Zugangspunkt diverse Parameter für das betreffende Endgerät zuweist.
- ▶ **Abrechnung**
Der Accounting-Server erfasst die während der Port-Authentifizierung gemäß IEEE 802.1X angefallenen Verkehrsdaten. Damit lässt sich nachträglich feststellen, welche Dienste die Benutzer in welchem Umfang genutzt haben.

Das Gerät arbeitet in der Rolle des RADIUS-Clients, wenn Sie im Dialog `radius` einer Anwendung die Richtlinie *Gerätesicherheit > Authentifizierungs-Liste* zuweisen. Das Gerät leitet die Zugangsdaten der Benutzer weiter an den primären Authentication-Server. Der Authentication-Server entscheidet, ob die Zugangsdaten gültig sind und übermittelt dem Gerät die Berechtigungen des Benutzers.

Den in der Antwort eines RADIUS-Servers übertragenen Service-Type weist das Gerät wie folgt einer auf dem Gerät vorhandenen Benutzer-Rolle zu:

- Administrative-User: administrator
- Login-User: operator
- NAS-Prompt-User: guest

Das Gerät bietet Ihnen die Möglichkeit, auch Endgeräte per IEEE 802.1X über einen Authentication-Server zu authentifizieren. Hierzu weisen Sie im Dialog `radius` der Liste `8021x` die Richtlinie *Gerätesicherheit > Authentifizierungs-Liste* zu.

Das Menü enthält die folgenden Dialoge:

- ▶ [RADIUS Global](#)
- ▶ [RADIUS Authentication-Server](#)
- ▶ [RADIUS Accounting-Server](#)
- ▶ [RADIUS Authentication Statistiken](#)
- ▶ [RADIUS Accounting-Statistiken](#)

4.3.1 RADIUS Global


Dieser Dialog bietet Ihnen die Möglichkeit, grundlegende Einstellungen für RADIUS festzulegen.

■ RADIUS-Konfiguration

Parameter	Bedeutung
Anfragen (max.)	Legt fest, wie viele Male das Gerät eine unbeantwortete Anfrage an den Authentication-Server wiederholt, bevor es die Anfrage an einen anderen Authentication-Server sendet. Mögliche Werte: ▶ 1..15 (Voreinstellung: 4)
Timeout [s]	Legt fest, wie viele Sekunden das Gerät nach einer Anfrage an den Authentication-Server auf Antwort wartet, bevor es die Anfrage erneut sendet. Mögliche Werte: ▶ 1..30 (Voreinstellung: 5)
Accounting	Aktiviert/deaktiviert das Accounting. Mögliche Werte: ▶ markiert Accounting ist aktiv. Das Gerät sendet die Verkehrsdaten an einen im Dialog <i>Netzsicherheit > RADIUS > Accounting-Server</i> festgelegten Accounting-Server. ▶ unmarkiert (Voreinstellung) Accounting ist inaktiv.
NAS-IP-Adresse (Attribut 4)	Legt die IP-Adresse fest, die das Gerät als Attribut 4 an den Authentication-Server überträgt. Legen Sie die IP-Adresse des Geräts oder eine andere, frei wählbare Adresse fest. Mögliche Werte: ▶ Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0) In vielen Fällen befindet sich zwischen Gerät und Authentication-Server eine Firewall. Bei der Network Address Translation (NAT) in der Firewall ändert sich die ursprüngliche IP-Adresse, der Authentication-Server empfängt die übersetzte IP-Adresse des Geräts. Die IP-Adresse in diesem Feld überträgt das Gerät unverändert über Network Address Translation (NAT) hinweg.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Löscht die Statistik im Dialog <i>Netzsicherheit > RADIUS > Authentication-Statistiken</i> und die Statistik im Dialog <i>Netzsicherheit > RADIUS > Accounting-Statistiken</i> .

4.3.2 RADIUS Authentication-Server

Dieser Dialog bietet Ihnen die Möglichkeit, bis zu 8 Authentication-Server festzulegen. Ein Authentication-Server authentifiziert und autorisiert die Benutzer, wenn das Gerät die Zugangsdaten an ihn weiterleitet.


Das Gerät sendet die Zugangsdaten an den als primär gekennzeichneten Authentication-Server. Bleibt dessen Antwort aus, kontaktiert das Gerät den obersten in der Tabelle festgelegten Authentication-Server. Bleibt auch dessen Antwort aus, kontaktiert das Gerät den jeweils nächsten Server in der Tabelle.

■ Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.
Name	Zeigt den Namen des Servers. Um den Wert zu ändern, klicken Sie in das betreffende Feld. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen (Voreinstellung: Default-RADIUS-Server)
Adresse	Legt die IP-Adresse des Servers fest. Mögliche Werte: ▶ Gültige IPv4-Adresse
Ziel-UDP-Port	Legt die Nummer des UDP-Ports fest, auf dem der Server Anfragen entgegennimmt. Mögliche Werte: ▶ 0..65535 (Voreinstellung: 1812) Ausnahme: Port 2222 ist für interne Funktionen reserviert.
Secret	Zeigt ***** (Sternchen), wenn ein Passwort festgelegt ist, mit dem sich das Gerät beim Server anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..64 Zeichen Das Passwort erfahren Sie vom Administrator des Authentication-Servers.
Primary server	Kennzeichnet den Authentication-Server als primär oder sekundär. Mögliche Werte: ▶ markiert Der Server ist als primärer Authentication-Server gekennzeichnet. Das Gerät sendet die Zugangsdaten zum Authentifizieren der Benutzer an diesen Authentication-Server. Wenn Sie mehrere Server markieren, kennzeichnet das Gerät den zuletzt markierten Server als primären Authentication-Server. ▶ unmarkiert (Voreinstellung) Der Server ist als sekundärer Authentication-Server gekennzeichnet. Das Gerät sendet die Zugangsdaten an den sekundären Authentication-Server, wenn es vom primären Authentication-Server keine Antwort erhält.
Aktiv	Aktiviert/deaktiviert die Verbindung zum Server. Das Gerät verwendet den Server, wenn Sie im Dialog <i>Gerätesicherheit</i> > Authentifizierungsliste den Wert <i>radius</i> in einer der Spalten <i>Richtlinie 1</i> bis <i>Richtlinie 5</i> festlegen. Mögliche Werte: ▶ markiert (Voreinstellung) Die Verbindung ist aktiv. Das Gerät sendet die Zugangsdaten zum Authentifizieren der Benutzer an diesen Server, wenn die obengenannten Voraussetzungen erfüllt sind. ▶ unmarkiert Die Verbindung ist inaktiv. Das Gerät sendet keine Zugangsdaten an diesen Server.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	<p>Öffnet das Fenster <i>Erzeugen</i>, um der Tabelle einen neuen Eintrag hinzuzufügen.</p> <ul style="list-style-type: none">▶ Im Feld <i>Index</i> legen Sie die Index-Nummer fest.▶ Im Feld <i>Adresse</i> legen Sie die IP-Adresse des Servers fest.

4.3.3 RADIUS Accounting-Server

Dieser Dialog bietet Ihnen die Möglichkeit, bis zu 8 Accounting-Server festzulegen. Ein Accounting-Server erfasst die während der Port-Authentifizierung gemäß IEEE 802.1X angefallenen Verkehrsdaten. Voraussetzung ist, dass im Menü *Netzsicherheit > RADIUS > Global* die Funktion *Accounting* eingeschaltet ist.


Das Gerät sendet die Verkehrsdaten an den ersten erreichbaren Accounting-Server. Bleibt dessen Antwort aus, kontaktiert das Gerät den jeweils nächsten Server aus der Tabelle.

■ Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht. Mögliche Werte: ▶ 1..8
Name	Zeigt den Namen des Servers. Um den Wert zu ändern, klicken Sie in das betreffende Feld. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen (Voreinstellung: Default-RADIUS-Server)
Adresse	Legt die IP-Adresse des Servers fest. Mögliche Werte: ▶ Gültige IPv4-Adresse
Ziel-UDP-Port	Legt die Nummer des UDP-Ports fest, auf dem der Server Anfragen entgegennimmt. Mögliche Werte: ▶ 0..65535 (Voreinstellung: 1813) Ausnahme: Port 2222 ist für interne Funktionen reserviert.
Secret	Zeigt ***** (Sternchen), wenn ein Passwort festgelegt ist, mit dem sich das Gerät beim Server anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..16 Zeichen Das Passwort erfahren Sie vom Administrator des Authentication-Servers.
Aktiv	Aktiviert/deaktiviert die Verbindung zum Server. Mögliche Werte: ▶ markiert (Voreinstellung) Die Verbindung ist aktiv. Das Gerät sendet Verkehrsdaten an diesen Server, wenn die obengenannten Voraussetzungen erfüllt sind. ▶ unmarkiert Die Verbindung ist inaktiv. Das Gerät sendet keine Verkehrsdaten an diesen Server.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Öffnet das Fenster <i>Erzeugen</i> , um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld <i>Index</i> legen Sie die Index-Nummer fest. ▶ Im Feld <i>Adresse</i> legen Sie die IP-Adresse des Servers fest.

4.3.4 RADIUS Authentication Statistiken

Dieser Dialog zeigt Informationen über die Kommunikation zwischen dem Gerät und dem Authentication-Server. Die Tabelle zeigt die Informationen für jeden Server in einer separaten Zeile.

Um die Statistik zu löschen, klicken Sie im Dialog *Netzicherheit > RADIUS > Global* die Schaltfläche *Clear RADIUS statistics?*.

■ Tabelle

Parameter	Bedeutung
Name	Zeigt den Namen des Servers.
Adresse	Zeigt die IP-Adresse des Servers.
Round-Trip-Time	Zeigt das Zeitintervall in Hundertstelsekunden zwischen der zuletzt empfangenen Antwort des Servers (Access-Reply/Access-Challenge) und dem zugehörigen gesendeten Datenpaket (Access-Request).
Zugriffsanforderungen	Zeigt, wie viele Access-Datenpakete das Gerät an den Server gesendet hat. Der Wert berücksichtigt keine Wiederholungen.
Neu gesendete Access-Request-Pakete	Zeigt, wie viele Access-Datenpakete das Gerät wiederholt an den Server gesendet hat.
Akzeptierte Anfragen	Zeigt, wie viele Access-Accept-Datenpakete das Gerät vom Server empfangen hat.
Verworfenen Anfragen	Zeigt, wie viele Access-Reject-Datenpakete das Gerät vom Server empfangen hat.
Access challenges	Zeigt, wie viele Access-Challenge-Datenpakete das Gerät vom Server empfangen hat.
Fehlerhafte Access-Antworten	Zeigt, wie viele fehlerhafte Access-Response-Datenpakete das Gerät vom Server empfangen hat (einschließlich Datenpakete mit ungültiger Länge).
Fehlerhafter Authentifikator	Zeigt, wie viele Access-Response-Datenpakete mit ungültigem Authentifikator das Gerät vom Server empfangen hat.
Offene Anfragen	Zeigt, wie viele Access-Request-Datenpakete das Gerät an den Server gesendet hat, auf die es noch keine Antwort vom Server empfangen hat.
Timeouts	Zeigt, wie viele Male die Antwort des Servers vor Ablauf der voreingestellten Wartezeit ausgeblieben ist.
Unbekannte Pakete	Zeigt, wie viele Datenpakete mit unbekanntem Datentyp das Gerät auf dem Authentication-Port vom Server empfangen hat.
Verworfenen Pakete	Zeigt, wie viele Datenpakete das Gerät auf dem Authentication-Port vom Server empfangen und anschließend verworfen hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

4.3.5 RADIUS Accounting-Statistiken

Dieser Dialog zeigt Informationen über die Kommunikation zwischen dem Gerät und dem Accounting-Server. Die Tabelle zeigt die Informationen für jeden Server in einer separaten Zeile.

Um die Statistik zu löschen, klicken Sie im Dialog *Netzsicherheit > RADIUS > Global* die Schaltfläche *Clear RADIUS statistics?*.

■ Tabelle

Parameter	Bedeutung
Name	Zeigt den Namen des Servers.
Adresse	Zeigt die IP-Adresse des Servers.
Round-Trip-Time	Zeigt das Zeitintervall in Hundertstelsekunden zwischen der zuletzt empfangenen Antwort des Servers (Accounting-Response) und dem zugehörigen gesendeten Datenpaket (Accounting-Request).
Accounting-Request-Pakete	Zeigt, wie viele Accounting-Request-Datenpakete das Gerät an den Server gesendet hat. Der Wert berücksichtigt keine Wiederholungen.
Neu gesendete Accounting-Request-Pakete	Zeigt, wie viele Accounting-Request-Datenpakete das Gerät wiederholt an den Server gesendet hat.
Empfangene Pakete	Zeigt, wie viele Accounting-Response-Datenpakete das Gerät vom Server empfangen hat.
Fehlerhafte Pakete	Zeigt, wie viele fehlerhafte Accounting-Response-Datenpakete das Gerät vom Server empfangen hat (einschließlich Datenpakete mit ungültiger Länge).
Fehlerhafter Authentifikator	Zeigt, wie viele Accounting-Response-Datenpakete mit ungültigem Authentifikator das Gerät vom Server empfangen hat.
Offene Anfragen	Zeigt, wie viele Accounting-Request-Datenpakete das Gerät an den Server gesendet hat, auf die es noch keine Antwort vom Server empfangen hat.
Timeouts	Zeigt, wie viele Male die Antwort des Servers vor Ablauf der voreingestellten Wartezeit ausgeblieben ist.
Unbekannte Pakete	Zeigt, wie viele Datenpakete mit unbekanntem Datentyp das Gerät auf dem Accounting-Port vom Server empfangen hat.
Verworfen Pakete	Zeigt, wie viele Datenpakete das Gerät auf dem Accounting-Port vom Server empfangen und anschließend verworfen hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

4.4 DoS

Denial-of-Service (DoS) ist ein Cyber-Angriff, der darauf abzielt, den Betrieb bestimmter Dienste oder Geräte zu stören. In diesem Menü können Sie mehrere Filter einrichten, um das Gerät vor DoS-Angriffen zu schützen.

Das Menü enthält die folgenden Dialoge:

► [DoS-Global](#)

4.4.1 DoS-Global

In diesem Dialog legen Sie die DoS-Einstellungen für die Protokolle TCP/UDP, IP und ICMP fest.

■ TCP/UDP

Scanner nutzen Port-Scans, um Angriffe auf das Netz vorzubereiten. Der Scanner verwendet unterschiedliche Techniken, um aktive Geräte und offene Ports zu ermitteln. Dieser Rahmen bietet Ihnen die Möglichkeit, Filter für bestimmte Scan-Techniken zu aktivieren.

Das Gerät unterstützt die Erkennung der folgenden Scan-Typen:

- ▶ Null-Scans
- ▶ Xmas-Scans
- ▶ SYN/FIN-Scans
- ▶ TCP-Offset-Angriffe
- ▶ TCP-SYN-Angriffe
- ▶ L4-Port-Angriffe
- ▶ Minimal-Header-Scans

Parameter	Bedeutung
Null-Scan-Filter	Aktiviert/deaktiviert den Null-Scan-Filter. Der Null-Scan-Filter erkennt eingehende Datenpakete ohne gesetzte TCP-Flags und verwirft diese. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Der Filter ist aktiv.▶ unmarkiert (Voreinstellung) Der Filter ist inaktiv.
Xmas-Filter	Aktiviert/deaktiviert den Xmas-Filter. Der Xmas-Filter erkennt eingehende Datenpakete mit gleichzeitig gesetzten TCP-Flags FIN, URG und PUSH und verwirft diese. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Der Filter ist aktiv.▶ unmarkiert (Voreinstellung) Der Filter ist inaktiv.
SYN/FIN-Filter	Aktiviert/deaktiviert den SYN/FIN-Filter. Der SYN/FIN-Filter erkennt eingehende Datenpakete mit gleichzeitig gesetzten TCP-Flags SYN und FIN und verwirft diese. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Der Filter ist aktiv.▶ unmarkiert (Voreinstellung) Der Filter ist inaktiv.
TCP-Offset-Protection	Aktiviert/deaktiviert den TCP-Offset-Schutz. Der TCP-Offset-Schutz erkennt eingehende TCP-Datenpakete, deren Fragment-Offset-Feld des IP-Headers gleich 1 ist und verwirft diese. Der TCP-Offset-Schutz akzeptiert UDP- und ICMP-Pakete mit Fragment-Offset-Feld des IP-Headers gleich 1. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Der Schutz ist aktiv.▶ unmarkiert (Voreinstellung) Der Schutz ist inaktiv.

Parameter	Bedeutung
TCP-SYN-Protection	<p>Aktiviert/deaktiviert den TCP-SYN-Schutz. Der TCP-SYN-Schutz erkennt eingehende Datenpakete mit gesetztem TCP-Flag SYN und L4-Quell-Port < 1024 und verwirft diese.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Der Schutz ist aktiv. ▶ unmarkiert (Voreinstellung) Der Schutz ist inaktiv.
L4-Port-Protection	<p>Aktiviert/deaktiviert den L4-Port-Schutz. Der L4-Port-Schutz erkennt eingehende TCP- und UDP-Datenpakete, bei denen Quell-Port-Nummer und Ziel-Port-Nummer identisch sind, und verwirft diese.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Der Schutz ist aktiv. ▶ unmarkiert (Voreinstellung) Der Schutz ist inaktiv.
Min.-Header-Size-Filter	<p>Aktiviert/deaktiviert den Minimal-Header-Filter. Der Minimal-Header-Filter vergleicht den TCP-Header von eingehenden Datenpaketen. Wenn der mit 4 multiplizierte Daten-Offset-Wert kleiner ist als die minimale TCP-Header-Größe, dann verwirft der Filter die Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Der Filter ist aktiv. ▶ unmarkiert (Voreinstellung) Der Filter ist inaktiv.
Min. TCP header size	Zeigt die minimale Größe eines gültigen TCP-Headers.

■ IP

Dieser Rahmen bietet Ihnen die Möglichkeit, den Land-Attack-Filter zu aktivieren und zu deaktivieren. Bei der Land-Attack-Methode sendet die angreifende Station Datenpakete, deren Quell- und Ziel-Adresse identisch mit denen des Empfängers ist. Wenn Sie diesen Filter aktivieren, erkennt das Gerät Datenpakete mit identischer Quell- und Ziel-Adresse und verwirft diese.

Parameter	Bedeutung
Land-Attack-Filter	<p>Aktiviert/deaktiviert den Land-Attack-Filter. Der Land-Attack-Filter erkennt eingehende IP-Datenpakete, deren Quell- und Ziel-IP-Adresse identisch ist, und verwirft diese.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Der Filter ist aktiv. ▶ unmarkiert (Voreinstellung) Der Filter ist inaktiv.

■ ICMP

Dieser Dialog bietet Ihnen Filtermöglichkeiten für folgende ICMP-Parameter:

- ▶ Fragmentierte Datenpakete
- ▶ ICMP-Pakete ab einer bestimmten Größe

Parameter	Bedeutung
Fragmentierte Pakete filtern	Aktiviert/deaktiviert den Filter für fragmentierte ICMP-Pakete. Der Filter erkennt fragmentierte ICMP-Pakete und verwirft diese. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Der Filter ist aktiv.▶ unmarkiert (Voreinstellung) Der Filter ist inaktiv.
Anhand Paketgröße verwerfen	Aktiviert/deaktiviert den Filter für eingehende ICMP-Pakete. Der Filter erkennt ICMP-Pakete, deren Größe die im Feld <i>Erlaubte Paketgröße [Byte]</i> festgelegte Paketgröße überschreitet und verwirft diese. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Der Filter ist aktiv.▶ unmarkiert (Voreinstellung) Der Filter ist inaktiv.
Erlaubte Paketgröße [Byte]	Legt die maximal erlaubte Payload-Größe von ICMP-Paketen in Byte fest. Markieren Sie das Kontrollkästchen <i>Anhand Paketgröße verwerfen</i> , wenn das Gerät eingehende Datenpakete verwerfen soll, deren Größe die maximal erlaubte Größe von ICMP-Paketen überschreitet. Mögliche Werte: <ul style="list-style-type: none">▶ 0..1472 (Voreinstellung: 512)

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5 Switching

Das Menü enthält die folgenden Dialoge:

- ▶ Switching Global
- ▶ Lastbegrenzer
- ▶ Filter für MAC-Adressen
- ▶ IGMP-Snooping
- ▶ MRP-IEEE
- ▶ QoS/Priorität
- ▶ VLAN
- ▶ L2-Redundanz

5.1 Switching Global

Dieser Dialog bietet Ihnen die Möglichkeit, folgende Einstellungen festzulegen:

- ▶ Aging-Time der Adresstabelle ändern
- ▶ Flusskontrolle im Gerät einschalten
- ▶ VLAN-Unaware-Modus einschalten

Treffen in der Warteschlange eines Ports sehr viele Datenpakete gleichzeitig ein, führt dies möglicherweise zum Überlaufen des Port-Speichers. Beispielsweise passiert dies dann, wenn das Gerät Daten an einem Gigabit-Port empfängt und diese an einen Port mit niedrigerer Bandbreite weiterleitet. Das Gerät verwirft überschüssige Datenpakete.

Der in der Norm IEEE 802.3 beschriebene Flusskontrollmechanismus sorgt dafür, dass keine Datenpakete durch Überlaufen eines Portspeichers verloren gehen. Kurz bevor ein Portspeicher vollständig gefüllt ist, signalisiert das Gerät den angeschlossenen Geräten, dass es keine Datenpakete von ihnen mehr annimmt.

- ▶ Im Vollduplex-Betrieb sendet das Gerät ein Pause-Datenpaket.
- ▶ Im Halbduplex-Betrieb simuliert das Gerät eine Kollision.

Die angeschlossenen Geräte senden daraufhin so lange keine Datenpakete mehr, wie die Signalisierung andauert. Auf Uplink-Ports führt dies möglicherweise zu unerwünschten Sendepausen im übergeordneten Netzsegment („Wandering Backpressure“).

Gemäß Norm IEEE 802.1Q leitet das Gerät Datenpakete mit VLAN-Tag in einem VLAN ≥ 1 weiter. Einige wenige Anwendungen auf angeschlossenen Endgeräten allerdings senden oder empfangen Datenpakete mit einer VLAN-ID=0. Wenn das Gerät ein solches Datenpaket empfängt, überschreibt es vor dem Weiterleiten den ursprünglichen Wert im Datenpaket mit der VLAN-ID des empfangenden Ports. Wenn Sie den VLAN-Unaware-Modus aktivieren, setzen Sie damit die VLAN-Einstellungen im Gerät außer Kraft. Das Gerät leitet dann die Datenpakete transparent weiter und wertet ausschließlich die im Datenpaket enthaltene Prioritätsinformation aus.

■ Konfiguration

Parameter	Bedeutung
MAC-Adresse	Zeigt die MAC-Adresse des Geräts.
Aging-Time [s]	Legt die Aging-Zeit in Sekunden fest. Mögliche Werte: ▶ 10..500000 (Voreinstellung: 30) Das Gerät überwacht das Alter der gelernten Unicast-MAC-Adressen. Adresseinträge, die ein bestimmtes Alter (Aging-Zeit) überschreiten, löscht das Gerät aus seiner Adresstabelle. Die Adresstabelle finden Sie im Dialog <i>Switching > Filter für MAC-Adressen</i> .

Parameter	Bedeutung
Flusskontrolle	<p>Aktiviert/deaktiviert die Flusskontrolle im Gerät.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Die Flusskontrolle ist im Gerät aktiviert. Aktivieren Sie die Flusskontrolle zusätzlich auf den erforderlichen Ports. Siehe Dialog <i>Grundeinstellungen > Port</i>, Registerkarte <i>Konfiguration</i>, Kontrollkästchen in Spalte <i>Flusskontrolle</i>.▶ <code>unmarkiert</code> (Voreinstellung) Die Flusskontrolle ist im Gerät deaktiviert. <p>Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Ports. Wenn Flusskontrolle und Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise nicht wie beabsichtigt.</p>
VLAN-Unaware-Modus	<p>Aktiviert/deaktiviert den VLAN-Unaware-Modus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Der VLAN-Unaware-Modus ist aktiv. Das Gerät arbeitet im Bridging-Modus VLAN-unaware (802.1Q):<ul style="list-style-type: none">– Das Gerät ignoriert die VLAN-Einstellungen im Gerät und das VLAN-Tag in den Datenpaketen. Das Gerät überträgt die Datenpakete anhand ihrer Ziel-MAC-Adresse oder Ziel-IP-Adresse im VLAN 1.– Das Gerät ignoriert die in den Dialogen <i>Switching > VLAN > Konfiguration</i> und <i>Switching > VLAN > Port</i> festgelegten VLAN-Einstellungen. Jeder Port ist VLAN 1 zugewiesen.– Das Gerät wertet die im Datenpaket enthaltene Prioritätsinformation aus.▶ <code>unmarkiert</code> (Voreinstellung) Der VLAN-Unaware-Modus ist inaktiv. Das Gerät arbeitet im Bridging-Modus VLAN-aware (802.1Q):<ul style="list-style-type: none">– Das Gerät wertet das VLAN-Tag in den Datenpaketen aus.– Das Gerät überträgt die Datenpakete anhand ihrer Ziel-MAC-Adresse oder Ziel-IP-Adresse im jeweiligen VLAN.– Das Gerät wertet die im Datenpaket enthaltene Prioritätsinformation aus. <p>Anmerkung: Legen Sie für jede Funktion im Gerät, die VLAN-Einstellungen nutzt, die VLAN-ID 1 fest. Dies betrifft unter anderem statische Filter, MRP und IGMP-Snooping.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.2 Lastbegrenzer

Das Gerät bietet Ihnen die Möglichkeit, den Verkehr an den Ports zu begrenzen, um auch bei hohem Verkehrsaufkommen einen zuverlässigen Betrieb zu gewährleisten. Überschreitet der Verkehr an einem Port den eingegebenen Grenzwert, dann verwirft das Gerät die Überlast an diesem Port.

Die Lastbegrenzerfunktion arbeitet ausschließlich auf Schicht 2 und dient dem Zweck, Stürme von Datenpaketen, die das Gerät flutet, in ihrer Auswirkung zu begrenzen (typischerweise Broadcasts).

Die Lastbegrenzerfunktion ignoriert die Protokollinformationen höherer Schichten wie IP oder TCP.

In diesem Dialog schalten Sie die *Lastbegrenzer*-Funktion ein. Der Grenzwert legt fest, welchen maximalen Verkehr der Port eingangsseitig vermittelt. Überschreitet der Verkehr auf dem Port den Grenzwert, verwirft das Gerät die Überlast auf diesem Port.

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Grenzwert	<p>Legt den Grenzwert fest für Broadcast-, Multicast- und Unicast-Verkehr an diesem Port:</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 0 (Voreinstellung) Die <i>Lastbegrenzer</i>-Funktion ist auf diesem Port deaktiviert.▶ 1..24414 bei 100 MBit/s 1..244140 bei 1000 MBit/s<ul style="list-style-type: none"><input type="checkbox"/> Wenn in Spalte <i>Grenzwert Einheit</i> der Wert <i>Prozent</i> festgelegt ist, legen Sie einen prozentualen Wert zwischen 1 und 100 fest.<input type="checkbox"/> Wenn in Spalte <i>Grenzwert Einheit</i> der Wert <i>pps</i> festgelegt ist, legen Sie einen absoluten Wert fest. Die Lastbegrenzerfunktion berechnet den Grenzwert auf Grundlage von 512 Byte großen Datenpaketen. <p>Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi sind abhängig von der Ausstattung des Geräts.</p>
Grenzwert Einheit	<p>Legt die Einheit für den Grenzwert fest:</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>Prozent</i> (Voreinstellung) Der Grenzwert ist festgelegt in Prozent der Datenrate des Ports.▶ <i>pps</i> Der Grenzwert ist festgelegt in Datenpaketen pro Sekunde.
Broadcast-Modus	<p>Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Broadcast-Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i>▶ <i>unmarkiert</i> (Voreinstellung) <p>Bei Überschreiten des Grenzwerts verwirft das Gerät an diesem Port die Überlast an Broadcast-Datenpaketen.</p>
Multicast-Modus	<p>Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Multicast-Datenpakete.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i>▶ <i>unmarkiert</i> (Voreinstellung) <p>Bei Überschreiten des Grenzwerts verwirft das Gerät an diesem Port die Überlast an Multicast-Datenpaketen.</p>

Parameter	Bedeutung
Unknown unicast mode	Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Unicast-Datenpakete mit unbekannter Zieladresse. Mögliche Werte: ▶ markiert ▶ unmarkiert (Voreinstellung) Bei Überschreiten des Grenzwerts verwirft das Gerät an diesem Port die Überlast an Unicast-Datenpaketen.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.3 Filter für MAC-Adressen

Dieser Dialog bietet Ihnen die Möglichkeit, Adressfilter für die Adresstabelle anzuzeigen und zu bearbeiten. Adressfilter legen die Vermittlungsweise der Datenpakete im Gerät anhand der Ziel-MAC-Adresse fest.

Jede Zeile in der Tabelle stellt einen Filter dar. Das Gerät richtet die Filter automatisch ein. Das Gerät bietet Ihnen die Möglichkeit, von Hand weitere Filter einzurichten.

Das Gerät vermittelt die Datenpakete wie folgt:

- ▶ Enthält die Tabelle einen Eintrag für die Zieladresse eines Datenpakets, vermittelt das Gerät das Datenpaket vom Empfangsport an die im Tabelleneintrag angegebenen Ports.
- ▶ Existiert kein Tabelleneintrag für die Zieladresse, vermittelt das Gerät das Datenpaket vom Empfangsport an jeden anderen Port.



■ Tabelle

Parameter	Bedeutung
Adresse	Zeigt die Ziel-MAC-Adresse, für die der Tabelleneintrag gilt.
VLAN-ID	Zeigt die ID des VLANs, für das der Tabelleneintrag gilt. Das Gerät lernt die MAC-Adressen für jedes VLAN separat (Independent VLAN Learning).
Status	Zeigt, auf welche Weise das Gerät den Adressfilter eingerichtet hat. Mögliche Werte: <ul style="list-style-type: none">▶ <code>learned</code> Adressfilter automatisch durch das Gerät eingerichtet anhand empfangener Datenpakete.▶ <code>permanent</code> Adressfilter manuell eingerichtet. Der Adressfilter bleibt dauerhaft eingerichtet.▶ <code>IGMP</code> Adressfilter automatisch eingerichtet durch IGMP-Snooping.▶ <code>mgmt</code> MAC-Adresse des Geräts. Der Adressfilter ist gegen Veränderungen geschützt.▶ <code>invalid</code> Löscht einen manuell eingerichteten Adressfilter.▶ <code>MRP-MMRP-MRP</code> Multicast-Adressfilter automatisch eingerichtet durch MMRP.
<Port-Nummer>	Zeigt, wie der betreffende Port Datenpakete vermittelt, die an nebenstehende Zieladresse adressiert sind. Mögliche Werte: <ul style="list-style-type: none">▶ <code>-</code> Der Port vermittelt keine Datenpakete an die Zieladresse.▶ <code>learned</code> Der Port vermittelt Datenpakete an die Zieladresse. Das Gerät hat den Filter anhand empfangener Datenpakete automatisch eingerichtet.▶ <code>IGMP learned</code> Der Port vermittelt Datenpakete an die Zieladresse. Das Gerät hat den Filter anhand von IGMP automatisch eingerichtet.▶ <code>unicast static</code> Der Port vermittelt Datenpakete an die Zieladresse. Ein Benutzer hat den Filter erzeugt.▶ <code>multicast static</code> Der Port vermittelt Datenpakete an die Zieladresse. Ein Benutzer hat den Filter erzeugt.

Um die gelernten MAC-Adressen aus der Adresstabelle zu entfernen, klicken Sie im Dialog *Grundeinstellungen* > *Neustart* die Schaltfläche *MAC-Adresstabelle zurücksetzen*.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	<p>Öffnet das Fenster <i>Erzeugen</i>, um der Tabelle einen neuen Eintrag hinzuzufügen.</p> <ul style="list-style-type: none"> ▶ Im Feld <i>Adresse</i> legen Sie die Ziel-MAC-Adresse fest. ▶ Im Feld <i>VLAN-ID</i> legen Sie die ID des VLANs fest. ▶ Im Feld <i>Port</i> legen Sie den Port fest. <ul style="list-style-type: none"> – Wählen Sie einen Port aus, wenn die Ziel-MAC-Adresse eine Unicast-Adresse ist. – Wählen Sie einen oder mehrere Ports aus, wenn die Ziel-MAC-Adresse eine Multicast-Adresse ist. – Wählen Sie keinen Port aus, um einen Discard-Filter einzurichten. Das Gerät verwirft Datenpakete mit der im Tabelleneintrag angegebenen Ziel-MAC-Adresse.
	Zeigt ein Untermenü mit folgenden Einträgen.
MAC-Adresstabelle zurücksetzen	Entfernt aus der Forwarding-Tabelle (FDB) die MAC-Adressen, die in Spalte <i>Status</i> den Wert <i>learned</i> haben.

5.4 IGMP-Snooping

Das Internet Group Management Protocol (IGMP) ist ein Protokoll für das dynamische Verwalten von Multicast-Gruppen. Das Protokoll beschreibt das Vermitteln von Multicast-Datenpaketen zwischen Routern und Endgeräten auf Schicht 3.

Das Gerät bietet Ihnen die Möglichkeit, mit der IGMP-Snooping-Funktion die IGMP-Mechanismen auch auf Schicht 2 zu nutzen:

- ▶ Ohne IGMP-Snooping vermittelt das Gerät die Multicast-Datenpakete an jeden Port.
 - ▶ Mit aktivierter IGMP-Snooping-Funktion vermittelt das Gerät die Multicast-Datenpakete ausschließlich an Ports, an denen Multicast-Empfänger angeschlossen sind. Dies reduziert die Netzlast. Das Gerät wertet die auf Schicht 3 übertragenen IGMP-Datenpakete aus und wendet die Informationen auf Schicht 2 an.
- Aktivieren Sie die IGMP-Snooping-Funktion erst, wenn folgende Voraussetzungen erfüllt sind:
- Im Netz ist ein Multicast-Router vorhanden, der IGMP-Queries (periodische Anfragen) erzeugt.
 - Die am IGMP-Snooping beteiligten Geräte im Netz leiten die IGMP-Queries weiter.

Das Gerät verknüpft die IGMP-Reports mit den Einträgen in seiner Adresstabelle. Tritt ein Multicast-Empfänger einer Multicast-Gruppe bei (report), erzeugt das Gerät für diesen Port einen Tabelleneintrag im Dialog *Switching > Filter für MAC-Adressen*. Verlässt der Multicast-Empfänger die Multicast-Gruppe (leave), entfernt das Gerät den Tabelleneintrag wieder.

Das Menü enthält die folgenden Dialoge:

- ▶ [IGMP-Snooping Global](#)
- ▶ [IGMP-Snooping Konfiguration](#)
- ▶ [IGMP-Snooping Erweiterungen](#)
- ▶ [IGMP Snooping-Querier](#)
- ▶ [IGMP Snooping Multicasts](#)

5.4.1 IGMP-Snooping Global

Dieser Dialog bietet Ihnen die Möglichkeit, das *IGMP-Snooping*-Protokoll im Gerät einzuschalten sowie pro Port und pro VLAN zu konfigurieren.

■ Funktion


Parameter	Bedeutung
Funktion	Schaltet die <i>IGMP-Snooping</i> -Funktion im Gerät ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ An Die <i>IGMP-Snooping</i>-Funktion ist im Gerät eingeschaltet gemäß RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) und Multicast Listener Discovery (MLD) Snooping Switches). ▶ Aus (Voreinstellung) Die <i>IGMP-Snooping</i>-Funktion ist im Gerät ausgeschaltet. Das Gerät vermittelt empfangene Query-, Report- und Leave-Datenpakete, ohne sie auszuwerten. Empfangene Datenpakete mit Multicast-Zieladresse vermittelt das Gerät an jeden Port.

■ Information

Parameter	Bedeutung
Verarbeitete Multicast-Control-Pakete	Zeigt die Anzahl der verarbeiteten Multicast-Kontroll-Datenpakete. Diese Statistik umfasst folgende Paketarten: <ul style="list-style-type: none"> – IGMP-Reports – IGMP-Queries Version V1 – IGMP-Queries Version V2 – IGMP-Queries Version V3 – IGMP-Queries mit falscher Version – PIM- oder DVMRP-Pakete Das Gerät verwendet die Multicast-Kontroll-Datenpakete für die Erstellung der Adresstabelle zur Vermittlung der Multicast-Datenpakete. Mögliche Werte: <ul style="list-style-type: none"> ▶ $0..2^{31}-1$ Mit der Schaltfläche <i>IGMP-Snooping-Daten zurücksetzen</i> im Dialog <i>Grundeinstellungen</i> > Neustart oder mit dem CLI-Kommando <code>clear igmp-snooping</code> setzen Sie die IGMP-Snooping-Einträge zurück, inklusive des Zählers für die verarbeiteten Multicast-Kontroll-Datenpakete.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
IGMP-Snooping-Zähler zurücksetzen	Entfernt die IGMP-Snooping-Einträge und setzt den Zähler im Rahmen <i>Information</i> auf 0.

5.4.2 IGMP-Snooping Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, die *IGMP-Snooping*-Funktion im Gerät einzuschalten sowie pro Port und pro VLAN zu konfigurieren.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [VLAN-ID]
- ▶ [Port]

[VLAN-ID]

In dieser Registerkarte konfigurieren Sie die *IGMP-Snooping*-Funktion für jedes VLAN.

■ Tabelle

Parameter	Bedeutung
VLAN-ID	Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.
Aktiv	<p>Aktiviert/deaktiviert die <i>IGMP-Snooping</i>-Funktion für dieses VLAN. Voraussetzung ist, dass die <i>IGMP-Snooping</i>-Funktion global aktiviert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> IGMP-Snooping ist für dieses VLAN aktiviert. Das VLAN ist am Multicast-Datenstrom angemeldet. ▶ <code>unmarkiert</code> (Voreinstellung) IGMP-Snooping ist für dieses VLAN deaktiviert. Das VLAN ist vom Multicast-Datenstrom abgemeldet.
Group-Membership-Intervall	<p>Legt die Zeit in Sekunden fest, in der ein VLAN aus einer dynamischen Multicast-Gruppe in der Adresstabelle eingetragen bleibt, wenn das Gerät keine Report-Datenpakete mehr von dem VLAN empfängt. Legen Sie den Wert größer fest als den Wert in Spalte <i>Max. Antwortzeit</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>2..3600</code> (Voreinstellung: 260)
Max. Antwortzeit	<p>Legt die Zeit in Sekunden fest, in der die Mitglieder einer Multicast-Gruppe auf ein Query-Datenpaket antworten sollen. Die Mitglieder wählen für ihre Antwort einen zufälligen Zeitpunkt innerhalb der Antwortzeit (Response Time) aus. Damit helfen Sie, zu verhindern, dass die Multicast-Gruppen-Mitglieder gleichzeitig auf den Query antworten. Legen Sie den Wert kleiner fest als den Wert in Spalte <i>Group-Membership-Intervall</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>1..25</code> (Voreinstellung: 10)
Fast-Leave-Admin-Modus	<p>Aktiviert/deaktiviert die Fast-Leave-Funktion für dieses VLAN.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Erhält das Gerät eine IGMP-Leave-Nachricht aus einer Multicast-Gruppe, entfernt es bei eingeschalteter Fast-Leave-Funktion sofort den Eintrag aus seiner Adresstabelle. ▶ <code>unmarkiert</code> (Voreinstellung) Bei ausgeschalteter Fast-Leave-Funktion sendet das Gerät zuerst MAC-basierte Queries an die Mitglieder der Multicast-Gruppe und entfernt einen Eintrag erst dann, wenn ein VLAN keine Report-Nachrichten mehr sendet.
MRP-Ablaufzeit	<p>Multicast-Router-Present-Ablaufzeit. Legt die Zeit in Sekunden fest, in der das Gerät auf einen Query an diesem Port, der einem VLAN angehört, wartet. Empfängt der Port kein Query-Datenpaket, entfernt das Gerät den Port aus der Liste der Ports mit angeschlossenen Multicast-Routern. Den Parameter können Sie ausschließlich dann konfigurieren, wenn der Port einem bestehenden VLAN angehört.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>0</code> unbegrenztes Time-Out, keine Ablaufzeit ▶ <code>1..3600</code> (Voreinstellung: 260)

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Port]

In dieser Registerkarte konfigurieren Sie die *IGMP-Snooping*-Funktion für jeden Port.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Aktiv	<p>Aktiviert/deaktiviert die <i>IGMP-Snooping</i>-Funktion für diesen Port. Voraussetzung ist, dass die <i>IGMP-Snooping</i>-Funktion global aktiviert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> IGMP-Snooping ist auf diesem Port eingeschaltet. Der Port ist am Multicast-Datenstrom angemeldet.▶ <code>unmarkiert</code> (Voreinstellung) IGMP-Snooping ist auf diesem Port ausgeschaltet. Der Port ist vom Multicast-Datenstrom abgemeldet.
Group-Membership-Intervall	<p>Legt die Zeit in Sekunden fest, in der ein Port aus einer dynamischen Multicast-Gruppe in der Adresstabelle eingetragen bleibt, wenn das Gerät keine Report-Datenpakete mehr von dem Port empfängt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>2..3600</code> (Voreinstellung: 260) <p>Wählen Sie den Wert im größer als den Wert in Spalte <i>Max. Antwortzeit</i>.</p>
Max. Antwortzeit	<p>Legt die Zeit in Sekunden fest, in der die Mitglieder einer Multicast-Gruppe auf ein Query-Datenpaket antworten sollen. Die Mitglieder wählen für ihre Antwort einen zufälligen Zeitpunkt innerhalb der Antwortzeit (Response Time) aus. Damit helfen Sie, zu verhindern, dass die Multicast-Gruppen-Mitglieder gleichzeitig auf den Query antworten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>1..25</code> (Voreinstellung: 10) <p>Wählen Sie den Wert kleiner als den Wert in Spalte <i>Group-Membership-Intervall</i>.</p>
MRP-Ablaufzeit	<p>Legt die Multicast-Router-Present-Ablaufzeit fest. Die MRP-Ablaufzeit ist die Zeit in Sekunden, in der das Gerät auf ein Query-Datenpaket an diesem Port wartet. Empfängt der Port kein Query-Datenpaket, entfernt das Gerät den Port aus der Liste der Ports mit angeschlossenen Multicast-Routern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>0</code> unbegrenzt Time-Out, keine Ablaufzeit▶ <code>1..3600</code> (Voreinstellung: 260)
Fast-Leave-Admin-Modus	<p>Aktiviert/deaktiviert die Fast-Leave-Funktion für diesen Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Erhält das Gerät eine IGMP-Leave-Nachricht aus einer Multicast-Gruppe, entfernt es bei eingeschalteter Fast-Leave-Funktion sofort den Eintrag aus seiner Adresstabelle.▶ <code>unmarkiert</code> (Voreinstellung) Bei ausgeschalteter Fast-Leave-Funktion sendet das Gerät zuerst MAC-basierte Queries an die Mitglieder der Multicast-Gruppe und entfernt einen Eintrag erst dann, wenn ein Port keine Report-Nachrichten mehr sendet.
Static-Query-Port	<p>Aktiviert/deaktiviert den <i>Static-Query-Port</i>-Modus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Der <i>Static-Query-Port</i>-Modus ist aktiv. Der Port ist ein statischer Query-Port in den eingerichteten VLANs.▶ <code>unmarkiert</code> (Voreinstellung) Der <i>Static-Query-Port</i>-Modus ist inaktiv. Der Port ist kein statischer Query-Port. Das Gerät vermittelt IGMP-Report-Nachrichten ausschließlich dann an den Port, wenn es IGMP-Queries empfängt.

Parameter	Bedeutung
VLAN-IDs	Zeigt die ID der VLANs, für die der Tabelleneintrag gilt.

■ **Schaltflächen**

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.4.3 IGMP-Snooping Erweiterungen

Dieser Dialog bietet Ihnen die Möglichkeit, für eine VLAN-ID einen Port auszuwählen und den Port zu konfigurieren.


■ Tabelle

Parameter	Bedeutung
VLAN-ID	Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.
<Port-Nummer>	<p>Zeigt für jedes im Gerät eingerichtete VLAN, ob der betreffende Port ein Query-Port ist. Außerdem zeigt das Feld, ob das Gerät jeden Multicast-Stream im VLAN an diesen Port vermittelt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ - Der Port ist in diesem VLAN kein Query-Port.▶ L = Learned Das Gerät hat den Port als Query-Port erkannt, weil der Port IGMP-Queries in diesem VLAN empfangen hat. Der Port ist kein statisch konfigurierter Query-Port.▶ A = Automatic Das Gerät hat den Port als Query-Port erkannt. Voraussetzung ist, dass der Port als <i>Learn by LLDP</i> konfiguriert ist.▶ S = Static (einstellbar) Ein Benutzer hat den Port als statischen Query-Port konfiguriert. Das Gerät vermittelt IGMP-Reports ausschließlich an Ports, an denen es zuvor IGMP-Queries empfangen hat – und an statisch konfigurierte Query-Ports. Um diesen Wert zuzuweisen, gehen Sie wie folgt vor:<ul style="list-style-type: none"><input type="checkbox"/> Öffnet das <i>Wizard</i>-Fenster.<input type="checkbox"/> Markieren Sie auf der Seite <i>Konfiguration</i> das Kontrollkästchen <i>Static</i>.▶ P = Learn by LLDP (einstellbar) Ein Benutzer hat den Port als <i>Learn by LLDP</i> konfiguriert. Mit dem Link Layer Discovery Protocol (LLDP) erkennt das Gerät direkt an den Port angeschlossene Hirschmann-Geräte. Erkannte Query-Ports kennzeichnet das Gerät mit A. Um diesen Wert zuzuweisen, gehen Sie wie folgt vor:<ul style="list-style-type: none"><input type="checkbox"/> Öffnet das <i>Wizard</i>-Fenster.<input type="checkbox"/> Markieren Sie auf der Seite <i>Konfiguration</i> das Kontrollkästchen <i>Learn by LLDP</i>.▶ F = Forward All (einstellbar) Ein Benutzer hat den Port so konfiguriert, dass das Gerät sämtliche empfangene Multicast-Streams in diesem VLAN an diesen Port vermittelt. Diese Einstellung ist zum Beispiel für Diagnosezwecke geeignet. Um diesen Wert zuzuweisen, gehen Sie wie folgt vor:<ul style="list-style-type: none"><input type="checkbox"/> Öffnet das <i>Wizard</i>-Fenster.<input type="checkbox"/> Markieren Sie auf der Seite <i>Konfiguration</i> das Kontrollkästchen <i>Forward all</i>.

Parameter	Bedeutung
Display categories	<p>Erhöht die Übersichtlichkeit der Anzeige. Die Tabelle hebt Zellen hervor, die den ausgewählten Wert enthalten. Dies erleichtert das bedarfsgerechte Analysieren und Sortieren der Tabelle.</p> <ul style="list-style-type: none"> ▶ Learned (L) Die Tabelle zeigt Zellen, die den Wert L und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als L enthalten, zeigt die Tabelle mit dem Zeichen “-“. ▶ Static (S) Die Tabelle zeigt Zellen, die den Wert S und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als S enthalten, zeigt die Tabelle mit dem Zeichen “-“. ▶ Automatic (A) Die Tabelle zeigt Zellen, die den Wert A und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als A enthalten, zeigt die Tabelle mit dem Zeichen “-“. ▶ Learn by LLDP Die Tabelle zeigt Zellen, die den Wert P und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als P enthalten, zeigt die Tabelle mit dem Zeichen “-“. ▶ Forward all (F) Die Tabelle zeigt Zellen, die den Wert F und gegebenenfalls weitere mögliche Werte enthalten. Zellen, die ausschließlich andere Werte als F enthalten, zeigt die Tabelle mit dem Zeichen “-“.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Öffnet das <i>Wizard</i> -Fenster, das Ihnen beim Auswählen und Einstellen der Ports hilft.

[Wizard : Selection VLAN/Port]

Nach Schließen des *Wizard*-Fensters klicken Sie die Schaltfläche , um Ihre Einstellungen zu speichern.

■ Selection VLAN/Port

Auf dieser Seite weisen Sie einem Port eine VLAN-ID zu.

Parameter	Bedeutung
VLAN-ID	Auswahl der ID des VLANs. Mögliche Werte: ▶ 1..4042
Port	Auswahl des Ports. Mögliche Werte: ▶ <Port-Nummer>

■ Konfiguration

Auf dieser Seite legen Sie die Einstellungen des Ports fest.

Parameter	Bedeutung
VLAN-ID	Zeigt die ID des ausgewählten VLANs.
Port	Zeigt die Nummer des ausgewählten Ports.
Static	Legt den Port als statischen Query-Port in den eingerichteten VLANs fest. Das Gerät überträgt IGMP-Benachrichtigungen ausschließlich an die Ports, an denen es IGMP-Queries empfängt. Bietet Ihnen die Möglichkeit, IGMP-Benachrichtigungen auch an andere ausgewählte Ports oder angeschlossene Hirschmann Geräte (<i>Automatic</i>) zu senden.
Learn by LLDP	Legt den Status <i>Learn by LLDP</i> für den Port fest. Ermöglicht es, direkt verbundene Hirschmann-Geräte per LLDP zu erkennen und als Query-Ports zu lernen.
Forward all	Legt den Status <i>Forward all</i> für den Port fest. Mit der Einstellung <i>Forward all</i> sendet das Gerät auf diesem Port jedes Datenpaket mit einer Multicast-Adresse im Zieladressfeld.

5.4.4 IGMP Snooping-Querier

Das Gerät bietet Ihnen die Möglichkeit, einen Multicast-Stream ausschließlich an die Ports zu vermitteln, an denen ein Multicast-Empfänger angeschlossen ist.

Um zu ermitteln, an welchen Ports Multicast-Empfänger angeschlossen sind, sendet das Gerät in einem einstellbaren Intervall Query-Datenpakete an die Ports. Ist ein Multicast-Empfänger angeschlossen, meldet er sich für den Multicast-Stream an, indem er dem Gerät mit einem Report-Datenpaket antwortet.

Dieser Dialog bietet Ihnen die Möglichkeit, die Snooping-Querier-Einstellungen global und für die eingerichteten VLANs zu konfigurieren.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die IGMP-Querier-Funktion im Gerät global ein/aus. Mögliche Werte: ▶ An ▶ Aus (Voreinstellung)

■ Konfiguration

In diesem Rahmen legen Sie die IGMP-Snooping-Querier-Einstellungen für die General-Query-Datenpakete fest.

Parameter	Bedeutung
Protokoll-Version	Legt die IGMP-Version der General-Query-Datenpakete fest. Mögliche Werte: ▶ 1 IGMP v1 ▶ 2 (Voreinstellung) IGMP v2 ▶ 3 IGMP v3
Query-Intervall [s]	Legt die Zeitspanne in Sekunden fest, nach der das Gerät selbst General-Query-Datenpakete generiert, wenn es Query-Datenpakete vom Multicast-Router empfangen hat. Mögliche Werte: ▶ 1..1800 (Voreinstellung: 60)
Ablauf-Intervall [s]	Legt die Zeitspanne in Sekunden fest, nach der ein aktiver Querier aus dem Passivzustand wieder in den Aktivzustand wechselt, wenn er länger als hier festgelegt keine Query-Pakete empfängt. Mögliche Werte: ▶ 60..300 (Voreinstellung: 125)

■ Tabelle

In der Tabelle legen Sie die Snooping-Querier-Einstellungen für die eingerichteten VLANs fest.

Parameter	Bedeutung
VLAN-ID	Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

Parameter	Bedeutung
Aktiv	Aktiviert/deaktiviert die IGMP-Snooping-Querier-Funktion für dieses VLAN. Mögliche Werte: ▶ <code>markiert</code> Die IGMP-Snooping-Querier-Funktion ist für dieses VLAN aktiv. ▶ <code>unmarkiert</code> (Voreinstellung) Die IGMP-Snooping-Querier-Funktion ist für dieses VLAN deaktiviert.
Momentaner Zustand	Zeigt, ob der Snooping-Querier in diesem VLAN aktiv ist. Mögliche Werte: ▶ <code>markiert</code> Der Snooping-Querier ist in diesem VLAN aktiv. ▶ <code>unmarkiert</code> Der Snooping-Querier ist in diesem VLAN inaktiv.
Adresse	Legt die IP-Adresse fest, die das Gerät als Absenderadresse in generierte Datenpakete mit allgemeinen Abfragen einfügt. Verwenden Sie die Adresse des Multicast-Routers. Mögliche Werte: ▶ Gültige IPv4-Adresse (Voreinstellung: <code>0.0.0.0</code>)
Protokoll-Version	Zeigt die IGMP-Protokoll-Version der General-Query-Datenpakete. Mögliche Werte: ▶ <code>1</code> IGMP v1 ▶ <code>2</code> IGMP v2 ▶ <code>3</code> IGMP v3
Max. Antwortzeit	Zeigt die Zeit in Sekunden, in der die Mitglieder einer Multicast-Gruppe auf ein Query-Datenpaket antworten sollen. Die Mitglieder wählen für ihre Antwort einen zufälligen Zeitpunkt innerhalb der Antwortzeit (Response Time) aus. Dies hilft, zu verhindern, dass jedes Multicast-Gruppen-Mitglied gleichzeitig auf den Query antwortet.
Letzte Querier-Adresse	Zeigt die IP-Adresse des Multicast-Routers, von dem die letzte eingegangene IGMP-Abfrage (Querier) ausging.
Letzte Querier-Version	Zeigt die IGMP-Version, die der Multicast-Router beim Aussenden der letzten in diesem VLAN eingegangenen IGMP-Abfrage (Querier) verwendete.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.4.5 IGMP Snooping Multicasts

Das Gerät bietet Ihnen die Möglichkeit, festzulegen, wie es Datenpakete unbekannter Multicast-Adressen vermittelt: Entweder verwirft das Gerät diese Datenpakete, flutet sie an jeden Port oder vermittelt sie ausschließlich an die Ports, die zuvor Query-Pakete empfangen haben.

Außerdem bietet Ihnen das Gerät die Möglichkeit, die Datenpakete bekannter Multicast-Adressen an die Query-Ports zu vermitteln.

■ Konfiguration

Parameter	Bedeutung
Unbekannte Multicasts	Legt fest, wie das Gerät die Datenpakete unbekannter Multicast-Adressen vermittelt. Mögliche Werte: <ul style="list-style-type: none">▶ Verwerfen Das Gerät verwirft Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse.▶ An alle Ports senden (Voreinstellung) Das Gerät sendet Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an die Ports.▶ An Query-Ports senden Das Gerät sendet Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an die Query-Ports.

■ Tabelle

In der Tabelle legen Sie die Einstellungen für bekannte Multicasts für die eingerichteten VLANs fest.

Parameter	Bedeutung
VLAN-ID	Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.
Bekannte Multicasts	Legt fest, wie das Gerät die Datenpakete bekannter Multicast-Adressen vermittelt. Mögliche Werte: <ul style="list-style-type: none">▶ an Query- und registrierte Ports senden Das Gerät sendet Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an die Query-Ports und an registrierte Ports.▶ an registrierte Ports senden (Voreinstellung) Das Gerät sendet Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an registrierte Ports.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.5 MRP-IEEE

Die Erweiterung IEEE 802.1ak der Norm IEEE 802.1Q führte das Multiple Registration Protocol (MRP) als Ersatz für das Generic Attribute Registration Protocol (GARP) ein. Zudem änderte und ersetzte das IEEE die GARP-Anwendungen, das GARP Multicast Registration Protocol (GMRP) und das GARP VLAN Registration Protocol (GVRP). Das Multiple MAC Registration Protocol (MMRP) und das Multiple VLAN Registration Protocol (MVRP) ersetzen diese Protokolle.

MRP-IEEE hilft, den Verkehr auf die erforderlichen Bereiche des LANs zu begrenzen. Um den Verkehr zu begrenzen, verteilen die MRP-IEEE-Anwendungen Attribut-Werte an teilnehmende MRP-IEEE-Geräte innerhalb eines LANs, wobei sie Multicast-Gruppen-Mitgliedschaften und VLAN-Kennungen registrieren und deregistrieren.

Die Registrierung von Gruppen-Teilnehmern bietet Ihnen die Möglichkeit, Ressourcen für bestimmte Daten im LAN zu reservieren. Die Festlegung der Ressourcen-Anforderungen reguliert den Grad des Verkehrs und ermöglicht den Geräten, die erforderlichen Ressourcen zu ermitteln und für die dynamische Verwaltung der zugeordneten Ressourcen bereitzustellen.

Das Menü enthält die folgenden Dialoge:

- ▶ [MRP-IEEE Konfiguration](#)
- ▶ [MRP-IEEE Multiple MAC Registration Protocol](#)
- ▶ [MRP-IEEE Multiple VLAN Registration Protocol](#)

5.5.1 MRP-IEEE Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, die verschiedenen MRP-Timer einzurichten. Mit der Aufrechterhaltung einer Beziehung zwischen den verschiedenen Timer-Werten arbeitet das Protokoll effizient bei geringerer Wahrscheinlichkeit von unnötigen Attributrücknahmen und erneuten Registrierungen. Die voreingestellten Timer-Werte erhalten wirksam diese Beziehungen.

Erhalten Sie folgende Beziehungen, wenn Sie die Timer neu konfigurieren:

- ▶ Für eine erneute Registrierung nach einem Leave- oder LeaveAll-Ereignis legen Sie – auch im Fall einer verlorenen Nachricht – den Wert für LeaveTime fest auf: $\geq (2 \times \text{JoinTime}) + 60$.
- ▶ Um das Volumen des nach einem LeaveAll-Ereignis neu hinzukommenden Verkehrs zu minimieren, legen Sie für den LeaveAll-Timer einen Wert fest, der höher ist als der LeaveTime-Wert.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Join-Time [1/100s]	Legt den Join-Timer fest, der den Intervall zwischen den Vermittlungsmöglichkeiten überwacht, die auf die Applicant-State-Machine angewendet werden. Mögliche Werte: ▶ 10..100 (Voreinstellung: 20)
Leave-Time [1/100s]	Legt den Leave-Timer fest, der die Zeitspanne überwacht, in der die Registrar-State-Machine im Leave(LV)-Zustand bleibt, bevor er in den Empty(MT)-Zustand wechselt. Mögliche Werte: ▶ 20..600 (Voreinstellung: 60)
Leave-all-Time [1/100s]	Legt den LeaveAll-Timer fest, der die Frequenz überwacht, mit welcher die LeaveAll-State-Machine LeaveAll-PDUs erzeugt. Mögliche Werte: ▶ 200..6000 (Voreinstellung: 1000)

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.5.2 MRP-IEEE Multiple MAC Registration Protocol

Das Multiple MAC Registration Protocol (MMRP) ermöglicht Endgeräten und MAC-Switches das Registrieren und Deregistrieren von Gruppen-Mitgliedschaften und individuellen MAC-Adressen-Informationen in Switches, die sich im selben LAN befinden. Die Switches im LAN verteilen die Information über Switches, die erweiterte Filter-Dienste unterstützen. MMRP bietet Ihnen die Möglichkeit, mit Hilfe der MAC-Adressen-Informationen den Multicast-Verkehr auf die erforderlichen Bereiche des Schicht-2-Netzes zu begrenzen.

Die Arbeitsweise von MMRP verdeutlicht das Beispiel einer Sicherheitskamera, die von einem Mast aus ein Gebäude überwacht. Die Kamera sendet Multicast-Pakete an ein LAN. Für die Überwachung haben Sie 2 Endgeräte an unterschiedlichen Orten installiert. Sie melden die MAC-Adressen der Kamera und die 2 Endgeräte in derselben Multicast-Gruppe an. Dann legen Sie die MMRP-Einstellungen an den Ports zum Senden der Multicast-Gruppen-Pakete an die 2 Endgeräte fest.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [\[Konfiguration\]](#)
- ▶ [\[Service-Requirement\]](#)
- ▶ [\[Statistiken\]](#)

[Konfiguration]

In dieser Registerkarte wählen Sie aktive MMRP-Port-Teilnehmer und stellen das Gerät so ein, dass es periodische Ereignisse überträgt. Der Dialog bietet Ihnen außerdem die Möglichkeit, das Broadcasting der im VLAN registrierten MAC-Adressen einzuschalten.

Für jeden Port existiert eine Periodic-State-Machine, die regelmäßig periodische Ereignisse an die mit aktiven Ports verbundenen Applicant-State-Machines überträgt. Periodische Ereignisse enthalten Informationen, die über den Status der mit dem aktiven Port verbundenen Geräte informieren.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die globale MMRP-Funktion im Gerät ein/aus. Das Gerät nimmt am Austausch von MMRP-Nachrichten teil. Mögliche Werte: <ul style="list-style-type: none"> ▶ An Das Gerät ist normaler Teilnehmer beim Austausch von MMRP-Nachrichten. ▶ Aus (Voreinstellung) Das Gerät ignoriert MMRP-Nachrichten.

■ Konfiguration

Parameter	Bedeutung
Periodische State-Machine	Schaltet die globale Periodic-State-Machine im Gerät ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ An Bei global eingeschalteter MMRP-<i>Funktion</i> überträgt das Gerät MMRP-Nachrichten im Intervall von 1 Sekunde an die an MMRP teilnehmenden Ports. ▶ Aus (Voreinstellung) Deaktiviert die Periodic-State-Machine im Gerät.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Aktiv	Aktiviert/deaktiviert die Teilnahme des Ports an MMRP. Mögliche Werte: <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Bei global und an diesem Port eingeschaltetem MMRP sendet und empfängt das Gerät MMRP-Nachrichten an diesem Port. ▶ <code>unmarkiert</code> Deaktiviert die Teilnahme des Ports an MMRP.
Eingeschränkte Gruppen-Registrierung	Aktiviert/deaktiviert die Begrenzung der dynamischen Registrierung von MAC-Adressen mittels MMRP an dem Port. Mögliche Werte: <ul style="list-style-type: none"> ▶ <code>markiert</code> Bei eingeschalteter Funktion und vorhandenem statischem MAC-Adressen-Filter im betreffenden VLAN bietet das Gerät die Möglichkeit, die MAC-Adressen-Attribute dynamisch zu registrieren. ▶ <code>unmarkiert</code> (Voreinstellung) Aktiviert/deaktiviert die Begrenzung der dynamischen Registrierung von MAC-Adressen mittels MMRP an dem Port.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

[Service-Requirement]

Diese Registerkarte enthält für jedes aktive VLAN Weiterleitungsparameter die festlegen, für welche Ports die Multicast-Weiterleitung zutrifft. Das Gerät bietet Ihnen die Möglichkeit, VLAN-Ports als `Forward all` oder `Forbidden` statisch einzurichten. Den Wert `Forbidden` für ein MMRP-Service-Requirement legen Sie ausschließlich statisch über die grafische Benutzeroberfläche oder das CLI fest. Ein Port ist ausschließlich als `ForwardAll` oder `Forbidden` eingerichtet.

■ Tabelle

Parameter	Bedeutung
VLAN-ID	Zeigt die ID des VLANs.
<Port-Nummer>	<p>Legt die Verarbeitung der Service-Requirements für den Port fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>FA</code> Legt die Einstellung <code>ForwardAll</code> am Port fest. Das Gerät leitet die an MMRP-registrierte Multicast-MAC-Adressen gerichteten Daten ans VLAN weiter. Das Gerät leitet die Daten an Ports weiter, die MMRP dynamisch eingerichtet hat oder die der Administrator statisch als <code>ForwardAll</code>-Ports eingerichtet hat. ▶ <code>F</code> Legt die Einstellung <code>Forbidden</code> am Port fest. Das Gerät blockiert die dynamischen MMRP-Service-Requirements für <code>ForwardAll</code>. Bei an diesem Port in diesem VLAN blockierten <code>ForwardAll</code>-Anfragen blockiert das Gerät an diesem Port auch Daten, die an MMRP-registrierte Multicast-MAC-Adressen gerichtet sind. Außerdem blockiert das Gerät MMRP-Service-Anfragen, diesen Wert an diesem Port zu ändern. ▶ <code>-</code> (Voreinstellung) Schaltet an diesem Port die Weiterleitungsfunktionen aus. ▶ <code>Learned</code> Zeigt die durch MMRP-Service-Anfragen eingesetzten Werte.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Statistiken]

Geräte in einem LAN tauschen Multiple MAC Registration Protocol Data Units (MMRPDU) aus, um die Geräte-Status an einem aktiven MMRP-Port aufrecht zu erhalten. Diese Registerkarte bietet Ihnen die Möglichkeit, die Statistiken des MMRP-Verkehrs für jeden Port zu überwachen.

■ Information


Parameter	Bedeutung
Gesendete MMRP-PDU	Zeigt die Anzahl der an das Gerät übermittelten MMRPDUs.
Empfangene MMRP-PDU	Zeigt die Anzahl der vom Gerät empfangenen MMRPDUs.
Empfangene Bad-Header-PDU	Zeigt die Anzahl der vom Gerät empfangenen MMRPDUs mit fehlerhaftem Header.
Empfangene Bad-Format-PDU	Zeigt die Anzahl der nicht an das Gerät übermittelten MMRPDUs mit fehlerhaftem Datenfeld.
Senden fehlgeschlagen	Zeigt die Anzahl der nicht an das Gerät übermittelten MMRPDUs.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Gesendete MMRP-PDU	Zeigt die Anzahl der an den Port übermittelten MMRPDUs.
Empfangene MMRP-PDU	Zeigt die Anzahl der vom Port empfangenen MMRPDUs.
Empfangene Bad-Header-PDU	Zeigt die Anzahl der vom Port empfangenen MMRPDUs mit fehlerhaftem Header.
Empfangene Bad-Format-PDU	Zeigt die Anzahl der nicht an den Port übermittelten MMRPDUs mit fehlerhaftem Datenfeld.
Senden fehlgeschlagen	Zeigt die Anzahl der nicht an den Port übermittelten MMRPDUs.
Letzte empfangene MAC-Adresse	Zeigt die letzte MAC-Adresse, von welcher der Port MMRPDUs empfangen hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Setzt die Zähler der Port-Statistiken und die Werte in Spalte <i>Letzte empfangene MAC-Adresse</i> zurück.

5.5.3 MRP-IEEE Multiple VLAN Registration Protocol

Das Multiple VLAN Registration Protocol (MVRP) besitzt einen Mechanismus, der das Verteilen von VLAN-Informationen und das dynamische Konfigurieren von VLANs ermöglicht. Wenn Sie zum Beispiel ein VLAN an einem aktiven MVRP-Port konfigurieren, verteilt das Gerät die VLAN-Informationen an andere Geräte mit eingeschaltetem MVRP. Anhand der erhaltenen Informationen erzeugt ein Gerät mit aktiviertem MVRP dynamisch nach Bedarf VLAN-Trunks in anderen Geräten mit aktiviertem MVRP.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [\[Konfiguration\]](#)
- ▶ [\[Statistiken\]](#)

[Konfiguration]

In dieser Registerkarte wählen Sie aktive MVRP-Port-Teilnehmer und stellen das Gerät so ein, dass es periodische Ereignisse überträgt.

Für jeden Port existiert eine Periodic-State-Machine, die regelmäßig periodische Ereignisse an die mit aktiven Ports verbundenen Applicant-State-Machines überträgt. Periodische Ereignisse enthalten eine Information, die über den Status der mit dem aktiven Port verbundenen VLANs informiert. Mit periodischen Ereignissen erhalten Switches mit eingeschaltetem MVRP dynamisch die VLANs aufrecht.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die globale Applicant-Administrative-Überwachung ein/aus, welche festlegt, ob die Applicant-State-Machine am Austausch von MMRP-Nachrichten teilnimmt. Mögliche Werte: <ul style="list-style-type: none">▶ <code>An</code> Normaler Teilnehmer. Die Applicant-State-Machine nimmt am Austausch von MMRP-Nachrichten teil.▶ <code>Aus</code> (Voreinstellung) Kein Teilnehmer. Die Applicant-State-Machine ignoriert MMRP-Nachrichten.

■ Konfiguration

Parameter	Bedeutung
Periodische State-Machine	Schaltet die Periodic-State-Machine im Gerät ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ <code>An</code> Die Periodic-State-Machine ist eingeschaltet. Bei global eingeschalteter MVRP-<i>Funktion</i> überträgt das Gerät periodische MVRP-Nachrichten im Intervall von 1 Sekunde an die an MVRP teilnehmenden Ports.▶ <code>Aus</code> (Voreinstellung) Die Periodic-State-Machine ist ausgeschaltet. Deaktiviert die Periodic-State-Machine im Gerät.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Aktiv	Aktiviert/deaktiviert die Teilnahme des Ports an MVRP. Mögliche Werte: <ul style="list-style-type: none">▶ <code>markiert</code> (Voreinstellung) Bei global und an diesem Port eingeschaltetem MVRP verteilt das Gerät Informationen zur VLAN-Mitgliedschaft an MVRP-fähige Geräte, die an diesen Port angeschlossen sind.▶ <code>unmarkiert</code> Schaltet die Teilnahme des Ports an MMRP aus.

Parameter	Bedeutung
Restricted VLAN registration	Aktiviert/deaktiviert die Funktion <i>Restricted VLAN registration</i> an diesem Port. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Bei eingeschalteter Funktion und vorhandenem statischem VLAN-Registrierungseintrag bietet Ihnen das Gerät die Möglichkeit, ein dynamisches VLAN für diesen Eintrag zu erzeugen.▶ unmarkiert (Voreinstellung) Schaltet die Funktion <i>Restricted VLAN registration</i> an diesem Port aus.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Statistiken]

Geräte in einem LAN tauschen Multiple VLAN Registration Protocol Data Units (MVRPDU) aus, um die Status von VLANs an einem aktiven Port aufrecht zu erhalten. Diese Registerkarte bietet Ihnen die Möglichkeit, die Statistiken des MVRP-Verkehrs zu überwachen.

■ Information


Parameter	Bedeutung
Gesendete MVRP-PDU	Zeigt die Anzahl der an das Gerät übermittelten MVRPDUs.
Empfangene MVRP-PDU	Zeigt die Anzahl der vom Gerät empfangenen MVRPDUs.
Empfangene Bad-Header-PDU	Zeigt die Anzahl der vom Gerät empfangenen MVRPDUs mit fehlerhaftem Header.
Empfangene Bad-Format-PDU	Zeigt die Anzahl der vom Gerät blockierten MVRPDUs mit fehlerhaftem Datenfeld.
Senden fehlgeschlagen	Zeigt die Anzahl der Fehler beim Hinzufügen einer Nachricht zur MVRP-Warteschlange.
Message-Queue-Fehler	Zeigt die Anzahl der vom Gerät blockierten MVRPDUs.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Gesendete MVRP-PDU	Zeigt die Anzahl der an den Port übermittelten MVRPDUs.
Empfangene MVRP-PDU	Zeigt die Anzahl der vom Port empfangenen MVRPDUs.
Empfangene Bad-Header-PDU	Zeigt die Anzahl der vom Gerät am Port empfangenen MVRPDUs mit fehlerhaftem Header.
Empfangene Bad-Format-PDU	Zeigt die Anzahl der vom Gerät am Port blockierten MVRPDUs mit fehlerhaftem Datenfeld.
Senden fehlgeschlagen	Zeigt die Anzahl der vom Gerät am Port blockierten MVRPDUs.
Registrierungen fehlgeschlagen	Zeigt die Anzahl der am Port fehlgeschlagenen Registrierungsversuche.
Letzte empfangene MAC-Adresse	Zeigt die letzte MAC-Adresse, von welcher der Port MVRPDUs empfangen hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Setzt die Zähler der Port-Statistiken und die Werte in Spalte <i>Letzte empfangene MAC-Adresse</i> zurück.

5.6 QoS/Priorität

Kommunikationsnetze übertragen gleichzeitig eine Vielzahl von Anwendungen, die jeweils unterschiedliche Anforderungen an Verfügbarkeit, Bandbreite und Latenzzeiten haben.

QoS (Quality of Service) ist ein in der Norm IEEE 802.1D beschriebenes Verfahren. Damit verteilen Sie die Ressourcen im Netz. Sie haben damit die Möglichkeit, wichtigen Anwendungen eine Mindest-Bandbreite zur Verfügung zu stellen. Voraussetzung ist, dass die Endgeräte und die Geräte im Netz die priorisierte Datenübertragung unterstützen. Hochpriorisierte Datenpakete vermitteln die Geräte im Netz bevorzugt. Datenpakete mit niedriger Priorität vermitteln sie, wenn keine höher priorisierten Datenpakete zu vermitteln sind.

Das Gerät bietet Ihnen folgende Einstellmöglichkeiten:

- ▶ Für eingehende Datenpakete legen Sie fest, wie das Gerät die QoS-/Priorisierungs-Information auswertet.
- ▶ Für ausgehende Datenpakete legen Sie fest, welche QoS-/Priorisierungs-Information das Gerät in das Datenpaket schreibt (zum Beispiel Priorität für Management-Pakete, Portpriorität).

Anmerkung: Schalten Sie die Flusskontrolle aus, wenn Sie die Funktionen in diesem Menü nutzen. Die Flusskontrolle ist ausgeschaltet, wenn im Dialog *Switching > Global*, Rahmen *Konfiguration*, das Kontrollkästchen *Flusskontrolle* unmarkiert ist.

Das Menü enthält die folgenden Dialoge:

- ▶ [QoS/Priorität Global](#)
- ▶ [QoS/Priorität Port-Konfiguration](#)
- ▶ [802.1D/p Zuweisung](#)
- ▶ [IP-DSCP-Zuweisung](#)
- ▶ [Queue-Management](#)

5.6.1 QoS/Priorität Global

Das Gerät bietet Ihnen die Möglichkeit, auch in Situationen mit großer Netzlast Zugriff auf die Management-Funktionen zu behalten. In diesem Dialog legen Sie die dazu notwendigen QoS-/Priorisierungseinstellungen fest.

■ Konfiguration

Parameter	Bedeutung
VLAN-Priorität für Management-Pakete	<p>Legt die VLAN-Priorität für zu sendende Management-Datenpakete fest. Abhängig von der VLAN-Priorität weist das Gerät das Datenpaket einer bestimmten Verkehrsklasse zu und dementsprechend einer bestimmten Warteschlange des Ports.</p> <p>Mögliche Werte: ▶ 0..7 (Voreinstellung: 0)</p> <p>Im Dialog <i>Switching > QoS/Priorität > 802.1D/p Zuweisung</i> weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.</p>
IP-DSCP-Wert für Management-Pakete	<p>Legt den IP-DSCP-Wert für zu sendende Management-Datenpakete fest. Abhängig vom IP-DSCP-Wert weist das Gerät das Datenpaket einer bestimmten Verkehrsklasse zu und dementsprechend einer bestimmten Warteschlange des Ports.</p> <p>Mögliche Werte: ▶ 0 (be/cs0) .. 63 (Voreinstellung: 0 (be/cs0))</p> <p>Einige Werte in der Liste haben zusätzlich ein DSCP-Schlüsselwort, zum Beispiel 0 (be/cs0) , 10 (af11) und 46 (ef) . Diese Werte sind kompatibel zum IP-Precedence-Modell.</p> <p>Im Dialog <i>Switching > QoS/Priorität > IP-DSCP-Zuweisung</i> weisen Sie jedem IP-DSCP-Wert eine Verkehrsklasse zu.</p>
Queues je Port	<p>Zeigt die Anzahl der Warteschlangen pro Port. Das Gerät verfügt über 4Warteschlangen pro Port. Jede Warteschlange ist einer bestimmten Verkehrsklasse zugewiesen (Traffic Class nach IEEE 802.1D).</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.6.2 QoS/Priorität Port-Konfiguration

In diesem Dialog legen Sie für jeden Port fest, wie das Gerät empfangene Datenpakete anhand ihrer QoS-/Prioritätsinformation verarbeitet.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Port-Priorität	<p>Legt fest, welche VLAN-Prioritätsinformation das Gerät in ein Datenpaket schreibt, wenn das Datenpaket keine Prioritätsinformation enthält. Das Gerät vermittelt das Datenpaket anschließend abhängig vom festgelegten Wert in Spalte <i>Trust-Mode</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..7 (Voreinstellung: 0)
Trust-Mode	<p>Legt fest, wie das Gerät ein empfangenes Datenpaket behandelt, wenn das Datenpaket eine Prioritätsinformation enthält.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ untrusted <p>Das Gerät vermittelt das Datenpaket gemäß der in Spalte <i>Port-Priorität</i> festgelegten Priorität. Das Gerät ignoriert die im Datenpaket enthaltene Prioritätsinformation. Im Dialog <i>Switching > QoS/Priorität > 802.1D/p Zuweisung</i> weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.</p> ▶ trustDot1p (Voreinstellung) <p>Das Gerät vermittelt das Datenpaket gemäß der Prioritätsinformation im VLAN-Tag. Im Dialog <i>Switching > QoS/Priorität > 802.1D/p Zuweisung</i> weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.</p> ▶ trustIpDscp <ul style="list-style-type: none"> – Wenn das Datenpaket ein IP-Paket ist: <p>Das Gerät vermittelt das Datenpaket gemäß des im Datenpaket enthaltenen IP-DSCP-Werts. Im Dialog <i>Switching > QoS/Priorität > IP-DSCP-Zuweisung</i> weisen Sie jedem IP-DSCP-Wert eine Verkehrsklasse zu.</p> – Wenn das Datenpaket kein IP-Paket ist: <p>Das Gerät vermittelt das Datenpaket gemäß der in Spalte <i>Port-Priorität</i> festgelegten Priorität. Im Dialog <i>Switching > QoS/Priorität > 802.1D/p Zuweisung</i> weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.</p>
Untrusted-Traffic-Klasse	<p>Zeigt die Verkehrsklasse, welche der in Spalte <i>Port-Priorität</i> festgelegten VLAN-Prioritätsinformation zugewiesen ist. Im Dialog <i>Switching > QoS/Priorität > 802.1D/p Zuweisung</i> weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..3

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

5.6.3 802.1D/p Zuweisung

Das Gerät vermittelt Datenpakete mit VLAN-Tag anhand der enthaltenen QoS-/Priorisierungsinformation mit hoher oder mit niedriger Priorität.

In diesem Dialog weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu. Die Verkehrsklassen sind den Warteschlangen der Ports (Prioritäts-Queues) fest zugewiesen.

■ Tabelle

Parameter	Bedeutung
VLAN-Priorität	Zeigt die VLAN-Priorität.
Traffic-Klasse	Legt die Verkehrsklasse fest, die der VLAN-Priorität zugewiesen ist. Mögliche Werte: ▶ 0..3 0 ist der Warteschlange mit der niedrigsten Priorität zugewiesen. 3 ist der Warteschlange mit der höchsten Priorität zugewiesen. Anmerkung: Unter anderem Redundanzmechanismen nutzen die höchste Verkehrsklasse. Wählen Sie deshalb für Anwendungsdaten eine andere Verkehrsklasse.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

■ Werksseitige Zuweisung der VLAN-Priorität zu Verkehrsklassen

VLAN-Priorität	Traffic Class	Inhaltskennzeichnung gemäß IEEE 802.1D
0	1	Best Effort Normale Daten ohne Priorisierung
1	0	Background Zeitunkritische Daten und Hintergrunddienste
2	0	Standard Normale Daten
3	1	Excellent Effort Wichtige Daten
4	2	Controlled Load Verzögerungsempfindliche Daten mit hoher Priorität
5	2	Video Bildübertragung mit Verzögerungen und Jitter < 100 ms
6	3	Voice Sprachübertragung mit Verzögerungen und Jitter < 10 ms
7	3	Network Control Daten für Netzmanagement und Redundanzmechanismen

5.6.4 IP-DSCP-Zuweisung

Das Gerät vermittelt IP-Datenpakete anhand des im Datenpaket enthaltenen DSCP-Werts mit hoher oder mit niedriger Priorität.

In diesem Dialog weisen Sie jedem DSCP-Wert eine Verkehrsklasse zu. Die Verkehrsklassen sind den Warteschlangen der Ports (Prioritäts-Queues) fest zugewiesen.

■ Tabelle

Parameter	Bedeutung
DSCP Wert	Zeigt den DSCP-Wert.
Traffic-Klasse	Legt die Verkehrsklasse fest, die dem DSCP-Wert zugewiesen ist. Mögliche Werte: ▶ 0..3 0 ist der Warteschlange mit der niedrigsten Priorität zugewiesen. 3 ist der Warteschlange mit der höchsten Priorität zugewiesen.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

■ Werksseitige Zuweisung der DSCP-Werte zu Verkehrsklassen

DSCP-Wert	DSCP-Name	Traffic Class
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

Switching

Switching > QoS/Priorität > IP-DSCP-Zuweisung

DSCP-Wert	DSCP-Name	Traffic Class
57-63		3

5.6.5 Queue-Management

Dieser Dialog bietet Ihnen die Möglichkeit, für die Verkehrsklassen die Funktion *Strict priority* ein- und auszuschalten. Bei ausgeschalteter Funktion *Strict priority* arbeitet das Gerät die Warteschlangen der Ports mit „Weighted Fair Queuing“ ab.

■ Tabelle

Parameter	Bedeutung
Traffic-Klasse	Zeigt die Verkehrsklasse.
Strict priority	<p>Aktiviert/deaktiviert für diese Verkehrsklasse die Abarbeitung der Port-Warteschlange mit <i>Strict priority</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) <ul style="list-style-type: none"> Die Abarbeitung der Port-Warteschlange mit <i>Strict priority</i> ist aktiv. <ul style="list-style-type: none"> – Der Port sendet ausschließlich Datenpakete, die sich in der Warteschlange mit der höchsten Priorität befinden. Ist diese Warteschlange leer, sendet der Port Datenpakete, die sich in der Warteschlange mit der nächst niedrigeren Priorität befinden. – Datenpakete mit niedriger Verkehrsklasse sendet der Port erst, wenn die Warteschlangen mit höherer Priorität leer sind. In ungünstigen Fällen sendet der Port diese Datenpakete nie. – Wenn Sie diese Einstellung für eine Verkehrsklasse festlegen, schaltet das Gerät die Funktion auch bei den Verkehrsklassen mit höherer Priorität ein. – Verwenden Sie diese Einstellung für Anwendungen wie VoIP oder Video, die möglichst verzögerungsfrei arbeiten sollen. ▶ unmarkiert <ul style="list-style-type: none"> Die Abarbeitung der Port-Warteschlange mit <i>Strict priority</i> ist inaktiv. Das Gerät verwendet „Weighted Fair Queuing“/„Weighted Round Robin“ (WRR), um die Port-Warteschlange abzuarbeiten. <ul style="list-style-type: none"> – Das Gerät weist jeder Verkehrsklasse eine Mindestbandbreite zu. – Der Port sendet auch bei hoher Netzlast Datenpakete mit niedriger Verkehrsklasse. – Wenn Sie diese Einstellung für eine Verkehrsklasse festlegen, schaltet das Gerät die Funktion auch bei den Verkehrsklassen mit niedriger Priorität aus.
Min. Bandbreite [%]	<p>Legt die Mindestbandbreite für diese Verkehrsklasse fest, wenn das Gerät die Warteschlangen der Ports mit „Weighted Fair Queuing“ abarbeitet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..100 (Voreinstellung: 0 = das Gerät reserviert für diese Verkehrsklasse keine Bandbreite) <p>Der festgelegte Wert in Prozent bezieht sich auf die auf dem Port verfügbare Bandbreite. Wenn Sie für jede Verkehrsklasse die Funktion <i>Strict priority</i> ausschalten, steht auf dem Port die maximale Bandbreite für „Weighted Fair Queuing“ zur Verfügung.</p> <p>Die Summe der zugewiesenen Bandbreiten ist höchstens 100%.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.7 VLAN

Mit VLAN (Virtual Local Area Network) verteilen Sie den Datenverkehr im physischen Netz auf logische Teilnetze. Das bietet Ihnen folgende Vorteile:

- ▶ Hohe Flexibilität
 - Mit VLAN verteilen Sie den Datenverkehr auf logische Netze in der vorhandenen Infrastruktur. Ohne VLAN wären dazu weitere Geräte und eine aufwendigere Verkabelung notwendig.
 - Mit VLAN definieren Sie Netzsegmente unabhängig vom Standort der einzelnen Endgeräte.
- ▶ Verbesserter Durchsatz
 - Datenpakete lassen sich in VLANs priorisiert übertragen. Bei höherer Priorisierung überträgt das Gerät den Datenverkehr eines VLANs bevorzugt, zum Beispiel mit zeitkritischen Anwendungen wie VoIP-Telefonaten.
 - Die Netzlast reduziert sich erheblich, wenn sich Datenpakete und Broadcasts in kleinen Netzsegmenten anstatt im gesamten Netz ausbreiten.
- ▶ Höhere Sicherheit
 - Das Verteilen des Datenverkehrs auf einzelne logische Netze erschwert ungewolltes Abhören und härtet das System gegen Angriffe, wie MAC-Flooding oder MAC-Spoofing.

Das Gerät unterstützt gemäß dem Standard IEEE 802.1Q paketbasierte „tagged“ VLANs. Das VLAN-Tag im Datenpaket kennzeichnet, zu welchem VLAN das Datenpaket gehört.

Das Gerät überträgt die markierten Datenpakete eines VLANs ausschließlich über Ports, die demselben VLAN zugewiesen sind. Dies reduziert die Netzlast.

Das Gerät lernt die MAC-Adressen für jedes VLAN separat (Independent VLAN Learning).

Das Menü enthält die folgenden Dialoge:

- ▶ [VLAN Global](#)
- ▶ [VLAN Konfiguration](#)
- ▶ [VLAN Port](#)

5.7.1 VLAN Global


Dieser Dialog bietet Ihnen die Möglichkeit, sich allgemeine VLAN-Parameter des Geräts anzusehen.

■ Konfiguration

Parameter	Bedeutung
Größte VLAN-ID	Größtmögliche ID, die Sie einem VLAN zuweisen können. Siehe Dialog <i>Switching > VLAN > Konfiguration</i> .
VLANs (max.)	Zeigt die maximale Anzahl der im Gerät einrichtbaren VLANs. Siehe Dialog <i>Switching > VLAN > Konfiguration</i> .
VLANs	Anzahl der VLANs, die im Gerät gegenwärtig eingerichtet sind. Siehe Dialog <i>Switching > VLAN > Konfiguration</i> . Das VLAN mit der ID 1 ist immer im Gerät eingerichtet.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Leeren...	Versetzt die VLAN-Einstellungen des Geräts in den Voreinstellung. Vorsicht: Sie trennen Ihre Verbindung zum Gerät, wenn Sie im Dialog <i>Grundeinstellungen > Netz</i> die VLAN-ID für die Management-Funktionen geändert haben.

5.7.2 VLAN Konfiguration

In diesem Dialog verwalten Sie die VLANs. Um ein VLAN einzurichten, erzeugen Sie in der Tabelle eine weitere Zeile. Dort legen Sie für jeden Port fest, ob er Datenpakete des betreffenden VLANs vermittelt und ob die Datenpakete ein VLAN-Tag enthalten.

Man unterscheidet zwischen folgenden VLANs:

- ▶ Statische VLANs sind durch den Benutzer eingerichtet.
- ▶ Dynamische VLANs richtet das Gerät automatisch ein und entfernt sie wieder, sobald die Voraussetzungen entfallen.

Für folgende Funktionen erzeugt das Gerät dynamische VLANs:

- **MRP**: Wenn Sie den Ring-Ports ein noch nicht eingerichtetes VLAN zuweisen, erzeugt das Gerät dieses VLAN.
- **MVRP**: Das Gerät erzeugt ein VLAN auf Grundlage der Meldungen benachbarter Geräte.

Anmerkung: Die Einstellungen sind ausschließlich dann wirksam, wenn der VLAN-Unaware-Modus ausgeschaltet ist. Siehe Dialog *Switching > Global*.


■ Tabelle

Parameter	Bedeutung
VLAN-ID	ID des VLANs. Das Gerät unterstützt bis zu 16gleichzeitig eingerichtete VLANs. Mögliche Werte: ▶ 1..4042
Status	Zeigt, auf welche Weise das VLAN eingerichtet ist. Mögliche Werte: ▶ other VLAN 1 oder VLAN eingerichtet durch Funktion <i>802.1X Port-Authentifizierung</i> . Siehe Dialog <i>Netzsicherheit > 802.1X Port-Authentifizierung</i> . ▶ permanent VLAN eingerichtet durch den Benutzer. oder VLAN eingerichtet durch Funktion <i>MRP</i> . Siehe Dialog <i>Switching > L2-Redundanz > MRP</i> . VLANs mit dieser Einstellung bleiben nach einem Neustart eingerichtet, wenn Sie die Änderungen im permanenten Speicher speichern. ▶ dynamicMvrp VLAN eingerichtet durch Funktion <i>MVRP</i> . Siehe Dialog <i>Switching > MRP-IEEE > MVRP</i> . VLANs mit dieser Einstellung sind schreibgeschützt. Das Gerät entfernt ein VLAN aus der Tabelle, sobald der letzte Port das VLAN verlässt.
Erstellungszeit	Zeigt, seit wann das VLAN eingerichtet ist. Das Feld zeigt den Zeitstempel der Betriebszeit (System Uptime).
Name	Legt die Bezeichnung des VLANs fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Parameter	Bedeutung
<Port-Nummer>	<p>Legt fest, ob der betreffende Port Datenpakete des VLANs vermittelt und ob die Datenpakete eine VLAN-Markierung enthalten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ - (Voreinstellung) Der Port ist kein Mitglied des VLANs und vermittelt keine Datenpakete des VLANs. ▶ T = Tagged Der Port ist Mitglied des VLANs und vermittelt die Datenpakete mit VLAN-Tag. Verwenden Sie diese Einstellung zum Beispiel auf Uplink-Ports. ▶ LT = Tagged Learned Der Port ist Mitglied des VLANs und vermittelt die Datenpakete mit VLAN-Tag. Das Gerät hat den Eintrag mit der Funktion <i>GVRP</i> oder <i>MVRP</i> automatisch eingerichtet. ▶ F = Forbidden Der Port ist kein Mitglied des VLANs und vermittelt keine Datenpakete dieses VLANs. Das Gerät verhindert zudem, dass der Port durch die Funktion <i>MVRP</i> Mitglied eines VLANs wird. ▶ U = Untagged (Voreinstellung für VLAN 1) Der Port ist Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag. Verwenden Sie diese Einstellung, wenn das angeschlossene Gerät kein VLAN-Tag auswertet, zum Beispiel auf EndPorts. ▶ LU = Untagged Learned Der Port ist Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag. Das Gerät hat den Eintrag mit der Funktion <i>GVRP</i> oder <i>MVRP</i> automatisch eingerichtet. <p>Anmerkung: Vergewissern Sie sich, dass der Port, an dem die Netzmanagement-Station angeschlossen ist, Mitglied des VLANs ist, in welchem das Gerät die Management-Daten vermittelt. In der Voreinstellung vermittelt das Gerät die Management-Daten im VLAN 1. Sonst bricht die Verbindung zum Gerät ab, sobald Sie die Änderungen an das Gerät übertragen. Der Management-Zugriff auf das Gerät ist ausschließlich mit dem CLI über die V.24-Schnittstelle möglich.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	<p>Öffnet das Fenster <i>Erzeugen</i>, um der Tabelle einen neuen Eintrag hinzuzufügen. Im Feld <i>VLAN-ID</i> legen Sie die ID des VLANs fest.</p>

5.7.3 VLAN Port

In diesem Dialog legen Sie fest, wie das Gerät empfangene Datenpakete behandelt, die kein VLAN-Tag haben oder deren VLAN-Tag von der VLAN-ID des Ports abweicht.

Dieser Dialog bietet Ihnen die Möglichkeit, den Ports ein VLAN zuzuweisen und damit die Port-VLAN-ID festzulegen.

Außerdem legen Sie für jeden Port fest, wie das Gerät bei ausgeschaltetem VLAN-Unaware-Modus Datenpakete überträgt, wenn eine der folgenden Situationen eintritt:

- ▶ Der Port empfängt Datenpakete ohne VLAN-Tag.
- ▶ Der Port empfängt Datenpakete mit VLAN-Prioritätsinformation (VLAN-ID 0, priority tagged).
- ▶ Das VLAN-Tag des Datenpaketes weicht ab von der VLAN-ID des Ports.

Anmerkung: Die Einstellungen sind ausschließlich dann wirksam, wenn der VLAN-Unaware-Modus ausgeschaltet ist. Siehe Dialog *Switching > Global*.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Port-VLAN-ID	Legt die ID des VLANs fest, die das Gerät Datenpaketen ohne eigenes VLAN-Tag zuweist. Voraussetzung ist, dass Sie in Spalte <i>Akzeptierte Datenpakete</i> den Wert festlegen. Mögliche Werte: <ul style="list-style-type: none">▶ ID eines bereits eingerichteten VLANs (Voreinstellung: 1) Wenn Sie die Funktion <i>MRP</i> verwenden und den Ring-Ports kein VLAN zugewiesen ist, legen Sie hier für die Ring-Ports den Wert 1 fest. Andernfalls weist das Gerät den Ring-Ports den Wert automatisch zu.
Akzeptierte Datenpakete	Legt fest, ob der Port empfangene Datenpakete ohne VLAN-Tag überträgt oder verwirft. Mögliche Werte: <ul style="list-style-type: none">▶ <i>admitAll</i> (Voreinstellung) Der Port akzeptiert Datenpakete sowohl mit als auch ohne VLAN-Tag.▶ <i>admitOnlyVlanTagged</i> Der Port akzeptiert ausschließlich Datenpakete, die mit einer VLANID ≥ 1 markiert sind.
Ingress-Filtering	Aktiviert/deaktiviert die Eingangsfilterung. Mögliche Werte: <ul style="list-style-type: none">▶ <i>markiert</i> Die Eingangsfilterung ist aktiv. Das Gerät vergleicht die im Datenpaket enthaltene VLAN-ID mit den VLANs, in denen der Port Mitglied ist. Siehe Dialog <i>Switching > VLAN > Konfiguration</i>. Stimmt die VLAN-ID im Datenpaket mit einem dieser VLANs überein, vermittelt das Gerät das Datenpaket. Andernfalls verwirft das Gerät das Datenpaket.▶ <i>unmarkiert</i> (Voreinstellung) Die Eingangsfilterung ist inaktiv. Das Gerät vermittelt empfangene Datenpakete, ohne die VLAN-ID zu vergleichen. Demzufolge vermittelt das Gerät auch Datenpakete mit VLAN-ID, in denen der Port kein Mitglied ist.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

5.8 L2-Redundanz

Das Menü enthält die folgenden Dialoge:

- ▶ MRP
- ▶ PRP (hardwareabhängig) (hardwareabhängig)
- ▶ HSR (hardwareabhängig) (hardwareabhängig)
- ▶ Spanning Tree
- ▶ Link-Aggregation
- ▶ Link-Backup

5.8.1 MRP

Das Media Redundancy Protocol (MRP) ist ein Protokoll, das den Aufbau hochverfügbarer, ringförmiger Netzstrukturen ermöglicht. Ein MRP-Ring mit Hirschmann-Geräten besteht aus bis zu 100 Geräten, die das MRP-Protokoll gemäß IEC 62439 unterstützen.

Die Ringstruktur eines MRP-Rings wandelt sich beim Ausfall einer Teilstrecke zurück in eine Linienstruktur. Die maximale Umschaltzeit ist konfigurierbar.

Die Ring-Manager-Funktion des Geräts schließt die Enden eines Backbones in Linienstruktur zu einem redundanten Ring.

Anmerkung: *Spanning Tree* und Ring-Redundanz beeinflussen sich gegenseitig. Deaktivieren Sie das *Spanning Tree*-Protokoll auf den Ports, die an den MRP-Ring angeschlossen sind. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>MRP</i> -Funktion ein/aus. Wenn alle Parameter für den MRP-Ring konfiguriert sind, schalten Sie hier die Funktion ein. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>MRP</i>-Funktion ist eingeschaltet. Sind alle Geräte im MRP-Ring konfiguriert, ist die Redundanz aktiv.▶ Aus (Voreinstellung) Die <i>MRP</i>-Funktion ist ausgeschaltet.

■ Ring-Port 1 / Ring-Port 2

Parameter	Bedeutung
Port	Legt die Nummer des Ports fest, der als Ring-Port arbeitet. Mögliche Werte: <ul style="list-style-type: none">▶ <Port-Nummer> Nummer des Ring-Ports Anmerkung: Wenn das Gerät die Software mit Unterstützung für Fast MRP verwendet, können Sie keinen <i>Link-Aggregation</i> -Port als Ringport auswählen.
Funktion	Zeigt den Betriebszustand des Ring-Ports. Mögliche Werte: <ul style="list-style-type: none">▶ forwarding Der Port ist eingeschaltet, Verbindung vorhanden.▶ blocked Der Port ist blockiert, Verbindung vorhanden.▶ disabled Der Port ist ausgeschaltet.▶ nicht verbunden Keine Verbindung vorhanden.

Parameter	Bedeutung
Fixed backup	<p>Aktiviert/deaktiviert die Backup-Port-Funktion für den <i>Ring-Port 2</i>.</p> <p>Anmerkung: Bei der Umschaltung auf den primären Port wird ggf. die maximal zulässige Ring-Wiederherstellungszeit überschritten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die Backup-Funktion für <i>Ring-Port 2</i> ist aktiviert. Ist der Ring geschlossen, schaltet der Ring-Manager auf den primären Ring-Port zurück. ▶ unmarkiert (Voreinstellung) Die Backup-Funktion für <i>Ring-Port 2</i> ist deaktiviert. Ist der Ring geschlossen, sendet der Ring-Manager weiterhin Daten an den sekundären Ring-Port.

■ Konfiguration

Parameter	Bedeutung
Ring-Manager	<p>Schaltet die <i>Ring-Manager</i>-Funktion ein/aus. Aktivieren Sie diese Funktion bei genau einem Gerät an den Enden der Linie.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An Die <i>Ring-Manager</i>-Funktion ist eingeschaltet. Das Gerät arbeitet als Ring-Manager. ▶ Aus (Voreinstellung) Die <i>Ring-Manager</i>-Funktion ist ausgeschaltet. Das Gerät arbeitet als Ring-Client.
Advanced mode	<p>Aktiviert/deaktiviert den Advanced-Modus für schnelle Umschaltzeiten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Advanced Mode eingeschaltet. MRP-fähige Hirschmann-Geräte unterstützen diesen Modus. ▶ unmarkiert Advanced Mode ausgeschaltet. Wählen Sie diese Einstellung, wenn ein anderes Gerät im Ring keine Unterstützung für diesen Modus bietet.
Ring-Rekonfiguration	<p>Legt die max. Umschaltzeit in Millisekunden bei der Rekonfiguration des Rings fest. Diese Einstellung ist ausschließlich dann wirksam, wenn das Gerät als Ring-Manager arbeitet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 500ms ▶ 200ms (Voreinstellung) ▶ 30ms (hardwareabhängig) ▶ 10ms (hardwareabhängig) <p>Kürzere Umschaltzeiten stellen höhere Anforderungen an die Reaktionszeit jedes einzelnen Geräts im Ring. Verwenden Sie kleinere Werte als 500ms ausschließlich dann, wenn die anderen Geräte im Ring ebenfalls diese kürzere Umschaltzeit unterstützen.</p> <p>Anmerkung: Umschaltzeiten von 30ms und 10ms sind für Geräte mit FPGA (Hardware für erweiterte Funktionen) verfügbar. Ob Ihr Gerät Fast MRP unterstützt, können Sie anhand des Produktcodes feststellen. Um die Funktionen zu nutzen, laden Sie die Geräte-Software mit Unterstützung für Fast MRP.</p> <p>Legen Sie die Umschaltzeit 10ms ausschließlich dann fest, wenn Sie im Ring bis zu 20 Geräte verwenden, die diese Umschaltzeit unterstützen. Verwenden Sie im Ring mehr als 20 solcher Geräte, legen Sie die Umschaltzeit mit mindestens 30ms fest.</p>


Parameter	Bedeutung
VLAN-ID	<p>Legt die ID des VLANs fest, das den Ring-Ports zugewiesen ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0 (Voreinstellung) Kein VLAN zugewiesen. Weisen Sie im Dialog <i>Switching > VLAN > Konfiguration</i> den Ring-Ports für VLAN 1 den Wert 0 zu. ▶ 1..4042 VLAN zugewiesen. Wenn Sie den Ring-Ports ein noch nicht eingerichtetes VLAN zuweisen, erzeugt das Gerät das VLAN. Im Dialog <i>Switching > VLAN > Konfiguration</i> erzeugt das Gerät in der Tabelle einen Eintrag für das VLAN und weist den Ring-Ports den Wert 1 zu.

■ Information

Parameter	Bedeutung
Information	<p>Zeigt Meldungen zur Redundanzkonfiguration und mögliche Fehlerursachen.</p> <p>Folgende Meldungen sind möglich, wenn das Gerät als Ring-Client oder als Ring-Manager arbeitet:</p> <ul style="list-style-type: none"> ▶ Redundanz verfügbar Die Redundanz ist eingerichtet. Fällt eine Komponente des Rings aus, übernimmt die redundante Strecke deren Funktion. ▶ Konfigurationsfehler: Ring-Port-Verbindung fehlerhaft Die Verkabelung der Ring-Ports ist fehlerhaft. <p>Folgende Meldungen sind möglich, wenn das Gerät als Ring-Manager arbeitet:</p> <ul style="list-style-type: none"> ▶ Konfigurationsfehler: Pakete eines anderen Ring-Managers empfangen Im Ring existiert ein weiteres Gerät, das als Ring-Manager arbeitet. Schalten Sie die Funktion <i>Ring-Manager</i> bei genau einem Gerät im Ring ein. ▶ Konfigurationsfehler: Verbindung im Ring ist mit falschem Port verbunden Eine Leitung des Rings ist anstatt mit einem Ring-Port mit einem anderen Port verbunden. Das Gerät empfängt Test-Datenpakete ausschließlich auf 1 Ring-Port.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Lösche Ring-Konfiguration	Schaltet die Redundanzfunktion aus und setzt alle Einstellungen im Dialog die voreingestellten Werte zurück.

5.8.2 PRP (hardwareabhängig)

Das Parallel Redundancy Protocol (PRP) ist in der internationalen Norm IEC 62439-3 definiert. PRP verwendet 2 unabhängige LANs mit beliebigen Ring-, Stern-, Bus- und Maschen-Topologien, was zu einer hohen Verfügbarkeit von Netzverbindungen führt.

Um das Gerät mit dem PRP-Netz zu verbinden, verwenden Sie 100 Mbit/s FDX auf den beiden, besonders gekennzeichneten Ports *Port A* und *Port B*.

Der Hauptvorteil von PRP liegt darin, dass der Zielknoten so lange Pakete von der Quelle empfängt, wie 1 LAN zur Verfügung steht. Das Fehlen des zweiten LANs aufgrund von Reparaturen oder einer Wartung hat keine Auswirkung auf die Paketübertragung.

Das Netzgerät, welches die Endgeräte mit dem Netz verbindet, setzt das PRP-Protokoll um. Bei den Ethernet-Switches in beiden LANs handelt es sich um Standard-Switches, welche PRP nicht auswerten. Bei einem sog. „Double Attached Node implementing PRP“ (DANP) handelt es sich um ein doppelt angebundenes Netzgerät mit PRP-Funktionalität, welches 1 Verbindung zu einem unabhängigen LAN hat. Ein sog. „Single Attached Node“ (SAN) ist ein Standard-Ethernet-Gerät, das über eine einzelne LAN-Schnittstelle direkt an eines der redundanten LANs angebunden ist. Aus diesem Grund ist ein SAN außerstande, das redundante LAN zu nutzen.

Bei einer Redundanz-Box (RedBox) handelt es sich um ein Netzgerät, welches die PRP-Funktionalität für Standard Ethernet-Geräte umsetzt. Verbindet man ein Standard Ethernet-Gerät über eine RedBox mit einem PRP-Netz, spricht man von einem virtuellen DANP (VDAN). Viele Anwendungen und Geräte, etwa im Bereich der Signal- und Steuerungsfunktionen oder bei VoIP, benötigen ein integriertes duales PRP-Interface, das Pakete ohne Unterbrechung sendet.

Anmerkung: *PRP* ist für Geräte mit FPGA (Hardware für erweiterte Funktionen) verfügbar. Ob Ihr Gerät *PRP* unterstützt, können Sie anhand des Produktcodes feststellen. Um die Funktionen zu nutzen, laden Sie die Geräte-Software mit Unterstützung für *PRP*.

Anmerkung: Wenn der Abstand zwischen den Paketen (Interframe-Gap) geringer ist als die Latenz zwischen den 2 LANs, sind fehlerhafte Paketreihenfolgen möglich. Fehlerhafte Paketreihenfolgen sind ein Phänomen des PRP-Protokolls. Fehlerhafte Paketreihenfolgen vermeiden Sie, wenn der Abstand zwischen den Paketen größer ist als die Latenz zwischen den LANs.

Das Menü enthält die folgenden Dialoge:

- ▶ PRP Konfiguration (hardwareabhängig)
- ▶ DAN/VDAN-Tabelle (hardwareabhängig)
- ▶ Proxy-Node-Tabelle (hardwareabhängig)
- ▶ PRP Statistiken (hardwareabhängig)

5.8.2.1 PRP Konfiguration (hardwareabhängig)

In diesem Dialog schalten Sie die *PRP*-Funktion ein/aus und konfigurieren das Empfangen/Senden der PRP-Supervision-Pakete.

Die *MRP*- und *Spanning Tree*-Funktion können nicht auf denselben Ports aktiv sein, auf denen Sie *PRP* verwenden. Schalten Sie die *MRP*-Funktion aus oder wählen Sie andere Ports dafür. Deaktivieren Sie die *Spanning Tree*-Funktion auf den PRP-Ports.

Anmerkung: Wenn PRP aktiv ist, verwendet es die Schnittstellen 1/1 und 1/2. Wie Sie anhand der Dialoge *Switching > VLAN*, *Switching > Lastbegrenzer* und *Switching > Filter für MAC-Adressen* feststellen können, ersetzt die *PRP*-Funktion die Interfaces 1/1 und 1/2 durch das Interface prp/1. Konfigurieren Sie die VLAN-Mitgliedschaft, die Ratenbegrenzung und die MAC-Filterung für das Interface prp/1.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>PRP</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>PRP</i>-Funktion ist global eingeschaltet. Bei Aktivierung verarbeitet das Gerät den Datenstrom gemäß den konfigurierten Funktionen.▶ Aus (Voreinstellung) Die <i>PRP</i>-Funktion ist global ausgeschaltet. Um Loops zu vermeiden, schalten Sie die <i>PRP</i>-Funktion auf <i>Port A</i> oder <i>Port B</i> aus, bevor die die <i>PRP</i>-Funktion global ausschalten. Anmerkung: Wenn Sie SFPs für die PRP-Ports verwenden und das Gerät ausschließlich 100 Mbit/s unterstützt, dass müssen die SFPs 100 Mbit/s unterstützen.

■ Port A

Parameter	Bedeutung
Physikalischer Port	Zeigt die Nummer des physischen Ports, den das Gerät als PRP- <i>Port A</i> verwendet.
Port A Admin-Status	Schaltet die <i>PRP</i> -Funktion auf dem Port ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An (Voreinstellung) Die <i>PRP</i>-Funktion auf dem Port ist eingeschaltet.▶ Aus Die <i>PRP</i>-Funktion auf dem Port ist ausgeschaltet.

■ Port B

Parameter	Bedeutung
Physikalischer Port	Zeigt die Nummer des physischen Ports, den das Gerät als PRP-Port B verwendet.
Port B Admin-Status	Schaltet die PRP-Funktion auf dem Port ein/aus. Mögliche Werte: ▶ An (Voreinstellung) Die PRP-Funktion auf dem Port ist eingeschaltet. ▶ Aus Die PRP-Funktion auf dem Port ist ausgeschaltet.

■ Empfänger Supervision-Paket

Parameter	Bedeutung
Supervision-Pakete evaluieren	Aktiviert/deaktiviert die Analyse der Supervision-Pakete. Mögliche Werte: ▶ markiert (Voreinstellung) Die Analyse der Supervision-Pakete ist aktiviert. Das Gerät empfängt Supervision-Pakete und analysiert diese. ▶ unmarkiert Die Analyse der Supervision-Pakete ist deaktiviert. Das Gerät empfängt Supervision-Pakete, ohne diese zu analysieren.

■ Absender Supervision-Paket

Parameter	Bedeutung
Aktiv	Schaltet die Übertragung der Supervision-Pakete ein- oder aus. Mögliche Werte: ▶ An (Voreinstellung) Die Übertragung der Supervision-Pakete ist eingeschaltet. Die RedBox überträgt ihre eigenen Supervision-Pakete. ▶ Aus Die Übertragung der Supervision-Pakete ist ausgeschaltet.
VDAN-Pakete senden	Schaltet die Übertragung der VDAN-Supervision-Pakete ein- oder aus. Voraussetzung dafür ist, dass Sie zuerst den Absender Supervision-Paket aktivieren. Mögliche Werte: ▶ markiert (Voreinstellung) Die Übertragung der VDAN-Supervision-Pakete ist eingeschaltet. Die RedBox überträgt sowohl ihre eigenen Supervision-Pakete wie auch Supervision-Pakete für die im Dialog Proxy-Node-Tabelle gelisteten VDANs. ▶ unmarkiert Die Übertragung der VDAN-Supervision-Pakete ist ausgeschaltet.

■ Konfiguration

Parameter	Bedeutung
MTU	<p>Legt die maximal zulässige Größe der Ethernet-Pakete auf dem Interface in Byte fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 1518..1530 (Voreinstellung: 1518) <p>Mit der Einstellung 1518 vermittelt der Port die Ethernet-Pakete bis zu einschließlich folgender Größe:</p> <ul style="list-style-type: none">– 1518 Byte ohne VLAN-Tag (1514 Byte + 4 Byte CRC)– 1522 Byte mit VLAN-Tag (1518 Byte + 4 Byte CRC) <p>Diese Einstellung bietet Ihnen die Möglichkeit, für bestimmte Anwendungen die Ethernet-Pakete zu vergrößern.</p>
Speed	<p>Legt die Geschwindigkeit des PRP-Interfaces fest. Voraussetzung ist, dass beide PRP-Mitglieds-Ports mit der festgelegten Geschwindigkeit arbeiten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ 100Mbps (Voreinstellung)▶ 1Gbps

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.8.2.2 DAN/VDAN-Tabelle (hardwareabhängig)

Dieser Dialog bietet Ihnen die Möglichkeit, die LANs zu analysieren. Dies ist zum Beispiel dann hilfreich, wenn der *Last seen A*-Zähler eines Ports kontinuierlich hochgezählt wird, während der *Last seen B*-Zähler unverändert bleibt (oder umgekehrt). Dieser Zustand zeigt den Verlust einer LAN-Verbindung.


DAN/VDAN bedeutet Double Attached Node / Virtual Double Attached Node.

■ Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.
MAC-Adresse	Zeigt die MAC-Adresse des Knotens.
Last seen A	Zeigt die Zeit zwischen den ersten empfangenen Paketen an diesem Knoten auf LAN A an. Wenn der Zähler den Schwellwert 497 Tage erreicht, fängt er wieder bei 0 an.
Last seen B	Zeigt die Zeit zwischen den ersten empfangenen Paketen an diesem Knoten auf LAN B an. Wenn der Zähler den Schwellwert 497 Tage erreicht, fängt er wieder bei 0 an.
Remote node type	Zeigt den Knotentyp an. Mögliche Werte: <ul style="list-style-type: none">▶ redboxp Verwaltung▶ vdanp Client

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Setzt die gesamte Tabelle zurück.

5.8.2.3 Proxy-Node-Tabelle (hardwareabhängig)

Dieser Dialog informiert Sie über die angebenen Geräte, für die dieses Gerät Parallelredundanz bereitstellt.


Anmerkung: Die RedBox unterstützt bis zu 128 Hosts. Beim Versuch, mehr als 128 Hosts mit der RedBox zu unterstützen, verwirft das Gerät Datenpakete.

■ Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht. Mögliche Werte: ▶ 1..128
MAC-Adresse	Gibt die MAC-Adressen der angebenen Geräte an, für die dieses Gerät Parallelredundanz umsetzt.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Setzt die gesamte Tabelle zurück.

5.8.2.4 PRP Statistiken (hardwareabhängig)


Dieser Dialog führt Empfangsereignisse für diverse, durch die MIB verwaltete Objekte auf. In jedem Eintrag werden Verschlechterungen der Verbindungsqualität gezählt, die sich bei den in der MIB verwalteten Objekten aus der Spalte „Beschreibung“ ergeben. Die Tabelle listet die Häufigkeit auf, mit der ein Ereignis im betreffenden Pfad durch das Gerät auftritt. Ein Beispiel: Die Einträge für Port A geben den Pfad vom Transceiver über die LRE-Einheit (Link Redundancy Entity) bis zu den UDP/TCP-Schichten an.

■ Tabelle

Parameter	Bedeutung
Beschreibung	Zeigt eine Beschreibung der durch die MIB verwalteten Objekte an, auf die sich die Einträge <i>Port A</i> , <i>Port B</i> und <i>Interlink</i> beziehen.
Port A	Zeigt die Anzahl der Ereignisse an, die durch MIB-verwaltete Objekte an <i>Port A</i> ausgelöst werden. Das Gerät untersucht den Datenverkehr auf seinem Weg vom Receiver/Transceiver A zur LRE-Einheit.
Port B	Zeigt die Anzahl der Ereignisse an, die durch MIB-verwaltete Objekte an <i>Port B</i> ausgelöst werden. Das Gerät untersucht den Datenverkehr auf seinem Weg vom Receiver/Transceiver B zur LRE-Einheit.
Interlink	Zeigt die Anzahl der Ereignisse an, die am Interlink durch die in der MIB verwalteten Objekte ausgelöst werden. Die Zähler sind erfassen diejenigen in der MIB verwalteten Objekte, die den Interlink betreffen. Die anderen Zähler bleiben leer. Der Datenverkehr wird auf seinem Weg von der LRE-Einheit zum Switch untersucht.
CPU-Port	Zeigt die Anzahl der Ereignisse an, die am CPU-Port durch die in der MIB verwalteten Objekte ausgelöst werden. Eines der in der MIB verwalteten Objekte betrifft den CPU-Port. Die anderen Zähler bleiben leer. Der Datenstrom wird auf seinem Weg vom Receiver/Transceiver zur CPU untersucht.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Setzt die gesamte Tabelle zurück.

5.8.3 HSR (hardwareabhängig)

Die Rekonfigurationszeit eines auf HSR basierten Rings liegt bei null (HSR = High-availability Seamless Redundancy, hochverfügbare, nahtlose Redundanz). HSR ist für Anwendungen geeignet, die eine hohe Verfügbarkeit und kurze Reaktionszeiten erfordern. Dies sind zum Beispiel Schutzanwendungen für die Automatisierung elektrischer Anlagen oder Steuerungen für Synchronantriebe, die eine konstante Verbindung benötigen.

Eine HSR-Redundanz-Box (RedBox) verwendet 2 parallel arbeitende Ethernet-Ports, um sich mit einem Ring zu verbinden. Bei einer in dieser Konfiguration arbeitenden HSR-RedBox handelt es sich um einen doppelt angebotenen Knoten, welcher das HSR-Protokoll umsetzt (DANH, Double Attached Node implementing HSR). Bei einem Standard Ethernet-Gerät, welches über eine HSR-RedBox an den HSR-Ring angeschlossen ist, spricht man von einem VDANH (Virtual Doubly Attached Node implementing HSR).

Der übertragende HSR-Knoten bzw. die HSR-RedBox sendet innerhalb des Rings doppelte Pakete, d. h. ein Paket in jede Richtung. Zur Identifizierung fügt der HSR-Knoten den doppelten Paketen eine HSR-Markierung hinzu. Die HSR-Markierung besteht aus einer Port-Kennung, der Länge der Nutzdaten und einer fortlaufenden Nummer. In einem normal arbeitenden Ring empfängt der Ziel-HSR-Knoten oder die RedBox beide Pakete innerhalb eines gewissen Zeitversatzes. Ein HSR-Knoten leitet das zuerst ankommende Paket an die oberen Schichten weiter und verwirft das zweite Paket bei dessen Ankunft. Eine RedBox hingegen leitet das zuerst ankommende Paket an die VDANHS weiter und verwirft das zweite Paket bei dessen Ankunft.

Das Gerät führt eine spezifische Funktion im Netz aus. Sie konfigurieren ein Gerät als HSR-RedBox, indem Sie ein Standard Ethernet-Gerät an einen HSR-Ring anschließen. Sie konfigurieren ein Gerät als HSR-Knoten, indem Sie ein PRP-LAN an einen HSR-Ring anschließen.

Ein einzelner HSR-Ring bietet Platz für bis zu 7 PRP-LANs. Konfigurieren Sie das Gerät dahingehend, dass es den Verkehr, der an das angeschlossene PRP-LAN adressiert ist, identifiziert und markiert.

Die Anzahl von HSR-Knoten im Ring sollte 50 nicht überschreiten.

Sinnvoll ist, den in den HSR Ring eingespeisten Verkehr zu limitieren. Befinden sich Fremdgeräte mit höheren Latenzzeiten im Ring, reduzieren Sie die Anzahl der Ringteilnehmer dementsprechend. Vergewissern Sie sich, dass die Summe der an den HSR-Knoten eingespeisten Bandbreiten unter 84 % liegt.

Anmerkung: *HSR* ist für Geräte mit FPGA (Hardware für erweiterte Funktionen) verfügbar. Ob Ihr Gerät *HSR* unterstützt, können Sie anhand des Produktcodes feststellen. Um die Funktionen zu nutzen, laden Sie die Geräte-Software mit Unterstützung für *HSR*.

Das Menü enthält die folgenden Dialoge:

- ▶ [HSR Konfiguration](#) (hardwareabhängig)
- ▶ [DAN/VDAN-Tabelle](#) (hardwareabhängig)
- ▶ [Proxy-Node-Tabelle](#) (hardwareabhängig)
- ▶ [HSR Statistiken](#) (hardwareabhängig)

5.8.3.1 HSR Konfiguration (hardwareabhängig)

In diesem Dialog schalten Sie die *HSR*-Funktion ein, konfigurieren HSR-Supervision-Pakete und legen die Funktion fest, die das Gerät im HSR-Ring ausführt.

Die *MRP*- und *Spanning Tree*-Funktion können nicht auf denselben Ports aktiv sein, auf denen Sie *HSR* verwenden. Schalten Sie die *MRP*-Funktion aus oder wählen Sie andere Ports dafür. Deaktivieren Sie die *Spanning Tree*-Funktion auf den HSR-Ports.

Anmerkung: Wenn HSR aktiv ist, verwendet es die Schnittstellen 1/1 und 1/2. Wie Sie anhand der Dialoge *Switching > Lastbegrenzer* und *Switching > Filter für MAC-Adressen* feststellen können, ersetzt die *HSR*-Funktion die Interfaces 1/1 und 1/2 durch das Interface `hsr/1`. Konfigurieren Sie die VLAN-Mitgliedschaft und die Ratenbegrenzung für das Interface `hsr/1`.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>HSR</i> -Funktion global ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ An Bei Aktivierung verarbeitet das Gerät den Datenstrom gemäß den konfigurierten Funktionen. ▶ Aus (Voreinstellung)
Anmerkung: Wenn Sie SFPs für die HSR-Ports verwenden und das Gerät ausschließlich 100 Mbit/s unterstützt, dann müssen die SFPs 100 Mbit/s unterstützen.	

■ Port A

Parameter	Bedeutung
Physikalischer Port	Zeigt die Nummer des physischen Ports, den das Gerät als <i>HSR-Port A</i> verwendet.
Port A Admin-Status	Schaltet die <i>HSR</i> -Funktion auf dem Port ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ An (Voreinstellung) Die <i>HSR</i>-Funktion auf dem Port ist eingeschaltet. ▶ Aus Die <i>HSR</i>-Funktion auf dem Port ist ausgeschaltet.

■ Port B

Parameter	Bedeutung
Physikalischer Port	Zeigt die Nummer des physischen Ports, den das Gerät als <i>HSR-Port B</i> verwendet.
Port B Admin-Status	Schaltet die <i>HSR</i> -Funktion auf dem Port ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ An (Voreinstellung) Die <i>HSR</i>-Funktion auf dem Port ist eingeschaltet. ▶ Aus Die <i>HSR</i>-Funktion auf dem Port ist ausgeschaltet.

■ Empfänger Supervision-Paket

Parameter	Bedeutung
Supervision-Pakete evaluieren	<p>Aktiviert/deaktiviert die Supervision-Paket-Analyse.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> (Voreinstellung) Supervision-Paket-Analyse ist eingeschaltet. Das Gerät empfängt Supervision-Datenpakete und analysiert diese.▶ <code>unmarkiert</code> Supervision-Paket-Analyse ist ausgeschaltet. Das Gerät empfängt Supervision-Datenpakete, ohne sie zu analysieren.

■ Absender Supervision-Paket

Parameter	Bedeutung
Aktiv	<p>Schaltet die Übertragung der Supervision-Pakete ein- oder aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>An</code> (Voreinstellung) Die Übertragung der Supervision-Pakete ist eingeschaltet. Die RedBox überträgt ihre eigenen Supervision-Pakete.▶ <code>Aus</code> Die Übertragung der Supervision-Pakete ist ausgeschaltet.
VDAN-Pakete senden	<p>Schaltet die Übertragung der VDAN-Supervision-Pakete ein- oder aus. Voraussetzung ist, dass die Übertragung der Supervision-Pakete eingeschaltet ist. Siehe Feld <i>Aktiv</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Die Übertragung der VDAN-Supervision-Pakete ist eingeschaltet. Die RedBox überträgt sowohl ihre eigenen Supervision-Pakete wie auch Supervision-Pakete für die im Dialog <i>Proxy-Node-Tabelle</i> gelisteten VDANs.▶ <code>unmarkiert</code> (Voreinstellung) Die Übertragung der VDAN-Supervision-Pakete ist ausgeschaltet.

■ HSR-Parameter

Parameter	Bedeutung
HSR mode	<p>Legt die Weiterleitungskapazität des Geräts für Unicast-Verkehr fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>modeh</code> (Voreinstellung) Sofern der Host als Proxy für ein Zielgerät arbeitet, entfernt er Unicast-Verkehr aus dem Ring und leitet diesen an die Zieladresse weiter.▶ <code>modeu</code> Sofern der Host als Proxy für ein Zielgerät arbeitet, leitet er Unicast-Verkehr um den Ring herum und an die Zieladresse weiter. Wenn die Pakete zurückkehren, verwirft der Quellknoten den Unicast-Verkehr.

Parameter	Bedeutung
Switching node type	<p>Legt die Funktion fest, die das Gerät im HSR-Ring ausführt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>hsrredboxsan</code> (Voreinstellung) Verwenden Sie diese Einstellung, wenn Sie innerhalb eines HSR-Rings SANs mit dem Gerät verbinden. ▶ <code>hsrredboxprpa</code> Verwenden Sie diese Einstellung, um das betreffende Gerät mit PRP-LAN A zu verbinden. Stellen Sie außerdem beim Parameter <i>Redbox-Identity</i> die entsprechende Netzverbindung ein. ▶ <code>hsrredboxprpb</code> Verwenden Sie diese Einstellung, um das betreffende Gerät mit PRP-LAN B zu verbinden. Stellen Sie außerdem beim Parameter <i>Redbox-Identity</i> die entsprechende Netzverbindung ein. <p>Anmerkung: Wenn Sie den Wert <code>hsrredboxprpa</code> oder <code>hsrredboxprpb</code> festlegen, erhöhen Sie die MTU-Größe auf dem Interface. Siehe Rahmen <i>Konfiguration</i>, Feld <i>MTU</i>. Erhöhen Sie außerdem die MTU-Größe der mit LAN A und B in den PRP-Netzen verbundenen Ports um den gleichen Betrag. Siehe Spalte <i>MTU</i> im Dialog <i>Grundeinstellungen > Port</i>, Registerkarte <i>Konfiguration</i>.</p>
Redbox-Identity	<p>Legt die Markierungen für den PRP-LAN-Verkehr fest.</p> <p>Der Parameter identifiziert und markiert den Datenverkehr für das PRP-LAN, welches mit diesem Gerät verbunden ist. Das Gerät identifiziert den Verkehr für bis zu 7 PRP-LANs, die an den HSR-Ring angekoppelt sind.</p> <p>Voraussetzung hierfür ist, dass Sie den Parameter <i>Switching node type</i> auf <code>hsrredboxprpa</code> oder auf <code>hsrredboxprpb</code> setzen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>id1a</code> (Voreinstellung) Verwenden Sie diesen Wert, um den HSR-Datenverkehr für LAN A im PRP-Netz 1 abzuwickeln. ▶ <code>id1b</code> Verwenden Sie diesen Wert, um den HSR-Datenverkehr für LAN B im PRP-Netz 1 abzuwickeln. ▶ <code>id2a</code> Verwenden Sie diesen Wert, um den HSR-Datenverkehr für LAN A im PRP-Netz 2 abzuwickeln. ▶ <code>id2b</code> Verwenden Sie diesen Wert, um den HSR-Datenverkehr für LAN B im PRP-Netz 2 abzuwickeln. ▶ <code>id7a</code> Verwenden Sie diesen Wert, um den HSR-Datenverkehr für LAN A im PRP-Netz 7 abzuwickeln. ▶ <code>id7b</code> Verwenden Sie diesen Wert, um den HSR-Datenverkehr für LAN B im PRP-Netz 7 abzuwickeln.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

5.8.3.2 DAN/VDAN-Tabelle (hardwareabhängig)

Dieser Dialog bietet Ihnen die Möglichkeit, die LANs zu analysieren. Dies ist zum Beispiel dann hilfreich, wenn der *Last seen A*-Zähler eines Ports kontinuierlich hochgezählt wird, während der *Last seen B*-Zähler unverändert bleibt (oder umgekehrt). Dieser Zustand zeigt den Verlust einer LAN-Verbindung.


DAN/VDAN bedeutet Double Attached Node / Virtual Double Attached Node.

■ Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.
MAC-Adresse	Zeigt die MAC-Adresse des Knotens.
Last seen A	Zeigt die Zeit zwischen den ersten empfangenen Paketen an diesem Knoten auf LAN A an. Wenn der Zähler den Schwellwert 497 Tage erreicht, fängt er wieder bei 0 an.
Last seen B	Zeigt die Zeit zwischen den ersten empfangenen Paketen an diesem Knoten auf LAN B an. Wenn der Zähler den Schwellwert 497 Tage erreicht, fängt er wieder bei 0 an.
Remote node type	Zeigt den Knotentyp an. Mögliche Werte: ▶ redboxh Management ▶ vdanh Client

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Setzt die gesamte Tabelle zurück.

5.8.3.3 Proxy-Node-Tabelle (hardwareabhängig)


Dieser Dialog informiert Sie über die angebotenen Geräte, für die dieses Gerät HSR-Redundanz bereitstellt.

■ Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht. Mögliche Werte: ▶ 1..128
MAC-Adresse	Zeigt die MAC-Adressen der angeschlossenen Geräte, für welche dieses Gerät die HSR-Redundanz implementiert.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Setzt die gesamte Tabelle zurück.

5.8.3.4 HSR Statistiken (hardwareabhängig)


Dieser Dialog führt Empfangsereignisse für diverse, durch die MIB verwaltete Objekte auf. In jedem Eintrag werden Verschlechterungen der Verbindungsqualität gezählt, die sich bei den in der MIB verwalteten Objekten aus der Spalte „Beschreibung“ ergeben. Die Tabelle listet die Häufigkeit auf, mit der ein Ereignis im betreffenden Pfad durch das Gerät auftritt. Ein Beispiel: Die Einträge für Port A geben den Pfad vom Transceiver über die LRE-Einheit (Link Redundancy Entity) bis zu den UDP/TCP-Schichten an.

■ Tabelle

Parameter	Bedeutung
Beschreibung	Zeigt eine Beschreibung der durch die MIB verwalteten Objekte an, auf die sich die Einträge <i>Port A</i> , <i>Port B</i> und <i>Interlink</i> beziehen.
Port A	Zeigt die Anzahl der Ereignisse an, die durch MIB-verwaltete Objekte an <i>Port A</i> ausgelöst werden. Das Gerät untersucht den Datenverkehr auf seinem Weg vom Receiver/Transceiver A zur LRE-Einheit.
Port B	Zeigt die Anzahl der Ereignisse an, die durch MIB-verwaltete Objekte an <i>Port B</i> ausgelöst werden. Das Gerät untersucht den Datenverkehr auf seinem Weg vom Receiver/Transceiver B zur LRE-Einheit.
Interlink	Zeigt die Anzahl der Ereignisse an, die am Interlink durch die in der MIB verwalteten Objekte ausgelöst werden. Die Zähler sind erfassen diejenigen in der MIB verwalteten Objekte, die den Interlink betreffen. Die anderen Zähler bleiben leer. Der Datenverkehr wird auf seinem Weg von der LRE-Einheit zum Switch untersucht.
CPU-Port	Zeigt die Anzahl der Ereignisse an, die am CPU-Port durch die in der MIB verwalteten Objekte ausgelöst werden. Eines der in der MIB verwalteten Objekte betrifft den CPU-Port. Die anderen Zähler bleiben leer. Der Datenstrom wird auf seinem Weg vom Receiver/Transceiver zur CPU untersucht.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Setzt die gesamte Tabelle zurück.

5.8.4 Spanning Tree

Das Spanning Tree Protocol (STP) ist ein Protokoll, das redundante Pfade eines Netzes deaktiviert, um Schleifen (Loops) zu vermeiden. Falls auf der Strecke eine Netzkomponente ausfällt, berechnet das Gerät die neue Topologie und aktiviert diese Pfade wieder.

Das Rapid Spanning Tree Protocol ermöglicht schnelles Umschalten auf eine neu berechnete Topologie, ohne dabei bestehende Verbindungen zu unterbrechen. RSTP erreicht durchschnittliche Rekonfigurationszeiten von unter einer Sekunde. Wenn Sie RSTP in einem Ring mit 10 bis 20 Geräten einsetzen, erreichen Sie Rekonfigurationszeiten im Millisekundenbereich.

Anmerkung: Wenn Sie das Gerät über TP-SFPs anstatt über herkömmliche TP-Ports an das Netz anbinden, dauert die Rekonfiguration des Netzes geringfügig länger.

Das Menü enthält die folgenden Dialoge:

- ▶ [Spanning Tree Global](#)
- ▶ [Spanning Tree Port](#)

5.8.4.1 Spanning Tree Global

In diesem Dialog schalten Sie die *Spanning Tree*-Funktion ein-/aus und legen die Bridge-Einstellungen fest.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die Spanning-Tree-Funktion im Gerät ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An (Voreinstellung)▶ Aus Das Gerät verhält sich transparent. Empfangene Spanning-Tree-Datenpakete flutet das Gerät wie Multicast-Datenpakete an den Ports.

■ Variante

Parameter	Bedeutung
Variante	Zeigt das für die <i>Spanning Tree</i> -Funktion verwendete Protokoll: Mögliche Werte: <ul style="list-style-type: none">▶ rstp Das Protokoll RSTP ist aktiv. Mit RSTP (IEEE 802.1Q-2005) ist die <i>Spanning Tree</i> -Funktion in jedem eingerichteten VLAN wirksam.

■ Traps

Parameter	Bedeutung
Trap senden	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn eines der folgenden Ereignisse eintritt: <ul style="list-style-type: none">– Eine andere Bridge übernimmt die Rolle der Root-Bridge.– Die Topologie ändert sich. Ein Port ändert <i>Port-Status</i> von <i>forwarding</i> zu <i>discarding</i> oder von <i>discarding</i> zu <i>forwarding</i>. Mögliche Werte: <ul style="list-style-type: none">▶ markiert▶ unmarkiert (Voreinstellung) Das Senden von SNMP-Traps ist aktiv. Das Senden von SNMP-Traps ist inaktiv.

■ Bridge-Konfiguration

Parameter	Bedeutung
Bridge-ID	Zeigt die Bridge-ID des Geräts. Das Gerät mit der numerisch niedrigsten Bridge-ID übernimmt die Rolle der Root-Bridge im Netz. Mögliche Werte: <ul style="list-style-type: none">▶ <Bridge-Priorität> / <MAC-Adresse> Wert im Feld <i>Priorität</i> / MAC-Adresse des Geräts

Parameter	Bedeutung
Priorität	<p>Legt die Bridge-Priorität des Geräts fest.</p> <p>Mögliche Werte: ▶ 0..61440 in 4096er-Schritten (Voreinstellung: 32768)</p> <p>Weisen Sie dem Gerät die numerisch niedrigste Priorität im Netz zu, um es zur Root-Bridge zu bestimmen.</p>
Hello-Time [s]	<p>Legt die Zeit in Sekunden fest zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Datenpakete).</p> <p>Mögliche Werte: ▶ 1..2 (Voreinstellung: 2)</p> <p>Übernimmt das Gerät die Rolle der Root-Bridge, verwenden die anderen Geräte im Netz den hier festgelegten Wert. Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen <i>Root-Information</i>.</p> <p>Aufgrund der Wechselwirkung mit dem Parameter <i>Tx holds</i> empfehlen wir, den voreinstellten Wert beizubehalten.</p>
Forward-Verzögerung [s]	<p>Legt die Verzögerungszeit für Zustandswechsel in Sekunden fest.</p> <p>Mögliche Werte: ▶ 4..30 (Voreinstellung: 15)</p> <p>Übernimmt das Gerät die Rolle der Root-Bridge, verwenden die anderen Geräte im Netz den hier festgelegten Wert. Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen <i>Root-Information</i>.</p> <p>Im Protokoll RSTP handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus.</p> <p>Das <i>Spanning Tree</i>-Protokoll verwendet den Parameter, um den Wechsel zwischen den Zuständen <i>disabled</i>, <i>discarding</i>, <i>learning</i>, <i>forwarding</i> zu verzögern.</p>
<p>Die Parameter <i>Forward-Verzögerung [s]</i> und <i>Max age</i> stehen in folgender Beziehung zueinander: $Forward-Verzögerung [s] \geq (Max\ age/2) + 1$ Wenn Sie in die Felder einen Wert einfügen, der dieser Beziehung widerspricht, ersetzt das Gerät diese Werte mit den zuletzt gültigen Werten oder mit der Voreinstellung.</p>	
Max age	<p>Legt die maximal zulässige Astlänge fest, d. h. die Anzahl der Geräte bis zur Root-Bridge.</p> <p>Mögliche Werte: ▶ 6..40 (Voreinstellung: 20)</p> <p>Übernimmt das Gerät die Rolle der Root-Bridge, verwenden die anderen Geräte im Netz den hier festgelegten Wert. Andernfalls verwendet das Gerät den von der Root-Bridge vorgegebenen Wert. Siehe Rahmen <i>Root-Information</i>.</p> <p>Das <i>Spanning Tree</i>-Protokoll verwendet den Parameter, um die Gültigkeit von STP-BPDUs in Sekunden festzulegen.</p>
Tx holds	<p>Begrenzt die maximale Übertragungsrate für das Senden von BPDUs.</p> <p>Mögliche Werte: ▶ 1..40 (Voreinstellung: 10)</p> <p>Sendet das Gerät eine BPDU, inkrementiert es an diesem Port einen Zähler. Erreicht der Zähler den hier festgelegten Wert, stellt der Port das Senden weiterer BPDUs ein. Dies reduziert einerseits die durch RSTP erzeugte Last, andererseits führt das Ausbleiben von BPDUs möglicherweise zu einem Loop.</p> <p>Das Gerät dekrementiert den Zähler jede Sekunde um 1. In der folgenden Sekunde sendet das Gerät maximal 1 neue BPDU.</p>

Parameter	Bedeutung
BPDU-Guard	<p>Schaltet die BPDU-Guard-Funktion im Gerät ein/aus. Mit dieser Funktion hilft das Gerät, Ihr Netz vor Fehlkonfigurationen, Angriffen mit STP-BPDUs und unerwünschten Topologieänderungen zu schützen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Der <i>BPDU-Guard</i> ist aktiv. <ul style="list-style-type: none"> – Das Gerät wendet die Funktion auf manuell festgelegte Edge-Ports an. Bei diesen Ports ist im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Port</i>, Registerkarte <i>CIST</i>, das Kontrollkästchen in Spalte <i>Admin-Edge-Port</i> markiert. – Empfängt ein Edge-Port eine STP-BPDU, schaltet das Gerät den Port aus. Im Dialog <i>Grundeinstellungen > Port</i>, Registerkarte <i>Konfiguration</i> ist bei diesem Port das Kontrollkästchen in Spalte <i>Port an</i> unmarkiert. ▶ unmarkiert (Voreinstellung) Der <i>BPDU-Guard</i> ist inaktiv. <p>Um den Status des Ports wieder auf den Wert <i>forwarding</i> zu setzen, gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Wenn der Port weiterhin BPDUs empfängt: <ul style="list-style-type: none"> – Heben Sie im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Port</i>, Registerkarte <i>CIST</i>, die Markierung des Kontrollkästchens in Spalte <i>Admin-Edge-Port</i> auf. oder – Heben Sie im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i> die Markierung des Kontrollkästchens <i>BPDU-Guard</i> auf. <input type="checkbox"/> Um den Port wieder einzuschalten, verwenden Sie die <i>Auto-Disable</i>-Funktion. Alternativ gehen Sie wie folgt vor: <ul style="list-style-type: none"> – Öffnen Sie den Dialog <i>Grundeinstellungen > Port</i>, Registerkarte <i>Konfiguration</i>. – Markieren Sie das Kontrollkästchen in Spalte <i>Port an</i>.
BPDU-Filter (alle Admin-Edge-Ports)	<p>Aktiviert/deaktiviert die Filterung von STP-BPDUs auf jedem manuell festgelegten Edge-Port. Bei diesen Ports ist im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Port</i>, Registerkarte <i>CIST</i>, das Kontrollkästchen in Spalte <i>Admin-Edge-Port</i> markiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Der BPDU-Filter ist auf jedem Edge-Port aktiv. Die Funktion schließt diese Ports von <i>Spanning Tree</i>-Operationen aus. <ul style="list-style-type: none"> – Das Gerät sendet keine STP-BPDUs auf diesen Ports. – Das Gerät verwirft jede STP-BPDU, die es auf diesen Ports empfängt. ▶ unmarkiert (Voreinstellung) Der globale BPDU-Filter ist inaktiv. Sie haben die Möglichkeit, den BPDU-Filter für einzelne Ports explizit zu aktivieren. Siehe Spalte <i>BPDU-Filter Port</i> im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Port</i>.
Auto-Disable	<p>Aktiviert/deaktiviert die <i>Auto-Disable</i>-Funktion für die Parameter, deren Einhaltung der <i>BPDU-Guard</i> auf dem Port überwacht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die <i>Auto-Disable</i>-Funktion für den <i>BPDU-Guard</i> ist aktiv. <ul style="list-style-type: none"> – Das Gerät schaltet einen Edge-Port aus, wenn der Port eine STP-BPDU empfängt. Die „Link-Status“-LED des Ports blinkt 3× pro Periode. – Der Dialog <i>Diagnose > Ports > Auto-Disable</i> zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind. – Die <i>Auto-Disable</i>-Funktion schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog <i>Diagnose > Ports > Auto-Disable</i> in Spalte <i>Reset-Timer [s]</i> eine Wartezeit für den betreffenden Port fest. ▶ unmarkiert (Voreinstellung) Die <i>Auto-Disable</i>-Funktion für den <i>BPDU-Guard</i> ist inaktiv.

■ Root-Information

Parameter	Bedeutung
Bridge-ID	Zeigt die Bridge-ID der gegenwärtigen Root-Bridge. Mögliche Werte: ▶ <Bridge-Priorität> / <MAC-Adresse>
Priorität	Zeigt die Bridge-Priorität der gegenwärtigen Root-Bridge. Mögliche Werte: ▶ 0..61440 in 4096er-Schritten
Hello-Time [s]	Zeigt die von der Root-Bridge vorgegebene Zeit in Sekunden zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Datenpakete). Mögliche Werte: ▶ 1..2 Das Gerät verwendet diesen vorgegebenen Wert. Siehe Rahmen <i>Bridge-Konfiguration</i> .
Forward-Verzögerung [s]	Zeigt die von der Root-Bridge vorgegebene Verzögerungszeit für Zustandswechsel in Sekunden. Mögliche Werte: ▶ 4..30 Das Gerät verwendet diesen vorgegebenen Wert. Siehe Rahmen <i>Bridge-Konfiguration</i> . Im Protokoll RSTP handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus. Das <i>Spanning Tree</i> -Protokoll verwendet den Parameter, um den Wechsel zwischen den Zuständen <i>disabled</i> , <i>discarding</i> , <i>learning</i> , <i>forwarding</i> zu verzögern.
Max age	Zeigt die von der Root-Bridge vorgegebene maximal zulässige Astlänge, d. h. die Anzahl der Geräte bis zur Root-Bridge. Mögliche Werte: ▶ 6..40 (Voreinstellung: 20) Das <i>Spanning Tree</i> -Protokoll verwendet den Parameter, um die Gültigkeit von STP-BPDUs in Sekunden festzulegen.

■ Topologie-Information

Parameter	Bedeutung
Bridge ist Root	Zeigt, ob das Gerät gegenwärtig die Rolle der Root-Bridge übernimmt. Mögliche Werte: ▶ <i>markiert</i> Das Gerät übernimmt gegenwärtig die Rolle der Root-Bridge. ▶ <i>unmarkiert</i> Gegenwärtig übernimmt ein anderes Gerät die Rolle der Root-Bridge.
Root-Port	Zeigt die Nummer des Ports, von dem der gegenwärtige Pfad zur Root-Bridge führt. Übernimmt das Gerät die Rolle der Root-Bridge, zeigt das Feld den Wert 0.
Root-Pfadkosten	Zeigt die Pfadkosten für den Pfad, der vom Root-Port des Geräts zur Root-Bridge des Schicht-2-Netzes führt. Mögliche Werte: ▶ 0..200000000 Wenn der Wert 0 festgelegt ist, übernimmt das Gerät die Rolle der Root-Bridge.
Topologie-Änderungen	Zeigt, wie viele Male das Gerät seit dem Start einen Port durch Spanning Tree in den Zustand <i>forwarding</i> gesetzt hat.
Zeit seit letzter Änderung	Zeigt die Zeit seit der letzten Topologieänderung. Mögliche Werte: ▶ <Tage, Stunden:Minuten:Sekunden>

■ **Schaltflächen**

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf [Seite 19](#).

5.8.4.2 Spanning Tree Port

In diesem Dialog aktivieren Sie die Spanning-Tree-Funktion auf den Ports, legen Edge-Ports sowie die Einstellungen für verschiedene Schutzfunktionen fest.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [\[CIST\]](#)
- ▶ [\[Guards\]](#)

[CIST]

In dieser Registerkarte haben Sie die Möglichkeit, an den Ports die Spanning-Tree-Funktion einzeln zu aktivieren, die Einstellungen für Edge-Ports festzulegen sowie gegenwärtige Werte anzusehen. Die Abkürzung CIST steht für „Common and Internal Spanning Tree“.

Anmerkung: Deaktivieren Sie die *Spanning Tree*-Funktion auf den Ports, die an anderen Schicht-2-Redundanzprotokollen beteiligt sind. Andernfalls arbeiten die Redundanz-Protokolle möglicherweise anders als vorgesehen. Dies kann zu Loops führen.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
STP aktiv	Schaltet die Spanning-Tree-Funktion auf dem Port ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) ▶ unmarkiert Wenn die <i>Spanning Tree</i> -Funktion im Gerät eingeschaltet und auf dem Port ausgeschaltet, sendet der Port keine STP-BPDUs und verwirft empfangene STP-BPDUs.
Port-Status	Zeigt den Vermittlungsstatus des Ports. Mögliche Werte: <ul style="list-style-type: none"> ▶ discarding Der Port ist blockiert und leitet ausschließlich STP-BPDUs weiter. ▶ learning Der Port ist blockiert, lernt jedoch die MAC-Adressen empfangener Datenpakete. ▶ forwarding Der Port leitet Datenpakete weiter. ▶ disabled Der Port ist inaktiv. Siehe Dialog <i>Grundeinstellungen > Port</i>, Registerkarte <i>Konfiguration</i>. ▶ manualFwd Die <i>Spanning Tree</i>-Funktion ist auf dem Port ausgeschaltet. Der Port leitet STP-BPDUs weiter. ▶ notParticipate Der Port nimmt nicht am STP teil.
Port-Rolle	Zeigt die gegenwärtige Rolle des Ports im CIST. Mögliche Werte: <ul style="list-style-type: none"> ▶ root Port mit dem günstigsten Pfad zur Root-Bridge. ▶ alternate Port mit dem alternativen Pfad zur Root-Bridge (gegenwärtig unterbrochen). ▶ designated Port zur von der Root-Bridge abgewandten Seite des Baums. ▶ backup Port empfängt STP-BPDUs des eigenen Geräts. ▶ disabled Der Port ist inaktiv. Siehe Dialog <i>Grundeinstellungen > Port</i>, Registerkarte <i>Konfiguration</i>.
Port-Pfadkosten	Legt die Pfadkosten des Ports fest. Mögliche Werte: <ul style="list-style-type: none"> ▶ 0..200000000 (Voreinstellung: 0) Mit dem Wert 0 ermittelt das Gerät die Pfadkosten in Abhängigkeit von der Datenrate des Ports automatisch.

Parameter	Bedeutung
Port-Priorität	<p>Legt die Priorität des Ports fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 16..240 in 16er-Schritten (Voreinstellung: 128) <p>Der Wert repräsentiert die ersten 4 Bits der Port-ID.</p>
Empfangene Bridge-ID	<p>Zeigt die Bridge-ID des Geräts an, von dem dieser Port zuletzt eine STP-BPDU empfangen hat.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Für Ports mit der Rolle <i>designated</i> zeigt das Gerät die Information der STP-BPDU an, die der Port zuletzt empfangen hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz. ▶ Für die Port-Rollen <i>alternate</i>, <i>backup</i>, <i>master</i> und <i>root</i> sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle <i>designated</i>. ▶ Hat ein Port keine Verbindung oder hat er noch keine STP-BDPU empfangen, zeigt das Gerät die Werte an, die der Port mit der Rolle <i>designated</i> senden würde.
Empfangene Port-ID	<p>Zeigt die Port-ID des Geräts an, von dem dieser Port zuletzt eine STP-BPDU empfangen hat.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Für Ports mit der Rolle <i>designated</i> zeigt das Gerät die Information der STP-BPDU an, die der Port zuletzt empfangen hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz. ▶ Für die Port-Rollen <i>alternate</i>, <i>backup</i>, <i>master</i> und <i>root</i> sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle <i>designated</i>. ▶ Hat ein Port keine Verbindung oder hat er noch keine STP-BDPU empfangen, zeigt das Gerät die Werte an, die der Port mit der Rolle <i>designated</i> senden würde.
Empfangene Port-Pfadkosten	<p>Zeigt die Pfadkosten an, welche die übergeordnete Bridge von ihrem Root-Port zur Root-Bridge hat.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Für Ports mit der Rolle <i>designated</i> zeigt das Gerät die Information der STP-BPDU an, die der Port zuletzt empfangen hat. Dies erleichtert die Diagnose von möglichen STP-Problemen im Netz. ▶ Für die Port-Rollen <i>alternate</i>, <i>backup</i>, <i>master</i> und <i>root</i> sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle <i>designated</i>. ▶ Hat ein Port keine Verbindung oder hat er noch keine STP-BDPU empfangen, zeigt das Gerät die Werte an, die der Port mit der Rolle <i>designated</i> senden würde.
Admin-Edge-Port	<p>Aktiviert/deaktiviert den <i>Admin-Edge-Port</i>-Modus. Verwenden Sie den <i>Admin-Edge-Port</i>-Modus, wenn ein Endgerät an den Port angeschlossen ist. Mit dieser Einstellung schaltet der Edge-Port nach dem LinkUp schneller in den Zustand 'forwarding' und macht damit das Endgerät schneller erreichbar.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>markiert</i> <ul style="list-style-type: none"> Der <i>Admin-Edge-Port</i>-Modus ist aktiv. Der Port ist mit einem Endgerät verbunden. <ul style="list-style-type: none"> – Nach Aufbau der Verbindung wechselt der Port in den Zustand <i>forwarding</i>, ohne zuvor in den Zustand <i>learning</i> zu wechseln. – Empfängt der Port eine STP-BPDU, deaktiviert das Gerät den Port, falls die BPDU-Guard-Funktion aktiv ist. Siehe Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i>. ▶ <i>unmarkiert</i> (Voreinstellung) <ul style="list-style-type: none"> Der <i>Admin-Edge-Port</i>-Modus ist inaktiv. Der Port ist mit einer anderen STP-Bridge verbunden. Nach Aufbau der Verbindung wechselt der Port in den Zustand <i>learning</i>, bevor er ggf. in den Zustand <i>forwarding</i> wechselt.

Parameter	Bedeutung
Auto-Edge-Port	<p>Aktiviert/deaktiviert die automatische Erkennung, ob am Port ein Endgerät angeschlossen ist. Voraussetzung ist, dass das Kontrollkästchen in Spalte <i>Admin-Edge-Port</i> unmarkiert ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Die automatische Erkennung ist aktiv. Nach Aufbau der Verbindung setzt das Gerät den Port nach $1,5 \times \text{Hello-Time [s]}$ in den Zustand <code>forwarding</code> (in der Voreinstellung $1,5 \times 2$ s), falls der Port währenddessen keine STP-BPDU empfängt. ▶ <code>unmarkiert</code> Die automatische Erkennung ist inaktiv. Nach Aufbau der Verbindung setzt das Gerät den Port nach <i>Max age</i> in den Zustand <code>forwarding</code>. (Voreinstellung: 20 s)
Oper-Edge-Port	<p>Zeigt, ob am Port ein Endgerät oder eine STP-Bridge angeschlossen ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Am Port ist ein Endgerät angeschlossen. Der Port empfängt keine STP-BPDUs. ▶ <code>unmarkiert</code> Am Port ist eine STP-Bridge angeschlossen. Der Port empfängt STP-BPDUs.
Oper PointToPoint	<p>Zeigt, ob der Port über eine direkte Vollduplex-Verbindung mit einem STP-Gerät verbunden ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>true</code> Der Port ist über eine Vollduplex-Verbindung direkt mit einem STP-Gerät verbunden. Die direkte, dezentrale Kommunikation zwischen 2 Bridges bewirkt kurze Rekonfigurationszeiten ▶ <code>false</code> Der Port ist auf andere Weise verbunden, zum Beispiel über eine Halbduplex-Verbindung oder über einen Hub.
BPDU-Filter Port	<p>Aktiviert/deaktiviert die Filterung von STP-BPDUs explizit auf diesem Port. Voraussetzung ist, dass der Port ein manuell festgelegter Edge-Port ist. Bei diesen Ports ist das Kontrollkästchen in Spalte <i>Admin-Edge-Port</i> markiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Der BPDU-Filter ist auf dem Port aktiv. Die Funktion schließt den Port von <i>Spanning Tree</i>-Operationen aus. <ul style="list-style-type: none"> – Das Gerät sendet keine STP-BPDUs auf dem Port. – Das Gerät verwirft jede STP-BPDU, die es auf dem Port empfängt. ▶ <code>unmarkiert</code> (Voreinstellung) Der BPDU-Filter ist auf dem Port inaktiv. Sie haben die Möglichkeit, den BPDU-Filter global für jeden manuell festgelegten Edge-Port zu aktivieren. Siehe Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i>, Rahmen <i>Bridge-Konfiguration</i>. Wenn das Kontrollkästchen <i>BPDU-Filter (alle Admin-Edge-Ports)</i> markiert ist, dann ist der BPDU-Filter auf dem Port noch aktiv.
Status BPDU-Filter	<p>Zeigt, ob der BPDU-Filter auf dem Port aktiv ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Der BPDU-Filter ist auf dem Port aktiv aufgrund der folgenden Einstellungen: <ul style="list-style-type: none"> – Das Kontrollkästchen in Spalte <i>BPDU-Filter Port</i> ist markiert. und/oder – Das Kontrollkästchen in Spalte <i>BPDU-Filter (alle Admin-Edge-Ports)</i> ist markiert. Siehe Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i>, Rahmen <i>Bridge-Konfiguration</i>. ▶ <code>unmarkiert</code> Der BPDU-Filter ist auf dem Port inaktiv.

Parameter	Bedeutung
BPDU flood	<p>Aktiviert/deaktiviert den <i>BPDU flood</i>-Modus auf dem Port, auch wenn die <i>Spanning Tree</i>-Funktion auf dem Port inaktiv ist. Voraussetzung ist, dass auch der <i>BPDU flood</i>-Modus für diese Ports aktiv ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Der <i>BPDU flood</i>-Modus ist aktiv. Das Gerät flutet STP-BPDUs, die es auf dem Port empfängt, an die Ports, für die <i>Spanning Tree</i>-Funktion inaktiv ist.▶ <i>unmarkiert</i> (Voreinstellung) Der <i>BPDU flood</i>-Modus ist inaktiv.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Guards]

Diese Registerkarte bietet Ihnen die Möglichkeit, an den Ports die Einstellungen für verschiedene Schutzfunktionen festzulegen.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Root guard	<p>Schaltet die Überwachung auf STP-BPDUs auf dem Port ein/aus. Voraussetzung ist, dass die Funktion <i>Loop guard</i> inaktiv ist.</p> <p>Mit dieser Einstellung hilft das Gerät, Ihr Netz vor Fehlkonfigurationen und Angriffen mit STP-BPDUs zu schützen, welche die Topologie zu verändern versuchen. Diese Einstellung gilt ausschließlich für Ports mit der STP-Rolle <i>designated</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Überwachung auf STP-BPDUs ist eingeschaltet.<ul style="list-style-type: none">– Empfängt der Port eine STP-BPDU mit besserer Pfadinformation zur Root-Bridge, verwirft das Gerät die STP-BPDU und setzt den Zustand des Ports auf den Wert <i>discarding</i> anstatt auf <i>root</i>.– Bleiben STP-BPDUs mit besserer Pfadinformation zur Root-Bridge aus, setzt das Gerät den Zustand des Ports nach $2 \times \text{Hello-Time [s]}$▶ <i>unmarkiert</i> (Voreinstellung) Überwachung auf STP-BPDUs ist inaktiv.
TCN guard	<p>Schaltet die Überwachung auf „Topology Change Notifications“ auf dem Port ein/aus. Mit dieser Einstellung hilft das Gerät, Ihr Netz vor Angriffen mit STP-BPDUs zu schützen, welche die Topologie zu verändern versuchen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Überwachung auf ‚Topology Change Notifications‘ ist eingeschaltet.<ul style="list-style-type: none">– Der Port ignoriert das Topology-Change-Flag in empfangenen STP-BPDUs.– Enthält die empfangene BPDU weitere Informationen, die eine Topologieänderung bewirken, verarbeitet das Gerät diese auch bei eingeschaltetem TCN-Guard. Beispiel: Das Gerät empfängt eine bessere Pfadinformation zur Root-Bridge.▶ <i>unmarkiert</i> (Voreinstellung) Überwachung auf ‚Topology Change Notifications‘ ist ausgeschaltet. Empfängt das Gerät STP-BPDUs mit Topology-Change-Flag, löscht es die Adresstabelle des Ports und leitet die Topology Change Notifications weiter.
Loop guard	<p>Schaltet die Überwachung auf Loops auf dem Port ein/aus. Voraussetzung ist, dass die Funktion <i>Root guard</i> inaktiv ist.</p> <p>Mit dieser Einstellung verhindert das Gerät Loops, falls der Port keine STP-BPDUs mehr empfängt. Verwenden Sie diese Einstellung ausschließlich für Ports mit der STP-Rolle <i>alternate</i>, <i>backup</i> und <i>root</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Überwachung auf Loops ist eingeschaltet. Dies verhindert Loops, zum Beispiel wenn Sie die Spanning-Tree-Funktion auf dem entfernten Gerät abschalten oder wenn die Verbindung lediglich in der Empfangsrichtung unterbrochen ist.<ul style="list-style-type: none">– Empfängt der Port eine Zeitlang keine STP-BPDUs, setzt das Gerät den Zustand des Ports auf den Wert <i>discarding</i> und den Wert in Spalte <i>Loop-Zustand</i> auf <i>true</i>.– Empfängt der Port anschließend wieder STP-BPDUs, setzt das Gerät den Zustand des Ports auf einen Wert gemäß <i>Port-Rolle</i> und den Wert in Spalte <i>Loop-Zustand</i> auf <i>false</i>.▶ <i>unmarkiert</i> (Voreinstellung) Überwachung auf Loops ist ausgeschaltet. Empfängt der Port eine Zeitlang keine STP-BPDUs, setzt das Gerät den Zustand des Ports auf den Wert <i>forwarding</i>.

Parameter	Bedeutung
Loop-Zustand	<p>Zeigt, ob der Loop-Status des Ports inkonsistent ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ true <ul style="list-style-type: none"> Der Loop-Status des Ports ist inkonsistent: <ul style="list-style-type: none"> – Der Port empfängt keine STP-BPDUs und die Funktion <i>Loop guard</i> ist eingeschaltet. – Das Gerät setzt den Status des Ports auf den Wert <i>discarding</i>. Damit verhindert das Gerät mögliche Loops. ▶ false <ul style="list-style-type: none"> Der Loop-Status des Ports ist konsistent. Der Port empfängt STP-BPDUs.
Übergänge in Loop-Zustand	Zeigt, wie viele Male das Gerät den Wert in Spalte <i>Loop-Zustand</i> von <i>false</i> auf <i>true</i> gesetzt hat.
Übergänge aus Loop-Zustand	Zeigt, wie viele Male das Gerät den Wert in Spalte <i>Loop-Zustand</i> von <i>true</i> auf <i>false</i> gesetzt hat.
BPDU guard effect	<p>Zeigt, ob der Port als Edge-Port eine STP-BPDU empfangen hat.</p> <p>Voraussetzung:</p> <ul style="list-style-type: none"> – Der Port ist ein manuell festgelegter Edge-Port. Im Dialog <i>Port</i> ist bei diesem Port das Kontrollkästchen in Spalte <i>Admin-Edge-Port</i> markiert. – Im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i> ist die BPDU-Guard-Funktion aktiv. <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert <ul style="list-style-type: none"> Der Port ist Edge-Port und hat eine STP-BPDU empfangen. Das Gerät deaktiviert den Port. Im Dialog <i>Grundeinstellungen > Port</i>, Registerkarte <i>Konfiguration</i> ist bei diesem Port das Kontrollkästchen in Spalte <i>Port an</i> unmarkiert. ▶ unmarkiert <ul style="list-style-type: none"> Der Port ist Edge-Port und hat keine STP-BPDU empfangen oder der Port ist kein Edge-Port. <p>Um den Status des Ports wieder auf den Wert <i>forwarding</i> zu setzen, gehen Sie wie folgt vor:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Wenn der Port weiterhin BPDUs empfängt: <ul style="list-style-type: none"> – Heben Sie in der Registerkarte <i>CIST</i> die Markierung des Kontrollkästchens in Spalte <i>Admin-Edge-Port</i> auf. oder – Heben Sie im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i> die Markierung des Kontrollkästchens <i>BPDU-Guard</i> auf. <input type="checkbox"/> Um den Port zu aktivieren, gehen Sie wie folgt vor: <ul style="list-style-type: none"> – Öffnen Sie den Dialog <i>Grundeinstellungen > Port</i>, Registerkarte <i>Konfiguration</i>. – Markieren Sie das Kontrollkästchen in Spalte <i>Port an</i>.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

5.8.5 Link-Aggregation

IEEE 802.1ax definiert eine Link-Aggregation-Gruppe (LAG) als eine Kombination von 2 oder mehr Punkt-zu-Punkt-Verbindungen, die mit derselben Geschwindigkeit und demselben Duplex-Modus arbeiten, um die Bandbreite zu erhöhen. Link-Aggregation ermöglicht zudem Redundanz. Beim Ausfall eines Links übernehmen die im LAG verbleibenden Links die Weiterleitung der Daten.

Link Aggregation Control Protocol Data Units (LACPDUs) enthalten 2 Felder mit jeweils 8 Bit Informationen, die der Actor periodisch an einen Partner sendet. Die Felder beschreiben den Status des Actors und seine Informationen über die Partner. Die 8 Bits enthalten Informationen über den Status des Actors und Partners. Der Port vermittelt LACPDUs, wenn er sich im aktiven Zustand befindet. Im passiven Zustand vermittelt der Port LACPDUs ausschließlich auf Anfrage.

■ Tabelle

Parameter	Bedeutung
Trunk-Port	Zeigt die Nummer des Link-Aggregation-Ports.
Name	Legt den Namen der Link-Aggregation-Gruppe fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..15 Zeichen
Aktiv	Aktiviert/deaktiviert die Link-Aggregation-Gruppe. Mögliche Werte: ▶ <code>markiert</code> (Voreinstellung) Die LAG-Instanz befindet sich in einem aktiven Zustand und verarbeitet den Datenverkehr entsprechend den festgelegten Werten. ▶ <code>unmarkiert</code> Die LAG-Instanz einschließlich der teilnehmenden Ports befindet sich in einem inaktiven Zustand. Die teilnehmenden Ports verbleiben in der LAG-Instanz und blockieren den Datenverkehr.
STP aktiv	Aktiviert/deaktiviert das <i>Spanning Tree</i> -Protokoll auf diesem LAG-Interface. Nach dem Erzeugen der Link-Aggregation-Instanz in der Tabelle fügt das Gerät den Port automatisch zum Dialog <i>Switching > L2-Redundanz > Spanning Tree > Port</i> hinzu. Mögliche Werte: ▶ <code>markiert</code> (Voreinstellung) Das Aktivieren des STP-Modus in diesem Dialog aktiviert den Port auch im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Port</i> . ▶ <code>unmarkiert</code> Das Deaktivieren des STP-Modus in diesem Dialog deaktiviert den Port auch im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Port</i> . Voraussetzung ist, dass Sie die Funktion global im Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i> einschalten.
Statische Link-Aggregation	Aktiviert/deaktiviert die Funktion <i>Statische Link-Aggregation</i> auf dem LAG-Interface. Mögliche Werte: ▶ <code>markiert</code> Wenn die Funktion <i>Statische Link-Aggregation</i> eingeschaltet ist, unterstützt sie ein stabiles Netz und der Administrator gibt manuell den Aggregation-Status des Ports weiter. ▶ <code>unmarkiert</code> (Voreinstellung) Das Gerät gibt den Aggregation-Status des Ports automatisch weiter.

Parameter	Bedeutung
Aktive Ports (min.)	<p>Legt fest, wie viele aktive Ports das Gerät für die Link-Aggregation-Gruppe verwendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..2 (Voreinstellung: 2) ▶ 1..4 (Voreinstellung: 4) <p>Anmerkung: Die tatsächlich zur Verfügung stehende Anzahl an Ports ist abhängig vom Gerät.</p>
Typ	<p>Zeigt den Typ der verwendeten Link-Aggregation-Gruppe.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ static Das Gerät verwendet statische Aggregation am Port, <i>Statische Link-Aggregation</i> ist eingeschaltet. ▶ dynamic Das Gerät verwendet dynamische Aggregation am Port, <i>Statische Link-Aggregation</i> ist ausgeschaltet.
Trap senden (Link-Up/Down)	<p>Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Link-Status-Änderungen auf dem Interface erkennt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv. Das Gerät sendet einen SNMP-Trap, wenn es eine Link-Status-Änderung erkennt. ▶ unmarkiert Das Senden von SNMP-Traps ist inaktiv. <p>Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose</i> > Statuskonfiguration > <i>Alarmer (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen.</p>
LACP admin key	<p>Legt den Administrativ-Wert für den lokalen Schlüssel an dieser LAG fest.</p> <p>Der Aggregator verwendet den Administrativ-Schlüssel, um Datenverbindungen in einer Gruppe zu bündeln. Der Wert für den Administrativ-Schlüssel kann vom Wert für den Operativ-Schlüssel abweichen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..65535 (Voreinstellung: 0)
LACP-Collector max. Verzögerung [µs]	<p>Legt die maximale Verzögerungszeit für den Datenpaket-Sammler in Mikrosekunden fest.</p> <p>Die LAG verwendet den Datenpaket-Sammler, um Datenpakete in derselben Reihenfolge an den MAC-Client weiterzuleiten, in der der Port sie erhält. Der Sammler verzögert entweder das Weiterleiten des Datenpaketes an seinen MAC-Client oder das Verwerfen des Datenpaketes entsprechend seinem Wert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..65535 (Voreinstellung: 0)
Port	<p>Zeigt die Mitglieder des Ports der LAG-Instanz.</p>
Status	<p>Zeigt den LAG-Status des Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ aktiv Der Port nimmt aktiv in der LAG-Instanz teil. ▶ inaktiv Der Port nimmt nicht in der LAG-Instanz teil.
LACP Aktiv	<p>Aktiviert/deaktiviert LACP an diesem Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Der Port nimmt aktiv in der LAG teil. ▶ unmarkiert Der Port nimmt nicht in der LAG teil.


Parameter	Bedeutung
LACP port actor admin key	<p>Legt den Wert des Administrativ-Schlüssels für den Aggregation-Port fest.</p> <p>Die LAG verwendet Schlüssel, um lokalen Ports die Mitgliedschaft beim Actor-Gerät zuzuweisen. Legen Sie für die in derselben LAG teilnehmenden Actor-Ports denselben Schlüsselwert fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..65535 (Voreinstellung: 0) <p>Wenn der Port zu einer LAG gehört, wählen Sie diesen Wert entsprechend dem Operativ-Schlüssel für die LAG.</p>
LACP actor admin state	<p>Legt die Administrativ-Werte für den in LACPDUs vermittelten Actor-Status fest. Sie haben die Möglichkeit, die Werte miteinander zu kombinieren. Dies bietet Ihnen die Möglichkeit, die LACPDU-Parameter administrativ zu verwalten. Wählen Sie in der Dropdown-Liste einen oder mehrere Werte.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ lacpActivity Legt fest, ob der Port aktiver oder passiver Teilnehmer ist. Ein aktiver Teilnehmer übermittelt LACPDUs periodisch. Ein passiver Teilnehmer übermittelt LACPDUs auf Anfrage. Wenn Sie die Option wählen, setzen Sie den Parameter auf aktiven Teilnehmer. ▶ lacpTimeout Der Actor übermittelt periodisch LACPDUs in Abhängigkeit von den Einstellungen des Partners entweder mit hoher oder mit niedriger Übertragungsrage. Sie setzen den Parameter entweder auf langes Timeout oder auf kurzes Timeout. Wenn Sie die Option wählen, setzen Sie den Parameter auf kurzes Timeout. ▶ aggregation Legt fest, ob der Port ein möglicher Kandidat für Aggregation oder für eine individuelle Datenverbindung ist. Wenn Sie die Option wählen, setzen Sie den Parameter auf aggregierbar. ▶ - Der Status ist nicht festgelegt. <p>Wenn der Parameter nicht festgelegt ist, zeigt das Gerät folgende Werte für die LACPDU-Parameter:</p> <ul style="list-style-type: none"> - synchronization Das System sieht diese Datenverbindung als der korrekten LAG zugewiesen an und die Gruppe ist mit einem kompatiblen Aggregator verknüpft. Außerdem ist die Identität der LAG konsistent mit der System-ID und der Information über den Operativ-Schlüssel. - collecting Die Sammlung von eingehenden Datenpaketen auf dieser Datenverbindung ist definitiv eingeschaltet. Die Sammlung ist beispielsweise gegenwärtig eingeschaltet und bleibt eingeschaltet, wenn administrative Änderungen oder Änderungen in der empfangenen Protokollinformation ausbleiben. - distributing Die Verteilung ist gegenwärtig ausgeschaltet und bleibt ausgeschaltet, wenn administrative Änderungen oder Änderungen in der empfangenen Protokoll-Information ausbleiben. - defaulted Die vom Actor empfangenen LACPDUs verwenden die statisch konfigurierte Partner-Information. - expired Die vom Actor empfangenen LACPDUs sind im Status "expired" (verfallen).
LACP actor port priority	<p>Legt die Port-Priorität für den LACP-Actor fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..65535 (Voreinstellung: 128) <p>Der Port mit dem niedrigeren Wert hat die höhere Priorität.</p>

Parameter	Bedeutung
LACP partner port admin key	<p>Legt den voreingestellten Wert für den Partner-Schlüssel fest, der vom Administrator oder durch eine Systemrichtlinie festgelegt ist, wenn die Information über den Partner unbekannt oder abgelaufen ist.</p> <p>Die LAG verwendet Schlüssel, um Partner-Ports die Mitgliedschaft zuzuweisen. Legen Sie für Partner, die in derselben LAG teilnehmen, denselben Schlüsselwert fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..65535 (Voreinstellung: 0) Wenn der Port der einzige einer LAG ist, setzen Sie diesen Wert auf 0. Wenn der Port zu einer LAG gehört, wählen Sie diesen Wert entsprechend dem Operativ-Schlüssel für die LAG. <p>Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten:</p> <ul style="list-style-type: none"> - <i>LACP Partner-Admin-Port</i> - <i>LACP partner admin port priority</i> - <i>LACP partner admin SysID</i> - <i>LACP partner admin sys priority</i>
LACP partner admin state	<p>Legt die Werte für den administrativen Status des Partners fest. Sie haben die Möglichkeit, die Werte miteinander zu kombinieren, was Ihnen die administrative Verwaltung der LACPDU-Parameter ermöglicht. Wählen Sie in der Dropdown-Liste einen oder mehrere Werte.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>lacpActivity</i> Legt fest, ob der Port aktiver oder passiver Teilnehmer ist. Ein aktiver Teilnehmer übermittelt LACPDUs periodisch. Ein passiver Teilnehmer übermittelt LACPDUs auf Anfrage. Wenn Sie die Option wählen, setzen Sie den Parameter auf aktiv. ▶ <i>lacpTimeout</i> Der Actor übermittelt periodisch LACPDUs in Abhängigkeit von den Einstellungen des Partners entweder mit langem oder kurzem Timeout. Wenn Sie die Option wählen, setzen Sie den Parameter auf kurzes Timeout. ▶ <i>aggregation</i> Legt fest, ob der Port ein möglicher Kandidat für Aggregation oder für eine individuelle Datenverbindung ist. Wenn Sie die Option wählen, setzen Sie den Parameter auf aggregierbar. ▶ - Der Status ist nicht festgelegt. <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>synchronization</i> Das System sieht diese Datenverbindung als der korrekten LAG zugewiesen an und die Gruppe ist mit einem kompatiblen Aggregator verknüpft. Außerdem ist die Identität der LAG konsistent mit der System-ID und der Information über den Operativ-Schlüssel. ▶ <i>collecting</i> Die Sammlung von eingehenden Datenpaketen auf dieser Datenverbindung ist definitiv eingeschaltet. Die Sammlung ist beispielsweise gegenwärtig eingeschaltet und bleibt eingeschaltet, wenn administrative Änderungen oder Änderungen in der empfangenen Protokollinformation ausbleiben. ▶ <i>distributing</i> Die Verteilung ist gegenwärtig ausgeschaltet und bleibt ausgeschaltet, wenn administrative Änderungen oder Änderungen in der empfangenen Protokoll-Information ausbleiben. ▶ <i>defaulted</i> Die vom Actor empfangenen LACPDUs verwenden die statisch konfigurierte Partner-Information. ▶ <i>expired</i> Die vom Partner empfangenen LACPDUs sind im Status "expired" (verfallen).
LACP Partner-Admin-Port	<p>Legt die Port-Nummer für den Partner-Port fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..65535 (Voreinstellung: 0) <p>Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten:</p> <ul style="list-style-type: none"> - <i>LACP partner port admin key</i> - <i>LACP partner admin port priority</i> - <i>LACP partner admin SysID</i> - <i>LACP partner admin sys priority</i>

Parameter	Bedeutung
LACP partner admin port priority	<p>Legt die Port-Priorität für den Partner-Port fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..65535 (Voreinstellung: 0) Der Port mit dem niedrigeren Wert hat die höhere Priorität. <p>Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten:</p> <ul style="list-style-type: none"> - <i>LACP partner port admin key</i> - <i>LACP Partner-Admin-Port</i> - <i>LACP partner admin SysID</i> - <i>LACP partner admin sys priority</i>
LACP partner admin SysID	<p>Legt einen Wert für die MAC-Adresse fest, die die Partner-System-ID darstellt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Gültige MAC-Adresse (Voreinstellung: 00:00:00:00:00:00) <p>Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten:</p> <ul style="list-style-type: none"> - <i>LACP partner port admin key</i> - <i>LACP Partner-Admin-Port</i> - <i>LACP partner admin port priority</i> - <i>LACP partner admin sys priority</i>
LACP partner admin sys priority	<p>Legt den voreingestellten Wert für die System-Prioritätskomponente des System Identifiers des Partners fest, der vom Administrator oder der Systemrichtlinie zugewiesen wurde zur Verwendung, falls die Information des Partners unbekannt oder verfallen ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..65535 (Voreinstellung: 0) Der Port mit dem niedrigeren Wert hat die höhere Priorität. <p>Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten:</p> <ul style="list-style-type: none"> - <i>LACP partner port admin key</i> - <i>LACP Partner-Admin-Port</i> - <i>LACP partner admin port priority</i> - <i>LACP partner admin SysID</i>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	<p>Öffnet das Fenster <i>Erzeugen</i>, um der Tabelle einen neuen Eintrag hinzuzufügen.</p> <ul style="list-style-type: none"> ▶ In der Dropdown-Liste <i>Trunk-Port</i> wählen Sie die Port-Nummer für den Trunk der Link-Aggregation-Gruppe. ▶ In der Dropdown-Liste <i>Port</i> wählen Sie den Port, der dem Interface zugewiesen wird.

5.8.6 Link-Backup

Mit Link Backup konfigurieren Sie Paare von redundanten Links. Jedes Paar besteht aus einem primären Port und einem Backup-Port. Der primäre Port leitet Daten weiter, bis das Gerät einen Fehler ermittelt. Wenn das Gerät einen Fehler am primären Port ermittelt, nutzt die Link-Backup-Funktion den Backup-Port zur Vermittlung der Daten.

Der Dialog bietet Ihnen außerdem die Möglichkeit, eine Fail-Back-Funktion einzurichten. Wenn Sie die Fail-Back-Funktion einrichten und der primäre Port in den Normalbetrieb zurückkehrt, blockiert das Gerät zuerst Daten am Backup-Port und leitet dann Daten an den primären Port weiter. Dieses Verfahren hilft zu verhindern, dass das Gerät Loops im Netz verursacht.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die Link-Backup-Funktion global im Gerät ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ An Schaltet die Link-Backup-Funktion ein. ▶ Aus (Voreinstellung) Schaltet die Link-Backup-Funktion aus.

■ Tabelle

Parameter	Bedeutung
Primärer Port	Zeigt den primären Port des Interface-Paares. Wenn Sie die Funktion Link-Backup einschalten, ist dieser Port für die Weiterleitung der Daten verantwortlich. Mögliche Werte: <ul style="list-style-type: none"> ▶ Physikalische Ports
Backup-Port	Zeigt den Backup-Port, an den das Gerät die Daten vermittelt, wenn es am primären Port einen Fehler ermittelt hat. Mögliche Werte: <ul style="list-style-type: none"> ▶ Physikalische Ports außer dem Port, den Sie als primären Port festlegen.
Beschreibung	Legt das Link-Backup-Paar fest. Geben Sie einen Namen ein, der das Backup-Paar identifiziert. Mögliche Werte: <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
Status Primärer Port	Zeigt den Status des primären Ports für dieses Link-Backup-Paar. Mögliche Werte: <ul style="list-style-type: none"> ▶ forwarding Der Link ist vorhanden, keine Abschaltung, Datenweiterleitung ▶ blocking Der Link ist vorhanden, keine Abschaltung, Blockierung der Daten ▶ down Am Port ist entweder der Link ausgefallen oder in der Software ausgeschaltet oder das Kabel ist entfernt, Abschaltung. ▶ unbekannt Die Link-Backup-Funktion ist global ausgeschaltet, oder das Port-Paar ist deaktiviert. Daher ignoriert das Gerät die Einstellungen für das Port-Paar.

Parameter	Bedeutung
Status Backup-Port	<p>Zeigt den Status des Backup-Ports für dieses Link-Backup-Paar.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ forwarding Der Link ist vorhanden, keine Abschaltung, Datenweiterleitung ▶ blocking Der Link ist vorhanden, keine Abschaltung, Blockierung der Daten ▶ down Am Port ist entweder der Link ausgefallen oder in der Software ausgeschaltet oder das Kabel ist entfernt, Abschaltung. ▶ unbekannt Die Link-Backup-Funktion ist global ausgeschaltet, oder das Port-Paar ist deaktiviert. Daher ignoriert das Gerät die Einstellungen für das Port-Paar.
Fail back	<p>Aktiviert/deaktiviert die automatische Fail-Back-Funktion.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Die automatische Fail-Back-Funktion ist aktiv. Nach Ablauf des Verzögerungszeit wechselt der Backup-Port zu <code>blocking</code> und der primäre Port wechselt zu <code>forwarding</code>. ▶ unmarkiert Die automatische Fail-Back-Funktion ist inaktiv. Der Backup-Port leitet Daten auch weiter, nachdem der primäre Port einen Link wiederherstellt oder Sie den Admin-Status des primären Ports manuell von <code>shutdown</code> zu <code>no shutdown</code> geändert haben.
Fail-Back-Verzögerung [s]	<p>Legt die Wartezeit in Sekunden fest, die das Gerät wartet, nachdem der primäre Port einen Link wiederhergestellt hat. Zudem wird der Timer aktiv, wenn Sie den Admin-Status des primären Ports manuell von <code>shutdown</code> zu <code>no shutdown</code> ändern. Nach Ablauf des Verzögerungszeit wechselt der Backup-Port zu <code>blocking</code> und der primäre Port wechselt zu <code>forwarding</code>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..3600 (Voreinstellung: 30) <p>Bei 0 wechselt der Backup-Port unmittelbar nachdem der primäre Port einen Link wiederhergestellt hat, zu <code>blocking</code> und der primäre Port wechselt zu <code>forwarding</code>. Unmittelbar nachdem Sie den Port-Status manuell von <code>shutdown</code> zu <code>no shutdown</code> ändern, wechselt der Backup-Port zu <code>blocking</code> und der primäre Port zu <code>forwarding</code>.</p>
Aktiv	<p>Aktiviert/deaktiviert die Konfiguration für das Link-Backup-Paar.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Das Link-Backup-Paar ist aktiviert. Das Gerät ermittelt den Link- und Administration-Status und leitet die Daten entsprechend der Paar-Konfiguration weiter. ▶ unmarkiert (Voreinstellung) Das Link-Backup-Paar ist deaktiviert. Die Ports leiten die Daten entsprechend den Grundeinstellungen weiter.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

■ Erzeugen

Parameter	Bedeutung
Primärer Port	<p>Legt den primären Port des Backup-Interface-Paares fest. Im Normalbetrieb ist dieser Port verantwortlich für die Weiterleitung der Daten.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Physikalische Ports

Parameter	Bedeutung
Backup-Port	Legt den Backup-Port fest, an den das Gerät die Daten vermittelt, wenn es am primären Port einen Fehler ermittelt. Mögliche Werte: ▶ Physikalische Ports außer dem Port, den Sie als primären Port festlegen.

6 Diagnose

Das Menü enthält die folgenden Dialoge:

- ▶ [Statuskonfiguration](#)
- ▶ [System](#)
- ▶ [Syslog](#)
- ▶ [Ports](#)
- ▶ [LLDP](#)
- ▶ [Bericht](#)

6.1 Statuskonfiguration

Das Menü enthält die folgenden Dialoge:

- ▶ [Gerätestatus](#)
- ▶ [Sicherheitsstatus](#)
- ▶ [Alarme \(Traps\)](#)

6.1.1 Gerätestatus

Der Gerätstatus gibt einen Überblick über den Gesamtzustand des Geräts. Viele Prozessvisualisierungssysteme erfassen den Gerätstatus eines Geräts, um dessen Zustand grafisch darzustellen.

Das Gerät zeigt seinen gegenwärtigen Status als `error` oder `ok` im Rahmen *Geräte-Status*. Das Gerät bestimmt diesen Status aus den einzelnen Überwachungsergebnissen.

Das Gerät zeigt ermittelte Fehler in der Registerkarte *Status* und zusätzlich im Dialog *Grundeinstellungen > System*, Rahmen *Gerätestatus*.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [Global]
- ▶ [Port]
- ▶ [Status]

[Global]

■ Geräte-Status

Parameter	Bedeutung
Geräte-Status	<p>Zeigt den gegenwärtigen Status des Geräts. Das Gerät bestimmt den Status aus den einzelnen überwachten Parametern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>error</code> Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen.▶ <code>ok</code>

■ Traps

Parameter	Bedeutung
Trap senden	<p>Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Änderungen an den überwachten Funktionen erkennt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Das Senden von SNMP-Traps ist aktiv. Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.▶ <code>unmarkiert</code> (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv. <p>Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose</i> > <i>Statuskonfiguration</i> > <i>Alarme (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen.</p>

■ Tabelle

Parameter	Bedeutung
Ring-Redundanz	<p>Aktiviert/deaktiviert die Überwachung der Ring-Redundanz.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Die Überwachung ist aktiv. In folgenden Situationen wechselt der Wert im Rahmen <i>Geräte-Status</i> auf <code>error</code>:<ul style="list-style-type: none">– Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve).– Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen.▶ <code>unmarkiert</code> (Voreinstellung) Die Überwachung ist inaktiv.
Verbindungsfehler	<p>Aktiviert/deaktiviert die Überwachung des Links auf den Ports/Interfaces.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>markiert</code> Die Überwachung ist aktiv. Der Wert im Rahmen <i>Geräte-Status</i> wechselt auf <code>error</code>, wenn der Link auf einem überwachten Port/Interface abbricht. In der Registerkarte <i>Port</i> haben Sie die Möglichkeit, die zu überwachenden Ports/Interfaces einzeln auszuwählen.▶ <code>unmarkiert</code> (Voreinstellung) Die Überwachung ist inaktiv.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Port]

■ Tabelle

Parameter	Bedeutung
Verbindungsfehler melden	<p>Aktiviert/deaktiviert die Überwachung des Links auf dem Port/Interface.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ markiert Die Überwachung ist aktiv. Der Wert im Rahmen <i>Geräte-Status</i> wechselt auf <code>error</code>, wenn der Link auf einem überwachten Port/Interface abbricht.▶ unmarkiert (Voreinstellung) Die Überwachung ist inaktiv. <p>Die Einstellung ist wirksam, wenn Sie in der Registerkarte <i>Global</i> das Kontrollkästchen <i>Verbindungsfehler</i> markieren.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Status]

■ Tabelle

Parameter	Bedeutung
Zeitstempel	Zeigt das Datum und die Uhrzeit des Ereignisses im Format Tag.Monat.Jahr hh:mm:ss.
Ursache	Zeigt das Ereignis, das den SNMP-Trap ausgelöst hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

6.1.2 Sicherheitsstatus

Dieser Dialog gibt einen Überblick über den Zustand der sicherheitsrelevanten Einstellungen im Gerät.

Das Gerät zeigt seinen gegenwärtigen Status als `error` oder `ok` im Rahmen *Sicherheits-Status*.

Das Gerät bestimmt diesen Status aus den einzelnen Überwachungsergebnissen.

Das Gerät zeigt ermittelte Fehler in der Registerkarte *Status* und zusätzlich im Dialog *Grundeinstellungen > System*, Rahmen *Sicherheits-Status*.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [\[Global\]](#)
- ▶ [\[Port\]](#)
- ▶ [\[Status\]](#)

[Global]

■ Sicherheits-Status

Parameter	Bedeutung
Sicherheits-Status	<p>Zeigt den gegenwärtigen Status der sicherheitsrelevanten Einstellungen im Gerät. Das Gerät bestimmt den Status aus den einzelnen überwachten Parametern.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>error</code> Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen. ▶ <code>ok</code>

■ Traps

Parameter	Bedeutung
Trap senden	<p>Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Änderungen an den überwachten Funktionen erkennt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Das Senden von SNMP-Traps ist aktiv. Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt. ▶ <code>unmarkiert</code> (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv. <p>Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose > Statuskonfiguration > Alarme (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen.</p>

■ Tabelle

Parameter	Bedeutung
Passwort-Voreinstellung unverändert	<p>Aktiviert/deaktiviert die Überwachung des Passworts für die lokal eingerichteten Benutzerkonten <code>user</code> und <code>admin</code>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn Sie für die Benutzerkonten <code>user</code> oder <code>admin</code> das voreingestellte Passwort unverändert verwenden. ▶ <code>unmarkiert</code> Die Überwachung ist inaktiv. <p>Das Passwort legen Sie fest im Dialog <i>Gerätesicherheit > Benutzerverwaltung</i>.</p>
Min. Passwort-Länge < 8	<p>Aktiviert/deaktiviert die Überwachung der Richtlinie <i>Min. Passwort-Länge</i>.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn für die Richtlinie <i>Min. Passwort-Länge</i> ein Wert kleiner als 8 festgelegt ist. ▶ <code>unmarkiert</code> Die Überwachung ist inaktiv. <p>Die Richtlinie für die <i>Min. Passwort-Länge</i> legen Sie fest im Dialog <i>Gerätesicherheit > Benutzerverwaltung</i>, Rahmen <i>Konfiguration</i>.</p>

Parameter	Bedeutung
Passwort-Richtlinien deaktiviert	<p>Aktiviert/deaktiviert die Überwachung der Passwort-Richtlinien-Einstellungen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn für die Richtlinie ein Wert kleiner als 1 festgelegt ist. <ul style="list-style-type: none"> – <i>Großbuchstaben (min.)</i> – <i>Kleinbuchstaben (min.)</i> – <i>Ziffern (min.)</i> – <i>Sonderzeichen (min.)</i> ▶ unmarkiert Die Überwachung ist inaktiv. <p>Die Einstellungen für die Richtlinie legen Sie fest im Dialog <i>Gerätesicherheit</i> > Benutzerverwaltung, Rahmen <i>Passwort-Richtlinien</i>.</p>
Prüfen der Passwort-Richtlinien im Benutzerkonto deaktiviert	<p>Aktiviert/deaktiviert die Überwachung der <i>Richtlinien überprüfen</i>-Funktion.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn die Funktion <i>Richtlinien überprüfen</i> bei mindestens 1 Benutzerkonto inaktiv ist. ▶ unmarkiert (Voreinstellung) Die Überwachung ist inaktiv. <p>Die Funktion <i>Richtlinien überprüfen</i> aktivieren Sie im Dialog <i>Gerätesicherheit</i> > Benutzerverwaltung.</p>
Telnet-Server aktiv	<p>Aktiviert/deaktiviert die Überwachung des Telnet-Servers.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn Sie den Telnet-Server einschalten. ▶ unmarkiert Die Überwachung ist inaktiv. <p>Den Telnet-Server schalten Sie ein/aus im Dialog <i>Gerätesicherheit</i> > <i>Management-Zugriff</i> > <i>Server</i>, Registerkarte <i>Telnet</i>.</p>
HTTP-Server aktiv	<p>Aktiviert/deaktiviert die Überwachung des HTTP-Servers.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn Sie den HTTP-Server einschalten. ▶ unmarkiert Die Überwachung ist inaktiv. <p>Den HTTP-Server schalten Sie ein/aus im Dialog <i>Gerätesicherheit</i> > <i>Management-Zugriff</i> > <i>Server</i>, Registerkarte <i>HTTP</i>.</p>

Parameter	Bedeutung
SNMP unverschlüsselt	<p>Aktiviert/deaktiviert die Überwachung des SNMP-Servers.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn mindestens eine der folgenden Bedingungen zutrifft: <ul style="list-style-type: none"> – Die <i>SNMPv1</i>-Funktion ist eingeschaltet. – Die <i>SNMPv2</i>-Funktion ist eingeschaltet. – Die Verschlüsselung für SNMPv3 ist ausgeschaltet. Die Verschlüsselung schalten Sie ein im Dialog <i>Gerätesicherheit</i> > Benutzerverwaltung, Spalte <i>SNMP-Verschlüsselung</i>. ▶ <code>unmarkiert</code> Die Überwachung ist inaktiv. <p>Die Einstellungen für den SNMP-Agenten legen Sie fest im Dialog <i>Gerätesicherheit</i> > Management-Zugriff > <i>Server</i>, Registerkarte <i>SNMP</i>.</p>
Zugriff auf System-Monitor mit V.24 möglich	<p>Aktiviert/deaktiviert die Überwachung des System-Monitors. Wenn der System-Monitor aktiviert ist, hat der Benutzer die Möglichkeit, während des Starts des Geräts über eine V.24-Verbindung in den System-Monitor zu wechseln.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn der System-Monitor aktiviert ist. ▶ <code>unmarkiert</code> (Voreinstellung) Die Überwachung ist inaktiv. <p>Den System-Monitor aktivieren/deaktivieren Sie im Dialog <i>Diagnose</i> > <i>System</i> > <i>Selbsttest</i>.</p>
Verbindungsabbruch auf eingeschalteten Ports	<p>Aktiviert/deaktiviert die Überwachung des Links auf den aktiven Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn der Link auf einem aktiven Port abbricht. In der Registerkarte <i>Port</i> haben Sie die Möglichkeit, die zu überwachenden Ports einzeln auszuwählen. ▶ <code>unmarkiert</code> (Voreinstellung) Die Überwachung ist inaktiv.
Zugriff mit HiDiscovery möglich	<p>Aktiviert/deaktiviert die Überwachung der HiDiscovery-Funktion.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn Sie die HiDiscovery-Funktion einschalten. ▶ <code>unmarkiert</code> Die Überwachung ist inaktiv. <p>Die HiDiscovery-Funktion schalten Sie im Dialog <i>Grundeinstellungen</i> > <i>Netz</i> ein/aus.</p>
IEC61850-MMS aktiv	<p>Aktiviert/deaktiviert die Überwachung der <i>IEC61850-MMS</i>-Funktion.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn Sie die <i>IEC61850-MMS</i>-Funktion einschalten. ▶ <code>unmarkiert</code> Die Überwachung ist inaktiv. <p>Die <i>IEC61850-MMS</i>-Funktion schalten Sie im Dialog <i>Industrie-Protokolle</i> > <i>IEC61850-MMS</i>, Rahmen <i>Funktion</i> ein/aus.</p>

Parameter	Bedeutung
Modbus TCP aktiv	<p>Aktiviert/deaktiviert die Überwachung der <i>Modbus TCP</i>-Funktion.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>markiert</i> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i>, wenn Sie die <i>Modbus TCP</i>-Funktion einschalten. ▶ <i>unmarkiert</i> Die Überwachung ist inaktiv. <p>Die <i>Modbus TCP</i>-Funktion schalten Sie im Dialog <i>Erweitert</i> > <i>Industrie-Protokolle</i> > <i>Modbus TCP</i>, Rahmen <i>Funktion</i> ein/aus.</p>
EtherNet/IP aktiv	<p>Aktiviert/deaktiviert die Überwachung der <i>EtherNet/IP</i>-Funktion.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>markiert</i> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i>, wenn Sie die <i>EtherNet/IP</i>-Funktion einschalten. ▶ <i>unmarkiert</i> Die Überwachung ist inaktiv. <p>Die <i>EtherNet/IP</i>-Funktion schalten Sie im Dialog <i>Erweitert</i> > <i>Industrie-Protokolle</i> > <i>EtherNet/IP</i>, Rahmen <i>Funktion</i> ein/aus.</p>
PROFINET aktiv	<p>Aktiviert/deaktiviert die Überwachung der <i>PROFINET</i>-Funktion.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>markiert</i> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i>, wenn Sie die <i>PROFINET</i>-Funktion einschalten. ▶ <i>unmarkiert</i> Die Überwachung ist inaktiv. <p>Die <i>PROFINET</i>-Funktion schalten Sie im Dialog <i>Erweitert</i> > <i>Industrie-Protokolle</i> > <i>PROFINET</i>, Rahmen <i>Funktion</i> ein/aus.</p>
Self-signed HTTPS-Zertifikat vorhanden	<p>Aktiviert/deaktiviert die Überwachung des HTTPS-Zertifikats.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <i>markiert</i> (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i>, wenn der HTTPS-Server ein selbst erzeugtes digitales Zertifikat verwendet. ▶ <i>unmarkiert</i> Die Überwachung ist inaktiv.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Port]

■ Tabelle

Parameter	Bedeutung
Verbindungsabbruch auf eingeschalteten Ports	<p>Aktiviert/deaktiviert die Überwachung des Links auf den aktiven Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Die Überwachung ist aktiv. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <code>error</code>, wenn der Port eingeschaltet ist (Dialog <i>Grundeinstellungen</i> > <i>Port</i>, Registerkarte <i>Konfiguration</i>, Kontrollkästchen <i>Port an</i> ist markiert) und wenn der Link auf dem Port abbricht. ▶ <code>unmarkiert</code> (Voreinstellung) Die Überwachung ist inaktiv. <p>Diese Einstellung ist wirksam, wenn Sie im Dialog <i>Diagnose</i> > <i>Statuskonfiguration</i> > <i>Sicherheitsstatus</i>, Registerkarte <i>Global</i>, das Kontrollkästchen <i>Verbindungsabbruch auf eingeschalteten Ports</i> markieren.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Status]

■ Tabelle

Parameter	Bedeutung
Zeitstempel	Zeigt das Datum und die Uhrzeit des Ereignisses im Format Tag.Monat.Jahr hh:mm:ss.
Ursache	Zeigt das Ereignis, das den SNMP-Trap ausgelöst hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

6.1.3 Alarme (Traps)

Das Gerät bietet Ihnen die Möglichkeit, als Reaktion auf bestimmte Ereignisse einen SNMP-Trap zu senden. In diesem Dialog legen Sie die Trap-Ziele fest, an die das Gerät die SNMP-Traps sendet.

Die Ereignisse, bei denen das Gerät einen SNMP-Trap auslöst, legen Sie zum Beispiel in den folgenden Dialogen fest:

- ▶ im Dialog *Diagnose > Statuskonfiguration > Gerätestatus*
- ▶ im Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*

■ Funktion


Parameter	Bedeutung
Funktion	Schaltet das Senden von SNMP-Traps an die Trap-Ziele ein/aus. Mögliche Werte: ▶ An (Voreinstellung) Das Senden von SNMP-Traps ist eingeschaltet. ▶ Aus Das Senden von SNMP-Traps ist ausgeschaltet.

■ Tabelle

Parameter	Bedeutung
Name	Legt die Bezeichnung des Trap-Ziels fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
Adresse	Legt die IP-Adresse und die Port-Nummer des Trap-Ziels fest. Mögliche Werte: ▶ <Gültige IPv4-Adresse>:<Port-Nummer>
Aktiv	Aktiviert/deaktiviert das Senden von SNMP-Traps an dieses Trap-Ziel. Mögliche Werte: ▶ markiert (Voreinstellung) Das Senden von SNMP-Traps an das Trap-Ziel ist aktiv. ▶ unmarkiert Das Senden von SNMP-Traps an das Trap-Ziel ist inaktiv.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Öffnet das Fenster <i>Erzeugen</i> , um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld <i>Name</i> legen Sie eine Bezeichnung für das Trap-Ziel fest. ▶ Im Feld <i>Adresse</i> legen Sie die IP-Adresse und die Port-Nummer des Trap-Ziels fest. Wenn Sie auf die Eingabe der Port-Nummer verzichten, fügt das Gerät automatisch die Port-Nummer 162 hinzu.

6.2 System

Das Menü enthält die folgenden Dialoge:


- ▶ Systeminformationen
- ▶ Hardware-Zustand
- ▶ Konfigurations-Check
- ▶ IP-Adressen Konflikterkennung
- ▶ ARP
- ▶ Selbsttest

6.2.1 Systeminformationen

Dieser Dialog zeigt den gegenwärtigen Betriebszustand einzelner Komponenten im Gerät. Die angezeigten Werte sind ein Schnappschuss, sie repräsentieren den Betriebszustand zum Zeitpunkt, zu dem der Dialog die Seite geladen hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Systeminformationen speichern	Öffnet die HTML-Seite in einem neuen Web-Browser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Web-Browser-Befehl auf Ihrem PC speichern.

6.2.2 Hardware-Zustand

Dieser Dialog gibt Auskunft über Aufteilung und Zustand des Flash-Speichers des Geräts.

■ Information

Parameter	Bedeutung
Betriebszeit	Zeigt die Gesamtbetriebszeit des Geräts seit Lieferung. Mögliche Werte: ▶ ..d ..h ..m ..s Tag(e) Stunde(n) Minute(n) Sekunde(n)

■ Tabelle

Parameter	Bedeutung
Flash-Region	Zeigt die Bezeichnung des jeweiligen Speicherbereichs.
Beschreibung	Zeigt eine Beschreibung, wofür das Gerät den Speicherbereich verwendet.
Flash-Sektoren	Zeigt, wie viele Sektoren dem Speicherbereich zugewiesen sind.
Lösch-Vorgänge	Zeigt, wie viele Male das Gerät die Sektoren des Speicherbereichs überschrieben hat.


■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.


6.2.3 Konfigurations-Check

Das Gerät bietet Ihnen die Möglichkeit, die Einstellungen im Gerät mit den Einstellungen seiner Nachbargeräte zu vergleichen. Dazu verwendet das Gerät die Informationen, die es mittels Topologie-Erkennung (LLDP) von seinen Nachbargeräten empfangen hat.

Der Dialog listet die erkannten Abweichungen auf, die die Leistungsfähigkeit der Kommunikation zwischen dem Gerät und den erkannten Nachbargeräten beeinflussen.

Durch Klicken der Schaltfläche  aktualisieren Sie den Inhalt der Tabelle. Bleibt die Tabelle leer, war der Konfigurations-Check erfolgreich und die Einstellungen im Gerät sind kompatibel zu den Einstellungen in den erkannten Nachbargeräten.

■ Zusammenfassung

Außerdem finden Sie diese Informationen, wenn Sie in der Symbolleiste im oberen Bereich des Navigationsbereichs den Mauszeiger über der Schaltfläche  positionieren.

Parameter	Bedeutung
Fehler	Zeigt die Anzahl der Fehler, die das Gerät beim Konfigurations-Check erkannt hat.
Warnung	Zeigt die Anzahl der Warnungen, die das Gerät beim Konfigurations-Check erkannt hat.
Information	Zeigt die Anzahl der Informationen, die das Gerät beim Konfigurations-Check erkannt hat.

■ Tabelle

Sobald Sie in der Tabelle eine Zeile auswählen, zeigt das Gerät im darunterliegenden Bereich weitere Informationen an.

Parameter	Bedeutung
ID	Zeigt die Regel-ID der aufgetretenen Abweichungen. Der Dialog fasst mehrere Abweichungen mit der gleichen Regel-ID unter einer Regel-ID zusammen.
Level	<p>Zeigt den Grad der Abweichung zwischen den Einstellungen dieses Geräts und den Einstellungen der erkannten Nachbargeräte.</p> <p>Das Gerät unterscheidet die folgenden Zustände:</p> <ul style="list-style-type: none"> ▶ INFORMATION Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten ist nicht beeinträchtigt. ▶ WARNING Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten kann beeinträchtigt sein. ▶ ERROR Die Kommunikation zwischen den beiden Geräten ist beeinträchtigt.
Nachricht	Der Dialog zeigt die aufgetretenen Informationen, Warnungen und Fehler etwas präziser.

Anmerkung: Der Dialog zeigt die am Nachbargerät angeschlossenen erkannten Geräte so an, als wären sie direkt am Gerät angeschlossen.

Anmerkung: Wenn im Gerät mehr als 39 VLANeingerichtet sind, dann zeigt der Dialog stets eine Warnung. Der Grund ist die begrenzte Anzahl der möglichen VLAN-Informationen in LLDP-Paketen mit begrenzter Länge. Das Gerät vergleicht die ersten 39 VLANs automatisch.

Wenn im Gerät 40 oder mehr VLANs eingerichtet sind, dann prüfen Sie die Übereinstimmung der weiteren VLANs gegebenenfalls manuell.

■ **Schaltflächen**

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

6.2.4 IP-Adressen Konflikterkennung

Mit der *IP-Adressen Konflikterkennung*-Funktion prüft das Gerät, ob ein weiteres Gerät im Netz die eigene IP-Adresse verwendet. Zu diesem Zweck analysiert das Gerät empfangene ARP-Pakete.

In diesem Dialog legen Sie das Verfahren fest, mit dem das Gerät Adresskonflikte erkennt und legen die erforderlichen Einstellungen dafür fest.

Das Gerät zeigt erkannte Adresskonflikte in der Tabelle.

■ Funktion

Parameter	Bedeutung
Funktion	<p>Schaltet die <i>IP-Adressen Konflikterkennung</i>-Funktion ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An (Voreinstellung) Die <i>IP-Adressen Konflikterkennung</i>-Funktion ist eingeschaltet. Das Gerät prüft, ob ein weiteres Gerät im Netz die eigene IP-Adresse verwendet. ▶ Aus Die <i>IP-Adressen Konflikterkennung</i>-Funktion ist ausgeschaltet.

■ Konfiguration

Parameter	Bedeutung
Erkennungs-Modus	<p>Legt das Verfahren fest, mit dem das Gerät Adresskonflikte erkennt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ aktiv und passiv (Voreinstellung) Das Gerät verwendet aktive und passive Adresskonflikt-Erkennung. ▶ aktiv Aktive Adresskonflikt-Erkennung. Das Gerät vermeidet aktiv, dass es mit einer bereits im Netz vorhandenen IP-Adresse kommuniziert. Die Adresskonflikt-Erkennung beginnt, sobald Sie das Gerät ans Netz anschließen oder seine IP-Parameter ändern. <ul style="list-style-type: none"> – Das Gerät sendet 4 ARP-Probe-Datenpakete mit dem im Feld <i>Erkennungs-Verzögerung [ms]</i> festgelegten zeitlichen Abstand. Empfängt das Gerät auf diese Datenpakete eine Antwort, liegt ein Adresskonflikt vor. – Erkennt das Gerät keinen Adresskonflikt, sendet es 2 Gratuitous-ARP-Datenpakete als Announcement. Diese Datenpakete sendet das Gerät auch dann, wenn die Adresskonflikt-Erkennung ausgeschaltet ist. – Ist die IP-Adresse bereits im Netz vorhanden, wechselt das Gerät zurück zu den zuvor verwendeten IP-Parametern (falls möglich). Erhält das Gerät seine IP-Parameter von einem DHCP-Server, sendet es eine DHCPDECLINE-Nachricht an den DHCP-Server zurück. – Das Gerät prüft jeweils nach der im Feld <i>Rückfallverzögerung [s]</i> festgelegten Zeit, ob der Adresskonflikt weiterhin besteht. Erkennt das Gerät 10 Adresskonflikte nacheinander, verlängert es die Wartezeit bis zur nächsten Prüfung auf 60 s. – Sobald der Adresskonflikt behoben ist, geht das Management des Geräts wieder ans Netz. ▶ passiv Passive Adresskonflikt-Erkennung. Das Gerät analysiert den Datenverkehr im Netz. Wenn ein weiteres Gerät im Netz die eigene IP-Adresse verwendet, „verteidigt“ das Gerät seine IP-Adresse zunächst. Das Gerät hört auf zu senden, wenn anschließend das andere Gerät weiter mit derselben IP-Adresse sendet. <ul style="list-style-type: none"> – Zur „Verteidigung“ sendet das Gerät Gratuitous-ARP-Datenpakete. Diesen Vorgang wiederholt das Gerät sooft wie im Feld <i>Address-Protections</i> festgelegt. – Sendet das andere Gerät weiter mit derselben IP-Adresse, prüft das Gerät zyklisch jeweils nach der im Feld <i>Rückfallverzögerung [s]</i> festgelegten Zeit, ob der Adresskonflikt weiterhin besteht. – Sobald der Adresskonflikt behoben ist, geht das Management des Geräts wieder ans Netz.
Periodische ARP-Überprüfung senden	<p>Schaltet die periodische Adresskonflikt-Erkennung ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Die periodische Adresskonflikt-Erkennung ist eingeschaltet. <ul style="list-style-type: none"> – Das Gerät sendet jeweils nach 90 bis 150 Sekunden ein ARP-Probe-Datenpaket und wartet solange wie im Feld <i>Erkennungs-Verzögerung [ms]</i> festgelegt auf Antwort. – Erkennt das Gerät einen Adresskonflikt, wendet es die Funktionen des passiven Erkennungsmodus an. Wenn die Funktion <i>Trap senden</i> eingeschaltet ist, sendet das Gerät einen SNMP-Trap. ▶ unmarkiert Die periodische Adresskonflikt-Erkennung ist ausgeschaltet.
Erkennungs-Verzögerung [ms]	<p>Legt die Zeitspanne in Millisekunden fest, in der das Gerät nach dem Senden eines ARP-Datenpakets auf Antwort wartet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 20..500 (Voreinstellung: 200)
Rückfallverzögerung [s]	<p>Legt die Zeit in Sekunden fest, nach der das Gerät erneut prüft, ob der Adresskonflikt weiterhin besteht.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 3..3600 (Voreinstellung: 15)
Address-Protections	<p>Legt fest, wie viele Male das Gerät im passiven Erkennungsmodus zum „Verteidigen“ seiner IP-Adresse Gratuitous-ARP-Datenpakete sendet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0..100 (Voreinstellung: 3)

Parameter	Bedeutung
Protektions-Intervall [ms]	Legt die Zeit in Millisekunden fest, nach der das Gerät im passiven Erkennungsmodus zum „Verteidigen“ seiner IP-Adresse erneut Gratuitous-ARP-Datenpakete sendet. Mögliche Werte: ▶ 20..5000 (Voreinstellung: 200)
Trap senden	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Adresskonflikte erkennt. Mögliche Werte: ▶ <code>markiert</code> Das Senden von SNMP-Traps ist aktiv. Das Gerät sendet einen SNMP-Trap, wenn es einen Adresskonflikt erkennt. ▶ <code>unmarkiert</code> (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose</i> > Statuskonfiguration > <i>Alarme (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen.

■ Information

Parameter	Bedeutung
Konflikt erkannt	Zeigt, ob gegenwärtig ein Adresskonflikt besteht. Mögliche Werte: ▶ <code>markiert</code> Das Gerät erkennt einen Adresskonflikt. ▶ <code>unmarkiert</code> Das Gerät erkennt keinen Adresskonflikt.

■ Tabelle

Parameter	Bedeutung
Zeitstempel	Zeigt den Zeitpunkt, zu dem das Gerät einen Adresskonflikt erkannt hat.
Port	Zeigt die Nummer des Ports, an dem das Gerät den Adresskonflikt erkannt hat.
IP-Adresse	Zeigt die IP-Adresse, die den Adresskonflikt hervorruft.
MAC-Adresse	Zeigt die MAC-Adresse des Geräts, mit dem der Adresskonflikt besteht.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

6.2.5 ARP


Dieser Dialog zeigt die MAC- und IP-Adressen der Nachbargeräte, die mit dem Management des Geräts verbunden sind.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
IP-Adresse	Zeigt die IP-Adresse eines Geräts, das auf eine ARP-Anfrage an diesem Port geantwortet hat.
MAC-Adresse	Zeigt die MAC-Adresse eines Geräts, das auf eine ARP-Anfrage an diesem Port geantwortet hat.
Letztes Update	Zeigt die Zeit in Sekunden, seit der die gegenwärtigen Einstellungen des Eintrags in der ARP-Tabelle eingetragen sind.
Typ	Zeigt die Art des ARP-Eintrags. Mögliche Werte: <ul style="list-style-type: none">▶ <code>static</code> Statischer ARP-Eintrag. Der ARP-Eintrag bleibt nach dem Löschen der ARP-Tabelle erhalten.▶ <code>dynamic</code> Dynamischer ARP-Eintrag. Das Gerät löscht den ARP-Eintrag nach Überschreiten der <i>Aging-Time [s]</i>, falls das Gerät während dieser Zeit keine Daten von diesem Gerät empfängt.▶ <code>local</code> IP- und MAC-Adresse des Geräte-Managements.
Aktiv	Zeigt, dass die ARP-Tabelle die IP/MAC-Adresszuweisung als aktiven Eintrag enthält.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
ARP-Tabelle zurücksetzen	Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

6.2.6 Selbsttest

Dieser Dialog bietet Ihnen die folgenden Möglichkeiten:

- ▶ RAM-Test während des Starts des Geräts aktivieren/deaktivieren.
- ▶ Während des Systemstarts das Wechseln in den System-Monitor ermöglichen/unterbinden.
- ▶ Festlegen, wie sich das Gerät im Fehlerfall verhält.

■ Konfiguration

Parameter	Bedeutung
RAM test	<p>Aktiviert/deaktiviert den RAM-Speicher-Test während des Neustarts.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Der RAM-Speicher-Test ist aktiviert. Während des Neustarts testet das Gerät den RAM-Speicher. ▶ <code>unmarkiert</code> Der RAM-Speicher-Test ist deaktiviert. Dies verkürzt die Startzeit des Geräts.
SysMon1 ist verfügbar	<p>Aktiviert/deaktiviert den Zugang zum System-Monitor während des Neustarts.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Das Gerät bietet Ihnen die Möglichkeit, während des Neustarts in den System-Monitor zu wechseln. ▶ <code>unmarkiert</code> Das Gerät startet ohne die Möglichkeit, in den System-Monitor zu wechseln. <p>Der System-Monitor bietet Ihnen u. a. die Möglichkeit, die Gerätsoftware zu aktualisieren und gespeicherte Konfigurationsprofile zu löschen.</p>
Bei Fehler Default-Konfiguration laden	<p>Aktiviert/deaktiviert das Laden der Werkseinstellungen, falls das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> (Voreinstellung) Das Gerät lädt die Werkseinstellungen. ▶ <code>unmarkiert</code> Das Gerät bricht den Neustart ab und hält an. Der Management-Zugriff auf das Gerät ist ausschließlich mit dem CLI über die V.24-Schnittstelle möglich. Um das Gerät wieder über das Netz erreichbar zu machen, wechseln Sie in den System-Monitor und setzen die Einstellungen zurück. Das Gerät lädt die Werkseinstellungen beim nächsten Neustart.

Anmerkung: Die folgenden Einstellungen sperren Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Neustart kein lesbares Konfigurationsprofil findet. Dies ist zum Beispiel dann der Fall, wenn sich das Passwort des zu ladenden Konfigurationsprofils von dem im Gerät festgelegten Passwort unterscheidet.

- ▶ Kontrollkästchen *SysMon1 ist verfügbar* ist unmarkiert.
- ▶ Kontrollkästchen *Bei Fehler Default-Konfiguration laden* ist unmarkiert.

Um das Gerät wieder entsperren zu lassen, wenden Sie sich an Ihren Vertriebspartner.

■ Tabelle

In dieser Tabelle legen Sie fest, wie sich das Gerät im Fehlerfall verhält.

Parameter	Bedeutung
Ursache	<p>Fehlerursachen, auf die das Gerät reagiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>task</code> Das Gerät erkennt Fehler in ausgeführten Anwendungen, zum Beispiel wenn eine Task abbricht oder nicht verfügbar ist.▶ <code>resource</code> Das Gerät erkennt Fehler in den verfügbaren Ressourcen, zum Beispiel bei knapp werdendem Speicher.▶ <code>software</code> Das Gerät erkennt Software-Fehler, zum Beispiel Fehler beim Konsistenz-Check.▶ <code>hardware</code> Das Gerät erkennt Hardware-Fehler, zum Beispiel im Chipsatz.
Aktion	<p>Legt das Verhalten des Geräts fest, wenn das nebenstehende Ereignis eintritt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>reboot</code> (Voreinstellung) Das Gerät löst einen Neustart aus.▶ <code>logOnly</code> Das Gerät protokolliert den Fehler in der Log-Datei. Siehe Dialog <i>Diagnose > Bericht > System Log</i>.▶ <code>sendTrap</code> Das Gerät sendet einen SNMP-Trap. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose > Statuskonfiguration > Alarme (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

6.3 Syslog

Das Gerät bietet Ihnen die Möglichkeit, ausgewählte Ereignisse abhängig vom Schweregrad des Ereignisses an unterschiedliche Syslog-Server zu melden. In diesem Dialog legen Sie die Einstellungen dafür fest und verwalten bis zu 8 Syslog-Server.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet das Senden von Ereignissen an die Syslog-Server ein/aus. Mögliche Werte: ▶ An Das Senden von Ereignissen ist eingeschaltet. Das Gerät sendet die in der Tabelle festgelegten Ereignisse zum jeweils festgelegten Syslog-Server. ▶ Aus (Voreinstellung) Das Senden von Ereignissen ist ausgeschaltet.

■ Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht. Wenn Sie einen Tabelleneintrag löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie einen neuen Tabelleneintrag erzeugen, schließt das Gerät die 1. Lücke. Mögliche Werte: ▶ 1..8
IP-Adresse	Legt die IP-Adresse des Syslog-Servers fest. Mögliche Werte: ▶ Gültige IPv4-Adresse (Voreinstellung: 0.0.0.0)
Ziel-UDP-Port	Legt den UDP-Port fest, auf dem der Syslog-Server die Log-Einträge erwartet. Mögliche Werte: ▶ 1..65535 (Voreinstellung: 514)
Transport-Typ	Zeigt den Transporttyp, den das Gerät verwendet, um Ereignisse an den Syslog-Server zu senden. Mögliche Werte: ▶ udp Das Gerät sendet die Ereignisse über den in Spalte <i>Ziel-UDP-Port</i> festgelegten UDP-Port.
Min. Schweregrad	Legt den Mindest-Schweregrad der Ereignisse fest. Das Gerät sendet einen Log-Eintrag für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden an den Syslog-Server. Mögliche Werte: ▶ emergency ▶ alert ▶ critical ▶ error ▶ warning (Voreinstellung) ▶ notice ▶ informational ▶ debug

Parameter	Bedeutung
Typ	Legt den Typ des Log-Eintrags fest, den das Gerät übermittelt. Mögliche Werte: <ul style="list-style-type: none">▶ systemlog (Voreinstellung)▶ audittrail
Aktiv	Aktiviert bzw. deaktiviert die Übermittlung der Ereignisse zum Syslog-Server: <ul style="list-style-type: none">▶ markiert Das Gerät sendet Ereignisse zum Syslog-Server.▶ unmarkiert (Voreinstellung) Die Übermittlung der Ereignisse zum Syslog-Server ist deaktiviert.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

6.4 Ports

Das Menü enthält die folgenden Dialoge:

- ▶ SFP
- ▶ Port-Monitor
- ▶ Auto-Disable
- ▶ Port-Mirroring

6.4.1 SFP

Dieser Dialog bietet Ihnen die Möglichkeit, die gegenwärtige Bestückung des Geräts mit SFP-Transceivern und deren Eigenschaften einzusehen.

■ Tabelle

Die Tabelle zeigt ausschließlich dann gültige Werte an, wenn das Gerät mit SFP-Transceivern bestückt ist.

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Modultyp	Typ des SFP-Transceivers, zum Beispiel M-SFP-SX/LC.
Seriennummer	Zeigt die Seriennummer des SFP-Transceivers.
Steckverbinder-Typ	Zeigt die Bauart des Steckverbinders.
Unterstützt	Zeigt, ob das Gerät den SFP-Transceiver unterstützt.
Temperatur [°C]	Betriebstemperatur des SFP-Transceivers in °Celsius.
Sendeleistung [mW]	Sendeleistung des SFP-Transceivers in mW.
Empfangsleistung [mW]	Empfangsleistung des SFP-Transceivers in mW.
Sendeleistung [dBm]	Sendeleistung des SFP-Transceivers in dBm.
Empfangsleistung [dBm]	Empfangsleistung des SFP-Transceivers in dBm.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

6.4.2 Port-Monitor

Die *Port-Monitor*-Funktion überwacht auf den Ports die Einhaltung festgelegter Parameter. Wenn die *Port-Monitor*-Funktion eine Überschreitung der Parameter erkennt, führt das Gerät eine Aktion aus.

Um die *Port-Monitor*-Funktion anzuwenden, gehen Sie wie folgt vor:

- ▶ Registerkarte *Global*
 - Schalten Sie im Rahmen *Funktion* die *Port-Monitor*-Funktion ein.
 - Aktivieren Sie für jeden Port diejenigen Parameter, deren Einhaltung die *Port-Monitor*-Funktion überwachen soll.
- ▶ Registerkarten *Link-Änderungen*, *CRC/Fragmente* und *Überlast-Erkennung*
 - Legen Sie für jeden Port die Schwellenwerte der Parameter fest.
- ▶ Registerkarte *Link-Speed-/Duplex-Mode-Erkennung*
 - Aktivieren Sie für jeden Port die erlaubten Kombinationen von Geschwindigkeit und Duplex-Modus.
- ▶ Registerkarte *Global*
 - Legen Sie für jeden Port eine Aktion fest, die das Gerät ausführt, wenn die *Port-Monitor*-Funktion eine Überschreitung der Parameter erkennt.
- ▶ Registerkarte *Auto-Disable*
 - Markieren Sie für die überwachten Parameter das Kontrollkästchen *Auto-Disable*, wenn Sie die Aktion `auto-disable` mindestens einmal festgelegt haben.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [Global]
- ▶ [Auto-Disable]
- ▶ [Link-Änderungen]
- ▶ [CRC/Fragmente]
- ▶ [Überlast-Erkennung]
- ▶ [Link-Speed-/Duplex-Mode-Erkennung]

[Global]

In dieser Registerkarte schalten Sie die *Port-Monitor*-Funktion ein und legen die Parameter fest, deren Einhaltung die *Port-Monitor*-Funktion überwacht. Außerdem legen Sie die Aktion fest, die das Gerät ausführt, wenn die *Port-Monitor*-Funktion eine Überschreitung der Parameter erkennt.


■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>Port-Monitor</i> -Funktion global ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>Port-Monitor</i>-Funktion ist eingeschaltet.▶ Aus (Voreinstellung) Die <i>Port-Monitor</i>-Funktion ist ausgeschaltet.

■ Tabelle


Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Link-Änderungen an	Aktiviert/deaktiviert auf dem Port die Überwachung von Linkänderungen. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Die Überwachung ist aktiv.<ul style="list-style-type: none">– Die <i>Port-Monitor</i>-Funktion überwacht Linkänderungen auf dem Port.– Wenn das Gerät zu viele Linkänderungen erkennt, führt es die in Spalte <i>Aktion</i> festgelegte Aktion aus.– In der Registerkarte <i>Link-Änderungen</i> legen Sie die zu überwachenden Parameter fest.▶ unmarkiert (Voreinstellung) Die Überwachung ist inaktiv.
CRC/Fragmente an	Aktiviert/deaktiviert auf dem Port die Überwachung von CRC-/Fragmentfehlern. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Die Überwachung ist aktiv.<ul style="list-style-type: none">– Die <i>Port-Monitor</i>-Funktion überwacht CRC-/Fragmentfehler auf dem Port.– Wenn das Gerät zu viele CRC-/Fragmentfehler erkennt, führt es die in Spalte <i>Aktion</i> festgelegte Aktion aus.– In der Registerkarte <i>CRC/Fragmente</i> legen Sie die zu überwachenden Parameter fest.▶ unmarkiert (Voreinstellung) Die Überwachung ist inaktiv.
Duplex-Mismatch-Erkennung an	Aktiviert/deaktiviert auf dem Port die Überwachung von Duplex-Mismatches. Mögliche Werte: <ul style="list-style-type: none">▶ markiert Die Überwachung ist aktiv.<ul style="list-style-type: none">– Die <i>Port-Monitor</i>-Funktion überwacht Duplex-Mismatches auf dem Port.– Wenn das Gerät einen Duplex-Mismatch erkennt, führt es die in Spalte <i>Aktion</i> festgelegte Aktion aus.▶ unmarkiert (Voreinstellung) Die Überwachung ist inaktiv.

Parameter	Bedeutung
Überlast-Erkennung an	<p>Aktiviert/deaktiviert auf dem Port die Überlast-Erkennung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die Überwachung ist aktiv. <ul style="list-style-type: none"> – Die <i>Port-Monitor</i>-Funktion überwacht die Last auf dem Port. – Wenn das Gerät Überlast auf dem Port erkennt, führt das Gerät die in Spalte <i>Aktion</i> festgelegte Aktion aus. – In der Registerkarte <i>Überlast-Erkennung</i> legen Sie die zu überwachenden Parameter fest. ▶ unmarkiert (Voreinstellung) Die Überwachung ist inaktiv.
Link-Speed-/Duplex-Mode-Erkennung an	<p>Aktiviert/deaktiviert auf dem Port die Überwachung von Verbindungsgeschwindigkeit und Duplex-Modus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Die Überwachung ist aktiv. <ul style="list-style-type: none"> – Die <i>Port-Monitor</i>-Funktion überwacht Verbindungsgeschwindigkeit und Duplex-Modus auf dem Port. – Wenn das Gerät eine unzulässige Kombination von Verbindungsgeschwindigkeit und Duplex-Modus feststellt, führt das Gerät die in Spalte <i>Aktion</i> festgelegte Aktion aus. – In der Registerkarte <i>Link-Speed-/Duplex-Mode-Erkennung</i> legen Sie die zu überwachenden Parameter fest. ▶ unmarkiert (Voreinstellung) Die Überwachung ist inaktiv.
Aktive Bedingung	<p>Zeigt den überwachten Parameter, der zur Aktion auf dem Port geführt hat.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ - Kein überwachter Parameter. Das Gerät führt keine Aktion aus. ▶ Link-Änderungen Zu viele Linkänderungen im betrachteten Zeitraum. ▶ CRC/Fragmente Zu viele CRC-/Fragmentfehler im betrachteten Zeitraum. ▶ Duplex-Mismatch-Erkennung Duplex-Mismatch erkannt. ▶ Überlast-Erkennung Überlast erkannt im betrachteten Zeitraum. ▶ Link-Speed-/Duplex-Mode-Erkennung Unerlaubte Kombination von Geschwindigkeit und Duplex-Modus erkannt.

Parameter	Bedeutung
Aktion	<p>Legt die Aktion fest, die das Gerät ausführt, wenn die <i>Port-Monitor</i>-Funktion eine Überschreitung der Parameter erkennt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>disable port</code> Das Gerät schaltet den Port aus und sendet einen SNMP-Trap. Die „Link-Status“-LED des Ports blinkt 3 × pro Periode. <ul style="list-style-type: none"> – Um den Port wieder einzuschalten, markieren Sie den Port und klicken die Schaltfläche  und dann den Eintrag <i>Zurücksetzen</i>. – Die <i>Auto-Disable</i>-Funktion schaltet nach der festgelegten Wartezeit den Port wieder ein, wenn die Überschreitung der Parameter aufgehoben ist. Voraussetzung ist, dass in der Registerkarte <i>Auto-Disable</i> das Kontrollkästchen für den überwachten Parameter markiert ist. ▶ <code>send trap</code> Das Gerät sendet einen SNMP-Trap. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog <i>Diagnose > Statuskonfiguration > Alarme (Traps)</i> einschalten und mindestens 1 Trap-Ziel festlegen. ▶ <code>auto-disable</code> (Voreinstellung) Das Gerät schaltet den Port aus und sendet einen SNMP-Trap. Die „Link-Status“-LED des Ports blinkt 3 × pro Periode. Voraussetzung ist, dass in der Registerkarte <i>Auto-Disable</i> das Kontrollkästchen für den überwachten Parameter markiert ist. <ul style="list-style-type: none"> – Der Dialog <i>Diagnose > Ports > Auto-Disable</i> zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind. – Die <i>Auto-Disable</i>-Funktion schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog <i>Diagnose > Ports > Auto-Disable</i> in Spalte <i>Reset-Timer [s]</i> eine Wartezeit für den betreffenden Port fest.
Status Port	<p>Zeigt den Betriebszustand des Ports.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>up</code> Der Port ist eingeschaltet. ▶ <code>down</code> Der Port ist ausgeschaltet. ▶ <code>notPresent</code> Kein physischer Port vorhanden.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	<p>Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf 0. Davon betroffen sind die Zähler in den folgenden Dialogen:</p> <ul style="list-style-type: none"> ▶ Dialog <i>Diagnose > Ports > Port-Monitor</i> <ul style="list-style-type: none"> – Registerkarte <i>Link-Änderungen</i> – Registerkarte <i>CRC/Fragmente</i> – Registerkarte <i>Überlast-Erkennung</i> ▶ Dialog <i>Diagnose > Ports > Auto-Disable</i>

[Auto-Disable]


In dieser Registerkarte aktivieren Sie die *Auto-Disable*-Funktion für die von der *Port-Monitor*-Funktion überwachten Parameter.

■ Tabelle

Parameter	Bedeutung
Grund	Zeigt die von der <i>Port-Monitor</i> -Funktion überwachten Parameter. Markieren Sie das nebenstehende Kontrollkästchen, damit die <i>Port-Monitor</i> -Funktion bei Erkennen einer Überschreitung der überwachten Parameter die Aktion <code>auto-disable</code> ausführt.
Auto-Disable	Aktiviert/deaktiviert die <i>Auto-Disable</i> -Funktion für nebenstehende Parameter. Mögliche Werte: <ul style="list-style-type: none"> ▶ <code>markiert</code> Die <i>Auto-Disable</i>-Funktion für nebenstehende Parameter ist aktiv. Bei Überschreiten der nebenstehenden Parameter führt das Gerät die <i>Auto-Disable</i>-Funktion aus, wenn in Spalte <i>Aktion</i> der Wert <code>auto-disable</code> festgelegt ist. ▶ <code>unmarkiert</code> (Voreinstellung) Die <i>Auto-Disable</i>-Funktion für nebenstehende Parameter ist inaktiv.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf 0. Davon betroffen sind die Zähler in den folgenden Dialogen: <ul style="list-style-type: none"> ▶ Dialog <i>Diagnose > Ports > Port-Monitor</i> <ul style="list-style-type: none"> – Registerkarte <i>Link-Änderungen</i> – Registerkarte <i>CRC/Fragmente</i> – Registerkarte <i>Überlast-Erkennung</i> ▶ Dialog <i>Diagnose > Ports > Auto-Disable</i>

[Link-Änderungen]

In dieser Registerkarte legen Sie für jeden Port die folgenden Einstellungen fest:

- ▶ Anzahl der Linkänderungen.
- ▶ Zeitraum, in welchem die *Port-Monitor*-Funktion einen Parameter überwacht, um Abweichungen zu erkennen.

Außerdem sehen Sie, wie viele Linkänderungen die *Port-Monitor*-Funktion bisher erkannt hat.


Die *Port-Monitor*-Funktion überwacht diejenigen Ports, für die in der Registerkarte *Global* das Kontrollkästchen in Spalte *Link-Änderungen an* markiert ist.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Abtast-Intervall [s]	Legt den Zeitraum in Sekunden fest, in welchem die <i>Port-Monitor</i> -Funktion einen Parameter überwacht, um Abweichungen zu erkennen. Mögliche Werte: ▶ 1..180 (Voreinstellung: 10)
Link-Änderungen	Legt die Anzahl der Linkänderungen fest. Wenn die <i>Port-Monitor</i> -Funktion diese Anzahl an Linkänderungen im überwachten Zeitraum erkennt, führt das Gerät die festgelegte Aktion aus. Mögliche Werte: ▶ 1..100 (Voreinstellung: 5)
Letztes Abtast-Intervall	Zeigt die Anzahl der Linkänderungen, die das Gerät im zurückliegenden Zeitraum erkannt hat.
Gesamt	Zeigt die Gesamtzahl der Linkänderungen, die das Gerät seit dem Einschalten des Ports erkannt hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf 0. Davon betroffen sind die Zähler in den folgenden Dialogen: <ul style="list-style-type: none">▶ Dialog <i>Diagnose > Ports > Port-Monitor</i><ul style="list-style-type: none">– Registerkarte <i>Link-Änderungen</i>– Registerkarte <i>CRC/Fragmente</i>– Registerkarte <i>Überlast-Erkennung</i>▶ Dialog <i>Diagnose > Ports > Auto-Disable</i>

[CRC/Fragmente]

In dieser Registerkarte legen Sie für jeden Port die folgenden Einstellungen fest:

- ▶ die Fragmentfehlerrate
- ▶ Zeitraum, in welchem die *Port-Monitor*-Funktion einen Parameter überwacht, um Abweichungen zu erkennen.

Außerdem sehen Sie die Fragmentfehlerrate, die das Gerät bisher erkannt hat.


Die *Port-Monitor*-Funktion überwacht diejenigen Ports, für die in der Registerkarte *Global* das Kontrollkästchen in Spalte *CRC/Fragmente an* markiert ist.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Abtast-Intervall [s]	Legt den Zeitraum in Sekunden fest, in welchem die <i>Port-Monitor</i> -Funktion einen Parameter überwacht, um Abweichungen zu erkennen. Mögliche Werte: ▶ 5..180 (Voreinstellung: 10)
CRC-/Fragment-Fehlerrate [ppm]	Legt die Fragmentfehlerrate (in parts per million) fest. Wenn die <i>Port-Monitor</i> -Funktion diese Fragmentfehlerrate im überwachten Zeitraum erkennt, führt das Gerät die festgelegte Aktion aus. Mögliche Werte: ▶ 1..1000000 (Voreinstellung: 1000)
Letztes aktives Intervall [ppm]	Zeigt die Fragmentfehlerrate, die das Gerät im zurückliegenden Zeitraum erkannt hat.
Gesamt [ppm]	Zeigt die Fragmentfehlerrate, die das Gerät seit dem Einschalten des Ports erkannt hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf 0. Davon betroffen sind die Zähler in den folgenden Dialogen: <ul style="list-style-type: none"> ▶ Dialog <i>Diagnose > Ports > Port-Monitor</i> <ul style="list-style-type: none"> – Registerkarte <i>Link-Änderungen</i> – Registerkarte <i>CRC/Fragmente</i> – Registerkarte <i>Überlast-Erkennung</i> ▶ Dialog <i>Diagnose > Ports > Auto-Disable</i>

[Überlast-Erkennung]

In dieser Registerkarte legen Sie für jeden Port die folgenden Einstellungen fest:

- ▶ Last-Grenzwerte.
- ▶ Zeitraum, in welchem die *Port-Monitor*-Funktion einen Parameter überwacht, um Abweichungen zu erkennen.

Außerdem sehen Sie die Anzahl an Datenpaketen, die das Gerät bisher erkannt hat.

Die *Port-Monitor*-Funktion überwacht diejenigen Ports, für die in der Registerkarte *Global* das Kontrollkästchen in Spalte *Überlast-Erkennung an* markiert ist.


Die *Port-Monitor*-Funktion überwacht keine Ports, die Mitglied einer Link-Aggregation-Gruppe oder PRP/HSR-Teilnehmer sind.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Traffic-Typ	Legt den Typ der Datenpakete fest, die das Gerät beim Überwachen der Last auf dem Port berücksichtigt. Mögliche Werte: <ul style="list-style-type: none">▶ all Die <i>Port-Monitor</i>-Funktion überwacht Broadcast-, Multicast- und Unicast-Pakete.▶ bc (Voreinstellung) Die <i>Port-Monitor</i>-Funktion überwacht ausschließlich Broadcast-Pakete.▶ bc-mc Die <i>Port-Monitor</i>-Funktion überwacht ausschließlich Broadcast- und Multicast-Pakete.
Grenzwert-Typ	Legt die Einheit der Datenrate fest. Mögliche Werte: <ul style="list-style-type: none">▶ pps (Voreinstellung) Pakete pro Sekunde▶ kbps Kbit pro Sekunde Voraussetzung ist, dass der Wert in Spalte <i>Traffic-Typ</i> = all ist.
Unterer Grenzwert	Legt den unteren Schwellenwert für die Datenrate fest. Die <i>Auto-Disable</i> -Funktion schaltet den Port erst dann wieder ein, wenn die Last auf dem Port niedriger ist als der hier festgelegte Wert. Mögliche Werte: <ul style="list-style-type: none">▶ 0..10000000 (Voreinstellung: 0)
Oberer Grenzwert	Legt den oberen Schwellenwert für die Datenrate fest. Wenn die <i>Port-Monitor</i> -Funktion diese Last im überwachten Zeitraum erkennt, führt das Gerät die festgelegte Aktion aus. Mögliche Werte: <ul style="list-style-type: none">▶ 0..10000000 (Voreinstellung: 0)
Intervall [s]	Legt den Zeitraum in Sekunden fest, den die <i>Port-Monitor</i> -Funktion für das Erkennen einer Überschreitung betrachtet. Mögliche Werte: <ul style="list-style-type: none">▶ 1..20 (Voreinstellung: 1)
Pakete	Zeigt die Anzahl an Broadcast-, Multicast- und Unicast-Paketen, die das Gerät im zurückliegenden Zeitraum erkannt hat.
Broadcast-Pakete	Zeigt die Anzahl an Broadcast-Paketen, die das Gerät im zurückliegenden Zeitraum erkannt hat.
Multicast-Pakete	Zeigt die Anzahl an Multicast-Paketen, die das Gerät im zurückliegenden Zeitraum erkannt hat.
Kbit/s	Zeigt die Datenrate in Kbit pro Sekunde, die das Gerät im zurückliegenden Zeitraum erkannt hat.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf 0. Davon betroffen sind die Zähler in den folgenden Dialogen: <ul style="list-style-type: none"> ▶ Dialog <i>Diagnose > Ports > Port-Monitor</i> <ul style="list-style-type: none"> – Registerkarte <i>Link-Änderungen</i> – Registerkarte <i>CRC/Fragmente</i> – Registerkarte <i>Überlast-Erkennung</i> ▶ Dialog <i>Diagnose > Ports > Auto-Disable</i>

[Link-Speed-/Duplex-Mode-Erkennung]

In dieser Registerkarte aktivieren Sie für jeden Port die erlaubten Kombinationen von Geschwindigkeit und Duplex-Modus.

Die *Port-Monitor*-Funktion überwacht diejenigen Ports, für die in der Registerkarte *Global* das Kontrollkästchen in Spalte *Link-Speed-/Duplex-Mode-Erkennung an* markiert ist.

Die *Port-Monitor*-Funktion überwacht ausschließlich eingeschaltete physische Ports.


■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
10 Mbit/s HDX	Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor. Mögliche Werte: <ul style="list-style-type: none"> ▶ markiert Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ unmarkiert Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte <i>Global</i> festgelegte Aktion aus.
10 Mbit/s FDX	Aktiviert/deaktiviert das Akzeptieren der Kombination von 10 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor. Mögliche Werte: <ul style="list-style-type: none"> ▶ markiert Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus. ▶ unmarkiert Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte <i>Global</i> festgelegte Aktion aus.

Parameter	Bedeutung
100 Mbit/s HDX	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus.▶ <i>unmarkiert</i> Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte <i>Global</i> festgelegte Aktion aus.
100 Mbit/s FDX	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus.▶ <i>unmarkiert</i> Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte <i>Global</i> festgelegte Aktion aus.
1.000 Mbit/s FDX	<p>Aktiviert/deaktiviert das Akzeptieren der Kombination von 1 Gbit/s und Vollduplex auf dem Port durch den Port-Monitor.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <i>markiert</i> Der Port-Monitor erlaubt die Kombinationen von Geschwindigkeit und Duplex-Modus.▶ <i>unmarkiert</i> Wenn der Port-Monitor die Kombinationen von Geschwindigkeit und Duplex-Modus auf dem Port feststellt, führt das Gerät die in der Registerkarte <i>Global</i> festgelegte Aktion aus.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	<p>Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf 0. Davon betroffen sind die Zähler in den folgenden Dialogen:</p> <ul style="list-style-type: none">▶ Dialog <i>Diagnose > Ports > Port-Monitor</i><ul style="list-style-type: none">– Registerkarte <i>Link-Änderungen</i>– Registerkarte <i>CRC/Fragmente</i>– Registerkarte <i>Überlast-Erkennung</i>▶ Dialog <i>Diagnose > Ports > Auto-Disable</i>

6.4.3 Auto-Disable

Die *Auto-Disable*-Funktion bietet Ihnen die Möglichkeit, überwachte Ports automatisch auszuschalten und auf Wunsch wieder einzuschalten.

Beispielsweise die *Port-Monitor*-Funktion und ausgewählte Funktionen im Menü *Netzsicherheit* verwenden die *Auto-Disable*-Funktion, um Ports bei Überschreiten überwachter Parameter auszuschalten.

Wenn die Überschreitung der Parameter aufgehoben ist, schaltet die *Auto-Disable*-Funktion den betreffenden Port nach einer festzulegenden Wartezeit wieder ein.

Der Dialog enthält die folgenden Registerkarten:

- ▶ [Port]
- ▶ [Status]

[Port]

Diese Registerkarte zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind. Wenn Sie in Spalte *Reset-Timer [s]* eine Wartezeit festlegen, schaltet die *Auto-Disable*-Funktion den betreffenden Port automatisch wieder ein, sofern die Überschreitung der Parameter aufgehoben ist.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Reset-Timer [s]	<p>Legt die Wartezeit in Sekunden fest, nach der die <i>Auto-Disable</i>-Funktion den Port wieder einschaltet.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 0 (Voreinstellung) Der Timer ist inaktiv. Der Port bleibt ausgeschaltet. ▶ 30..4294967295 Die <i>Auto-Disable</i>-Funktion schaltet den Port nach der hier festgelegten Wartezeit wieder ein, wenn die Überschreitung der Parameter aufgehoben ist.
Zeitpunkt des Fehlers	Zeigt, wann das Gerät aufgrund einer Überschreitung der Parameter den Port ausgeschaltet hat.
Verbleibende Zeit [s]	Zeigt die verbleibende Zeit in Sekunden, bis die <i>Auto-Disable</i> -Funktion den Port wieder einschaltet.

Parameter	Bedeutung
Komponente	<p>Zeigt, welche Software-Komponente im Gerät das Ausschalten des Ports veranlasst hat.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ PORT_MON <i>Port-Monitor</i> Siehe Dialog <i>Diagnose > Ports > Port-Monitor</i>. ▶ PORT_ML <i>Port-Sicherheit</i> Siehe Dialog <i>Netzsicherheit > Port-Sicherheit</i>. ▶ DOT1S <i>BPDUGuard</i> Siehe Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i>.
Grund	<p>Zeigt den überwachten Parameter, der zum Ausschalten des Ports geführt hat.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ none Kein überwachter Parameter. Der Port ist eingeschaltet. ▶ link-flap Zu viele Linkänderungen. Siehe Dialog <i>Diagnose > Ports > Port-Monitor</i>, Registerkarte <i>Link-Änderungen</i>. ▶ crc-error Zu viele CRC-/Fragmentfehler. Siehe Dialog <i>Diagnose > Ports > Port-Monitor</i>, Registerkarte <i>CRC/Fragmente</i>. ▶ duplex-mismatch Duplex-Mismatch erkannt. Siehe Dialog <i>Diagnose > Ports > Port-Monitor</i>, Registerkarte <i>Global</i>. ▶ bpdu-rate STP-BPDUs empfangen. Siehe Dialog <i>Switching > L2-Redundanz > Spanning Tree > Global</i>. ▶ mac-based-port-security Zu viele Datenpakete von unerwünschten Absendern. Siehe Dialog <i>Netzsicherheit > Port-Sicherheit</i>. ▶ overload-detection Überlast. Siehe Dialog <i>Diagnose > Ports > Port-Monitor</i>, Registerkarte <i>Überlast-Erkennung</i>. ▶ speed-duplex Unerlaubte Kombination von Geschwindigkeit und Duplex-Modus erkannt. Siehe Dialog <i>Diagnose > Ports > Port-Monitor</i>, Registerkarte <i>Link-Speed-/Duplex-Mode-Erkennung</i>.
Aktiv	<p>Zeigt, ob der Port aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet ist.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert Der Port ist gegenwärtig ausgeschaltet. ▶ unmarkiert Der Port ist eingeschaltet.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

[Status]


Diese Registerkarte zeigt, für welche überwachten Parameter die *Auto-Disable*-Funktion aktiviert ist.

■ Tabelle

Parameter	Bedeutung
Grund	Zeigt die Parameter, die das Gerät überwacht. Markieren Sie das nebenstehende Kontrollkästchen, damit die <i>Auto-Disable</i> -Funktion bei Überschreiten der überwachten Parameter den Port ausschaltet und ggf. wieder einschaltet.
Kategorie	Zeigt, zu welcher Funktion der nebenstehende Parameter gehört. Mögliche Werte: <ul style="list-style-type: none"> ▶ port-monitor Der Parameter gehört zur <i>Port-Monitor</i>-Funktion. Siehe Dialog <i>Diagnose > Port > Port-Monitor</i>. ▶ network-security Der Parameter gehört zu den Funktionen im Menü <i>Netzicherheit</i>. ▶ l2-redundancy Der Parameter gehört zu den <i>L2-Redundanz</i>-Funktionen. Siehe Dialog <i>Switching > L2-Redundanz</i>.
Auto-Disable	Zeigt, ob die <i>Auto-Disable</i> -Funktion für den nebenstehenden Parameter aktiviert/deaktiviert ist. Mögliche Werte: <ul style="list-style-type: none"> ▶ markiert Die <i>Auto-Disable</i>-Funktion für nebenstehende Parameter ist aktiv. die <i>Auto-Disable</i>-Funktion schaltet bei Überschreiten der überwachten Parameter den betreffenden Port aus und ggf. wieder ein. ▶ unmarkiert (Voreinstellung) Die <i>Auto-Disable</i>-Funktion für nebenstehende Parameter ist inaktiv.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Zurücksetzen	Schaltet den in der Tabelle markierten Port wieder ein und setzt dessen Zähler zurück auf 0. Davon betroffen sind die Zähler in den folgenden Dialogen: <ul style="list-style-type: none"> ▶ Dialog <i>Diagnose > Ports > Port-Monitor</i> <ul style="list-style-type: none"> – Registerkarte <i>Link-Änderungen</i> – Registerkarte <i>CRC/Fragmente</i> – Registerkarte <i>Überlast-Erkennung</i> ▶ Dialog <i>Diagnose > Ports > Auto-Disable</i>

6.4.4 Port-Mirroring

Die *Port-Mirroring*-Funktion bietet Ihnen die Möglichkeit, die empfangenen und gesendeten Datenpakete von ausgewählten Ports auf einen Ziel-Port zu kopieren. Mit einem Analyzer oder einer RMON-Probe, am Ziel-Port angeschlossen, lässt sich der Datenstrom beobachten und auswerten. Am Quell-Port bleiben die Datenpakete unverändert.

Anmerkung: Um den Management-Zugriff über den Ziel-Port einzuschalten, markieren Sie vor Einschalten der *Port-Mirroring*-Funktion das Kontrollkästchen *Management erlauben* im Rahmen *Ziel-Port*.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>Port-Mirroring</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>Port-Mirroring</i>-Funktion ist eingeschaltet. Das Gerät kopiert die Datenpakete von den ausgewählten Quell-Ports auf den Ziel-Port.▶ Aus (Voreinstellung) Die <i>Port-Mirroring</i>-Funktion ist ausgeschaltet.

■ Ziel-Port

Parameter	Bedeutung
Primärer Port	Legt den Ziel-Port fest. Als Ziel-Port eignen sich Ports, die nicht für folgende Zwecke verwendet werden: <ul style="list-style-type: none">– Quell-Port– L2-Redundanz-Protokolle Mögliche Werte: <ul style="list-style-type: none">▶ no Port (Voreinstellung) Kein Ziel-Port ausgewählt.▶ <Port-Nummer> Nummer des Ziel-Ports. Das Gerät kopiert die Datenpakete von den Quell-Ports auf diesen Port. Das Gerät fügt den Datenpaketen, die der Quell-Port sendet, am Ziel-Port ein VLAN-Tag hinzu. Datenpakete, die der Quell-Port empfängt, sendet der Ziel-Port unmodifiziert. Anmerkung: Der Ziel-Port benötigt ausreichend Bandbreite, um den Datenstrom aufzunehmen. Wenn der kopierte Datenstrom die Bandbreite des Ziel-Ports überschreitet, verwirft das Gerät überschüssige Datenpakete auf dem Ziel-Port.


Parameter	Bedeutung
Management erlauben	<p>Aktiviert/deaktiviert den Management-Zugriff über den Ziel-Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Der Management-Zugriff über den Ziel-Port ist aktiv. Das Gerät ermöglicht den Management-Zugriff auf das Gerät über den Ziel-Port, ohne die aktive <i>Port-Mirroring</i>-Sitzung zu unterbrechen. <ul style="list-style-type: none"> – Das Gerät dupliziert auf dem Ziel-Port Multicasts, Broadcasts und unbekannte Unicasts. – Die VLAN-Einstellungen auf dem Ziel-Port bleiben unverändert. Voraussetzung für den Management-Zugriff über den Ziel-Port ist, dass der Ziel-Port Mitglied im Management-VLAN ist. ▶ <code>unmarkiert</code> (Voreinstellung) Der Management-Zugriff über den Ziel-Port ist inaktiv. Das Gerät unterbindet den Management-Zugriff auf das Gerät über den Ziel-Port.

■ Tabelle

Parameter	Bedeutung
Quell-Port	<p>Legt die Nummer des Ports fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code><Port-Nummer></code>
Eingeschaltet	<p>Aktiviert/deaktiviert das Kopieren der Datenpakete von diesem Quell-Port auf den Ziel-Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Das Kopieren der Datenpakete ist aktiv. Der Port ist als Quell-Port festgelegt. ▶ <code>unmarkiert</code> (Voreinstellung) Das Kopieren der Datenpakete ist inaktiv. ▶ (Ausgegraute Darstellung) Das Kopieren der Datenpakete dieses Ports ist nicht möglich. Mögliche Ursachen: <ul style="list-style-type: none"> – Der Port ist bereits als Ziel-Port festgelegt. – Der Port ist ein logischer Port, kein physischer Port. <p>Anmerkung: Das Gerät bietet Ihnen die Möglichkeit, abzüglich des Ziel-Ports jeden physischen Port als Quell-Port zu festzulegen.</p>
Typ	<p>Legt fest, welche Datenpakete das Gerät auf den Ziel-Port kopiert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>none</code> (Voreinstellung) Keine Datenpakete. ▶ <code>tx</code> Datenpakete, die der Quell-Port sendet. ▶ <code>rx</code> Datenpakete, die der Quell-Port empfängt. ▶ <code>txrx</code> Datenpakete, die der Quell-Port sendet und empfängt. <p>Anmerkung: Mit der Einstellung <code>txrx</code> kopiert das Gerät gesendete und empfangene Datenpakete. Der Ziel-Port benötigt mindestens eine Bandbreite, die der Summe aus Sendee- und Empfangskanal der Quell-Ports entspricht. Beispielsweise ist bei gleichartigen Ports der Ziel-Port bereits zu 100 % ausgelastet, wenn Sendee- und Empfangskanal eines Quell-Ports zu jeweils 50 % ausgelastet sind.</p> <p>Das Gerät fügt den Datenpaketen, die der Quell-Port sendet, am Ziel-Port ein VLAN-Tag hinzu. Datenpakete, die der Quell-Port empfängt, sendet der Ziel-Port unmodifiziert.</p>

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Konfiguration zurücksetzen	Setzt die Einstellungen des Dialogs auf die voreingestellten Werte zurück und überträgt die Änderungen in den flüchtigen Speicher des Geräts (RAM).

6.5 LLDP

Das Gerät bietet Ihnen die Möglichkeit, Informationen über benachbarte Geräte zu sammeln. Dazu nutzt das Gerät Link Layer Discovery Protocol (LLDP). Mit diesen Informationen ist eine Netzmanagement-Station in der Lage, die Struktur Ihres Netzes darzustellen.

Dieses Menü bietet Ihnen die Möglichkeit, die Topologie-Erkennung zu konfigurieren und die empfangenen Informationen in Tabellenform anzuzeigen.

Das Menü enthält die folgenden Dialoge:

- ▶ [LLDP Konfiguration](#)
- ▶ [LLDP Topologie-Erkennung](#)

6.5.1 LLDP Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, die Topologie-Erkennung für jeden Port zu konfigurieren.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die <i>LLDP</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An (Voreinstellung) Die <i>LLDP</i>-Funktion ist eingeschaltet. Die Topologie-Erkennung mit LLDP ist auf dem Gerät aktiv.▶ Aus Die <i>LLDP</i>-Funktion ist ausgeschaltet.

■ Konfiguration

Parameter	Bedeutung
Sende-Intervall [s]	Legt das Intervall in Sekunden fest, in dem das Gerät LLDP-Datenpakete sendet. Mögliche Werte: <ul style="list-style-type: none">▶ 5..32768 (Voreinstellung: 30)
Sende-Intervall Multiplikator	Legt den Faktor zur Bestimmung des Time-to-live-Werts für die LLDP-Datenpakete fest. Mögliche Werte: <ul style="list-style-type: none">▶ 2..10 (Voreinstellung: 4) Der im LLDP-Header kodierte Time-to-live-Wert ergibt sich aus der Multiplikation dieses Wertes mit dem Wert im Feld <i>Sende-Intervall [s]</i> .
Reinitialisierungs-Verzögerung [s]	Legt die Verzögerung in Sekunden für die Re-Initialisierung eines Ports fest. Mögliche Werte: <ul style="list-style-type: none">▶ 1..10 (Voreinstellung: 2) Wenn in Spalte <i>Funktion</i> der Wert <i>Aus</i> festgelegt ist, versucht das Gerät nach Ablauf der hier festgelegten Zeit den Port erneut zu initialisieren.
Sende-Verzögerung [s]	Legt die Verzögerung in Sekunden für die Übertragung von aufeinanderfolgenden LLDP-Datenpaketen fest, nachdem Konfigurationsänderungen im Gerät wirksam geworden sind. Mögliche Werte: <ul style="list-style-type: none">▶ 1..8192 (Voreinstellung: 2) Der empfohlene Wert liegt zwischen einem Minimum von 1 und einem Maximum, das einem Viertel des Wertes im Feld entspricht.
Benachrichtigungs-Intervall [s]	Legt das Intervall in Sekunden für das Senden von LLDP-Benachrichtigungen fest. Mögliche Werte: <ul style="list-style-type: none">▶ 5..3600 (Voreinstellung: 5) Nach Senden eines Benachrichtigungs-Traps wartet das Gerät mindestens die hier festgelegte Zeit, bis es den nächsten Benachrichtigungs-Trap sendet.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Funktion	<p>Legt fest, ob der Port LLDP-Datenpakete sendet und empfängt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ transmit Der Port sendet LLDP-Datenpakete, speichert jedoch keine Informationen über benachbarte Geräte. ▶ receive Der Port empfängt LLDP-Datenpakete, sendet jedoch keine Informationen an benachbarte Geräte. ▶ receive and transmit (Voreinstellung) Der Port sendet LLDP-Datenpakete und speichert Informationen über benachbarte Geräte. ▶ disabled Der Port sendet keine LLDP-Datenpakete und speichert keine Informationen über benachbarte Geräte.
Benachrichtigung	<p>Aktiviert/deaktiviert LLDP-Benachrichtigungen auf dem Port.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert LLDP-Benachrichtigungen auf dem Port sind aktiv. ▶ unmarkiert (Voreinstellung) LLDP-Benachrichtigungen auf dem Port sind inaktiv.
Port-Beschreibung senden	<p>Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit der Port-Beschreibung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Das Senden des TLV ist aktiv. Das Gerät sendet den TLV mit der Port-Beschreibung. ▶ unmarkiert Das Senden des TLV ist inaktiv. Das Gerät sendet keinen TLV mit der Port-Beschreibung.
Systemname senden	<p>Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit dem Gerätenamen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Das Senden des TLV ist aktiv. Das Gerät sendet den TLV mit dem Gerätenamen. ▶ unmarkiert Das Senden des TLV ist inaktiv. Das Gerät sendet keinen TLV mit dem Gerätenamen.
Systembeschreibung senden	<p>Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit der Systembeschreibung.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Das Senden des TLV ist aktiv. Das Gerät sendet den TLV mit der Systembeschreibung. ▶ unmarkiert Das Senden des TLV ist inaktiv. Das Gerät sendet keinen TLV mit der Systembeschreibung.
System-Ressourcen senden	<p>Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit den System-Ressourcen (Leistungsfähigkeitsdaten).</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ markiert (Voreinstellung) Das Senden des TLV ist aktiv. Das Gerät sendet den TLV mit den System-Ressourcen. ▶ unmarkiert Das Senden des TLV ist inaktiv. Das Gerät sendet keinen TLV mit den System-Ressourcen.
Nachbarn (max.)	<p>Begrenzt für diesen Port die Anzahl der zu erfassenden benachbarten Geräte.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..50 (Voreinstellung: 10)

Parameter	Bedeutung
FDB-Modus	<p>Legt fest, welche Funktion das Gerät verwendet, um benachbarte Geräte an diesem Port zu erfassen.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none">▶ <code>lldpOnly</code> Das Gerät verwendet ausschließlich LLDP-Datenpakete, um benachbarte Geräte an diesem Port zu erfassen.▶ <code>macOnly</code> Das Gerät verwendet gelernte MAC-Adressen, um benachbarte Geräte an diesem Port zu erfassen. Das Gerät verwendet die MAC-Adresse ausschließlich dann, wenn kein weiterer Eintrag in der Adresstabelle (FDB, Forwarding Database) für diesen Port vorhanden ist.▶ <code>both</code> Das Gerät verwendet LLDP-Datenpakete und gelernte MAC-Adressen, um benachbarte Geräte an diesem Port zu erfassen.▶ <code>autoDetect</code> (Voreinstellung) Empfängt das Gerät auf diesem Port LLDP-Datenpakete, arbeitet das Gerät wie mit der Einstellung <code>lldpOnly</code>. Andernfalls arbeitet das Gerät wie mit der Einstellung <code>macOnly</code>.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

6.5.2 LLDP Topologie-Erkennung

Geräte in Netzen senden Mitteilungen in Form von Paketen, welche auch unter dem Namen „LLDPDU“ (LLDP-Dateneinheit) bekannt sind. Die über LLDPDUs sendeten und empfangenen Daten sind aus vielen Gründen nützlich. So erkennt das Gerät etwa, bei welchen Geräten innerhalb des Netzes es sich um Nachbarn handelt und über welche Ports diese miteinander verbunden sind.

Der Dialog bietet Ihnen die Möglichkeit, das Netz darzustellen und die angeschlossenen Geräte mitsamt ihren Funktionsmerkmalen zu ermitteln.

Dieser Dialog zeigt Ihnen die gesammelten LLDP-Informationen zu den Nachbargeräten an. Mit diesen Informationen ist eine Netzmanagement-Station in der Lage, die Struktur Ihres Netzes darzustellen.

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 Topologieerkennung an einen Port angeschlossen sind, dann enthält die Tabelle eine Zeile für diesen Port, um jedes Gerät zu repräsentieren. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.

Die Weiterleitungstabelle (FDB) enthält MAC-Adressen von Geräten, welche die Topologietabelle aus Gründen der Übersicht ausblendet.

Wenn Sie an Port 1 mehrere Geräte anschließen (zum Beispiel über einen Hub), zeigt die Tabelle pro angeschlossenem Gerät eine Zeile an.

■ Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Nachbar-Bezeichner	Zeigt die Chassis-ID des Nachbargeräts. Dies kann zum Beispiel die Basis-MAC-Adresse des Nachbargeräts sein.
FDB	<p>Zeigt, ob das angeschlossene Gerät LLDP aktiv unterstützt.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ <code>markiert</code> Das angeschlossene Gerät unterstützt kein LLDP. Das Gerät verwendet Informationen aus seiner Adresstabelle (FDB, Forwarding Database). ▶ <code>unmarkiert</code> (Voreinstellung) Das angeschlossene Gerät unterstützt aktiv LLDP.
Nachbar-IP-Adresse	Zeigt die IP-Adresse, mit der der Management-Zugriff auf das Nachbargerät möglich ist.
Nachbar-Port-Beschreibung	Zeigt eine Beschreibung für den Port des Nachbargeräts.
Nachbar-Systemname	Zeigt den Gerätenamen des Nachbargeräts.
Nachbar-Systembeschreibung	Zeigt eine Beschreibung für das Nachbargerät.
Port ID	Zeigt die ID des Ports, über den das Nachbargerät mit dem Gerät verbunden ist.
Autonegotiation-Unterstützung	Zeigt, ob der Port des Nachbargeräts Auto-Negotiation unterstützt.
Autonegotiation	Zeigt, ob Auto-Negotiation auf dem Port des Nachbargeräts aktiviert ist.
Unterstützt PoE	Zeigt, ob der Port des Nachbargeräts Power over Ethernet (PoE) unterstützt.

Parameter	Bedeutung
PoE eingeschaltet	Zeigt, ob Power over Ethernet (PoE) auf dem Port des Nachbargeräts aktiviert ist.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

6.6 Bericht

Das Menü enthält die folgenden Dialoge:

- ▶ Bericht Global
- ▶ System Log
- ▶ Audit Trail

6.6.1 Bericht Global

Das Gerät bietet Ihnen die Möglichkeit, über die folgenden Ausgaben bestimmte Ereignisse zu protokollieren:

- ▶ auf der Konsole
- ▶ auf einen oder mehreren Syslog-Servern
- ▶ auf einer per SSH aufgebauten CLI-Verbindung
- ▶ auf einer per Telnet aufgebauten CLI-Verbindung

In diesem Dialog legen Sie die erforderlichen Einstellungen fest. Durch Zuweisen eines Schweregrads legen Sie fest, welche Ereignisse das Gerät protokolliert.

Der Dialog bietet Ihnen die Möglichkeit, ein ZIP-Archiv mit System-Informationen auf Ihrem PC zu speichern.

■ Console-Logging

Parameter	Bedeutung
Funktion	Schaltet die <i>Console-Logging</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>Console-Logging</i>-Funktion ist eingeschaltet. Das Gerät protokolliert die Ereignisse auf der Konsole.▶ Aus (Voreinstellung) Die <i>Console-Logging</i>-Funktion ist ausgeschaltet.
Schweregrad	Legt den Mindest-Schweregrad für die Ereignisse fest. Das Gerät protokolliert Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden. Das Gerät gibt die Meldungen auf der V.24-Schnittstelle aus. Mögliche Werte: <ul style="list-style-type: none">▶ emergency▶ alert▶ critical▶ error▶ warning (Voreinstellung)▶ notice▶ informational▶ debug

■ Buffered-Logging

Das Gerät puffert protokollierte Ereignisse in 2 getrennten Speicherbereichen, damit die Log-Einträge für dringliche Ereignisse erhalten bleiben.

Dieser Rahmen bietet Ihnen die Möglichkeit, den Mindest-Schweregrad für Ereignisse festzulegen, die das Gerät im höher priorisierten Speicherbereich puffert.

Parameter	Bedeutung
Schweregrad	<p>Legt den Mindest-Schweregrad für die Ereignisse fest. Das Gerät puffert Log-Einträge für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden im höher priorisierten Speicherbereich.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ emergency ▶ alert ▶ critical ▶ error ▶ warning (Voreinstellung) ▶ notice ▶ informational ▶ debug

■ SNMP-Logging

Parameter	Bedeutung
Protokolliere SNMP-Get-Requests	<p>Schaltet die Protokollierung von SNMP Get requests ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An Die Protokollierung ist eingeschaltet. Das Gerät protokolliert SNMP Get requests als Ereignis im Syslog. Den Schweregrad für dieses Ereignis wählen Sie in der Dropdown-Liste <i>Schweregrad Get-Request</i> aus. ▶ Aus (Voreinstellung) Die Protokollierung ist ausgeschaltet.
Protokolliere SNMP-Set-Requests	<p>Schaltet die Protokollierung von SNMP Set requests ein/aus.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ An Die Protokollierung ist eingeschaltet. Das Gerät protokolliert SNMP Set requests als Ereignis im Syslog. Den Schweregrad für dieses Ereignis wählen Sie in der Dropdown-Liste <i>Schweregrad Set-Request</i> aus. ▶ Aus (Voreinstellung) Die Protokollierung ist ausgeschaltet.
Schweregrad Get-Request	<p>Legt den Schweregrad des Ereignisses fest, welches das Gerät bei SNMP Get requests protokolliert.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ emergency ▶ alert ▶ critical ▶ error ▶ warning ▶ notice (Voreinstellung) ▶ informational ▶ debug

Parameter	Bedeutung
Schweregrad Set-Request	Legt den Schweregrad des Ereignisses fest, welches das Gerät bei SNMP Set requests protokolliert. Mögliche Werte: <ul style="list-style-type: none">▶ emergency▶ alert▶ critical▶ error▶ warning▶ notice (Voreinstellung)▶ informational▶ debug

Wenn Sie die Protokollierung von SNMP-Anfragen einschalten, sendet das Gerät diese als Ereignisse mit dem voreingestellten Schweregrad `notice` an die Liste der Syslog-Server. Der voreingestellte Mindest-Schweregrad für einen Syslog-Server-Eintrag ist `critical`.

Um SNMP-Anfragen an einen Syslog-Server zu senden, haben Sie mehrere Möglichkeiten, die Voreinstellungen zu ändern. Wählen Sie diejenige, die am besten zu Ihren Anforderungen passt.


- Setzen Sie den Schweregrad, mit dem das Gerät SNMP-Anfragen als Ereignisse erzeugt, auf `warning` oder `error` und ändern Sie den Mindest-Schweregrad für einen Syslog-Eintrag bei einem oder mehreren Syslog-Servern auf den gleichen Wert.
Sie haben auch die Möglichkeit, dafür einen eigenen Syslog-Server-Eintrag zu erzeugen.
- Setzen Sie ausschließlich den Schweregrad der SNMP-Anfragen auf `critical` oder höher. Das Gerät sendet dann SNMP-Anfragen als Ereignisse mit dem Schweregrad `critical` oder schwerer an die Syslog-Server.
- Setzen Sie ausschließlich den Mindest-Schweregrad bei einem oder mehreren Syslog-Server-Einträgen auf `notice` oder niedriger. Das Gerät sendet dann u. U. sehr viele Ereignisse an die Syslog-Server.

■ CLI-Logging

Parameter	Bedeutung
Funktion	Schaltet die <i>CLI-Logging</i> -Funktion ein/aus. Mögliche Werte: <ul style="list-style-type: none">▶ An Die <i>CLI-Logging</i>-Funktion ist eingeschaltet. Das Gerät protokolliert jeden Befehl, den es über das Command Line Interface (CLI) empfängt.▶ Aus (Voreinstellung) Die <i>CLI-Logging</i>-Funktion ist ausgeschaltet.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Support-Informationen herunterladen	Erzeugt ein ZIP-Archiv, das der Web-Browser Ihnen zum Download auf Ihren PC anbietet. Das ZIP-Archiv enthält Systeminformationen über das Gerät. Eine Erläuterung zu den im ZIP-Archiv enthaltenen Dateien finden Sie im folgenden Abschnitt.

■ Support Informationen: Im ZIP-Archiv enthaltene Dateien

Dateiname	Format	Bemerkungen
audittrail.html	HTML	Enthält die im Audit Trail chronologisch aufgezeichneten Systemereignisse und gespeicherten Änderungen durch die Benutzer.
defaultconfig.xml	XML	Enthält das Konfigurationsprofil mit den Werkseinstellungen.
script	TEXT	Enthält die Ausgaben des CLI-Kommandos <code>show running-config script</code> .
runningconfig.xml	XML	Enthält das Konfigurationsprofil mit den gegenwärtigen Betriebseinstellungen.
supportinfo.html	TEXT	Enthält geräteinterne Service-Information.
systeminfo.html	HTML	Enthält Information über die gegenwärtigen Einstellungen und Betriebsparameter.
systemlog.html	HTML	Enthält die in der Log-Datei protokollierten Ereignisse. Siehe Dialog <i>Diagnose > Bericht > System Log</i> .

■ Bedeutung der Schweregrade für Ereignisse

Schweregrad	Bedeutung
emergency	Gerät nicht betriebsbereit
alert	Sofortiger Bedienereingriff erforderlich
critical	Kritischer Zustand
error	Fehlerhafter Zustand
warning	Warnung
notice	Signifikanter, normaler Zustand
informational	Informelle Nachricht
debug	Debug-Nachricht

6.6.2 System Log

Das Gerät protokolliert wichtige geräteinterne Ereignisse in einer Log-Datei (System Log).


Dieser Dialog zeigt die Log-Datei (System Log). Der Dialog bietet Ihnen die Möglichkeit, die Log-Datei im HTML-Format auf Ihrem PC zu speichern.

Um die Log-Datei nach Suchbegriffen zu durchsuchen, verwenden Sie die Suchfunktion Ihres Web-Browsers.

Die Log-Datei bleibt bis zu einem Neustart des Geräts erhalten. Nach dem Neustart erstellt das Gerät die Datei neu.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Log-Datei speichern	Öffnet die HTML-Seite in einem neuen Web-Browser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Web-Browser-Befehl auf Ihrem PC speichern.
Log-Datei löschen	Entfernt die protokollierten Einträge aus der Log-Datei.

6.6.3 Audit Trail

Dieser Dialog zeigt die Log-Datei (Audit Trail). Der Dialog bietet Ihnen die Möglichkeit, die Log-Datei als HTML-Datei auf Ihrem PC zu speichern.

Um die Log-Datei nach Suchbegriffen zu durchsuchen, verwenden Sie die Suchfunktion Ihres Web-Browsers.

Das Gerät protokolliert Systemereignisse und schreibende Benutzeraktionen auf dem Gerät. Damit haben Sie die Möglichkeit, nachzuvollziehen, WER WANN WAS auf dem Gerät ändert. Voraussetzung ist, dass Ihrem Benutzerkonto die Benutzer-Rolle `auditor` oder `administrator` zugewiesen ist.

Unter anderem protokolliert das Gerät die folgenden Benutzeraktionen:


- ▶ Anmeldung eines Benutzers per CLI (lokal oder remote)
- ▶ Manuelle Abmeldung eines Benutzers
- ▶ Automatische Abmeldung eines Benutzers im CLI nach vorgegebener Zeit der Inaktivität
- ▶ Neustart des Geräts
- ▶ Sperrung eines Benutzerkontos aufgrund zu oft fehlgeschlagener Anmeldeversuche
- ▶ Sperrung des Management-Zugriffs aufgrund fehlgeschlagener Anmeldeversuche
- ▶ Im CLI ausgeführte Befehle, außer show-Befehle
- ▶ Änderungen an Konfigurationsvariablen
- ▶ Änderungen der Systemzeit
- ▶ Datei-Transfer-Operationen einschließlich Firmware-Updates
- ▶ Konfigurationsänderungen per HiDiscovery
- ▶ Firmware-Updates und Automatisches Konfigurieren des Geräts über den externen Speicher
- ▶ Öffnen und Schließen von SNMP über einen HTTPS-Tunnel

Das Gerät protokolliert keine Passwörter. Die protokollierten Einträge sind schreibgeschützt und bleiben nach einem Neustart im Gerät gespeichert.

Anmerkung: In der Voreinstellung des Geräts ist der Zugang zum System-Monitor während des Neustarts möglich. Ein Angreifer, der sich physisch Zugriff auf das Gerät verschafft, kann mit dem System-Monitor die Einstellungen im Gerät auf die voreingestellten Werte zurücksetzen. Anschließend ist der Zugriff auf das Gerät mit dem Standard-Passwort möglich, auch auf die Protokoll-Datei. Treffen Sie entsprechende Maßnahmen, um den physischen Zugriff auf das Gerät zu beschränken. Andernfalls deaktivieren Sie den Zugang zum System-Monitor. Siehe Dialog *Diagnose > System > Selbsttest*, Kontrollkästchen *SysMon1 ist verfügbar*.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Audit-Trail-Datei speichern	Öffnet die HTML-Seite in einem neuen Web-Browser-Fenster oder -Tab. Sie können die HTML-Seite mit dem entsprechenden Web-Browser-Befehl auf Ihrem PC speichern.

7 **Erweitert**

Das Menü enthält die folgenden Dialoge:

- ▶ [Industrie-Protokolle](#)

7.1 Industrie-Protokolle

Das Menü enthält die folgenden Dialoge:

- ▶ IEC61850-MMS
- ▶ Modbus TCP
- ▶ EtherNet/IP
- ▶ PROFINET

7.1.1 IEC61850-MMS

IEC61850 MMS ist ein von der International Electrotechnical Commission (IEC) standardisiertes industrielles Kommunikationsprotokoll. Switches verwenden beispielsweise dieses Protokoll, wenn sie mit Anlagenkomponenten kommunizieren.

Das Paket-orientierte Protokoll definiert eine einheitliche Kommunikationssprache auf Grundlage des Transport-Protokolls TCP/IP. Das Protokoll verwendet einen Manufacturing-Message-Specification(MMS)-Server für die Kommunikation der Client-Server. Das Protokoll beinhaltet Funktionen für SCADA, Intelligent Electronic Device (IED) und die Netzüberwachungssysteme.

Anmerkung: IEC61850/MMS bietet keine Authentifizierungsmechanismen. Ist der Schreibzugriff für IEC61850/MMS eingeschaltet, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Geräts ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Geräts und zu Ausfällen im Netz.

Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (zum Beispiel Firewall, VPN etc.) getroffen haben, um das Risiko unautorisierter Zugriffe zu reduzieren.

Dieser Dialog bietet Ihnen die Möglichkeit, folgende Server-Einstellungen für MMS festzulegen:

- ▶ Aktiviert/deaktiviert den MMS-Server.
- ▶ Aktiviert/deaktiviert den Schreibzugriff auf den MMS-Server
- ▶ TCP-Port des MMS-Servers.
- ▶ Die maximale Anzahl an MMS-Server-Sitzungen.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet den <i>IEC61850-MMS</i> -Server ein/aus. Mögliche Werte: ▶ An Der <i>IEC61850-MMS</i> -Server ist eingeschaltet. ▶ Aus (Voreinstellung) Der <i>IEC61850-MMS</i> -Server ist ausgeschaltet. Die IEC61850 MIBs bleiben zugänglich.

■ Konfiguration

Parameter	Bedeutung
Schreibzugriff	Aktiviert/deaktiviert den Schreibzugriff auf den MMS-Server Mögliche Werte: ▶ markiert Der Schreibzugriff auf den MMS-Server ist aktiviert. Diese Einstellung bietet Ihnen die Möglichkeit, die Geräte-Einstellungen über das Protokoll IEC 61850 MMS zu ändern. ▶ unmarkiert (Voreinstellung) Der Schreibzugriff auf den MMS-Server ist deaktiviert. Der MMS-Server ist mit Lese-Zugriff erreichbar.


Parameter	Bedeutung
Technical-Key	<p>Legt den IED-Namen fest. Der IED-Name ist unabhängig vom System-Namen einstellbar.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen Die folgenden Zeichen sind zulässig: - - 0..9 - a..z - A..Z (Voreinstellung: KEY) <p>Damit der MMS-Server den IED-Namen verwendet, klicken Sie die Schaltfläche <input checked="" type="checkbox"/> und starten Sie den MMS-Server neu. Dabei bricht die Verbindung zu verbundenen Clients ab.</p>
TCP-Port	<p>Legt den TCP-Port für den Zugriff auf den MMS-Server fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..65535 (Voreinstellung: 102) Ausnahme: Port 2222 ist für interne Funktionen reserviert. <p>Anmerkung: Nachdem Sie den Port geändert haben, startet der Server automatisch neu. Offene Verbindungen zum Server beendet das Gerät dabei.</p>
Sessions (max.)	<p>Legt die maximale Anzahl an MMS-Server-Verbindungen fest.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ 1..15 (Voreinstellung: 5)

Information

Parameter	Bedeutung
Status	<p>Zeigt den gegenwärtigen Status des <i>IEC61850-MMS</i>-Servers.</p> <p>Mögliche Werte:</p> <ul style="list-style-type: none"> ▶ unavailable ▶ starting ▶ running ▶ stopping ▶ halted ▶ error

Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Download	Kopiert die ICD-Datei auf Ihren PC.

7.1.2 Modbus TCP

Modbus TCP ist ein Protokoll für die SCADA-Systemintegration (Supervisory Control and Data Acquisition). *Modbus TCP* ist ein herstellerunabhängiges Protokoll, das für die Überwachung und Steuerung von Automatisierungstechnik im Industriebereich eingesetzt wird, zum Beispiel für speicherprogrammierbare Steuerungen (SPS), Sensoren und Messgeräte.

Dieser Dialog bietet Ihnen die Möglichkeit, die Parameter des Protokolls festzulegen. Um die Parameter des Geräts zu überwachen und zu steuern, benötigen Sie Mensch-Maschine-Schnittstellen(HMI)-Software sowie die Speicherzuordnungstabelle. Die unterstützten Objekte und die Speicherzuordnung finden Sie in den Tabellen im Anwender-Handbuch "Industrie-Protokolle".

Der Dialog bietet Ihnen die Möglichkeit, die Funktion sowie den Schreibzugriff zu aktivieren und zu steuern, welchen TCP-Port die Mensch-Maschine-Schnittstelle (Human Machine Interface, HMI) nach Daten abfragt. Darüber hinaus können Sie in diesem Dialog die Anzahl der Sitzungen festlegen, die zeitgleich geöffnet sein dürfen.

Anmerkung: Das Aktivieren des -Schreibzugriffs stellt möglicherweise ein Sicherheitsrisiko dar, da das Protokoll keinen Benutzerzugriff authentifiziert.

Um das Sicherheitsrisiko zu verringern, legen Sie im Dialog *Gerätesicherheit > Management-Zugriff* den IP-Adressbereich fest. Bevor Sie die Funktion einschalten, geben Sie ausschließlich die IP-Adressen ein, die die Ihren Geräten zugewiesen sind. Darüber hinaus ist die Voreinstellung für das Aktivieren der Überwachungsfunktion in der Registerkarte *Gerätesicherheit > Management-Zugriff* aktiviert.

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet den <i>Modbus TCP</i> -Server im Gerät ein/aus. Mögliche Werte: ▶ An Der <i>Modbus TCP</i> -Server ist eingeschaltet. ▶ Aus (Voreinstellung) Der <i>Modbus TCP</i> -Server ist ausgeschaltet.

■ Konfiguration

Parameter	Bedeutung
Schreibzugriff	Aktiviert/deaktiviert den Schreibzugriff auf die <i>Modbus TCP</i> parameter. Anmerkung: Das Aktivieren des -Schreibzugriffs stellt möglicherweise ein Sicherheitsrisiko dar, da das Protokoll keinen Benutzerzugriff authentifiziert. Mögliche Werte: ▶ markiert (Voreinstellung) Der Lese-/Schreibzugriff für den <i>Modbus TCP</i> -Server ist aktiv. Dies bietet Ihnen die Möglichkeit, die Geräte-Konfiguration über das <i>Modbus TCP</i> -Protokoll zu ändern. ▶ unmarkiert Der Lesezugriff für den <i>Modbus TCP</i> -Server ist aktiv.

Parameter	Bedeutung
TCP-Port	Legt die TCP-Port-Nummer fest, die der <i>Modbus TCP</i> -Server für die Kommunikation verwendet. Mögliche Werte: ▶ <TCP-Port-Nummer> (Voreinstellung: 502) Das Festlegen von 0 ist unzulässig.
Sessions (max.)	Legt die maximale Anzahl von gleichzeitigen Sitzungen fest, die der <i>Modbus TCP</i> -Server zulässt. Mögliche Werte: ▶ 1..5 (Voreinstellung: 5)

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

7.1.3 PROFINET

Dieser Dialog bietet Ihnen die Möglichkeit, das PROFINET-Protokoll im Gerät zu konfigurieren, das zusammen mit PROFINET-Controllern und PROFINET-Geräten verwendet wird. Die PROFINET-Funktion des Geräts basiert auf dem PROFINET-Stack V2.2 von Siemens für gängige Ethernet-Controller. Das PROFINET-Protokoll im Gerät entspricht Class B für Antworten in Echtzeit gemäß IEC 61158.

Funktionen mit direktem Einfluss auf die *PROFINET*-Funktion erfordern das Ändern folgender voreingestellter Werte. Wenn Sie das Gerät in einer speziell erhältlichen *PROFINET*-Variante erworben haben, sind diese Werte bereits voreingestellt:

PROFINET	Dialog <i>Erweitert > Industrie-Protokolle > PROFINET</i> – Rahmen <i>Funktion</i> <i>Funktion</i> = An – Rahmen <i>Konfiguration</i> Feld <i>Stationsname</i> = <leer>
Netz	Dialog <i>Grundeinstellungen > Netz</i> – Rahmen <i>Management-Schnittstelle</i> Optionsfeld <i>Zuweisung IP-Adresse</i> = Lokal – Rahmen <i>HiDiscovery Protokoll v1/v2</i> Dropdown-Liste <i>Zugriff</i> = readOnly – Rahmen <i>IP-Parameter</i> Feld <i>IP-Adresse</i> = 0.0.0.0 Feld <i>Netzmaske</i> = 0.0.0.0 Feld <i>Gateway-Adresse</i> = 0.0.0.0
VLAN	Dialog <i>Switching > Global</i> – Rahmen <i>Konfiguration</i> Kontrollkästchen <i>VLAN-Unaware-Modus</i> = markiert
LLDP	Dialog <i>Diagnose > LLDP > Konfiguration</i> – Rahmen <i>Konfiguration</i> Feld <i>Sende-Intervall [s]</i> = 5 Feld <i>Sende-Verzögerung [s]</i> = 1

■ Funktion

Parameter	Bedeutung
Funktion	Schaltet die PROFINET-Funktion im Gerät ein/aus. Mögliche Werte: ▶ An Die PROFINET-Funktion ist eingeschaltet. ▶ Aus (Voreinstellung) Die PROFINET-Funktion ist ausgeschaltet.

■ Konfiguration

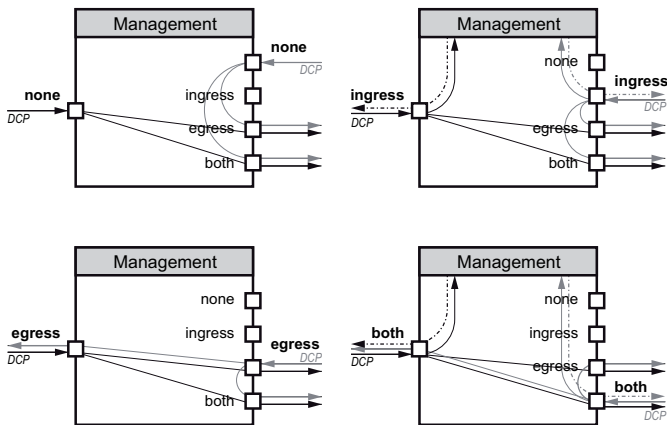
Parameter	Bedeutung
Stationsname	Legt den Namen des Geräts fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..240 Zeichen Das Gerät erlaubt keine Verwendung einer Ziffer als erstes Zeichen.

■ **Information**

Parameter	Bedeutung
Aktive Application-Relations	Zeigt, wie viele Application-Relations aktiv sind.

■ **Tabelle**

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
DCP mode	<p>Legt die Richtung des Datenstroms für DCP-Pakete am zu überwachenden Port fest.</p> <p>Die speicherprogrammierbare Steuerung (SPS) erkennt PROFINET-Geräte über das Discovery-and-Configuration-Protokoll (DCP).</p> <p>Die DCP-Identifizierungsanfrage-Pakete sind multicast, die Antworten der Agenten sind unicast. Unabhängig von den Einstellungen leitet das Gerät die empfangenen DCP-Pakete an andere Ports mit der Einstellung <code>egress</code> oder <code>both</code> weiter.</p>




Mögliche Werte:

- ▶ `none`
Der Agent antwortet auf keine Pakete, die auf diesem Port empfangen wurden. Der Port leitet keine Pakete weiter, die auf anderen Ports empfangen wurden.
- ▶ `ingress`
Der Agent antwortet auf Pakete, die auf diesem Port empfangen wurden. Der Port leitet keine Pakete weiter, die auf anderen Ports empfangen wurden.
- ▶ `egress`
Der Agent antwortet auf keine Pakete, die auf diesem Port empfangen wurden. Der Port leitet Pakete weiter, die auf anderen Ports empfangen wurden.
- ▶ `both` (Voreinstellung)
Der Agent antwortet auf Pakete, die auf diesem Port empfangen wurden. Der Port leitet Pakete weiter, die auf anderen Ports empfangen wurden.

■ **Schaltflächen**

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „Schaltflächen“ auf Seite 19.

Parameter	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
GSDML-Datei herunterladen	Kopiert die GSDML-Datei auf Ihren PC.

7.1.4 EtherNet/IP

Dieser Dialog bietet Ihnen die Möglichkeit, das Protokoll zu aktivieren, die SET/GET-Funktion zu ändern und die EDS-Datei vom Gerät herunterzuladen.

■ Funktion


Parameter	Bedeutung
Funktion	Schaltet die <i>EtherNet/IP</i> -Funktion im Gerät ein/aus. Mögliche Werte: <ul style="list-style-type: none"> ▶ An Die <i>EtherNet/IP</i>-Funktion ist eingeschaltet. ▶ Aus (Voreinstellung) Die <i>EtherNet/IP</i>-Funktion ist ausgeschaltet. Das Gerät liest weiterhin die EtherNet/IP-Daten.

■ Konfiguration

Parameter	Bedeutung
Schreibzugriff	Aktiviert/deaktiviert den Lese-/Schreibzugriff des Protokolls. Mögliche Werte: <ul style="list-style-type: none"> ▶ markiert Das Protokoll erlaubt GET- und SET-Requests. ▶ unmarkiert (Voreinstellung) Das Protokoll erlaubt ausschließlich GET-Requests.

■ Schaltflächen

Die Beschreibung der Standard-Schaltflächen finden Sie im Abschnitt „[Schaltflächen](#)“ auf Seite 19.

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
EDS-Datei herunterladen	Kopiert die folgenden Informationen in eine Zip-Datei auf Ihren PC: <ul style="list-style-type: none"> ▶ ElektronischesDatenblatt (EDS) mit gerätebezogenen Informationen ▶ Gerätsymbol

A Index

1			
802.1D/p-Mapping		174	
802.1X		86, 119	
A			
Adresskonflikt-Erkennung		243	
Aging Time		142, 246	
Alarmer		237	
Anforderungsintervall		60	
ARP		243	
ARP-Tabelle		246	
Audit-Trail		281	
Ausgangs-Lastbegrenzer		144	
Authentifizierungs-Historie		127	
Authentifizierungs-Liste		86	
Auto-Disable		115, 204, 256, 257, 257, 263	
B			
Benutzerverwaltung		82	
Boundary Clock		68	
Bridge		202	
C			
CLI		107	
Command Line Interface		107	
Community-Namen		110	
D			
DoS		137	
DSCP		175	
E			
EAPOL		126	
Eingangs-Lastbegrenzer		144	
Einstellungen		32	
ENVM		31	
Ereignis-Schweregrad		279	
EtherNet/IP		234, 291	
Externer Speicher		31	
F			
Fast\ MRP		184, 185	
FAQ		295	
FDB		146	
Fingerprint		97, 101	
Flash-Speicher		31, 240	
Flusskontrolle		142	
Forwarding-Tabelle		146	
G			
Gerätstatus		22, 225	
Geräte-Software		30	
Grenzwerte Netzlast		144	
Guards		212	
H			
Hardware-Zustand		240	
HiDiscovery		25, 26, 27, 93, 233, 281	
Host-Key		98	
HSR (hardwareabhängig)		194	
HTML		239, 280	
HTTP		99	
HTTPS		100	
HTTP-Server		232	
I			
IAS		86, 129	
IEC61850 MMS		233, 285	
IEEE 802.1X		86	
IGMP-Snooping		148	
Industrial HiVision		11, 93	
Ingress Filtering		182	
Integrierter Authentifikations-Server		86, 129	
IP-Adressen Konflikterkennung		243	
IP-DSCP-Mapping		175	
IP-Zugriffsbeschränkung		103	
IRIG-B		55	
K			
Konfigurationsprofil		17, 32	
Konfigurations-Check		241	
Kontextmenü		17	
L			
Laden/Speichern		32	
Lastbegrenzer		144	
Link-Aggregation		214	
Link-Backup		219	
LLDP		269	
Logdatei		48, 280	
Login-Banner		109, 111	
Loops		201	
M			
Management-VLAN		26	
Management-Zugriff		25, 103	
Manufacturing Message Specification		285	
MAC-Adress-Filter		146	
MAC-Adress-Tabelle		146	
MAC-Flooding		114	
MAC-Spoofing		114	
Media Redundancy Protocol		184	
Menü		17	
MMRP		162	
MMS		285	
Modbus TCP		234, 287	
MRP		184	
MRP-IEEE		160	
MVRP		167	
N			
Netzlast		47, 47	
Neustart		48	
NVM		16, 18, 31, 35	
P			
Parallel Redundancy Protocol (hardwareabhängig)		187	
Passwort		82, 231, 232	
Passwort-Länge		82, 231	
Portsicherheit		114	
Port-basierte Zugriffskontrolle		119	

Port-Clients	125	VLAN	26, 178
Port-Konfiguration	122, 173	VLAN Konfiguration	180
Port-Mirroring	266	VLAN-Ports	182
Port-Monitor	263	VLAN-Unaware-Modus	142
Port-Priorität	173	V.24	233
Port-Statistiken	126	W	
Port-VLAN	182	Warteschlange (Queue)	172
PPS	55	Watchdog	32, 34
Pre-Login-Banner	111	Webserver	99, 100
PROFINET	234, 289	Z	
PRP (hardwareabhängig)	187	Zähler-Reset	48
Q		Zeitzeichen	55
Queues	172	Zertifikat	23, 39, 101, 102, 234
Queue-Management	177	ZIP-Archiv	279
R		Zugriffsbeschränkung	103
RADIUS	86, 130	Zugriffskontrolle	119
RAM	35		
RAM-Test	247		
Ringstruktur	184		
Root-Bridge	202		
RSTP	201, 202		
S			
Schulungsangebote	295		
Schweregrad	279		
Secure Shell	96		
Selbsttest	247		
SFP-Modul	252		
Sicherheitsstatus	22, 230		
Signatur	97		
SNMPv1/v2	110		
SNMP-Server	93, 233		
SNMP-Traps	43, 115, 202, 215, 226, 231, 237, 245, 256		
SNTP	59		
SNTP-Client	60		
SNTP-Server	63		
Software-Update	30		
Sommerzeit	52		
Spanning Tree Protocol	201		
SSH-Server	96		
Stromversorgung	23		
Switch-Dump	279		
Syslog	249		
Systeminformationen	239		
Systemzeit	51		
System Log	280		
System-Monitor	247		
T			
Technische Fragen	295		
Telnet-Server	95, 232		
Topologie-Erkennung	273		
Transparent Clock	75		
Traps	43, 115, 202, 215, 226, 231, 237, 245, 256		
Trap-Ziel	237		
Trust Modus	173		
U			
Unaware-Modus	142		
V			
Verschlüsselung	32		
Virtual Local Area Network	178		

B 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>.

Eine Liste von Telefonnummern und E-Mail-Adressen für direkten technischen Support durch Hirschmann finden Sie unter <https://hirschmann-support.belden.eu.com>.

Sie finden auf dieser Website außerdem eine kostenfreie Wissensdatenbank sowie einen Download-Bereich für Software.

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.hicom-center.com>.
- ▶ Der Support reicht von der Inbetriebnahme über den Bereitschaftsservice 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>

C Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, um Sie beim Einsatz dieses Produkts zu unterstützen. Ihre Kommentare und Anregungen helfen uns dabei, die Qualität und den Informationsgrad dieser Dokumentation weiter zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	gut	befriedigend	mäßig	schlecht
Exakte Beschreibung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lesbarkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verständlichkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Beispiele	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Aufbau	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vollständigkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Grafiken	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Zeichnungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tabellen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Haben Sie in diesem Handbuch Fehler entdeckt?

Wenn ja, welche auf welcher Seite?

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- ▶ als Fax an die Nummer +49 (0)7127 14-1600 oder
- ▶ per Post an

Hirschmann Automation and Control GmbH
Abteilung 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen



HIRSCHMANN

A **BELDEN** BRAND



HIRSCHMANN

A **BELDEN** BRAND

Reference Manual

Command Line Interface HiOS-2E EES (Embedded Ethernet Switch)

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

© 2016 Hirschmann Automation and Control GmbH

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

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

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

You can get the latest version of this manual on the Internet at the Hirschmann product site (www.hirschmann.com).

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

Contents

Safety instructions	25
About this Manual	27
1 Command reference	29
2 Address Conflict Detection (ACD)	31
2.1 address-conflict	32
2.1.1 address-conflict operation	32
2.1.2 address-conflict detection-mode	32
2.1.3 address-conflict detection-ongoing	33
2.1.4 address-conflict delay	33
2.1.5 address-conflict release-delay	33
2.1.6 address-conflict max-protection	34
2.1.7 address-conflict protect-interval	34
2.1.8 address-conflict trap-status	34
2.2 show	35
2.2.1 show address-conflict global	35
2.2.2 show address-conflict detected	35
2.2.3 show address-conflict fault-state	35
2.2.4 show mac-address-conflict global	36
3 Application Lists	37
3.1 applists	38
3.1.1 applists set-authlist	38
3.1.2 applists enable	38
3.1.3 applists disable	38
3.2 show	39
3.2.1 show applists	39
4 Authentication Lists	41
4.1 authlists	42
4.1.1 authlists add	42
4.1.2 authlists delete	42
4.1.3 authlists set-policy	42
4.1.4 authlists enable	43
4.1.5 authlists disable	44
4.2 show	45
4.2.1 show authlists	45
5 Auto Disable	47
5.1 auto-disable	48
5.1.1 auto-disable reason	48
5.2 auto-disable	49
5.2.1 auto-disable timer	49
5.2.2 auto-disable reset	49
5.3 show	50
5.3.1 show auto-disable brief	50
5.3.2 show auto-disable reasons	50
6 Class Of Service	51
6.1 classofservice	52

6.1.1	classofservice ip-dscp-mapping	52
6.1.2	classofservice dot1p-mapping	55
6.2	classofservice	56
6.2.1	classofservice trust	56
6.3	cos-queue	57
6.3.1	cos-queue strict	57
6.3.2	cos-queue weighted	57
6.3.3	cos-queue min-bandwidth	57
6.4	show	59
6.4.1	show classofservice ip-dscp-mapping	59
6.4.2	show classofservice dot1p-mapping	59
6.4.3	show classofservice trust	59
6.4.4	show cos-queue	60
7	Command Line Interface (CLI)	61
7.1	cli	62
7.1.1	cli serial-timeout	62
7.1.2	cli prompt	62
7.1.3	cli numlines	63
7.1.4	cli banner operation	63
7.1.5	cli banner text	63
7.2	show	64
7.2.1	show cli global	64
7.2.2	show cli command-tree	64
7.3	logging	65
7.3.1	logging cli-command	65
7.4	show	66
7.4.1	show logging cli-command	66
8	Clock	67
8.1	clock	68
8.1.1	clock set	68
8.1.2	clock timezone offset	68
8.1.3	clock timezone zone	68
8.1.4	clock summer-time mode	69
8.1.5	clock summer-time recurring start	69
8.1.6	clock summer-time recurring end	70
8.1.7	clock summer-time zone	70
8.2	show	71
8.2.1	show clock	71
9	Configuration	73
9.1	save	74
9.1.1	save profile	74
9.2	config	75
9.2.1	config watchdog admin-state	75
9.2.2	config watchdog timeout	75
9.2.3	config encryption password set	76
9.2.4	config encryption password clear	76
9.2.5	config envm auto-update	76
9.2.6	config envm sshkey-auto-update	77
9.2.7	config envm config-save	77
9.2.8	config envm load-priority	78
9.2.9	config profile select	78
9.2.10	config profile delete	78
9.2.11	config fingerprint verify	79
9.3	copy	80

9.3.1	copy sysinfo system envm	80
9.3.2	copy sysinfoall system envm	80
9.3.3	copy firmware remote	80
9.3.4	copy config running-config nvm	81
9.3.5	copy config running-config remote	81
9.3.6	copy config nvm	81
9.3.7	copy config remote	82
9.3.8	copy sfp-white-list remote	82
9.3.9	copy sfp-white-list envm	82
9.4	clear	83
9.4.1	clear config	83
9.4.2	clear factory	83
9.5	show	84
9.5.1	show running-config xml	84
9.5.2	show running-config script	84
9.6	show	85
9.6.1	show config envm settings	85
9.6.2	show config envm properties	85
9.6.3	show config watchdog	85
9.6.4	show config encryption	86
9.6.5	show config profiles	86
9.6.6	show config status	86
10	Debugging	87
10.1	debug	88
10.1.1	debug tcpdump help	88
10.1.2	debug tcpdump start cpu	88
10.1.3	debug tcpdump stop	88
10.1.4	debug tcpdump filter show	89
10.1.5	debug tcpdump filter list	89
10.1.6	debug tcpdump filter delete	89
10.2	show	90
10.2.1	show debug logic-modules	90
10.3	copy	91
10.3.1	copy tcpdumpcap nvm remote	91
10.3.2	copy tcpdumpfilter remote	91
10.3.3	copy tcpdumpfilter nvm	91
11	Device Monitoring	93
11.1	device-status	94
11.1.1	device-status monitor link-failure	94
11.1.2	device-status monitor ring-redundancy	94
11.1.3	device-status trap	95
11.2	device-status	96
11.2.1	device-status link-alarm	96
11.3	show	97
11.3.1	show device-status monitor	97
11.3.2	show device-status state	97
11.3.3	show device-status trap	97
11.3.4	show device-status events	98
11.3.5	show device-status link-alarm	98
11.3.6	show device-status all	98
12	Device Security	99
12.1	security-status	100
12.1.1	security-status monitor pwd-change	100
12.1.2	security-status monitor pwd-min-length	100
12.1.3	security-status monitor pwd-policy-config	101

12.1.4	security-status monitor pwd-str-not-config	101
12.1.5	security-status monitor pwd-policy-inactive	101
12.1.6	security-status monitor bypass-pwd-strength	102
12.1.7	security-status monitor telnet-enabled	102
12.1.8	security-status monitor http-enabled	103
12.1.9	security-status monitor snmp-unsecure	103
12.1.10	security-status monitor sysmon-enabled	103
12.1.11	security-status monitor no-link-enabled	104
12.1.12	security-status monitor hidisc-write-enabled	104
12.1.13	security-status monitor iec61850-mms-enabled	105
12.1.14	security-status monitor https-certificate	105
12.1.15	security-status monitor modbus-tcp-enabled	105
12.1.16	security-status monitor ethernet-ip-enabled	106
12.1.17	security-status monitor profinet-io-enabled	106
12.1.18	security-status trap	107
12.2	security-status	108
12.2.1	security-status no-link	108
12.3	show	109
12.3.1	show security-status monitor	109
12.3.2	show security-status state	109
12.3.3	show security-status no-link	109
12.3.4	show security-status trap	110
12.3.5	show security-status events	110
12.3.6	show security-status all	110
13	DHCP Layer 2 Relay	111
13.1	clear	112
13.1.1	clear dhcp-l2relay statistics	112
13.2	show	113
13.2.1	show dhcp-l2relay global	113
13.2.2	show dhcp-l2relay statistics	113
13.2.3	show dhcp-l2relay interfaces	113
13.2.4	show dhcp-l2relay vlan	114
14	DHCP Snooping	115
14.1	clear	116
14.1.1	clear ip dhcp-snooping bindings	116
14.1.2	clear ip dhcp-snooping statistics	116
14.2	show	117
14.2.1	show ip dhcp-snooping global	117
14.2.2	show ip dhcp-snooping statistics	117
14.2.3	show ip dhcp-snooping interfaces	117
14.2.4	show ip dhcp-snooping vlan	118
14.2.5	show ip dhcp-snooping bindings	118
15	DoS Mitigation	119
15.1	dos	120
15.1.1	dos tcp-null	120
15.1.2	dos tcp-xmas	120
15.1.3	dos tcp-syn-fin	121
15.1.4	dos tcp-min-header	121
15.1.5	dos icmp-fragmented	121
15.1.6	dos icmp payload-check	122
15.1.7	dos icmp payload-size	122
15.1.8	dos ip-land	123
15.1.9	dos tcp-offset	123
15.1.10	dos tcp-syn	123
15.1.11	dos l4-port	124
15.2	show	125

15.2.1	show dos	125
16	IEEE 802.1x (Dot1x)	127
16.1	dot1x	128
16.1.1	dot1x dynamic-vlan	128
16.1.2	dot1x system-auth-control	128
16.1.3	dot1x monitor	129
16.2	dot1x	130
16.2.1	dot1x guest-vlan	130
16.2.2	dot1x max-req	130
16.2.3	dot1x port-control	130
16.2.4	dot1x re-authentication	131
16.2.5	dot1x unauthenticated-vlan	131
16.2.6	dot1x timeout guest-vlan-period	132
16.2.7	dot1x timeout reauth-period	132
16.2.8	dot1x timeout quiet-period	132
16.2.9	dot1x timeout tx-period	132
16.2.10	dot1x timeout supp-timeout	133
16.2.11	dot1x timeout server-timeout	133
16.2.12	dot1x initialize	133
16.2.13	dot1x re-authenticate	134
16.3	show	135
16.3.1	show dot1x global	135
16.3.2	show dot1x auth-history	135
16.3.3	show dot1x detail	135
16.3.4	show dot1x summary	136
16.3.5	show dot1x clients	136
16.3.6	show dot1x statistics	136
16.4	clear	137
16.4.1	clear dot1x statistics port	137
16.4.2	clear dot1x statistics all	137
16.4.3	clear dot1x auth-history port	137
16.4.4	clear dot1x auth-history all	138
17	IEEE 802.3ad (Dot3ad)	139
17.1	link-aggregation	140
17.1.1	link-aggregation add	140
17.1.2	link-aggregation modify	140
17.1.3	link-aggregation delete	141
17.2	lACP	142
17.2.1	lACP admin-key	142
17.2.2	lACP collector-max-delay	142
17.2.3	lACP lacpmode	142
17.2.4	lACP actor admin key	143
17.2.5	lACP actor admin state lacp-activity	143
17.2.6	lACP actor admin state lacp-timeout	144
17.2.7	lACP actor admin state aggregation	144
17.2.8	lACP actor admin port priority	144
17.2.9	lACP partner admin key	145
17.2.10	lACP partner admin state lacp-activity	145
17.2.11	lACP partner admin state lacp-timeout	145
17.2.12	lACP partner admin state aggregation	146
17.2.13	lACP partner admin port priority	146
17.2.14	lACP partner admin port id	146
17.2.15	lACP partner admin system-priority	147
17.2.16	lACP partner admin system-id	147
17.3	show	148
17.3.1	show link-aggregation port	148
17.3.2	show link-aggregation statistics	148
17.3.3	show link-aggregation members	148

17.3.4	show lacp interface	149
17.3.5	show lacp mode	149
17.3.6	show lacp actor	149
17.3.7	show lacp partner operational	149
17.3.8	show lacp partner admin	150
18	Ethernet IP	151
18.1	ethernet-ip	152
18.1.1	ethernet-ip operation	152
18.1.2	ethernet-ip write-access	152
18.2	show	153
18.2.1	show ethernet-ip	153
18.3	copy	154
18.3.1	copy eds-ethernet-ip system remote	154
19	Filtering Database (FDB)	155
19.1	mac-filter	156
19.1.1	mac-filter	156
19.2	bridge	157
19.2.1	bridge aging-time	157
19.3	show	158
19.3.1	show mac-filter-table static	158
19.4	show	159
19.4.1	show bridge aging-time	159
19.5	show	160
19.5.1	show mac-addr-table	160
19.6	clear	161
19.6.1	clear mac-addr-table	161
20	HiDiscovery	163
20.1	network	164
20.1.1	network hidiscovery operation	164
20.1.2	network hidiscovery mode	164
20.1.3	network hidiscovery blinking	165
20.1.4	network hidiscovery relay	165
20.2	show	166
20.2.1	show network hidiscovery	166
21	High-availability Seamless Redundancy (HSR)	167
21.1	hsr	168
21.1.1	hsr operation	168
21.1.2	hsr instance	168
21.2	clear	170
21.2.1	clear hsr proxy-node-table	170
21.2.2	clear hsr node-table	170
21.2.3	clear hsr counters	170
21.3	show	171
21.3.1	show hsr global	171
21.3.2	show hsr instance	171
21.3.3	show hsr node-table	171
21.3.4	show hsr proxy-node-table	172
21.3.5	show hsr counters	172
22	Hypertext Transfer Protocol (HTTP)	173

22.1	http	174
	22.1.1 http port	174
	22.1.2 http server	174
22.2	show	175
	22.2.1 show http	175
23	HTTP Secure (HTTPS)	177
23.1	https	178
	23.1.1 https server	178
	23.1.2 https port	178
	23.1.3 https certificate	179
23.2	copy	180
	23.2.1 copy https-cert remote	180
	23.2.2 copy https-cert envm	180
23.3	show	181
	23.3.1 show https	181
24	Integrated Authentication Server (IAS)	183
24.1	ias-users	184
	24.1.1 ias-users add	184
	24.1.2 ias-users delete	184
	24.1.3 ias-users enable	184
	24.1.4 ias-users disable	185
	24.1.5 ias-users password	185
24.2	show	186
	24.2.1 show ias-users	186
25	IEC 61850 MMS Server	187
25.1	iec61850-mms	188
	25.1.1 iec61850-mms operation	188
	25.1.2 iec61850-mms write-access	188
	25.1.3 iec61850-mms port	189
	25.1.4 iec61850-mms max-sessions	189
	25.1.5 iec61850-mms technical-key	189
25.2	show	190
	25.2.1 show iec61850-mms	190
26	Internet Group Management Protocol (IGMP)	191
26.1	show	192
	26.1.1 show ip igmp global	192
	26.1.2 show ip igmp interface	192
	26.1.3 show ip igmp membership	192
	26.1.4 show ip igmp groups	193
	26.1.5 show ip igmp statistics	193
27	IGMP Proxy	195
27.1	show	196
	27.1.1 show ip igmp-proxy global	196
	27.1.2 show ip igmp-proxy groups	196
	27.1.3 show ip igmp-proxy source-list	196
28	IGMP Snooping	197
28.1	igmp-snooping	198
	28.1.1 igmp-snooping mode	198
	28.1.2 igmp-snooping querier mode	198
	28.1.3 igmp-snooping querier query-interval	199

28.1.4	igmp-snooping querier timer-expiry	199
28.1.5	igmp-snooping querier version	199
28.1.6	igmp-snooping forward-unknown	200
28.2	igmp-snooping	201
28.2.1	igmp-snooping vlan-id	201
28.3	igmp-snooping	203
28.3.1	igmp-snooping mode	203
28.3.2	igmp-snooping fast-leave	203
28.3.3	igmp-snooping groupmembership-interval	204
28.3.4	igmp-snooping maxresponse	204
28.3.5	igmp-snooping mcrtrexpiretime	204
28.3.6	igmp-snooping static-query-port	204
28.4	show	206
28.4.1	show igmp-snooping global	206
28.4.2	show igmp-snooping interface	206
28.4.3	show igmp-snooping vlan	206
28.4.4	show igmp-snooping querier global	207
28.4.5	show igmp-snooping querier vlan	207
28.4.6	show igmp-snooping enhancements vlan	207
28.4.7	show igmp-snooping enhancements unknown-filtering	207
28.4.8	show igmp-snooping statistics global	208
28.4.9	show igmp-snooping statistics interface	208
28.5	show	209
28.5.1	show mac-filter-table igmp-snooping	209
28.6	clear	210
28.6.1	clear igmp-snooping	210
29	Interface	211
29.1	shutdown	212
29.1.1	shutdown	212
29.2	auto-negotiate	213
29.2.1	auto-negotiate	213
29.3	auto-power-down	214
29.3.1	auto-power-down	214
29.4	cable-crossing	215
29.4.1	cable-crossing	215
29.5	linktraps	216
29.5.1	linktraps	216
29.6	link-loss-alert	217
29.6.1	link-loss-alert operation	217
29.7	speed	218
29.7.1	speed	218
29.8	name	219
29.8.1	name	219
29.9	power-state	220
29.9.1	power-state	220
29.10	mac-filter	221
29.10.1	mac-filter	221
29.11	led-signaling	222
29.11.1	led-signaling operation	222
29.12	show	223
29.12.1	show port	223
29.13	show	224
29.13.1	show link-loss-alert	224

29.14	show	225
29.14.1	show led-signaling operation	225
30	Interface Statistics	227
30.1	utilization	228
30.1.1	utilization control-interval	228
30.1.2	utilization alarm-threshold lower	228
30.1.3	utilization alarm-threshold upper	228
30.2	clear	230
30.2.1	clear port-statistics	230
30.3	show	231
30.3.1	show interface counters	231
30.3.2	show interface layout	231
30.3.3	show interface utilization	231
30.3.4	show interface statistics	232
30.3.5	show interface ether-stats	232
31	Intern	233
31.1	help	234
31.2	logout	235
31.3	history	236
31.4	vlan-mode	237
31.4.1	vlan-mode	237
31.5	exit	238
31.6	end	239
31.7	serviceshell	240
31.7.1	serviceshell deactivate	240
31.8	serviceshell-f	241
31.8.1	serviceshell-f deactivate	241
31.9	traceroute	242
31.9.1	traceroute maxttl	242
31.10	traceroute	243
31.10.1	traceroute source	243
31.11	reboot	244
31.11.1	reboot after	244
31.12	ping	245
31.12.1	ping	245
31.13	ping	246
31.13.1	ping source	246
31.14	show	247
31.14.1	show reboot	247
31.14.2	show serviceshell	247
32	Open Shortest Path First (OSPF)	249
32.1	show	250
32.1.1	show ip ospf global	250
32.1.2	show ip ospf area	250
32.1.3	show ip ospf stub	250
32.1.4	show ip ospf database internal	251
32.1.5	show ip ospf database external	251
32.1.6	show ip ospf range	251
32.1.7	show ip ospf interface	251
32.1.8	show ip ospf virtual-link	252

32.1.9	show ip ospf virtual-neighbor	252
32.1.10	show ip ospf neighbor	252
32.1.11	show ip ospf statistics	252
32.1.12	show ip ospf re-distribute	253
32.1.13	show ip ospf nssa	253
32.1.14	show ip ospf route	253
33	Internet Protocol Version 4 (IPv4)	255
33.1	network	256
33.1.1	network protocol	256
33.1.2	network parms	256
33.2	clear	257
33.2.1	clear arp-table-switch	257
33.3	show	258
33.3.1	show network parms	258
33.4	show	259
33.4.1	show arp	259
34	Inter Range Instrumentation Group IRIG-B	261
34.1	irig-b	262
34.1.1	irig-b operation	262
34.1.2	irig-b mode	262
34.1.3	irig-b pps	263
34.1.4	irig-b time	263
34.2	show	264
34.2.1	show irig-b	264
35	Link Backup	265
35.1	link-backup	266
35.1.1	link-backup operation	266
35.2	link-backup	267
35.2.1	link-backup add	267
35.2.2	link-backup delete	267
35.2.3	link-backup modify	268
35.3	show	269
35.3.1	show link-backup operation	269
35.3.2	show link-backup pairs	269
36	Link Layer Discovery Protocol (LLDP)	271
36.1	lldp	272
36.1.1	lldp operation	272
36.1.2	lldp config chassis admin-state	272
36.1.3	lldp config chassis notification-interval	273
36.1.4	lldp config chassis re-init-delay	273
36.1.5	lldp config chassis tx-delay	273
36.1.6	lldp config chassis tx-hold-multiplier	274
36.1.7	lldp config chassis tx-interval	274
36.2	show	275
36.2.1	show lldp global	275
36.2.2	show lldp port	275
36.2.3	show lldp remote-data	275
36.3	lldp	276
36.3.1	lldp admin-state	276
36.3.2	lldp fdb-mode	276
36.3.3	lldp max-neighbors	277
36.3.4	lldp notification	277

36.3.5	lldp tlv inline-power	277
36.3.6	lldp tlv link-aggregation	278
36.3.7	lldp tlv mac-phy-config-state	278
36.3.8	lldp tlv max-frame-size	278
36.3.9	lldp tlv mgmt-addr	279
36.3.10	lldp tlv port-desc	279
36.3.11	lldp tlv port-vlan	280
36.3.12	lldp tlv protocol	280
36.3.13	lldp tlv sys-cap	281
36.3.14	lldp tlv sys-desc	281
36.3.15	lldp tlv sys-name	281
36.3.16	lldp tlv vlan-name	282
36.3.17	lldp tlv protocol-based-vlan	282
36.3.18	lldp tlv igmp	283
36.3.19	lldp tlv portsec	283
36.3.20	lldp tlv ptp	283
36.3.21	lldp tlv pnio	284
36.3.22	lldp tlv pnio-alias	284
36.3.23	lldp tlv pnio-mrp	285
37	Media Endpoint Discovery LLDP-MED	287
37.1	lldp	288
37.1.1	lldp med confignotification	288
37.1.2	lldp med transmit-tlv capabilities	288
37.1.3	lldp med transmit-tlv network-policy	289
37.2	lldp	290
37.2.1	lldp med faststartrepeatcount	290
37.3	show	291
37.3.1	show lldp med global	291
37.3.2	show lldp med interface	291
37.3.3	show lldp med local-device	291
37.3.4	show lldp med remote-device detail	292
37.3.5	show lldp med remote-device summary	292
38	Logging	293
38.1	logging	294
38.1.1	logging audit-trail	294
38.1.2	logging buffered severity	294
38.1.3	logging host add	295
38.1.4	logging host delete	295
38.1.5	logging host enable	296
38.1.6	logging host disable	296
38.1.7	logging host modify	296
38.1.8	logging syslog operation	297
38.1.9	logging current-console operation	297
38.1.10	logging current-console severity	298
38.1.11	logging console operation	298
38.1.12	logging console severity	299
38.1.13	logging persistent operation	299
38.1.14	logging persistent numfiles	300
38.1.15	logging persistent filesize	300
38.1.16	logging persistent severity-level	300
38.1.17	logging email operation	301
38.1.18	logging email from-addr	301
38.1.19	logging email duration	302
38.1.20	logging email severity urgent	302
38.1.21	logging email severity non-urgent	303
38.1.22	logging email to-addr add	303
38.1.23	logging email to-addr delete	304
38.1.24	logging email to-addr modify	304
38.1.25	logging email mail-server add	304

38.1.26	logging email mail-server delete	305
38.1.27	logging email mail-server modify	305
38.1.28	logging email subject add	306
38.1.29	logging email subject delete	306
38.1.30	logging email subject modify	307
38.1.31	logging email test msgtype	307
38.2	show	308
38.2.1	show logging buffered	308
38.2.2	show logging traplogs	308
38.2.3	show logging console	308
38.2.4	show logging syslog	309
38.2.5	show logging host	309
38.2.6	show logging email statistics	309
38.2.7	show logging email global	309
38.2.8	show logging email to-addr	310
38.2.9	show logging email subject	310
38.2.10	show logging email mail-server	310
38.3	copy	311
38.3.1	copy eventlog buffered remote	311
38.3.2	copy traplog system remote	311
38.3.3	copy audittrail system remote	311
38.3.4	copy mailcert remote	312
38.3.5	copy mailcert envm	312
38.3.6	copy syslogcert remote	312
38.3.7	copy syslogcert envm	313
38.4	clear	314
38.4.1	clear logging buffered	314
38.4.2	clear logging email statistics	314
38.4.3	clear eventlog	314
39	Parallel Redundancy Protocol (PRP)	315
39.1	prp	316
39.1.1	prp operation	316
39.1.2	prp instance	316
39.2	show	318
39.2.1	show prp global	318
39.2.2	show prp instance	318
39.2.3	show prp node-table	318
39.2.4	show prp proxy-node-table	319
39.2.5	show prp counters	319
39.3	clear	320
39.3.1	clear prp proxy-node-table	320
39.3.2	clear prp node-table	320
39.3.3	clear prp counters	320
40	Management Access	321
40.1	network	322
40.1.1	network management access web timeout	322
40.1.2	network management access add	322
40.1.3	network management access delete	323
40.1.4	network management access modify	323
40.1.5	network management access operation	324
40.1.6	network management access status	325
40.2	show	326
40.2.1	show network management access global	326
40.2.2	show network management access rules	326
41	Management Address	327

41.1	network	328
	41.1.1 network management mac	328
	41.1.2 network management port	328
41.2	show	329
	41.2.1 show network management mac	329
	41.2.2 show network management port	329
42	Modbus	331
42.1	modbus-tcp	332
	42.1.1 modbus-tcp operation	332
	42.1.2 modbus-tcp write-access	332
	42.1.3 modbus-tcp port	333
	42.1.4 modbus-tcp max-sessions	333
42.2	show	334
	42.2.1 show modbus-tcp	334
43	Media Redundancy Protocol (MRP)	335
43.1	mrp	336
	43.1.1 mrp domain modify advanced-mode	336
	43.1.2 mrp domain modify manager-priority	336
	43.1.3 mrp domain modify mode	336
	43.1.4 mrp domain modify name	337
	43.1.5 mrp domain modify operation	337
	43.1.6 mrp domain modify port primary	337
	43.1.7 mrp domain modify port secondary	338
	43.1.8 mrp domain modify recovery-delay	338
	43.1.9 mrp domain modify round-trip-delay	338
	43.1.10 mrp domain modify vlan	339
	43.1.11 mrp domain add default-domain	339
	43.1.12 mrp domain add domain-id	339
	43.1.13 mrp domain delete	339
	43.1.14 mrp operation	340
43.2	show	341
	43.2.1 show mrp	341
44	MRP IEEE	343
44.1	mrp-ieee	344
	44.1.1 mrp-ieee global join-time	344
	44.1.2 mrp-ieee global leave-time	344
	44.1.3 mrp-ieee global leave-all-time	345
44.2	show	346
	44.2.1 show mrp-ieee global interface	346
45	MRP IEEE MMRP	347
45.1	mrp-ieee	348
	45.1.1 mrp-ieee mmrp vlan-id	348
45.2	show	349
	45.2.1 show mrp-ieee mmrp global	349
	45.2.2 show mrp-ieee mmrp interface	349
	45.2.3 show mrp-ieee mmrp statistics global	349
	45.2.4 show mrp-ieee mmrp statistics interface	350
	45.2.5 show mrp-ieee mmrp service-requirement forward-all vlan	350
	45.2.6 show mrp-ieee mmrp service-requirement forbidden vlan	350
45.3	mrp-ieee	351
	45.3.1 mrp-ieee mmrp operation	351
	45.3.2 mrp-ieee mmrp periodic-machine	351

45.4	clear	352
45.4.1	clear mrp-ieee mmrp	352
45.5	mrp-ieee	353
45.5.1	mrp-ieee mmrp operation	353
45.5.2	mrp-ieee mmrp restrict-register	353
45.6	show	354
45.6.1	show mac-filter-table mmrp	354
46	MRP IEEE MVRP	355
46.1	mrp-ieee	356
46.1.1	mrp-ieee mvrp operation	356
46.1.2	mrp-ieee mvrp periodic-machine	356
46.2	mrp-ieee	357
46.2.1	mrp-ieee mvrp operation	357
46.2.2	mrp-ieee mvrp restrict-register	357
46.3	show	358
46.3.1	show mrp-ieee mvrp global	358
46.3.2	show mrp-ieee mvrp interface	358
46.3.3	show mrp-ieee mvrp statistics global	358
46.3.4	show mrp-ieee mvrp statistics interface	359
46.4	clear	360
46.4.1	clear mrp-ieee mvrp	360
47	Out-of-band Management	361
47.1	network	362
47.1.1	network out-of-band operation	362
47.1.2	network out-of-band protocol	362
47.1.3	network out-of-band parms	363
47.2	show	364
48	Protocol Based VLAN	365
48.1	vlan	366
48.1.1	vlan protocol group add	366
48.1.2	vlan protocol group modify	366
48.1.3	vlan protocol group delete	367
48.2	vlan	368
48.2.1	vlan protocol group add	368
48.2.2	vlan protocol group delete	368
48.3	show	369
49	Port Monitor	371
49.1	port-monitor	372
49.1.1	port-monitor operation	372
49.2	port-monitor	373
49.2.1	port-monitor condition crc-fragments interval	373
49.2.2	port-monitor condition crc-fragments count	373
49.2.3	port-monitor condition crc-fragments mode	373
49.2.4	port-monitor condition link-flap interval	374
49.2.5	port-monitor condition link-flap count	374
49.2.6	port-monitor condition link-flap mode	374
49.2.7	port-monitor condition duplex-mismatch mode	375
49.2.8	port-monitor condition overload-detection traffic-type	375
49.2.9	port-monitor condition overload-detection unit	376
49.2.10	port-monitor condition overload-detection upper-threshold	376
49.2.11	port-monitor condition overload-detection lower-threshold	376

49.2.12	port-monitor condition overload-detection polling-interval	377
49.2.13	port-monitor condition overload-detection mode	377
49.2.14	port-monitor condition speed-duplex mode	377
49.2.15	port-monitor condition speed-duplex speed	378
49.2.16	port-monitor condition speed-duplex clear	378
49.2.17	port-monitor action	378
49.2.18	port-monitor reset	379
49.3	show	380
49.3.1	show port-monitor operation	380
49.3.2	show port-monitor brief	380
49.3.3	show port-monitor overload-detection counters	380
49.3.4	show port-monitor overload-detection port	381
49.3.5	show port-monitor speed-duplex	381
49.3.6	show port-monitor port	381
49.3.7	show port-monitor link-flap	381
49.3.8	show port-monitor crc-fragments	382
50	Port Security	383
50.1	port-security	384
50.1.1	port-security operation	384
50.2	port-security	385
50.2.1	port-security operation	385
50.2.2	port-security max-dynamic	385
50.2.3	port-security max-static	386
50.2.4	port-security mac-address add	386
50.2.5	port-security mac-address move	386
50.2.6	port-security mac-address delete	386
50.2.7	port-security violation-traps	387
50.3	show	388
50.3.1	show port-security global	388
50.3.2	show port-security interface	388
50.3.3	show port-security dynamic	388
50.3.4	show port-security static	389
50.3.5	show port-security violation	389
51	Profinet IO	391
51.1	profinet	392
51.1.1	profinet operation	392
51.1.2	profinet name-of-station	392
51.2	profinet	393
51.2.1	profinet dcp-mode	393
51.3	copy	394
51.3.1	copy gsdml-profinet system remote	394
51.4	show	395
51.4.1	show profinet global	395
51.4.2	show profinet port	395
52	Precision Time Protocol (PTP)	397
52.1	ptp	398
52.1.1	ptp operation	398
52.1.2	ptp clock-mode	398
52.1.3	ptp sync-lower-bound	399
52.1.4	ptp sync-upper-bound	399
52.1.5	ptp management	399
52.1.6	ptp v2-transparent-clock syntonization	400
52.1.7	ptp v2-transparent-clock network-protocol	400
52.1.8	ptp v2-transparent-clock multi-domain	400
52.1.9	ptp v2-transparent-clock sync-local-clock	401

52.1.10	ptp v2-transparent-clock delay-mechanism	401
52.1.11	ptp v2-transparent-clock primary-domain	401
52.1.12	ptp v2-transparent-clock vlan	402
52.1.13	ptp v2-transparent-clock vlan-priority	402
52.1.14	ptp v2-boundary-clock domain	402
52.1.15	ptp v2-boundary-clock priority1	403
52.1.16	ptp v2-boundary-clock priority2	403
52.1.17	ptp v2-boundary-clock utc-offset	403
52.1.18	ptp v2-boundary-clock utc-offset-valid	403
52.2	ptp	405
52.2.1	ptp v2-transparent-clock operation	405
52.2.2	ptp v2-transparent-clock asymmetry	405
52.2.3	ptp v2-transparent-clock pdelay-interval	406
52.2.4	ptp v2-boundary-clock operation	406
52.2.5	ptp v2-boundary-clock pdelay-interval	406
52.2.6	ptp v2-boundary-clock announce-interval	407
52.2.7	ptp v2-boundary-clock sync-interval	407
52.2.8	ptp v2-boundary-clock announce-timeout	408
52.2.9	ptp v2-boundary-clock asymmetry	408
52.2.10	ptp v2-boundary-clock v1-compatibility-mode	408
52.2.11	ptp v2-boundary-clock delay-mechanism	409
52.2.12	ptp v2-boundary-clock network-protocol	409
52.2.13	ptp v2-boundary-clock vlan-priority	409
52.2.14	ptp v2-boundary-clock vlan	410
52.3	show	411
52.3.1	show ptp	411
53	Password Management	413
53.1	passwords	414
53.1.1	passwords min-length	414
53.1.2	passwords max-login-attempts	414
53.1.3	passwords min-uppercase-chars	414
53.1.4	passwords min-lowercase-chars	415
53.1.5	passwords min-numeric-chars	415
53.1.6	passwords min-special-chars	415
53.2	show	416
53.2.1	show passwords	416
54	Radius	417
54.1	authorization	418
54.1.1	authorization network radius	418
54.2	radius	419
54.2.1	radius accounting mode	419
54.2.2	radius server attribute 4	419
54.2.3	radius server acct add	420
54.2.4	radius server acct delete	420
54.2.5	radius server acct modify	420
54.2.6	radius server auth add	421
54.2.7	radius server auth delete	421
54.2.8	radius server auth modify	422
54.2.9	radius server retransmit	422
54.2.10	radius server timeout	423
54.3	show	424
54.3.1	show radius global	424
54.3.2	show radius auth servers	424
54.3.3	show radius auth statistics	424
54.3.4	show radius acct statistics	425
54.3.5	show radius acct servers	425
54.4	clear	426

54.4.1 clear radius	426
55 Remote Monitoring (RMON)	427
55.1 rmon-alarm	428
55.1.1 rmon-alarm add	428
55.1.2 rmon-alarm enable	428
55.1.3 rmon-alarm disable	429
55.1.4 rmon-alarm delete	429
55.1.5 rmon-alarm modify	429
55.2 show	431
55.2.1 show rmon statistics	431
55.2.2 show rmon alarm	431
56 Script File	433
56.1 script	434
56.1.1 script apply	434
56.1.2 script validate	434
56.1.3 script list system	434
56.1.4 script delete	435
56.2 copy	436
56.2.1 copy script remote	436
56.2.2 copy script nvm	436
56.2.3 copy script running-config nvm	437
56.2.4 copy script running-config remote	437
56.3 show	438
56.3.1 show script system	438
57 Selftest	439
57.1 selftest	440
57.1.1 selftest action	440
57.1.2 selftest ramtest	440
57.1.3 selftest system-monitor	441
57.1.4 selftest boot-default-on-error	441
57.2 show	442
57.2.1 show selftest action	442
57.2.2 show selftest settings	442
58 Small Form-factor Pluggable (SFP)	443
58.1 show	444
58.1.1 show sfp	444
59 Switched Monitoring (SMON)	445
59.1 monitor	446
59.1.1 monitor session	446
59.2 show	448
59.2.1 show monitor session	448
59.3 clear	449
59.3.1 clear monitor session	449
60 Simple Network Management Protocol (SNMP)	451
60.1 snmp	452
60.1.1 snmp access version v1	452
60.1.2 snmp access version v2	452
60.1.3 snmp access version v3	453
60.1.4 snmp access port	453
60.1.5 snmp access snmp-over-802	453

60.2	show	454
60.2.1	show snmp access	454
61	SNMP Community	455
61.1	snmp	456
61.1.1	snmp community ro	456
61.1.2	snmp community rw	456
61.2	show	457
61.2.1	show snmp community	457
62	SNMP Logging	459
62.1	logging	460
62.1.1	logging snmp-request get operation	460
62.1.2	logging snmp-request get severity	460
62.1.3	logging snmp-request set operation	461
62.1.4	logging snmp-request set severity	462
62.2	show	463
62.2.1	show logging snmp	463
63	Simple Network Time Protocol (SNTP)	465
63.1	sntp	466
63.1.1	sntp client operation	466
63.1.2	sntp client operating-mode	466
63.1.3	sntp client request-interval	467
63.1.4	sntp client broadcast-rcv-timeout	467
63.1.5	sntp client disable-after-sync	467
63.1.6	sntp client server add	468
63.1.7	sntp client server delete	468
63.1.8	sntp client server mode	468
63.1.9	sntp server operation	469
63.1.10	sntp server port	469
63.1.11	sntp server only-if-synchronized	469
63.1.12	sntp server broadcast operation	470
63.1.13	sntp server broadcast address	470
63.1.14	sntp server broadcast port	470
63.1.15	sntp server broadcast interval	471
63.1.16	sntp server broadcast vlan	471
63.2	show	472
63.2.1	show sntp global	472
63.2.2	show sntp client status	472
63.2.3	show sntp client server	472
63.2.4	show sntp server status	473
63.2.5	show sntp server broadcast	473
64	Spanning Tree	475
64.1	spanning-tree	476
64.1.1	spanning-tree operation	476
64.1.2	spanning-tree bpdu-filter	476
64.1.3	spanning-tree bpdu-guard	477
64.1.4	spanning-tree bpdu-migration-check	477
64.1.5	spanning-tree forceversion	477
64.1.6	spanning-tree forward-time	478
64.1.7	spanning-tree hello-time	478
64.1.8	spanning-tree hold-count	478
64.1.9	spanning-tree max-age	478
64.1.10	spanning-tree ring-only-mode operation	479
64.1.11	spanning-tree ring-only-mode first-port	479
64.1.12	spanning-tree ring-only-mode second-port	479

64.1.13	spanning-tree mst	480
64.2	spanning-tree	481
64.2.1	spanning-tree mode	481
64.2.2	spanning-tree bpdu-flood	481
64.2.3	spanning-tree edge-auto	482
64.2.4	spanning-tree edge-port	482
64.2.5	spanning-tree guard-loop	482
64.2.6	spanning-tree guard-root	483
64.2.7	spanning-tree guard-tcn	483
64.2.8	spanning-tree cost	484
64.2.9	spanning-tree priority	484
64.3	show	485
64.3.1	show spanning-tree global	485
64.3.2	show spanning-tree mst instance	485
64.3.3	show spanning-tree mst port	485
64.3.4	show spanning-tree port	486
65	Secure Shell (SSH)	487
65.1	ssh	488
65.1.1	ssh server	488
65.1.2	ssh timeout	488
65.1.3	ssh port	489
65.1.4	ssh max-sessions	489
65.1.5	ssh outbound max-sessions	489
65.1.6	ssh outbound timeout	489
65.1.7	ssh key rsa	490
65.1.8	ssh key dsa	490
65.2	copy	491
65.2.1	copy sshkey remote	491
65.3	show	492
65.3.1	show ssh	492
66	Storm Control	493
66.1	storm-control	494
66.1.1	storm-control flow-control	494
66.2	traffic-shape	495
66.2.1	traffic-shape bw	495
66.3	mtu	496
66.3.1	mtu	496
66.4	mtu	497
66.4.1	mtu	497
66.5	mtu	498
66.5.1	mtu	498
66.6	storm-control	499
66.6.1	storm-control flow-control	499
66.6.2	storm-control ingress unit	499
66.6.3	storm-control ingress threshold	500
66.6.4	storm-control ingress unicast operation	500
66.6.5	storm-control ingress multicast operation	500
66.6.6	storm-control ingress broadcast operation	501
66.7	show	502
66.7.1	show storm-control flow-control	502
66.7.2	show storm-control ingress	502
66.7.3	show traffic-shape	502
66.7.4	show mtu	503
67	System	505

67.1	system	506
67.1.1	system name	506
67.1.2	system location	506
67.1.3	system contact	506
67.1.4	system pre-login-banner operation	507
67.1.5	system pre-login-banner text	507
67.1.6	system resources operation	508
67.2	show	509
67.2.1	show eventlog	509
67.2.2	show system info	509
67.2.3	show system pre-login-banner	509
67.2.4	show system flash-status	510
67.2.5	show system temperature limits	510
67.2.6	show system temperature extremes	510
67.2.7	show system temperature histogram	510
67.2.8	show system temperature counters	511
67.2.9	show system resources	511
67.2.10	show psu slot	511
67.2.11	show psu unit	511
68	Telnet	513
68.1	telnet	514
68.1.1	telnet server	514
68.1.2	telnet timeout	514
68.1.3	telnet port	515
68.1.4	telnet max-sessions	515
68.2	show	516
68.2.1	show telnet	516
69	Traps	517
69.1	snmp	518
69.1.1	snmp trap operation	518
69.1.2	snmp trap mode	518
69.1.3	snmp trap delete	519
69.1.4	snmp trap add	519
69.2	show	520
69.2.1	show snmp traps	520
70	User Management	521
70.1	show	522
70.1.1	show custom-role global	522
70.1.2	show custom-role commands	522
71	Users	523
71.1	users	524
71.1.1	users add	524
71.1.2	users delete	524
71.1.3	users enable	524
71.1.4	users disable	525
71.1.5	users password	525
71.1.6	users snmpv3 authentication	525
71.1.7	users snmpv3 encryption	526
71.1.8	users access-role	526
71.1.9	users lock-status	526
71.1.10	users password-policy-check	527
71.2	show	528
71.2.1	show users	528

72	Virtual LAN (VLAN)	529
72.1	name	530
	72.1.1 name	530
72.2	vlan-unaware-mode	531
	72.2.1 vlan-unaware-mode	531
72.3	vlan	532
	72.3.1 vlan add	532
	72.3.2 vlan delete	532
72.4	vlan	533
	72.4.1 vlan acceptframe	533
	72.4.2 vlan ingressfilter	533
	72.4.3 vlan priority	534
	72.4.4 vlan pvid	534
	72.4.5 vlan tagging	534
	72.4.6 vlan participation include	535
	72.4.7 vlan participation exclude	535
	72.4.8 vlan participation auto	535
72.5	show	536
	72.5.1 show vlan id	536
	72.5.2 show vlan brief	536
	72.5.3 show vlan port	536
	72.5.4 show vlan member current	537
	72.5.5 show vlan member static	537
72.6	network	538
	72.6.1 network management vlan	538
	72.6.2 network management priority dot1p	538
	72.6.3 network management priority ip-dscp	538
A	Further Support	539

Safety instructions

 **WARNING**

UNCONTROLLED MACHINE ACTIONS

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

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

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

About this Manual

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “GUI” reference manual contains detailed information on using the graphical interface to operate the individual functions of the device.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

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

The “Redundancy Configuration” user manual document contains the information you require to select the suitable redundancy procedure and configure it.

The document “HiView User Manual” contains information about the GUI application HiView. This application offers you the possibility to use the graphical user interface without other applications such as a Web browser or an installed Java Runtime Environment (JRE).

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:

- ▶ ActiveX control for SCADA integration
- ▶ Auto-topology discovery
- ▶ Browser interface
- ▶ Client/server structure
- ▶ Event handling
- ▶ Event log
- ▶ Simultaneous configuration of multiple devices
- ▶ Graphical user interface with network layout
- ▶ SNMP/OPC gateway

1 Command reference

2 Address Conflict Detection (ACD)

2.1 address-conflict

Configure the address conflict settings.

2.1.1 address-conflict operation

Enable or disable the address conflict component.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict operation

■ no address-conflict operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no address-conflict operation

2.1.2 address-conflict detection-mode

Configure the detection mode.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict detection-mode <P-1>

Parameter	Value	Meaning
P-1	active-and-passive	Configure active and passive detection. During the ip address configuration, if you set the detection to 'active', then the device sends ARP or NDP probes into the network, and if you set the detection to 'passive', then the device listens continuously on the network.
	active-only	Configure only active detection. During ip address configuration 'active' the device sends only one ARP or NDP probe into the network.
	passive-only	Configure passive detection. The device listens passively on the network to verify that another device does not have the same ip address assigned.

2.1.3 address-conflict detection-ongoing

Enable or disable the ongoing detection. If enabled, the device sends periodic ARP or NDP probes.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict detection-ongoing

■ no address-conflict detection-ongoing

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no address-conflict detection-ongoing

2.1.4 address-conflict delay

The maximum detection delay time in milliseconds. Time gap between ARP or NDP probes.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict delay <P-1>

Parameter	Value	Meaning
P-1	20..500	Time gap between consecutive ARP or NDP probes ([ms], default 200).

2.1.5 address-conflict release-delay

Delay in seconds to the next ARP or NDP probe cycle after an ip address conflict was detected.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict release-delay <P-1>

Parameter	Value	Meaning
P-1	3..3600	Delay between consecutive probe cycles after a conflict was detected ([sec], default 15).

2.1.6 address-conflict max-protection

Maximum number of frequent address protections.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict max-protection <P-1>

Parameter	Value	Meaning
P-1	0..100	Maximum number of frequent address protections (default 1).

2.1.7 address-conflict protect-interval

Delay in milliseconds between two consecutive address protections.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict protect-interval <P-1>

Parameter	Value	Meaning
P-1	20..10000	Delay between two consecutive protections ([ms], default 10000).

2.1.8 address-conflict trap-status

If enabled, this trap reports an address conflict.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: address-conflict trap-status

■ no address-conflict trap-status

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no address-conflict trap-status

2.2 show

Display device options and settings.

2.2.1 show address-conflict global

Displays the component mode.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show address-conflict global

2.2.2 show address-conflict detected

Displays the last detected address conflict.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show address-conflict detected

2.2.3 show address-conflict fault-state

Displays the current conflict status.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show address-conflict fault-state

2.2.4 show mac-address-conflict global

Displays the component mode.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-address-conflict global

3 Application Lists

3.1 appllists

Configure an application list.

3.1.1 appllists set-authlist

Set an authentication list reference that shall be used by given application.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `appllists set-authlist <P-1> <P-2>`

Parameter	Value	Meaning
P-1	string	<application> Name of an application list.
P-2	string	<authlist_name> Name of referenced authentication list.

3.1.2 appllists enable

Activate a login application list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `appllists enable <P-1>`

Parameter	Value	Meaning
P-1	string	<application> Name of an application list.

3.1.3 appllists disable

Deactivate a login application list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `appllists disable <P-1>`

Parameter	Value	Meaning
P-1	string	<application> Name of an application list.

3.2 show

Display device options and settings.

3.2.1 show appllists

Display ordered methods for application lists.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show appllists

4 Authentication Lists

4.1 authlists

Configure an authentication list.

4.1.1 authlists add

Create a new login authentication list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: authlists add <P-1>

Paramete Value	Meaning
P-1 string	<authlist_name> Name of an authentication list.

4.1.2 authlists delete

Delete an existing login authentication list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: authlists delete <P-1>

Paramete Value	Meaning
P-1 string	<authlist_name> Name of an authentication list.

4.1.3 authlists set-policy

Set the policies of a login authentication list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: authlists set-policy <P-1> <P-2> [<P-3> [<P-4> [<P-5> [<P-6>]]]]

Paramete Value	Meaning
P-1 string	<authlist_name> Name of an authentication list.

Parameter	Value	Meaning
P-2	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server
P-3	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server
P-4	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server
P-5	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server
P-6	reject	Authentication is rejected / not allowed
	local	Authentication by local user DB
	radius	Authentication by RADIUS server
	ias	Authentication by IAS server
	cam	Authentication by CAM server
	ldap	Authentication by remote server

4.1.4 authlists enable

Activate a login authentication list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: authlists enable <P-1>

Parameter	Value	Meaning
P-1	string	<authlist name> Name of an authentication list.

4.1.5 authlists disable

Deactivate a login authentication list.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: authlists disable <P-1>

Parameter	Value	Meaning
P-1	string	<authlist name> Name of an authentication list.

4.2 show

Display device options and settings.

4.2.1 show authlists

Display ordered methods for authentication lists.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show authlists

5 Auto Disable

5.1 auto-disable

Configure the Auto Disable condition settings.

5.1.1 auto-disable reason

Enables/disables port Recovery by reason on this device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-disable reason <P-1>

Parameter	Value	Meaning
P-1	link-flap	Enable/disable link-flap.
	crc-error	Enable/disable crc-error.
	duplex-mismatch	Enable/disable duplex-mismatch.
	dhcp-snooping	Enable/disable dhcp-snooping.
	arp-rate	Enable/disable arp-rate.
	bpdu-rate	Enable/disable bpdu-rate.
	port-security	Enable/disable MAC based port security.
	overload-detection	Enable/disable overload-detection.
	speed-duplex	Enable/disable link speed and duplex monitor.

■ no auto-disable reason

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no auto-disable reason <P-1>

5.2 auto-disable

Configure the Auto Disable condition settings.

5.2.1 auto-disable timer

Timer value in seconds after a deactivated port is activated again. Possible values are: 30-4294967295. A value of 0 disables the timer.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-disable timer <P-1>

Parameter	Value	Meaning
P-1	xxx_30..4294967295	Timer value in seconds.

5.2.2 auto-disable reset

Reset the specific interface and reactivate the port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-disable reset [<P-1>]

Parameter	Value	Meaning
P-1	port	Press Enter to execute the command.

■ no auto-disable reset

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no auto-disable reset [<P-1>]

5.3 show

Display device options and settings.

5.3.1 show auto-disable brief

Display Auto Disable summary by interface.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show auto-disable brief

5.3.2 show auto-disable reasons

Display summary of Auto Disable error reasons.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show auto-disable reasons

6 Class Of Service

6.1 classofservice

Class of service configuration.

6.1.1 classofservice ip-dscp-mapping

ip-dscp-mapping configuration

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: classofservice ip-dscp-mapping <P-1> <P-2> <P-3>

Parameter	Value	Meaning
P-1	af11	
	af12	
	af13	
	af21	
	af22	
	af23	
	af31	
	af32	
	af33	
	af41	
	af42	
	af43	
	be	
	cs0	
	cs1	
	cs2	
	cs3	
	cs4	
	cs5	
	cs6	
	cs7	
	ef	
	0	
	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
12		
13		
14		
15		
16		
17		
18		
19		
20		
21		
22		
23		
24		
25		
26		
27		
28		
29		
30		
31		
32		
33		
34		

Parameter	Value	Meaning
P-2	0..7	Enter the Traffic Class value.
P-3	0..3	Enter the Traffic Class value.

6.1.2 classofservice dot1p-mapping

Enter a VLAN priority and the traffic class it should be mapped to.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: classofservice dot1p-mapping <P-1> <P-2> <P-3>

Parameter	Value	Meaning
P-1	0..7	Enter the 802.1p priority.
P-2	0..7	Enter the Traffic Class value.
P-3	0..3	Enter a number in the given range.

6.2 classofservice

Interface classofservice configuration.

6.2.1 classofservice trust

trust configuration

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: classofservice trust <P-1>

Parameter	Value	Meaning
P-1	untrusted	Sets the class of service trust mode to untrusted
	dot1p	Sets the class of service trust mode to dot1p.
	ip-dscp	Sets the class of service trust mode to IP DSCP.

6.3 cos-queue

COS queue configuration

6.3.1 cos-queue strict

strict priority scheduler (default)

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cos-queue strict <P-1> <P-2>`

Parameter	Value	Meaning
P-1	0..7	Enter a Queue Id from 0 to 7.
P-2	0..3	Enter a number in the given range.

6.3.2 cos-queue weighted

weighted scheduler

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cos-queue weighted <P-1> <P-2>`

Parameter	Value	Meaning
P-1	0..7	Enter a Queue Id from 0 to 7.
P-2	0..3	Enter a number in the given range.

6.3.3 cos-queue min-bandwidth

Minimum/guaranteed bandwidth for the queues when in weighted mode

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cos-queue min-bandwidth <P-1> <P-2> <P-3>`

Class Of Service
6.3 cos-queue

Parameter	Value	Meaning
P-1	0..3	Enter a number in the given range.
P-2	0..7	Enter a Queue Id from 0 to 7.
P-3	0..100	Enter a number in the given range.

6.4 show

Display device options and settings.

6.4.1 show classofservice ip-dscp-mapping

Show ip-dscp-mapping configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show classofservice ip-dscp-mapping

6.4.2 show classofservice dot1p-mapping

Display a table containing the vlan priority to traffic class mappings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show classofservice dot1p-mapping

6.4.3 show classofservice trust

Show a table containing the trust mode of all interfaces.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show classofservice trust

6.4.4 show cos-queue

Show cosqueue parameters

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show cos-queue

7 Command Line Interface (CLI)

7.1 cli

Set the CLI preferences.

7.1.1 cli serial-timeout

Set login timeout for serial line connection to CLI. Setting to 0 will disable the timeout. The value is active after next login.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: cli serial-timeout <P-1>

Parameter	Value	Meaning
P-1	0..160	Enter a number in the given range. Setting to 0 will disable the timeout.

7.1.2 cli prompt

Change the system prompt. Following wildcards are allowed: %d date, %t time, %i IP address, %m MAC address, %p product name

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: cli prompt <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters. Following wildcards are allowed: %d date, %t time, %i IP address, %m MAC address, %p product name

7.1.3 cli numlines

Screen size for 'more' (23 = default). Enter a 0 will disable the feature. The value is only valid for the current session.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: cli numlines <P-1>

Parameter	Value	Meaning
P-1	0..250	Screen size for 'more' (23 = default). Enter a 0 will disable the feature. The value is only valid for the current session.

7.1.4 cli banner operation

Enable or disable the CLI login banner.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: cli banner operation

■ no cli banner operation

Disable the option

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no cli banner operation

7.1.5 cli banner text

Set the text for the CLI login banner (C printf format syntax allowed: \n \t).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: cli banner text <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).

7.2 show

Display device options and settings.

7.2.1 show cli global

Display CLI preferences.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show cli global

7.2.2 show cli command-tree

Show a list of all commands.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show cli command-tree

7.3 logging

Logging configuration.

7.3.1 logging cli-command

Enable or disable the CLI command logging.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** logging cli-command

■ **no logging cli-command**

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no logging cli-command

7.4 show

Display device options and settings.

7.4.1 show logging cli-command

Show the CLI command logging preferences.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging cli-command

8 Clock

8.1 clock

Configure local and DST clock settings.

8.1.1 clock set

Edit current local time.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock set <P-1> <P-2>

Parameter	Value	Meaning
P-1	YYYY-MM-DD	Local date (range: 2004-01-01 - 2037-12-31).
P-2	HH:MM:SS	Local time.

8.1.2 clock timezone offset

Local time offset (in minutes) with respect to UTC (positive values for locations east of Greenwich).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock timezone offset <P-1>

Parameter	Value	Meaning
P-1	-780..840	Edit the timezone offset (in minutes).

8.1.3 clock timezone zone

Edit the timezone acronym (max. 4 characters).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock timezone zone <P-1>

Parameter	Value	Meaning
P-1	string	Edit the timezone acronym (max 4 characters).

8.1.4 clock summer-time mode

Configure summer-time mode parameters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock summer-time mode <P-1>

Parameter	Value	Meaning
P-1	disable	Disable recurring summer-time mode.
	recurring	Enable recurring summer-time mode.
	eu	Enable recurring summer-time used in most parts of the European Union.
	usa	Enable recurring summer-time used in most parts of the USA.

8.1.5 clock summer-time recurring start

Edit the starting date and time for daylight saving time.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock summer-time recurring start <P-1> <P-2> <P-3> <P-4>

Parameter	Value	Meaning
P-1	none	
	first	
	second	
	third	
	fourth	
	last	
P-2	none	
	sun	Sunday
	mon	Monday
	tue	Tuesday
	wed	Wednesday
	thu	Thursday
	fri	Friday
sat	Saturday	
P-3	none	
	jan	January
	feb	February
	mar	March
	apr	April
	may	May
	jun	June
	jul	July
	aug	August
	sep	September
	oct	October
	nov	November
dec	December	
P-4	string	<hh:mm> Present time in hh:mm format (00:00-23:59).

8.1.6 clock summer-time recurring end

Edit the ending date and time for daylight saving time.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock summer-time recurring end <P-1> <P-2> <P-3> <P-4>

Parameter	Value	Meaning
P-1	none	
	first	
	second	
	third	
	fourth	
	last	
	P-2	none
sun		Sunday
mon		Monday
tue		Tuesday
wed		Wednesday
thu		Thursday
fri		Friday
sat	Saturday	
P-3	none	
	jan	January
	feb	February
	mar	March
	apr	April
	may	May
	jun	June
	jul	July
	aug	August
	sep	September
	oct	October
	nov	November
dec	December	
P-4	string	<hh:mm> Present time in hh:mm format (00:00-23:59).

8.1.7 clock summer-time zone

Edit timezone acronym for summer-time (max. 4 characters).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clock summer-time zone <P-1>

Parameter	Value	Meaning
P-1	string	Edit the timezone acronym (max 4 characters).

8.2 show

Display device options and settings.

8.2.1 show clock

Display the current time information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show clock [summer-time]
[summer-time]: Display summer-time parameters.

9 Configuration

9.1 save

Save the configuration to the specified destination.

9.1.1 save profile

Save the configuration to the specific profile.

- ▶ Mode: All Privileged Modes
- ▶ Privilege Level: Operator
- ▶ Format: save profile <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

9.2 config

Configure the configuration saving settings.

9.2.1 config watchdog admin-state

Enable or disable the configuration undo feature.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: config watchdog admin-state

■ no config watchdog admin-state

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no config watchdog admin-state

9.2.2 config watchdog timeout

Configure the configuration undo timeout (unit: seconds).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: config watchdog timeout <P-1>

Parameter	Value	Meaning
P-1	30..600	Enter a number in the given range.

9.2.3 config encryption password set

Set the configuration file password.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: config encryption password set [<P-1>] [<P-2>]

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.
P-2	string	Enter a user-defined text, max. 64 characters.

9.2.4 config encryption password clear

Clear the configuration file password.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: config encryption password clear [<P-1>]

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.

9.2.5 config envm auto-update

Allow automatic firmware updates with this memory device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: config envm auto-update <P-1>

Parameter	Value	Meaning
P-1	sd	SD-Card
	usb	USB Storage Device

■ no config envm auto-update

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no config envm auto-update <P-1>

9.2.6 config envm sshkey-auto-update

Allow automatic ssh key updates with this memory device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: config envm sshkey-auto-update <P-1>

Parameter	Value	Meaning
P-1	sd	SD-Card
	usb	USB Storage Device

■ no config envm sshkey-auto-update

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no config envm sshkey-auto-update <P-1>

9.2.7 config envm config-save

Allow the configuration to be saved to this memory device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: config envm config-save <P-1>

Parameter	Value	Meaning
P-1	sd	SD-Card
	usb	USB Storage Device

■ no config envm config-save

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no config envm config-save <P-1>

9.2.8 config envm load-priority

Configure the order of configuration load attempts from memory devices at boot time. If one load is successful, then the device discards further attempts.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `config envm load-priority <P-1> <P-2>`

Parameter	Value	Meaning
P-1	sd	SD-Card
	usb	USB Storage Device
P-2	disable	Config will not be loaded at all
	first	Config will be loaded first. If successful, no other config will be tried.
	second	Config will be loaded if first one does not succeed.

9.2.9 config profile select

Select a configuration profile to be the active configuration.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `config profile select <P-1> <P-2>`

Parameter	Value	Meaning
P-1	nvm	You can only select nvm for this command.
P-2	1..20	Index of the profile entry.

9.2.10 config profile delete

Delete a specific configuration profile.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `config profile delete <P-1> num <P-2> profile <P-3>`

num: Select the index of a profile to delete.

profile: Select the name of a profile to delete.

Parameter	Value	Meaning
P-1	nvm	non-volatile memory
	envm	external non-volatile memory device
P-2	1..20	Index of the profile entry.
P-3	string	Enter a user-defined text, max. 32 characters.

9.2.11 config fingerprint verify

Verify the fingerprint of the selected profile.

▶ **Mode:** Global Config Mode

▶ **Privilege Level:** Administrator

▶ **Format:** config fingerprint verify <P-1> profile <P-2> <P-3> num <P-4> <P-5>

profile: Select the name of a profile to be verified.

num: Select the index number of a profile to be verified.

Parameter	Value	Meaning
P-1	nvm	non-volatile memory
	envm	external non-volatile memory device
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	string	Enter hash as 40 hexa-decimal characters.
P-4	1..20	Index of the profile entry.
P-5	string	Enter hash as 40 hexa-decimal characters.

9.3 copy

Copy different kinds of items.

9.3.1 copy sysinfo system envm

Copy the system information to external non-volatile memory.

▶ Mode: Privileged Exec Mode

▶ Privilege Level: Operator

▶ Format: copy sysinfo system envm [filename <P-1>]

[filename]: Enter the filename (format xyz.html) to be saved in external non-volatile memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

9.3.2 copy sysinfoall system envm

Copy the system information and the event log from the device to external non-volatile memory.

▶ Mode: Privileged Exec Mode

▶ Privilege Level: Operator

▶ Format: copy sysinfoall system envm

9.3.3 copy firmware remote

Copy a firmware image to the device from a server.

▶ Mode: Privileged Exec Mode

▶ Privilege Level: Administrator

▶ Format: copy firmware remote <P-1> system

system: Copy a firmware image to the device from a file server.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

9.3.4 copy config running-config nvm

Copy the running-config to non-volatile memory.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: copy config running-config nvm [profile <P-1>]
[profile]: Save the configuration as a specific profile name.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

9.3.5 copy config running-config remote

Copy the running-config to a file server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy config running-config remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

9.3.6 copy config nvm

Load a configuration from non-volatile memory to the running-config.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy config nvm [profile <P-1>] running-config remote <P-2>
[profile]: Load a configuration from a specific profile name.

running-config: (Re)-load a configuration from non-volatile memory to the running-config.
remote: Copy a configuration from non-volatile memory to a server.

Parameter	Value	Meaning
P-1	string	Filename.
P-2	string	Enter a user-defined text, max. 128 characters.

9.3.7 copy config remote

Copy a configuration file to the device from a server.

▶ Mode: Privileged Exec Mode

▶ Privilege Level: Administrator

▶ Format: copy config remote <P-1> nvm [profile <P-2>] running-config

nvm: Copy a configuration file from a server to non-volatile memory.

[profile]: Copy a configuration from a server to a specific profile in non-volatile memory.

running-config: Copy a configuration file from a server to the running-config.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 32 characters.

9.3.8 copy sfp-white-list remote

Copy the SFP WhiteList from server to the device.

▶ Mode: Privileged Exec Mode

▶ Privilege Level: Operator

▶ Format: copy sfp-white-list remote <P-1> nvm

nvm: Copy the SFP WhiteList from server to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

9.3.9 copy sfp-white-list envm

Copy the SFP WhiteList from external non-volatile memory.

▶ Mode: Privileged Exec Mode

▶ Privilege Level: Operator

▶ Format: copy sfp-white-list envm <P-1> nvm

nvm: Copy the SFP WhiteList from external non-volatile memory to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

9.4 clear

Clear several items.

9.4.1 clear config

Clear the running configuration.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear config

9.4.2 clear factory

Set the device back to the factory settings (use with care).

- ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: clear factory [erase-all]
- [erase-all]: Set to factory settings and also erase file systems (use with extreme care).

9.5 show

Display device options and settings.

9.5.1 show running-config xml

Show the currently running configuration (XML file).

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Administrator
- ▶ Format: show running-config xml

9.5.2 show running-config script

Show the currently running configuration (CLI script).

- ▶ Mode: Command is in all modes available.
 - ▶ Privilege Level: Administrator
 - ▶ Format: show running-config script [all]
- [all]: Show the currently running configuration (CLI script).

9.6 show

Display device options and settings.

9.6.1 show config envm settings

Show the settings of the external non-volatile memory.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show config envm settings

9.6.2 show config envm properties

Show the properties of the external non-volatile memory.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show config envm properties

9.6.3 show config watchdog

Show the Auto Configuration Undo settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show config watchdog

9.6.4 show config encryption

Show the settings for config encryption.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show config encryption

9.6.5 show config profiles

Show the configuration profiles.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Administrator
- ▶ Format: show config profiles <P-1> [<P-2>]

Parameter	Value	Meaning
P-1	nvm	non-volatile memory
	envm	external non-volatile memory device
P-2	1..20	Index of the profile entry.

9.6.6 show config status

Show the sync status of the running-config with non-volatile memory and ACA.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show config status

10 Debugging

10.1 debug

Different tools to assist in debugging the device.

10.1.1 debug tcpdump help

Display help file for the tcpdump tool.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump help

10.1.2 debug tcpdump start cpu

Start capture with default values.

- ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: debug tcpdump start cpu [filter <P-1>] [parms <P-2>]
- [filter]: Start capture with values from a filter file.
[parms]: Start capture with the tcpdump parameters (for details see tcpdump help).

Paramete Value	Meaning
P-1	string <filename> Enter a valid filename.
P-2	string Enter a user-defined text, max. 255 characters.

10.1.3 debug tcpdump stop

Abort capture of network traffic.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump stop

10.1.4 debug tcpdump filter show

Display a known filter file.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump filter show <P-1>

Parameter	Value	Meaning
P-1	string	<filename> Enter a valid filename.

10.1.5 debug tcpdump filter list

Display all available filter files.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump filter list

10.1.6 debug tcpdump filter delete

Delete a known filter file.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: debug tcpdump filter delete <P-1>

Parameter	Value	Meaning
P-1	string	<filename> Enter a valid filename.

10.2 show

Display device options and settings.

10.2.1 show debug logic-modules

List logic module information

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: show debug logic-modules

10.3 copy

Copy different kinds of items.

10.3.1 copy tcpdumpcap nvm remote

Copy the capture file from the device to a server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `copy tcpdumpcap nvm remote <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

10.3.2 copy tcpdumpfilter remote

Copy the filter file from a server to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `copy tcpdumpfilter remote <P-1> nvm <P-2>`

nvm: Copy the filter file from a server to non-volatile memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	<filename> Enter a valid filename.

10.3.3 copy tcpdumpfilter nvm

Copy the capture filter from non-volatile memory to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `copy tcpdumpfilter nvm <P-1> envm [<P-2>] remote <P-3>`

envm: Copy the capture filter from non-volatile memory to external non-volatile memory.

remote: Copy the capture file from non-volatile memory to a server.

Parameter	Value	Meaning
P-1	string	Filename.
P-2	string	<filename> Enter a valid filename.
P-3	string	Enter a user-defined text, max. 128 characters.

11 Device Monitoring

11.1 device-status

Configure various device conditions to be monitored.

11.1.1 device-status monitor link-failure

Enable or disable monitor state of network connection(s).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: device-status monitor link-failure

■ no device-status monitor link-failure

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no device-status monitor link-failure

11.1.2 device-status monitor ring-redundancy

Enable or disable monitoring if ring-redundancy is present.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: device-status monitor ring-redundancy

■ no device-status monitor ring-redundancy

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no device-status monitor ring-redundancy

11.1.3 device-status trap

Configure the device to send a trap when the device status changes.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: device-status trap

■ no device-status trap

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no device-status trap

11.2 device-status

Configure various device conditions to be monitored.

11.2.1 device-status link-alarm

Configure the monitor settings of the port link.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** device-status link-alarm

■ **no device-status link-alarm**

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no device-status link-alarm

11.3 show

Display device options and settings.

11.3.1 show device-status monitor

Display the device monitoring configurations.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show device-status monitor

11.3.2 show device-status state

Display the current state of the device.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show device-status state

11.3.3 show device-status trap

Display the device trap information and configurations.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show device-status trap

11.3.4 show device-status events

Display occurred device status events.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status events

11.3.5 show device-status link-alarm

Display the monitor configurations of the network ports.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status link-alarm

11.3.6 show device-status all

Display the configurable device status settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show device-status all

12 Device Security

12.1 security-status

Configure the security status settings.

12.1.1 security-status monitor pwd-change

Sets the monitoring of default password change for 'user' and 'admin'.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor pwd-change

■ no security-status monitor pwd-change

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor pwd-change

12.1.2 security-status monitor pwd-min-length

Sets the monitoring of minimum length of the password (smaller 8).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor pwd-min-length

■ no security-status monitor pwd-min-length

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor pwd-min-length

12.1.3 security-status monitor pwd-policy-config

Sets the monitoring whether the minimum password policy is configured. The device changes the security status to the value "error" if the value for at least one of the following password rules is 0:\n"minimum upper cases", "minimum lower cases", "minimum numbers", "minimum special characters".

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor pwd-policy-config

■ no security-status monitor pwd-policy-config

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor pwd-policy-config

12.1.4 security-status monitor pwd-str-not-config

Sets the monitoring whether the password minimum\nstrength check is configured.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor pwd-str-not-config

■ no security-status monitor pwd-str-not-config

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor pwd-str-not-config

12.1.5 security-status monitor pwd-policy-inactive

Sets the monitoring whether at least one user is\nconfigured with inactive policy check.\nThe device changes the security status to the value "error" if the function "policy check" is inactive for at least 1 user account.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor pwd-policy-inactive

■ **no security-status monitor pwd-policy-inactive**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor pwd-policy-inactive

12.1.6 security-status monitor bypass-pwd-strength

Sets the monitoring whether at least one user is configured to bypass strength check.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor bypass-pwd-strength

■ **no security-status monitor bypass-pwd-strength**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor bypass-pwd-strength

12.1.7 security-status monitor telnet-enabled

Sets the monitoring of the activation of telnet on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor telnet-enabled

■ **no security-status monitor telnet-enabled**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor telnet-enabled

12.1.8 security-status monitor http-enabled

Sets the monitoring of the activation of http on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor http-enabled

■ no security-status monitor http-enabled

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor http-enabled

12.1.9 security-status monitor snmp-unsecure

Sets the monitoring of SNMP security\n(SNMP v1/v2 is enabled or v3 encryption is disabled).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor snmp-unsecure

■ no security-status monitor snmp-unsecure

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor snmp-unsecure

12.1.10 security-status monitor sysmon-enabled

Sets the monitoring of the activation of System Monitor 1 on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor sysmon-enabled

■ **no security-status monitor sysmon-enabled**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor sysmon-enabled

12.1.11 security-status monitor no-link-enabled

Sets the monitoring of no link detection.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor no-link-enabled

■ **no security-status monitor no-link-enabled**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor no-link-enabled

12.1.12 security-status monitor hidisc-write-enabled

Sets the monitoring of HiDiscovery write enabled.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor hidisc-write-enabled

■ **no security-status monitor hidisc-write-enabled**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor hidisc-write-enabled

12.1.13 security-status monitor iec61850-mms-enabled

Sets the monitoring of the activation of IEC 61850 MMS on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor iec61850-mms-enabled

■ no security-status monitor iec61850-mms-enabled

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor iec61850-mms-enabled

12.1.14 security-status monitor https-certificate

Sets the monitoring whether auto generated self-signed HTTPS certificate is in use.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor https-certificate

■ no security-status monitor https-certificate

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor https-certificate

12.1.15 security-status monitor modbus-tcp-enabled

Sets the monitoring of the activation of Modbus/TCP server on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor modbus-tcp-enabled

■ **no security-status monitor modbus-tcp-enabled**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor modbus-tcp-enabled

12.1.16 security-status monitor ethernet-ip-enabled

Sets the monitoring of the activation of EtherNet/IP protocol on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor ethernet-ip-enabled

■ **no security-status monitor ethernet-ip-enabled**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor ethernet-ip-enabled

12.1.17 security-status monitor profinet-io-enabled

Sets the monitoring of the activation of PROFINET protocol on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status monitor profinet-io-enabled

■ **no security-status monitor profinet-io-enabled**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status monitor profinet-io-enabled

12.1.18 security-status trap

Configure if a trap is sent when the security status changes.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status trap

■ no security-status trap

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status trap

12.2 security-status

Configure the security status interface settings.

12.2.1 security-status no-link

Configure the monitoring of the specific ports.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: security-status no-link

■ no security-status no-link

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no security-status no-link

12.3 show

Display device options and settings.

12.3.1 show security-status monitor

Display the security status monitoring settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show security-status monitor

12.3.2 show security-status state

Display the current security status.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show security-status state

12.3.3 show security-status no-link

Display the settings of the monitoring of the specific network ports.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show security-status no-link

12.3.4 show security-status trap

Display the security status trap information and settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show security-status trap

12.3.5 show security-status events

Display occurred security status events.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show security-status events

12.3.6 show security-status all

Display all security status settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show security-status all

13 DHCP Layer 2 Relay

13.1 clear

Clear several items.

13.1.1 clear dhcp-l2relay statistics

This command clears the DHCP Layer 2 Relay statistics.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear dhcp-l2relay statistics`

13.2 show

Display device options and settings.

13.2.1 show dhcp-l2relay global

This command displays the global DHCP Layer 2 Relay configuration.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show dhcp-l2relay global

13.2.2 show dhcp-l2relay statistics

This command displays interface statistics specific to DHCP Layer 2 Relay.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show dhcp-l2relay statistics

13.2.3 show dhcp-l2relay interfaces

This command displays the DHCP Layer 2 Relay status of all interfaces.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show dhcp-l2relay interfaces

13.2.4 show dhcp-l2relay vlan

This command displays the VLAN based DHCP Layer 2 Relay status.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show dhcp-l2relay vlan

14 DHCP Snooping

14.1 clear

Clear several items.

14.1.1 clear ip dhcp-snooping bindings

This command clears all dynamic DHCP Snooping (and IP Source Guard) bindings on all interfaces or on a specific interface.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear ip dhcp-snooping bindings [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

14.1.2 clear ip dhcp-snooping statistics

This command clears the DHCP Snooping statistics.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear ip dhcp-snooping statistics

14.2 show

Display device options and settings.

14.2.1 show ip dhcp-snooping global

This command displays the global DHCP Snooping configuration.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show ip dhcp-snooping global

14.2.2 show ip dhcp-snooping statistics

This command displays statistics for DHCP Snooping security violations on untrusted ports.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show ip dhcp-snooping statistics

14.2.3 show ip dhcp-snooping interfaces

This command shows the DHCP Snooping status of all interfaces.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show ip dhcp-snooping interfaces

14.2.4 show ip dhcp-snooping vlan

This command displays the VLAN based DHCP Snooping status.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show ip dhcp-snooping vlan

14.2.5 show ip dhcp-snooping bindings

This command displays the DHCP Snooping binding entries from the static and/or dynamic bindings table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show ip dhcp-snooping bindings [<P-1>] [interface <P-2>] [vlan <P-3>]
[interface]: Restrict the output based on a specific interface.
[vlan]: Restrict the output based on VLAN.

Parameter	Value	Meaning
P-1	static	Restrict the output based on static bindings.
	dynamic	Restrict the output based on dynamic bindings.
P-2	slot no./port no.	
P-3	1..4042	Enter the VLAN ID.

15 DoS Mitigation

15.1 dos

Manage DoS Mitigation

15.1.1 dos tcp-null

Enables TCP Null scan protection - all TCP flags and TCP sequence number zero.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-null

■ no dos tcp-null

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-null

15.1.2 dos tcp-xmas

Enables TCP XMAS scan protection - TCP FIN, URG, PSH equal 1 and SEQ equals 0.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-xmas

■ no dos tcp-xmas

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-xmas

15.1.3 dos tcp-syn-fin

Enables TCP SYN/FIN scan protection - TCP with SYN and FIN flags set.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-syn-fin

■ no dos tcp-syn-fin

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-syn-fin

15.1.4 dos tcp-min-header

Enables TCP minimal header size check.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-min-header

■ no dos tcp-min-header

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-min-header

15.1.5 dos icmp-fragmented

Enables fragmented ICMP protection.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos icmp-fragmented

■ **no dos icmp-fragmented**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos icmp-fragmented

15.1.6 dos icmp payload-check

Enables ICMP max payload size protection for IPv4 and IPv6.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos icmp payload-check

■ **no dos icmp payload-check**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos icmp payload-check

15.1.7 dos icmp payload-size

Configures maximum ICMP payload size (default: 512).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos icmp payload-size <P-1>

Parameter	Value	Meaning
P-1	0..1472	Max. ICMP payload size (default: 512)

15.1.8 dos ip-land

Enables LAND attack protection - source IP equals destination IP.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos ip-land <P-1>

Parameter	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

15.1.9 dos tcp-offset

Enables TCP offset check - ingress TCP packets with fragment offset 1 are dropped.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-offset

■ no dos tcp-offset

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-offset

15.1.10 dos tcp-syn

Enables TCP source port smaller than 1024 protection.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dos tcp-syn

■ no dos tcp-syn

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dos tcp-syn

15.1.11 dos l4-port

Enables UDP or TCP source port equals destination port check.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** dos l4-port

■ **no dos l4-port**

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no dos l4-port

15.2 show

Display device options and settings.

15.2.1 show dos

Show DoS Mitigation parameters

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show dos

16 IEEE 802.1x (Dot1x)

16.1 dot1x

Configure 802.1X parameters.

16.1.1 dot1x dynamic-vlan

Creates VLANs dynamically when a RADIUS-assigned VLAN does not exist.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x dynamic-vlan

■ no dot1x dynamic-vlan

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dot1x dynamic-vlan

16.1.2 dot1x system-auth-control

Enable or disable 802.1X authentication support on the switch.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x system-auth-control

■ no dot1x system-auth-control

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dot1x system-auth-control

16.1.3 dot1x monitor

Enable or disable 802.1X monitor mode.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** dot1x monitor

■ **no dot1x monitor**

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no dot1x monitor

16.2 dot1x

Configure 802.1X interface parameters.

16.2.1 dot1x guest-vlan

Configure a VLAN as 802.1X guest VLAN.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x guest-vlan <P-1>

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.

16.2.2 dot1x max-req

Configure the maximum number of requests to be sent.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x max-req <P-1>

Parameter	Value	Meaning
P-1	1..10	Maximum number of requests (default: 2).

16.2.3 dot1x port-control

Set the authentication mode on the specified port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x port-control <P-1>

Parameter	Value	Meaning
P-1	<code>auto</code>	Port is actually controlled by protocol.
	<code>force-authorized</code>	Port is authorized unconditionally (default).
	<code>force-unauthorized</code>	Port is unauthorized unconditionally.
	<code>multi-client</code>	If more than one client is attached to the port, then each client needs to authenticate separately.

16.2.4 dot1x re-authentication

Enable or disable re-authentication for the given interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `dot1x re-authentication`

■ no dot1x re-authentication

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `no dot1x re-authentication`

16.2.5 dot1x unauthenticated-vlan

Configure a VLAN as 802.1X unauthenticated VLAN.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `dot1x unauthenticated-vlan <P-1>`

Parameter	Value	Meaning
P-1	<code>0..4042</code>	Enter the VLAN ID. Entering of ID 0 disables the feature.

16.2.6 dot1x timeout guest-vlan-period

Configure the guest-vlan period value.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout guest-vlan-period <P-1>

Parameter	Value	Meaning
P-1	1..300	Guest-vlan timeout in seconds (default: 90).

16.2.7 dot1x timeout reauth-period

Configure the re-authentication period.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout reauth-period <P-1>

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

16.2.8 dot1x timeout quiet-period

Configure the quiet period value.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout quiet-period <P-1>

Parameter	Value	Meaning
P-1	0..65535	Quiet period in seconds (default: 60).

16.2.9 dot1x timeout tx-period

Configure the transmit timeout period.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout tx-period <P-1>

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

16.2.10 dot1x timeout supp-timeout

Configure the supplicant timeout period.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout supp-timeout <P-1>

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

16.2.11 dot1x timeout server-timeout

Configure the server timeout period.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x timeout server-timeout <P-1>

Parameter	Value	Meaning
P-1	1..65535	Timeout in seconds.

16.2.12 dot1x initialize

Begins the initialization sequence on the specified port (port-control mode must be 'auto').

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x initialize

■ **no dot1x initialize**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dot1x initialize

16.2.13 dot1x re-authenticate

Begins the re-authentication sequence on the specified port (port-control mode must be 'auto').

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: dot1x re-authenticate

■ **no dot1x re-authenticate**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no dot1x re-authenticate

16.3 show

Display device options and settings.

16.3.1 show dot1x global

Display global 802.1X configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x global

16.3.2 show dot1x auth-history

Display 802.1X authentication events and information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x auth-history [<P-1> [<P-2>]]

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	1..4294967294	802.1X history log entry index. This can be specified only if interface is provided. Parameter Usage: [<slot/port> [index]]

16.3.3 show dot1x detail

Display the detailed 802.1X configuration for the specified port.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show dot1x detail <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

16.3.4 show dot1x summary

Display summary information of the 802.1X configuration for a specified port or all ports.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show dot1x summary [<P-1>]

Paramete	Value	Meaning
P-1	slot no./port no.	

16.3.5 show dot1x clients

Display 802.1X client information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show dot1x clients [<P-1>]

Paramete	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

16.3.6 show dot1x statistics

Display the 802.1X statistics for the specified port.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show dot1x statistics <P-1>

Paramete	Value	Meaning
P-1	slot no./port no.	

16.4 clear

Clear several items.

16.4.1 clear dot1x statistics port

Resets the 802.1X statistics for specified port.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear dot1x statistics port <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

16.4.2 clear dot1x statistics all

Resets the 802.1X statistics for all ports.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear dot1x statistics all`

16.4.3 clear dot1x auth-history port

Clears the 802.1X authentication history for specified port.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear dot1x auth-history port <P-1>`

Parameter	Value	Meaning
P-1	slot no./port no.	

16.4.4 clear dot1x auth-history all

Clears the 802.1X authentication history for all ports.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear dot1x auth-history all

17 IEEE 802.3ad (Dot3ad)

17.1 link-aggregation

Configure 802.3ad link aggregation parameters to increase bandwidth and provide redundancy by combining connections.

17.1.1 link-aggregation add

Create a new Link Aggregation Group to increase bandwidth and provide link redundancy. If desired, enter a name up to 15 alphanumeric characters in length.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: link-aggregation add <P-1>

Paramete Value	Meaning
P-1	lag/<lagport> Enter a lag interface in lag/lagport format.

17.1.2 link-aggregation modify

Modify the parameters for the specified Link Aggregation Group.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: link-aggregation modify <P-1> name <P-2> addport <P-3> deleteport <P-4> adminmode linktrap static hashmode <P-5> min-links <P-6>

name: Modify the name of the specified Link Aggregation Group.

addport: Add the specified port to the Link Aggregation Group.

deleteport: Delete the specified port from the Link Aggregation Group.

adminmode: Modify the administration mode of the specified Link Aggregation Group. To activate the group, enable the administration mode.

linktrap: Enable/Disable link trap notifications for the specified Link Aggregation Group

static: Enable or disable static capability for the specified Link Aggregation Group on a device. When enabled, LACP automatically helps prevent loops and allows non-link aggregation partners to support LACP.

hashmode: Set the hash mode to be used by the load balancing algorithm for specified Link Aggregation Group.

min-links: Set the minimum links for the specified Link Aggregation Group.

Paramete Value	Meaning
P-1	slot no./port no.
P-2	string Enter a user-defined text, max. 15 characters.
P-3	slot no./port no.

Parameter	Value	Meaning
P-4	slot no./port no.	
P-5	src-mac	Source MAC, VLAN, EtherType, and incoming port associated with the packet.
	dst-mac	Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
	src-dst-mac	Source/Destination MAC, VLAN, EtherType, and incoming port associated with the packet.
	src-ip	Source IP and Source TCP/UDP fields of the packet.
	dst-ip	Destination IP and Destination TCP/UDP Port fields of the packet.
	src-dst-ip	Source/Destination IP and source/destination TCP/UDP Port fields of the packet.
P-6	slot no./port no.	

■ no link-aggregation modify

Disable the option

▶ **Mode:** Global Config Mode

▶ **Privilege Level:** Operator

▶ **Format:** no link-aggregation modify <P-1> name addport deleteport adminmode linktrap static hashmode min-links

17.1.3 link-aggregation delete

Delete the Link Aggregation Group to divide the group into individual connections.

▶ **Mode:** Global Config Mode

▶ **Privilege Level:** Operator

▶ **Format:** link-aggregation delete <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

17.2 lacp

Configure lacp parameters.

17.2.1 lacp admin-key

Configure the administrative value of the key on this LAG.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp admin-key <P-1>

Paramete Value	Meaning
P-1 0..65535	Enter a number between 0 and 65535

17.2.2 lacp collector-max-delay

Configure the collector max delay on this LAG (default is 0).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp collector-max-delay <P-1>

Paramete Value	Meaning
P-1 0..65535	Enter a number between 0 and 65535

17.2.3 lacp lacpmode

Activate/deactivate LACP on an interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp lacpmode

■ no lacp lacpmode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp lacpmode

17.2.4 lacp actor admin key

Configure the value of the LACP actor admin key on this port(default 0).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp actor admin key <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

17.2.5 lacp actor admin state lacp-activity

Enable/disable the LACP activity on the actor admin state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp actor admin state lacp-activity

■ no lacp actor admin state lacp-activity

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp actor admin state lacp-activity

17.2.6 lacp actor admin state lacp-timeout

Enable/disable the LACP timeout on the actor admin state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp actor admin state lacp-timeout

■ no lacp actor admin state lacp-timeout

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp actor admin state lacp-timeout

17.2.7 lacp actor admin state aggregation

Enable/disable the aggregation on the actor admin state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp actor admin state aggregation

■ no lacp actor admin state aggregation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp actor admin state aggregation

17.2.8 lacp actor admin port priority

Set LACP actor port priority value (default 128).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp actor admin port priority <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

17.2.9 lacp partner admin key

Configure the administrative value of the LACP key for the protocol partner on this LAG (default 0).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin key <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

17.2.10 lacp partner admin state lacp-activity

Enable/disable the LACP activity on the partner admin state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin state lacp-activity

■ no lacp partner admin state lacp-activity

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp partner admin state lacp-activity

17.2.11 lacp partner admin state lacp-timeout

Enable/disable the LACP timeout on the partner admin state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin state lacp-timeout

■ no lacp partner admin state lacp-timeout

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp partner admin state lacp-timeout

17.2.12 lacp partner admin state aggregation

Enable/disable the state aggregation on the partner admin state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin state aggregation

■ no lacp partner admin state aggregation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lacp partner admin state aggregation

17.2.13 lacp partner admin port priority

Set LACP partner port priority value (default 128).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin port priority <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

17.2.14 lacp partner admin port id

Set LACP partner port value (default 0).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin port id <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

17.2.15 lacp partner admin system-priority

Configure the partner system priority.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin system-priority <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

17.2.16 lacp partner admin system-id

Configure the MAC address representing the administrative value of the LAG ports protocol partner system ID default (00:00:00:00:00:00).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lacp partner admin system-id <P-1>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

17.3 show

Display device options and settings.

17.3.1 show link-aggregation port

Show LAG configuration of a single port.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show link-aggregation port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

17.3.2 show link-aggregation statistics

Show ports LAG statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show link-aggregation statistics [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

17.3.3 show link-aggregation members

Show the member ports for specified LAG.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show link-aggregation members <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

17.3.4 show lacp interface

Show LAG interfaces attributes.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lacp interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

17.3.5 show lacp mode

Show lacp mode.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lacp mode [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

17.3.6 show lacp actor

Show Link Aggregation Control protocol actor attributes.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lacp actor [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

17.3.7 show lacp partner operational

Show Operational partner attributes.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lacp partner operational [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

17.3.8 show lacp partner admin

Show administrative partner attributes.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show lacp partner admin [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

18 Ethernet IP

18.1 ethernet-ip

Enable or disable the EtherNet/IP operation on this device. If disabled, the EtherNet/IP protocol is deactivated, but the EtherNet/IP MIBs can be accessed.

18.1.1 ethernet-ip operation

Enable or disable the EtherNet-IP(TM) operation on this device. If disabled, the EtherNet/IP protocol is deactivated, but the EtherNet/IP MIBs can be accessed.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: ethernet-ip operation

■ no ethernet-ip operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no ethernet-ip operation

18.1.2 ethernet-ip write-access

Enable or disable the write-access of the EtherNet/IP protocol. - Possible security risk, as EtherNet/IP communication is not authenticated - .

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: ethernet-ip write-access

■ no ethernet-ip write-access

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no ethernet-ip write-access

18.2 show

Display device options and settings.

18.2.1 show ethernet-ip

Show the Ethernet-ip settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show ethernet-ip

18.3 copy

Copy different kinds of items.

18.3.1 copy eds-ethernet-ip system remote

Copy the EDS file from the device to a file server

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: copy eds-ethernet-ip system remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

19 Filtering Database (FDB)

19.1 mac-filter

19.1.1 mac-filter

Static MAC filter configuration.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mac-filter <P-1> <P-2>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	Enter the VLAN ID.

■ no mac-filter

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no mac-filter <P-1> <P-2>

19.2 bridge

Bridge configuration.

19.2.1 bridge aging-time

Aging time configuration.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: bridge aging-time <P-1>

Parameter	Value	Meaning
P-1	10..500000	Enter a number in the given range.

19.3 show

Display device options and settings.

19.3.1 show mac-filter-table static

Displays the MAC address filter table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-filter-table static

19.4 show

Display device options and settings.

19.4.1 show bridge aging-time

Address aging time.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show bridge aging-time

19.5 show

Display device options and settings.

19.5.1 show mac-addr-table

Displays the MAC address table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-addr-table [<P-1>]

Parameter	Value	Meaning
P-1	a:b:c:d:e:f	Enter a MAC address.
	1..4042	Enter a VLAN ID.

19.6 clear

Clear several items.

19.6.1 clear mac-addr-table

Clears the MAC address table.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear mac-addr-table

20 HiDiscovery

20.1 network

Configure the inband and outband connectivity.

20.1.1 network hidiscovery operation

Enable/disable the HiDiscovery protocol on this device.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network hidiscovery operation <P-1>

Parameter	Value	Meaning
P-1	enable	Enable the HiDiscovery protocol.
	disable	Disable the HiDiscovery protocol.

■ no network hidiscovery operation

Disable the option

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: no network hidiscovery operation <P-1>

20.1.2 network hidiscovery mode

Set the access level for HiDiscovery.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network hidiscovery mode <P-1>

Parameter	Value	Meaning
P-1	read-write	Allow detection and configuration.
	read-only	Allow only detection, no configuration.

20.1.3 network hidiscovery blinking

Enable/disable the HiDiscovery blinking sequence on this device. This preference is not saved in configuration

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network hidiscovery blinking

■ no network hidiscovery blinking

Disable the option

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: no network hidiscovery blinking

20.1.4 network hidiscovery relay

Enable/disable the HiDiscovery relay status.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network hidiscovery relay

■ no network hidiscovery relay

Disable the option

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: no network hidiscovery relay

20.2 show

Display device options and settings.

20.2.1 show network hidiscovery

Show the HiDiscovery settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show network hidiscovery

21 High-availability Seamless Redundancy (HSR) (hardwareabhängig)

21.1 hsr (hardwareabhängig)

Configure High-availability Seamless Redundancy protocol (HSR) parameters.

21.1.1 hsr operation

Enable or disable the High-availability Seamless Redundancy protocol (HSR).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: hsr operation

■ no hsr operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no hsr operation

21.1.2 hsr instance

Configure HSR instances

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: hsr instance <P-1> operation port-a port-b supervision evaluate send redbox-exclusively mode <P-2> switching-node-type <P-3> redbox-id <P-4>

operation: Enable or disable the HSR instance.

port-a: Enable or disable the first port of HSR line.

port-b: Enable or disable the second port of the HSR line.

supervision: Configure the HSR supervision tx and rx packet handling.

evaluate: Enable or disable evaluation of received supervision packets.

send: Enable or disable sending of supervision packets.

redbox-exclusively: Enable sending of supervision packets for this RedBox exclusively. Use the no form of the command to send supervision packets for each connected VDAN and this RedBox (if send is enabled).

mode: Modify HSR operating mode.

switching-node-type: Modify HSR switching end node type.

redbox-id: Modify RedBox identity.

Parameter	Value	Meaning
P-1	1..1	Enter HSR instance number (only 1 supported).
P-2	modeh	HSR mode h - bridging of HSR traffic (default HSR mode).
	modeu	HSR mode u - like mode h, but unicast messages are not removed.
P-3	hsrredboxsan	An HSR RedBox with regular Ethernet traffic on its interlink.
	hsrredboxprpa	An HSR RedBox with PRP traffic for LAN A on its interlink.
	hsrredboxprpb	An HSR RedBox with PRP traffic for LAN B on its interlink.
P-4	id1a	Redbox pair 1 to LAN A.
	id1b	Redbox pair 1 to LAN B.
	id2a	Redbox pair 2 to LAN A.
	id2b	Redbox pair 2 to LAN B.
	id3a	Redbox pair 3 to LAN A.
	id3b	Redbox pair 3 to LAN B.
	id4a	Redbox pair 4 to LAN A.
	id4b	Redbox pair 4 to LAN B.
	id5a	Redbox pair 5 to LAN A.
	id5b	Redbox pair 5 to LAN B.
	id6a	Redbox pair 6 to LAN A.
	id6b	Redbox pair 6 to LAN B.
	id7a	Redbox pair 7 to LAN A.
	id7b	Redbox pair 7 to LAN B.

■ **no hsr instance**

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no hsr instance <P-1> operation port-a port-b supervision evaluate send redbox-exclusively mode switching-node-type redbox-id

21.2 clear

Clear several items.

21.2.1 clear hsr proxy-node-table

Clear proxy-node-table.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear hsr proxy-node-table [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter HSR instance number (only 1 supported).

21.2.2 clear hsr node-table

Clear node-table (received supervision packets).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear hsr node-table [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter HSR instance number (only 1 supported).

21.2.3 clear hsr counters

Clear HSR counters.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear hsr counters [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter HSR instance number (only 1 supported).

21.3 show

Display device options and settings.

21.3.1 show hsr global

Show global preferences.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show hsr global

21.3.2 show hsr instance

Show HSR instances.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show hsr instance [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter HSR instance number (only 1 supported).

21.3.3 show hsr node-table

Show node table (received supervision packets).

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show hsr node-table [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter HSR instance number (only 1 supported).

21.3.4 show hsr proxy-node-table

Show proxy node table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show hsr proxy-node-table [<P-1>]

Paramete	Value	Meaning
P-1	1..1	Enter HSR instance number (only 1 supported).

21.3.5 show hsr counters

Show HSR counters.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show hsr counters [<P-1>]

Paramete	Value	Meaning
P-1	1..1	Enter HSR instance number (only 1 supported).

22 Hypertext Transfer Protocol (HTTP)

22.1 http

Set HTTP parameters.

22.1.1 http port

Set the HTTP port number.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** http port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the HTTP server (default: 80).

22.1.2 http server

Enable or disable the HTTP server.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** http server

■ no http server

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no http server

22.2 show

Display device options and settings.

22.2.1 show http

Show HTTP server information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show http

23 HTTP Secure (HTTPS)

23.1 https

Set HTTPS parameters.

23.1.1 https server

Enable or disable the HTTPS server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: https server

■ no https server

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no https server

23.1.2 https port

Set the HTTPS port number.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: https port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the web server (default: 443).

23.1.3 https certificate

Generate/Delete HTTPS X509/PEM certificate.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: https certificate <P-1>

Parameter	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

23.2 copy

Copy different kinds of items.

23.2.1 copy httpscert remote

Copy X509/PEM certificate from a server to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy httpscert remote <P-1> nvm

nvm: Copy HTTPS certificate (PEM) from a server to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

23.2.2 copy httpscert envm

Copy X509/PEM certificate from external non-volatile memory to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy httpscert envm <P-1> nvm

nvm: Copy X509/PEM certificate from external non-volatile memory to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

23.3 show

Display device options and settings.

23.3.1 show https

Show HTTPS server information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show https

24 Integrated Authentication Server (IAS)

24.1 ias-users

Manage IAS Users and User Accounts.

24.1.1 ias-users add

Add a new IAS user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ias-users add <P-1>`

Paramete Value	Meaning
P-1 string	<user> User name (up to 32 characters).

24.1.2 ias-users delete

Delete an existing IAS user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ias-users delete <P-1>`

Paramete Value	Meaning
P-1 string	<user> User name (up to 32 characters).

24.1.3 ias-users enable

Enable IAS user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `ias-users enable <P-1>`

Paramete Value	Meaning
P-1 string	<user> User name (up to 32 characters).

24.1.4 ias-users disable

Disable IAS user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ias-users disable <P-1>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

24.1.5 ias-users password

Change IAS user password.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ias-users password <P-1> [<P-2>]

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	string	Enter a user-defined text, max. 64 characters.

24.2 show

Display device options and settings.

24.2.1 show ias-users

Display IAS users and user accounts information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show ias-users

25 IEC 61850 MMS Server

25.1 iec61850-mms

Configure the IEC61850 MMS Server settings.

25.1.1 iec61850-mms operation

Enable or disable the IEC61850 MMS Server. The MMS server facilitates real-time distribution of data and supervisory control functions for substations.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: iec61850-mms operation

■ no iec61850-mms operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no iec61850-mms operation

25.1.2 iec61850-mms write-access

Enable or disable the Write-Access on IEC61850 bridge objects via MMS. Write services allow the MMS client to access application content. - Possible security risk, as MMS communication is not authenticated -

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: iec61850-mms write-access

■ no iec61850-mms write-access

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no iec61850-mms write-access

25.1.3 iec61850-mms port

Defines the port number of the IEC61850 MMS server (default: 102).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: iec61850-mms port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the IEC61850 MMS server (default: 102).

25.1.4 iec61850-mms max-sessions

Defines the maximum number of concurrent IEC61850 MMS sessions (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: iec61850-mms max-sessions <P-1>

Parameter	Value	Meaning
P-1	1..15	Maximum number of concurrent IEC61850 MMS sessions (default: 5).

25.1.5 iec61850-mms technical-key

Defines the IEC61850 MMS Technical Key (default: KEY).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: iec61850-mms technical-key <P-1>

Parameter	Value	Meaning
P-1	string	Enter a IEC61850-7-2 Ed. VisibleString, max. 32 characters. The following characters are allowed: VisibleString (FROM ('A' 'a' 'B' 'b' 'C' 'c' 'D' 'd' 'E' 'e' 'F' 'f' 'G' 'g' 'H' 'h' 'I' 'i' 'J' 'j' 'K' 'k' 'L' 'l' 'M' 'm' 'N' 'n' 'O' 'o' 'P' 'p' 'Q' 'q' 'R' 'r' 'S' 's' 'T' 't' 'U' 'u' 'V' 'v' 'W' 'w' 'X' 'x' 'Y' 'y' 'Z' 'z' ' ' '0' '1' '2' '3' '4' '5' '6' '7' '8' '9')

25.2 show

Display device options and settings.

25.2.1 show iec61850-mms

Show the IEC61850 MMS Server settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show iec61850-mms

26 Internet Group Management Protocol (IGMP)

26.1 show

Display device options and settings.

26.1.1 show ip igmp global

Display IGMP global configuration.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Operator
- ▶ **Format:** show ip igmp global

26.1.2 show ip igmp interface

Display IGMP interface information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Operator
- ▶ **Format:** show ip igmp interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

26.1.3 show ip igmp membership

Display interfaces subscribed to the multicast group.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Operator
- ▶ **Format:** show ip igmp membership

26.1.4 show ip igmp groups

Display the subscribed multicast groups.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Operator
- ▶ **Format:** show ip igmp groups

26.1.5 show ip igmp statistics

Display IGMP statistical information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Operator
- ▶ **Format:** show ip igmp statistics [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

27 IGMP Proxy

27.1 show

Display device options and settings.

27.1.1 show ip igmp-proxy global

Displays a summary of the host interface status parameters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip igmp-proxy global

27.1.2 show ip igmp-proxy groups

Displays informations about the subscribed multicast groups that IGMP Proxy reported.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip igmp-proxy groups

27.1.3 show ip igmp-proxy source-list

Displays the source-list of each subscribed multicast group that IGMP Proxy reported.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip igmp-proxy source-list

28 IGMP Snooping

28.1 igmp-snooping

Configure IGMP snooping.

28.1.1 igmp-snooping mode

Enable or disable IGMP snooping.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping mode

■ no igmp-snooping mode

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no igmp-snooping mode

28.1.2 igmp-snooping querier mode

Enable or disable IGMP snooping querier on the system.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping querier mode

■ no igmp-snooping querier mode

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no igmp-snooping querier mode

28.1.3 igmp-snooping querier query-interval

Sets the IGMP querier query interval time (1-1800) in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping querier query-interval <P-1>

Parameter	Value	Meaning
P-1	1..1800	Enter a number in the given range.

28.1.4 igmp-snooping querier timer-expiry

Sets the IGMP querier timer expiration period (60-300) in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping querier timer-expiry <P-1>

Parameter	Value	Meaning
P-1	60..300	Enter a number in the given range.

28.1.5 igmp-snooping querier version

Sets the IGMP version (1-3) of the query.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping querier version <P-1>

Parameter	Value	Meaning
P-1	1..3	IGMP snooping querier's protocol version(1 to 3,default: 2).

28.1.6 igmp-snooping forward-unknown

Configure if and how unknown multicasts are forwarded. The setting can be discard, flood or query-ports. The default is flood.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping forward-unknown <P-1>

Parameter	Value	Meaning
P-1	discard	Unknown multicast frames will be discarded.
	flood	Unknown multicast frames will be flooded.
	query-ports	Unknown multicast frames will be forwarded only to query ports.

28.2 igmp-snooping

Configure IGMP snooping.

28.2.1 igmp-snooping vlan-id

Configure the VLAN parameters.

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** `igmp-snooping vlan-id <P-1> mode fast-leave groupmembership-interval <P-2> maxresponse <P-3> mcrtreptime <P-4> querier mode address <P-5> forward-known <P-6> forward-all <P-7> static-query-port <P-8> automatic-mode <P-9>`

`mode:` Enable or disable IGMP snooping per VLAN.

`fast-leave:` Enable or disable IGMP snooping fast-leave per VLAN.

`groupmembership-interval:` Set IGMP group membership interval time (2-3600) in seconds per VLAN.

`maxresponse:` Set the igmp maximum response time (1-25) in seconds per VLAN.

`mcrtreptime:` Sets the multicast router present expiration time (0-3600) in seconds per VLAN.

`querier:` Set IGMP snooping querier on the system.

`mode:` Enable or disable IGMP snooping querier per VLAN.

`address:` Set IGMP snooping querier address on the system using a VLAN.

`forward-known:` Sets the mode how known multicast packets will be treated. The default value is `registered-ports-only(2)`.

`forward-all:` Enable or disable IGMP snooping forward-all.

`static-query-port:` Enable or disable IGMP snooping static-query-port.

`automatic-mode:` Enable or disable IGMP snooping automatic-mode.

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	2..3600	Enter a number in the given range.
P-3	1..25	Enter a number in the given range.
P-4	0..3600	Enter a number in the given range.
P-5	a.b.c.d	IP address.
P-6	query-and-registered-ports	Addition of query ports to multicast filter portmasks.
	registered-ports-only	No addition of query ports to multicast filter portmasks.
P-7	slot no./port no.	
P-8	slot no./port no.	
P-9	slot no./port no.	

■ **no igmp-snooping vlan-id**

Disable the option

▶ **Mode:** VLAN Database Mode

▶ **Privilege Level:** Operator

▶ **Format:** no igmp-snooping vlan-id <P-1> mode fast-leave groupmembership-interval maxresponse mcrtrexpiretime querier mode address forward-known forward-all <P-7> static-query-port <P-8> automatic-mode <P-9>

28.3 igmp-snooping

Configure IGMP snooping.

28.3.1 igmp-snooping mode

Enable or disable IGMP snooping per interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping mode

■ no igmp-snooping mode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no igmp-snooping mode

28.3.2 igmp-snooping fast-leave

Enable or disable IGMP snooping fast-leave per interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping fast-leave

■ no igmp-snooping fast-leave

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no igmp-snooping fast-leave

28.3.3 igmp-snooping groupmembership-interval

Set IGMP group membership interval time (2-3600) in seconds per interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping groupmembership-interval <P-1>

Parameter	Value	Meaning
P-1	2..3600	Enter a number in the given range.

28.3.4 igmp-snooping maxresponse

Set the igmp maximum response time (1-25) in seconds per interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping maxresponse <P-1>

Parameter	Value	Meaning
P-1	1..25	Enter a number in the given range.

28.3.5 igmp-snooping mcrtrexpiretime

Sets the multicast router present expiration time (0-3600) in seconds per interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping mcrtrexpiretime <P-1>

Parameter	Value	Meaning
P-1	0..3600	Enter a number in the given range.

28.3.6 igmp-snooping static-query-port

Configures the interface as a static query interface in all VLANs.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: igmp-snooping static-query-port

■ **no igmp-snooping static-query-port**

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no igmp-snooping static-query-port

28.4 show

Display device options and settings.

28.4.1 show igmp-snooping global

Show IGMP snooping global information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping global

28.4.2 show igmp-snooping interface

Show IGMP snooping interface information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

28.4.3 show igmp-snooping vlan

Show IGMP snooping VLAN information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

28.4.4 show igmp-snooping querier global

Show IGMP snooping querier information per VLAN.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping querier global

28.4.5 show igmp-snooping querier vlan

Show IGMP snooping querier VLAN information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping querier vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

28.4.6 show igmp-snooping enhancements vlan

Show IGMP snooping VLAN information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping enhancements vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

28.4.7 show igmp-snooping enhancements unknown-filtering

Show unknown multicast filtering information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping enhancements unknown-filtering

28.4.8 show igmp-snooping statistics global

Show number of control packets processed by CPU.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping statistics global

28.4.9 show igmp-snooping statistics interface

Show number of control packets processed by CPU per interface.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show igmp-snooping statistics interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

28.5 show

Display device options and settings.

28.5.1 show mac-filter-table igmp-snooping

Display IGMP snooping entries in the MFDB table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-filter-table igmp-snooping

28.6 clear

Clear several items.

28.6.1 clear igmp-snooping

Clear all IGMP snooping entries.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear igmp-snooping`

29 Interface

29.1 shutdown

29.1.1 shutdown

Enable or disable the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: shutdown

■ no shutdown

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no shutdown

29.2 auto-negotiate

29.2.1 auto-negotiate

Enable or disable automatic negotiation on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-negotiate

■ no auto-negotiate

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no auto-negotiate

29.3 auto-power-down

29.3.1 auto-power-down

Set the auto-power-down mode on the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: auto-power-down <P-1>

Parameter	Value	Meaning
P-1	auto-power-save	The port goes in a low power mode.
	no-power-save	The port does not use the automatic power save mode.

29.4 cable-crossing

29.4.1 cable-crossing

Cable crossing settings on the interface. The cable crossing settings have no effect if auto-negotiation is enabled. In this case cable crossing is always set to auto. Cable crossing is set to the value chosen by the user if auto-negotiation is disabled.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `cable-crossing <P-1>`

Parameter	Value	Meaning
P-1	mdi	The port does not use the crossover mode.
	mdix	The port uses the crossover mode.
	auto-mdix	The port uses the auto crossover mode.

29.5 linktraps

29.5.1 linktraps

Enable/disable link up/down traps on the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: linktraps

■ no linktraps

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no linktraps

29.6 link-loss-alert

Configure Link Loss Alert on the interface.

29.6.1 link-loss-alert operation

Enable or disable Link Loss Alert on the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** link-loss-alert operation

■ **no link-loss-alert operation**

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no link-loss-alert operation

29.7 speed

29.7.1 speed

Sets the speed and duplex setting for the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: speed <P-1> [<P-2>]

Parameter	Value	Meaning
P-1	10	10 MBit/s.
	100	100 MBit/s.
	1000	1000 MBit/s.
P-2	full	full duplex.
	half	half duplex.

29.8 name

29.8.1 name

Set or remove a descriptive name for the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: name <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 64 characters.

29.9 power-state

29.9.1 power-state

Enable or disable the power state on the interface. The interface power state settings have no effect if the interface admin state is enabled.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: power-state

■ no power-state

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no power-state

29.10 mac-filter

29.10.1 mac-filter

static mac filter configuration

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mac-filter <P-1> <P-2>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	Enter the VLAN ID.

■ no mac-filter

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no mac-filter <P-1> <P-2>

29.11 led-signaling

Enable or disable Port LED signaling.

29.11.1 led-signaling operation

Enable or disable Port LED signaling.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: led-signaling operation

■ no led-signaling operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no led-signaling operation

29.12 show

Display device options and settings.

29.12.1 show port

Show interface parameters.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

29.13 show

Display device options and settings.

29.13.1 show link-loss-alert

Show link-loss-alert parameters.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show link-loss-alert [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

29.14 show

Display device options and settings.

29.14.1 show led-signaling operation

Show Port LED signaling operation.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show led-signaling operation

30 Interface Statistics

30.1 utilization

Configure the interface utilization parameters.

30.1.1 utilization control-interval

Add interval time to monitor the bandwidth utilization of the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: utilization control-interval <P-1>

Parameter	Value	Meaning
P-1	1..3600	Add interval time to monitor the bandwidth utilization.

30.1.2 utilization alarm-threshold lower

Lower threshold value

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: utilization alarm-threshold lower <P-1>

Parameter	Value	Meaning
P-1	0..10000	Add alarm threshold lower value for monitoring bandwidth utilization in hundredths of a percent.

30.1.3 utilization alarm-threshold upper

Upper threshold value

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: utilization alarm-threshold upper <P-1>

Parameter	Value	Meaning
P-1	0..10000	Add alarm threshold upper value for monitoring bandwidth utilization in hundredths of a percent.

30.2 clear

Clear several items.

30.2.1 clear port-statistics

Clear all statistics counter.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear port-statistics

30.3 show

Display device options and settings.

30.3.1 show interface counters

Show Table with interface counters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show interface counters

30.3.2 show interface layout

Show interface layout of the device.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show interface layout

30.3.3 show interface utilization

Show interface utilization.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show interface utilization [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

30.3.4 show interface statistics

Show summary interface statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show interface statistics [<P-1>]

Paramete	Value	Meaning
r		
P-1	slot no./port no.	

30.3.5 show interface ether-stats

Show detailed interface statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show interface ether-stats [<P-1>]

Paramete	Value	Meaning
r		
P-1	slot no./port no.	

31 Intern

31.1 help

Display help for various special keys.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** help

31.2 logout

Exit this session.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** any
- ▶ **Format:** logout

31.3 history

Show a list of previously run commands.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** history

31.4 vlan-mode

31.4.1 vlan-mode

Enter VLAN Configuration Mode.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan-mode <P-1>

Parameter	Value	Meaning
P-1	all	Select all VLAN configured.
	vlan	Enter single VLAN.
	vlan range	Enter VLAN range separated by hyphen e.g 1-4.
	vlan list	Enter VLAN list separated by comma e.g 2,4,6,... .
	complex range	Enter VLAN range and several VLAN separated by comma for a list and hyphen for ranges e.g 2-4,6-9,11.

31.5 exit

Exit from vlan mode.

- ▶ Mode: VLAN Mode
- ▶ Privilege Level: Operator
- ▶ Format: `exit`

31.6 end

Exit to exec mode.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** end

31.7 serviceshell

Enter system mode.

31.7.1 serviceshell deactivate

Disable the service shell access permanently (Cannot be undone).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: serviceshell deactivate

31.8 serviceshell-f

Enter system mode.

31.8.1 serviceshell-f deactivate

Disable the service shell access permanently (Cannot be undone).

- ▶ Mode: Factory Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `serviceshell-f deactivate`

31.9 traceroute

Trace route to a specified host.

31.9.1 traceroute maxttl

Set max TTL value.

► **Mode:** Privileged Exec Mode

► **Privilege Level:** Operator

► **Format:** traceroute <P-1> maxttl <P-2> [initttl <P-3>] [interval <P-4>] [count <P-5>] [maxFail <P-6>] [size <P-7>] [port <P-8>]

[initttl]: Initial TTL value.

[interval]: Timeout until probe failure.

[count]: Number of probes for each TTL.

[maxFail]: Maximum number of consecutive probes that can fail.

[size]: Size of payload in bytes.

[port]: UDP destination port.

Parameter	Value	Meaning
P-1	string	Hostname or IP address.
P-2	1..255	Enter a number in the given range.
P-3	0..255	Enter a number in the given range.
P-4	1..60	Enter a number in the given range.
P-5	1..10	Enter a number in the given range.
P-6	0..255	Enter a number in the given range.
P-7	0..65507	Enter a number in the given range.
P-8	1..65535	Enter port number between 1 and 65535

31.10 traceroute

Trace route to a specified host.

31.10.1 traceroute source

Source address for traceroute command.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: traceroute <P-1> source <P-2>

Parameter	Value	Meaning
P-1	string	Hostname or IP address.
P-2	A.B.C.D	IP address.

31.11 reboot

Reset the device (cold start).

31.11.1 reboot after

Schedule reboot after specified time.

- ▶ Mode: All Privileged Modes
- ▶ Privilege Level: any
- ▶ Format: reboot after <P-1>

Parameter	Value	Meaning
P-1	0..2147483	Enter Seconds Between 0 to 2147483. Setting 0 will clear scheduled Reboot if configured.

31.12 ping

31.12.1 ping

Send ICMP echo packets to a specified IP address.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** ping <P-1>

Parameter	Value	Meaning
P-1	string	Hostname or IP address.

31.13 ping

Send ICMP echo packets to a specified host or IP address.

31.13.1 ping source

Source address for ping command.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** ping <P-1> source <P-2>

Parameter	Value	Meaning
P-1	string	Hostname or IP address.
P-2	A.B.C.D	IP address.

31.14 show

Display device options and settings.

31.14.1 show reboot

Display Configured reboot in seconds

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show reboot

31.14.2 show serviceshell

Display the service shell access.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show serviceshell

32 Open Shortest Path First (OSPF)

32.1 show

Display device options and settings.

32.1.1 show ip ospf global

Display OSPF global configurations.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf global

32.1.2 show ip ospf area

Display OSPF area related information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf area [<P-1>]

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.

32.1.3 show ip ospf stub

Display OSPF stub area related information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf stub

32.1.4 show ip ospf database internal

Display the internal LSA database information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf database internal

32.1.5 show ip ospf database external

Display the external LSA database information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf database external

32.1.6 show ip ospf range

Display OSPF area range information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf range

32.1.7 show ip ospf interface

Display OSPF interface related information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

32.1.8 show ip ospf virtual-link

Display OSPF virtual-link related information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf virtual-link <P-1> <P-2>

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	A.B.C.D	IP address.

32.1.9 show ip ospf virtual-neighbor

Display OSPF Virtual-link neighbor information

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf virtual-neighbor

32.1.10 show ip ospf neighbor

Display OSPF neighbor related information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf neighbor [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

32.1.11 show ip ospf statistics

Display OSPF statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf statistics

32.1.12 show ip ospf re-distribute

Display OSPF re-distribute related information

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf re-distribute <P-1>

Parameter	Value	Meaning
P-1	connected	Select the source protocol as connected.
	static	Select the source protocol as static.
	rip	Select the source protocol as RIP.

32.1.13 show ip ospf nssa

Display OSPF NSSA related information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf nssa <P-1>

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.

32.1.14 show ip ospf route

Display OSPF routes.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ip ospf route

33 Internet Protocol Version 4 (IPv4)

33.1 network

Configure the inband and outband connectivity.

33.1.1 network protocol

Select DHCP, BOOTP or none as the network configuration protocol.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network protocol <P-1>

Parameter	Value	Meaning
P-1	none	No network config protocol
	bootp	BOOTP
	dhcp	DHCP

33.1.2 network parms

Set network address, netmask and gateway

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network parms <P-1> <P-2> [<P-3>]

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	A.B.C.D	IP address.
P-3	A.B.C.D	IP address.

33.2 clear

Clear several items.

33.2.1 clear arp-table-switch

Clear the agent's ARP table (cache).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear arp-table-switch

33.3 show

Display device options and settings.

33.3.1 show network parms

Show network settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show network parms

33.4 show

Display device options and settings.

33.4.1 show arp

Show ARP table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show arp

34 Inter Range Instrumentation Group IRIG-B

34.1 irig-b

Set IRIG-B parameters

34.1.1 irig-b operation

Enable or disable the IRIG-B output.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: irig-b operation

■ no irig-b operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no irig-b operation

34.1.2 irig-b mode

Set IRIG-B mode

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: irig-b mode <P-1>

Parameter	Value	Meaning
P-1	b000	Mode IRIG-B000 (BCDtoy, CF, SBS)
	b001	Mode IRIG-B001 (BCDtoy, CF)
	b002	Mode IRIG-B002 (BCDtoy)
	b003	Mode IRIG-B003 (BCDtoy, SBS)
	b004	Mode IRIG-B004 (BCDtoy, BCDyear, CF, SBS)
	b005	Mode IRIG-B005 (BCDtoy, BCDyear, CF)
	b006	Mode IRIG-B006 (BCDtoy, BCDyear)
	b007	Mode IRIG-B007 (BCDtoy, BCDyear, SBS)

34.1.3 irig-b pps

Set IRIG-B pps output parameters

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: irig-b pps

■ no irig-b pps

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no irig-b pps

34.1.4 irig-b time

Set IRIG-B time mode

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: irig-b time <P-1>

Parameter	Value	Meaning
P-1	utc	Transmit UTC.
	local	Transmit local time.

34.2 show

Display device options and settings.

34.2.1 show irig-b

Show IRIG-B settings

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show irig-b

35 Link Backup

35.1 link-backup

Configure Link Backup parameters.

35.1.1 link-backup operation

Enable or disable Link Backup.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: link-backup operation

■ no link-backup operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no link-backup operation

35.2 link-backup

Configure Link Backup parameters.

35.2.1 link-backup add

Add a Link Backup interface pair.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** link-backup add <P-1> [failback-time <P-2>] [description <P-3>]
[failback-time]: FailBack time in seconds for the interface pair.
[description]: Description for the interface pair.

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	0..3600	FailBack time interval.(default: 30)
P-3	string	Enter a user-defined text, max. 256 characters.

35.2.2 link-backup delete

Delete the associated backup interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** link-backup delete <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

35.2.3 link-backup modify

Modify a Link Backup interface pair.

► **Mode:** Interface Range Mode

► **Privilege Level:** Administrator

► **Format:** link-backup modify <P-1> [failback-status <P-2>] [failback-time <P-3>] [description <P-4>] [status <P-5>]

[failback-status]: **Modify failback status.**(default: enabled)

[failback-time]: **Modify failback time.**(default: 30)

[description]: **Description for the interface pair.**

[status]: **Enable or disable a Link Backup interface pair entry.**

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	enable	Enable the option.
	disable	Disable the option.
P-3	0..3600	FailBack time interval.(default: 30)
P-4	string	Enter a user-defined text, max. 256 characters.
P-5	enable	Enable the option.
	disable	Disable the option.

35.3 show

Display device options and settings.

35.3.1 show link-backup operation

Display Link Backup global information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show link-backup operation

35.3.2 show link-backup pairs

Display Link Backup interface pairs.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show link-backup pairs [<P-1>] [<P-2>]

Parameter	Value	Meaning
P-1	slot no./port no.	
P-2	slot no./port no.	

36 Link Layer Discovery Protocol (LLDP)

36.1 lldp

Configure of Link Layer Discovery Protocol.

36.1.1 lldp operation

Enable or disable the LLDP operational state.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp operation

■ no lldp operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp operation

36.1.2 lldp config chassis admin-state

Enable or disable the LLDP operational state.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp config chassis admin-state <P-1>

Parameter	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

36.1.3 lldp config chassis notification-interval

Enter the LLDP notification interval in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp config chassis notification-interval <P-1>

Parameter	Value	Meaning
P-1	5..3600	Enter a number in the given range.

36.1.4 lldp config chassis re-init-delay

Enter the LLDP re-initialization delay in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp config chassis re-init-delay <P-1>

Parameter	Value	Meaning
P-1	1..10	Enter a number in the given range.

36.1.5 lldp config chassis tx-delay

Enter the LLDP transmit delay in seconds (tx-delay smaller than $(0.25 \times \text{tx-interval})$)

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp config chassis tx-delay <P-1>

Parameter	Value	Meaning
P-1	1..8192	Enter a number in the given range (tx-delay smaller than $(0.25 \times \text{tx-interval})$)

36.1.6 lldp config chassis tx-hold-multiplier

Enter the LLDP transmit hold multiplier.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp config chassis tx-hold-multiplier <P-1>

Parameter	Value	Meaning
P-1	2..10	Enter a number in the given range.

36.1.7 lldp config chassis tx-interval

Enter the LLDP transmit interval in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp config chassis tx-interval <P-1>

Parameter	Value	Meaning
P-1	5..32768	Enter a number in the given range.

36.2 show

Display device options and settings.

36.2.1 show lldp global

Display the LLDP global configurations.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp global

36.2.2 show lldp port

Display port specific LLDP configurations.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

36.2.3 show lldp remote-data

Remote information collected with LLDP.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp remote-data [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

36.3 lldp

Configure of Link Layer Discovery Protocol on a port.

36.3.1 lldp admin-state

Configure how the interface processes LLDP frames.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp admin-state <P-1>

Parameter	Value	Meaning
P-1	tx-only	Interface will only transmit LLDP frames. Received frames are not processed.
	rx-only	Interface will only receive LLDP frames. Frames are not transmitted.
	tx-and-rx	Interface will transmit and receive LLDP frames. This is the default setting.
	disable	Interface will neither transmit nor process received LLDP frames.

36.3.2 lldp fdb-mode

Configure the LLDP FDB mode for this interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp fdb-mode <P-1>

Parameter	Value	Meaning
P-1	lldp-only	Collected remote data will be based on received LLDP frames only.
	mac-only	Collected remote data will be based on the switch's FDB entries only.
	both	Collected remote data will be based on received LLDP frames as well as on the switch's FDB entries.
	auto-detect	As long as no LLDP frames are received, the collected remote data will be based on the switch's FDB entries only. After the first LLDP frame is received, the remote data will be based on received LLDP frames only. This is the default setting.

36.3.3 lldp max-neighbors

Enter the LLDP max neighbors for interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp max-neighbors <P-1>

Parameter	Value	Meaning
P-1	1..50	Enter a number in the given range.

36.3.4 lldp notification

Enable or disable the LLDP notification operation for interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp notification

■ no lldp notification

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp notification

36.3.5 lldp tlv inline-power

Enable or disable inline-power TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv inline-power <P-1>

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ no lldp tlv inline-power

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv inline-power <P-1>

36.3.6 lldp tlv link-aggregation

Enable or disable link-aggregation TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv link-aggregation <P-1>

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ no lldp tlv link-aggregation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv link-aggregation <P-1>

36.3.7 lldp tlv mac-phy-config-state

Enable or disable mac-phy-config-state TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv mac-phy-config-state <P-1>

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ no lldp tlv mac-phy-config-state

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv mac-phy-config-state <P-1>

36.3.8 lldp tlv max-frame-size

Enable or disable max-frame-size TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv max-frame-size <P-1>

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no lldp tlv max-frame-size**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv max-frame-size <P-1>

36.3.9 lldp tlv mgmt-addr

Enable or disable mgmt-addr TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv mgmt-addr

■ **no lldp tlv mgmt-addr**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv mgmt-addr

36.3.10 lldp tlv port-desc

Enable or disable port description TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv port-desc <P-1>

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no lldp tlv port-desc**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv port-desc <P-1>

36.3.11 lldp tlv port-vlan

Enable or disable port-vlan TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv port-vlan

■ **no lldp tlv port-vlan**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv port-vlan

36.3.12 lldp tlv protocol

Enable or disable protocol TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv protocol

■ **no lldp tlv protocol**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv protocol

36.3.13 lldp tlv sys-cap

Enable or disable system capabilities TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv sys-cap <P-1>

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ no lldp tlv sys-cap

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv sys-cap <P-1>

36.3.14 lldp tlv sys-desc

Enable or disable system description TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv sys-desc <P-1>

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ no lldp tlv sys-desc

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv sys-desc <P-1>

36.3.15 lldp tlv sys-name

Enable or disable system name TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv sys-name <P-1>

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

■ **no lldp tlv sys-name**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv sys-name <P-1>

36.3.16 lldp tlv vlan-name

Enable or disable vlan name TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv vlan-name

■ **no lldp tlv vlan-name**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv vlan-name

36.3.17 lldp tlv protocol-based-vlan

Enable or disable protocol-based vlan TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv protocol-based-vlan

■ **no lldp tlv protocol-based-vlan**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv protocol-based-vlan

36.3.18 lldp tlv igmp

Enable or disable igmp TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv igmp

■ no lldp tlv igmp

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv igmp

36.3.19 lldp tlv portsec

Enable or disable portsec TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv portsec

■ no lldp tlv portsec

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv portsec

36.3.20 lldp tlv ptp

Enable or disable PTP TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv ptp

■ **no lldp tlv ptp**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv ptp

36.3.21 lldp tlv pnio

Enable or disable PROFINET TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv pnio

■ **no lldp tlv pnio**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv pnio

36.3.22 lldp tlv pnio-alias

Enable or disable PROFINET alias TLV transmission.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp tlv pnio-alias

■ **no lldp tlv pnio-alias**

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp tlv pnio-alias

36.3.23 lldp tlv pnio-mrp

Enable or disable PROFINET MRP TLV transmission.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lldp tlv pnio-mrp

■ **no lldp tlv pnio-mrp**

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no lldp tlv pnio-mrp

37 Media Endpoint Discovery LLDP-MED

37.1 lldp

Configure of Link Layer Discovery Protocol on a port.

37.1.1 lldp med confignotification

Enable or disable LLDP-MED notification send for this interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp med confignotification

■ no lldp med confignotification

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp med confignotification

37.1.2 lldp med transmit-tlv capabilities

Include/Exclude LLDP MED capabilities TLV.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp med transmit-tlv capabilities

■ no lldp med transmit-tlv capabilities

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no lldp med transmit-tlv capabilities

37.1.3 lldp med transmit-tlv network-policy

Include/Exclude LLDP network policy TLV.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** lldp med transmit-tlv network-policy

■ **no lldp med transmit-tlv network-policy**

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no lldp med transmit-tlv network-policy

37.2 lldp

Configure of Link Layer Discovery Protocol.

37.2.1 lldp med faststartrepeatcount

Configure LLDP-MED fast start repeat count.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: lldp med faststartrepeatcount <P-1>

Parameter	Value	Meaning
P-1	1..10	Enter a value representing the number of LLDP PDUs that will be transmitted. Default is 3.

37.3 show

Display device options and settings.

37.3.1 show lldp med global

Display a summary of the current LLDP-MED configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp med global

37.3.2 show lldp med interface

Display the current LLDP-MED configuration on a specific port.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp med interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

37.3.3 show lldp med local-device

Display detailed information about the LLDP-MED data

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp med local-device <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

37.3.4 show lldp med remote-device detail

Display LLDP-MED detail configuration for a remote device.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp med remote-device detail <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

37.3.5 show lldp med remote-device summary

Display LLDP-MED summary configuration for a remote device.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show lldp med remote-device summary [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

38 Logging

38.1 logging

Logging configuration.

38.1.1 logging audit-trail

Add a comment for the audit trail.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging audit-trail <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 80 characters.

38.1.2 logging buffered severity

Configure the minimum severity level to be logged to the high priority buffer.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging buffered severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical

38.1.3 logging host add

Add a new logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host add <P-1> addr <P-2> <P-3> [transport <P-4>] [port <P-5>] [severity <P-6>] [type <P-7>]

addr: Enter the IP address of the server.

[transport]: Configure the type of transport used for syslog server transmission.

[port]: Enter the port used for syslog server transmission.

[severity]: Configure the minimum severity level to be sent to this syslog server.

[type]: Configure the type of log messages to be sent to the syslog server.

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index
P-2	string	Hostname or IP address.
P-3	a.b.c.d	IP address.
P-4	udp	The UDP-based transmission.
	tls	The TLS-based transmission.
P-5	1..65535	Port number to be used
P-6	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
P-7	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug
	systemlog	the system event log entries
audittrail	the audit trail log entries	

38.1.4 logging host delete

Delete a logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host delete <P-1>

Parameter	Value	Meaning
P-1	1..8	Syslog server entry index

38.1.5 logging host enable

Enable a logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host enable <P-1>

Paramete	Value	Meaning
P-1	1..8	Syslog server entry index

38.1.6 logging host disable

Disable a logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host disable <P-1>

Paramete	Value	Meaning
P-1	1..8	Syslog server entry index

38.1.7 logging host modify

Modify an existing logging host.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging host modify <P-1> [addr <P-2> <P-3>] [transport <P-4>] [port <P-5>] [severity <P-6>] [type <P-7>]

[addr]: Enter the IP address of the server.

[transport]: Configure the type of transport used for syslog server transmission.

[port]: Enter the port used for syslog server transmission.

[severity]: Configure the minimum severity level to be sent to this syslog server.

[type]: Configure the type of log messages to be sent to the syslog server.

Paramete	Value	Meaning
P-1	1..8	Syslog server entry index
P-2	string	Hostname or IP address.
P-3	a.b.c.d	IP address.
P-4	udp	The UDP-based transmission.
	tls	The TLS-based transmission.
P-5	1..65535	Port number to be used

Parameter	Value	Meaning
P-6	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
6	Same as informational	
7	Same as debug	
P-7	systemlog	the system event log entries
	audittrail	the audit trail log entries

38.1.8 logging syslog operation

Enable or disable the syslog client.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging syslog operation

■ no logging syslog operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging syslog operation

38.1.9 logging current-console operation

Enable or disable logging messages to the current remote console.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging current-console operation

■ no logging current-console operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging current-console operation

38.1.10 logging current-console severity

Configure the minimum severity level to be sent to the current remote console.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging current-console severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
7	Same as debug	

38.1.11 logging console operation

Enable or disable logging to the local V.24 console.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging console operation

■ no logging console operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging console operation

38.1.12 logging console severity

Configure the minimum severity level to be logged to the V.24 console.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging console severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
6	Same as informational	
7	Same as debug	

38.1.13 logging persistent operation

Enable or disable persistent logging. This feature is only available when an ENVM is connected to the device. The logging information is saved on the selected ENVM.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging persistent operation

■ no logging persistent operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging persistent operation

38.1.14 logging persistent numfiles

Enter the maximum number of log files.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging persistent numfiles <P-1>

Paramete	Value	Meaning
P-1	0..25	number of logfiles

38.1.15 logging persistent filesize

Enter the maximum size of a log file.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging persistent filesize <P-1>

Paramete	Value	Meaning
P-1	0..4096	Maximum persistent logfile size on the non-volatile memory in kBytes

38.1.16 logging persistent severity-level

Configure the minimum severity level to be logged into files.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging persistent severity-level <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
6	Same as informational	
7	Same as debug	

38.1.17 logging email operation

Enable or disable logging email-alert globally.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email operation

■ no logging email operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging email operation

38.1.18 logging email from-addr

Configure mail address used by device to send email-alert.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email from-addr <P-1>

Parameter	Value	Meaning
P-1	string	Enter a valid email address

38.1.19 logging email duration

Periodic timer (in minutes) to send an non-critical logs in mail.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email duration <P-1>

Parameter	Value	Meaning
P-1	30..1440	Time duration in minutes

38.1.20 logging email severity urgent

Urgent severity level

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email severity urgent <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
2	Same as critical	
3	Same as error	
4	Same as warning	
5	Same as notice	
6	Same as informational	
7	Same as debug	

38.1.21 logging email severity non-urgent

Non-urgent severity level

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email severity non-urgent <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
3	Same as error	
4	Same as warning	
5	Same as notice	
6	Same as informational	
7	Same as debug	

38.1.22 logging email to-addr add

Create a destination address entry with default values

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email to-addr add <P-1> [addr <P-2>] [msgtype <P-3>]

[addr]: Create an entry with specified address

[msgtype]: Create an entry with specified message type

Parameter	Value	Meaning
P-1	1..10	Destination address entry index
P-2	string	Enter a valid email address
P-3	urgent	Urgent message type
	non-urgent	Non-urgent message type

38.1.23 logging email to-addr delete

Delete a destination address

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email to-addr delete <P-1>

Parameter	Value	Meaning
P-1	1..10	Destination address entry index

38.1.24 logging email to-addr modify

Modify a destination address

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: logging email to-addr modify <P-1> [addr <P-2>] [msgtype <P-3>]
- [addr]: Modify the destination address
[msgtype]: Modify the message type

Parameter	Value	Meaning
P-1	1..10	Destination address entry index
P-2	string	Enter a valid email address
P-3	urgent	Urgent message type
	non-urgent	Non-urgent message type

38.1.25 logging email mail-server add

Add a server entry to SMTP address table

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: logging email mail-server add <P-1> [addr <P-2>] [security <P-3>] [username <P-4>] [password <P-5>] [port <P-6>] [timeout <P-7>] [description <P-8>]
- [addr]: SMTP server address
[security]: Security mode used in SMTP server.
[username]: Login ID to access SMTP server.
[password]: Password to access SMTP server.
[port]: SMTP server port number.
[timeout]: SMTP server connection timeout
[description]: SMTP server description

Parameter	Value	Meaning
P-1	1..5	SMTP server index
P-2	string	Hostname or IP address.
P-3	none	Security mode none
	tlsv1	Security mode TLSv1
P-4	string	Enter a user-defined text, max. 32 characters.
P-5	string	Enter a user-defined text, max. 32 characters.
P-6	1..65535	Port number to be used
P-7	1..15	SMTP server timeout range
P-8	string	Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).

38.1.26 logging email mail-server delete

Delete a server entry from SMTP address table

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email mail-server delete <P-1>

Parameter	Value	Meaning
P-1	1..5	SMTP server index

38.1.27 logging email mail-server modify

Modify an SMTP server entry

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email mail-server modify <P-1> [addr <P-2>] [security <P-3>] [username <P-4>] [password <P-5>] [port <P-6>] [timeout <P-7>] [description <P-8>]

[addr]: SMTP server address

[security]: Security mode used in SMTP server.

[username]: Login ID to access SMTP server.

[password]: Password to access SMTP server.

[port]: SMTP server port number.

[timeout]: SMTP Timeout

[description]: SMTP server description

Parameter	Value	Meaning
P-1	1..5	SMTP server index
P-2	string	Hostname or IP address.

Parameter	Value	Meaning
P-3	none	Security mode none
	tlsv1	Security mode TLSv1
P-4	string	Enter a user-defined text, max. 32 characters.
P-5	string	Enter a user-defined text, max. 32 characters.
P-6	1..65535	Port number to be used
P-7	1..15	SMTP server timeout range
P-8	string	Enter a user-defined text, max. 1024 characters (allowed characters are from ASCII 32 to 127).

38.1.28 logging email subject add

Create an email subject entry

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email subject add <P-1> [<P-2>]

Parameter	Value	Meaning
P-1	urgent	Urgent message type
	non-urgent	Non-urgent message type
P-2	string	<string> Enter the email subject (Within double quotations if subject includes space)

38.1.29 logging email subject delete

Delete an email subject entry

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email subject delete <P-1>

Parameter	Value	Meaning
P-1	urgent	Urgent message type
	non-urgent	Non-urgent message type

38.1.30 logging email subject modify

Modify an email subject entry

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email subject modify <P-1> <P-2>

Parameter	Value	Meaning
P-1	urgent	Urgent message type
	non-urgent	Non-urgent message type
P-2	string	<string> Enter the email subject (Within double quotations if subject includes space)

38.1.31 logging email test msgtype

Configure the message type for test mail.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging email test msgtype <P-1> <P-2>

Parameter	Value	Meaning
P-1	urgent	Urgent message type
	non-urgent	Non-urgent message type
P-2	string	Enter a user-defined text, max. 255 characters.

38.2 show

Display device options and settings.

38.2.1 show logging buffered

Display buffered (in-memory) log entries.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging buffered [<P-1>]

Parameter	Value	Meaning
P-1	string	<filter> Enter a comma separated list of severity ranges, numbers or enum strings are allowed. Example: 0-1,informational-debug

38.2.2 show logging traplogs

Display trap log entries.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging traplogs

38.2.3 show logging console

Display console logging configurations.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging console

38.2.4 show logging syslog

Display current syslog operational setting.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging syslog

38.2.5 show logging host

Display a list of logging hosts currently configured.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging host

38.2.6 show logging email statistics

Display the statistics of email logging.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging email statistics

38.2.7 show logging email global

Display global settings of email logging feature.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging email global

38.2.8 show logging email to-addr

Display list of destination addresses configured.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging email to-addr [<P-1>]

Parameter	Value	Meaning
P-1	1..10	Destination address entry index

38.2.9 show logging email subject

Display the subject entries configured.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging email subject [<P-1>]

Parameter	Value	Meaning
P-1	urgent	Urgent message type
	non-urgent	Non-urgent message type

38.2.10 show logging email mail-server

Display SMTP server settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show logging email mail-server [<P-1>]

Parameter	Value	Meaning
P-1	1..5	SMTP server index

38.3 copy

Copy different kinds of items.

38.3.1 copy eventlog buffered remote

Copy a buffered log from the device to a file server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: copy eventlog buffered remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

38.3.2 copy traplog system remote

Copy the traplog from the device to a file server

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: copy traplog system remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

38.3.3 copy audittrail system remote

Copy the audit trail from the device to a file server.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator, Auditor
- ▶ Format: copy audittrail system remote <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

38.3.4 copy mailcacert remote

Copy CA certificate file (*.pem) from the remote AD server to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy mailcacert remote <P-1> nvm [<P-2>]

nvm: Copy CA certificate file (*.pem) from the remote AD server to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 100 characters.

38.3.5 copy mailcacert envm

Copy CA certificate file (*.pem) from external non-volatile memory to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy mailcacert envm <P-1> nvm [<P-2>]

nvm: Copy CA certificate file (*.pem) from external non-volatile memory to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 100 characters.

38.3.6 copy syslogcacert remote

Copy CA certificate file (*.pem) from the remote AD server to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy syslogcacert remote <P-1> nvm [<P-2>]

nvm: Copy CA certificate file (*.pem) from the remote AD server to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 100 characters.

38.3.7 copy syslogcert envm

Copy CA certificate file (*.pem) from external non-volatile memory to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy syslogcert envm <P-1> nvm [<P-2>]

nvm: Copy CA certificate file (*.pem) from external non-volatile memory to the device.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 100 characters.

38.4 clear

Clear several items.

38.4.1 clear logging buffered

Clear buffered log from memory.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear logging buffered

38.4.2 clear logging email statistics

Clear email statistics

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear logging email statistics

38.4.3 clear eventlog

Clear the event log entries from memory.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear eventlog

39 Parallel Redundancy Protocol (PRP)

(hardwareabhängig)

39.1 prp (hardwareabhängig)

Configure parallel redundancy protocol (PRP) parameters and clear tables and counters.

39.1.1 prp operation

Enable or disable the parallel redundancy protocol (PRP).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: prp operation

■ no prp operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no prp operation

39.1.2 prp instance

Configure PRP instances

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: prp instance <P-1> operation port-a port-b supervision evaluate send redbox-exclusively speed <P-2>

operation: Enable or disable the PRP instance.

port-a: Enable or disable the first port of the PRP line.

port-b: Enable or disable the second port of the PRP line.

supervision: Configure the PRP supervision tx and rx packet handling.

evaluate: Enable or disable evaluation of received supervision packets.

send: Enable or disable sending of supervision packets.

redbox-exclusively: Enable sending of supervision packets for this RedBox exclusively. Use the no form of the command to send supervision packets for each connected VDAN and this RedBox (if send is enabled).

speed: Configure the speed of LRE interfaces.

Parameter	Value	Meaning
P-1	1..1	Enter PRP instance number (only 1 supported).

Parameter	Value	Meaning
P-2	100	100 MBit/s
	1000	1000 MBit/s

■ **no prp instance**

Disable the option

▶ **Mode:** Global Config Mode

▶ **Privilege Level:** Operator

▶ **Format:** no prp instance <P-1> operation port-a port-b supervision evaluate
send redbox-exclusively speed

39.2 show

Display device options and settings.

39.2.1 show prp global

Show global preferences.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show prp global

39.2.2 show prp instance

Show PRP instances.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show prp instance [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter PRP instance number (only 1 supported).

39.2.3 show prp node-table

Show node table (received supervision packets).

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show prp node-table [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter PRP instance number (only 1 supported).

39.2.4 show prp proxy-node-table

Show proxy node table.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show prp proxy-node-table [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter PRP instance number (only 1 supported).

39.2.5 show prp counters

Show PRP counters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show prp counters [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter PRP instance number (only 1 supported).

39.3 clear

Clear several items.

39.3.1 clear prp proxy-node-table

Clear proxy-node-table.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear prp proxy-node-table [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter PRP instance number (only 1 supported).

39.3.2 clear prp node-table

Clear node-table (received supervision packets).

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear prp node-table [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter PRP instance number (only 1 supported).

39.3.3 clear prp counters

Clear PRP counters.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear prp counters [<P-1>]

Parameter	Value	Meaning
P-1	1..1	Enter PRP instance number (only 1 supported).

40 Management Access

40.1 network

Configure the inband and outband connectivity.

40.1.1 network management access web timeout

Set the web interface idle timeout.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** network management access web timeout <P-1>

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

40.1.2 network management access add

Add a new entry with index.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** network management access add <P-1> [ip <P-2>] [mask <P-3>] [http <P-4>] [https <P-5>] [snmp <P-6>] [telnet <P-7>] [iec61850-mms <P-8>] [modbus-tcp <P-9>] [ssh <P-10>] [ethernet-ip <P-11>] [profinet-io <P-12>]

[ip]: Configure IP address which should have access to management.

[mask]: Configure network mask to allow a subnet for management access.

[http]: Configure if HTTP is allowed to have management access.

[https]: Configure if HTTPS is allowed to have management access.

[snmp]: Configure if SNMP is allowed to have management access.

[telnet]: Configure if TELNET is allowed to have management access.

[iec61850-mms]: Configure if IEC61850-MMS is allowed to have management access.

[modbus-tcp]: Configure if Modbus TCP/IP is allowed to have management access.

[ssh]: Configure if SSH is allowed to have management access.

[ethernet-ip]: Configure if EtherNet/IP is allowed to have management access.

[profinet-io]: Configure if PROFINET is allowed to have management access.

Parameter	Value	Meaning
P-1	1..16	Pool entry index.
P-2	a.b.c.d	IP address.
P-3	0..32	Prefix length netmask.
P-4	enable	Enable the option.
	disable	Disable the option.

Parameter	Value	Meaning
P-5	enable	Enable the option.
	disable	Disable the option.
P-6	enable	Enable the option.
	disable	Disable the option.
P-7	enable	Enable the option.
	disable	Disable the option.
P-8	enable	Enable the option.
	disable	Disable the option.
P-9	enable	Enable the option.
	disable	Disable the option.
P-10	enable	Enable the option.
	disable	Disable the option.
P-11	enable	Enable the option.
	disable	Disable the option.
P-12	enable	Enable the option.
	disable	Disable the option.

40.1.3 network management access delete

Delete an entry with index.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: network management access delete <P-1>

Parameter	Value	Meaning
P-1	1..16	Pool entry index.

40.1.4 network management access modify

Modify an entry with index.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: network management access modify <P-1> ip <P-2> mask <P-3> http <P-4> https <P-5> snmp <P-6> telnet <P-7> iec61850-mms <P-8> modbus-tcp <P-9> ssh <P-10> ethernet-ip <P-11> profinet-io <P-12>

ip: Configure ip-address which should have access to management.

mask: Configure network mask to allow a subnet for management access.

http: Configure if HTTP is allowed to have management access.

https: Configure if HTTPS is allowed to have management access.

snmp: Configure if SNMP is allowed to have management access.

telnet: Configure if TELNET is allowed to have management access.

`iec61850-mms`: Configure if IEC61850-MMS is allowed to have management access.

`modbus-tcp`: Configure if Modbus TCP/IP is allowed to have management access.

`ssh`: Configure if SSH is allowed to have management access.

`ethernet-ip`: Configure if EtherNet/IP is allowed to have management access.

`profinet-io`: Configure if PROFINET is allowed to have management access.

Parameter	Value	Meaning
P-1	1..16	Pool entry index.
P-2	a.b.c.d	IP address.
P-3	0..32	Prefix length netmask.
P-4	enable	Enable the option.
	disable	Disable the option.
P-5	enable	Enable the option.
	disable	Disable the option.
P-6	enable	Enable the option.
	disable	Disable the option.
P-7	enable	Enable the option.
	disable	Disable the option.
P-8	enable	Enable the option.
	disable	Disable the option.
P-9	enable	Enable the option.
	disable	Disable the option.
P-10	enable	Enable the option.
	disable	Disable the option.
P-11	enable	Enable the option.
	disable	Disable the option.
P-12	enable	Enable the option.
	disable	Disable the option.

40.1.5 network management access operation

Enable/Disable operation for RMA.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: network management access operation

■ no network management access operation

Disable the option

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no network management access operation

40.1.6 network management access status

Activate/Deactivate an entry.

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** network management access status <P-1>

Parameter	Value	Meaning
P-1	1..16	Pool entry index.

■ no network management access status

Disable the option

- ▶ **Mode:** Privileged Exec Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** no network management access status <P-1>

40.2 show

Display device options and settings.

40.2.1 show network management access global

Show global restricted management access preferences.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show network management access global

40.2.2 show network management access rules

Show restricted management access rules.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show network management access rules [<P-1>]

Parameter	Value	Meaning
P-1	1..16	Pool entry index.

41 Management Address

41.1 network

Configure the inband and outband connectivity.

41.1.1 network management mac

Configure the locally administered MAC address.

▶ Mode: Privileged Exec Mode

▶ Privilege Level: Operator

▶ Format: network management mac [local-address <P-1>]

[local-address]: Enter the local admin MAC address (xx:xx:xx:xx:xx:xx). If the local address is nonzero, the device starts with this MAC address at the next boot. If the MAC address is changed, they must be stored by the configuration manager. A MAC address with a set multicast bit will not be accepted

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.

41.1.2 network management port

Configure management access per port. Setting to 'all' will allowed access from all ports.

▶ Mode: Privileged Exec Mode

▶ Privilege Level: Operator

▶ Format: network management port <P-1>

Parameter	Value	Meaning
P-1	all or slot no./port no.	

41.2 show

Display device options and settings.

41.2.1 show network management mac

Displays the MAC address settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show network management mac

41.2.2 show network management port

Show the management access port.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show network management port

42 Modbus

42.1 modbus-tcp

Configure Modbus TCP/IP server settings.

42.1.1 modbus-tcp operation

Enable or disable the Modbus TCP/IP server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: modbus-tcp operation

■ no modbus-tcp operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no modbus-tcp operation

42.1.2 modbus-tcp write-access

Enable or disable the write-access on Modbus TCP/IP registers. - Possible security risk, as Modbus TCP/IP communication is not authenticated - .

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: modbus-tcp write-access

■ no modbus-tcp write-access

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no modbus-tcp write-access

42.1.3 modbus-tcp port

Defines the port number of the Modbus TCP/IP server (default: 502).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: modbus-tcp port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Enter port number between 1 and 65535

42.1.4 modbus-tcp max-sessions

Defines the maximum number of concurrent Modbus TCP/IP sessions (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: modbus-tcp max-sessions <P-1>

Parameter	Value	Meaning
P-1	1..5	Maximum number of concurrent Modbus TCP/IP server sessions (default: 5).

42.2 show

Display device options and settings.

42.2.1 show modbus-tcp

Show the Modbus TCP/IP server settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show modbus-tcp

43 Media Redundancy Protocol (MRP)

43.1 mrp

Configure the MRP settings.

43.1.1 mrp domain modify advanced-mode

Configure the MRM Advanced Mode.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify advanced-mode <P-1>

Parameter	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

43.1.2 mrp domain modify manager-priority

Configure the MRM priority.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify manager-priority <P-1>

Parameter	Value	Meaning
P-1	0..65535	Enter the MRM priority (default: 32768).

43.1.3 mrp domain modify mode

Configure the role of the MRP device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify mode <P-1>

Parameter	Value	Meaning
P-1	client	The device will be in the role of a ring client (MRC).
	manager	The device will be in the role of a ring manager (MRM).

43.1.4 mrp domain modify name

Configure the logical name of the MRP domain.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify name <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

43.1.5 mrp domain modify operation

Enable or disable the MRP function.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify operation <P-1>

Parameter	Value	Meaning
P-1	enable	Enable the option.
	disable	Disable the option.

43.1.6 mrp domain modify port primary

Configure the primary ringport.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify port primary <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

43.1.7 mrp domain modify port secondary

Configure the secondary ringport.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify port secondary <P-1> [fixed-backup <P-2>]
[fixed-backup]: Enable or disable the secondary ringport of the manager to be the backup port permanently.

Paramete r	Value	Meaning
P-1	slot no./port no.	
P-2	enable	Enable the option.
	disable	Disable the option.

43.1.8 mrp domain modify recovery-delay

Configure the MRM Recovery Delay.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify recovery-delay <P-1>

Paramete r	Value	Meaning
P-1	500ms	Maximum recovery delay of 500ms in the MRP domain.
	200ms	Maximum recovery delay of 200ms in the MRP domain.
	30ms	Maximum recovery delay of 30ms in the MRP domain.
	10ms	Maximum recovery delay of 10ms in the MRP domain.

43.1.9 mrp domain modify round-trip-delay

Configure the round-trip-delay counters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify round-trip-delay <P-1>

Paramete r	Value	Meaning
P-1	reset	Reset the round-trip-delay counters.

43.1.10 mrp domain modify vlan

Configure the VLAN identifier of the MRP domain.\n(VLAN ID 0 means that no VLAN is used).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain modify vlan <P-1>

Parameter	Value	Meaning
P-1	0..4042	VLAN identifier of the MRP domain.\n(VLAN ID 0 means that no VLAN is used).

43.1.11 mrp domain add default-domain

Default MRP domain ID.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain add default-domain

43.1.12 mrp domain add domain-id

MRP domain ID. Format: 16 bytes in decimal notation.\n(Example: 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain add domain-id <P-1>

Parameter	Value	Meaning
P-1	string	<domain id> MRP domain ID. Format: 16 bytes in decimal notation.\n(Example: 1.2.3.4.5.6.7.8.9.10.11.12.13.14.15.16).

43.1.13 mrp domain delete

Delete the current MRP domain.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp domain delete

43.1.14 mrp operation

Enable or disable MRP.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp operation

■ no mrp operation

Disable the option

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp operation

43.2 show

Display device options and settings.

43.2.1 show mrp

Show MRP settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp

44 MRP IEEE

44.1 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

44.1.1 mrp-ieee global join-time

Set the IEEE multiple registration protocol join time-interval. The join timer controls the interval between join message transmissions sent to applicant state machines. An instance of this timer is required on a per-Port, per-MRP participant basis.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `mrp-ieee global join-time <P-1>`

Parameter	Value	Meaning
P-1	10..100	Join time-interval in centi-seconds.

44.1.2 mrp-ieee global leave-time

Set the IEEE multiple registration protocol leave time-interval. The leave timer controls the period of time that the registrar state machine waits in the leave state before transiting to the empty state. An instance of the timer is required for each state machine in the leave state.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `mrp-ieee global leave-time <P-1>`

Parameter	Value	Meaning
P-1	20..600	Leave time-interval in centi-seconds.

44.1.3 mrp-ieee global leave-all-time

Set the IEEE multiple registration protocol leave-all time-interval. The leave all timer controls the frequency with which the leaveall state machine generates leaveall PDUs. The timer is required on a per-Port, per-MRP Participant basis.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp-ieee global leave-all-time <P-1>

Parameter	Value	Meaning
P-1	200..6000	Leave-All time-interval in centi-seconds.

44.2 show

Display device options and settings.

44.2.1 show mrp-ieee global interface

Show the global configuration of IEEE multiple registration protocol per interface.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee global interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

45 MRP IEEE MMRP

45.1 mrp-ieee

Configure IEEE MRP protocols.

45.1.1 mrp-ieee mmrp vlan-id

Configure the VLAN parameters.

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** mrp-ieee mmrp vlan-id <P-1> forward-all <P-2> forbidden-servicereq <P-3>

forward-all: Enable or disable 'Forward All Groups' in a given Vlan for a given interface.

forbidden-servicereq: Enable or disable the mmrp feature 'Forbidden Service Requirement' in a given Vlan for a given interface.

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	slot no./port no.	
P-3	slot no./port no.	

■ no mrp-ieee mmrp vlan-id

Disable the option

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no mrp-ieee mmrp vlan-id <P-1> forward-all <P-2> forbidden-servicereq <P-3>

45.2 show

Display device options and settings.

45.2.1 show mrp-ieee mmrp global

Display the IEEE MMRP global configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mmrp global

45.2.2 show mrp-ieee mmrp interface

Display the IEEE MMRP interface configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mmrp interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

45.2.3 show mrp-ieee mmrp statistics global

Display the IEEE MMRP global statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mmrp statistics global

45.2.4 show mrp-ieee mmrp statistics interface

Display the IEEE MMRP interface statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mmrp statistics interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

45.2.5 show mrp-ieee mmrp service-requirement forward-all vlan

Show Forward-All setting for port in given VLAN.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mmrp service-requirement forward-all vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

45.2.6 show mrp-ieee mmrp service-requirement forbidden vlan

Show Forward-All setting for port in given VLAN.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mmrp service-requirement forbidden vlan [<P-1>]

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

45.3 mrp-ieee

Configure IEEE MRP protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration.

45.3.1 mrp-ieee mmrp operation

Enable or disable MMRP globally. Devices use MMRP information for dynamic registration of group membership and individual MAC addresses with end devices and switches that support extended filtering services, within the connected LAN.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp-ieee mmrp operation

■ no mrp-ieee mmrp operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no mrp-ieee mmrp operation

45.3.2 mrp-ieee mmrp periodic-machine

Enable or disable MMRP periodic state machine globally. When enabled, the periodic state machine sends extra MMRP messages when the periodic timer expires.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp-ieee mmrp periodic-machine

■ no mrp-ieee mmrp periodic-machine

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no mrp-ieee mmrp periodic-machine

45.4 clear

Clear several items.

45.4.1 clear mrp-ieee mmrp

Clear the IEEE MMRP global and port statistic tables.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear mrp-ieee mmrp`

45.5 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

45.5.1 mrp-ieee mmrp operation

Enable or disable MMRP on the interface, with MMRP enabled globally and on this interface, the device sends and receives MMRP messages on this port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp-ieee mmrp operation

■ no mrp-ieee mmrp operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no mrp-ieee mmrp operation

45.5.2 mrp-ieee mmrp restrict-register

Enable or disable restriction of dynamic mac address registration using IEEE MMRP on the port. When enabled, the dynamic registration of mac address attributes is allowed only if the attribute has already been statically registered on the device.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp-ieee mmrp restrict-register

■ no mrp-ieee mmrp restrict-register

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no mrp-ieee mmrp restrict-register

45.6 show

Display device options and settings.

45.6.1 show mac-filter-table mmrp

Display MMRP entries in the MFDB table.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mac-filter-table mmrp

46 MRP IEEE MVRP

46.1 mrp-ieee

Configure IEEE MRP protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration.

46.1.1 mrp-ieee mvrp operation

Enable or disable IEEE MVRP globally. When enabled, the device distributes VLAN membership information on MVRP enable active ports. MVRP-aware devices use the information to dynamically create VLAN members and update the local VLAN member database.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `mrp-ieee mvrp operation`

■ no mrp-ieee mvrp operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `no mrp-ieee mvrp operation`

46.1.2 mrp-ieee mvrp periodic-machine

Enable or disable IEEE MVRP periodic state machine globally. When enabled, the device sends MVRP messages to the connected MVRP-aware devices when the periodic timer expires.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `mrp-ieee mvrp periodic-machine`

■ no mrp-ieee mvrp periodic-machine

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: `no mrp-ieee mvrp periodic-machine`

46.2 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

46.2.1 mrp-ieee mvrp operation

Enable or disable IEEE MVRP on the port. When enabled, globally and on this port, the device distributes VLAN membership information to MVRP aware devices connected to this port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp-ieee mvrp operation

■ no mrp-ieee mvrp operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no mrp-ieee mvrp operation

46.2.2 mrp-ieee mvrp restrict-register

Enable or disable restriction of dynamic VLAN registration using IEEE MVRP on the port. When enabled, the dynamic registration of VLAN attributes is allowed only if the attribute has already been statically registered on the device.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mrp-ieee mvrp restrict-register

■ no mrp-ieee mvrp restrict-register

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no mrp-ieee mvrp restrict-register

46.3 show

Display device options and settings.

46.3.1 show mrp-ieee mvrp global

Display the IEEE MVRP global configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mvrp global

46.3.2 show mrp-ieee mvrp interface

Display the IEEE MVRP interface configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mvrp interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

46.3.3 show mrp-ieee mvrp statistics global

Display the IEEE MVRP global statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show mrp-ieee mvrp statistics global

46.3.4 show mrp-ieee mvrp statistics interface

Display the IEEE MVRP interface statistics.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mrp-ieee mvrp statistics interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

46.4 clear

Clear several items.

46.4.1 clear mrp-ieee mvrp

Clear the IEEE MVRP global and port statistic tables.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `clear mrp-ieee mvrp`

47 Out-of-band Management

47.1 network

Configure the inband and outband connectivity.

47.1.1 network out-of-band operation

Enable or disable the out-of-band management.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network out-of-band operation

■ no network out-of-band operation

Disable the option

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: no network out-of-band operation

47.1.2 network out-of-band protocol

Select DHCP or none as the out-of-band configuration protocol.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network out-of-band protocol <P-1>

Parameter	Value	Meaning
P-1	none	No out-of-band config protocol.
	dhcp	DHCP

47.1.3 network out-of-band parms

Set out-of-band IP address, subnet mask and gateway.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network out-of-band parms <P-1> <P-2> [<P-3>]

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	A.B.C.D	IP address.
P-3	A.B.C.D	IP address.

47.2 show

Display device options and settings.

48 Protocol Based VLAN

48.1 vlan

Creation and configuration of VLANs.

48.1.1 vlan protocol group add

Add a new group or add protocols to an existing group.

▶ **Mode:** VLAN Database Mode

▶ **Privilege Level:** Operator

▶ **Format:** `vlan protocol group add <P-1> name <P-2> vlan-id <P-3> ethertype <P-4>`

`name`: Assign a group name .

`vlan-id`: Associate a VLAN ID to a group.

`ethertype`: Add protocols to an existing group. Before adding protocols to a group please create one.

Parameter	Value	Meaning
P-1	1..128	Protocol based VLANs group index.
P-2	string	Enter a user-defined text, max. 256 characters.
P-3	1..4042	Enter the VLAN ID.
P-4	string	<protocol-list> Enter a comma-separated list of mnemonics or values, max. 256 chars (eg.: 1536-65535, ip, arp, ipx). Hexadecimal values are entered with a leading \'0x\', eg. 0x600-0xffff.

■ no vlan protocol group add

Disable the option

▶ **Mode:** VLAN Database Mode

▶ **Privilege Level:** Operator

▶ **Format:** `no vlan protocol group add name vlan-id ethertype <P-4>`

48.1.2 vlan protocol group modify

Modify a protocol group.

▶ **Mode:** VLAN Database Mode

▶ **Privilege Level:** Operator

▶ **Format:** `vlan protocol group modify <P-1> [name <P-2>] [vlan-id <P-3>] [ethertype <P-4>]`

`[name]`: Modify the group name.

`[vlan-id]`: Modify the VLAN ID of a group.

[ethertype]: Modify ethertypes from a protocol group.

Parameter	Value	Meaning
P-1	1..128	Protocol based VLANs group index.
P-2	string	Enter a user-defined text, max. 256 characters.
P-3	1..4042	Enter the VLAN ID.
P-4	string	<protocol-list> Enter a comma-separated list of mnemonics or values, max. 256 chars (eg.: 1536-65535, ip, arp, ipx). Hexadecimal values are entered with a leading '\0x\'', eg. 0x600-0xffff.

48.1.3 vlan protocol group delete

Delete a protocol group.

- ▶ Mode: VLAN Database Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan protocol group delete <P-1> [ethertype <P-2>]

[ethertype]: Remove ethertypes from a protocol group.

Parameter	Value	Meaning
P-1	1..128	Protocol based VLANs group index.
P-2	string	<protocol-list> Enter a comma-separated list of mnemonics or values, max. 256 chars (eg.: 1536-65535, ip, arp, ipx). Hexadecimal values are entered with a leading '\0x\'', eg. 0x600-0xffff.

48.2 vlan

Configure 802.1Q port parameters for VLANs.

48.2.1 vlan protocol group add

Add this interface to a group.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `vlan protocol group add <P-1>`

Parameter	Value	Meaning
P-1	1..128	Protocol based VLANs group index.

48.2.2 vlan protocol group delete

Remove this interface from a group.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `vlan protocol group delete <P-1>`

Parameter	Value	Meaning
P-1	1..128	Protocol based VLANs group index.

48.3 show

Display device options and settings.

49 Port Monitor

49.1 port-monitor

Configure the Port Monitor condition settings.

49.1.1 port-monitor operation

Enable or disable the port monitor.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor operation

■ no port-monitor operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-monitor operation

49.2 port-monitor

Configure the Port Monitor condition settings.

49.2.1 port-monitor condition crc-fragments interval

Configure the measure interval in seconds (5-180s) for CRC-Fragment detection. Default 10.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `port-monitor condition crc-fragments interval <P-1>`

Parameter	Value	Meaning
P-1	5..180	Enter a number in the given range.

49.2.2 port-monitor condition crc-fragments count

Configure the CRC-Fragment counter in parts per million (1-1000000 [ppm]). Default 1000 [ppm].

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `port-monitor condition crc-fragments count <P-1>`

Parameter	Value	Meaning
P-1	1..1000000	Enter a number in the given range.

49.2.3 port-monitor condition crc-fragments mode

Enable or disable CRC-Fragments condition to trigger an action.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `port-monitor condition crc-fragments mode`

■ no port-monitor condition crc-fragments mode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-monitor condition crc-fragments mode

49.2.4 port-monitor condition link-flap interval

Configure the measure interval in seconds (1-180s) for Link Flap detection. Default 10.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition link-flap interval <P-1>

Paramete	Value	Meaning
P-1	1..180	Enter a number in the given range.

49.2.5 port-monitor condition link-flap count

Configure the Link Flap counter (1-100). Default 5.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition link-flap count <P-1>

Paramete	Value	Meaning
P-1	1..100	Enter a number in the given range.

49.2.6 port-monitor condition link-flap mode

Enable or disable link-flap condition to trigger an action.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition link-flap mode

■ no port-monitor condition link-flap mode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-monitor condition link-flap mode

49.2.7 port-monitor condition duplex-mismatch mode

Enable or disable duplex mismatch detection condition to trigger an action.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition duplex-mismatch mode

■ no port-monitor condition duplex-mismatch mode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-monitor condition duplex-mismatch mode

49.2.8 port-monitor condition overload-detection traffic-type

Configure Overload detection condition traffic type.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition overload-detection traffic-type <P-1>

Parameter	Value	Meaning
P-1	all	All packets.
	bc	Broadcast packets.
	bc-mc	Broadcast and multicast packets.

49.2.9 port-monitor condition overload-detection unit

Configure Overload detection condition threshold type.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition overload-detection unit <P-1>

Parameter	Value	Meaning
P-1	pps	Packets per second.
	kbps	Kilobits per second.

49.2.10 port-monitor condition overload-detection upper-threshold

Configure Overload detection condition threshold type upper-threshold.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition overload-detection upper-threshold <P-1>

Parameter	Value	Meaning
P-1	0..10000000	Enter a number in the given range.

49.2.11 port-monitor condition overload-detection lower-threshold

Configure Overload detection condition threshold type lower-threshold.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition overload-detection lower-threshold <P-1>

Parameter	Value	Meaning
P-1	0..10000000	Enter a number in the given range.

49.2.12 port-monitor condition overload-detection polling-interval

Configure Overload detection condition detection interval.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition overload-detection polling-interval <P-1>

Parameter	Value	Meaning
P-1	1..20	Enter a number in the given range.

49.2.13 port-monitor condition overload-detection mode

Enable or disable Overload-Detection condition to trigger an action.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition overload-detection mode

■ no port-monitor condition overload-detection mode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-monitor condition overload-detection mode

49.2.14 port-monitor condition speed-duplex mode

Enable or disable link speed and duplex condition to trigger an action.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition speed-duplex mode

■ no port-monitor condition speed-duplex mode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-monitor condition speed-duplex mode

49.2.15 port-monitor condition speed-duplex speed

Set speed-duplex combination.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition speed-duplex speed [<P-1>] [<P-2>] [<P-3>] [<P-4>] [<P-5>] [<P-6>] [<P-7>]

Parameter	Value	Meaning
P-1	[hdx10]	10 Mbit/s - half duplex
P-2	[fdx10]	10 Mbit/s - full duplex
P-3	[hdx100]	100 Mbit/s - half duplex
P-4	[fdx100]	100 Mbit/s - full duplex
P-5	[hdx-1000]	1000 Mbit/s - half duplex
P-6	[fdx-1000]	1000 Mbit/s - full duplex
P-7	[fdx-2500]	2500 Mbit/s - full duplex

49.2.16 port-monitor condition speed-duplex clear

Clear the allowed speed-duplex combination list.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor condition speed-duplex clear

49.2.17 port-monitor action

Enable or disable interface on port condition.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-monitor action <P-1>

Parameter	Value	Meaning
P-1	port-disable	Disable interface on port condition.
	trap-only	Send only a trap.
	auto-disable	Enable or disable interface on port condition by AUTODIS.

49.2.18 port-monitor reset

Reset the port monitor.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-monitor reset [<P-1>]

Parameter	Value	Meaning
P-1	port	Press Enter to execute the command.

■ no port-monitor reset

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no port-monitor reset [<P-1>]

49.3 show

Display device options and settings.

49.3.1 show port-monitor operation

Display the Port Monitor operation.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show port-monitor operation

49.3.2 show port-monitor brief

Display the Port Monitor summary.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show port-monitor brief

49.3.3 show port-monitor overload-detection counters

Display the overload-detection counters of last interval.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show port-monitor overload-detection counters

49.3.4 show port-monitor overload-detection port

Display the Port Monitor overload detection interface details.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor overload-detection port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

49.3.5 show port-monitor speed-duplex

Display the Port Monitor link speed and duplex interface settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor speed-duplex [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

49.3.6 show port-monitor port

Display the Port Monitor interface details.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor port <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

49.3.7 show port-monitor link-flap

Display the link-flaps counts for a specific interface.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-monitor link-flap <P-1>

Paramete	Value	Meaning
P-1	slot no./port no.	

49.3.8 show port-monitor crc-fragments

Display CRC-Fragments counts for a specific interface.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show port-monitor crc-fragments <P-1>

Paramete	Value	Meaning
P-1	slot no./port no.	

50 Port Security

50.1 port-security

Port MAC locking/security

50.1.1 port-security operation

Enable/Disable Port MAC locking/security

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-security operation

■ no port-security operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-security operation

50.2 port-security

Port MAC locking/security

50.2.1 port-security operation

Enable/Disable Port MAC locking/security for the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-security operation

■ no port-security operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no port-security operation

50.2.2 port-security max-dynamic

Set dynamic limit for the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-security max-dynamic <P-1>

Parameter	Value	Meaning
P-1	0..600	maximum number of dynamically locked MAC addresses allowed

50.2.3 port-security max-static

Set Static Limit for the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-security max-static <P-1>

Parameter	Value	Meaning
P-1	0..64	maximum number of statically locked MAC addresses allowed

50.2.4 port-security mac-address add

Add Static MAC address to the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-security mac-address add <P-1> <P-2>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	VLAN ID

50.2.5 port-security mac-address move

Make dynamic MAC addresses static for the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-security mac-address move

50.2.6 port-security mac-address delete

Remove Static MAC address from the interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: port-security mac-address delete <P-1> <P-2>

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	1..4042	VLAN ID

50.2.7 port-security violation-traps

SNMP violation traps for the interface.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** port-security violation-traps operation [frequency <P-1>]
operation: Enable/Disable SNMP violation traps for the interface.
[frequency]: The minimum seconds between two successive violation traps on this port.

Parameter	Value	Meaning
P-1	0..3600	time in seconds

■ no port-security violation-traps

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no port-security violation-traps operation [frequency]

50.3 show

Display device options and settings.

50.3.1 show port-security global

Port Security global status

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security global

50.3.2 show port-security interface

Display port-security (port MAC locking) information for system.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security interface [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

50.3.3 show port-security dynamic

Display dynamically learned MAC addresses

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security dynamic <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

50.3.4 show port-security static

Display statically locked MAC addresses

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security static <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

50.3.5 show port-security violation

Display port security violation information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show port-security violation <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

51 Profinet IO

51.1 profinet

Configures the PROFINET functionality on this device.

51.1.1 profinet operation

Enables or disables the PROFINET functionality on this device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: profinet operation

■ no profinet operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no profinet operation

51.1.2 profinet name-of-station

Sets the name of the station.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: profinet name-of-station <P-1>

Parameter	Value	Meaning
P-1	string	Enter the name of the station, alphanumeric ascii string, max. 240 characters.

51.2 profinet

Configures the PROFINET functionality on this device.

51.2.1 profinet dcp-mode

Sets the PROFINET DCP mode on an interface.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: `profinet dcp-mode <P-1>`

Parameter	Value	Meaning
P-1	none	Sets the PROFINET DCP mode on an interface to none (neither ingress or egress). The agent does not respond to frames received on this interface. The interface does not forward frames received on other interfaces.
	ingress	Sets the PROFINET DCP mode on an interface to ingress only. The agent responds to frames received on this interface. The interface does not forward frames received on other interfaces.
	egress	Sets the PROFINET DCP mode on an interface to egress only. The agent does not respond to frames received on this interface. The interface forwards frames received on other interfaces.
	both	Sets the PROFINET DCP mode on an interface to both (ingress and egress). The agent responds to frames received on this interface. The interface forwards frames received on other interfaces.

51.3 copy

Copy different kinds of items.

51.3.1 copy gsdml-profinet system remote

Copy the GSDML file from the device to the file server

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: `copy gsdml-profinet system remote <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

51.4 show

Display device options and settings.

51.4.1 show profinet global

Show the PROFINET global settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show profinet global

51.4.2 show profinet port

Show the port-related PROFINET settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show profinet port

52 Precision Time Protocol (PTP)

52.1 ptp

Enable or disable the Precision Time Protocol (IEEE 1588-2008).

52.1.1 ptp operation

Enable or disable the Precision Time Protocol (IEEE 1588-2008).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp operation

■ no ptp operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp operation

52.1.2 ptp clock-mode

Configure PTPv2 (IEEE1588-2008) clock mode. \nIf the clock mode is changed, PTP will be initialized.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp clock-mode <P-1>

Parameter	Value	Meaning
P-1	v2-boundary-clock	
	v2-transparent-clock	

52.1.3 ptp sync-lower-bound

Configure the lower bound for the PTP clock synchronization status (unit: nanoseconds). If the absolute value of the offset to the master clock is smaller than the lower bound, the clock's status is set to synchronized (true).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp sync-lower-bound <P-1>

Parameter	Value	Meaning
P-1	1..999999999	

52.1.4 ptp sync-upper-bound

Configure the upper bound for the PTP clock synchronization status (unit: nanoseconds). If the absolute value of the offset to the master clock is bigger than the upper bound, the clock's status is set to unsynchronized (false).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp sync-upper-bound <P-1>

Parameter	Value	Meaning
P-1	31..1000000000	

52.1.5 ptp management

Enable or disable PTP management via PTP management messages.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp management

■ no ptp management

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp management

52.1.6 ptp v2-transparent-clock syntonization

Enable or disable the syntonization (frequency synchronization) of the transparent-clock.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock syntonization

■ no ptp v2-transparent-clock syntonization

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp v2-transparent-clock syntonization

52.1.7 ptp v2-transparent-clock network-protocol

Configure the network-protocol of the transparent-clock.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock network-protocol <P-1>

Parameter	Value	Meaning
P-1	ieee802.3 udp-ipv4	

52.1.8 ptp v2-transparent-clock multi-domain

Enable or disable the transparent-clock to process only the primary-domain or all domain numbers.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock multi-domain

■ no ptp v2-transparent-clock multi-domain

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp v2-transparent-clock multi-domain

52.1.9 ptp v2-transparent-clock sync-local-clock

Enable or disable synchronization of the local clock (also enables syntonization).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock sync-local-clock

■ no ptp v2-transparent-clock sync-local-clock

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp v2-transparent-clock sync-local-clock

52.1.10 ptp v2-transparent-clock delay-mechanism

Configure the delay mechanism of the transparent-clock.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock delay-mechanism <P-1>

Parameter	Value	Meaning
P-1	e2e	
	p2p	
	e2e-optimized	
	disable	

52.1.11 ptp v2-transparent-clock primary-domain

Configure the primary-domain (for syntonization) of the transparent-clock.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock primary-domain <P-1>

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

52.1.12 ptp v2-transparent-clock vlan

VLAN in which PTP packets are send. With a value of none all packets are send untagged.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock vlan <P-1>

Parameter	Value	Meaning
P-1	vlanId	Send ptp to vlanId Use 0 for priority only tagged frames
	none	Send all ptp packets untagged

52.1.13 ptp v2-transparent-clock vlan-priority

VLAN priority of tagged ptp packets.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock vlan-priority <P-1>

Parameter	Value	Meaning
P-1	0..7	

52.1.14 ptp v2-boundary-clock domain

Configure the PTP domain number (0..255)

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock domain <P-1>

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

52.1.15 ptp v2-boundary-clock priority1

Configure the priority1 value (0..255) for the BMCA

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock priority1 <P-1>

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

52.1.16 ptp v2-boundary-clock priority2

Configure the priority2 value (0..255) for the BMCA

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock priority2 <P-1>

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

52.1.17 ptp v2-boundary-clock utc-offset

Configure the current UTC offset (TAI - UTC) in seconds.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock utc-offset <P-1>

Parameter	Value	Meaning
P-1	-32768..32767	

52.1.18 ptp v2-boundary-clock utc-offset-valid

Configure the UTC offset valid flag

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock utc-offset-valid <P-1>

Parameter	Value	Meaning
P-1	true	True
	false	False

■ **no ptp v2-boundary-clock utc-offset-valid**

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp v2-boundary-clock utc-offset-valid <P-1>

52.2 ptp

Enable or disable the Precision Time Protocol (IEEE 1588-2008) on a port.

52.2.1 ptp v2-transparent-clock operation

Enable or disable the sending and receiving / processing of PTP synchronization messages.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock operation

■ no ptp v2-transparent-clock operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp v2-transparent-clock operation

52.2.2 ptp v2-transparent-clock asymmetry

Set the asymmetry of the link connected to this interface

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock asymmetry <P-1>

Parameter	Value	Meaning
P-1	- 2000000000..20000000 00	

52.2.3 ptp v2-transparent-clock pdelay-interval

Configure the Peer Delay Interval in seconds {1|2|4|8|16|32}. \nThis interval is used if delay-mechanism is set to p2p

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-transparent-clock pdelay-interval <P-1>

Parameter	Value	Meaning
P-1	1	
	2	
	4	
	8	
	16	
	32	

52.2.4 ptp v2-boundary-clock operation

Enable or disable the sending and receiving/processing of PTP synchronization messages.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock operation

■ no ptp v2-boundary-clock operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ptp v2-boundary-clock operation

52.2.5 ptp v2-boundary-clock pdelay-interval

Configure the Peer Delay Interval in seconds {1|2|4|8|16|32}. \nThis interval is used if delay-mechanism is set to p2p

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock pdelay-interval <P-1>

Parameter	Value	Meaning
P-1	1	
	2	
	4	
	8	
	16	
	32	

52.2.6 ptp v2-boundary-clock announce-interval

Configure the Announce Interval in seconds {1|2|4|8|16}.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock announce-interval <P-1>

Parameter	Value	Meaning
P-1	1	
	2	
	4	
	8	
	16	

52.2.7 ptp v2-boundary-clock sync-interval

Configure the Sync Interval in seconds {0.25|0.5|1|2}.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock sync-interval <P-1>

Parameter	Value	Meaning
P-1	0.25	
	0.5	
	1	
	2	

52.2.8 ptp v2-boundary-clock announce-timeout

Configure the Announce Receipt Timeout (2..10).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock announce-timeout <P-1>

Parameter	Value	Meaning
P-1	2..10	

52.2.9 ptp v2-boundary-clock asymmetry

Set the asymmetry of the link connected to this interface

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock asymmetry <P-1>

Parameter	Value	Meaning
P-1	- 2000000000..20000000 00	

52.2.10 ptp v2-boundary-clock v1-compatibility-mode

Set the PTPv1 Hardware compatibility mode {auto|on|off}.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock v1-compatibility-mode <P-1>

Parameter	Value	Meaning
P-1	on	
	off	
	auto	

52.2.11 ptp v2-boundary-clock delay-mechanism

Configure the delay mechanism of the boundary-clock.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock delay-mechanism <P-1>

Parameter	Value	Meaning
P-1	e2e	
	p2p	
	disable	

52.2.12 ptp v2-boundary-clock network-protocol

Configure the network-protocol

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock network-protocol <P-1>

Parameter	Value	Meaning
P-1	ieee802.3	
	udp-ipv4	

52.2.13 ptp v2-boundary-clock vlan-priority

VLAN priority of tagged ptp packets.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock vlan-priority <P-1>

Parameter	Value	Meaning
P-1	0..7	

52.2.14 ptp v2-boundary-clock vlan

VLAN in which PTP packets are send. With a value of none all packets are send untagged.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ptp v2-boundary-clock vlan <P-1>

Parameter	Value	Meaning
P-1	vlanId	Send ptp to vlanId Use 0 for priority only tagged frames
	none	Send all ptp packets untagged

52.3 show

Display device options and settings.

52.3.1 show ptp

Show PTP parameters and status

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show ptp [global] [v2-boundary-clock] [v2-transparent-clock] [port] [v2-transparent-clock] [v2-boundary-clock]
[global]: Show PTP global status
[v2-boundary-clock]: Show PTP Boundary Clock status
[v2-transparent-clock]: Show PTP Transparent Clock status
[port]: Show PTP port values
[v2-transparent-clock]: Show the PTP Transparent Clock port values
[v2-boundary-clock]: Show the PTP Boundary Clock port values.

53 Password Management

53.1 passwords

Manage password policies and options.

53.1.1 passwords min-length

Set minimum password length for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: passwords min-length <P-1>

Parameter	Value	Meaning
P-1	1..64	Enter a number in the given range.

53.1.2 passwords max-login-attempts

Set maximum login attempts for the users.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: passwords max-login-attempts <P-1>

Parameter	Value	Meaning
P-1	0..5	Enter a number in the given range.

53.1.3 passwords min-uppercase-chars

Set minimum upper case characters for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: passwords min-uppercase-chars <P-1>

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

53.1.4 passwords min-lowercase-chars

Set minimum lower case characters for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: passwords min-lowercase-chars <P-1>

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

53.1.5 passwords min-numeric-chars

Set minimum numeric characters for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: passwords min-numeric-chars <P-1>

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

53.1.6 passwords min-special-chars

Set minimum special characters for user passwords.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: passwords min-special-chars <P-1>

Parameter	Value	Meaning
P-1	0..16	Enter a number in the given range.

53.2 show

Display device options and settings.

53.2.1 show passwords

Display password policies and options.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show passwords

54 Radius

54.1 authorization

Configure authorization parameters.

54.1.1 authorization network radius

Enable or disable the switch to accept VLAN assignment by the RADIUS server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: authorization network radius

■ no authorization network radius

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no authorization network radius

54.2 radius

Configure RADIUS parameters.

54.2.1 radius accounting mode

Enable or disable RADIUS accounting function.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius accounting mode

■ no radius accounting mode

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no radius accounting mode

54.2.2 radius server attribute 4

Specifies the RADIUS client to use the NAS-IP Address attribute in the RADIUS requests.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server attribute 4 <P-1>

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.

54.2.3 radius server acct add

Add a RADIUS accounting server.

▶ Mode: Global Config Mode

▶ Privilege Level: Administrator

▶ Format: radius server acct add <P-1> ip <P-2> [name <P-3>] [port <P-4>]

ip: RADIUS accounting server IP address.

[name]: RADIUS accounting server name.

[port]: RADIUS accounting server port (default: 1813).

Parameter	Value	Meaning
P-1	1..8	Next RADIUS server valid index (it can be seen with '#show radius global' command).
P-2	string	Hostname or IP address.
P-3	string	Enter a user-defined text, max. 32 characters.
P-4	1..65535	Enter port number between 1 and 65535

54.2.4 radius server acct delete

Delete a RADIUS accounting server.

▶ Mode: Global Config Mode

▶ Privilege Level: Administrator

▶ Format: radius server acct delete <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

54.2.5 radius server acct modify

Change a RADIUS accounting server parameters.

▶ Mode: Global Config Mode

▶ Privilege Level: Administrator

▶ Format: radius server acct modify <P-1> [name <P-2>] [port <P-3>] [status <P-4>] [secret [<P-5>]] [encrypted <P-6>]

[name]: RADIUS accounting server name.

[port]: RADIUS accounting server port (default: 1813).

[status]: Enable or disable a RADIUS accounting server entry.

[secret]: Configure the shared secret for the RADIUS accounting server.

[encrypted]: Configure the encrypted shared secret.

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.
P-2	string	Enter a user-defined text, max. 32 characters.

Parameter	Value	Meaning
P-3	1..65535	Enter port number between 1 and 65535
P-4	enable	Enable the option.
	disable	Disable the option.
P-5	string	Enter a user-defined text, max. 128 characters.
P-6	string	Enter a user-defined text, max. 128 characters.

54.2.6 radius server auth add

Add a RADIUS authentication server.

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: radius server auth add <P-1> ip <P-2> [name <P-3>] [port <P-4>]
- ip: RADIUS authentication server IP address.
[name]: RADIUS authentication server name.
[port]: RADIUS authentication server port (default: 1812).

Parameter	Value	Meaning
P-1	1..8	Next RADIUS server valid index (it can be seen with '#show radius global' command).
P-2	string	Hostname or IP address.
P-3	string	Enter a user-defined text, max. 32 characters.
P-4	1..65535	Enter port number between 1 and 65535

54.2.7 radius server auth delete

Delete a RADIUS authentication server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server auth delete <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

54.2.8 radius server auth modify

Change a RADIUS authentication server parameters.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** radius server auth modify <P-1> [name <P-2>] [port <P-3>] [msgauth <P-4>] [primary <P-5>] [status <P-6>] [secret [<P-7>]] [encrypted <P-8>]
[name]: RADIUS authentication server name.
[port]: RADIUS authentication server port (default: 1812).
[msgauth]: Enable or disable the message authenticator attribute for this server.
[primary]: Configure the primary RADIUS server.
[status]: Enable or disable a RADIUS authentication server entry.
[secret]: Configure the shared secret for the RADIUS authentication server.
[encrypted]: Configure the encrypted shared secret.

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	1..65535	Enter port number between 1 and 65535
P-4	enable disable	Enable the option. Disable the option.
P-5	enable disable	Enable the option. Disable the option.
P-6	enable disable	Enable the option. Disable the option.
P-7	string	Enter a user-defined text, max. 128 characters.
P-8	string	Enter a user-defined text, max. 128 characters.

54.2.9 radius server retransmit

Configure the retransmit value for the RADIUS server.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** radius server retransmit <P-1>

Parameter	Value	Meaning
P-1	1..15	Maximum number of retransmissions (default: 4).

54.2.10 radius server timeout

Configure the RADIUS server timeout value.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: radius server timeout <P-1>

Parameter	Value	Meaning
P-1	1..30	Timeout in seconds (default: 5).

54.3 show

Display device options and settings.

54.3.1 show radius global

Display global RADIUS configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show radius global

54.3.2 show radius auth servers

Display all configured RADIUS authentication servers.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show radius auth servers [<P-1>]

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

54.3.3 show radius auth statistics

Display RADIUS authentication server statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show radius auth statistics <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

54.3.4 show radius acct statistics

Display RADIUS accounting server statistics.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show radius acct statistics <P-1>

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

54.3.5 show radius acct servers

Display all configured RADIUS accounting servers.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show radius acct servers [<P-1>]

Parameter	Value	Meaning
P-1	1..8	RADIUS server index.

54.4 clear

Clear several items.

54.4.1 clear radius

Clear the RADIUS statistics.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: clear radius <P-1>

Paramete	Value	Meaning
P-1	statistics	Clear the RADIUS statistics.

55 Remote Monitoring (RMON)

55.1 rmon-alarm

Create a RMON alarm action.

55.1.1 rmon-alarm add

Add RMON alarm.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** rmon-alarm add <P-1> [mib-variable <P-2>] [rising-threshold <P-3>] [falling-threshold <P-4>]
[mib-variable]: MIB variable
[rising-threshold]: Rising threshold
[falling-threshold]: Falling threshold

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.
P-2	string	Enter an object identifier of the particular variable to be sampled, max. 32 characters.
P-3	1..2147483647	Enter the rising threshold for the sampled statistic.
P-4	1..2147483647	Enter the falling threshold for the sampled statistic.

55.1.2 rmon-alarm enable

Enable RMON alarm.

- ▶ **Mode:** Global Config Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** rmon-alarm enable <P-1>

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

55.1.3 rmon-alarm disable

Disable RMON alarm.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: rmon-alarm disable <P-1>

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

55.1.4 rmon-alarm delete

Delete RMON alarm.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: rmon-alarm delete <P-1>

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

55.1.5 rmon-alarm modify

Modify RMON alarm parameters.

- ▶ Mode: Global Config Mode
 - ▶ Privilege Level: Operator
 - ▶ Format: rmon-alarm modify <P-1> [mib-variable <P-2>] [rising-threshold <P-3>] [falling-threshold <P-4>] [interval <P-5>] [sample-type <P-6>] [startup-alarm <P-7>] [rising-event <P-8>] [falling-event <P-9>]
- [mib-variable]: Enter the alarm mib variable.
- [rising-threshold]: Enter the alarm rising threshold.
- [falling-threshold]: Enter the alarm falling-threshold.
- [interval]: Enter the alarm interval in seconds over which the data is sampled.
- [sample-type]: Enter the alarm method of sampling the selected variable.
- [startup-alarm]: Enter the alarm type.
- [rising-event]: Enter the alarm rising-event index.
- [falling-event]: Enter the alarm falling-event index.

Parameter	Value	Meaning
P-1	1..150	Enter an index that uniquely identifies an entry in the alarm table.

Parameter	Value	Meaning
P-2	string	Enter an object identifier of the particular variable to be sampled, max. 32 characters.
P-3	1..2147483647	Enter the rising threshold for the sampled statistic.
P-4	1..2147483647	Enter the falling threshold for the sampled statistic.
P-5	1..2147483647	Enter the interval in seconds over which the data is sampled and compared with the rising and falling thresholds.
P-6	absoluteValue	Variable is compared directly with the thresholds.
	deltaValue	Variable is subtracted from the current value and the difference compared with the thresholds.
P-7	risingAlarm	Single rising alarm generated when the sample is greater than or equal to the rising threshold.
	fallingAlarm	Single falling alarm generated when the sample is less than or equal to the falling threshold.
	risingOrFallingAlarm	Single Rising alarm generated when the sample is greater than or equal to risingThreshold and single falling alarm generated when the sample is less than or equal to fallingThreshold.
P-8	1..65535	Enter the index of the eventEntry that is used when a rising threshold is crossed.
P-9	1..65535	Enter the index of the eventEntry that is used when a falling threshold is crossed.

55.2 show

Display device options and settings.

55.2.1 show rmon statistics

Show RMON statistics configuration.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show rmon statistics [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

55.2.2 show rmon alarm

Display configuration on RMON alarms.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show rmon alarm

56 Script File

56.1 script

CLI Script File.

56.1.1 script apply

Executes the CLI script file available in the device.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: script apply <P-1>

Parameter	Value	Meaning
P-1	string	Filename.

56.1.2 script validate

Only validates the CLI script file available in the device.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: script validate <P-1>

Parameter	Value	Meaning
P-1	string	Filename.

56.1.3 script list system

List all the script files available in the device memory.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: script list system

56.1.4 script delete

Delete the CLI script files.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: script delete [<P-1>]

Parameter	Value	Meaning
P-1	string	Filename.

56.2 copy

Copy different kinds of items.

56.2.1 copy script remote

Copy script file from server to specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy script remote <P-1> running-config nvm <P-2>

running-config: Copy script file from file server to running-config.

nvm: Copy script file to non-volatile memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.
P-2	string	Enter a user-defined text, max. 32 characters.

56.2.2 copy script nvm

Copy Script file from non-volatile memory to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy script nvm <P-1> running-config envm <P-2> remote <P-3>

running-config: Copy Script file from non-volatile system memory to running-config.

envm: Copy Script file to external non-volatile memory device.

remote: Copy Script file to file server.

Parameter	Value	Meaning
P-1	string	Filename.
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	string	Enter a user-defined text, max. 128 characters.

56.2.3 copy script running-config nvm

Copy running configuration to non-volatile memory.

- ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: copy script running-config nvm <P-1> [all]
- [all]: Copy all running configuration to non-volatile memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

56.2.4 copy script running-config remote

Copy running configuration to a file server.

- ▶ Mode: Privileged Exec Mode
 - ▶ Privilege Level: Administrator
 - ▶ Format: copy script running-config remote <P-1> [all]
- [all]: Copy all running configuration to file server.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

56.3 show

Display device options and settings.

56.3.1 show script system

Displays the content of the CLI script file present in the device.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show script system <P-1>

Parameter	Value	Meaning
P-1	string	Filename.

57 Selftest

57.1 selftest

Configure the selftest settings.

57.1.1 selftest action

Configure the action that a selftest component should take.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: selftest action <P-1> <P-2>

Parameter	Value	Meaning
P-1	task	Configure the action for task errors.
	resource	Configure the action for lack of resources.
	software	Configure the action for broken software integrity.
	hardware	Configure the action for detected hardware errors.
P-2	log-only	Write a message to the logging file.
	send-trap	Send a trap to the management station.
	reboot	Reboot the device.

57.1.2 selftest ramtest

Enable or disable the RAM selftest on cold start of the device. When disabled the device booting time is reduced.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: selftest ramtest

■ no selftest ramtest

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no selftest ramtest

57.1.3 selftest system-monitor

Enable or disable the System Monitor 1 access during the boot phase. Please note: If the System Monitor is disabled it is possible to loose access to the device permanently in case of loosing administrator password or mis-configuration.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: selftest system-monitor

■ no selftest system-monitor

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no selftest system-monitor

57.1.4 selftest boot-default-on-error

Enable or disable loading of the default configuration in case there is any error loading the configuration during boot phase. If disabled the system will be halted.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: selftest boot-default-on-error

■ no selftest boot-default-on-error

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no selftest boot-default-on-error

57.2 show

Display device options and settings.

57.2.1 show selftest action

Displays the actions of the device takes if an error occurs.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show selftest action

57.2.2 show selftest settings

Displays the selftest settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show selftest settings

58 Small Form-factor Pluggable (SFP)

58.1 show

Display device options and settings.

58.1.1 show sfp

Show info about plugged in SFP modules

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show sfp [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

59 Switched Monitoring (SMON)

59.1 monitor

Configure port mirroring.

59.1.1 monitor session

Configure port mirroring.

► **Mode:** Global Config Mode

► **Privilege Level:** Operator

► **Format:** monitor session <P-1> destination interface <P-2> remote vlan <P-3>
source interface <P-4> direction <P-5> operation vlan <P-6> remote vlan <P-7> mode

destination: Configure the probe interface.

interface: Configure interface.

remote: Destination RSPAN configuration.

vlan: Set the destination RSPAN VLAN used to tag the mirrored frames.

source: Configure the source interface.

interface: Configure interface

direction: Select interface.

operation: Enable/disable mirroring on an interface.

vlan: Set the VLAN to mirror.

remote: Source RSPAN configuration.

vlan: Set the source RSPAN VLAN on which mirrored frames are expected.

mode: Enable/Disable port mirroring session. Note: does not affect the source or destination interfaces.

Parameter	Value	Meaning
P-1	1	Monitor session index.
P-2	slot no./port no.	
P-3	integer	VLAN Mirror Remote VLAN ID List.
P-4	slot no./port no.	
P-5	none	None.
	tx	Packets that are transmitted on the source interfaces are copied to the destination interface.
	rx	Packets that are received on the source interfaces are copied to the destination interface.
	txrx	Packets that are transmitted or received on the source interfaces are copied to the destination interface.
P-6	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.
P-7	integer	VLAN Mirror Remote VLAN ID List.

■ **no monitor session**

Disable the option

▶ **Mode:** Global Config Mode

▶ **Privilege Level:** Operator

▶ **Format:** no monitor session <P-1> destination interface remote vlan source
interface <P-4> direction operation vlan remote vlan mode

59.2 show

Display device options and settings.

59.2.1 show monitor session

Display port monitor session settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show monitor session <P-1>

Parameter	Value	Meaning
P-1	1	Monitor session index.

59.3 clear

Clear several items.

59.3.1 clear monitor session

Delete configuration for this session.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: clear monitor session <P-1>

Parameter	Value	Meaning
P-1	1	Monitor session index.

60 Simple Network Management Protocol (SNMP)

60.1 snmp

Configure of SNMP versions and traps.

60.1.1 snmp access version v1

Enable or disable SNMP version V1.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access version v1

■ no snmp access version v1

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no snmp access version v1

60.1.2 snmp access version v2

Enable or disable SNMP version V2.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access version v2

■ no snmp access version v2

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no snmp access version v2

60.1.3 snmp access version v3

Enable or disable SNMP version V3.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access version v3

■ no snmp access version v3

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no snmp access version v3

60.1.4 snmp access port

Configure the SNMP access port.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the SNMP server (default: 161).

60.1.5 snmp access snmp-over-802

Configure SNMPover802.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp access snmp-over-802

■ no snmp access snmp-over-802

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no snmp access snmp-over-802

60.2 show

Display device options and settings.

60.2.1 show snmp access

Show SNMP access configuration settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show snmp access

61 **SNMP Community**

61.1 snmp

Configure of SNMP versions and traps.

61.1.1 snmp community ro

SNMP v1/v2 read-only community.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp community ro

61.1.2 snmp community rw

SNMP v1/v2 read-write community.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp community rw

61.2 show

Display device options and settings.

61.2.1 show snmp community

Display SNMP v1/2 community.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show snmp community

62 SNMP Logging

62.1 logging

Logging configuration.

62.1.1 logging snmp-request get operation

Enable or disable logging of SNMP GET or SET requests.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging snmp-request get operation <P-1>

Parameter	Value	Meaning
P-1	enable	Enable logging of SNMP GET or SET requests.
	disable	Disable logging of SNMP GET or SET requests.

■ no logging snmp-request get operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging snmp-request get operation <P-1>

62.1.2 logging snmp-request get severity

Define severity level.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging snmp-request get severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
6	Same as informational	
7	Same as debug	

62.1.3 logging snmp-request set operation

Enable or disable logging of SNMP GET or SET requests.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging snmp-request set operation <P-1>

Parameter	Value	Meaning
P-1	enable	Enable logging of SNMP GET or SET requests.
	disable	Disable logging of SNMP GET or SET requests.

■ no logging snmp-request set operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no logging snmp-request set operation <P-1>

62.1.4 logging snmp-request set severity

Define severity level.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: logging snmp-request set severity <P-1>

Parameter	Value	Meaning
P-1	emergency	System is unusable. System failure has occurred.
	alert	Action must be taken immediately. Unrecoverable failure of a component. System failure likely.
	critical	Recoverable failure of a component that may lead to system failure.
	error	Error conditions. Recoverable failure of a component.
	warning	Minor failure, e.g. misconfiguration of a component.
	notice	Normal but significant conditions.
	informational	Informational messages.
	debug	Debug-level messages.
	0	Same as emergency
	1	Same as alert
	2	Same as critical
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

62.2 show

Display device options and settings.

62.2.1 show logging snmp

Show the SNMP logging settings.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show logging snmp

63 Simple Network Time Protocol (SNTP)

63.1 sntp

Configure SNTP settings.

63.1.1 sntp client operation

Enable or disable the SNTP client

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client operation

■ no sntp client operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no sntp client operation

63.1.2 sntp client operating-mode

Set the operating mode of the SNTP client. \n\n unicast-mode, the client sends a request to the SNTP Server. \n\n broadcast-mode, the client waits for a broadcast message from the SNTP Server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client operating-mode <P-1>

Parameter	Value	Meaning
P-1	unicast	Set the operating mode to unicast.
	broadcast	Set the operating mode to broadcast.

63.1.3 sntp client request-interval

Set the SNTP client request interval in seconds. \n\nThe request-interval is only used in the operating-mode unicast.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client request-interval <P-1>

Parameter	Value	Meaning
P-1	5..3600	Enter a number in the given range.

63.1.4 sntp client broadcast-rcv-timeout

Set the SNTP client broadcast receive timeout in seconds. \n\nThe broadcast receive timeout is only used in the operating-mode broadcast.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client broadcast-rcv-timeout <P-1>

Parameter	Value	Meaning
P-1	128..2048	Enter a number in the given range.

63.1.5 sntp client disable-after-sync

If this option is activated, the SNTP client disables itself \n\nonce it is synchronized to a SNTP server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client disable-after-sync

■ no sntp client disable-after-sync

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no sntp client disable-after-sync

63.1.6 sntp client server add

Add a SNTP client server connection

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client server add <P-1> <P-2> [port <P-3>] [description <P-4>]
[port]: Set the port number of the external time server.
[description]: Description of the external time server

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.
P-2	string	Hostname or IP address.
P-3	1..65535	Port number of SNTP Server (default 123).
P-4	string	Enter a user-defined text, max. 32 characters.

63.1.7 sntp client server delete

delete a SNTP client server connection

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client server delete <P-1>

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

63.1.8 sntp client server mode

Enable or disable a SNTP client server connection

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp client server mode <P-1>

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

■ no sntp client server mode

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no sntp client server mode <P-1>

63.1.9 sntp server operation

Enable or disable the SNTP server

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server operation

■ no sntp server operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no sntp server operation

63.1.10 sntp server port

Set the local socket port number used to listen for client requests.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of SNTP Server (default 123).

63.1.11 sntp server only-if-synchronized

Set the disabling of the SNTP server function, \nif it is not synchronized to another external time reference

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server only-if-synchronized

■ no sntp server only-if-synchronized

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no sntp server only-if-synchronized

63.1.12 sntp server broadcast operation

Enable or disable the SNTP server broadcast mode

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast operation

■ no sntp server broadcast operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no sntp server broadcast operation

63.1.13 sntp server broadcast address

Set the SNTP server's broadcast or multicast IP address\n(default: 0.0.0.0 (none)).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast address <P-1>

Parameter	Value	Meaning
P-1	a.b.c.d	IP address.

63.1.14 sntp server broadcast port

Set the destination socket port number used to send\nbroadcast or multicast messages to the client.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of SNTP Server (default 123).

63.1.15 sntp server broadcast interval

Set the SNTP server's interval in seconds for sending broadcast or multicast messages.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast interval <P-1>

Parameter	Value	Meaning
P-1	64..1024	Enter a number in the given range.

63.1.16 sntp server broadcast vlan

Set the SNTP server's broadcast VLAN ID used for sending broadcast or multicast messages.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: sntp server broadcast vlan <P-1>

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 uses the management VLAN ID.

63.2 show

Display device options and settings.

63.2.1 show sntp global

Show SNTP configuration parameters and information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show sntp global

63.2.2 show sntp client status

Show SNTP client status.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show sntp client status

63.2.3 show sntp client server

Show SNTP client server connections.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show sntp client server [<P-1>]

Parameter	Value	Meaning
P-1	1..4	Enter a number in the given range.

63.2.4 show sntp server status

Show SNTP server configuration parameters and information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show sntp server status

63.2.5 show sntp server broadcast

Show SNTP server broadcast configuration parameters.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show sntp server broadcast

64 Spanning Tree

64.1 spanning-tree

Enable or disable the Spanning Tree protocol.

64.1.1 spanning-tree operation

Enable or disable the function.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree operation

■ no spanning-tree operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree operation

64.1.2 spanning-tree bpdu-filter

Enable or disable the BPDU filter on the edge ports.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree bpdu-filter

■ no spanning-tree bpdu-filter

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree bpdu-filter

64.1.3 spanning-tree bpdu-guard

Enable or disable the BPDU guard on the edge ports.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree bpdu-guard

■ no spanning-tree bpdu-guard

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree bpdu-guard

64.1.4 spanning-tree bpdu-migration-check

Force the specified port to transmit RST or MST BPDUs.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree bpdu-migration-check <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

64.1.5 spanning-tree forceversion

Set the force protocol version parameter.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree forceversion <P-1>

Parameter	Value	Meaning
P-1	stp	Spanning Tree Protocol (STP).
	rstp	Rapid Spanning Tree Protocol (RSTP).

64.1.6 spanning-tree forward-time

Set the Bridge Forward Delay parameter [s].

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree forward-time <P-1>

Paramete Value	Meaning
P-1 4..30	Enter the bridge forward delay as an integer.

64.1.7 spanning-tree hello-time

Set the Hello Time parameter [s].

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree hello-time <P-1>

Paramete Value	Meaning
P-1 1..2	Set the Hello Time parameter (unit: seconds).

64.1.8 spanning-tree hold-count

Set the bridge hold count parameter.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree hold-count <P-1>

Paramete Value	Meaning
P-1 1..40	Set bridge hold count parameter.

64.1.9 spanning-tree max-age

Set the bridge Max Age parameter.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree max-age <P-1>

Parameter	Value	Meaning
P-1	6..40	Set the bridge Max Age parameter.

64.1.10 spanning-tree ring-only-mode operation

Enable or disable the RSTP Ring Only Mode.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree ring-only-mode operation

■ no spanning-tree ring-only-mode operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree ring-only-mode operation

64.1.11 spanning-tree ring-only-mode first-port

Configure the first ring port.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree ring-only-mode first-port <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

64.1.12 spanning-tree ring-only-mode second-port

Configure the second ring port.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree ring-only-mode second-port <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

64.1.13 spanning-tree mst

MST instance related configuration.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree mst

64.2 spanning-tree

Enable or disable the Spanning Tree protocol on a port.

64.2.1 spanning-tree mode

Enable or disable the function.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree mode

■ no spanning-tree mode

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree mode

64.2.2 spanning-tree bpdu-flood

Enable or disable BPDU flooding on a port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree bpdu-flood

■ no spanning-tree bpdu-flood

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree bpdu-flood

64.2.3 spanning-tree edge-auto

Enable or disable auto edge detection on a port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree edge-auto

■ no spanning-tree edge-auto

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree edge-auto

64.2.4 spanning-tree edge-port

Enable or disable edge port usage on a port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree edge-port

■ no spanning-tree edge-port

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no spanning-tree edge-port

64.2.5 spanning-tree guard-loop

Enable or disable the loop guard on a port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree guard-loop

■ **no spanning-tree guard-loop**

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no spanning-tree guard-loop

64.2.6 spanning-tree guard-root

Enable or disable the root guard on a port.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** spanning-tree guard-root

■ **no spanning-tree guard-root**

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no spanning-tree guard-root

64.2.7 spanning-tree guard-tcn

Enable or disable the TCN guard on a port.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** spanning-tree guard-tcn

■ **no spanning-tree guard-tcn**

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no spanning-tree guard-tcn

64.2.8 spanning-tree cost

Specify the port path cost for STP, RSTP and CIST.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree cost <P-1>

Parameter	Value	Meaning
P-1	0..200000000	Specify the port path cost.

64.2.9 spanning-tree priority

Specify the port priority for STP, RSTP and CIST.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: spanning-tree priority <P-1>

Parameter	Value	Meaning
P-1	0..240	Specify the port priority.

64.3 show

Display device options and settings.

64.3.1 show spanning-tree global

Display the Common and Internal Spanning Tree information and settings.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show spanning-tree global

64.3.2 show spanning-tree mst instance

Display summarized information and settings for all ports in an MST instance.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show spanning-tree mst instance

64.3.3 show spanning-tree mst port

Display summarized information and settings for all ports in an MST instance.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show spanning-tree mst port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

64.3.4 show spanning-tree port

Spanning Tree information and settings for an interface.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show spanning-tree port <P-1>

Parameter	Value	Meaning
P-1	slot no./port no.	

65 Secure Shell (SSH)

65.1 ssh

Set SSH parameters.

65.1.1 ssh server

Enable or disable the SSH server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh server

■ no ssh server

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no ssh server

65.1.2 ssh timeout

Set the SSH connection idle timeout in minutes (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh timeout <P-1>

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

65.1.3 ssh port

Set the SSH server port number (default: 22).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Port number of the SSH server (default: 22).

65.1.4 ssh max-sessions

Set the maximum number of concurrent SSH sessions (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh max-sessions <P-1>

Parameter	Value	Meaning
P-1	1..5	Maximum number of concurrent SSH sessions.

65.1.5 ssh outbound max-sessions

Set the maximum number of concurrent outbound SSH sessions (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh outbound max-sessions <P-1>

Parameter	Value	Meaning
P-1	1..5	Maximum number of concurrent SSH sessions.

65.1.6 ssh outbound timeout

Set the SSH connection idle timeout in minutes (default: 5).

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh outbound timeout <P-1>

Paramete Value	Meaning
P-1 0..160	Idle timeout of a session in minutes (default: 5).

65.1.7 ssh key rsa

Generate or delete RSA key

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh key rsa <P-1>

Paramete Value	Meaning
P-1 generate	Generates the item
delete	Deletes the item

65.1.8 ssh key dsa

Generate or delete DSA key

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: ssh key dsa <P-1>

Paramete Value	Meaning
P-1 generate	Generates the item
delete	Deletes the item

65.2 copy

Copy different kinds of items.

65.2.1 copy sshkey remote

Copy the SSH key from a server to the specified destination.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Administrator
- ▶ Format: copy sshkey remote <P-1> nvm

nvm: Copy the SSH key from a server to non-volatile memory.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 128 characters.

65.3 show

Display device options and settings.

65.3.1 show ssh

Show SSH server and client information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show ssh

66 Storm Control

66.1 storm-control

Configure the global storm-control settings.

66.1.1 storm-control flow-control

Enable or disable flow control globally.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: storm-control flow-control

■ no storm-control flow-control

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: no storm-control flow-control

66.2 traffic-shape

Traffic shape commands.

66.2.1 traffic-shape bw

Set threshold value

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: traffic-shape bw <P-1>

Parameter	Value	Meaning
P-1	0..100	Enter a number in the given range.

66.3 mtu

66.3.1 mtu

Set the MTU size (without VLAN tag size, because the VLAN tag is ignored for size calculation).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mtu <P-1>

Parameter	Value	Meaning
P-1	1518..12288	Enter a number in the given range.

66.4 mtu

66.4.1 mtu

Set the MTU size (without VLAN tag size, because the VLAN tag is ignored for size calculation).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mtu <P-1>

Parameter	Value	Meaning
P-1	1518..1530	Enter a number in the given range.

66.5 mtu

66.5.1 mtu

Set the MTU size (without VLAN tag size, because the VLAN tag is ignored for size calculation).

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: mtu <P-1>

Parameter	Value	Meaning
P-1	1518..12288	Enter a number in the given range.

66.6 storm-control

Storm control commands

66.6.1 storm-control flow-control

Enable or disable flow control (802.3x) for this port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: storm-control flow-control

■ no storm-control flow-control

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no storm-control flow-control

66.6.2 storm-control ingress unit

Set unit.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: storm-control ingress unit <P-1>

Parameter	Value	Meaning
P-1	percent	Metering unit expressed in percentage of bandwidth.
	pps	Metering unit expressed in packets per second.

66.6.3 storm-control ingress threshold

Set threshold value. The rate limiter function calculates the threshold based on data packets sized 512 bytes. When the unit is set to pps, the maximum value is 24414 for 100Mb/s and 244140 for 1000Mb/s.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: storm-control ingress threshold <P-1>

Parameter	Value	Meaning
P-1	0..14880000	Enter a number in the given range. If the configured unit is percent enter a number in (0..100) range.

66.6.4 storm-control ingress unicast operation

Enable/disable ingress unicast storm control.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: storm-control ingress unicast operation

■ no storm-control ingress unicast operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no storm-control ingress unicast operation

66.6.5 storm-control ingress multicast operation

enable/disable ingress multicast storm control.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: storm-control ingress multicast operation

■ no storm-control ingress multicast operation

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no storm-control ingress multicast operation

66.6.6 storm-control ingress broadcast operation

Enable/disable ingress broadcast storm control.

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** storm-control ingress broadcast operation

■ no storm-control ingress broadcast operation

Disable the option

- ▶ **Mode:** Interface Range Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no storm-control ingress broadcast operation

66.7 show

Display device options and settings.

66.7.1 show storm-control flow-control

Global flow control status.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show storm-control flow-control

66.7.2 show storm-control ingress

Show storm control ingress parameters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show storm-control ingress [<P-1>]

Paramete	Value	Meaning
P-1	slot no./port no.	

66.7.3 show traffic-shape

Show Traffic Shape Parameters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show traffic-shape

66.7.4 show mtu

Show mtu Parameters.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show mtu

67 System

67.1 system

Set system related values e.g. name of the device, location of the device, contact data for the person responsible for the device, and pre-login banner text.

67.1.1 system name

Edit the name of the device. The system name consists of an alphanumeric ASCII character string with 0..255 characters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: system name <P-1>

Paramete Value	Meaning
P-1 string	Enter a user-defined text, max. 255 characters.

67.1.2 system location

Edit the location of the device. The system location consists of an alphanumeric ASCII character string with 0..255 characters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: system location <P-1>

Paramete Value	Meaning
P-1 string	Enter a user-defined text, max. 255 characters.

67.1.3 system contact

Edit the contact information for the person responsible for the device. The contact data consists of an alphanumeric ASCII character string with 0..255 characters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Operator
- ▶ Format: system contact <P-1>

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 255 characters.

67.1.4 system pre-login-banner operation

Enable or disable the pre-login banner. You use the pre-login banner to display a greeting or information to users before they login to the device.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `system pre-login-banner operation`

■ no system pre-login-banner operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `no system pre-login-banner operation`

67.1.5 system pre-login-banner text

Edit the text for the pre-login banner (C printf format syntax allowed: `\n\t`) The device allows you to edit an alphanumeric ASCII character string with up to 512 characters.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: `system pre-login-banner text <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 512 characters (allowed characters are from ASCII 32 to 127).

67.1.6 system resources operation

Enable or disable the measurement operation.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: system resources operation

■ no system resources operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no system resources operation

67.2 show

Display device options and settings.

67.2.1 show eventlog

Show event log notice and warning entries with time stamp.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show eventlog

67.2.2 show system info

Show system related information.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system info

67.2.3 show system pre-login-banner

Show pre-login banner status and text.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system pre-login-banner

67.2.4 show system flash-status

Show the flash memory statistics of the device.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system flash-status

67.2.5 show system temperature limits

Show temperature limits.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system temperature limits

67.2.6 show system temperature extremes

Show minimum and maximum recorded temperature.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system temperature extremes

67.2.7 show system temperature histogram

Show the temperature histogram of the device.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system temperature histogram

67.2.8 show system temperature counters

Display number of 20 centigrade C variations in maximum one hour period.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system temperature counters

67.2.9 show system resources

Display the system resources information (cpu utilization, memory and network cpu utilization).

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show system resources

67.2.10 show psu slot

Display power supply slots

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show psu slot

67.2.11 show psu unit

Display information for power supply units.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show psu unit

68 Telnet

68.1 telnet

Set Telnet parameters.

68.1.1 telnet server

Enable or disable the telnet server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: telnet server

■ no telnet server

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no telnet server

68.1.2 telnet timeout

Set the idle timeout for a telnet connection in minutes.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: telnet timeout <P-1>

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

68.1.3 telnet port

Set the listening port for the telnet server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: telnet port <P-1>

Parameter	Value	Meaning
P-1	1..65535	Set the listening port for the telnet server.

68.1.4 telnet max-sessions

Set the maximum number of sessions for the telnet server.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: telnet max-sessions <P-1>

Parameter	Value	Meaning
P-1	1..5	Set the maximum number of connections for the telnet server.

68.2 show

Display device options and settings.

68.2.1 show telnet

Show telnet server information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show telnet

69 Traps

69.1 snmp

Configure of SNMP versions and traps.

69.1.1 snmp trap operation

Global enable/disable SNMP trap.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp trap operation

■ no snmp trap operation

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no snmp trap operation

69.1.2 snmp trap mode

Enable/disable SNMP trap entry.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp trap mode <P-1>

Parameter	Value	Meaning
P-1	string	<name> Trap name (1 to 32 characters)

■ no snmp trap mode

Disable the option

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: no snmp trap mode <P-1>

69.1.3 snmp trap delete

Delete SNMP trap entry.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp trap delete <P-1>

Parameter	Value	Meaning
P-1	string	<name> Trap name (1 to 32 characters)

69.1.4 snmp trap add

Add SNMP trap entry.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: snmp trap add <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<name> Trap name (1 to 32 characters)
P-2	<a.b.c.d>	a.b.c.d Single IP address.
	a.b.c.d:n	a.b.c.d:n Address with port.

69.2 show

Display device options and settings.

69.2.1 show snmp traps

Display SNMP traps.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show snmp traps

70 User Management

70.1 show

Display device options and settings.

70.1.1 show custom-role global

Display the common information of custom role.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show custom-role global [<P-1>]

Paramete Value	Meaning
r	
P-1	slot no./port no.

70.1.2 show custom-role commands

Display the included and excluded commands.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show custom-role commands [<P-1>]

Paramete Value	Meaning
r	
P-1	slot no./port no.

71 Users

71.1 users

Manage Users and User Accounts.

71.1.1 users add

Add a new user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users add <P-1>

Paramete Value	Meaning
P-1 string	<user> User name (up to 32 characters).

71.1.2 users delete

Delete an existing user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users delete <P-1>

Paramete Value	Meaning
P-1 string	<user> User name (up to 32 characters).

71.1.3 users enable

Enable user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users enable <P-1>

Paramete Value	Meaning
P-1 string	<user> User name (up to 32 characters).

71.1.4 users disable

Disable user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users disable <P-1>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

71.1.5 users password

Change user password.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users password <P-1> [<P-2>]

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	string	Enter a user-defined text, max. 64 characters.

71.1.6 users snmpv3 authentication

Specify authentication setting for a user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users snmpv3 authentication <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	md5	MD5 as SNMPv3 user authentication mode.
	sha1	SHA1 as SNMPv3 user authentication mode.

71.1.7 users snmpv3 encryption

Specify encryption settings for a user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users snmpv3 encryption <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	none	SNMPv3 encryption method is none.
	des	DES as SNMPv3 encryption method.
	aes128	AES-128 as SNMPv3 encryption method.

71.1.8 users access-role

Specify snmpv3 access role for a user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users access-role <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	slot no./port no.	

71.1.9 users lock-status

Set the lockout status of a specified user.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users lock-status <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	unlock	Unlock specific user. User can login again.

71.1.10 users password-policy-check

Set password policy check option. The device checks the "minimum password length", regardless of the setting for this option.

- ▶ Mode: Global Config Mode
- ▶ Privilege Level: Administrator
- ▶ Format: users password-policy-check <P-1> <P-2>

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).
P-2	enable	Enable the option.
	disable	Disable the option.

71.2 show

Display device options and settings.

71.2.1 show users

Display users and user accounts information.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Administrator
- ▶ **Format:** show users

72 Virtual LAN (VLAN)

72.1 name

72.1.1 name

Assign a name to a VLAN

- ▶ Mode: VLAN Database Mode
- ▶ Privilege Level: Operator
- ▶ Format: name <P-1> <P-2>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.
P-2	string	Enter a user-defined text, max. 32 characters.

72.2 vlan-unaware-mode

72.2.1 vlan-unaware-mode

Enable or disable VLAN unaware mode.

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** vlan-unaware-mode

■ **no vlan-unaware-mode**

Disable the option

- ▶ **Mode:** VLAN Database Mode
- ▶ **Privilege Level:** Operator
- ▶ **Format:** no vlan-unaware-mode

72.3 vlan

Creation and configuration of VLANS.

72.3.1 vlan add

Create a VLAN

- ▶ Mode: VLAN Database Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan add <P-1>

Paramete	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

72.3.2 vlan delete

Delete a VLAN

- ▶ Mode: VLAN Database Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan delete <P-1>

Paramete	Value	Meaning
P-1	2..4042	Enter VLAN ID. VLAN ID 1 can not be deleted or created

72.4 vlan

Configure 802.1Q port parameters for VLANs.

72.4.1 vlan acceptframe

Configure how to handle tagged/untagged frames received.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan acceptframe <P-1>

Parameter	Value	Meaning
P-1	all	Untagged frames or priority frames received on this interface are accepted and \n assigned the value of the interface VLAN ID for this port.
	vlanonly	Only frames received with a VLAN tag will be forwarded. All other frames will be dropped.

72.4.2 vlan ingressfilter

Enable/Disable application of Ingress Filtering Rules.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan ingressfilter

■ no vlan ingressfilter

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no vlan ingressfilter

72.4.3 vlan priority

Configure the priority for untagged frames.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan priority <P-1>

Parameter	Value	Meaning
P-1	0..7	Enter a number in the given range.

72.4.4 vlan pvid

Configure the VLAN id for a specific port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan pvid <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

72.4.5 vlan tagging

Enable or disable tagging for a specific VLAN port.

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan tagging <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

■ no vlan tagging

Disable the option

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: no vlan tagging <P-1>

72.4.6 vlan participation include

vlan participation to include

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan participation include <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

72.4.7 vlan participation exclude

vlan participation to exclude

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan participation exclude <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

72.4.8 vlan participation auto

vlan participation to auto

- ▶ Mode: Interface Range Mode
- ▶ Privilege Level: Operator
- ▶ Format: vlan participation auto <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

72.5 show

Display device options and settings.

72.5.1 show vlan id

Display configuration of a single specified VLAN.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show vlan id <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

72.5.2 show vlan brief

Show general VLAN parameters.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show vlan brief

72.5.3 show vlan port

Show VLAN configuration of a single port.

- ▶ Mode: Command is in all modes available.
- ▶ Privilege Level: Guest
- ▶ Format: show vlan port [<P-1>]

Parameter	Value	Meaning
P-1	slot no./port no.	

72.5.4 show vlan member current

Show membership of ports in static VLAN or dynamically created.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show vlan member current

72.5.5 show vlan member static

Show membership of ports in static VLAN.

- ▶ **Mode:** Command is in all modes available.
- ▶ **Privilege Level:** Guest
- ▶ **Format:** show vlan member static

72.6 network

Configure the inband and outband connectivity.

72.6.1 network management vlan

Configure the management VLAN ID of the switch.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network management vlan <P-1>

Parameter	Value	Meaning
P-1	1..4042	Enter the VLAN ID.

72.6.2 network management priority dot1p

Configure the management VLAN priority of the switch.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network management priority dot1p <P-1>

Parameter	Value	Meaning
P-1	0..7	Enter a number in the given range.

72.6.3 network management priority ip-dscp

Configure the management VLAN ip-dscp priority of the switch.

- ▶ Mode: Privileged Exec Mode
- ▶ Privilege Level: Operator
- ▶ Format: network management priority ip-dscp <P-1>

Parameter	Value	Meaning
P-1	0..63	Enter a number in the given range.

A Further Support

■ Technical Questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly.

You will find the addresses of our partners on the Internet at

<http://www.hirschmann.com>

Contact our support at

<https://hirschmann-support.belden.eu.com>

You can contact us

in the EMEA region at

- ▶ Tel.: +49 (0)1805 14-1538
- ▶ E-mail: hac.support@belden.com

in the America region at

- ▶ Tel.: +1 (717) 217-2270
- ▶ E-mail: inet-support.us@belden.com

in the Asia-Pacific region at

- ▶ Tel.: +65 6854 9860
- ▶ E-mail: inet-ap@belden.com

■ Hirschmann Competence Center

The Hirschmann Competence Center is ahead of its competitors:

- ▶ Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- ▶ Training offers you an introduction to the basics, product briefing and user training with certification.

The current technology and product training courses can be found at <http://www.hicomcenter.com>

- ▶ Support ranges from the first installation through the standby service to maintenance concepts.

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

Internet:

<http://www.hicomcenter.com>



HIRSCHMANN

A **BELDEN** BRAND



HIRSCHMANN

A **BELDEN** BRAND

Anwender-Handbuch

Konfiguration

HiOS-2E EES (Embedded Ethernet Switch)

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.

© 2017 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.

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

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

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

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

Inhalt

Sicherheitshinweise	9
Über dieses Handbuch	11
Legende	13
Einleitung	15
1 Benutzeroberflächen	17
1.1 Grafische Benutzeroberfläche	18
1.2 Command Line Interface	19
1.2.1 Datenverbindung vorbereiten	19
1.2.2 CLI-Zugang über Telnet	19
1.2.3 CLI über SSH (Secure Shell)	22
1.2.4 CLI über den V.24-Port	24
1.3 System-Monitor	26
1.3.1 Funktionsumfang	26
1.3.2 System-Monitor starten	26
2 IP-Parameter festlegen	29
2.1 Grundlagen IP Parameter	30
2.1.1 IP-Adresse (Version 4)	30
2.1.2 Netzmaske	31
2.1.3 Classless Inter-Domain Routing	33
2.2 IP-Parameter mit dem CLI festlegen	34
2.3 IP-Parameter mit HiDiscovery festlegen	36
2.4 IP-Parameter mit grafischer Benutzeroberfläche festlegen	38
2.5 IP-Parameter mit BOOTP festlegen	39
2.6 IP-Parameter mit DHCP festlegen	40
2.7 Erkennung von Adresskonflikten verwalten	42
2.7.1 Aktive und passive Erkennung	42
3 Zugriff auf das Gerät	45
3.1 Authentifizierungs-Listen	46
3.1.1 Anwendungen	46
3.1.2 Richtlinien	46
3.1.3 Authentifizierungs-Listen verwalten	47
3.1.4 Einstellungen anpassen	47
3.2 Benutzerverwaltung	49
3.2.1 Berechtigungen	49
3.2.2 Benutzerkonten verwalten	50
3.2.3 Voreinstellung	50
3.2.4 Voreingestellte Passwörter ändern	51
3.2.5 Neues Benutzerkonto einrichten	52
3.2.6 Benutzerkonto deaktivieren	53
3.2.7 Richtlinien für Passwörter anpassen	54
3.3 SNMP-Zugriff	55
3.3.1 SNMPv1/v2-Zugriff	55
3.3.2 SNMPv3-Zugriff	56
3.4 Service Shell	57

4	Konfigurationsprofile verwalten	59
4.1	Geänderte Einstellungen erkennen	60
4.2	Einstellungen speichern	61
	4.2.1 Konfigurationsprofil im Gerät speichern	61
	4.2.2 Konfigurationsprofil auf entferntem Server sichern	62
	4.2.3 Konfigurationsprofil exportieren	63
4.3	Einstellungen laden	65
	4.3.1 Konfigurationsprofil aktivieren	65
	4.3.2 Konfigurationsprofil importieren	66
4.4	Gerät auf Lieferzustand zurücksetzen	68
	4.4.1 Mit grafischer Benutzeroberfläche oder CLI	68
	4.4.2 System-Monitor starten	68
5	Neueste Software laden	71
5.1	Software-Update vom PC	72
5.2	Software-Update von einem Server	73
5.3	Ältere Software laden	74
6	Ports konfigurieren	75
6.1	Port ein-/ausschalten	76
6.2	Betriebsart wählen	77
7	Unterstützung beim Schutz vor unberechtigtem Zugriff	79
7.1	SNMPv1/v2-Community ändern	80
7.2	SNMPv1/v2 ausschalten	81
7.3	HTTP ausschalten	82
7.4	Telnet ausschalten	83
7.5	HiDiscovery-Zugriff ausschalten	84
7.6	IP-Zugriffsbeschränkung aktivieren	85
7.7	Session-Timeouts anpassen	87
8	Datenverkehr kontrollieren	89
8.1	Unterstützung beim Schutz vor Denial of Service (DoS)	90
9	Die Systemzeit im Netz synchronisieren	91
9.1	Grundeinstellungen	92
	9.1.1 Uhrzeit einstellen	92
	9.1.2 Automatische Sommerzeitumschaltung	93
9.2	SNTP	94
	9.2.1 Vorbereitung	95
	9.2.2 Einstellungen des SNTP-Clients festlegen	96
	9.2.3 Einstellungen des SNTP-Servers festlegen	96
9.3	PTP	98
	9.3.1 Typen von Uhren	98
	9.3.2 Best-Master-Clock-Algorithmus	99
	9.3.3 Laufzeitmessung	100
	9.3.4 PTP-Domänen	101
	9.3.5 PTP verwenden	101
9.4	IRIG-B/PPS	103
	9.4.1 Vorbereitung	103

9.4.2	IRIG-B einschalten	104
9.4.3	PPS einschalten	104
10	Netzlaststeuerung	105
10.1	Gezielte Paketvermittlung	106
10.1.1	Lernen der MAC-Adressen	107
10.1.2	Aging gelernter MAC-Adressen	107
10.1.3	Statische Adresseinträge	107
10.2	Multicasts	109
10.2.1	Beispiel für eine Multicast-Anwendung	109
10.2.2	IGMP-Snooping	109
10.3	Lastbegrenzung	114
10.4	QoS/Priorität	115
10.4.1	Beschreibung Priorisierung	115
10.4.2	Behandlung empfangener Prioritätsinformationen	116
10.4.3	VLAN-Tagging	117
10.4.4	IP ToS (Type of Service)	118
10.4.5	Handhabung der Verkehrsklassen	118
10.4.6	Queue-Management	119
10.4.7	Management-Priorisierung	120
10.4.8	Priorisierung einstellen	121
10.5	Flusskontrolle	124
10.5.1	Halbduplex- oder Vollduplex-Verbindung	125
10.5.2	Flusskontrolle einrichten	125
11	VLANs	127
11.1	Beispiele für ein VLAN	128
11.1.1	Beispiel 1	128
11.1.2	Beispiel 2	131
11.2	Gast-VLAN / Unauthentifiziertes VLAN	135
11.3	RADIUS-VLAN-Zuordnung	137
11.4	VLAN-Unaware-Modus	138
12	Redundanz	139
12.1	Netz-Topologie vs. Redundanzprotokolle	140
12.1.1	Netz-Topologien	141
12.1.2	Redundanzprotokolle	142
12.1.3	Redundanzkombinationen	142
12.2	Media Redundancy Protocol (MRP)	144
12.2.1	Netzstruktur	144
12.2.2	Rekonfigurationszeit	145
12.2.3	Advanced Mode	145
12.2.4	Voraussetzungen für MRP	145
12.2.5	Beispiel-Konfiguration	146
12.3	Parallelredundanz-Protokoll (PRP)	150
12.3.1	Implementierung	150
12.3.2	LRE-Funktionalität	151
12.3.3	PRP-Netzstruktur	152
12.3.4	RedBoxes und DANPs mit einem PRP-Netz verbinden	152
12.3.5	Beispiel-Konfiguration	153
12.4	High-availability Seamless Redundancy (HSR)	156
12.4.1	Implementierung	156
12.4.2	HSR-Netzstruktur	157
12.5	Spanning Tree	164
12.5.1	Grundlagen	165
12.5.2	Regeln für die Erstellung der Baumstruktur	168

12.5.3	Beispiele	170
12.5.4	Das Rapid Spanning Tree Protokoll	173
12.5.5	Gerät konfigurieren	176
12.5.6	Guards	178
12.5.7	Ring only mode	181
12.5.8	RSTP over HSR	182
12.6	Link-Aggregation	183
12.6.1	Funktionsweise	183
12.6.2	Link-Aggregation Beispiel	184
12.7	Link-Backup	185
12.7.1	Beschreibung Fail-Back	185
12.7.2	Beispiel-Konfiguration	186
13	Funktionsdiagnose	189
13.1	SNMP-Traps senden	190
13.1.1	Auflistung der SNMP-Traps	191
13.1.2	SNMP-Traps für Konfigurationsaktivitäten	191
13.1.3	SNMP-Trap-Einstellung	192
13.1.4	ICMP-Messaging	192
13.2	Gerätstatus überwachen	193
13.2.1	Ereignisse, die überwacht werden können	193
13.2.2	Gerätstatus konfigurieren	194
13.2.3	Gerätstatus anzeigen	195
13.3	Sicherheitsstatus	196
13.3.1	Ereignisse, die überwacht werden können	196
13.3.2	Konfigurieren des Sicherheitsstatus	197
13.3.3	Anzeigen des Sicherheitsstatus	198
13.4	Portereignis-Zähler	199
13.4.1	Erkennen der Nichtübereinstimmung der Duplex-Modi	199
13.5	Auto-Disable	201
13.6	SFP-Zustandsanzeige	203
13.7	Topologie-Erkennung	204
13.7.1	Anzeige der Topologie-Erkennung	205
13.8	Erkennen von Schleifen	206
13.9	Berichte	207
13.9.1	Globale Einstellungen	207
13.9.2	Syslog	209
13.9.3	System-Log	210
13.9.4	Audit Trail	210
13.10	Netzanalyse mit TCPDump	212
13.11	Datenverkehr beobachten	213
13.11.1	Port-Mirroring	213
13.12	Selbsttest	215
14	Erweiterte Funktionen des Gerätes	217
14.1	MRP-IEEE	218
14.1.1	MRP-Funktion	218
14.1.2	MRP-Timer	219
14.1.3	MMRP	219
14.1.4	MVRP	221
14.2	CLI Client	223
15	Industrieprotokolle	225
15.1	IEC 61850/MMS	226

15.1.1	Switch-Modell für IEC 61850	226
15.1.2	Integration in ein Steuerungssystem	227
15.2	Modbus TCP	229
15.2.1	Modbus TCP/IP Client/Server-Modus	229
15.2.2	Unterstützte Funktionen und Speicherzuordnung	230
15.2.3	Beispiel-Konfiguration	232
15.3	EtherNet/IP	235
15.3.1	Integration in ein Steuerungssystem	235
15.3.2	EtherNet/IP -Entity-Parameter	237
15.4	PROFINET	246
15.4.1	Integration in ein Steuerungssystem	248
15.4.2	PROFINET -Parameter	254
A	Konfigurationsumgebung einrichten	259
A.1	DHCP/BOOTP-Server einrichten	260
A.2	DHCP-Server Option 82 einrichten	264
A.3	MAC-Adresse ändern	267
A.4	Management-Port festlegen	268
A.5	SSH-Zugriff vorbereiten	269
A.5.1	Schlüssel auf dem Gerät erzeugen	269
A.5.2	Eigenen Schlüssel in das Gerät laden	269
A.5.3	SSH-Client-Programm vorbereiten	271
A.6	HTTPS-Zertifikat	273
A.6.1	HTTPS-Zertifikatsverwaltung	273
A.6.2	Zugang über HTTPS	274
B	Anhang	275
B.1	Literaturhinweise	276
B.2	Wartung	277
B.3	Management Information BASE (MIB)	278
B.4	Liste der RFCs	280
B.5	Zugrundeliegende IEEE-Normen	282
B.6	Zugrundeliegende IEC-Normen	283
B.7	Zugrundeliegende ANSI-Normen	284
B.8	Technische Daten	285
B.9	Copyright integrierter Software	286
B.10	Verwendete Abkürzungen	287
C	Index	289
D	Weitere Unterstützung	293
E	Leserkritik	294

Sicherheitshinweise

WARNUNG

UNKONTROLLIERTE MASCHINENBEWEGUNGEN

Um unkontrollierte Maschinenbewegungen aufgrund von Datenverlust zu vermeiden, konfigurieren Sie alle Geräte zur Datenübertragung individuell.

Nehmen Sie eine Maschine, die mittels Datenübertragung gesteuert wird, erst in Betrieb, wenn Sie alle Geräte zur Datenübertragung vollständig konfiguriert haben.

Das Nicht-Beachten dieser Anweisung kann zu Tod, schwerer Körperverletzung oder Materialschäden führen.

Über dieses Handbuch

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

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

Das Dokument „Referenz-Handbuch Grafische Benutzeroberfläche“ enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Gerätes über die grafische Oberfläche.

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

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

- ▶ Autotopologie-Erkennung
- ▶ Browser-Interface
- ▶ Client/Server-Struktur
- ▶ Ereignisbehandlung
- ▶ Ereignisprotokoll
- ▶ Gleichzeitige Konfiguration mehrerer Geräte
- ▶ Grafische Benutzeroberfläche mit Netz-Layout
- ▶ SNMP/OPC-Gateway

Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
□	Arbeitsschritt
■	Zwischenüberschrift
Verweis	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
<code>Courier</code>	ASCII-Darstellung in der grafischen Benutzeroberfläche

 Auszuführen in der grafische Benutzeroberfläche

 Auszuführen im Command Line Interface

Einleitung

Das Gerät ist für die Praxis in der rauen Industrieumgebung entwickelt. Dementsprechend einfach ist die Installation. Mit wenigen Einstellungen können Sie dank der gewählten Voreinstellungen das Gerät sofort in Betrieb nehmen.

1 Benutzeroberflächen

Das Gerät bietet Ihnen die Möglichkeit, die Einstellungen des Gerätes über folgende Benutzeroberflächen festzulegen.

Benutzeroberfläche	Erreichbar über ...	Voraussetzung
Grafische Benutzeroberfläche (GUI)	Ethernet (In-Band)	Web-Browser
Command Line Interface (CLI)	Ethernet (In-Band) V.24 (Out-of-Band)	Terminalemulations-Software
System-Monitor	V.24 (Out-of-Band)	Terminalemulations-Software

Tab. 1: Benutzeroberflächen für Zugriff auf das Management des Gerätes

1.1 Grafische Benutzeroberfläche

■ Systemanforderungen

Um die grafische Benutzeroberfläche zu öffnen, benötigen Sie die Desktop-Version eines Web-Browsers mit HTML5- und JavaScript-Unterstützung.

Anmerkung: Software von Drittanbietern wie Web-Browser validieren Zertifikate anhand von Kriterien wie Verfallsdatum und aktuellen kryptografischen Parameter-Empfehlungen. Alte Zertifikate können Fehler verursachen, zum Beispiel wenn sie verfallen oder sich kryptographische Empfehlungen ändern. Laden Sie Ihr eigenes, aktuelles Zertifikat hoch oder erzeugen Sie das Zertifikat mit der neuesten Firmware neu, um Validierungskonflikte mit Software von Drittanbietern zu beheben.

■ Grafische Benutzeroberfläche starten

Voraussetzung für das Starten der grafischen Benutzeroberfläche ist, dass die IP-Parameter im Gerät konfiguriert sind. [Siehe „IP-Parameter festlegen“ auf Seite 29.](#)

- Starten Sie Ihren Web-Browser.
- Schreiben Sie die IP-Adresse des Gerätes in das Adressfeld des Web-Browsers.
Verwenden Sie die folgende Form: `https://xxx.xxx.xxx.xxx`
Der Web-Browser stellt die Verbindung zum Gerät her und zeigt die Login-Seite.
- Wenn Sie die Sprache der grafischen Benutzeroberfläche ändern möchten, klicken Sie auf den entsprechenden Link oben rechts auf der Login-Seite.
- Fügen Sie den Benutzernamen ein.
- Fügen Sie das Passwort ein.
- Klicken Sie die Schaltfläche *Login*.
Der Web-Browser zeigt die grafische Benutzeroberfläche.

1.2 Command Line Interface

Das Command Line Interface bietet Ihnen die Möglichkeit, die Funktionen des Gerätes über eine lokale oder eine Fernverbindung zu bedienen.

IT-Spezialisten finden im Command Line Interface die gewohnte Umgebung zum Konfigurieren von IT-Geräten. Als erfahrener Benutzer oder Administrator verfügen Sie über Wissen zu den Grundlagen und den Einsatz von Hirschmann-Geräten.

1.2.1 Datenverbindung vorbereiten

Informationen zur Montage und Inbetriebnahme Ihres Gerätes finden Sie im Anwender-Handbuch „Installation“.

- Verbinden Sie das Gerät mit dem Datennetz. Voraussetzung für die erfolgreiche Datenverbindung ist die korrekte Einstellung der Netzparameter.

Einen Zugang zur Benutzeroberfläche des Command Line Interface erhalten Sie zum Beispiel mit Hilfe des Freeware-Programms *PuTTY*.

Dieses Programm finden Sie auf der Produkt-CD.

- Installieren Sie auf Ihrem Rechner das Programm *PuTTY*.

1.2.2 CLI-Zugang über Telnet

■ Telnet-Verbindung über Windows

Anmerkung: Telnet ist ausschließlich bei Windows-Versionen vor Windows Vista standardmäßig installiert.

- Starten Sie auf Ihrem Rechner das Programm *Eingabeaufforderung*.
- Fügen Sie das Kommando `telnet <IP_address>` ein.

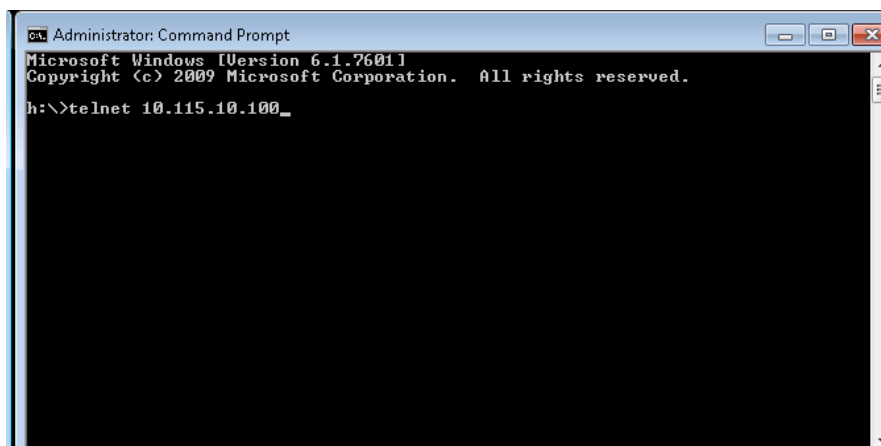


Abb. 1: Eingabeaufforderung: Telnet-Verbindung zum Gerät herstellen

■ Telnet-Verbindung über PuTTY

- Starten Sie auf Ihrem Rechner das Programm *PuTTY*.

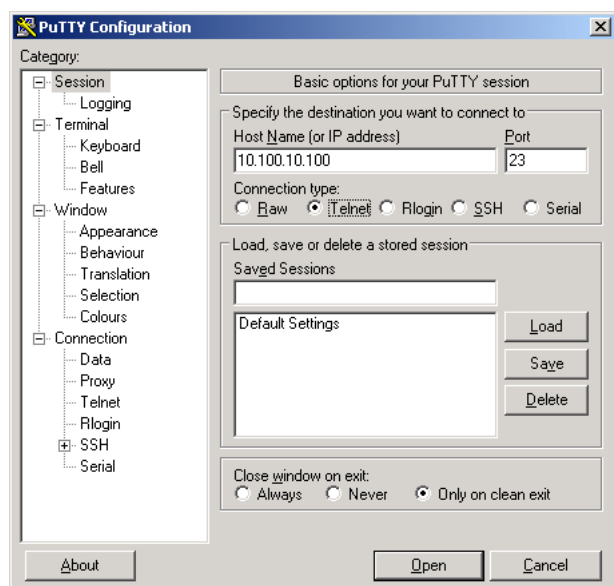


Abb. 2: PuTTY-Eingabemaske

- In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Gerätes ein. Die IP-Adresse (a.b.c.d) besteht aus 4 Dezimalzahlen im Wert von 0 bis 255. Die 4 Dezimalzahlen sind durch einen Punkt getrennt.
- Um den Verbindungstyp auszuwählen, wählen Sie unter *Connection type* das Optionsfeld *Telnet*.
- Klicken Sie die Schaltfläche *Open*, um die Datenverbindung zu Ihrem Gerät aufzubauen.

Das CLI meldet sich auf dem Bildschirm mit einem Fenster für die Eingabe des Benutzernamens. Das Gerät bietet bis zu 2 Benutzern gleichzeitig die Möglichkeit, auf das Command Line Interface zuzugreifen.

```
User: admin
Password:*****
```

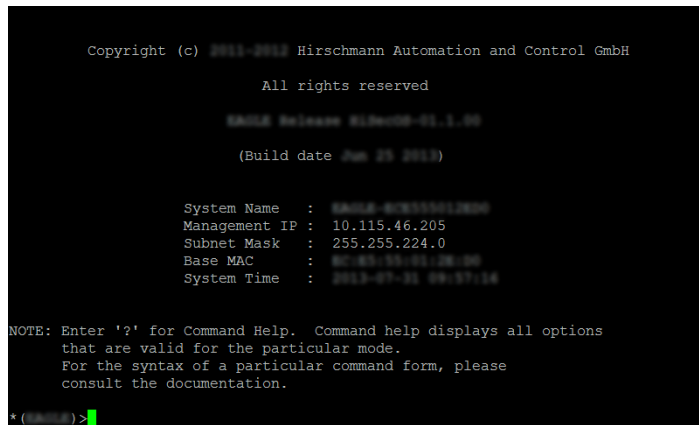
Abb. 3: Login-Bildschirm im CLI

Anmerkung: Ändern Sie das Passwort gleich bei der ersten Inbetriebnahme.

- Fügen Sie den Benutzernamen ein. Der voreingestellte Benutzername ist `admin`. Drücken Sie die <Enter>-Taste.
- Fügen Sie das Passwort ein. Das voreingestellte Passwort ist `private`. Drücken Sie die <Enter>-Taste. Das Gerät bietet Ihnen die Möglichkeit, den Benutzernamen und das Passwort später im Command Line Interface zu ändern. Beachten Sie die Schreibweise in Groß-/Kleinbuchstaben.

Das Gerät zeigt den Start-Bildschirm des CLI mit Eingabeprompt:

(EES) >



```
Copyright (c) 2011-2017 Hirschmann Automation and Control GmbH
All rights reserved

HiOS Release 7.0.11.17
(Build date Jun 29 2017)

System Name : EES-825101200
Management IP : 10.115.46.205
Subnet Mask : 255.255.224.0
Base MAC : 8C:8E:8C:8E:8C:8E
System Time : 2017-07-21 09:57:14

NOTE: Enter '?' for Command Help. Command help displays all options
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.

*(EES)>
```

Abb. 4: Start-Bildschirm des CLI

1.2.3 CLI über SSH (Secure Shell)

- Starten Sie auf Ihrem Rechner das Programm *PuTTY*.

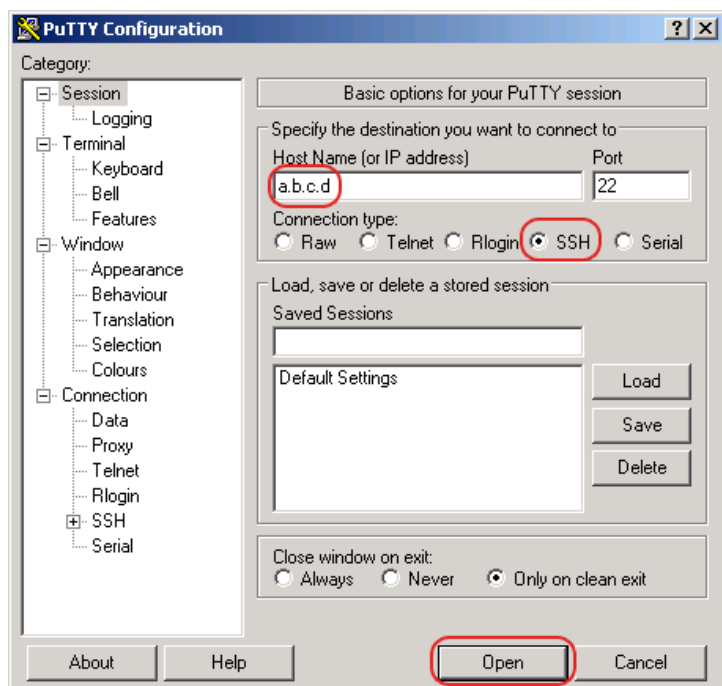


Abb. 5: *PuTTY*-Eingabemaske

- In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Gerätes ein. Die IP-Adresse (a.b.c.d) besteht aus 4 Dezimalzahlen im Wert von 0 bis 255. Die 4 Dezimalzahlen sind durch einen Punkt getrennt.
- Um den Verbindungstyp festzulegen, wählen Sie unter *Connection type* das Optionsfeld *SSH*.
- Nach Auswahl und Einstellung der notwendigen Parameter bietet das Gerät Ihnen die Möglichkeit, die Datenverbindung über SSH herzustellen. Klicken Sie die Schaltfläche *Open*, um die Datenverbindung zu Ihrem Gerät aufzubauen. Abhängig vom Gerät und vom Zeitpunkt des Konfigurierens von SSH dauert der Verbindungsaufbau bis zu eine Minute.

Bei der 1. Anmeldung an Ihrem Gerät zeigt das Programm *PuTTY* gegen Ende des Verbindungsaufbaus eine Sicherheitswarnmeldung und bietet Ihnen die Möglichkeit, den Fingerabdruck des Schlüssels zu prüfen.



Abb. 6: Sicherheitsabfrage für den Fingerabdruck

- Prüfen Sie den Fingerabdruck. Das hilft Ihnen dabei, sich vor unliebsamen Gästen zu schützen.
- Stimmt der Fingerabdruck mit dem des Geräteschlüssels überein, klicken Sie die Schaltfläche **Yes**.

Das Gerät bietet Ihnen die Möglichkeit, die Fingerabdrücke der Geräteschlüssel mit dem CLI-Kommando `show ssh` oder in der grafischen Benutzeroberfläche im Dialog *Gerätesicherheit* > Management-Zugriff > *Server*, Registerkarte *SSH* auszulesen.

Anmerkung: Erfahrenen Netzadministratoren bietet die OpenSSH-Suite eine weitere Möglichkeit, mittels SSH auf Ihr Gerät zuzugreifen. Zum Einrichten der Datenverbindung fügen Sie das folgende Kommando ein:

```
ssh admin@10.149.112.53
```

admin ist der Benutzername.

10.149.112.53 ist die IP-Adresse Ihres Gerätes.

Das CLI meldet sich auf dem Bildschirm mit einem Fenster für die Eingabe des Benutzernamens. Das Gerät bietet bis zu 2 Benutzern gleichzeitig die Möglichkeit, auf das Command Line Interface zuzugreifen.

```
login as: adminadmin@a.b.c.d's password:
```

a.b.c.d ist die IP-Adresse Ihres Gerätes.

- Fügen Sie den Benutzernamen ein. Der voreingestellte Benutzername ist `admin`. Drücken Sie die <Enter>-Taste.
- Fügen Sie das Passwort ein. Das voreingestellte Passwort ist `private`. Drücken Sie die <Enter>-Taste. Das Gerät bietet Ihnen die Möglichkeit, den Benutzernamen und das Passwort später im Command Line Interface zu ändern. Beachten Sie die Schreibweise in Groß-/Kleinbuchstaben.

Das Gerät zeigt den Start-Bildschirm des CLI an.

Anmerkung: Dieses Gerät ist ein sicherheitsrelevantes Produkt. Ändern Sie das Passwort gleich bei der ersten Inbetriebnahme.

```
login as: admin
admin@10.115.46.205's password:

Copyright (c) 2011-2012 Hirschmann Automation and Control GmbH
All rights reserved

HIOS-2E Release 7.0 (2012-02-13)
(Build date Jun 25 2013)

System Name      : HIOS-2E-1000-0000
Management IP    : 10.115.46.205
Subnet Mask      : 255.255.224.0
Base MAC         : 90:80:70:00:00:00
System Time      : 2013-07-31 10:23:47

NOTE: Enter '?' for Command Help.  Command help displays all options
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.

* (HIOS-2E) >
```

Abb. 7: Start-Bildschirm des CLI

1.2.4 CLI über den V.24-Port

Die V.24-Schnittstelle ist eine serielle Schnittstelle zum lokalen Anschließen einer externen Netz-Management-Station (VT100-Terminal oder PC mit Terminal-Emulation). Die Schnittstelle bietet Ihnen die Möglichkeit, eine Datenverbindung zum Command Line Interface (CLI) und zum Systemmonitor herzustellen.

Einstellungen VT 100 Terminal	
Speed	9600 bit/s
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

- Verbinden Sie das Gerät über V.24 mit einem Terminal. Alternativ verbinden Sie das Gerät mit einem COM-Port Ihres PCs mit Terminal-Emulation nach VT100 und drücken Sie eine beliebige Taste.
- Alternativ erstellen Sie die serielle Datenverbindung zum Gerät über V.24 mit dem Programm *PuTTY*. Drücken Sie die <Enter>-Taste.

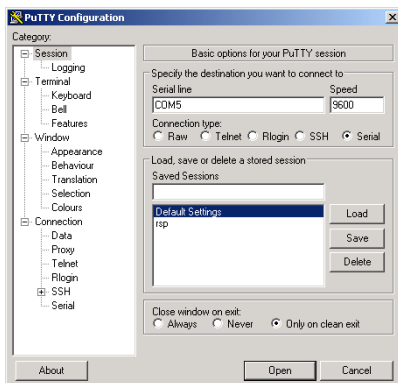


Abb. 8: Serielle Datenverbindung über V.24 mit dem Programm *PuTTY*

Nach erfolgreichem Aufbau der Datenverbindung zeigt das Gerät ein Fenster für die Eingabe des Benutzernamens.

Anmerkung: Sie haben die Möglichkeit, die V.24-Schnittstelle als Terminal-/CLI-Schnittstelle zu konfigurieren.

Drücken Sie mehrfach eine beliebige Taste Ihrer Terminal-Tastatur, bis Ihnen der Login-Bildschirm den CLI-Modus signalisiert.

- Fügen Sie den Benutzernamen ein. Der voreingestellte Benutzername ist `admin`. Drücken Sie die <Enter>-Taste.
- Fügen Sie das Passwort ein. Das voreingestellte Passwort ist `private`. Drücken Sie die <Enter>-Taste. Das Gerät bietet Ihnen die Möglichkeit, den Benutzernamen und das Passwort später im Command Line Interface zu ändern. Beachten Sie die Schreibweise in Groß-/Kleinbuchstaben.

```
Copyright (c) 2013-2018 Hirschmann Automation and Control GmbH
All rights reserved
HiOS Release 7.0.0-24-02.1-02-002
(Build date 2017-04-28 12:36)

System Name   : HSI-24-02-002-002
Management IP : 10.0.1.32
Subnet Mask   : 255.255.255.0
Base MAC      : 98-9D-70-19-00-00
System Time   : 2017-07-20 10:19:32

User:admin
Password:*****
```

Abb. 9: Einloggen in das Command Line Interface Programm

```
NOTE: Enter '?' for Command Help. Command help displays all opt
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.

! ( ) >
```

Abb. 10: CLI-Bildschirm nach dem Einloggen

1.3 System-Monitor

Der System-Monitor bietet Ihnen die Möglichkeit, vor dem Starten des Betriebssystems grundlegende Betriebsparameter einzustellen.

1.3.1 Funktionsumfang

Im System-Monitor erledigen Sie beispielsweise folgende Aufgaben:

- ▶ Betriebssystem aktualisieren
- ▶ Betriebssystem starten
- ▶ Konfigurationsprofile löschen, Gerät auf Lieferzustand zurücksetzen
- ▶ Bootcode-Information prüfen

1.3.2 System-Monitor starten

Voraussetzung:

- ▶ Terminal-Kabel für die Verbindung vom Gerät zu Ihren PC (als optionales Zubehör erhältlich).
- ▶ PC mit einer VT100-Terminalemulation (zum Beispiel Programm *PuTTY*) oder serielles Terminal

Führen Sie die folgenden Schritte aus:

- Verbinden Sie mit Hilfe des Terminal-Kabels den V.24-Anschluss des Gerätes mit dem COM-Port des PCs.
- Starten Sie die VT100-Terminalemulation auf dem PC.
- Legen Sie folgende Übertragungsparameter fest:

Einstellungen VT 100 Terminal	
Speed	9600 bit/s
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

- Stellen Sie eine Verbindung zu dem Gerät her.
- Schalten Sie das Gerät ein. Wenn das Gerät bereits eingeschaltet ist, führen Sie einen Neustart durch.

Der Bildschirm zeigt nach dem Neustart die folgende Meldung:

```
Press <1> to enter System Monitor 1.
```

- Drücken Sie innerhalb von 3 Sekunden die Taste <1>.
Das Gerät startet den System-Monitor. Der Bildschirm zeigt die folgende Ansicht:

```
System Monitor 1
(Selected OS: ...-7.0 (2017-11-20 19:17))

1 Manage operating system
2 Update operating system
3 Start selected operating system
4 Manage configurations
5 Show boot code information
q End (reset and reboot)

sysMon1>
```

Abb. 11: Bildschirmsicht System Monitor 1

- Wählen Sie durch Eingabe der Zahl den gewünschten Menüpunkt aus.
- Um ein Untermenü zu verlassen und zum Hauptmenü des System Monitor 1 zurückzukehren, drücken Sie die <ESC>-Taste.

2 IP-Parameter festlegen

Bei der Erstinstallation des Gerätes benötigen Sie die IP-Parameter.

Das Gerät bietet bei der Erstinstallation die folgenden Möglichkeiten zur Eingabe der IP-Parameter:

- ▶ Eingabe über das Command Line Interface.
Wählen Sie diese „Out-of-Band“-Methode, wenn Sie Ihr Gerät außerhalb seiner Betriebsumgebung vorkonfigurieren oder Sie den Netzzugang („In-Band“) zu dem Gerät wiederherstellen.
- ▶ Eingabe über das Protokoll HiDiscovery.
Wählen Sie diese „In-Band“-Methode für ein bereits installiertes Netzgerät, oder wenn eine weitere Ethernet-Verbindung zwischen Ihrem PC und dem Gerät besteht.
- ▶ Verwendung von BOOTP.
Wählen Sie diese „In-Band“-Methode, um die Konfiguration des installierten Gerätes über BOOTP vorzunehmen. Hierzu benötigen Sie einen BOOTP-Server. Der BOOTP-Server weist dem Gerät anhand seiner MAC-Adresse die Konfigurationsdaten zu. Der DHCP-Modus ist der Standardmodus für den Bezug der Konfigurationsdaten.
- ▶ Konfiguration über DHCP.
Wählen Sie diese „In-Band“-Methode, um die Konfiguration des installierten Gerätes über DHCP vorzunehmen. Hierzu benötigen Sie einen DHCP-Server. Der DHCP-Server weist dem Gerät anhand seiner MAC-Adresse oder seines Systemnamens die Konfigurationsdaten zu.
- ▶ Konfiguration über die grafische Benutzeroberfläche.
Verfügt das Gerät bereits über eine IP-Adresse und ist über das Netz erreichbar, dann bietet Ihnen die grafische Benutzeroberfläche eine weitere Möglichkeit, die IP-Parameter zu konfigurieren.

2.1 Grundlagen IP Parameter

2.1.1 IP-Adresse (Version 4)

Die IP-Adressen bestehen aus 4 Bytes. Diese 4 Bytes werden durch einen Punkt getrennt, dezimal dargestellt.

Seit 1992 sind im RFC 1340 fünf Klassen von IP-Adressen definiert.

Klasse	Netzadresse	Hostadresse	Adressbereich
A	1 Byte	3 Bytes	0.0.0.0 bis 127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 bis 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 bis 223.255.255.255
D			224.0.0.0 bis 239.255.255.255
E			240.0.0.0 bis 255.255.255.255

Tab. 2: IP-Adressklassen

Der erste Byte einer IP-Adresse ist die Netzadresse. Der Regulierungsausschuss für die weltweite Zuweisung von Netzadressen ist IANA („Internet Assigned Numbers Authority“). Falls Sie einen IP-Adressenblock benötigen, wenden Sie sich an Ihren Internet Service Provider (ISP). Ihr ISP wendet sich an seine lokale übergeordnete Organisation, um einen IP-Adressenblock zu reservieren:

- ▶ APNIC (Asia Pacific Network Information Center)
Asien/Pazifik
- ▶ ARIN (American Registry for Internet Numbers)
Amerika und Subsahara-Afrika
- ▶ LACNIC (Regional Latin-American and Caribbean IP Address Registry)
Lateinamerika und weitere Karibik-Inseln
- ▶ RIPE NCC (Réseaux IP Européens)
Europa und umliegende Regionen

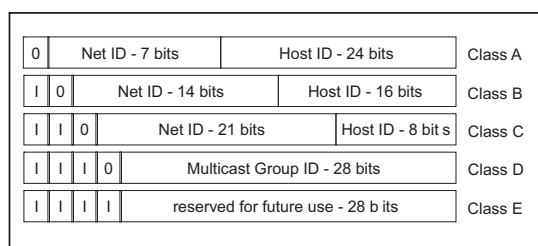


Abb. 12: Bitdarstellung der IP-Adresse

Ist das erste Oktett einer IP-Adresse eine Null, d. h. kleiner als 128, gehört sie der Klasse A an.

Ist das erste Bit einer IP-Adresse eine Eins und das zweite Bit eine Null, d. h. das erste Oktett liegt im Bereich von 128 bis 191, dann gehört die IP-Adresse der Klasse B an.

Sind die ersten beiden Bits einer IP-Adresse eine Eins, d. h. das erste Oktett ist größer als 191, dann handelt es sich um eine IP-Adresse der Klasse C.

Die Vergabe der Hostadresse (host ID) obliegt dem Netzbetreiber. Der Netzbetreiber allein ist für die Einmaligkeit der IP-Adressen, die er vergibt, verantwortlich.

2.1.2 Netzmaske

Router und Gateways unterteilen große Netze in Subnetze. Die Netzmaske ordnet die IP-Adressen der einzelnen Geräte einem bestimmten Subnetz zu.

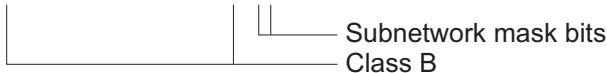
Die Einteilung in Subnetze erfolgt über die Netzmaske analog zu der Einteilung der Netzadresse (net id) in die Klassen A bis C.

Setzen Sie die Bits der Hostadresse (host id), die die Maske darstellen, auf Eins. Setzen Sie die restlichen Bits der Hostadresse auf Null (vgl. folgende Beispiele).

Beispiel für eine Subnetzmaske:

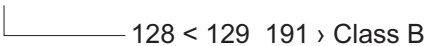
Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000




Beispiel für IP-Adressen mit Subnetzzuordnung gemäß der Netzmaske:

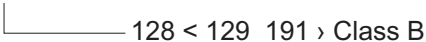
Decimal notation
129.218.65.17




Binary notation
10000001.11011010.01000001.00010001



Decimal notation
129.218.129.17



Binary notation
10000001.11011010.10000001.00010001



■ Beispiel für die Anwendung der Netzmaske

In einem großen Netz ist es möglich, dass Gateways oder Router den Management-Agenten von ihrer Netz-Management-Station trennen. Wie erfolgt in einem solchen Fall die Adressierung?

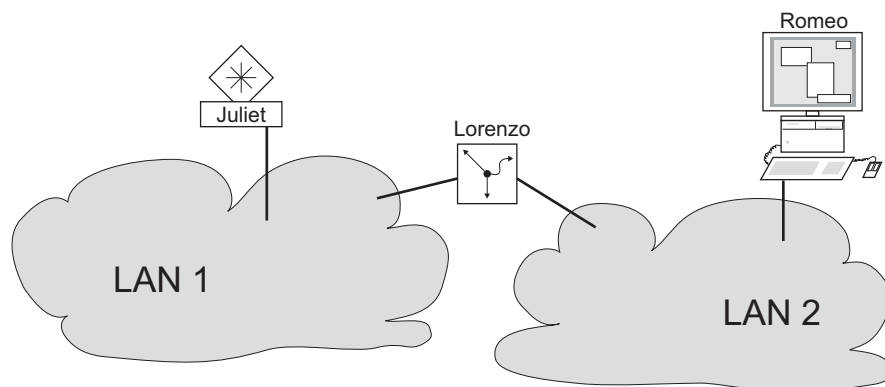


Abb. 13: Management-Agent durch Router von der Netz-Management-Station getrennt

Die Netz-Management-Station „Romeo“ möchte Daten an den Management-Agenten „Julia“ schicken. Romeo kennt die IP-Adresse von Julia und weiß, dass der Router „Lorenzo“ den Weg zu Julia kennt.

Also packt Romeo seine Botschaft in einen Umschlag und schreibt als Zieladresse die IP-Adresse von Julia und als Quelladresse seine eigene IP-Adresse darauf.

Diesen Umschlag steckt Romeo in einen weiteren Umschlag mit der MAC-Adresse von Lorenzo als Zieladresse und seiner eigenen MAC-Adresse als Quelladresse. Dieser Vorgang ist vergleichbar mit dem Übergang von der Schicht 3 zur Schicht 2 des ISO/OSI-Basis-Referenzmodells.

Nun steckt Romeo das gesamte Datenpaket in den Briefkasten, vergleichbar mit dem Übergang von der Schicht 2 zur Schicht 1, das heißt dem Senden des Datenpaketes in das Ethernet.

Lorenzo erhält den Brief, entfernt den äußeren Umschlag und erkennt auf dem inneren Umschlag, dass der Brief für Julia bestimmt ist. Er steckt den inneren Umschlag in einen neuen äußeren Umschlag, schaut in seiner Adressliste, der ARP-Tabelle, nach der MAC-Adresse von Julia und schreibt diese auf den äußeren Umschlag als Zieladresse und seine eigene MAC-Adresse als Quelladresse. Das gesamte Datenpaket steckt er anschließend in den Briefkasten.

Julia empfängt den Brief, entfernt den äußeren Umschlag. Übrig bleibt der innere Umschlag mit Romeos IP-Adresse. Das Öffnen des inneren Umschlages und Lesen der Botschaft entspricht einer Übergabe an höhere Protokollschichten des ISO/OSI-Schichtenmodells.

Julia möchte eine Antwort an Romeo zurücksenden. Sie steckt ihre Antwort in einen Umschlag mit der IP-Adresse von Romeo als Zieladresse und ihrer eigenen IP-Adresse als Quelladresse. Doch wohin soll Sie die Antwort schicken? Die MAC-Adresse von Romeo hat sie ja nicht erhalten. Die MAC-Adresse von Romeo blieb beim Wechseln des äußeren Umschlages bei Lorenzo zurück.

Julia findet in der MIB unter der Variablen `hmNetGatewayIPAddr` Lorenzo als Vermittler zu Romeo. So steckt sie den Umschlag mit den IP-Adressen in einen weiteren Umschlag mit der MAC-Zieladresse von Lorenzo.

Nun findet der Brief den gleichen Weg über Lorenzo zu Romeo, so wie der Brief von Romeo zu Julia fand.

2.1.3 Classless Inter-Domain Routing

Die Klasse C mit maximal 254 Adressen war zu klein, und die Klasse B mit maximal 65534 Adressen war für die meisten Anwender zu groß. Hieraus resultierte eine nicht effektive Nutzung der zur Verfügung stehenden Klasse-B-Adressen.

Die Klasse D enthält reservierte Multicast-Adressen. Die Klasse E ist für experimentelle Zwecke vorgesehen. Ein Gateway, das nicht an diesen Experimenten teilnimmt, ignoriert experimentelle Datagramme mit diesen Zieladressen.

Seit 1993 verwendet RFC 1519 Classless Inter-Domain Routing (CIDR) zur Lösung dieses Problems. Das CIDR überwindet diese Klassenschranken und unterstützt klassenlose IP-Adressbereiche.

Mit CIDR legen Sie die Anzahl der Bits fest, die den IP-Adressbereich kennzeichnen. Hierzu stellen Sie den IP-Adressbereich in binärer Form dar und zählen die Maskenbits zur Bezeichnung der Netzmaske. Die Maskenbits entsprechen der Anzahl der Bits, die in einem bestimmten IP-Bereich für das Subnetz verwendet werden.

Beispiel:

IP address, decimal	Network mask, decimal	IP address, binary
149.218.112.1	255.255.255.128	10010101 11011010 01110000 00000001
149.218.112.127		10010101 11011010 01110000 01111111
		----- 25 mask bits -----
CIDR notation: 149.218.112.0/25		
	----- Mask bits -----	

Die Zusammenfassung mehrerer Adressbereiche der Klasse C wird als „Supernetting“ bezeichnet. Mit Supernetting lassen sich Adressbereiche der Klasse B sehr fein untergliedern.

2.2 IP-Parameter mit dem CLI festlegen

Es gibt verschiedene Möglichkeiten, die Systemkonfiguration einzugeben: entweder über BOOTP/DHCP oder über das HiDiscovery-Protokoll. Sie können die Konfiguration auch über die V.24-Schnittstelle mit Hilfe des CLI vornehmen.

Das Gerät bietet Ihnen die Möglichkeit, die IP-Parameter über das HiDiscovery-Protokoll oder über die V.24-Schnittstelle mit Hilfe des CLI festzulegen.

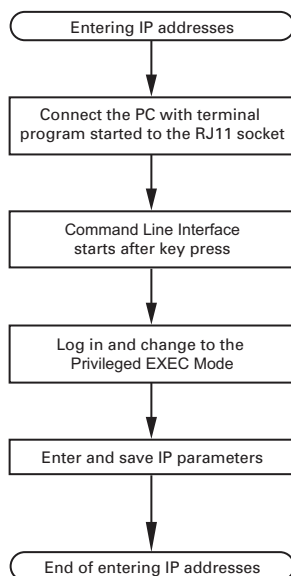


Abb. 14: Ablaufdiagramm Eintragen der IP-Adressen

Anmerkung: Sollten Sie in der Nähe des Installationsortes kein Terminal oder keinen PC mit Terminalemulation zur Verfügung haben, können Sie das Gerät an ihrem Arbeitsplatz konfigurieren und danach an seinen endgültigen Installationsort bringen.

- Stellen Sie eine Verbindung zu dem Gerät her.
Der Startbildschirm erscheint.

```
NOTE: Enter '?' for Command Help. Command help displays all opt
that are valid for the particular mode.
For the syntax of a particular command form, please
consult the documentation.

! (####) >
```

- Schalten Sie DHCP aus.
- Fügen Sie die IP-Parameter ein.
 - ▶ Lokale IP-Adresse
In der Voreinstellung ist die lokale IP-Adresse 0.0.0.0.
 - ▶ Netzmaske
Wenn Sie Ihr Netz in Subnetze aufgeteilt haben und diese mit einer Netzmaske identifizieren, fügen Sie an dieser Stelle die Netzmaske ein. In der Voreinstellung ist die Netzmaske 0.0.0.0.
 - ▶ IP-Adresse des Gateways.
Diese Eingabe ist ausschließlich dann notwendig, wenn sich das Gerät und die Netz-Management-Station bzw. der TFTP-Server in unterschiedlichen Subnetzen befinden ([siehe auf Seite 32 „Beispiel für die Anwendung der Netzmaske“](#)).
Legen Sie die IP-Adresse des Gateways fest, welches das Subnetz mit dem Gerät vom Pfad zur Netz-Management-Station trennt.
In der Voreinstellung ist die IP-Adresse 0.0.0.0.
- Speichern Sie die festgelegte Konfiguration durch Verwendung von `copy config running-config nvram`.

<pre>enable</pre>	Wechsel in den Privileged-EXEC-Modus.
<pre>network protocol none</pre>	DHCP ausschalten.
<pre>network parms 10.0.1.23 255.255.255.0</pre>	Dem Gerät die IP-Adresse 10.0.1.23 und die Netzmaske 255.255.255.0 zuweisen. Optional können Sie zusätzlich eine Gateway-Adresse zuweisen.
<pre>copy config running-config nvram</pre>	Speichern der aktuellen Einstellungen im „ausgewählten“ Konfigurationsprofil im permanenten Speicher (nvram).

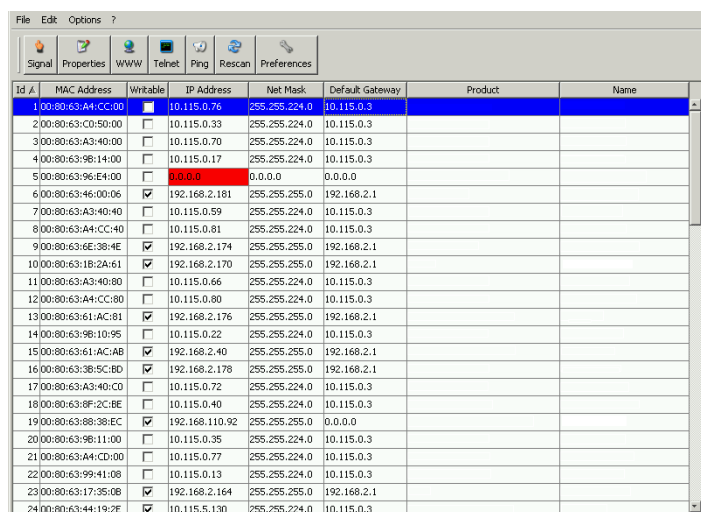
Nach Eingabe der IP-Parameter können Sie das Gerät über die grafische Benutzeroberfläche komfortabel konfigurieren.

2.3 IP-Parameter mit HiDiscovery festlegen

Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät über das Ethernet IP-Parameter zuzuweisen. Die anderen Parameter konfigurieren Sie komfortabel über die grafische Benutzeroberfläche.

Installieren Sie die HiDiscovery-Software auf Ihrem PC. Sie finden die Software auf der Produkt-DVD, die Sie mit dem Gerät erhalten haben.

- Zur Installation starten Sie das Installationsprogramm auf der DVD.
- Starten Sie das Programm .



ID	MAC Address	Writable	IP Address	Net Mask	Default Gateway	Product	Name
1	00:80:63:A4:CC:00	<input checked="" type="checkbox"/>	10.115.0.76	255.255.224.0	10.115.0.3		
2	00:80:63:C0:50:00	<input type="checkbox"/>	10.115.0.33	255.255.224.0	10.115.0.3		
3	00:80:63:A3:40:00	<input type="checkbox"/>	10.115.0.70	255.255.224.0	10.115.0.3		
4	00:80:63:98:14:00	<input type="checkbox"/>	10.115.0.17	255.255.224.0	10.115.0.3		
5	00:80:63:96:E4:00	<input type="checkbox"/>	0.0.0.0	0.0.0.0	0.0.0.0		
6	00:80:63:46:00:06	<input checked="" type="checkbox"/>	192.168.2.181	255.255.255.0	192.168.2.1		
7	00:80:63:A3:40:40	<input type="checkbox"/>	10.115.0.59	255.255.224.0	10.115.0.3		
8	00:80:63:A4:CC:40	<input type="checkbox"/>	10.115.0.81	255.255.224.0	10.115.0.3		
9	00:80:63:6E:38:4E	<input checked="" type="checkbox"/>	192.168.2.174	255.255.255.0	192.168.2.1		
10	00:80:63:18:2A:61	<input checked="" type="checkbox"/>	192.168.2.170	255.255.255.0	192.168.2.1		
11	00:80:63:A3:40:80	<input type="checkbox"/>	10.115.0.66	255.255.224.0	10.115.0.3		
12	00:80:63:A4:CC:80	<input type="checkbox"/>	10.115.0.80	255.255.224.0	10.115.0.3		
13	00:80:63:61:AC:81	<input checked="" type="checkbox"/>	192.168.2.176	255.255.255.0	192.168.2.1		
14	00:80:63:98:10:95	<input type="checkbox"/>	10.115.0.22	255.255.224.0	10.115.0.3		
15	00:80:63:61:AC:AB	<input checked="" type="checkbox"/>	192.168.2.40	255.255.255.0	192.168.2.1		
16	00:80:63:38:5C:BD	<input checked="" type="checkbox"/>	192.168.2.178	255.255.255.0	192.168.2.1		
17	00:80:63:A3:40:C0	<input type="checkbox"/>	10.115.0.72	255.255.224.0	10.115.0.3		
18	00:80:63:8F:2C:BE	<input type="checkbox"/>	10.115.0.40	255.255.224.0	10.115.0.3		
19	00:80:63:88:38:EC	<input checked="" type="checkbox"/>	192.168.110.92	255.255.255.0	0.0.0.0		
20	00:80:63:98:11:00	<input type="checkbox"/>	10.115.0.35	255.255.224.0	10.115.0.3		
21	00:80:63:A4:CD:00	<input type="checkbox"/>	10.115.0.77	255.255.224.0	10.115.0.3		
22	00:80:63:99:41:08	<input type="checkbox"/>	10.115.0.13	255.255.224.0	10.115.0.3		
23	00:80:63:17:35:0B	<input checked="" type="checkbox"/>	192.168.2.164	255.255.255.0	192.168.2.1		
24	00:80:63:44:19:2E	<input checked="" type="checkbox"/>	10.115.5.130	255.255.224.0	10.115.0.3		

Abb. 15: HiDiscovery

Beim Start von HiDiscovery untersucht HiDiscovery automatisch das Netz nach Geräten, die das HiDiscovery-Protokoll unterstützen.

HiDiscovery benutzt das erste gefundene Netz-Interface des PCs. Sollte Ihr Rechner über mehrere Netzwerkkarten verfügen, können Sie das gewünschte in der Werkzeugleiste von HiDiscovery auswählen.

HiDiscovery zeigt eine Zeile für jedes Gerät, das auf eine HiDiscovery-Protokoll-Abfrage reagiert.

HiDiscovery ermöglicht das Identifizieren der angezeigten Geräte.

- Wählen Sie eine Gerätezeile aus.
- Um für das ausgewählte Gerät das Blinken der LEDs einzuschalten, klicken Sie in der Werkzeugleiste die Schaltfläche *Signal*. Um das Blinken auszuschalten, klicken Sie noch einmal die Schaltfläche *Signal*.
- Mit Doppelklick in eine Zeile öffnen Sie ein Fenster, in welchem Sie den Gerätenamen und die IP-Parameter festlegen.

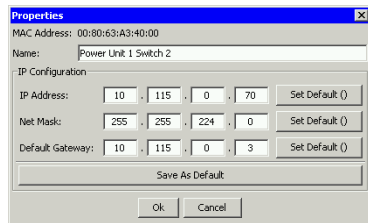


Abb. 16: HiDiscovery – IP-Parameter-Zuweisung

Anmerkung: Schalten Sie aus Sicherheitsgründen im Graphical User Interface die HiDiscovery-Funktion des Gerätes aus, nachdem Sie dem Gerät die IP-Parameter zugewiesen haben.

Anmerkung: Speichern Sie die Einstellungen, sodass die Eingaben nach einem Neustart wieder zur Verfügung stehen.

2.4 IP-Parameter mit grafischer Benutzeroberfläche festlegen

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Netz*.

In diesem Dialog legen Sie zum einen fest, aus welcher Quelle das Gerät seine IP-Parameter nach dem Start erhält. Zum anderen bestimmen Sie das VLAN, in dem das Geräte-Management erreichbar ist, konfigurieren den HiDiscovery-Zugriff und weisen manuelle IP-Parameter zu.

- Legen Sie im Rahmen *Management-Schnittstelle* zunächst fest, woher das Gerät seine IP-Parameter bezieht:
 - ▶ Im Modus erfolgt die Konfiguration durch einen BOOTP- oder DHCP-Server auf Basis der MAC-Adresse des Gerätes.
 - ▶ Im Modus *DHCP* erfolgt die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Gerätes.
 - ▶ Im Modus verwendet das Gerät die Netzparameter aus dem internen Gerätespeicher.

Anmerkung: Wenn Sie den Modus für die IP-Adress-Zuweisung ändern, aktiviert das Gerät sofort den neuen Modus, wenn Sie die Schaltfläche klicken.

- Legen Sie in Spalte *VLAN-ID* das VLAN fest, in welchem das Management des Gerätes über das Netz erreichbar ist.
- Beachten Sie hierbei, dass das Management des Gerätes ausschließlich über Ports erreichbar ist, die Mitglied des betreffenden VLANS sind.

Das Feld *MAC-Adresse* zeigt die MAC-Adresse des Gerätes an, mit der Sie das Gerät über das Netz erreichen.

- Legen Sie im Rahmen *HiDiscovery Protokoll v1/v2* die Einstellungen für den Zugriff auf das Gerät mit der HiDiscovery-Software fest.
- Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät anhand seiner MAC-Adresse eine IP-Adresse zuzuweisen. Aktivieren Sie das HiDiscovery-Protokoll, wenn Sie von Ihrem PC aus mit der HiDiscovery-Software dem Gerät eine IP-Adresse zuweisen wollen.
- Fügen Sie im Rahmen *IP-Parameter* die IP-Adresse, die Netzmaske und das Gateway bei Bedarf ein.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

2.5 IP-Parameter mit BOOTP festlegen

Bei aktivierter -Funktion sendet das Gerät eine Boot-Anforderungsnachricht an den BOOTP-Server. Die Boot-Anforderungsnachricht enthält die in dem Dialog `BOOTP` konfigurierte Client-ID. Der BOOTP-Server gibt die Client-ID in eine Datenbank ein und weist eine IP-Adresse zu. Der Server antwortet mit einer Boot-Antwort-Nachricht. Die Boot-Antwort-Nachricht enthält die zugewiesene IP-Adresse.

2.6 IP-Parameter mit DHCP festlegen

Das DHCP (Dynamic Host Configuration Protocol) ist eine Weiterentwicklung von BOOTP und hat dieses abgelöst. DHCP bietet zusätzlich die Konfiguration eines DHCP-Clients über einen Namen anstatt über die MAC-Adresse an.

Dieser Name heißt bei DHCP nach RFC 2131 „Client Identifier“.

Das Gerät verwendet den in der System-Gruppe der MIB II unter sysName festgelegten Namen als Client Identifier. Den Systemnamen können Sie in der grafischen Benutzeroberfläche (siehe Dialog *Grundeinstellungen* > *System*), im Command Line Interface oder mit SNMP ändern.

Das Gerät übermittelt dem DHCP-Server seinen Systemnamen. Der DHCP-Server verwendet anschließend den Systemnamen für die Zuweisung einer IP-Adresse als Alternative für die MAC-Adresse.

Neben der IP-Adresse überträgt der DHCP-Server

- ▶ die Netzmaske
- ▶ das Standard-Gateway (falls verfügbar)
- ▶ die TFTP-URL der Konfigurationsdatei (falls verfügbar).

Das Gerät wendet die Konfigurationsdaten auf die entsprechenden Parameter an. Wenn der DHCP-Server die IP-Adresse zuweist, speichert das Gerät die Konfigurationsdaten permanent im nichtflüchtigen Speicher.

Optionen	Bedeutung
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Tab. 3: DHCP-Optionen, die das Gerät anfordert

Der Vorteil beim Einsatz von DHCP gegenüber BOOTP ist, dass der DHCP-Server die Gültigkeit der Konfigurationsparameter („Lease“) auf eine bestimmte Zeitspanne einschränken kann (sogenannte dynamische Adress-Vergabe). Rechtzeitig vor Ablauf dieser Zeitspanne („Lease Duration“), kann der DHCP-Client versuchen, dieses Lease zu erneuern. Alternativ kann er ein neues Lease aushandeln. Der DHCP-Server weist dann eine beliebige freie Adresse zu.

Um dies zu umgehen, bieten DHCP-Server die explizite Konfigurationsmöglichkeit, einem bestimmten Client anhand einer eindeutigen Hardware-ID dieselbe IP-Adresse zuzuweisen (sogenannte statische Adressvergabe).

In der Voreinstellung ist DHCP aktiviert. Solange DHCP aktiviert ist, versucht das Gerät, eine IP-Adresse zu bekommen. Findet das Gerät nach einem Neustart keinen DHCP-Server, hat es keine IP-Adresse. Der Dialog *Grundeinstellungen* > *Netz* bietet Ihnen die Möglichkeit, DHCP zu aktivieren oder zu deaktivieren.

Anmerkung: Achten Sie bei der Anwendung des Netzmanagements Industrial HiVision darauf, dass DHCP jedem Gerät die original IP-Adresse zuweist.

Der Anhang enthält eine Beispielkonfiguration des BOOTP/DHCP-Servers.

Beispiel für eine DHCP-Konfigurationsdatei:

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

Zeilen, die mit dem Zeichen # beginnen, enthalten Kommentare.

Die Zeilen vor den einzeln aufgeführten Geräten bezeichnen Einstellungen, die auf das folgende Gerät angewendet werden.

Die Zeile für die feste Adresse weist dem Gerät eine feste IP-Adresse zu.

Weitere Informationen entnehmen Sie Ihrem DHCP-Server-Handbuch.

2.7 Erkennung von Adresskonflikten verwalten

Sie weisen dem Gerät eine IP-Adresse mithilfe mehrerer verschiedener Methoden zu. Diese Funktion unterstützt das Gerät bei der Erkennung von IP-Adresskonflikten in einem Netz nach dem Starten sowie die Durchführung von regelmäßigen Prüfungen während des Betriebes. Diese Funktion wird im RFC 5227 beschrieben.

Ist die Funktion aktiviert, sendet das Gerät einen SNMP-Trap, der Sie darüber informiert, dass es einen IP-Adresskonflikt erkannt hat.

Die folgende Liste enthält die Voreinstellungen für diese Funktion:

- *Funktion*:
- *Erkennungs-Modus*:
- *Periodische ARP-Überprüfung senden*: markiert
- *Erkennungs-Verzögerung [ms]*: 200
- *Rückfallverzögerung [s]*:
- *Address-Protections*:
- *Protektions-Intervall [ms]*:
- *Trap senden*: markiert

2.7.1 Aktive und passive Erkennung

Durch aktives Prüfen des Netzes wird verhindert, dass das Gerät mit einer doppelten IP-Adresse eine Verbindung mit dem Netz herstellt. Nachdem das Gerät mit dem Netz verbunden oder die IP-Adresse konfiguriert wurde, prüft das Gerät sofort, ob seine IP-Adresse innerhalb des Netzes bereits vorhanden ist. Um zu prüfen, ob Adresskonflikte im Netz vorhanden sind, sendet das Gerät 4 ARP-Probes mit einer Erkennungsverzögerung von 200 ms in das Netz. Ist die IP-Adresse vorhanden, stellt das Gerät (wenn möglich) wieder die vorherige Konfiguration her und führt nach Ablauf der konfigurierten Verzögerungszeit für die Freigabe eine weitere Prüfung durch.

Wenn Sie die aktive Erkennung deaktivieren, sendet das Gerät 2 unaufgeforderte ARP-Ankündigungen mit einem Intervall von 2 s. Ist bei der Verwendung von ARP-Ankündigungen die passive Erkennung aktiviert, fragt das Gerät das Netz ab, um zu ermitteln, ob ein Adresskonflikt vorliegt. Nach dem Lösen eines Adresskonfliktes oder nach dem Ablauf der Verzögerungszeit für die Freigabe stellt das Gerät erneut eine Verbindung mit dem Netz her. Nach 10 erkannten Konflikten setzt das Gerät das Verzögerungsintervall für die Freigabe auf 60 s, wenn das konfigurierte Verzögerungsintervall weniger als 60 s beträgt.

Nachdem das Gerät die aktive Erkennung durchgeführt hat oder Sie die Funktion für die aktive Erkennung deaktiviert haben, hört das Gerät mit aktivierter passiver Erkennung das Netzwerk auf Geräte ab, die dieselbe IP-Adresse verwenden. Erkennt das Gerät eine doppelte IP-Adresse, verteidigt es anfangs seine Adresse, indem es den ACD-Mechanismus im Modus für die passive Erkennung anwendet und unaufgeforderte ARP-Ankündigungen übermittelt. Die Anzahl der Schutzmaßnahmen, die das Gerät sendet, sowie das Schutzintervall sind konfigurierbar. Zur Lösung von Konflikten trennt die Netzschchnittstelle des lokalen Gerätes die Verbindung mit dem Netz, sofern weiterhin eine Verbindung des entfernten Gerätes mit dem Netz besteht.

Weist der DHCP-Server dem Gerät eine IP-Adresse zu, gibt das Gerät eine DHCP-Denial-Nachricht zurück, wenn ein Adresskonflikt auftritt.

Das Gerät verwendet die ARP-Probe-Methode. Diese hat die folgenden Vorteile:

- ▶ ARP-Cache-Speicher auf anderen Geräten bleiben unverändert.
- ▶ Die Methode bleibt über mehrere ARP-Probe-Übertragungen stabil.

3 Zugriff auf das Gerät

3.1 Authentifizierungs-Listen

Eine Authentifizierungs-Liste enthält die Richtlinien, die das Gerät für die Authentifizierung anwendet, wenn ein Benutzer über eine bestimmte Verbindung auf das Gerät zugreift.

Voraussetzung für den Zugriff eines Benutzers auf das Management des Gerätes ist, dass der Authentifizierungs-Liste derjenigen Anwendung, über die der Zugriff erfolgt, mindestens eine Richtlinie zugeordnet ist.

3.1.1 Anwendungen

Das Gerät stellt für jede Art von Verbindung, über die jemand auf das Gerät zugreift, eine Anwendung zur Verfügung:

- ▶ Zugriff mit dem CLI über eine serielle Verbindung: `Console (V.24)`
- ▶ Zugriff mit dem CLI über SSH: `SSH`
- ▶ Zugriff mit dem CLI über Telnet: `Telnet`
- ▶ Konfiguration über die grafische Benutzeroberfläche: `WebInterface`

Außerdem stellt das Gerät eine Anwendung zur Verfügung, um den Zugriff von angeschlossenen Endgeräten auf das Netz mit Port-basierter Zugriffskontrolle zu kontrollieren: `8021x`

3.1.2 Richtlinien

Das Gerät gewährt Benutzern Zugriff auf das Management, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Benutzer mit folgenden Richtlinien:

- ▶ Benutzerverwaltung des Geräts
- ▶ RADIUS

Mit der portbasierten Zugriffskontrolle gemäß IEEE 802.1X gewährt das Gerät angeschlossenen Endgeräten ausschließlich dann Zugriff auf das Netz, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Endgeräte mit folgenden Richtlinien:

- ▶ RADIUS
- ▶ IAS (Integrated Authentication Server)

Das Gerät bietet Ihnen die Möglichkeit einer Fall-Back-Lösung. Legen Sie hierfür in der Authentifizierungs-Liste mehr als eine Richtlinie fest. Wenn die Authentifizierung mit der aktuellen Richtlinie erfolglos ist, wendet das Gerät die nächste festgelegte Richtlinie an.

3.1.3 Authentifizierungs-Listen verwalten

Die Authentifizierungs-Listen verwalten Sie in der grafischen Benutzeroberfläche oder im Command Line Interface.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*. Der Dialog zeigt die eingerichteten Authentifizierungs-Listen.

```
show authlists
```

Zeigt die eingerichteten Authentifizierungs-Listen.

- Deaktivieren Sie die Authentifizierungs-Liste für diejenigen Anwendungen, über die kein Zugriff auf das Gerät erfolgt, zum Beispiel 8021x.

- Heben Sie in Spalte *Aktiv* der Authentifizierungs-Liste `defaultDot1x8021AuthList` die Markierung des Kontrollkästchens auf.

- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
authlists disable  
defaultDot1x8021AuthList
```

Deaktiviert die Authentifizierungs-Liste `defaultDot1x8021AuthList`.

3.1.4 Einstellungen anpassen

Beispiel:

Richten Sie eine eigenständige Authentifizierungs-Liste für die Anwendung `WebInterface` ein, die per Voreinstellung in der Authentifizierungs-Liste `defaultLoginAuthList` enthalten ist. Das Gerät leitet Authentifizierungsanfragen an einen RADIUS-Server im Netz weiter. Als Fallback-Lösung authentifiziert das Gerät die Benutzer über die lokale Benutzerverwaltung.

Führen Sie die folgenden Schritte aus:

- Erzeugen Sie eine Authentifizierungs-Liste `loginGUI`.

- Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

- Klicken Sie die Schaltfläche .

Der Dialog zeigt das Fenster *Erzeugen*.

- Fügen Sie in das Feld *Name* eine aussagekräftige Bezeichnung ein.

Fügen Sie in diesem Beispiel den Namen `loginGUI` ein.

- Klicken Sie die Schaltfläche *Ok*.

Das Gerät fügt einen neuen Tabelleneintrag hinzu.

```
enable
configure
authlists add loginGUI
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Erzeugt die Authentifizierungs-Liste loginGUI.


Wählen Sie die Richtlinien für die Authentifizierungs-Liste loginGUI.

- Markieren Sie in Spalte **Richtlinie 1** den Wert radius.
- Markieren Sie in Spalte **Richtlinie 2** den Wert lokal.
- Wählen Sie in den Spalten **Richtlinie 3** bis **Richtlinie 5** den Wert reject, um weiteres Fall-Back zu verhindern.
- Markieren Sie in Spalte **Aktiv** das Kontrollkästchen.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
authlists set-policy loginGUI radius
local reject reject reject
show authlists
authlists enable loginGUI
```

Weist die Richtlinien radius, local und reject der Authentifizierungs-Liste loginGUI zu.
Zeigt die eingerichteten Authentifizierungs-Listen.
Aktiviert die Authentifizierungs-Liste loginGUI.

Weist der Authentifizierungs-Liste loginGUI eine Anwendung zu.

- Markieren Sie im Dialog **Gerätesicherheit > Authentifizierungs-Liste** die Authentifizierungsliste loginGUI.
- Klicken Sie die Schaltfläche  und dann den Eintrag **Anwendungen zuordnen**. Der Dialog zeigt das Fenster **Anwendungen zuordnen**.
- Markieren Sie in der linken Spalte die Anwendung WebInterface.
- Klicken Sie die Schaltfläche . Die rechte Spalte zeigt jetzt die Anwendung WebInterface.
- Klicken Sie die Schaltfläche **Ok**. Der Dialog zeigt die aktualisierten Einstellungen:
 - Die Spalte **Zugeordnete Anwendungen** der Authentifizierungs-Liste loginGUI zeigt die Anwendung WebInterface.
 - Die Spalte **Zugeordnete Anwendungen** der Authentifizierungs-Liste defaultLoginAuthList zeigt die Anwendung WebInterface nicht mehr.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
show appllists
appllists set-authlist WebInterface
loginGUI
```

Zeigt die Anwendungen und die zugewiesenen Listen.
Weist die Anwendung loginGUI der Authentifizierungs-Liste WebInterface zu.

3.2 Benutzerverwaltung

Das Gerät gewährt Benutzern Zugriff auf seine Management-Funktionen, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Benutzer entweder anhand der lokalen Benutzerverwaltung oder mit einem RADIUS-Server im Netz. Damit das Gerät auf die Benutzerverwaltung zurückgreift, weisen Sie einer Authentifizierungsliste die Richtlinie `local` zu, siehe Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

In der lokalen Benutzerverwaltung verwalten Sie die Benutzerkonten. Jedem Benutzer ist in aller Regel jeweils ein Benutzerkonto zugeordnet.

3.2.1 Berechtigungen

Das Gerät bietet Ihnen die Möglichkeit, durch ein rollenbasiertes Berechtigungsmodell die Zugriffe auf die Management-Funktionen differenziert zu steuern. Benutzer, denen ein bestimmtes Berechtigungsprofil zugeordnet ist, sind befugt, Kommandos und Funktionen aus demselben oder einem niedrigeren Berechtigungsprofil anzuwenden.

Das Gerät wendet die Berechtigungsprofile auf sämtliche Anwendungen an, mit denen Zugriffe auf die Management-Funktionen möglich sind.

Jedes Benutzerkonto ist mit einer Berechtigung verknüpft, das den Zugriff auf die einzelnen Funktionen des Gerätes reguliert. Abhängig von der vorgesehenen Tätigkeit des jeweiligen Benutzers weisen Sie ihm eine vordefinierte Berechtigung zu. Das Gerät unterscheidet die folgenden Berechtigungen.

Rolle	Beschreibung	Autorisiert für folgende Tätigkeiten
Administrator	Der Benutzer ist berechtigt, das Gerät zu überwachen und zu administrieren.	Sämtliche Tätigkeiten mit Lese-/Schreibzugriff einschließlich der folgenden, einem Administrator vorbehaltenen Tätigkeiten: <ul style="list-style-type: none"> ▶ Benutzerkonten hinzufügen, ändern und löschen ▶ Benutzerkonten aktivieren, deaktivieren und entsperren ▶ Alle Passwörter ändern ▶ Passwort-Management konfigurieren ▶ Systemzeit einstellen und ändern ▶ Dateien auf das Gerät laden, zum Beispiel Gerätekonfigurationen, Zertifikate oder Software-Images ▶ Einstellungen und sicherheitsbezogene Einstellungen auf den Lieferzustand zurücksetzen ▶ RADIUS-Server und Authentifizierungslisten konfigurieren ▶ CLI-Skripte anwenden ▶ CLI-Logging und SNMP-Logging ein- und ausschalten ▶ System-Monitor aktivieren und deaktivieren ▶ Dienste für den Management-Zugriff (zum Beispiel SNMP) ein- und ausschalten. ▶ Zugriffsbeschränkungen auf die Benutzeroberfläche oder auf das CLI auf Basis der IP-Adresse konfigurieren
Operator	Der Benutzer ist berechtigt, das Gerät zu überwachen und zu konfigurieren – mit Ausnahme sicherheitsbezogener Einstellungen.	Sämtliche Tätigkeiten mit Lese-/Schreibzugriff mit Ausnahme der o.g. Tätigkeiten, die ausschließlich einem Administrator vorbehalten sind.

Tab. 4: Berechtigungen für Benutzerkonten

Rolle	Beschreibung	Autorisiert für folgende Tätigkeiten
Auditor	Der Benutzer ist berechtigt, das Gerät zu überwachen und das Protokoll im Dialog <i>Diagnose</i> > <i>Bericht</i> > Audit Trail zu speichern.	Überwachende Tätigkeiten mit Lesezugriff.
Guest	Der Benutzer ist berechtigt, das Gerät zu überwachen – mit Ausnahme sicherheitsbezogener Einstellungen.	Überwachende Tätigkeiten mit Lesezugriff.
Unauthorized	Kein Zugriff auf das Gerät möglich. ▶ Als Administrator weisen Sie diese Berechtigung zu, um ein Benutzerkonto vorübergehend zu sperren. ▶ Das Gerät weist diese Berechtigung einem Benutzerkonto zu, falls beim Zuweisen einer anderen Berechtigung ein Fehler auftritt.	Keine erlaubten Tätigkeiten.

Tab. 4: Berechtigungen für Benutzerkonten (Forts.)

3.2.2 Benutzerkonten verwalten

Die Benutzerkonten verwalten Sie in der grafischen Benutzeroberfläche (GUI) oder im CLI.

Führen Sie die folgenden Schritte aus:

-  Öffnen Sie den Dialog *Gerätesicherheit* > *Benutzerverwaltung*.
Der Dialog zeigt die eingerichteten Benutzerkonten.

 `show users` Zeigt die eingerichteten Benutzerkonten.

3.2.3 Voreinstellung

Im Lieferzustand sind die Benutzerkonten `admin` und `user` im Gerät eingerichtet.

Parameter	Voreinstellung	
Benutzername	<code>admin</code>	<code>user</code>
Passwort	<code>private</code>	<code>public</code>
Rolle	<code>administrator</code>	<code>guest</code>
Benutzer gesperrt	<code>unmarkiert</code>	<code>unmarkiert</code>
Richtlinien überprüfen	<code>unmarkiert</code>	<code>unmarkiert</code>
SNMP-Authentifizierung	<code>hmacmd5</code>	<code>hmacmd5</code>
SNMP-Verschlüsselung	<code>des</code>	<code>des</code>

Tab. 5: Voreinstellungen der werkseitig eingerichteten Benutzerkonten

Ändern Sie das Passwort des Benutzerkontos `admin`, bevor Sie das Gerät im Netz zugänglich machen.

3.2.4 Voreingestellte Passwörter ändern

Um ungewünschten Eingriffen vorzubeugen, ändern Sie das Passwort der voreingestellten Benutzerkonten.

Führen Sie die folgenden Schritte aus:

Ändern Sie das Passwort für die Benutzerkonten `admin` und `user`.

Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.

Der Dialog zeigt die eingerichteten Benutzerkonten.

Um eine höhere Komplexität des Passwortes zu erzielen, markieren Sie das Kontrollkästchen in Spalte *Richtlinien überprüfen*.

Das Gerät prüft das Passwort vor dem Speichern anhand der im Rahmen *Passwort-Richtlinien* festgelegten Richtlinien.

Anmerkung: Das Prüfen des Passwortes führt möglicherweise zu einer Meldung im Dialog *Grundeinstellungen > System*, Rahmen *Sicherheits-Status*. Die Einstellungen, die zu dieser Meldung führen, legen Sie fest im Dialog *Grundeinstellungen > System*.

Klicken Sie in der Zeile des betreffenden Benutzerkontos in das Feld *Passwort*. Fügen Sie das Passwort mit mindestens 6 Zeichen ein.

Erlaubt sind bis zu 64 alphanumerische Zeichen.

▶ Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.

▶ Die Mindestlänge des Passwortes ist im Rahmen *Konfiguration* festgelegt. Die Mindestlänge des Passwortes prüft das Gerät immer.

Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

`enable`

`configure`

`users password-policy-check <user>`

`enable`

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den Konfigurationsmodus.

Aktiviert für das Benutzerkonto `<user>` das Prüfen des Passwortes anhand der festgelegten Richtlinien. Damit erzielen Sie eine höhere Komplexität des Passwortes.

Anmerkung: Das Prüfen des Passwortes führt möglicherweise zu einer Meldung, wenn Sie den Sicherheitsstatus anzeigen (`show security-status all`). Die Einstellungen, die zu dieser Meldung führen, legen Sie fest mit dem Kommando `security-status monitor pwd-policy-inactive`.

`users password <user> SECRET`

Legt für das Benutzerkonto `<user>` das Passwort `SECRET` fest. Fügen Sie mindestens 6 Zeichen ein.

`save`



Speichern der Einstellungen im permanenten Speicher (NVM) im „ausgewählten“ Konfigurationsprofil.

3.2.5 Neues Benutzerkonto einrichten

Weisen Sie Benutzern, die auf das Management des Gerätes zugreifen, jeweils ein eigenes Benutzerkonto zu. Auf diese Weise haben Sie die Möglichkeit, die Berechtigungen für die Zugriffe differenziert zu steuern.

Im folgenden Beispiel werden wir das Benutzerkonto für einen Benutzer `USER` mit der Rolle `operator` einrichten. Benutzer mit der Rolle `operator` sind berechtigt, das Gerät zu überwachen und zu konfigurieren – mit Ausnahme sicherheitsbezogener Einstellungen.

Führen Sie die folgenden Schritte aus:

- Erzeugen Sie ein neues Benutzerkonto.
 - Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
 - Klicken Sie die Schaltfläche .
Der Dialog zeigt das Fenster *Erzeugen*.
 - Fügen Sie in das Feld *Benutzername* die Bezeichnung ein.
In diesem Beispiel geben wir dem Benutzerkonto die Bezeichnung `USER`.
 - Klicken Sie die Schaltfläche *Ok*.
 - Um eine höhere Komplexität des Passwortes zu erzielen, markieren Sie das Kontrollkästchen in Spalte *Richtlinien überprüfen*.
Das Gerät prüft das Passwort vor dem Speichern anhand der im Rahmen *Passwort-Richtlinien* festgelegten Richtlinien.
 - Fügen Sie in das Feld *Passwort* das Passwort mit mindestens 6 Zeichen ein.
Erlaubt sind bis zu 64 alphanumerische Zeichen.
 - ▶ Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
 - ▶ Die Mindestlänge des Passwortes ist im Rahmen *Konfiguration* festgelegt. Die Mindestlänge des Passwortes prüft das Gerät immer.
 - Wählen Sie in Spalte *Rolle* die Benutzer-Rolle.
In diesem Beispiel wählen wir den Wert `operator`.
 - Um das Benutzerkonto zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
 - Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
Der Dialog zeigt die eingerichteten Benutzerkonten.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>configure</code>	Wechsel in den Konfigurationsmodus.
<code>users add USER</code>	Erzeugt das Benutzerkonto <code>USER</code> .
<code>users password-policy-check USER enable</code>	Aktiviert für das Benutzerkonto <code>USER</code> das Prüfen des Passwortes anhand der festgelegten Richtlinien. Damit erzielen Sie eine höhere Komplexität des Passwortes.
<code>users password USER SECRET</code>	Legt für das Benutzerkonto <code>USER</code> das Passwort <code>SECRET</code> fest. Fügen Sie mindestens 6 Zeichen ein.
<code>users access-role USER operator</code>	Weist die Rolle <code>operator</code> dem Benutzerkonto <code>USER</code> zu.
<code>users enable USER</code>	Aktiviert das Benutzerkonto <code>USER</code> .
<code>show users</code>	Zeigt die eingerichteten Benutzerkonten.
<code>save</code>	Speichern der Einstellungen im permanenten Speicher (<code>nvm</code>) im „ausgewählten“ Konfigurationsprofil.


Anmerkung: Denken Sie daran, das Passwort zuzuweisen, wenn Sie ein neues Benutzerkonto im CLI einrichten.

3.2.6 Benutzerkonto deaktivieren

Nach Deaktivieren eines Benutzerkontos verweigert das Gerät Zugriffe des zugehörigen Benutzers auf die Management-Funktionen. Im Gegensatz zum vollständigen Löschen bietet das Deaktivieren Ihnen die Möglichkeit, die Einstellungen des Benutzerkontos für eine künftige Wiederverwendung beizubehalten.

Führen Sie die folgenden Schritte aus:


- Um die Einstellungen des Benutzerkontos für eine künftige Wiederverwendung beizubehalten, deaktivieren Sie das Benutzerkonto temporär.

- Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
Der Dialog zeigt die eingerichteten Benutzerkonten.
- Heben Sie in der Zeile des betreffenden Benutzerkontos die Markierung des Kontrollkästchens *Aktiv* auf.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche  .

```
enable
configure
users disable <user>
show users
save
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Deaktivieren eines Benutzerkontos.
Zeigt die eingerichteten Benutzerkonten.
Speichern der Einstellungen im permanenten Speicher (NVM) im „ausgewählten“ Konfigurationsprofil.

- Um die Einstellungen des Benutzerkontos dauerhaft zu deaktivieren, löschen Sie das Benutzerkonto.

- Markieren Sie die Zeile des betreffenden Benutzerkontos.
- Klicken Sie die Schaltfläche  .

```
users delete <user>
show users
save
```

Löscht das Benutzerkonto <user>.
Zeigt die eingerichteten Benutzerkonten.
Speichern der Einstellungen im permanenten Speicher (NVM) im „ausgewählten“ Konfigurationsprofil.

3.2.7 Richtlinien für Passwörter anpassen

Das Gerät bietet Ihnen die Möglichkeit, die Passwörter der Benutzerkonten auf Einhaltung vorgegebener Richtlinien zu prüfen. Durch Einhaltung der Richtlinien erzielen Sie Passwörter mit höherer Komplexität.

Die Benutzerverwaltung des Gerätes bietet Ihnen die Möglichkeit, die Prüfung in jedem Benutzerkonto individuell ein- oder auszuschalten. Bei eingeschalteter Prüfung akzeptiert das Gerät ein geändertes Passwort ausschließlich dann, wenn es die Anforderungen der Richtlinien erfüllt.

Im Lieferzustand sind praxistaugliche Werte für die Richtlinien im Gerät eingerichtet. Sie haben die Möglichkeit, die Richtlinien an Ihre Erfordernisse anzupassen.

Führen Sie die folgenden Schritte aus:

Passen Sie die Richtlinien für Passwörter an Ihre Erfordernisse an.

Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.

Im Rahmen *Konfiguration* legen Sie fest, wie viele Login-Versuche das Gerät zulässt, bevor es den Benutzer sperrt. Sie legen ebenfalls die Mindestanzahl von Zeichen fest, aus denen ein Passwort besteht.

Legen Sie die Werte entsprechend Ihren Anforderungen fest.

- ▶ Die Anzahl der Login-Versuche eines Benutzers legen Sie fest im Feld *Login-Versuche* fest. Das Feld bietet Ihnen die Möglichkeit, diesen Wert im Bereich 0..5 festzulegen. Im obigen Beispiel deaktiviert der Wert 0 die Funktion.
- ▶ Im Feld *Min. Passwort-Länge* sind Werte im Bereich 1..64 zulässig.

Der Dialog zeigt im Rahmen *Passwort-Richtlinien* die eingerichteten Richtlinien.

Passen Sie die Werte an Ihre Erfordernisse an.

- ▶ Erlaubt sind Werte im Bereich 1 bis 16.
Der Wert 0 deaktiviert die betreffende Richtlinie.

Um die in den Rahmen *Konfiguration* und *Passwort-Richtlinien* festgelegten Einträge anzuwenden, markieren Sie das Kontrollkästchen in Spalte *Richtlinien überprüfen* für einen bestimmten Benutzer.

Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
passwords min-length 6	Legt die Richtlinie für die Mindestlänge des Passworts fest.
passwords min-lowercase-chars 1	Legt die Richtlinie für die Mindestanzahl von Kleinbuchstaben im Passwort fest.
passwords min-numeric-chars 1	Legt die Richtlinie für die Mindestanzahl von Ziffern im Passwort fest.
passwords min-special-chars 1	Legt die Richtlinie für die Mindestanzahl von Sonderzeichen im Passwort fest.
passwords min-uppercase-chars 1	Legt die Richtlinie für die Mindestanzahl von Großbuchstaben im Passwort fest.
show passwords	Zeigt die eingerichteten Richtlinien.
save	Speichern der Einstellungen im permanenten Speicher (nvram) im „ausgewählten“ Konfigurationsprofil.

3.3 SNMP-Zugriff

Das Protokoll SNMP bietet Ihnen die Möglichkeit, mit einem Netzmanagementsystem das Gerät über das Netz zu überwachen und seine Einstellungen zu ändern.

3.3.1 SNMPv1/v2-Zugriff

Mit SNMPv1 oder SNMPv2 kommunizieren das Netzmanagementsystem und das Gerät unverschlüsselt. Jedes SNMP-Paket enthält den Community-Namen im Klartext und die IP-Adresse des Absenders.

Im Gerät voreingestellt sind die Community-Namen `public` für Lese-Zugriffe und `private` für Schreib-Zugriffe. Wenn SNMPv1/v2 eingeschaltet ist, erlaubt das Gerät jedem, der den Community-Namen kennt, Zugriff auf das Gerät.

Treffen Sie folgende grundsätzlichen Vorkehrungen, um unerwünschte Zugriffe auf das Gerät zu erschweren:

- Ändern Sie im Gerät die voreingestellten Community-Namen.
Behandeln Sie die Community-Namen vertraulich.
Jeder, der den Community-Namen für Schreibzugriffe kennt, hat die Möglichkeit, die Einstellungen des Gerätes zu ändern.
- Legen Sie für Lese-/Schreibzugriffe einen anderen Community-Namen fest als für Lesezugriffe.
- Verwenden Sie SNMPv1 oder SNMPv2 ausschließlich in abhörsicheren Umgebungen. Die Protokolle verwenden keine Verschlüsselung.
- Wir empfehlen, SNMPv3 zu nutzen und im Gerät den Zugriff über SNMPv1 und SNMPv2 auszuschalten.

3.3.2 SNMPv3-Zugriff

Mit SNMPv3 kommunizieren das Netzmanagementsystem und das Gerät verschlüsselt. Das Netzmanagementsystem authentifiziert sich gegenüber dem Gerät mit den Zugangsdaten eines Benutzers. Voraussetzung für den SNMPv3-Zugriff ist, dass im Netzmanagementsystem dieselben Einstellungen wie im Gerät festgelegt sind.

Das Gerät bietet Ihnen die Möglichkeit, für jedes Benutzerkonto die Parameter *SNMP-Authentifizierung* und *SNMP-Verschlüsselung* individuell festzulegen.

Wenn Sie im Gerät ein neues Benutzerkonto einrichten, sind die Parameter so voreingestellt, dass das Netzmanagementsystem Industrial HiVision das Gerät damit sofort erreicht.

Die im Gerät eingerichteten Benutzerkonten verwenden in der Grafischen Benutzeroberfläche, im Command Line Interface (CLI) und für SNMPv3 dieselben Passwörter.

Um die SNMPv3-Parameter des Benutzerkontos an die Einstellungen in Ihrem Netzmanagementsystem anzupassen, führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*. Der Dialog zeigt die eingerichteten Benutzerkonten.
- Klicken Sie in der Zeile des betreffenden Benutzerkontos in das Feld *SNMP-Authentifizierung*. Wählen Sie die gewünschte Einstellung.
- Klicken Sie in der Zeile des betreffenden Benutzerkontos in das Feld *SNMP-Verschlüsselung*. Wählen Sie die gewünschte Einstellung.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

<pre>enable configure users snmpv3 authentication <user> md5 sha1 users snmpv3 encryption <user> des aes128 none show users save</pre>	<p>Wechsel in den Privileged-EXEC-Modus. Wechsel in den Konfigurationsmodus. Protokoll HMAC-MD5 oder HMAC-SHA dem Benutzerkonto <user> für Authentifizierungsanfragen zuweisen. Algorithmus DES oder AES-128 dem Benutzerkonto <user> zuweisen. Mit dem Algorithmus verschlüsselt das Gerät Authentifizierungsanfragen. Der Wert none hebt die Verschlüsselung auf. Eingerichtete Benutzerkonten anzeigen. Speichern der Einstellungen im permanenten Speicher (nvm) im „ausgewählten“ Konfigurationsprofil.</p>
---	--

3.4 Service Shell

Wenn Sie beim Zugriff auf Ihr Gerät Unterstützung benötigen, verwendet das Service-Personal die Service Shell, um interne Bedingungen wie Schieberegister und CPU-Register zu überwachen.

Die Service Shell dient ausschließlich zu Service-Zwecken. Sie ermöglicht den Zugriff auf interne Funktionen des Geräts. Führen Sie keinesfalls interne Funktionen ohne die Anweisung eines Servicetechnikers aus. Das Ausführen interner Funktionen wie beispielsweise das Löschen des NVM-Inhalts (permanenter Speicher) führt unter Umständen dazu, dass Ihr Gerät funktionsunfähig wird.

■ Service Shell starten

Führen Sie die folgenden Schritte aus:

- Um vom User-Exec-Modus in den Privileged-Exec-Modus zu wechseln, geben Sie `enable` ein, oder `en` und ein Leerzeichen, und drücken die <Enter>-Taste.
- Um sich die in diesem Modus verfügbaren Kommandos auflisten zu lassen, drücken Sie die Taste <?>.

```
!(EES) >enable

!(EES) #?
clear          Clear several items.
configure      Enter into global config mode.
copy           Copy different kinds of items.
debug          Service functions to find configuration errors.
exit           Exit from current mode.
help           Display help for various special keys.
history        Show a list of previously run commands.
login          Set login parameters.
logout         Exit this session.
network        Modify network parameters.
ping           Send ICMP echo packets to a specified
              IP address.
profile        Activate or delete configuration profiles.
reboot         Reset the device (cold start).
save           Save configuration.
serviceshell  Enter system mode.
set            Set device parameters.
show           Display device options and settings.
traceroute     Trace route to a specified host.

!(EES) #serviceshell

-> exit
Au revoir!

!* (EES) #
```

- Um die Service Shell zu starten, geben Sie im Privileged-Exec-Modus `serviceshell` ein, oder `ser` und ein Leerzeichen, und drücken die <Enter>-Taste.

Um Inkonsistenzen in der Gerätekonfiguration zu vermeiden, loggen Sie sich aus der Service Shell aus, bevor ein anderer Benutzer den Upload einer neuen Konfiguration auf das Gerät startet.

- Um die Service Shell zu beenden, geben Sie `exit` ein und drücken die <Enter>-Taste.

Anmerkung: Wenn die Service Shell aktiv ist, ist das Timeout des Command Line Interfaces inaktiv.

■ Service Shell permanent deaktivieren

Wenn Sie die Service Shell nicht benötigen, haben Sie die Möglichkeit, diese Funktion zu deaktivieren. In diesem Fall haben Sie weiterhin die Möglichkeit, das Gerät zu konfigurieren. Der Service-Techniker hat jedoch keine Möglichkeit mehr, auf interne Funktionen Ihres Geräts zuzugreifen, um zusätzlich benötigte Informationen abzurufen.

Anmerkung: Wenn Sie die Service Shell deaktivieren, haben Sie weiterhin die Möglichkeit, das Gerät zu konfigurieren, beschränken jedoch die Möglichkeiten des Service-Personals auf System-Diagnosen. Die Deaktivierung ist unumkehrbar, die Service Shell bleibt dauerhaft deaktiviert. **Um die Service Shell zu reaktivieren ist das Öffnen des Gerätes seitens des Herstellers erforderlich.**

Führen Sie die folgenden Schritte aus:

- Um die Service Shell anzuzeigen, geben Sie `serviceshell` ein, oder `ser` und ein Leerzeichen, und drücken die <Enter>-Taste.
- Dieser Schritt ist unumkehrbar!
Um die Service Shell permanent zu deaktivieren, geben Sie `deactivate` ein, oder `d` und ein Leerzeichen, und drücken die <Enter>-Taste.

```
!(EES) >enable

!(EES) #serviceshell?
[deactivate]          Disable the service shell access permanently
                      (Cannot be undone).
<cr>                  Press Enter to execute the command.

!(EES) #serviceshell deactivate
```

4 Konfigurationsprofile verwalten


Wenn Sie die Einstellungen des Gerätes im laufenden Betrieb ändern, speichert das Gerät diese Änderungen im flüchtigen Speicher (RAM). Nach einem Neustart sind diese Einstellungen verloren.

Damit die Änderungen einen Neustart überdauern, bietet Ihnen das Gerät die Möglichkeit, die Einstellungen zusätzlich in einem Konfigurationsprofil im permanenten Speicher (NVM) zu speichern. Um gegebenenfalls schnell auf andere Einstellungen umzuschalten, bietet der permanente Speicher Platz für mehrere Konfigurationsprofile.

4.1 Geänderte Einstellungen erkennen

Einstellungsänderungen im laufenden Betrieb speichert das Gerät im flüchtigen Speicher (RAM). Das Konfigurationsprofil im permanenten Speicher (NVM) bleibt dabei unverändert, bis Sie es explizit speichern. Bis dahin unterscheiden sich die Konfigurationsprofile im flüchtigen und im permanenten Speicher.

Das Gerät unterstützt Sie dabei, geänderte Einstellungen zu erkennen. Wenn sich das Konfigurationsprofil im flüchtigen Speicher (RAM) vom „ausgewählten“ Konfigurationsprofil im permanenten Speicher (NVM) unterscheidet, erkennen Sie diesen Unterschied an den folgenden Kriterien:

Die Statusleiste im oberen Bereich des Menüteils zeigt das Symbol . Stimmen die Konfigurationsprofile überein, ist das Symbol ausgeblendet.

Im Dialog *Grundeinstellungen* > *Laden/Speichern*, Rahmen *Information* ist das Kontrollkästchen unmarkiert. Stimmen dagegen die Konfigurationsprofile überein, ist das Kontrollkästchen markiert.

```
show config status
Configuration Storage sync State
-----
running-config to NV.....out of sync
...
```

4.2 Einstellungen speichern


4.2.1 Konfigurationsprofil im Gerät speichern

Wenn Sie die Einstellungen des Gerätes im laufenden Betrieb ändern, speichert das Gerät diese Änderungen im flüchtigen Speicher (RAM). Damit die Änderungen einen Neustart überdauern, speichern Sie das Konfigurationsprofil im permanenten Speicher (NVM).

■ Konfigurationsprofil speichern

Das Gerät speichert die Einstellungen immer im „ausgewählten“ Konfigurationsprofil im permanenten Speicher (NVM).

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- Vergewissern Sie sich, dass das gewünschte Konfigurationsprofil „ausgewählt“ ist. Das „ausgewählte“ Konfigurationsprofil erkennen Sie daran, dass in Spalte *Ausgewählt* das Kontrollkästchen markiert ist.
- Klicken Sie die Schaltfläche  .

`show config profiles nvm`

Zeigt die im permanenten Speicher (nvm) enthaltenen Konfigurationsprofile.

`enable`

Wechsel in den Privileged-EXEC-Modus.


`save`

Speichern der Einstellungen im permanenten Speicher (nvm) im „ausgewählten“ Konfigurationsprofil.

■ Einstellungen in Konfigurationsprofil kopieren

Das Gerät bietet Ihnen die Möglichkeit, die im flüchtigen Speicher (RAM) gespeicherten Einstellungen anstatt im „ausgewählten“ Konfigurationsprofil in ein anderes Konfigurationsprofil zu kopieren. Auf diese Weise erzeugen Sie im permanenten Speicher (NVM) ein neues oder überschreiben ein vorhandenes Konfigurationsprofil.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- Klicken Sie die Schaltfläche  und dann den Eintrag *Speichern unter....*. Der Dialog zeigt das Fenster *Speichern unter....*
- Passen Sie im Feld *Name* die Bezeichnung des Konfigurationsprofils an. Wenn Sie die vorgeschlagene Bezeichnung beibehalten, überschreibt das Gerät ein vorhandenes, namensgleiches Konfigurationsprofil.
- Klicken Sie die Schaltfläche *Ok*.

Das neue Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

```
show config profiles nvm
```

Zeigt die im permanenten Speicher (NVM) enthaltenen Konfigurationsprofile.

```
enable
```

Wechsel in den Privileged-EXEC-Modus.

```
copy config running-config nvm profile  
<string>
```

Speichern der aktuellen Einstellungen im Konfigurationsprofil mit der Bezeichnung <string> im permanenten Speicher (NVM). Wenn vorhanden, überschreibt das Gerät ein namensgleiches Konfigurationsprofil. Das neue Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

■ Konfigurationsprofil auswählen

Enthält der permanente Speicher (NVM) mehrere Konfigurationsprofile, haben Sie die Möglichkeit, dort ein beliebiges Konfigurationsprofil auszuwählen. Das Gerät speichert die Einstellungen immer im „ausgewählten“ Konfigurationsprofil. Das Gerät lädt die Einstellungen des „ausgewählten“ Konfigurationsprofils beim Neustart in den flüchtigen Speicher (RAM).

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.

Die Tabelle zeigt die im Gerät vorhandenen Konfigurationsprofile. Das „ausgewählte“ Konfigurationsprofil erkennen Sie daran, dass in Spalte *Ausgewählt* das Kontrollkästchen markiert ist.

- Markieren Sie den Tabelleneintrag des gewünschten Konfigurationsprofils, das im permanenten Speicher (NVM) gespeichert ist.

- Klicken Sie die Schaltfläche  und dann den Eintrag *Auswählen*.

In Spalte *Ausgewählt* ist jetzt das Kontrollkästchen des Konfigurationsprofils markiert.

```
enable
```

Wechsel in den Privileged-EXEC-Modus.

```
show config profiles nvm
```

Zeigt die im permanenten Speicher (NVM) enthaltenen Konfigurationsprofile.

```
configure
```

Wechsel in den Konfigurationsmodus.

```
config profile select nvm 1
```

Kennzeichnen des Konfigurationsprofils.

Orientieren Sie sich am nebenstehenden Namen des Konfigurationsprofils.

```
save
```

Speichern der Einstellungen im permanenten Speicher (NVM) im „ausgewählten“ Konfigurationsprofil.

4.2.2 Konfigurationsprofil auf entferntem Server sichern

Das Gerät bietet Ihnen die Möglichkeit, eine Kopie des Konfigurationsprofils automatisch auf einem Remote-Server zu sichern. Voraussetzung ist, dass Sie die Funktion vor dem Speichern des Konfigurationsprofils aktivieren.

Nach dem Speichern des Konfigurationsprofils im permanenten Speicher (NVM) sendet das Gerät eine Kopie an die festgelegte Adresse.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.

Die folgenden Schritte führen Sie im Rahmen *Sichere Konfiguration auf Remote-Server beim Speichern* aus.

- Legen Sie im Rahmen *URL* den Server sowie Pfad und Dateinamen des kopierten Konfigurationsprofils fest.
- Klicken Sie die Schaltfläche *Zugangsdaten setzen*. Der Dialog zeigt das Fenster *Anmeldeinformationen*.
- Geben Sie die Anmeldedaten ein, die für die Authentifizierung auf dem entfernten Server erforderlich sind.
- Schalten Sie die Funktion in der Optionsliste *Funktion* ein.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

enable	Wechsel in den Privileged-EXEC-Modus.
show config remote-backup	Status der Funktion prüfen.
configure	Wechsel in den Konfigurationsmodus.
config remote-backup destination	Ziel-URL für das kopierte Konfigurationsprofil einfügen.
config remote-backup username	Benutzernamen einfügen für die Authentifizierung auf dem entfernten Server.
config remote-backup password	Passwort einfügen für die Authentifizierung auf dem entfernten Server.
config remote-backup operation	Einschalten der Funktion.

Wenn die Übertragung zum entfernten Server scheitert, protokolliert das Gerät dieses Ereignis in der Protokolldatei System Log.

4.2.3 Konfigurationsprofil exportieren

Das Gerät bietet Ihnen die Möglichkeit, ein Konfigurationsprofil als XML-Datei auf einem Server zu speichern. Wenn Sie die grafische Benutzeroberfläche verwenden, haben Sie die Möglichkeit, die XML-Datei direkt auf Ihrem PC zu speichern.

Voraussetzung:

- ▶ Um die Datei auf einem Server zu speichern, benötigen Sie einen eingerichteten Server im Netz.
- ▶ Um die Datei auf einem SCP- oder SFTP-Server zu speichern, benötigen Sie zusätzlich Benutzernamen und Passwort für den Zugriff auf diesen Server.


Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- Markieren Sie den Tabelleneintrag des gewünschten Konfigurationsprofils.

Um das Konfigurationsprofil auf Ihren PC zu exportieren, führen Sie die folgenden Schritte aus:

- Klicken Sie den Link in Spalte *Profilname*.
 - Wählen Sie den Speicherort und legen den Dateinamen fest.
 - Klicken Sie die Schaltfläche *Ok*.
- Das Konfigurationsprofil ist jetzt als XML-Datei am angegebenen Ort gespeichert.

Um das Konfigurationsprofil auf einen Remote-Server zu exportieren, führen Sie die folgenden Schritte aus:

- Klicken Sie die Schaltfläche  und dann den Eintrag *Exportieren...*.
Der Dialog zeigt das Fenster *Exportieren...*
- Legen Sie im Feld *URL* die URL der Datei auf dem Remote-Server fest.
 - ▶ Um die Datei auf einem FTP-Server zu speichern, legen Sie den URL zur Datei in der folgenden Form fest:
ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>
 - ▶ Um die Datei auf einem TFTP-Server zu speichern, legen Sie den URL zur Datei in der folgenden Form fest:
tftp://<IP-Adresse>/<Pfad>/<Dateiname>
 - ▶ Um die Datei auf einem SCP- oder SFTP-Server zu speichern, legen Sie den URL zur Datei in einer der folgenden Formen fest:
scp:// oder sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>
scp:// oder sftp://<IP-Adresse>/<Pfad>/<Dateiname>Nach Klicken der Schaltfläche *Ok* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
- Klicken Sie die Schaltfläche *Ok*.
Das Konfigurationsprofil ist jetzt als XML-Datei am angegebenen Ort gespeichert.

show config profiles nvm	Zeigt die im permanenten Speicher (nvm) enthaltenen Konfigurationsprofile.
enable	Wechsel in den Privileged-EXEC-Modus.
copy config running-config remote tftp://<IP_address>/ <path>/<file_name>	Speichern der aktuellen Einstellungen auf einem TFTP-Server.
copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>	Speichern des „ausgewählten“ Konfigurationsprofils im permanenten Speicher nvm auf einem SFTP-Server.
copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>	Speichern des Konfigurationsprofils config3 im permanenten Speicher (nvm) auf einem TFTP-Server.
copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>	Speichern des Konfigurationsprofils config3 im permanenten Speicher (nvm) auf einem FTP-Server.


4.3 Einstellungen laden

Mit dem Laden der Einstellungen bietet Ihnen das Gerät die Möglichkeit, gegebenenfalls schnell auf andere Einstellungen umzuschalten.

4.3.1 Konfigurationsprofil aktivieren

Der permanente Speicher des Gerätes bietet Platz für mehrere Konfigurationsprofile. Wenn Sie ein dort gespeichertes Konfigurationsprofil aktivieren, ändern Sie damit die Einstellungen des Gerätes im laufenden Betrieb ohne Neustart.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- Markieren Sie den Tabelleneintrag des gewünschten Konfigurationsprofils.
- Klicken Sie die Schaltfläche  und dann den Eintrag *Aktivieren*.

Das Gerät kopiert die Einstellungen in den flüchtigen Speicher (*RAM*) und trennt die Verbindung zur grafischen Benutzeroberfläche. Das Gerät verwendet die Einstellungen des Konfigurationsprofils ab sofort im laufenden Betrieb.

- Laden Sie die grafische Benutzeroberfläche neu.
- Melden Sie sich erneut an.

In Spalte *Ausgewählt* ist das Kontrollkästchen des soeben aktivierten Konfigurationsprofils markiert.

```
show config profiles nvm
```

Zeigt die im permanenten Speicher (*nvm*) enthaltenen Konfigurationsprofile.

```
enable
```

Wechsel in den Privileged-EXEC-Modus.

```
copy config nvm profile config3 running-  
config
```

Einstellungen des Konfigurationsprofils *config3* im permanenten Speicher (*nvm*) anwenden.

Das Gerät kopiert die Einstellungen in den flüchtigen Speicher und trennt die CLI-Verbindung. Das Gerät wendet die Einstellungen des Konfigurationsprofils *config3* sofort im laufenden Betrieb an.


4.3.2 Konfigurationsprofil importieren

Das Gerät bietet Ihnen die Möglichkeit, ein als XML-Datei gespeichertes Konfigurationsprofil von einem Server zu importieren. Wenn Sie die grafische Benutzeroberfläche verwenden, haben Sie die Möglichkeit, die XML-Datei direkt von Ihrem PC zu importieren.

Voraussetzung:

- ▶ Um die Datei auf einem Server zu speichern, benötigen Sie einen eingerichteten Server im Netz.
- ▶ Um die Datei auf einem SCP- oder SFTP-Server zu speichern, benötigen Sie zusätzlich Benutzernamen und Passwort für den Zugriff auf diesen Server.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- Klicken Sie die Schaltfläche  und dann den Eintrag *Importieren...*.
Der Dialog zeigt das Fenster *Importieren...*
- Wählen Sie in der Dropdown-Liste *Select source* aus, woher das Gerät das Konfigurationsprofil importiert.
 - ▶ PC/URL
Das Gerät importiert das Konfigurationsprofil vom lokalen PC oder von einem Remote-Server.

Um das Konfigurationsprofil vom lokalen PC oder von einem Remote-Server zu importieren, führen Sie die folgenden Schritte aus:

- Importieren Sie das Konfigurationsprofil.
 - Befindet sich die Datei auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
`ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
 - Befindet sich die Datei auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
`tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
 - Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in einer der folgenden Formen fest:
`scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
`scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`
- Legen Sie im Rahmen *Ziel* fest, wo das Gerät das importierte Konfigurationsprofil speichert.
 - Legen Sie im Feld *Profilname* den Namen fest, unter dem das Gerät das Konfigurationsprofil speichert.
 - Legen Sie im Feld *Speicher-Typ* den Speicherort für das Konfigurationsprofil fest.
- Klicken Sie die Schaltfläche *Ok*.

Das Gerät kopiert das Konfigurationsprofil in den festgelegten Speicher.

Wenn Sie im Rahmen *Ziel* den Wert `ram` festgelegt haben, trennt das Gerät die Verbindung zur grafischen Benutzeroberfläche und verwendet die Einstellungen sofort im laufenden Betrieb.

```
enable
copy config remote ftp://
<IP_address>:<port>/<path>/<file_name>
running-config
```

Wechsel in den Privileged-EXEC-Modus.

Konfigurationsprofil-Einstellungen von einem FTP-Server importieren und anwenden.

Das Gerät kopiert die Einstellungen in den flüchtigen Speicher und trennt die CLI-Verbindung. Das Gerät wendet die Einstellungen des importierten Konfigurationsprofils sofort im laufenden Betrieb an.

```
copy config remote tftp://<IP_address>/
<path>/<file_name> running-config
```

Konfigurationsprofil-Einstellungen von einem TFTP-Server importieren und anwenden.

Das Gerät kopiert die Einstellungen in den flüchtigen Speicher und trennt die CLI-Verbindung. Das Gerät wendet die Einstellungen des importierten Konfigurationsprofils sofort im laufenden Betrieb an.

```
copy config remote sftp://
<user name>:<password>@<IP_address>/
<path>/<file_name> running-config
```

Konfigurationsprofil-Einstellungen von einem SFTP-Server importieren und anwenden.

Das Gerät kopiert die Einstellungen in den flüchtigen Speicher und trennt die CLI-Verbindung. Das Gerät wendet die Einstellungen des importierten Konfigurationsprofils sofort im laufenden Betrieb an.

```
copy config remote ftp://  
<IP_address>:<port>/<path>/<file_name>  
nvm profile config3
```

Einstellungen des auf einem FTP-Server gespeicherten Konfigurationsprofils importieren und die Einstellungen im Konfigurationsprofil `config3` im permanenten Speicher (nvm) speichern.

```
copy config remote tftp://<IP_address>/  
<path>/<file_name> nvm profile config3
```

Einstellungen des auf einem TFTP-Server gespeicherten Konfigurationsprofils importieren und die Einstellungen im Konfigurationsprofil `config3` im permanenten Speicher (nvm) speichern.


4.4 Gerät auf Lieferzustand zurücksetzen

Wenn Sie die Einstellungen im Gerät auf den Lieferzustand zurücksetzen, löscht das Gerät die Konfigurationsprofile im flüchtigen Speicher und im permanenten Speicher.

Anschließend startet das Gerät neu und lädt die Werkseinstellungen.

4.4.1 Mit grafischer Benutzeroberfläche oder CLI

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- Klicken Sie die Schaltfläche , anschließend *Auf Lieferzustand zurücksetzen...*. Der Dialog zeigt eine Warnmeldung.
- Klicken Sie die Schaltfläche *Ok*.

Das Gerät löscht die Konfigurationsprofile im flüchtigen Speicher (RAM) und im permanenten Speicher (NVM).

Nach kurzer Zeit startet das Gerät neu und lädt die Werkseinstellungen.

enable
clear factory

Wechsel in den Privileged-EXEC-Modus.
Löscht die Konfigurationsprofile im flüchtigen Speicher und im permanenten Speicher.
Nach kurzer Zeit startet das Gerät neu und lädt die Werkseinstellungen.

4.4.2 System-Monitor starten

Voraussetzung:

Ihr PC ist per Terminal-Kabel mit dem V.24-Anschluss des Gerätes verbunden.

Führen Sie die folgenden Schritte aus:

- Starten Sie das Gerät neu.
- Um in den System-Monitor zu wechseln, drücken Sie die Taste <1> bei Aufforderung während des Neustarts innerhalb von 3 Sekunden.
Das Gerät lädt den System-Monitor.
- Um aus dem Hauptmenü in das Menü `Manage configurations` zu wechseln, drücken Sie die Taste <4>.
- Um das Kommando `Clear configs and boot params` auszuführen, drücken Sie die Taste <1>.

- Um die Werkseinstellungen zu laden, drücken Sie die <Enter>-Taste.
Das Gerät löscht die Konfigurationsprofile im flüchtigen Speicher (RAM) und im permanenten Speicher (NVM).
Ist ein externer Speicher angeschlossen, löscht das Gerät auch die auf dem externen Speicher gespeicherten Konfigurationsprofile.
- Um in das Hauptmenü zu wechseln, drücken Sie die Taste <q>.
- Um das Gerät mit Werkseinstellungen neuzustarten, drücken Sie die Taste <q>.

5 Neueste Software laden

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

Das Gerät bietet Ihnen folgende Möglichkeiten, die Geräte-Software zu aktualisieren:

- ▶ [Software-Update vom PC](#)
- ▶ [Software-Update von einem Server](#)
- ▶ [Ältere Software laden](#)

Anmerkung: Die Einstellungen im Gerät bleiben nach dem Aktualisieren der Geräte-Software erhalten. Die Version der installierten Geräte-Software sehen Sie auf der Login-Seite der grafischen Benutzeroberfläche. Wenn Sie bereits angemeldet sind, führen Sie die folgenden Schritte aus, um die Version der installierten Software anzuzeigen:

- Öffnen Sie den Dialog *Grundeinstellungen > Software*.

Das Feld *Running version* zeigt Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Neustart geladen hat und derzeit ausführt.

```
enable
show system info
```


Wechsel in den Privileged-EXEC-Modus.

Zeigt die Systeminformationen, unter anderem Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Neustart geladen hat und derzeit ausführt.

5.1 Software-Update vom PC

Voraussetzung ist, dass die Image-Datei der Geräte-Software auf einem Datenträger gespeichert ist, den Sie von Ihrem PC aus erreichen.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie das Verzeichnis, in dem die Image-Datei der Geräte-Software gespeichert ist.
- Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- Ziehen Sie die Image-Datei in den -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.
- Um den Update-Vorgang zu starten, klicken Sie die Schaltfläche *Start*.
Sobald der Update-Vorgang erfolgreich beendet ist, zeigt das Gerät eine Information, dass die Software erfolgreich aktualisiert wurde.
Beim nächsten Neustart lädt das Gerät die installierte Geräte-Software.

5.2 Software-Update von einem Server

Für ein Software-Update mit SFTP oder SCP benötigen Sie einen Server, auf dem die Image-Datei der Geräte-Software abgelegt ist.

Für ein Software-Update mit TFTP, SFTP oder SCP benötigen Sie einen Server, auf dem die Image-Datei der Geräte-Software abgelegt ist.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- Fügen Sie im Rahmen *Software-Update*, Feld *URL* den URL zur Image-Datei in der folgenden Form ein:
 - ▶ Wenn die Image-Datei auf einem FTP-Server abgelegt ist:
`ftp://<IP-Adresse>:<Port>/<Pfad>/<Name_der_Image-Datei>.bin`
 - ▶ Wenn die Image-Datei auf einem TFTP-Server abgelegt ist:
`tftp://<IP-Adresse>/<Pfad>/<Name_der_Image-Datei>.bin`
 - ▶ Wenn die Image-Datei auf einem SCP- oder SFTP-Server abgelegt ist:
`scp:// oder sftp://<IP-Adresse>/<Pfad>/<Name_der_Image-Datei>.bin`
`scp:// oder sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/ <Name_der_Image-Datei>.bin`
Wenn Sie den URL ohne Benutzername und Passwort einfügen, zeigt das Gerät das Fenster *Anmeldeinformationen*. Fügen Sie dort die Anmeldedaten ein, um sich am Server anzumelden.
- Um den Update-Vorgang zu starten, klicken Sie die Schaltfläche *Start*.
Sobald der Update-Vorgang erfolgreich beendet ist, zeigt das Gerät eine Information, dass die Software erfolgreich aktualisiert wurde.
Beim nächsten Neustart lädt das Gerät die installierte Geräte-Software.

```
enable
```

```
copy firmware remote tftp://10.0.1.159/  
product.bin system
```

Wechsel in den Privileged-EXEC-Modus.

Übertragen der Datei `product.bin` vom TFTP-Server mit der IP-Adresse `10.0.1.159` auf das Gerät.

5.3 Ältere Software laden

Das Gerät bietet Ihnen die Möglichkeit, die Geräte-Software durch eine ältere Version zu ersetzen. Nach dem Ersetzen der Geräte-Software bleiben die Grundeinstellungen im Gerät erhalten.

Anmerkung: Die Einstellungen von Funktionen, die ausschließlich in der neueren Geräte-Software-Version zur Verfügung stehen, gehen verloren.

6 Ports konfigurieren

Folgende Funktionen für die Port-Konfiguration stehen zur Verfügung:

- ▶ Port ein-/ausschalten
- ▶ Betriebsart wählen

6.1 Port ein-/ausschalten

In der Voreinstellung ist jeder Port eingeschaltet. Um einen höheren Zugangsschutz zu erzielen, schalten Sie die Ports aus, an die Sie nichts anschließen.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen* > *Port*, Registerkarte .
- Um einen Port einzuschalten, markieren Sie das Kontrollkästchen in Spalte *Port an*.
- Um einen Port auszuschalten, heben Sie die Markierung des Kontrollkästchens in Spalte *Port an* auf.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
interface 1/1
no shutdown
```

```
Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/
1.
Aktivieren der Schnittstelle
```

6.2 Betriebsart wählen

In der Voreinstellung befinden sich die Ports im Betriebsmodus *Automatische Konfiguration*.

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

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen* > *Port*, Registerkarte .
- Falls das an diesem Port angeschlossene Gerät eine feste Einstellung voraussetzt:
 - Deaktivieren Sie die Funktion. Heben Sie die Markierung des Kontrollkästchens in Spalte *Automatische Konfiguration* auf.
 - Legen Sie in Spalte *Manuelle Konfiguration* die Betriebsart (Übertragungsgeschwindigkeit, Duplexbetrieb) fest.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
enable
configure
interface 1/1

no auto-negotiate
speed 10 full
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
Ausschalten des Modus für die automatische Konfiguration.
Portgeschwindigkeit 10 MBit/s, Vollduplex

7 Unterstützung beim Schutz vor unberechtigtem Zugriff

Das Gerät bietet Ihnen Funktionen, die Ihnen helfen, das Gerät vor unberechtigten Zugriffen zu schützen.

Führen Sie nach dem Einrichten des Gerätes die folgenden Schritte aus, um das Risiko unberechtigter Zugriffe auf das Gerät zu reduzieren.

- ▶ SNMPv1/v2-Community ändern
- ▶ SNMPv1/v2 ausschalten
- ▶ HTTP ausschalten
- ▶ Eigenes HTTPS-Zertifikat verwenden
- ▶ Eigenen SSH-Schlüssel verwenden
- ▶ Telnet ausschalten
- ▶ HiDiscovery ausschalten
- ▶ IP Zugriffsbeschränkung aktivieren
- ▶ Session-Timeouts anpassen

7.1 SNMPv1/v2-Community ändern

SNMPv1/v2 arbeitet unverschlüsselt. Jedes SNMP-Paket enthält die IP-Adresse des Absenders und im Klartext den Community-Namen, mit dem der Absender auf das Gerät zugreift. Wenn SNMPv1/v2 eingeschaltet ist, erlaubt das Gerät jedem, der den Community-Namen kennt, Zugriff auf das Gerät.

Voreingestellt sind die Community-Namen `public` für Lese-Zugriffe und `private` für Schreib-Zugriffe. Wenn Sie SNMPv1 oder SNMPv2 verwenden, ändern Sie die voreingestellten Community-Namen. Behandeln Sie die Community-Namen vertraulich.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community*.

Der Dialog zeigt die eingerichteten Communitys.

- Legen Sie für die -Community in Spalte *Name* den Community-Namen fest.
 - ▶ Erlaubt sind bis zu 32 alphanumerische Zeichen.
 - ▶ Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
 - ▶ Legen Sie einen anderen Community-Namen fest als für Lesezugriffe.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
snmp community rw <community name>
show snmp community
save
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Community für Lese-/Schreibzugriffe festlegen.
Eingerichtete Communities anzeigen.
Speichern der Einstellungen im permanenten Speicher (NVM) im „ausgewählten“ Konfigurationsprofil.


7.2 SNMPv1/v2 ausschalten

Falls Sie SNMPv1 oder SNMPv2 benötigen, verwenden Sie diese Protokolle ausschließlich in abhörsicheren Umgebungen. SNMPv1 und SNMPv2 verwenden keine Verschlüsselung. Die SNMP-Pakete enthalten die Community im Klartext. Wir empfehlen, im Gerät SNMPv3 zu nutzen und den Zugriff über SNMPv1 und SNMPv2 auszuschalten.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SNMP*.

Der Dialog zeigt die Einstellungen des SNMP-Servers.

- Um das Protokoll SNMPv1 zu deaktivieren, heben Sie die Markierung des Kontrollkästchens *SNMPv1* auf.
- Um das Protokoll SNMPv2 zu deaktivieren, heben Sie die Markierung des Kontrollkästchens *SNMPv2* auf.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche  .

```
enable
configure
no snmp access version v1
no snmp access version v2
show snmp access
save
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Deaktivieren des Protokolls SNMPv1.
Deaktivieren des Protokolls SNMPv2.
Einstellungen des SNMP-Servers anzeigen.
Speichern der Einstellungen im permanenten Speicher (NVRAM) im „ausgewählten“ Konfigurationsprofil.

7.3 HTTP ausschalten

Der Webserver liefert die grafische Benutzeroberfläche mit dem Protokoll HTTP oder HTTPS aus. HTTP-Verbindungen sind im Gegensatz zu HTTPS-Verbindungen unverschlüsselt.

Per Voreinstellung ist das Protokoll HTTP eingeschaltet. Wenn Sie HTTP ausschalten, ist kein unverschlüsselter Zugriff auf die grafische Benutzeroberfläche mehr möglich.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTP*.
- Um das Protokoll HTTP auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
no http server
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Ausschalten des Protokolls HTTP.

Wenn das Protokoll HTTP ausgeschaltet ist, erreichen Sie die grafische Benutzeroberfläche des Gerätes ausschließlich über HTTPS. In der Adresszeile des Web-Browsers fügen Sie vor der IP-Adresse des Gerätes die Zeichenfolge `https://` ein.

Wenn das Protokoll HTTPS ausgeschaltet ist und Sie auch HTTP ausschalten, dann ist die grafische Benutzeroberfläche unerreichbar. Um mit der grafischen Benutzeroberfläche zu arbeiten, schalten Sie HTTPS über das Command Line Interface ein.

Führen Sie die folgenden Schritte aus:

```
enable
configure
https server
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Einschalten des Protokolls HTTPS.

7.4 Telnet ausschalten

Das Gerät bietet Ihnen die Möglichkeit, über Telnet oder SSH per Fernzugriff auf die Management-Funktionen des Gerätes zuzugreifen. Telnet-Verbindungen sind im Gegensatz zu SSH-Verbindungen unverschlüsselt.

Per Voreinstellung ist der Telnet-Server im Gerät eingeschaltet. Wenn Sie Telnet ausschalten, ist kein unverschlüsselter Fernzugriff auf das Command Line Interface mehr möglich.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *Telnet*.
- Um den Telnet-Server auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

enable
configure
no telnet server

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Ausschalten des Telnet-Servers.

Wenn der SSH-Server ausgeschaltet ist und Sie auch Telnet ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die V.24-Schnittstelle des Gerätes möglich. Um per Fernzugriff mit dem Command Line Interface zu arbeiten, schalten Sie SSH ein.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- Um den *SSH*-Server einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

enable
configure
ssh server

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Einschalten des SSH-Servers.

7.5 HiDiscovery-Zugriff ausschalten

HiDiscovery bietet Ihnen die Möglichkeit, dem Gerät bei der Inbetriebnahme seine IP-Parameter über das Netz zuzuweisen. HiDiscovery kommuniziert unverschlüsselt und ohne Authentifizierung im Management-VLAN.

Wir empfehlen, nach Inbetriebnahme des Gerätes HiDiscovery ausschließlich Leserechte zu gewähren oder den HiDiscovery-Zugriff vollständig auszuschalten.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Netz*, Registerkarte *Global*.
- Um der HiDiscovery-Software die Schreibrechte zu entziehen, legen Sie im Rahmen *HiDiscovery Protokoll v1/v2*, Feld *Zugriff* den Wert `readOnly` fest.
- Um den HiDiscovery-Zugriff vollständig auszuschalten, wählen Sie im Rahmen *HiDiscovery Protokoll v1/v2* das Optionsfeld .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
enable
network hidiscovery mode read-only
no network hidiscovery operation
```

Wechsel in den Privileged-EXEC-Modus.
Der HiDiscovery-Software die Schreibrechte entziehen.
HiDiscovery-Zugriff ausschalten.

7.6 IP-Zugriffsbeschränkung aktivieren

Per Voreinstellung erreichen Sie die Management-Funktionen des Gerätes von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle.

Die IP-Zugriffsbeschränkung bietet Ihnen die Möglichkeit, den Zugriff auf die Management-Funktionen auf ausgewählte IP-Adressbereiche und auf ausgewählte IP-basierte Protokolle zu beschränken.

Beispiel:

Das Gerät soll ausschließlich aus dem Firmennetz über die grafische Benutzeroberfläche erreichbar sein. Der Administrator soll zusätzlich Fernzugriff per SSH erhalten. Das Firmennetz hat den Adressbereich 192.168.1.0/24 und der Fernzugriff erfolgt aus einem Mobilfunknetz mit dem IP-Adressbereich 109.237.176.0/24. Das SSH-Anwendungsprogramm kennt den Fingerprint des RSA/DSA-Schlüssels.


Parameter	Firmennetz	Mobilfunknetz
Netzadresse	192.168.1.0	109.237.176.0
Netzmaske	24	24
Gewünschte Protokolle	https, snmp	ssh

Tab. 6: Parameter für die IP-Zugriffsbeschränkung


Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung*.
- Heben Sie für den Eintrag in Spalte *Aktiv* die Markierung des Kontrollkästchens auf. Dieser Eintrag ermöglicht den Zugriff auf das Gerät von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle.


Adressbereich des Firmennetzes:

- Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- Legen Sie den Adressbereich des Firmennetzes in Spalte *IP-Adressbereich* fest: 192.168.1.0/24
- Deaktivieren Sie für den Adressbereich des Firmennetzes die ungewünschten Protokolle. Die Kontrollkästchen in den Feldern *HTTPS*, *SNMP* und *Aktiv* bleiben markiert.

Adressbereich des Mobilfunknetzes:

- Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- Legen Sie den Adressbereich des Mobilfunknetzes in Spalte *IP-Adressbereich* fest: 109.237.176.0/24
- Deaktivieren Sie für den Adressbereich des Mobilfunknetzes die ungewünschten Protokolle. Die Kontrollkästchen in den Feldern *SSH* und *Aktiv* bleiben markiert.

Bevor Sie die Funktion einschalten, vergewissern Sie sich, dass mindestens ein aktiver Eintrag in der Tabelle Ihnen den Zugriff ermöglicht. Andernfalls bricht die Verbindung zum Gerät ab, sobald Sie die Einstellungen ändern. Der Zugriff auf die Management-Funktionen ist dann ausschließlich per CLI über die V.24-Schnittstelle des Gerätes möglich.

- Um die IP-Zugriffsbeschränkung einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

Unterstützung beim Schutz vor unberechtigtem Zugriff

7.6 IP-Zugriffsbeschränkung aktivieren

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>show network management access global</code>	Zeigt, ob die IP-Zugriffsbeschränkung eingeschaltet oder ausgeschaltet ist.
<code>show network management access rules</code>	Eingerichtete Einträge anzeigen.
<code>no network management access operation</code>	IP-Zugriffsbeschränkung ausschalten.
<code>network management access add 2</code>	Eintrag für den Adressbereich des Firmennetzes erzeugen. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: 2.
<code>network management access modify 2 ip 192.168.1.0</code>	IP-Adresse des Firmennetzes festlegen.
<code>network management access modify 2 mask 24</code>	Netzmaske des Firmennetzes festlegen.
<code>network management access modify 2 ssh disable</code>	SSH für den Adressbereich des Firmennetzes deaktivieren. Schritt für sämtliche ungewünschten Protokolle wiederholen.
<code>network management access add 3</code>	Eintrag für den Adressbereich des Mobilfunknetzes erzeugen. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: 3.
<code>network management access modify 3 ip 109.237.176.0</code>	IP-Adresse des Mobilfunknetzes festlegen.
<code>network management access modify 3 mask 24</code>	Netzmaske des Mobilfunknetzes festlegen.
<code>network management access modify 3 snmp disable</code>	SNMP für den Adressbereich des Mobilfunknetzes deaktivieren. Schritt für sämtliche ungewünschten Protokolle wiederholen.
<code>no network management access status 1</code>	Voreingestellten Eintrag deaktivieren. Dieser Eintrag ermöglicht den Zugriff auf das Gerät von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle.
<code>network management access status 2</code>	Eintrag für den Adressbereich des Firmennetzes aktivieren.
<code>network management access status 3</code>	Eintrag für den Adressbereich des Mobilfunknetzes aktivieren.
<code>show network management access rules</code>	Eingerichtete Einträge anzeigen.
<code>network management access operation</code>	IP-Zugriffsbeschränkung einschalten.

7.7 Session-Timeouts anpassen

Das Gerät bietet Ihnen die Möglichkeit, bei Inaktivität eines angemeldeten Benutzers die Sitzung automatisch zu beenden. Das Session-Timeout ist die Zeit der Inaktivität nach der letzten Benutzeraktion.

Ein Session-Timeout können Sie für folgende Anwendungen festlegen:

- ▶ CLI-Sitzungen über SSH-Verbindung
- ▶ CLI-Sitzungen über Telnet-Verbindung
- ▶ CLI-Sitzungen über V.24-Verbindung
- ▶ Grafische Benutzeroberfläche

■ Timeout für CLI-Sitzungen über SSH-Verbindung

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- Legen Sie im Rahmen *Konfiguration*, Feld *Session-Timeout [min]* die Timeout-Zeit in Minuten fest.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
enable
configure
ssh timeout <0..160>
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Timeout-Zeit in Minuten festlegen für CLI-Sitzungen über SSH-Verbindung.

■ Timeout für CLI-Sitzungen über Telnet-Verbindung

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *Telnet*.
- Legen Sie im Rahmen *Konfiguration*, Feld *Session-Timeout [min]* die Timeout-Zeit in Minuten fest.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
enable
configure
telnet timeout <0..160>
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Timeout-Zeit in Minuten festlegen für CLI-Sitzungen über Telnet-Verbindung.

■ Session-Timeout für CLI-Sitzungen über V.24-Verbindung

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > CLI*, Registerkarte *Global*.
- Legen Sie im Rahmen *Konfiguration*, Feld *V.24-Timeout [min]* die Timeout-Zeit in Minuten fest.

- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
cli serial-timeout <0..160>
```

Wechsel in den Privileged-EXEC-Modus.
Timeout-Zeit in Minuten festlegen für CLI-Sitzungen über V.24-Verbindung.

■ **Session-Timeout für die grafische Benutzeroberfläche**

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Web*.
- Legen Sie im Rahmen *Konfiguration*, Feld *Web-Interface Session-Timeout [min]* die Timeout-Zeit in Minuten fest.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
network management access web timeout
<0..160>
```

Wechsel in den Privileged-EXEC-Modus.
Timeout-Zeit in Minuten festlegen für Sitzungen mit der grafischen Benutzeroberfläche.

8 Datenverkehr kontrollieren

Das Gerät prüft die zur Weiterleitung bestimmten Datenpakete nach vorgegebenen Regeln. Wenn Datenpakete diesen Regeln entsprechen, leitet das Gerät die Pakete weiter oder blockiert sie. Wenn Datenpakete keinen Regeln entsprechen, blockiert das Gerät die Pakete.

Routing-Ports, denen keine Regeln zugewiesen sind, lassen Pakete passieren. Sobald eine Regel zugewiesen ist, werden zuerst die zugewiesenen Regeln abgearbeitet. Danach wirkt die festgelegte Standard-Aktion des Gerätes.

Zur Kontrolle des Datenstroms bietet das Gerät folgende Funktionen:

- ▶ Prüfen der Dienstanforderungen (Denial of Service, DoS)

Das Gerät beobachtet und überwacht den Datenstrom. Aus den Ergebnissen der Beobachtung und Überwachung sowie aus den Regeln für die Netzsicherheit erzeugt das Gerät eine sogenannte Zustandstabelle. Anhand dieser Zustandstabelle entscheidet das Gerät, ob es die Daten vermittelt, verwirft oder zurückweist.

8.1 Unterstützung beim Schutz vor Denial of Service (DoS)

Mit dieser Funktion unterstützt Sie das Gerät beim Schutz gegen ungültigen oder gefälschten Datenpaketen, der auf den Ausfall bestimmter Dienste oder Geräte abzielt. Sie haben die Möglichkeit, Filter festzulegen, die den Datenstrom zum Schutz vor Denial-of-Service-Angriffen begrenzen. Die aktivierten Filter prüfen eingehende Datenpakete und verwerfen diese, sobald sich eine Übereinstimmung zu den Filterkriterien ergibt.

Der Dialog *Netzsicherheit > DoS > Global* beinhaltet 2 Rahmen, in denen Sie die unterschiedlichen Filter aktivieren können. Zum Aktivieren markieren Sie die betreffenden Kontrollkästchen.

Im Rahmen *TCP/UDP* können Sie bis zu 4 Filter aktivieren, die ausschließlich auf TCP- und UDP-Pakete Einfluss nehmen. Mittels dieser Filter können Sie die Port-Scans deaktivieren, mit deren Hilfe Angreifer versuchen könnten, Geräte und angebotene Dienste zu erkennen. Die Filter arbeiten wie folgt:

Filter	Aktion
Null-Scan-Filter aktivieren	Das Gerät erkennt TCP-Pakete, bei denen keine TCP-Flags gesetzt sind und verwirft diese.
Xmas-Filter aktivieren	Das Gerät erkennt TCP-Pakete, bei denen die TCP-Flags FIN, URG und PUSH gleichzeitig gesetzt sind und verwirft diese.
SYN/FIN-Filter aktivieren	Das Gerät erkennt TCP-Pakete, bei denen die TCP-Flags SYN und FIN gleichzeitig gesetzt sind und verwirft diese.
Minimal-Header-Filter aktivieren	Das Gerät erkennt TCP-Pakete, bei denen der TCP-Header zu kurz ist und verwirft diese.

Tab. 7: DoS-Filter für TCP-Pakete

Der Rahmen *ICMP* bietet Ihnen 2 Filtermöglichkeiten für ICMP-Pakete. Die Fragmentierung eingehender ICMP-Pakete lässt grundsätzlich auf einen Angriff schließen. Wenn Sie diesen Filter aktivieren, erkennt das Gerät fragmentierte ICMP-Pakete und verwirft diese. Über den Parameter *Erlaubte Paketgröße [Byte]* können Sie zudem die maximal zulässige Größe der Nutzlast von ICMP-Paketen festlegen. Das Gerät verwirft Datenpakete, welche diese Byte-Angabe überschreiten.

Anmerkung: Sie können die Filter im Dialog *Netzsicherheit > DoS > Global* beliebig kombinieren. Bei Auswahl mehrerer Filter gilt ein logisches Oder: Das Gerät verwirft ein Datenpaket, wenn es auf den ersten oder den zweiten (oder den dritten usw.) Filter zutrifft.

9 Die Systemzeit im Netz synchronisieren

Viele Anwendungen sind auf eine möglichst korrekte Zeit angewiesen. Die notwendige Genauigkeit, also die zulässige Abweichung zur Echtzeit, hängt vom Anwendungsgebiet ab.

Anwendungsgebiete sind beispielsweise:

- ▶ Logbucheinträge
- ▶ Produktionsdaten mit Zeitstempel versehen
- ▶ Prozesssteuerung

Das Gerät bietet folgende Möglichkeiten, die Zeit im Netz zu synchronisieren:

- ▶ Das Simple Network Time Protocol (SNTP) ist eine einfache Lösung für geringere Genauigkeitsanforderungen. Unter idealen Bedingungen erzielt SNTP eine Genauigkeit im Millisekunden-Bereich. Die Genauigkeit ist abhängig von der Signallaufzeit.
- ▶ IEEE 1588 mit dem Precision Time Protocol (PTP) erreicht eine Genauigkeit im Submikrosekunden-Bereich. Diese Methode eignet sich auch für anspruchsvolle Anwendungen bis hin zur Prozesssteuerung.

PTP ist immer dann die bessere Wahl, wenn die beteiligten Geräte dieses Protokoll unterstützen. PTP ist exakter, verfügt über fortgeschrittene Methoden zur Fehlerkorrektur und verursacht eine geringe Netzlast. Die Implementation von PTP ist vergleichsweise einfach.

Anmerkung: Laut PTP- und SNTP-Standard funktionieren beide Protokolle parallel in einem Netz. Da beide Protokolle die Systemzeit des Gerätes beeinflussen, sind Situationen denkbar, in denen beide Protokolle konkurrieren.

Das Gerät verfügt zudem über 2 spezielle Ausgänge für die Synchronisation anderer Geräte. Ein Ausgang stellt die Gerätezeit als IRIG-B-Signal zur Verfügung, ein zweiter Ausgang ein PPS-Frequenzsignal (1 Puls pro Sekunde).

9.1 Grundeinstellungen

Im Dialog *Zeit > Grundeinstellungen* legen Sie allgemeine Einstellungen für die Zeit fest.

9.1.1 Uhrzeit einstellen

Steht Ihnen keine Referenzzeitquelle zur Verfügung, haben Sie die Möglichkeit, im Gerät die Uhrzeit einzustellen.

Sofern keine Echtzeituhr vorhanden ist oder diese eine ungültige Zeit übermittelt, initialisiert das Gerät nach einem Kalt- oder Neustart seine Uhr auf den 1. Januar, 00:00 Uhr. Nach Abschalten der Stromzufuhr puffert das Gerät die Einstellungen der Echtzeituhr bis zu 24 Stunden lang.

Alternativ legen Sie die Einstellungen im Gerät so fest, dass es die aktuelle Uhrzeit automatisch von einer PTP-Uhr oder von einem SNTP-Server bezieht.

Alternativ legen Sie die Einstellungen im Gerät so fest, dass es die aktuelle Uhrzeit automatisch von einem SNTP-Server bezieht.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Zeit > Grundeinstellungen*.
 - ▶ Das Feld *Systemzeit (UTC)* zeigt die aktuelle UTC (Universal Time Coordinated) des Gerätes an. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die UTC ist weltweit gleich und berücksichtigt keine lokalen Zeitverschiebungen.
 - ▶ Die Zeit im Feld *Systemzeit* ergibt sich aus der *Systemzeit (UTC)* zuzüglich dem Wert *Lokaler Offset [min]* sowie einer möglichen Verschiebung durch die Sommerzeit.
- Damit das Gerät die Zeit Ihres PCs in das Feld *Systemzeit* übernimmt, klicken Sie die Schaltfläche *Setze Zeit vom PC*.

Anhand des Werts im Feld *Lokaler Offset [min]* berechnet das Gerät die Zeit im Feld *Systemzeit (UTC)*: Die Zeit im Feld *Systemzeit (UTC)* ergibt sich aus der *Systemzeit* abzüglich dem Wert *Lokaler Offset [min]* sowie einer möglichen Verschiebung durch die Sommerzeit.

 - ▶ Das Feld *Quelle der Zeit* zeigt den Ursprung der Zeitangabe an. Das Gerät wählt automatisch die Quelle mit der höchsten Genauigkeit.

Die Quelle ist zunächst `local`.
Ist SNTP aktiviert und empfängt das Gerät ein gültiges SNTP-Paket, setzt es seine Zeitquelle auf `sntp`.
Ist PTP aktiviert und empfängt das Gerät eine gültige PTP-Nachricht, setzt es seine Zeitquelle auf `ptp`. Das Gerät gibt der Zeitquelle PTP den Vorrang vor SNTP.
 - ▶ Der Wert *Lokaler Offset [min]* legt die Zeitdifferenz fest zwischen der lokalen Zeit und der *Systemzeit (UTC)*.
- Damit das Gerät die Zeitzone Ihres PCs ermittelt, klicken Sie die Schaltfläche *Setze Zeit vom PC*. Das Gerät berechnet daraus die lokale Zeitdifferenz zur UTC-Zeit und trägt die Differenz in das Feld *Lokaler Offset [min]* ein.

Anmerkung: Das Gerät bietet die Möglichkeit, den lokalen Offset von einem DHCP-Server beziehen.

- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
enable
configure
clock set <YYYY-MM-DD> <HH:MM:SS>
clock timezone offset <-780..840>

save
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Einstellen der Systemzeit des Gerätes.
Eingabe der Zeitdifferenz zwischen der lokalen Zeit und der empfangenen UTC-Zeit in Minuten.
Speichern der Einstellungen im permanenten Speicher (NVRAM) im „ausgewählten“ Konfigurationsprofil.

9.1.2 Automatische Sommerzeitumschaltung

Wenn Sie das Gerät in einer Zeitzone betreiben, in der es die Sommerzeitumschaltung gibt, so richten Sie auf der Registerkarte *Sommerzeit* die automatische Sommerzeitumstellung ein.

Wenn die Sommerzeitumschaltung aktiviert ist, erhöht das Gerät zu Beginn der Sommerzeit die lokale Systemzeit um 1 Stunde. Zum Ende der Sommerzeit reduziert das Gerät die lokale Systemzeit wieder um 1 Stunde.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Zeit > Grundeinstellungen*, Registerkarte *Sommerzeit*.
- Um ein ein vordefiniertes Profil für Beginn und Ende der Sommerzeit auszuwählen, klicken Sie im Rahmen *Funktion* die Schaltfläche *Profil...*
- Wenn kein passendes Sommerzeitprofil verfügbar ist, dann legen Sie in den Feldern *Sommerzeit Beginn* und *Sommerzeit Ende* die Zeitpunkte der Zeitumstellung fest. Für beide Zeitpunkte legen Sie den Monat, die Woche innerhalb dieses Monats, den Wochentag sowie die Uhrzeit fest.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
enable
configure
clock summer-time mode
<disable|recurring|eu|usa>
clock summer-time recurring start
clock summer-time recurring end
save
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Konfigurieren der automatischen Sommerzeitumstellung: einschalten, ausschalten oder mit Profil aktivieren.
Eingabe des Startzeitpunkts für die Umschaltung.
Eingabe des Endzeitpunkts für die Umschaltung.
Speichern der Einstellungen im permanenten Speicher (NVRAM) im „ausgewählten“ Konfigurationsprofil.

9.2 SNTP

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

Der SNTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die UTC ist weltweit gleich und ignoriert lokale Zeitverschiebungen.

SNTP ist eine vereinfachte Version des NTP (Network Time Protocol). Die Datenpakete sind bei SNTP und NTP identisch aufgebaut. Demzufolge dienen sowohl NTP- als auch SNTP-Server als Zeitquelle für SNTP-Clients.

Anmerkung: Aussagen in diesem Kapitel, die sich auf externe SNTP-Server beziehen, gelten ebenso für NTP-Server.

SNTP kennt die folgenden Betriebsmodi zur Übertragung der Zeit:

- ▶ **Unicast**
Im Unicast-Betriebsmodus sendet ein SNTP-Client Anfragen an einen SNTP-Server und erwartet eine Antwort von diesem Server.
- ▶ **Broadcast**
Im Broadcast-Betriebsmodus sendet ein SNTP-Server in definierten Abständen SNTP-Nachrichten in das Netz aus. SNTP-Clients empfangen diese SNTP-Nachrichten und werten sie aus.

IP-Zieladresse	SNTP-Pakete senden an
0.0.0.0	Niemand
224.0.1.1	Multicast-Adresse für SNTP-Nachrichten
255.255.255.255	Broadcast-Adresse

Tab. 8: Zieladressklassen für den Broadcast-Betriebsmodus

Anmerkung: Ein SNTP-Server im Broadcast-Betriebsmodus beantwortet auch direkte Anfragen per Unicast von SNTP-Clients. SNTP-Clients arbeiten hingegen entweder im Unicast- oder im Broadcast-Betriebsmodus.

9.2.1 Vorbereitung

Führen Sie die folgenden Schritte aus:

- Zeichnen Sie einen Netzplan mit den am SNTP beteiligten Geräten, um einen Überblick über die Weitergabe der Uhrzeit zu erhalten.

Beachten Sie bei der Planung, dass die Genauigkeit der Uhrzeit von den Laufzeiten der SNTP-Nachrichten abhängig ist. Um die Laufzeiten und deren Varianz zu minimieren, platzieren Sie in jedem Netzsegment einen SNTP-Server. Jeder dieser SNTP-Server synchronisiert seine eigene Systemzeit als SNTP-Client am jeweils übergeordneten SNTP-Server (SNTP-Kaskade). Der oberste SNTP-Server in der SNTP-Kaskade hat möglichst direkten Zugriff auf eine Referenzzeitquelle.

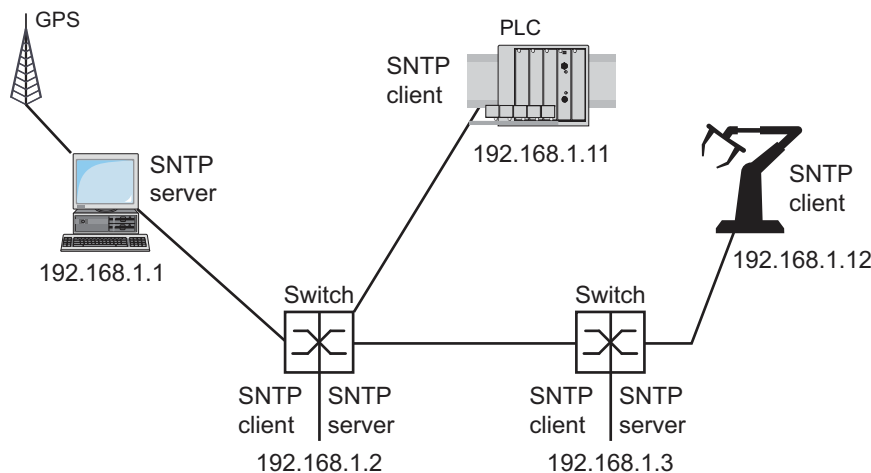


Abb. 17: Beispiel SNTP-Kaskade

Anmerkung: Für eine genaue Zeitverteilung verwenden Sie zwischen SNTP-Servern und SNTP-Clients bevorzugt Netzkomponenten (Router und Switches), die SNTP-Pakete mit möglichst geringer und gleichmäßiger Durchlaufzeit (Latenz) weiterleiten.

- Ein SNTP-Client sendet seine Anfragen an bis zu 4 konfigurierte SNTP-Server. Bleibt die Antwort des 1. SNTP-Servers aus, sendet der SNTP-Client seine Anfragen an den 2. SNTP-Server. Ist auch diese Anfrage erfolglos, so versucht er die Anfrage beim 3. und schließlich beim 4. SNTP-Server. Antwortet keiner dieser SNTP-Server, so verliert der SNTP-Client seine Synchronisation. Der SNTP-Client fragt solange zyklisch nacheinander bei den SNTP-Servern an, bis ein Server eine gültige Zeit liefert.



Anmerkung: Das Gerät bietet die Möglichkeit, eine Liste von SNTP-Server-IP-Adressen von einem DHCP-Server beziehen.

- Wenn Sie keine Referenzzeitquelle zur Verfügung haben, bestimmen Sie ein Gerät mit SNTP-Server zur Referenzzeitquelle. Justieren Sie dessen Systemzeit turnusmäßig.

9.2.2 Einstellungen des SNTP-Clients festlegen

Als SNTP-Client bezieht das Gerät die Zeitinformationen von SNTP- oder NTP-Servern und synchronisiert seine Systemuhr dementsprechend.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Zeit > SNTP > Client*.
- Legen Sie den SNTP-Betriebsmodus fest.
Markieren Sie im Rahmen *Konfiguration*, Feld *Modus* einen der folgenden Werte:
 - ▶ unicast
Das Gerät sendet Anfragen an einen SNTP-Server und erwartet von diesem Server eine Antwort.
 - ▶ broadcast
Das Gerät wartet auf Broadcast-Nachrichten von SNTP-Servern im Netz.
- Um die Zeit ausschließlich ein einziges Mal zu synchronisieren, markieren Sie das Kontrollkästchen *Deaktiviere Client nach erfolgreicher Synchronisierung*.
Nach erfolgreicher Synchronisation schaltet das Gerät die *SNTP Client*-Funktion aus.
 - ▶ Die Tabelle zeigt die SNTP-Server, die der SNTP-Client im Unicast-Betriebsmodus anfragt. Die Tabelle enthält bis zu 4 SNTP-Server-Definitionen.
- Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- Legen Sie die Verbindungsdaten des SNTP-Servers fest.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
- ▶ Das Feld *Zustand* zeigt den aktuellen Status der *SNTP Client*-Funktion.

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Client -Funktion	Aus	An	An	An	An
Konfiguration : <i>Modus</i>	unicast	unicast	unicast	unicast	unicast
Request-Intervall [s]	30	30	30	30	30
SNTP Server -Adresse(n)	–	192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.3 192.168.1.2 192.168.1.1

Tab. 9: Einstellungen der SNTP-Clients für das Beispiel

9.2.3 Einstellungen des SNTP-Servers festlegen

Wenn das Gerät als SNTP-Server arbeitet, stellt es seine Systemzeit als koordinierte Weltzeit (UTC) im Netz zur Verfügung.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Zeit > SNTP > Server*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .

- Um den Broadcast-Betriebsmodus einzuschalten, markieren Sie im Rahmen *Konfiguration* das Kontrollkästchen *Broadcast-Admin-Modus*.
Im Broadcast-Betriebsmodus sendet der SNTP-Server in definierten Abständen SNTP-Nachrichten in das Netz aus. Außerdem beantwortet der SNTP-Server Anfragen von SNTP-Clients im Unicast-Betriebsmodus.
 - Im Feld *Broadcast-Ziel-Adresse* legen Sie die IP-Adresse fest, an die der SNTP-Server die SNTP-Pakete sendet. Legen Sie eine Broadcast-Adresse oder eine Multicast-Adresse fest.
 - Im Feld *Broadcast-UDP-Port* legen Sie die Nummer des UDP-Ports fest, auf dem der SNTP-Server die SNTP-Pakete im Broadcast-Betriebsmodus sendet.
 - Im Feld *Broadcast VLAN-ID* legen Sie die ID des VLANs fest, in welches der SNTP-Server die SNTP-Pakete im Broadcast-Betriebsmodus sendet.
 - Im Feld *Broadcast-Sende-Intervall [s]* legen Sie den Zeitabstand fest, in dem der SNTP-Server die SNTP-Pakete im Broadcast-Betriebsmodus sendet.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
- ▶ Das Feld *Zustand* zeigt den aktuellen Status der *SNTP Server*-Funktion.

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Server -Funktion	An	An	An	Aus	Aus
UDP-Port	123	123	123	123	123
Broadcast-Admin-Modus	unmarkiert	unmarkiert	unmarkiert	unmarkiert	unmarkiert
Broadcast-Ziel-Adresse	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast-UDP-Port	123	123	123	123	123
Broadcast VLAN-ID	1	1	1	1	1
Broadcast-Sende-Intervall [s]	128	128	128	128	128
Server deaktivieren bei lokaler Zeitquelle	unmarkiert	unmarkiert	unmarkiert	unmarkiert	unmarkiert

Tab. 10: Einstellungen für das Beispiel

9.3 PTP

Damit über ein LAN gesteuerte Anwendungen ohne Latenz arbeiten, ist ein präzises Zeitmanagement erforderlich. IEEE 1588 beschreibt mit PTP (Precision Time Protocol) ein Verfahren, das die präzise Synchronisation der Uhren im Netz ermöglicht.

Das PTP erlaubt die Synchronisation mit einer Genauigkeit bis zu wenigen 100 ns. PTP verwendet Multicasts für die Synchronisationsnachrichten, dadurch ist die Netzlast gering.

9.3.1 Typen von Uhren

Das PTP definiert für die Uhren im Netz die Rollen „Master“ und „Slave“:

- ▶ Eine Master-Uhr (Referenzzeitquelle) verteilt ihre Zeit.
- ▶ Eine Slave-Uhr synchronisiert sich auf das von der Master-Uhr empfangene Zeitsignal.

■ Boundary-Clock

Die Durchlaufzeit (Latenz) in Routern und Switches wirkt sich messbar auf die Präzision der Zeitübertragung aus. Um solche Ungenauigkeiten zu korrigieren, definiert PTP sogenannte Boundary-Clocks.

Eine Boundary-Clock ist die Referenzzeitquelle (Master-Uhr) in einem Netzsegment, auf die sich die untergeordneten Slave-Uhren synchronisieren. Typischerweise übernehmen Router und Switches die Rolle der Boundary-Clock.

Die Boundary-Clock bezieht ihrerseits die Uhrzeit von einer übergeordneten Referenzzeitquelle (Grandmaster).

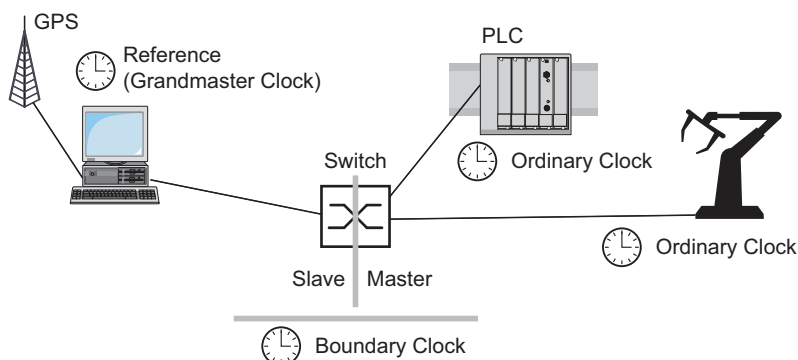


Abb. 18: Position der Boundary-Clock in einem Netz

■ **Transparent Clock**

Typischerweise übernehmen Switches die Rolle der Transparent Clock, um über Kaskaden hinweg eine hohe Genauigkeit zu ermöglichen. Die Transparent Clock ist eine Slave-Uhr, die beim Weiterleiten empfangener Synchronisationsnachrichten die eigene Durchlaufzeit korrigiert.

■ **Ordinary Clock**

Die Uhr in einem Endgerät bezeichnet PTP als „Ordinary Clock“. Eine Ordinary Clock funktioniert entweder als Master-Uhr oder als Slave-Uhr.

9.3.2 **Best-Master-Clock-Algorithmus**

Die an PTP beteiligten Geräte bestimmen ein Gerät im Netz zur Referenzzeitquelle (Grandmaster). Dabei kommt der „Best Master Clock“-Algorithmus zum Einsatz, der die Genauigkeit der verfügbaren Uhren im Netz ermittelt.

Der „Best Master Clock“-Algorithmus bewertet dabei folgende Kriterien:

- ▶ *Priorität 1*
- ▶ *Uhren-Klasse*
- ▶ *Präzision*
- ▶ *Uhren-Varianz*
- ▶ *Priorität 2*

Der Algorithmus bewertet zuerst den Wert im Feld *Priorität 1* der beteiligten Geräte. Das Gerät mit dem kleinsten Wert im Feld *Priorität 1* wird Referenzzeitquelle (Grandmaster). Ist der Wert bei mehreren Geräten gleich, zieht der Algorithmus das nächste Kriterium heran, bei erneuter Übereinstimmung das jeweils nächste Kriterium. Sind sämtliche Werte bei mehreren Geräten gleich, entscheidet der kleinste Wert im Feld *Uhr-Kennung*, welches Gerät Referenzzeitquelle (Grandmaster) wird.

Das Gerät bietet Ihnen die Möglichkeit, in den Einstellungen der Boundary-Clock den Wert für *Priorität 1* und *Priorität 2* individuell festzulegen. Damit haben Sie selbst Einfluss darauf, welches Gerät die Referenzzeitquelle (Grandmaster) im Netz wird.

9.3.3 Laufzeitmessung

Die Laufzeit der Synchronisationsnachrichten zwischen den beteiligten Geräten hat Einfluss auf die Genauigkeit. Durch die Laufzeitmessung berücksichtigen die Geräte die mittlere Laufzeit.

PTP Version 2 bietet folgende Verfahren für die Laufzeitmessung:

- ▶ (End to End)
Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
- ▶ e2e-optimized
Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
Dieses Verfahren ist ausschließlich für Transparent-Clocks verfügbar. Das Gerät vermittelt die per Multicast gesendeten Synchronisationsnachrichten ausschließlich an die Master-Uhr und hält dadurch die Netzlast gering. Wenn das Gerät eine Synchronisationsnachricht von einer anderen Master-Uhr empfängt, vermittelt es die Synchronisationsnachrichten ausschließlich an diesen neuen Port.
Kennt das Gerät keine Master-Uhr, vermittelt es Synchronisationsnachrichten an jeden Port.
- ▶ (Peer to Peer)
Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
Zusätzlich misst die Master-Uhr die Laufzeit zu jeder Slave-Uhr, auch über blockierte Ports hinweg.
Voraussetzung ist, dass Master- und Slave-Uhr Peer-to-Peer (p2p) unterstützen.
Bei Unterbrechung eines redundanten Rings beispielsweise wird eine Slave-Uhr zur Master-Uhr und die Master-Uhr zur Slave-Uhr. Dieser Wechsel findet ohne Präzisionsverlust statt, weil die Uhren die Laufzeit in die andere Richtung bereits kennen.

Anmerkung: Wenn Sie den Wert festlegen, können Sie in Spalte *Netz-Protokoll* ausschließlich den Wert `IEEE 802.3` festlegen.

9.3.4 PTP-Domänen

Synchronisationsnachrichten überträgt das Gerät ausschließlich von und zu Geräten in derselben PTP-Domäne. Das Gerät bietet Ihnen die Möglichkeit, die Domäne für die Boundary-Clock und für die Transparent-Clock individuell festzulegen.

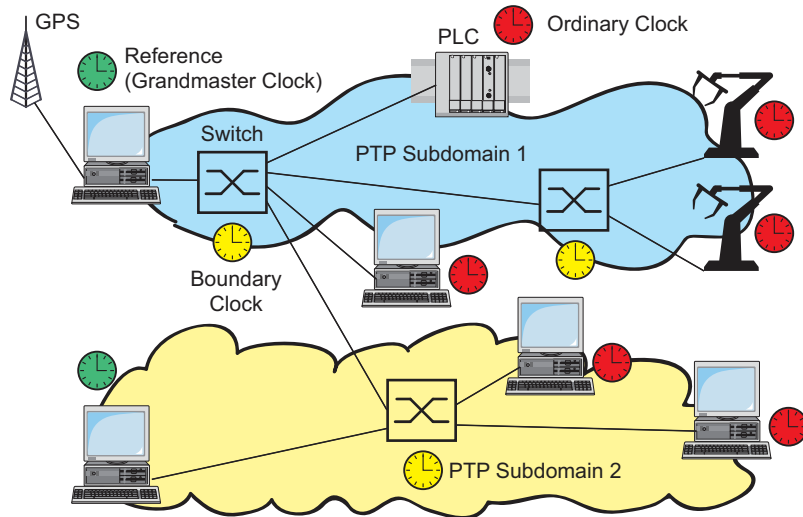


Abb. 19: Beispiel für PTP-Domänen

9.3.5 PTP verwenden

Um die Uhren präzise mit PTP zu synchronisieren, verwenden Sie als Netzknoten ausschließlich Switches mit Boundary-Clock oder Transparent-Clock.

Führen Sie die folgenden Schritte aus:

- Um sich einen Überblick über die Uhrenverteilung zu verschaffen, zeichnen Sie einen Netzplan mit den am PTP beteiligten Geräten.
- Legen Sie für jeden beteiligten Switch die Rolle fest (Boundary-Clock oder Transparent-Clock). Im Gerät heißt diese Einstellung *PTP-Modus*.

PTP-Modus	Anwendung
v2-boundary-clock	Als Boundary-Clock verteilt das Gerät die Synchronisationsnachrichten an die Slave-Uhren im untergeordneten Netzsegment. Die Boundary-Clock bezieht ihrerseits die Uhrzeit von einer übergeordneten Referenzzeitquelle (Grandmaster).
v2-transparent-clock	Als Transparent-Clock leitet das Gerät empfangene Synchronisationsnachrichten korrigiert um die eigene Durchlaufzeit weiter.

Tab. 11: Mögliche Einstellwerte für den PTP-Modus

- Schalten Sie PTP auf jedem beteiligten Switch ein.
PTP konfiguriert sich anschließend weitestgehend automatisch.
- Schalten Sie PTP auf den Endgeräten ein.
- Sie können Einfluss darauf nehmen, welches Gerät im Netz Referenzzeitquelle (Grandmaster) wird.
Ändern Sie dazu für die Boundary Clock den voreingestellten Wert in den Feldern *Priorität 1* und *Priorität 2*.

9.4 IRIG-B/PPS

Ihr Gerät verfügt über die folgenden Ausgänge, auf denen es hochexakte Zeit- und Frequenzsignale für andere Geräte bereitstellt:

- ▶ IRIG-B
Am IRIG-B-Ausgang sendet das Gerät wahlweise die koordinierte Weltzeit (UTC) oder seine lokale Systemzeit mit einer Frequenz von 100 Impulsen pro Sekunde. Die Zeitsignale entsprechen dem IRIG-Zeitcode-Standard, der unterschiedliche Zeitformate zur Auswahl anbietet.
- ▶ PPS
Der PPS-Ausgang (Pulse per Second) stellt ein hochexaktes Frequenzsignal zur Verfügung. Die Periodendauer des Pulses beträgt 1 Sekunde (200 ms High-Pegel, 800 ms Low-Pegel).

Schließen Sie an beiden Ausgängen ausschließlich Geräte an, die über entsprechende Signaleingänge verfügen und die Signale verarbeiten können.

9.4.1 Vorbereitung

Führen Sie die folgenden Schritte aus:

- Prüfen Sie die Eignung des anzuschließenden Endgerätes für den jeweiligen Signalausgang.
- Klären Sie, welche IRIG-Zeitformate das anzuschließende Endgerät verarbeitet.
- Der IRIG-B-Ausgang stellt die Zeit als koordinierte Weltzeit (UTC) oder als lokale Zeit bereit. Prüfen Sie, welche Option in Ihrem Anwendungsfall besser geeignet ist.

Code	Zeitformat
irig-b000	Signal enthält BCDtoy, CF, SBS (siehe Legende am Tabellenende).
irig-b001	Signal enthält BCDtoy, CF.
irig-b002	Signal enthält BCDtoy.
irig-b003	Signal enthält BCDtoy, SBS (Voreinstellung).
irig-b004	Signal enthält BCDtoy, BCDyear, CF, SBS.
irig-b005	Signal enthält BCDtoy, BCDyear, CF.
irig-b006	Signal enthält BCDtoy, BCDyear.
irig-b007	Signal enthält BCDtoy, BCDyear, SBS.

Legende

BCDtoy	Binary Coded Decimal time of year Zeit innerhalb des Jahres als dualkodierter Dezimalziffernwert
BCDyear	Binary Coded Decimal year Jahr als dualkodierter Dezimalziffernwert
CF	Control Functions (nach IEEE 1344)
SBS	Straight Binary Seconds of day Tagessekunde, 0...86400

Tab. 12: Zulässige Codes für unterschiedliche IRIG-Zeitformate

9.4.2 IRIG-B einschalten

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Zeit > IRIG-B/PPS*, Registerkarte *IRIG-B*.
- Markieren Sie im Feld *Modus* das gewünschte IRIG-Zeitformat.
- Markieren Sie im Feld *Zeit-Modus* die auszugebende Uhrzeit.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

9.4.3 PPS einschalten

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Zeit > IRIG-B/PPS*, Registerkarte *PPS*.
- Um die Ausgabe der Frequenzsignale einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

10 Netzlaststeuerung

Das Gerät bietet Ihnen eine Reihe von Funktionen, mit denen es die Netzlast reduziert:

- ▶ Gezielte Paketvermittlung
- ▶ Multicasts
- ▶ Lastbegrenzung
- ▶ Priorisierung - QoS
- ▶ Flusskontrolle

10.1 Gezielte Paketvermittlung

Durch gezielte Paketvermittlung reduziert das Gerät die Netzlast.

An jedem seiner Ports lernt das Gerät die Absender-MAC-Adresse empfangener Datenpakete. Die Kombination „Port und MAC-Adresse“ speichert das Gerät in seiner MAC-Adresstabelle (FDB).

Durch Anwenden des „Store and Forward“-Verfahrens speichert das Gerät empfangene Daten zwischen und prüft sie vor dem Weiterleiten auf Gültigkeit. Ungültige und fehlerhafte Datenpakete verwirft das Gerät.

10.1.1 Lernen der MAC-Adressen

Wenn das Gerät ein Datenpaket empfängt, prüft es, ob die MAC-Adresse des Absenders bereits in der MAC-Adresstabelle (FDB) gespeichert ist. Ist die MAC-Adresse des Absenders noch unbekannt, erzeugt das Gerät einen neuen Eintrag. Anschließend vergleicht das Gerät die Ziel-MAC-Adresse des Datenpakets mit den in der MAC-Adresstabelle (FDB) gespeicherten Einträgen:

- ▶ Datenpakete mit bekannter Ziel-MAC-Adresse vermittelt das Gerät gezielt an Ports, die bereits Datenpakete von dieser MAC-Adresse empfangen haben.
- ▶ Datenpakete mit unbekannter Zieladresse flutet das Gerät, d. h. das Gerät leitet diese Datenpakete an sämtliche Ports weiter.

10.1.2 Aging gelernter MAC-Adressen

Adressen, die das Gerät seit einer einstellbaren Zeitspanne (Aging-Zeit) nicht noch einmal erkannt hat, löscht das Gerät aus der MAC-Adresstabelle (FDB). Ein Neustart oder das Zurücksetzen der MAC-Adresstabelle löscht die Einträge in der MAC-Adresstabelle (FDB).

10.1.3 Statische Adresseinträge

Ergänzend zum Lernen der Absender-MAC-Adresse bietet Ihnen das Gerät die Möglichkeit, MAC-Adressen von Hand einzurichten. Diese MAC-Adressen bleiben eingerichtet und überdauern das Zurücksetzen der MAC-Adresstabelle (FDB) sowie den Neustart des Gerätes.

Anhand von statischen Adresseinträgen bietet Ihnen das Gerät die Möglichkeit, Datenpakete gezielt an ausgewählte Ports zu vermitteln. Wenn Sie keinen Ziel-Port festlegen, verwirft das Gerät betreffende Datenpakete.

Die statischen Adresseinträge verwalten Sie in der grafischen Benutzeroberfläche (GUI) oder im CLI.

Führen Sie die folgenden Schritte aus:

Statischen Adresseintrag erzeugen.

Öffnen Sie den Dialog *Switching > Filter für MAC-Adressen*.

Fügen Sie eine benutzerdefinierte MAC-Adresse hinzu:

▶ Klicken Sie die Schaltfläche .

Der Dialog zeigt das Fenster *Erzeugen*.

▶ Legen Sie im Feld *Adresse* die Ziel-MAC-Adresse fest.

▶ Legen Sie im Feld *VLAN-ID* die ID des VLANs fest.

▶ Markieren Sie in der Liste *Port* die Ports, an die das Gerät Datenpakete mit der angegebenen Ziel-MAC-Adresse im angegebenen VLAN vermittelt.

Markieren Sie genau einen Port, wenn Sie im Feld *Adresse* eine Unicast-MAC-Adresse festgelegt haben.

Markieren Sie einen oder mehrere Ports, wenn Sie im Feld *Adresse* eine Multicast-MAC-Adresse festgelegt haben.


Markieren Sie keinen Port, damit das Gerät Datenpakete mit der Ziel-MAC-Adresse verwirft.

▶ Klicken Sie die Schaltfläche *Ok*.


- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

<pre>enable configure mac-filter <MAC address> <VLAN ID> interface 1/1 mac-filter <MAC address> <VLAN ID> save</pre>	<p>Wechsel in den Privileged-EXEC-Modus. Wechsel in den Konfigurationsmodus. Erzeugen des MAC-Adressfilters, bestehend aus MAC-Adresse und VLAN-ID. Wechsel in den Interface-Konfigurationsmodus von Interface 1/1. Weist dem Port einen bereits erzeugten MAC-Adressfilter zu. Speichern der Einstellungen im permanenten Speicher (NVRAM) im „ausgewählten“ Konfigurationsprofil.</p>
--	---

- Gelernte MAC-Adresse in statischen Adresseintrag umwandeln.

- Öffnen Sie den Dialog *Switching* > *Filter für MAC-Adressen*.
- Um eine gelernte MAC-Adresse in einen statischen Adresseintrag umzuwandeln, markieren Sie in Spalte *Status* den Wert *permanent*.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

- Statischen Adresseintrag deaktivieren.

- Öffnen Sie den Dialog *Switching* > *Filter für MAC-Adressen*.
- Um einen statischen Adresseintrag zu deaktivieren, markieren Sie in Spalte *Status* den Wert *invalid*.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

<pre>enable configure interface 1/1 no mac-filter <MAC address> <VLAN ID> exit no mac-filter <MAC address> <VLAN ID> exit save</pre>	<p>Wechsel in den Privileged-EXEC-Modus. Wechsel in den Konfigurationsmodus. Wechsel in den Interface-Konfigurationsmodus von Interface 1/1. Hebt auf dem Port die Zuweisung des MAC-Adressfilters auf. Wechsel in den Konfigurationsmodus. Löschen des MAC-Adressfilters, bestehend aus MAC-Adresse und VLAN-ID. Wechsel in den Privileged-EXEC-Modus. Speichern der Einstellungen im permanenten Speicher (NVRAM) im „ausgewählten“ Konfigurationsprofil.</p>
--	---

- Gelernte MAC-Adressen löschen.

- Um die gelernten Adressen aus der MAC-Adresstabelle (FDB) zu löschen, öffnen Sie den Dialog *Grundeinstellungen* > *Neustart* und klicken die Schaltfläche *MAC-Adresstabelle zurücksetzen*.

<pre>clear mac-addr-table</pre>	<p>Löschen der gelernten MAC-Adressen aus der MAC-Adresstabelle (FDB).</p>
---------------------------------	--

10.2 Multicasts

In der Grundeinstellung flutet das Gerät Datenpakete mit einer Multicast-Adresse, d.h. das Gerät leitet diese Datenpakete an sämtliche Ports weiter. Dies führt zu erhöhter Netzlast.

Durch den Einsatz von IGMP-Snooping lässt sich die Netzlast reduzieren, die der Multicast-Datenverkehr verursacht. IGMP-Snooping ermöglicht dem Gerät, Multicast-Datenpakete ausschließlich an diejenigen Ports zu vermitteln, an denen am Multicast „interessierte“ Geräte angeschlossen sind.

10.2.1 Beispiel für eine Multicast-Anwendung

Überwachungskameras übertragen Bilder auf Monitore im Maschinenraum und im Überwachungsraum. Bei einer IP-Multicast-Übertragung senden die Kameras ihre Bilddaten in Multicast-Paketen über das Netz.

Das Internet Group Management Protocol (IGMP) organisiert den Multicast-Datenverkehr zwischen den Multicast-Routern und den Monitoren. Die Switches, die im Netz zwischen den Multicast-Routern und den Monitoren liegen, beobachten den IGMP-Datenverkehr kontinuierlich („IGMP Snooping“).

Switches registrieren Anmeldungen für den Empfang eines Multicast-Stroms (IGMP-Report). Daraufhin erzeugt das Gerät einen Eintrag in der MAC-Adresstabelle (FDB) und leitet Multicast-Pakete ausschließlich an die Ports weiter, an denen es zuvor IGMP-Reports empfangen hat.

10.2.2 IGMP-Snooping

Das Internet Group Management Protocol (IGMP) beschreibt die Verteilung von Multicast-Informationen zwischen Routern und angeschlossenen Empfängern auf Schicht 3. IGMP Snooping beschreibt die Funktion eines Switches, kontinuierlich den IGMP-Datenverkehr zu beobachten und die eigenen Vermittlungseinstellungen für diesen Datenverkehr zu optimieren.

Die IGMP-Snooping-Funktion im Gerät funktioniert gemäß RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Multicast-Router mit aktiver *IGMP*-Funktion fordern periodisch zur Registrierung von Multicast-Strömen auf (Query), um die angeschlossenen IP-Multicast-Gruppen-Mitglieder zu ermitteln. IP-Multicast-Gruppen-Mitglieder antworten mit einer Report-Nachricht. Diese Report-Nachricht enthält für die *IGMP*-Funktion notwendige Parameter. Der Multicast-Router trägt die IP-Multicast-Gruppen-Adresse aus der Report-Nachricht in seine Router-Tabelle ein. Dies bewirkt, dass er Datenpakete mit dieser IP-Multicast-Gruppen-Adresse im Zieladressfeld entsprechend seiner Router-Tabelle weiterleitet.

Empfänger melden sich beim Verlassen einer Multicast-Gruppe mit einer „Leave“-Nachricht ab (ab IGMP-Version 2) und senden keine Report-Nachrichten mehr. Der Multicast-Router entfernt den Routing-Tabelleneintrag eines Empfängers, wenn er innerhalb einer bestimmten Zeitspanne (Aging-Zeit) keine Report-Nachricht mehr von diesem empfängt.

Sind mehrere IGMP-Multicast-Router im selben Netz, dann übernimmt das Gerät mit der kleineren IP-Adresse die Query-Funktion. Befindet sich kein Multicast-Router im Netz, dann haben Sie die Möglichkeit, die Query-Funktion in einen entsprechend ausgestatteten Switch einzuschalten.

Ein Switch, der einen Multicast-Empfänger mit einem Multicast-Router verbindet, analysiert mit dem IGMP-Snooping-Verfahren die IGMP-Information.

Das IGMP-Snooping-Verfahren ermöglicht auch Switches, die IGMP-Funktion zu nutzen. Ein Switch speichert die aus IP-Adressen gewonnenen MAC-Adressen der Multicast-Empfänger als erkannte Multicast-Adressen in seiner MAC-Adresstabelle (FDB). Außerdem kennzeichnet der Switch die Ports, an denen er Reports für eine bestimmte Multicast-Adresse empfangen hat. Dadurch vermittelt der Switch Multicast-Pakete ausschließlich an Ports, an denen Multicast-Empfänger angeschlossen sind. Die anderen Ports bleiben frei von diesen Paketen.

Als Besonderheit bietet Ihnen das Gerät die Möglichkeit, die Verarbeitung von Datenpaketen mit unbekanntem Multicast-Adressen zu bestimmen. Je nach Einstellung verwirft das Gerät diese Datenpakete oder vermittelt sie an sämtliche Ports. In der Grundeinstellung überträgt das Gerät die Datenpakete ausschließlich an Ports mit angeschlossenen Geräten, die ihrerseits Query-Pakete empfangen. Sie haben außerdem die Möglichkeit, bekannte Multicast-Pakete zusätzlich an Query-Ports zu senden.

■ IGMP-Snooping einstellen

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > IGMP-Snooping > Global*.
 - Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Wenn die *IGMP-Snooping*-Funktion ausgeschaltet ist, dann verhält sich das Gerät wie folgt:
- ▶ Das Gerät ignoriert die empfangenen Query- und Report-Nachrichten.
 - ▶ Das Gerät versendet (flutet) empfangene Datenpakete mit einer Multicast-Adresse als Zieladresse an jeden Port.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Einstellungen für einen Port festlegen:

- Öffnen Sie den Dialog *Switching > IGMP-Snooping > Konfiguration*, Registerkarte *Port*.
- Um die *IGMP-Snooping*-Funktion auf einem Port zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv* für den betreffenden Port.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Einstellungen für ein VLAN festlegen.

- Öffnen Sie den Dialog *Switching > IGMP-Snooping > Konfiguration*, Registerkarte *VLAN-ID*.
- Um die *IGMP-Snooping*-Funktion für ein bestimmtes VLAN zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv* für das betreffende VLAN.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

■ IGMP-Querier-Funktion einstellen

Das Gerät versendet optional selber aktiv Query-Nachrichten, alternativ antwortet es auf Query-Nachrichten oder erkennt andere Multicast-Querier im Netz (*IGMP Snooping-Querier*-Funktion).

Voraussetzung:

Die *IGMP-Snooping*-Funktion ist global eingeschaltet.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > IGMP-Snooping > Querier*.
- Im Rahmen *Funktion* schalten Sie die *IGMP Snooping-Querier*-Funktion des Gerätes global ein oder aus.
- Um die *IGMP Snooping-Querier*-Funktion für ein bestimmtes VLAN zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv* für das betreffende VLAN.
 - ▶ Das Gerät führt einen einfachen Auswahlprozess durch: Wenn die IP-Quell-Adresse des anderen Multicast-Queriers niedriger ist als die eigene, so wechselt das Gerät in den Passivzustand, in dem es keine Query-Anfragen mehr aussendet.
 - ▶ In Spalte *Adresse* legen Sie die IP-Multicast-Adresse fest, die das Gerät als Absenderadresse in generierte Query-Abfragen einfügt. Verwenden Sie die Adresse des Multicast-Routers.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

■ IGMP-Snooping-Erweiterungen (Tabelle)

Der Dialog *Switching > IGMP-Snooping > Snooping Erweiterungen* gibt Ihnen Zugriff auf erweiterte Einstellungen für die *IGMP-Snooping*-Funktion. Sie aktivieren oder deaktivieren die Einstellungen jeweils für einen Port in einem VLAN.

Folgende Einstellungen sind möglich:

► Static

Mit dieser Einstellung legen Sie den Port als statischen Query-Port fest. An einem statischen Query-Port vermittelt das Gerät jede IGMP-Nachricht, auch wenn es an diesem Port zuvor keine IGMP-Query-Nachrichten empfangen hat. Bei deaktivierter Static-Option vermittelt das Gerät IGMP-Nachrichten an diesen Port ausschließlich dann, wenn es zuvor IGMP-Query-Nachrichten empfangen hat. Wenn das der Fall ist, zeigt der Eintrag ein **L** („learned“) an.

► Learn by LLDP

Ein Port mit dieser Einstellung ermittelt automatisch andere Hirschmann-Geräte über LLDP (Link Layer Discovery Protocol). Das Gerät lernt dann von diesen Hirschmann-Geräten den IGMP-Query-Status auf diesem Port und konfiguriert die *IGMP Snooping-Querier*-Funktion entsprechend. Der Eintrag **ALA** zeigt an, dass die *Learn by LLDP*-Funktion aktiviert ist. Wenn das Gerät auf diesem Port in diesem VLAN ein anderes Hirschmann-Gerät gefunden hat, zeigt der Eintrag zusätzlich ein **A** („automatic“).

► Forward All

Mit dieser Einstellung sendet das Gerät an diesem Port die Datenpakete, die an eine Multicast-Adresse adressiert sind. Die Einstellung ist zum Beispiel in folgenden Situationen geeignet:

- Für Diagnosezwecke.
- Für Geräte in einem MRP-Ring: Nach einer Ringumschaltung ermöglicht die *Forward All*-Funktion eine schnelle Rekonfiguration des Netzes für Datenpakete mit registrierten Multicast-Zieladressen. Aktivieren Sie die *Forward All*-Funktion auf allen Ring-Ports.

Voraussetzung:

Die *IGMP-Snooping*-Funktion ist global eingeschaltet.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > IGMP-Snooping > Snooping Erweiterungen*.
- Klicken Sie den gewünschten Port im gewünschten VLAN doppelt.
- Um eine oder mehrere Funktionen zu aktivieren, markieren Sie die entsprechenden Optionen.
- Klicken Sie die Schaltfläche *Ok*.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

enable

vlan database

igmp-snooping vlan-id 1 forward-all 1/1

Wechsel in den Privileged-EXEC-Modus.

Wechsel in den VLAN-Konfigurationsmodus.

Aktivieren der *Forward All*-Funktion für Port 1/1 in VLAN 1.

■ Multicasts konfigurieren

Das Gerät bietet Ihnen die Möglichkeit, die Vermittlung von Multicast-Datenpaketen zu konfigurieren. Dabei bietet das Gerät unterschiedliche Optionen an, je nachdem, ob die Datenpakete für unbekannte oder bekannte Multicast-Empfänger bestimmt sind.

Die Einstellungen für unbekannte Multicast-Adressen gelten global für das gesamte Gerät. Folgende Optionen stehen zur Auswahl:

- ▶ Das Gerät verwirft unbekannte Multicasts.
- ▶ Das Gerät sendet unbekannte Multicasts an jeden Port aus.
- ▶ Das Gerät sendet unbekannte Multicasts ausschließlich an den Ports aus, die zuvor Query-Nachrichten empfangen haben (Query-Ports).

Anmerkung: Die Vermittlungseinstellungen für unbekannte Multicast-Adressen gilt auch für die reservierten IP-Adressen aus dem „Local Network Control Block“ (224.0.0.0..224.0.0.255). Dieses Verhalten beeinflusst ggf. übergeordnete Routing-Protokolle.

Die Vermittlung von Multicast-Datenpaketen an bekannte Multicast-Adressen legen Sie für jedes VLAN individuell fest. Folgende Optionen stehen zur Auswahl:

- ▶ Das Gerät sendet bekannte Multicasts an den Ports aus, die zuvor Query-Nachrichten empfangen haben (Query-Ports) sowie an die registrierten Ports. Registrierte Ports sind Ports, an denen sich Multicast-Empfänger befinden, die bei der entsprechenden Multicast-Gruppe angemeldet sind. Diese Option gewährleistet, dass die Übermittlung bei grundlegenden Anwendungen ohne weitere Konfiguration funktioniert.
- ▶ Das Gerät sendet bekannte Multicasts ausschließlich an den registrierten Ports aus. Diese Einstellung hat den Vorteil, die verfügbare Bandbreite durch gezielte Vermittlung optimal zu nutzen.

Voraussetzung:

Die *IGMP-Snooping*-Funktion ist global eingeschaltet.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > IGMP-Snooping > Multicasts*.
- Im Rahmen *Konfiguration* legen Sie fest, wie das Gerät Datenpakete an unbekannte Multicast-Adressen vermittelt.
 - ▶ *an registrierte Ports senden*
Das Gerät sendet Pakete mit unbekannter Multicast-Adresse an jeden Query-Port.
 - ▶ *an Query- und registrierte Ports senden*
Das Gerät sendet Pakete mit unbekannter Multicast-Adresse an jeden Port.
- In Spalte *Bekannte Multicasts* legen Sie fest, wie das Gerät im entsprechenden VLAN Datenpakete an bekannte Multicast-Adressen vermittelt. Klicken Sie in das betreffende Feld und wählen Sie den gewünschten Wert.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

10.3 Lastbegrenzung

Die Lastbegrenzer-Funktion bietet Ihnen die Möglichkeit, für einen stabilen Betrieb auch bei hohem Verkehrsaufkommen den Datenverkehr an den Ports zu begrenzen. Die Lastbegrenzung erfolgt individuell für jeden Port sowie separat für Eingangs- und Ausgangsdatenverkehr.

Überschreitet die Datenrate an einem Port den definierten Grenzwert, so verwirft das Gerät die Überlast an diesem Port.

Die Lastbegrenzung erfolgt ausschließlich auf Schicht 2. Die Lastbegrenzer-Funktion übergeht dabei Protokollinformationen höherer Schichten wie IP oder TCP. Dies beeinflusst möglicherweise den TCP-Verkehr.

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

- ▶ Beschränken Sie die Lastbegrenzung auf bestimmte Paket-Typen, zum Beispiel auf Broadcasts, Multicasts und Unicasts mit unbekannter Zieladresse.
- ▶ Begrenzen Sie den ausgehenden Datenverkehr statt des eingehenden. Die Ausgangs-Lastbegrenzung arbeitet durch die geräte-interne Pufferung der Datenpakete besser mit der TCP-Flusssteuerung zusammen.
- ▶ Erhöhen Sie die Aging-Zeit für erlernte Unicast-Adressen.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > Lastbegrenzer*.
- ▶ Aktivieren Sie den Lastbegrenzer und legen Sie Grenzwerte für die Datenrate fest. Die Einstellungen gelten jeweils für einen Port und sind aufgeteilt nach Art des Datenverkehrs:
 - ▶ Empfangene Broadcast-Datenpakete
 - ▶ Empfangene Multicast-Datenpakete
 - ▶ Empfangene Unicast-Datenpakete mit unbekannter Zieladresse

Um die Funktion auf einem Port zu aktivieren, markieren Sie das Kontrollkästchen für mindestens eine Kategorie. In Spalte *Grenzwert Einheit* legen Sie fest, ob das Gerät die Grenzwerte als Prozent der Port-Bandbreite oder als Datenpakete pro Sekunde interpretiert. Der Grenzwert 0 deaktiviert den Lastbegrenzer.

- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

10.4 QoS/Priorität

QoS (Quality of Service) ist ein in der Norm IEEE 802.1D beschriebenes Verfahren, mit dem Sie die Ressourcen im Netz verteilen. QoS gibt Ihnen die Möglichkeit, Daten wichtiger Anwendungen zu priorisieren.

Die Priorisierung verhindert insbesondere bei starker Netzlast, dass Datenverkehr mit geringerer Priorität verzögerungsempfindlichen Datenverkehr stört. Zum verzögerungsempfindlichen Datenverkehr zählen beispielsweise Sprach-, Video- und Echtzeitdaten.

10.4.1 Beschreibung Priorisierung

Zur Priorisierung des Datenverkehrs sind im Gerät Verkehrsklassen („Traffic Classes“) vordefiniert. Höhere Verkehrsklassen priorisiert das Gerät gegenüber niedrigeren Verkehrsklassen. Die Anzahl der Verkehrsklassen hängt vom Gerätetyp ab.

Um verzögerungsempfindlichen Daten einen optimierten Datenfluss zu bieten, weisen Sie diesen Daten höhere Verkehrsklassen zu. Weniger verzögerungsempfindlichen Daten weisen Sie entsprechend niedrigere Verkehrsklassen zu.

■ Den Daten Verkehrsklassen zuweisen

Das Gerät weist eingehenden Daten automatisch Verkehrsklassen zu (Verkehrsklassifizierung). Das Gerät berücksichtigt folgende Klassifizierungskriterien:

- ▶ Methode, gemäß derer das Gerät die Zuordnung empfangener Datenpakete zu den Verkehrsklassen durchführt:
 - ▶ `trustDot1p`
Das Gerät verwendet die im VLAN-Tag enthaltene Priorität des Datenpaketes.
 - ▶ `trustIpDscp`
Das Gerät verwendet die im IP-Header enthaltene QoS-Information (ToS/DiffServ).
 - ▶ `untrusted`
Das Gerät ignoriert mögliche Prioritätsinformationen innerhalb der Datenpakete und verwendet direkt die Priorität des Empfangsports.
- ▶ Die Priorität, die dem Empfangsport zugewiesen ist.

Beide Klassifizierungskriterien sind konfigurierbar.

Bei der Verkehrsklassifizierung wendet das Gerät folgende Regeln an:

- ▶ Wenn der Empfangsport auf `trustDot1p` eingestellt ist (Voreinstellung), verwendet das Gerät die im VLAN-Tag enthaltene Priorität des Datenpaketes. Wenn die Datenpakete kein VLAN-Tag enthalten, richtet sich das Gerät nach der Priorität des Empfangsports.
- ▶ Wenn der Empfangsport auf `trustIpDscp` eingestellt ist, verwendet das Gerät die im IP-Header enthaltene QoS-Information (ToS/DiffServ). Wenn die Datenpakete keine IP-Pakete sind, richtet sich das Gerät nach der Priorität des Empfangsports.
- ▶ Wenn der Empfangsport auf `untrusted` eingestellt ist, richtet sich das Gerät nach der Priorität des Empfangsports.

■ Die Verkehrsklassen priorisieren

Zur Priorisierung von Verkehrsklassen verwendet das Gerät folgende Methoden:

- ▶ `Strict`
Wenn kein Versand von Daten einer höheren Verkehrsklasse mehr stattfindet oder die betreffenden Daten noch in der Warteschlange stehen, sendet das Gerät Daten der entsprechenden Verkehrsklasse. Wenn jede Verkehrsklasse nach der Methode `Strict` priorisiert ist, blockiert das Gerät bei hoher Netzlast die Daten niedrigerer Verkehrsklassen möglicherweise permanent.
- ▶ `Weighted Fair Queuing`
Die Verkehrsklasse erhält eine garantierte Bandbreite zugewiesen. Dies gewährleistet, dass das Gerät die Daten dieser Verkehrsklasse versendet, auch wenn in höheren Verkehrsklassen sehr viel Datenverkehr herrscht.

10.4.2 Behandlung empfangener Prioritätsinformationen

Anwendungen kennzeichnen Datenpakete mit folgenden Priorisierungs-Informationen:

- ▶ VLAN-Priorität nach IEEE 802.1Q/ 802.1D (Schicht 2)
- ▶ Type-of-Service (ToS) oder DiffServ (DSCP) bei VLAN Management IP-Paketen (Schicht 3)

Das Gerät bietet folgende Möglichkeiten, diese Prioritätsinformation auszuwerten:

- ▶ `trustDot1p`
Das Gerät weist VLAN-getaggte Datenpakete entsprechend ihrer VLAN-Priorität den unterschiedlichen Verkehrsklassen zu. Die entsprechende Zuordnung ist konfigurierbar. Das Gerät weist Datenpaketen, die es ohne VLAN-Tag empfängt, die Priorität des Empfangsports zu.
- ▶ `trustIpDscp`
Das Gerät weist IP-Pakete gemäß dem DSCP-Wert im IP-Header den unterschiedlichen Verkehrsklassen zu, auch wenn das Paket zusätzlich VLAN-getagged war. Die entsprechende Zuordnung ist konfigurierbar. Nicht-IP-Pakete priorisiert das Gerät entsprechend der Priorität des Empfangsports.
- ▶ `untrusted`
Das Gerät ignoriert die Prioritätsinformationen in Datenpaketen und weist den Paketen die Priorität des Empfangsports zu.

10.4.3 VLAN-Tagging

Für die Funktionen VLAN und Priorisierung sieht die Norm IEEE 802.1Q die Einbindung eines MAC-Datenrahmens in das VLAN-Tag vor. Das VLAN-Tag besteht aus 4 Bytes und steht zwischen dem Quelladressfeld („Source Address Field“) und dem Typfeld („Length/Type Field“).

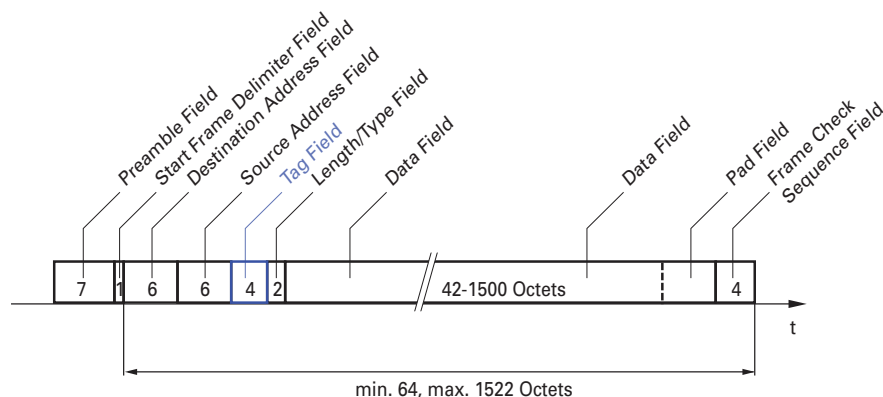


Abb. 20: Ethernet-Datenpaket mit Tag

Das Gerät wertet bei Datenpaketen mit VLAN-Tags folgende Informationen aus:

- ▶ Prioritätsinformation
- ▶ VLAN-Tag, sofern VLANs eingerichtet sind

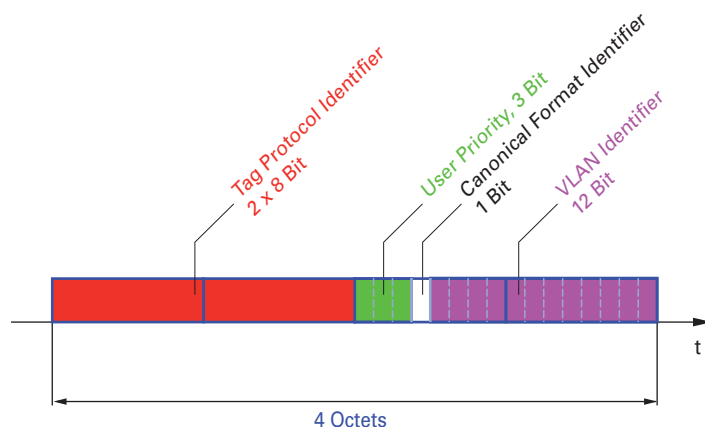


Abb. 21: Aufbau des VLAN-Tag

Ein Datenpaket, dessen VLAN-Tag eine Prioritätsinformation, aber keine VLAN-Information (VLAN-Kennung = 0) enthält, bezeichnet man als „Priority Tagged Frame“.

Anmerkung: Netzprotokolle und Redundanzmechanismen nutzen die höchste Verkehrsklasse 7. Wählen Sie für Anwendungsdaten deshalb niedrigere Verkehrsklassen.

Beachten Sie beim Einsatz der VLAN-Priorisierung folgende Besonderheiten:

- ▶ Eine Ende-zu-Ende-Priorisierung erfordert die durchgängige Übertragung der VLAN-Tags im gesamten Netz. Voraussetzung ist, dass jede beteiligte Netzkomponente VLAN-fähig ist.
- ▶ Router haben keine Möglichkeit, über Port-basierte Router-Interfaces Pakete mit VLAN-Tag zu empfangen und zu senden.

10.4.4 IP ToS (Type of Service)

Das Type-of-Service-Feld (ToS) im IP-Header ist bereits von Beginn an Bestandteil des IP-Protokolls und war zur Unterscheidung unterschiedlicher Dienstgütern in IP-Netzen vorgesehen. Schon damals machte man sich aufgrund der geringen zur Verfügung stehenden Bandbreiten und der unzuverlässigen Verbindungswege Gedanken um eine differenzierte Behandlung von IP-Paketen. Durch die kontinuierliche Steigerung der zur Verfügung stehenden Bandbreiten bestand keine Notwendigkeit, das ToS-Feld zu nutzen.

Erst die Echtzeitanforderungen an heutige Netze rücken das ToS-Feld in den Blickpunkt. Eine Markierung im ToS-Byte des IP-Headers ermöglicht eine Unterscheidung unterschiedlicher Dienstgütern. In der Praxis hat sich die Nutzung dieses Feldes jedoch nicht durchgesetzt.

Bits	0	1	2	3	4	5	6	7
	Precedence		Type of Service				MBZ	
Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined			Bit (7)				
111 - Network Control	0000 - [all normal]			0 - Must be zero				
110 - Internetwork Control	1000 - [minimize delay]							
101 - CRITIC / ECP	0100 - [maximize throughput]							
100 - Flash Override	0010 - [maximize reliability]							
011 - Flash	0001 - [minimize monetary cost]							
010 - Immediate								
001 - Priority								
000 - Routine								

Tab. 13: ToS-Feld im IP-Header

10.4.5 Handhabung der Verkehrsklassen

Das Gerät bietet folgende Möglichkeiten zur Handhabung der Verkehrsklassen:

- ▶ Strict Priority
- ▶ Weighted Fair Queuing
- ▶ Strict Priority kombiniert mit Weighted Fair Queuing
- ▶ Queue-Management

■ Beschreibung Strict Priority

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

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

■ Beschreibung Weighted Fair Queuing

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

Die reservierten Werte liegen im Bereich von 0 % bis 100 % der verfügbaren Bandbreite und sind einstellbar in Schritten von 1 %.

- ▶ Eine Reservierung von „0“ entspricht der Einstellung „keine Bandbreitengarantie“.
- ▶ Die Summe der einzelnen Bandbreiten darf bis zu 100% betragen.

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

■ Strict Priority und Weighted Fair Queuing kombinieren

Achten Sie beim Kombinieren von Weighted Fair Queuing mit Strict Priority darauf, dass die höchste Verkehrsklasse von Weighted Fair Queuing niedriger ist als die niedrigste Verkehrsklasse von Strict Priority.

Wenn Sie Weighted Fair Queuing mit Strict Priority kombinieren, kann eine hohe Strict Priority-Netzlast die für Weighted Fair Queuing verfügbare Bandbreite deutlich reduzieren.

10.4.6 Queue-Management

■ Einstellungen für das Queue-Management festlegen

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > QoS/Priorität > Queue-Management*.
- Die insgesamt zugewiesene Bandbreite in Spalte *Min. Bandbreite [%]* ist 100 %.
- Um das Weighted Fair Queuing für *Traffic-Klasse* = 0 zu aktivieren, gehen Sie wie folgt vor:
 - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
 - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert 5 fest.
- Um das Weighted Fair Queuing für *Traffic-Klasse* = 1 zu aktivieren, gehen Sie wie folgt vor:
 - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
 - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert 20 fest.
- Um das Weighted Fair Queuing für *Traffic-Klasse* = 2 zu aktivieren, gehen Sie wie folgt vor:
 - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
 - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert 30 fest.
- Um das Strict Priority für *Traffic-Klasse* = 3 zu aktivieren, gehen Sie wie folgt vor:
 - ▶ Markieren Sie das Kontrollkästchen in Spalte *Strict priority*.

- Um das Weighted Fair Queuing für *Traffic-Klasse* = 4 zu aktivieren, gehen Sie wie folgt vor:
 - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
 - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert 10 fest.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
cos-queue weighted 0
cos-queue min-bandwidth: 0 5
cos-queue weighted 1
cos-queue min-bandwidth: 1 20
cos-queue weighted 2
cos-queue min-bandwidth: 2 30
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
-----  -
0          5                weighted
1          20                weighted
2          30                weighted
3          0                strict
4          0                strict
5          0                strict
6          0                strict
7          0                strict
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Weighted Fair Queuing für die Verkehrsklasse 0 einschalten.
Gewichtung 5 % der Verkehrsklasse 0 zuweisen.
Weighted Fair Queuing für die Verkehrsklasse 1 einschalten.
Gewichtung 20 % der Verkehrsklasse 1 zuweisen.
Weighted Fair Queuing für die Verkehrsklasse 2 einschalten.
Gewichtung 30 % der Verkehrsklasse 2 zuweisen.

10.4.7 Management-Priorisierung

Damit Sie in Situationen mit hoher 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 sendet das Gerät die Management-Pakete mit einer Prioritäts-Information.

- ▶ Auf Schicht 2 modifiziert das Gerät die VLAN-Priorität im VLAN-Tag.
Das sinnvolle Nutzen dieser Funktion setzt voraus, dass die Konfiguration der entsprechenden Ports das Senden von Paketen mit VLAN-Tag erlaubt.
- ▶ Auf Schicht 3 modifiziert das Gerät den IP-DSCP-Wert.

10.4.8 Priorisierung einstellen

■ Port-Priorität zuweisen

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > QoS/Priorität > QoS/Priorität Port-Konfiguration*.
- In Spalte *Port-Priorität* legen Sie die Priorität fest, mit welcher das Gerät die auf diesem Port empfangenen Datenpakete ohne VLAN-Tag vermittelt.
- In Spalte *Trust-Mode* legen Sie fest, nach welchem Kriterium das Gerät empfangenen Datenpaketen eine Verkehrsklasse zuweist.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .


```
enable
configure
interface 1/1

vlan priority 3
exit
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
Interface 1/1 die Port-Priorität 3 zuweisen.
Wechsel in den Konfigurationsmodus.

■ VLAN-Priorität einer Verkehrsklasse zuweisen

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > QoS/Priorität > 802.1D/p Zuweisung*.
- Um einer VLAN-Priorität eine Verkehrsklasse zuzuweisen, fügen Sie in Spalte *Traffic-Klasse* den betreffenden Wert ein.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
classofservice dot1p-mapping 0 2
classofservice dot1p-mapping 1 2
exit
show classofservice dot1p-mapping
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Der VLAN-Priorität 0 die Verkehrsklasse 2 zuweisen.
Der VLAN-Priorität 1 die Verkehrsklasse 2 zuweisen.
Wechsel in den Privileged-EXEC-Modus.
Zeigt die Zuordnung an.

■ Empfangenen Datenpaketen die Port-Priorität zuweisen

Führen Sie die folgenden Schritte aus:

```
enable
configure
interface 1/1

classofservice trust untrusted
classofservice dot1p-mapping 0 2
classofservice dot1p-mapping 1 2
vlan priority 1
exit
exit
show classofservice trust
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
Dem Interface den Modus *untrusted* zuweisen.
Der VLAN-Priorität 0 die Verkehrsklasse 2 zuweisen.
Der VLAN-Priorität 1 die Verkehrsklasse 2 zuweisen.
Für die Port-Priorität den Wert 1 festlegen.
Wechsel in den Konfigurationsmodus.
Wechsel in den Privileged-EXEC-Modus.
Trust-Modus der Ports/Interfaces anzeigen.


```

Interface Trust Mode
-----
1/1      untrusted
1/2      dot1p
1/3      dot1p
1/4      dot1p
1/5      dot1p
1/6      dot1p
1/7      dot1p

```

■ DSCP einer Verkehrsklasse zuweisen

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > QoS/Priorität > IP-DSCP-Zuweisung*.
- Legen Sie in Spalte *Traffic-Klasse* den gewünschten Wert fest.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```

enable
configure
classofservice ip-dscp-mapping cs1 1
show classofservice ip-dscp-mapping

```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Dem DSCP CS1 die Verkehrsklasse 1 zuweisen.
IP-DSCP-Zuweisungen anzeigen.

```

IP DSCP      Traffic Class
-----
be           2
1            2
.            .
.            .
(cs1)       1
.            .

```

■ Empfangenen IP-Datenpaketen die DSCP-Priorität zuweisen

Führen Sie die folgenden Schritte aus:

```

enable
configure
interface 1/1

classofservice trust ip-dscp
exit
show classofservice trust

```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
Den Modus `trust ip-dscp global` zuweisen.
Wechsel in den Konfigurationsmodus.
Trust-Modus der Ports/Interfaces anzeigen.

```

Interface      Trust Mode
-----
1/1            ip-dscp
1/2            dot1p
1/3            dot1p
.              .
.              .
1/5            dot1p
.              .

```

■ Management-Priorität Schicht 2 konfigurieren

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > QoS/Priorität > QoS/Priorität Global*.
- Legen Sie im Feld *VLAN-Priorität für Management-Pakete* die VLAN-Priorität fest, mit der das Gerät Management-Datenpakete sendet.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
network management priority dot1p 7

show network parms
```

Wechsel in den Privileged-EXEC-Modus.
Management-Paketen die VLAN-Priorität 7 zuweisen. Das Gerät sendet Management-Pakete mit höchster Priorität.
Priorität des VLANs anzeigen, in dem sich das Management des Geräts befindet.

```
IPv4 Network
-----
...
Management VLAN priority.....7
...
```

■ Management-Priorität Schicht 3 konfigurieren

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > QoS/Priorität > QoS/Priorität Global*.
- Legen Sie im Feld *IP-DSCP-Wert für Management-Pakete* den DSCP-Wert fest, mit dem das Gerät Management-Datenpakete sendet.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
network management priority ip-dscp 56

show network parms
```

Wechsel in den Privileged-EXEC-Modus.
Management-Paketen den DSCP-Wert 56 zuweisen. Das Gerät sendet Management-Pakete mit höchster Priorität.
Priorität des VLANs anzeigen, in dem sich das Management des Geräts befindet.

```
IPv4 Network
-----
...
Management IP-DSCP value.....56
```

10.5 Flusskontrolle

Treffen in der Warteschlange eines Ports sehr viele Datenpakete gleichzeitig ein, führt dies möglicherweise zum Überlaufen des Port-Speichers. Beispielsweise passiert dies dann, wenn das Gerät Daten auf einem Gigabit-Port empfängt und diese an einen Port mit niedrigerer Bandbreite weiterleitet. Das Gerät verwirft überschüssige Datenpakete.

Der in der Norm IEEE 802.3 beschriebene Flusskontrollmechanismus sorgt dafür, dass keine Datenpakete durch Überlaufen eines Portspeichers verloren gehen. Kurz bevor ein Portspeicher vollständig gefüllt ist, signalisiert das Gerät den angeschlossenen Geräten, dass es keine Datenpakete von ihnen mehr annimmt.

- ▶ Im Vollduplex-Betrieb sendet das Gerät ein Pause-Datenpaket.
- ▶ Im Halbduplex-Betrieb simuliert das Gerät eine Kollision.

Die folgende Abbildung zeigt die Wirkungsweise der Flusskontrolle. Die Workstations 1, 2 und 3 wollen zur gleichen Zeit viele Daten an die Workstation 4 übertragen. Die gemeinsame Bandbreite der Workstations 1, 2 und 3 ist größer als die Bandbreite von Workstation 4. So kommt es zum Überlaufen der Empfangs-Warteschlange von Port 4. Der linke Trichter symbolisiert diesen Zustand.

Wenn an den Ports 1, 2 und 3 des Gerätes die Funktion Flusskontrolle eingeschaltet ist, reagiert das Gerät, bevor der Trichter überläuft. Der Trichter auf der rechten Seite veranschaulicht die Ports 1, 2 und 3, die zwecks Kontrolle der Übertragungsgeschwindigkeit eine Nachricht an die übertragenden Geräte senden. Als Resultat hiervon wird der Empfangsport nicht länger überfordert und ist in der Lage, den eingehenden Verkehr zu verarbeiten.

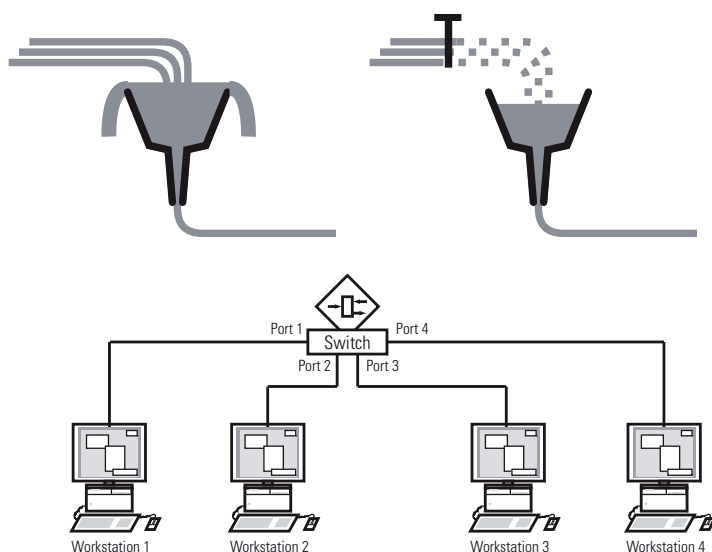


Abb. 22: Beispiel für Flusskontrolle

10.5.1 Halbduplex- oder Vollduplex-Verbindung

■ Flusskontrolle bei Halbduplex-Verbindung

Im Beispiel besteht zwischen der Arbeitsstation 2 und dem Gerät eine Halbduplex-Verbindung. Bevor die Sende-Warteschlange von Port 2 überläuft, sendet das Gerät Daten zurück an Arbeitsstation 2. Arbeitsstation 2 erkennt eine Kollision und unterbricht den Sendevorgang.

■ Flusskontrolle bei Vollduplex-Verbindung

Im Beispiel besteht zwischen der Arbeitsstation 2 und dem Gerät eine Vollduplex-Verbindung. Bevor die Sende-Warteschlange von Port 2 überläuft, sendet das Gerät eine Aufforderung an Arbeitsstation 2, beim Senden eine kleine Pause einzulegen.

10.5.2 Flusskontrolle einrichten

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > Global*.
- Markieren Sie das Kontrollkästchen *Flusskontrolle*.
Mit dieser Einstellung schalten Sie die Flusskontrolle im Gerät ein.
- Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- Um die Flusskontrolle auf einem Port einzuschalten, markieren Sie das Kontrollkästchen in Spalte *Flusskontrolle*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

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

11 VLANs

Ein virtuelles LAN (VLAN) besteht im einfachsten Fall aus einer Gruppe von Netzteilnehmern in einem Netzsegment, die so miteinander kommunizieren, als bildeten sie ein eigenständiges LAN.

Komplexere VLANs erstrecken sich über mehrere Netzsegmente und basieren zusätzlich auf logischen (statt ausschließlich physikalischen) Verbindungen zwischen Netzteilnehmern. VLANs sind ein Element der flexiblen Netzgestaltung. Das zentrale Umkonfigurieren lokaler Verbindungen lässt sich so leichter bewerkstelligen als über Kabel.

Das Gerät unterstützt das unabhängige Erlernen von VLANs nach Maßgabe des Standards IEEE 802.1Q, welcher die **VLAN**-Funktion definiert.

Die Verwendung von VLANS bietet zahlreiche Vorteile. Nachstehend sind die wesentlichen Vorteile aufgelistet:

- ▶ **Netzlastbegrenzung**
VLANs reduzieren die Netzlast erheblich, da die Geräte Broadcast-, Multicast- und Unicast-Pakete mit unbekanntem (nicht gelerntem) Zieladressen ausschließlich innerhalb des virtuellen LANs vermitteln. Der Rest des Datennetzes übermitteln den Verkehr wie üblich.
- ▶ **Flexibilität**
Sie haben die Möglichkeit, Anwender-Arbeitsgruppen zu bilden, die – abgesehen vom physikalischen Standort oder Medium der Teilnehmer – auf der Funktion der Teilnehmer basieren.
- ▶ **Übersichtlichkeit**
VLANs strukturieren Netze überschaubarer und vereinfachen die Wartung.

11.1 Beispiele für ein VLAN

Die folgenden Beispiele aus der Praxis vermitteln einen schnellen Einstieg in den Aufbau eines VLANs.

Anmerkung: Für die Konfiguration von VLANs verwenden Sie eine gleichbleibende Management-Oberfläche. In diesem Beispiel verwenden Sie für die Konfiguration der VLANs entweder Interface 1/6 oder die serielle V.24-Verbindung.

11.1.1 Beispiel 1

Das Beispiel zeigt eine minimale VLAN-Konfiguration (Port-basiertes VLAN). Ein Administrator hat an einem Vermittlungsgerät mehrere Endgeräte angeschlossen und diese 2 VLANs zugewiesen. Dies unterbindet wirksam jeglichen Datenverkehr zwischen verschiedenen VLANs; deren Mitglieder kommunizieren ausschließlich innerhalb ihres eigenen VLANs.

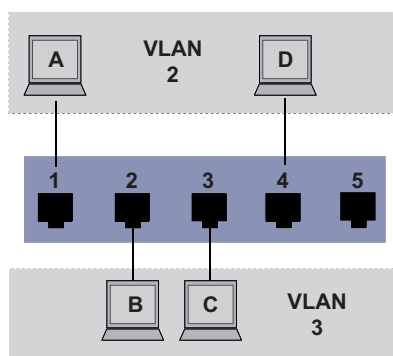


Abb. 23: Beispiel für ein einfaches Port-basiertes VLAN

Während der Einrichtung der VLANs erzeugen Sie für jeden Port Kommunikationsregeln, die Sie in einer Ingress-Tabelle (Eingang) und einer Egress-Tabelle (Ausgang) erfassen.

Die Ingress-Tabelle legt fest, welche VLAN-ID ein Port den eingehenden Datenpaketen zuweist. Hierbei weisen Sie das Endgerät über seine Portadresse einem VLAN zu.

Die Egress-Tabelle legt fest, an welchen Ports das Gerät die Pakete aus diesem VLAN sendet.

- ▶ T = Tagged (mit Tag-Feld, markiert)
- ▶ U = Untagged (ohne Tag-Feld, nicht markiert)

Für obiges Beispiel hat das TAG der Datenpakete keine Relevanz, verwenden Sie die Einstellung U.

Endgerät	Port	Port VLAN Identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1


Tab. 14: Ingress-Tabelle

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Tab. 15: Egress-Tabelle


Führen Sie die folgenden Schritte aus:

VLAN einrichten

- Öffnen Sie den Dialog *Switching > VLAN > VLAN Konfiguration*.
- Klicken Sie die Schaltfläche  .
Der Dialog zeigt das Fenster *Erzeugen*.
- Legen Sie im Feld *VLAN-ID* den Wert 2 fest.
- Klicken Sie die Schaltfläche *Ok*.
- Legen Sie für das VLAN den Namen *VLAN2* fest:
Doppelklicken Sie in Spalte *Name* und legen den Namen fest.
Ändern Sie für VLAN 1 den Wert in Spalte *Name* von Default zu *VLAN1*.
- Wiederholen Sie die vorherigen Schritte, um ein VLAN 3 mit dem Namen *VLAN3* zu erzeugen.

```
enable
vlan database
vlan add 2
name 2 VLAN2
vlan add 3
name 3 VLAN3
name 1 VLAN1
exit
show vlan brief
Max. VLAN ID..... 4042
Max. supported VLANs..... 16
Number of currently configured VLANs..... 3
vlan unaware mode..... disabled
VLAN ID VLAN Name          VLAN Type  VLAN Creation Time
-----
1      VLAN1                    default    0 days, 00:00:05
2      VLAN2                    static     0 days, 02:44:29
3      VLAN3                    static     0 days, 02:52:26
```

Ports einrichten

- Öffnen Sie den Dialog *Switching > VLAN > Port*.
- Um einem VLAN einen Port zuzuweisen, legen Sie in der betreffenden Spalte den gewünschten Wert fest.
Mögliche Werte:
 - ▶ T = Der Port ist Mitglied im VLAN. Der Port sendet Datenpakete mit Tag.
 - ▶ U = Der Port ist Mitglied im VLAN. Der Port sendet Datenpakete ohne Tag.
 - ▶ F = Der Port ist kein Mitglied im VLAN.
 - ▶ - = Der Port ist kein Mitglied in diesem VLAN.
- Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie den Wert U fest.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche  .
- Öffnen Sie den Dialog *Switching > VLAN > Port*.

- Legen Sie in Spalte *Port-VLAN-ID* die VLAN-ID des zugehörigen VLANs fest:
2 oder 3
- Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie für die Endgeräte-Ports in Spalte *Akzeptierte Datenpakete* den Wert `admitAll` fest.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Der Wert in Spalte *Ingress-Filtering* hat in diesem Beispiel keinen Einfluss auf die Funktion.

```
enable
configure
interface 1/1

vlan participation include 2

vlan pvid 2
exit
interface 1/2

vlan participation include 3

vlan pvid 3
exit
interface 1/3

vlan participation include 3

vlan pvid 3
exit
interface 1/4

vlan participation include 2

vlan pvid 2
exit
exit
show vlan id 3
VLAN ID          : 3
VLAN Name        : VLAN3
VLAN Type        : Static
Interface        Current   Configured   Tagging
-----
1/1              -       Autodetect   Tagged
1/2              Include  Include      Untagged
1/3              Include  Include      Untagged
1/4              -       Autodetect   Tagged
1/5              -       Autodetect   Tagged
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
Port 1/1 wird Mitglied des VLANs 2 und vermittelt die Datenpakete ohne VLAN-Tag.
Port 1/1 die Port-VLAN-ID 2 zuweisen.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
Port 1/2 wird Mitglied des VLANs 3 und vermittelt die Datenpakete ohne VLAN-Tag.
Port 1/2 die Port-VLAN-ID 3 zuweisen.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/3.
Port 1/3 wird Mitglied des VLANs 3 und vermittelt die Datenpakete ohne VLAN-Tag.
Port 1/3 die Port-VLAN-ID 3 zuweisen.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/4.
Port 1/4 wird Mitglied des VLANs 2 und vermittelt die Datenpakete ohne VLAN-Tag.
Port 1/4 die Port-VLAN-ID 2 zuweisen.
Wechsel in den Konfigurationsmodus.
Wechsel in den Privileged-EXEC-Modus.
Details zu VLAN 3 anzeigen.

11.1.2 Beispiel 2

Das zweite Beispiel zeigt eine komplexere Konfiguration mit 3 VLANs (1 bis 3). Zusätzlich zu dem schon bekannten Switch aus Beispiel 1 verwenden Sie einen 2. Switch (im Beispiel rechts gezeichnet).

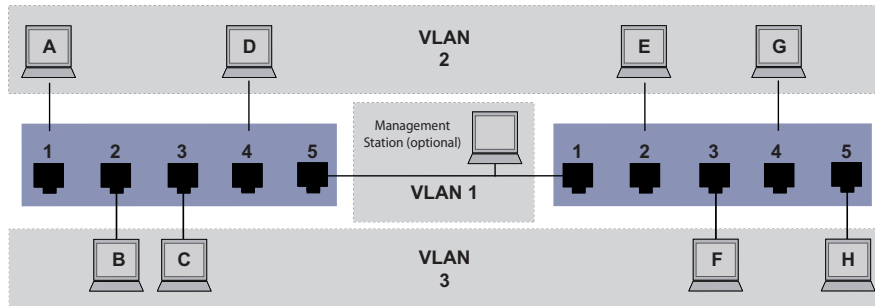


Abb. 24: Beispiel für eine komplexere VLAN-Konfiguration

Die Endgeräte der einzelnen VLANs (A bis H) erstrecken sich über 2 Vermittlungsgeräte (Switch). Derartige VLANs heißen deshalb verteilte VLANs. Zusätzlich ist eine optionale Netz-Management-Station gezeigt, die bei richtiger VLAN-Konfiguration Zugriff auf jede Netzkomponente hat.

Anmerkung: Das VLAN 1 hat in diesem Fall keine Bedeutung für die Endgerätekommunikation, ist aber notwendig für die Administration der Vermittlungsgeräte über das sogenannte Management-VLAN.

Weisen Sie die Ports mit ihren angeschlossenen Endgeräten eindeutig einem VLAN zu (wie im vorherigen Beispiel gezeigt). Bei der direkten Verbindung zwischen den beiden Übertragungsgeräten (Uplink) transportieren die Ports Pakete für beide VLANs. Um diese Uplinks zu unterscheiden, verwenden Sie VLAN-Tags, welche für die entsprechende Behandlung der Datenpakete sorgen. So bleibt die Zuordnung zu den jeweiligen VLANs erhalten.

Führen Sie die folgenden Schritte aus:

- Ergänzen Sie die Ingress- und Egress-Tabelle aus Beispiel 1 um den Uplink Port 5.
- Erfassen Sie für den rechten Switch je eine neue Ingress- und Egress-Tabelle wie im ersten Beispiel beschrieben.

Die Egress-Tabelle legt fest, an welchen Ports das Gerät die Pakete aus diesem VLAN sendet.

- ▶ T = Tagged (mit Tag-Feld, markiert)
- ▶ U = Untagged (ohne Tag-Feld, nicht markiert)

Markierte (Tagged) Pakete kommen in diesem Beispiel in der Kommunikation zwischen den Vermittlungsgeräten (Uplink) zum Einsatz, da auf diesen Ports Pakete für unterschiedliche VLANs unterschieden werden.

Endgerät	Port	Port VLAN Identifier (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Tab. 16: Ingress-Tabelle Gerät links

Endgerät	Port	Port VLAN Identifier (PVID)
Uplink	1	1
E	2	2
F	3	3

Tab. 17: Ingress-Tabelle Gerät rechts

VLANs

11.1 Beispiele für ein VLAN

Endgerät	Port	Port VLAN Identifier (PVID)
G	4	2
H	5	3

Tab. 17: Ingress-Tabelle Gerät rechts

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tab. 18: Egress-Tabelle Gerät links

VLAN-ID	Port				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Tab. 19: Egress-Tabelle Gerät rechts

Die Kommunikationsbeziehungen sind hierbei wie folgt: Endgeräte an Port 1 und 4 des linken Gerätes sowie Endgeräte an Port 2 und 4 des rechten Gerätes sind Mitglied im VLAN 2 und können somit untereinander kommunizieren. Ebenso verhält es sich mit den Endgeräten an Port 2 und 3 des linken Gerätes sowie den Endgeräten an Port 3 und 5 des rechten Gerätes. Diese gehören zu VLAN 3.

Die Endgeräte „sehen“ jeweils ihren Teil des Netzes. Teilnehmer außerhalb dieses VLANs sind unerreichbar. Das Gerät vermittelt auch Broadcast-, Multicast- und Unicast-Pakete mit unbekannter (nicht gelernter) Zieladresse ausschließlich innerhalb der Grenzen eines VLANs.

Hier verwenden die Geräte das VLAN-Tag (IEEE 801.1Q) innerhalb des VLANs mit der ID 1 (Uplink). Der Buchstabe **T** in der Egress-Tabelle der Ports zeigt das VLAN-Tag.

Die Konfiguration des Beispiels erfolgt exemplarisch für das rechte Gerät. Verfahren Sie analog, um das zuvor bereits konfigurierte linke Gerät unter Anwendung der oben erzeugten Ingress- und Egress-Tabellen an die neue Umgebung anzupassen.

Führen Sie die folgenden Schritte aus:

VLAN einrichten

Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.

Klicken Sie die Schaltfläche .

Der Dialog zeigt das Fenster *Erzeugen*.

Legen Sie im Feld *VLAN-ID* die VLAN-ID fest, zum Beispiel 2.

Klicken Sie die Schaltfläche *Ok*.

Legen Sie für das VLAN den Namen `VLAN2` fest:

Doppelklicken Sie in Spalte *Name* und legen den Namen fest.

Ändern Sie für VLAN 1 den Wert in Spalte *Name* von `Default` zu `VLAN1`.

Wiederholen Sie die vorherigen Schritte, um ein VLAN 3 mit dem Namen `VLAN3` zu erzeugen.

```
enable
vlan database
vlan add 2
name 2 VLAN2
vlan add 3
name 3 VLAN3
name 1 VLAN1
exit
show vlan brief
Max. VLAN ID..... 4042
Max. supported VLANs..... 16
Number of currently configured VLANs..... 3
vlan unaware mode..... disabled
VLAN ID VLAN Name                VLAN Type VLAN Creation Time
-----
1          VLAN1                default   0 days, 00:00:05
2          VLAN2                static   0 days, 02:44:29
3          VLAN3                static   0 days, 02:52:26
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den VLAN-Konfigurationsmodus.
Erzeugt ein neues VLAN mit VLAN-ID 2.
Dem VLAN 2 den Namen `VLAN2` zuweisen.
Erzeugt ein neues VLAN mit VLAN-ID 3.
Dem VLAN 3 den Namen `VLAN3` zuweisen.
Dem VLAN 1 den Namen `VLAN1` zuweisen.
Wechsel in den Privileged-EXEC-Modus.
Zeigt die aktuelle VLAN Konfiguration an.

Ports einrichten

- Öffnen Sie den Dialog *Switching > VLAN > Port*.
- Um einem VLAN einen Port zuzuweisen, legen Sie in der betreffenden Spalte den gewünschten Wert fest.

Mögliche Werte:

- ▶ T = Der Port ist Mitglied im VLAN. Der Port sendet Datenpakete mit Tag.
- ▶ U = Der Port ist Mitglied im VLAN. Der Port sendet Datenpakete ohne Tag.
- ▶ F = Der Port ist kein Mitglied im VLAN.
- ▶ - = Der Port ist kein Mitglied in diesem VLAN.

Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie den Wert `U` fest.

Auf dem Uplink-Port, über den die VLANs miteinander kommunizieren, legen Sie den Wert `T` fest.

- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Switching > VLAN > Port*.
- Legen Sie in Spalte *Port-VLAN-ID* die VLAN-ID des zugehörigen VLANs fest:
1, 2 oder 3
- Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie für die Endgeräte-Ports in Spalte *Akzeptierte Datenpakete* den Wert `admitAll` fest.
- Legen Sie für den Uplink-Port in Spalte *Akzeptierte Datenpakete* den Wert `admitOnlyVlanTagged` fest.
- Markieren Sie für den Uplink-Port das Kontrollkästchen in Spalte *Ingress-Filtering*, um VLAN-Tags auf diesem Port auszuwerten.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
interface 1/1

vlan participation include 1
vlan participation include 2

vlan tagging 2 enable
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
Port 1/1 wird Mitglied des VLANs 1 und vermittelt die Datenpakete ohne VLAN-Tag.
Port 1/1 wird Mitglied des VLANs 2 und vermittelt die Datenpakete ohne VLAN-Tag.
Port 1/1 wird Mitglied des VLANs 2 und vermittelt die Datenpakete mit VLAN-Tag.

VLANs

11.1 Beispiele für ein VLAN

<pre>vlan participation include 3 vlan tagging 3 enable vlan pvid 1 vlan ingressfilter vlan acceptframe vlanonly exit interface 1/2 vlan participation include 2 vlan pvid 2 exit interface 1/3 vlan participation include 3 vlan pvid 3 exit interface 1/4 vlan participation include 2 vlan pvid 2 exit interface 1/5 vlan participation include 3 vlan pvid 3 exit exit show vlan id 3 VLAN ID.....3 VLAN Name.....VLAN3 VLAN Type.....Static VLAN Creation Time.....0 days, 00:07:47 (System Uptime) VLAN Routing.....disabled</pre>	<p>Port 1/1 wird Mitglied des VLANs 3 und vermittelt die Datenpakete ohne VLAN-Tag.</p> <p>Port 1/1 wird Mitglied des VLANs 3 und vermittelt die Datenpakete mit VLAN-Tag.</p> <p>Port-VLAN-ID 1 dem Port 1/1 zuweisen.</p> <p>Aktivieren von Ingress Filtering auf Port 1/1.</p> <p>Port 1/1 überträgt ausschließlich Pakete mit VLAN Tag.</p> <p>Wechsel in den Konfigurationsmodus.</p> <p>Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.</p> <p>Port 1/2 wird Mitglied des VLANs 2 und vermittelt die Datenpakete ohne VLAN-Tag.</p> <p>Port-VLAN-ID 2 dem Port 1/2 zuweisen.</p> <p>Wechsel in den Konfigurationsmodus.</p> <p>Wechsel in den Interface-Konfigurationsmodus von Interface 1/3.</p> <p>Port 1/3 wird Mitglied des VLANs 3 und vermittelt die Datenpakete ohne VLAN-Tag.</p> <p>Port-VLAN-ID 3 dem Port 1/3 zuweisen.</p> <p>Wechsel in den Konfigurationsmodus.</p> <p>Wechsel in den Interface-Konfigurationsmodus von Interface 1/4.</p> <p>Port 1/4 wird Mitglied des VLANs 2 und vermittelt die Datenpakete ohne VLAN-Tag.</p> <p>Port-VLAN-ID 2 dem Port 1/4 zuweisen.</p> <p>Wechsel in den Konfigurationsmodus.</p> <p>Wechsel in den Interface-Konfigurationsmodus von Interface 1/5.</p> <p>Port 1/5 wird Mitglied des VLANs 3 und vermittelt die Datenpakete ohne VLAN-Tag.</p> <p>Port-VLAN-ID 3 dem Port 1/5 zuweisen.</p> <p>Wechsel in den Konfigurationsmodus.</p> <p>Wechsel in den Privileged-EXEC-Modus.</p> <p>Details zu VLAN 3 anzeigen.</p>																								
<table border="1"> <thead> <tr> <th>Interface</th> <th>Current</th> <th>Configured</th> <th>Tagging</th> </tr> </thead> <tbody> <tr> <td>1/1</td> <td>Include</td> <td>Include</td> <td>Tagged</td> </tr> <tr> <td>1/2</td> <td>-</td> <td>Autodetect</td> <td>Untagged</td> </tr> <tr> <td>1/3</td> <td>Include</td> <td>Include</td> <td>Untagged</td> </tr> <tr> <td>1/4</td> <td>-</td> <td>Autodetect</td> <td>Untagged</td> </tr> <tr> <td>1/5</td> <td>Include</td> <td>Include</td> <td>Untagged</td> </tr> </tbody> </table>	Interface	Current	Configured	Tagging	1/1	Include	Include	Tagged	1/2	-	Autodetect	Untagged	1/3	Include	Include	Untagged	1/4	-	Autodetect	Untagged	1/5	Include	Include	Untagged	
Interface	Current	Configured	Tagging																						
1/1	Include	Include	Tagged																						
1/2	-	Autodetect	Untagged																						
1/3	Include	Include	Untagged																						
1/4	-	Autodetect	Untagged																						
1/5	Include	Include	Untagged																						

11.2 Gast-VLAN / Unauthentifizierte VLAN

Die Gast-VLAN-Funktion ermöglicht einem Gerät die Bereitstellung einer Port-basierten Netz Zugriffssteuerung (IEEE 802.1x) für Supplikanten ohne 802.1x-Fähigkeit. Diese Funktion stellt eine Vorrichtung zur Verfügung, die es Gästen ermöglicht, ausschließlich auf externe Netze zuzugreifen. Wenn Sie Supplikanten ohne 802.1x-Fähigkeit an einen aktiven, nicht autorisierten 802.1x-Port anschließen, senden die Supplikanten keine Antworten auf 802.1x-Anfragen. Da die Supplikanten keine Antworten senden, bleibt der Port im Status „nicht autorisiert“. Die Supplikanten haben keinen Zugriff auf externe Netze.




Bei der Supplikanten-Funktion von Gast-VLANs handelt es sich um eine Konfiguration auf Basis einzelner Ports. Wenn Sie einen Port als Gast-VLAN konfigurieren und Supplikanten ohne 802.1x-Fähigkeit an diesen Port anschließen, weist das Gerät die Supplikanten dem Gast-VLAN zu. Durch Hinzufügen von Supplikanten zu einem Gast-VLAN wechselt der Port in den Status „autorisiert“ und erlaubt so den Supplikanten den Zugriff auf externe Netze.

Mittels der Funktionalität eines nicht authentifizierten VLANs kann das Gerät Dienste für Supplikanten mit 802.1x-Fähigkeit bereitstellen, welche sich nicht korrekt authentisieren. Diese Funktion ermöglicht den nicht autorisierten Supplikanten den Zugriff auf eine begrenzte Zahl von Diensten. Wenn Sie an einem Port ein nicht authentifiziertes VLAN konfigurieren und die 802.1x-Port-Authentifizierung ebenso wie die globale Funktion aktiviert haben, ordnet das Gerät den Port dem nicht authentifizierten VLAN zu. Wenn sich ein Supplikant mit 802.1x-Fähigkeit nicht korrekt an dem Port authentisiert, fügt das Gerät den Supplikanten dem nicht authentifizierten VLAN hinzu. Wenn Sie zudem ein Gast-VLAN an dem Port konfigurieren, verwenden Supplikanten ohne 802.1x-Fähigkeit das Gast-VLAN.

Bei Zuweisung eines nicht authentifizierten VLANs zählt der Zähler für die Reauthentifizierung herunter. Das nicht authentifizierte VLAN authentisiert sich erneut, wenn die in Spalte *Reauthentifizierungs-Periode [s]* festgelegte Zeit abläuft und Supplikanten am Port vorhanden sind. Falls keine Supplikanten vorhanden sind, ordnet das Gerät den Port dem konfigurierten Gast-VLAN zu.

Das nachstehende Beispiel erläutert das Erzeugen eines Gast-VLANs. Ein nicht autorisiertes VLAN erzeugen Sie auf die gleiche Weise.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- Klicken Sie die Schaltfläche  .
Der Dialog zeigt das Fenster *Erzeugen*.
- Legen Sie im Feld *VLAN-ID* den Wert 10 fest.
- Klicken Sie die Schaltfläche *Ok*.
- Legen Sie für das VLAN den Namen *Gast* fest:
Doppelklicken Sie in Spalte *Name* und legen den Namen fest.
- Klicken Sie die Schaltfläche  .
Der Dialog zeigt das Fenster *Erzeugen*.
- Legen Sie im Feld *VLAN-ID* den Wert 20 fest.
- Klicken Sie die Schaltfläche *Ok*.
- Legen Sie für das VLAN den Namen *Nicht autorisiert* fest:
Doppelklicken Sie in Spalte *Name* und legen den Namen fest.
- Öffnen Sie den Dialog *Netzicherheit > 802.1X Port-Authentifizierung > Global*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche  .

- Öffnen Sie den Dialog *Netzicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration*.
- Legen Sie für Port 1/4 die folgenden Einstellungen fest:
 - Den Wert *auto* in Spalte *Port-Kontrolle*
 - Den Wert *10* in Spalte *Gast VLAN-ID*
 - Den Wert *20* in Spalte *Unauthenticated-VLAN-ID*
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
vlan database
vlan add 10
vlan add 20
name 10 Guest
name 20 Unauth
exit
configure
dot1x system-auth-control enable
dot1x port-control auto
interface 1/4

dot1x guest-vlan 10
dot1x unauthenticated-vlan 20
exit
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den VLAN-Konfigurationsmodus.
Erzeugt VLAN 10.
Erzeugt VLAN 20.
Benennt VLAN 10 um in *Guest*.
Benennt VLAN 20 um in *Unauth*.
Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Schalten Sie die Funktion 802.1X global ein.
Schaltet die Port-Kontrolle auf Port 1/4 ein.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/4.
Weist Port 1/4 das Gast-VLAN zu.
Weist Port 1/4 das nicht autorisierte VLAN zu.
Wechsel in den Konfigurationsmodus.

11.3 RADIUS-VLAN-Zuordnung

Die Funktion der RADIUS-VLAN-Zuordnung bietet Ihnen die Möglichkeit, eine RADIUS-VLAN-Kennung mit einem authentisierten Client zu verknüpfen. Wenn sich ein Client erfolgreich authentisiert und der RADIUS-Server ein VLAN-Attribut sendet, verknüpft das Gerät den Client mit dem vom RADIUS-Server zugewiesenen VLAN. Infolgedessen fügt das Gerät den physikalischen Port dem entsprechenden VLAN als nicht markiertes Mitglied hinzu und setzt die Port-VLAN-ID (PVID) auf den vorgegebenen Wert.

11.4 VLAN-Unaware-Modus

Die VLAN-Unaware-Funktion legt die Funktion des Gerätes in einem durch VLANs aufgeteilten LAN fest. Das Gerät akzeptiert Pakete und verarbeitet diese entsprechend der Eingangsregeln. Auf Grundlage der 802.1Q-Spezifikation legt diese Funktion fest, wie das Gerät Pakete mit VLAN-Tag verarbeitet.

Verwenden Sie den VLAN-Aware-Modus, um die benutzerdefinierte, vom Netzadministrator konfigurierte VLAN-Topologie anzuwenden. Bei der Weiterleitung von Paketen verwendet das Gerät das VLAN-Tag in Kombination mit der IP- oder Ethernet-Adresse. Das Gerät verarbeitet ein- und ausgehende Pakete gemäß den festgelegten Regeln. Die Konfiguration eines VLANs ist ein manueller Vorgang.

Verwenden Sie den VLAN-Unaware-Modus, um Datenverkehr so weiterzuleiten, wie er angekommen ist, d. h. ohne jegliche Modifizierung. Das Gerät versendet dann Pakete mit Markierung, wenn diese mit Markierung angekommen sind. Ebenso versendet es Pakete ohne Markierung, wenn diese ohne Markierung angekommen sind. Unabhängig von den VLAN-Zuweisungsmechanismen weist das Gerät Datenpakete der VLAN-ID 1 und einer Multicast-Gruppe zu und signalisiert auf diese Weise, dass die Domäne für die Paketflutung dem VLAN entspricht.

12 Redundanz

12.1 Netz-Topologie vs. Redundanzprotokolle

Bei Einsatz von Ethernet ist eine wichtige Voraussetzung, dass Datenpakete auf einem einzigen (eindeutigen) Weg vom Absender zum Empfänger gelangen. Die folgenden Netz-Topologien unterstützen diese Voraussetzung:

- ▶ Linien-Topologie
- ▶ Stern-Topologie
- ▶ Baum-Topologie

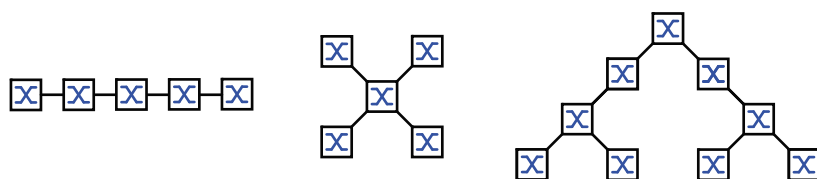


Abb. 25: Netz mit Linien-, Stern- und Baum-Topologie

Um bei Ausfall einer Verbindung die Kommunikation dennoch aufrecht zu erhalten, installieren Sie zwischen den Netzknoten zusätzliche physikalische Verbindungen. Redundanzprotokolle sorgen dafür, dass die zusätzlichen Verbindungen abgeschaltet bleiben, so lange die ursprüngliche Verbindung besteht. Fällt die Verbindung aus, generiert das Redundanzprotokoll einen neuen Weg vom Absender zum Empfänger über die alternative Verbindung.

Um auf Schicht 2 eines Netzes Redundanz einzuführen, legen Sie zunächst fest, welche Netz-Topologie Sie benötigen. In Abhängigkeit von der gewählten Netz-Topologie wählen Sie danach unter den Redundanzprotokollen aus, die sich mit dieser Netz-Topologie einsetzen lassen.

12.1.1 Netz-Topologien

■ Maschen-Topologie

Für Netze mit Stern- oder Baum-Topologie sind Redundanzverfahren ausschließlich im Zusammenhang mit physikalischer Schleifenbildung möglich. Ergebnis ist eine Maschen-Topologie.

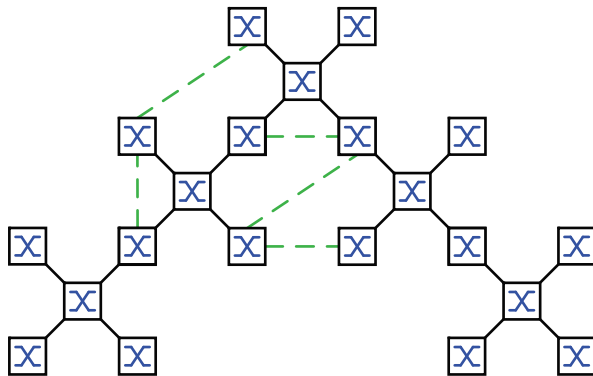


Abb. 26: Maschen-Topologie: Baum-Topologie mit physikalischen Schleifen

Für den Betrieb in dieser Netz-Topologie stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:

- ▶ Rapid Spanning Tree (RSTP)

■ Ring-Topologie

In Netzen mit Linien-Topologie lassen sich Redundanzverfahren nutzen, indem Sie die Enden der Linie verbinden. Dadurch entsteht eine Ring-Topologie.

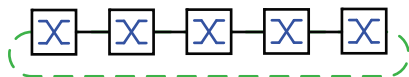


Abb. 27: Ring-Topologie: Linien-Topologie mit verbundenen Enden

Für den Betrieb in dieser Netz-Topologie stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:

- ▶ Media Redundancy Protocol (MRP)
- ▶ High-availability Seamless Redundancy (HSR) (hardwareabhängig)
- ▶ Rapid Spanning Tree (RSTP)

12.1.2 Redundanzprotokolle

Für den Betrieb in unterschiedlichen Netz-Topologien stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:

Redundanzprotokoll	Netz-Topologie	Bemerkungen
MRP	Ring	Die Umschaltzeit ist wählbar und nahezu unabhängig von der Anzahl der Geräte. Ein MRP-Ring besteht aus bis zu 50 Geräten, die das MRP-Protokoll nach IEC 62439 unterstützen. Wenn Sie ausschließlich Hirschmann-Geräte einsetzen, sind bis zu 100 Geräte im MRP-Ring möglich.
Fast MRP	Ring	Geräte mit Hardware für erweiterte Redundanz-Funktionen bieten kurze Umschaltzeiten von 30ms und 10ms.
PRP	beliebige Struktur der PRP-LANs	Unterbrechungsfreie Verfügbarkeit. Auf dem Weg vom Sender zum Empfänger transportiert PRP ein Datenpaket parallel durch 2 voneinander unabhängige LANs.
HSR	Ring	Unterbrechungsfreie Verfügbarkeit. Auf dem Weg vom Sender zum Empfänger transportiert HSR die Datenpakete in beiden Richtungen durch einen Ring.
RSTP	beliebige Struktur	Die Umschaltzeit ist abhängig von der Netz-Topologie und von Anzahl der Geräte. ▶ typ. < 1 s bei RSTP ▶ typ. < 30 s bei STP
Link-Aggregation	beliebige Struktur	Eine Link-Aggregation-Gruppe ist eine Kombination von 2 oder mehr Punkt-zu-Punkt-Verbindungen, die mit derselben Geschwindigkeit und demselben Duplex-Modus arbeiten, um die Bandbreite zu erhöhen.
Link-Backup	beliebige Struktur	Wenn das Gerät einen Fehler auf dem primären Link erkannt hat, leitet das Gerät den Datenverkehr zum Backup-Link um. Sie verwenden Link-Backup üblicherweise in Netzen von Dienst Anbietern oder Unternehmen.

Tab. 20: Redundanzprotokolle im Überblick

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

12.1.3 Redundanzkombinationen

	MRP	RSTP/ MSTP	Link Aggreg.	Link Backup	Subring	HIPER Ring	Fast MRP	DLR	HSR	PRP
MRP	✓									
RSTP/ MSTP ³⁾	✓ ¹⁾	✓								
Link Aggreg.	✓ ⁴⁾	✓ ⁴⁾	✓							
Link Backup	✓	✓	✓	✓						
Fast MRP ²⁾		✓ ¹⁾	✓	✓			✓			
HSR ²⁾	✓	✓ ¹⁾	✓	✓					✓ ²⁾	
PRP ²⁾	✓	✓ ¹⁾	✓	✓					A	✓ ²⁾

Tab. 21: Redundanzprotokolle im Überblick

Symbol	Bedeutung
✓	Kombinierbar
A	HSR-/PRP-Kopplung: Identische PRP-ID auf allen Nicht-HSR-Ports.
1)	Eine redundante Kopplung zwischen diesen Netztopologien führt möglicherweise zu Datenvervielfachungen.
2)	Ausschließlich auf Port 1 und Port 2 verfügbar.
3)	In Kombination mit MSTP können sich die Umschaltzeiten anderer Redundanzprotokolle geringfügig erhöhen.
4)	Kombinierbar auf demselben Port

12.2 Media Redundancy Protocol (MRP)

Das Media Redundancy Protocol (MRP) ist eine seit Mai 2008 standardisierte Lösung für Ring-Redundanz im industriellen Umfeld.

MRP ist kompatibel zur redundanten Ringkopplung, unterstützt VLANs und zeichnet sich durch sehr kurze Rekonfigurationszeiten aus.

Ein MRP-Ring besteht aus bis zu 50 Geräten, die das MRP-Protokoll nach IEC 62439 unterstützen. Wenn Sie ausschließlich Hirschmann-Geräte einsetzen, sind bis zu 100 Geräte im MRP-Ring möglich.

Sie verwenden den festgelegten MRP-Redundanzport (Fixed Backup) wenn der primäre Ring-Link ausfällt; der Ring-Manager sendet den Datenstrom auf den sekundären Ring-Link. Bei Wiederherstellung des primären Links wird der sekundäre Link weiterhin benutzt.

12.2.1 Netzstruktur

Das Konzept der Ring-Redundanz erlaubt den Aufbau hochverfügbarer, ringförmiger Netzstrukturen. Mit Hilfe der RM-Funktion (**R**ing-**M**anager) können die beiden Enden eines Backbones in Linienstruktur zu einem redundanten Ring geschlossen werden. Der Ring-Manager hält die redundante Strecke solange offen, wie die Linienstruktur intakt ist. Fällt ein Segment aus, schließt der Ring-Manager sofort die redundante Strecke und die Linienstruktur ist wieder intakt.

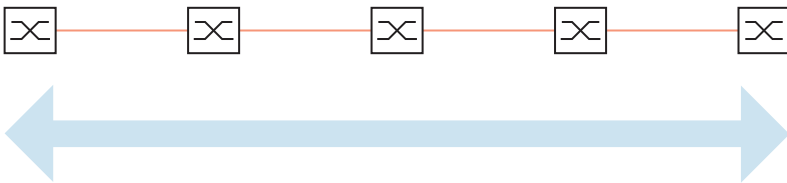


Abb. 28: Linienstruktur

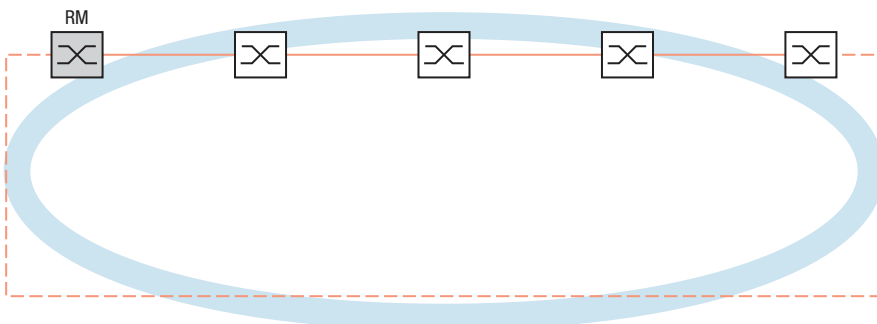


Abb. 29: Redundante Ringstruktur
RM = Ring-Manager
— Hauptleitung
- - - redundante Leitung

12.2.2 Rekonfigurationszeit

Beim Ausfall einer Teilstrecke wandelt der Ring-Manager den MRP-Ring zurück in eine Linienstruktur. Die maximale Zeit für die Rekonfiguration der Strecke legen Sie im Ring-Manager fest.

Mögliche Werte für die maximale Verzögerungszeit sind:

- 500 ms
- 200 ms
- 30 ms (hardwareabhängig)
- 10 ms (hardwareabhängig)

Die Verzögerungszeiten 30ms und 10ms stehen Ihnen ausschließlich auf Geräten mit Hardware für erweiterte Redundanz-Funktionen zur Verfügung.

Um diese kurzen Verzögerungszeiten zu nutzen, laden Sie die Geräte-Software mit Fast MRP-Unterstützung.

Legen Sie die Verzögerungszeit 10ms ausschließlich dann fest, wenn Sie im Ring bis zu 20 Geräte verwenden, die diese Verzögerungszeit unterstützen. Verwenden Sie im Ring mehr als 20 solcher Geräte, legen Sie eine Verzögerungszeit von mindestens 30ms fest.

Anmerkung: Konfigurieren Sie die Rekonfigurationszeit ausschließlich dann mit einem kleineren Wert als 500 ms, wenn alle Geräte im Ring die kürzere Verzögerungszeit unterstützen. Andernfalls sind die Geräte, die ausschließlich längere Verzögerungszeiten unterstützen, wegen Überlastung möglicherweise unerreichbar. Infolgedessen können Loops entstehen.

12.2.3 Advanced Mode

Für noch kürzere als die garantierten Rekonfigurationszeiten bietet das Gerät den Advanced Mode. Der Advanced Mode beschleunigt die Link-Ausfall-Erkennung, wenn die Ringteilnehmer dem Ring-Manager Unterbrechungen im Ring durch Link-Down-Meldungen signalisieren.

Hirschmann-Geräte unterstützen Link-Down-Meldungen. Aktivieren Sie deshalb generell im Ring-Manager den Advanced Mode.

Falls Sie Geräte einsetzen, die keine Link-Down-Meldungen senden, rekonfiguriert der Ring-Manager die Strecke in der gewählten, maximalen Rekonfigurationszeit.

12.2.4 Voraussetzungen für MRP

Bevor Sie einen MRP-Ring einrichten, vergewissern Sie sich, dass die folgenden Voraussetzungen erfüllt sind:

- ▶ Alle Ringteilnehmer unterstützen MRP.
- ▶ Die Ring-Teilnehmer sind über die Ring-Ports miteinander verbunden. Am jeweiligen Gerät sind außer seinen Nachbarn keine weiteren Ring-Teilnehmer angeschlossen.

- ▶ Alle Ringteilnehmer unterstützen die im Ring-Manager festgelegte Rekonfigurationszeit.
- ▶ Im Ring existiert genau 1 Ring-Manager.

Wenn Sie VLANs verwenden, konfigurieren Sie jeden Ring-Port mit folgenden Einstellungen:

- Ingress-Filtering deaktivieren, siehe Dialog *Switching > VLAN > Port*.
- Port-VLAN-ID (PVID) festlegen, siehe Dialog *Switching > VLAN > Port*.
 - PVID = 1, wenn das Gerät die MRP-Datenpakete unmarkiert überträgt (VLAN-ID = 0 im Dialog *Switching > L2-Redundanz > MRP*)
Durch die Einstellung PVID = 1 weist das Gerät die unmarkiert empfangenen Pakete automatisch dem VLAN 1 zu.
 - PVID = any, wenn das Gerät die MRP-Datenpakete in einem VLAN überträgt (VLAN-ID ≥ 1 im Dialog *Switching > L2-Redundanz > MRP*)
- Egress-Regeln festlegen, siehe Dialog *Switching > VLAN > Konfiguration*.
 - U (untagged) für die Ring-Ports von VLAN 1, wenn das Gerät die MRP-Datenpakete unmarkiert überträgt (VLAN-ID = 0 im Dialog *Switching > L2-Redundanz > MRP*, der MRP-Ring ist keinem VLAN zugewiesen).
 - T (tagged), für die Ring-Ports in dem VLAN, das Sie dem MRP-Ring zuweisen. Wählen Sie T, wenn das Gerät die MRP-Datenpakete in einem VLAN überträgt (VLAN-ID ≥ 1 im Dialog *Switching > L2-Redundanz > MRP*).

12.2.5 Beispiel-Konfiguration

Ein Backbone-Netz enthält 3 Geräte in einer Linienstruktur. Um die Verfügbarkeit des Netzes zu erhöhen, überführen Sie die Linienstruktur in eine redundante Ringstruktur. Zum Einsatz kommen Geräte unterschiedlicher Hersteller. Alle Geräte unterstützen MRP. Auf jedem Gerät legen Sie die Ports 1.1 und 1.2 als Ring-Ports fest.

Wenn der primäre Ring-Link ausfällt, sendet der Ring-Manager Daten auf dem sekundären Ring-Link. Bei Wiederherstellung des primären Links wechselt der sekundäre Link zurück in den Backup-Modus.

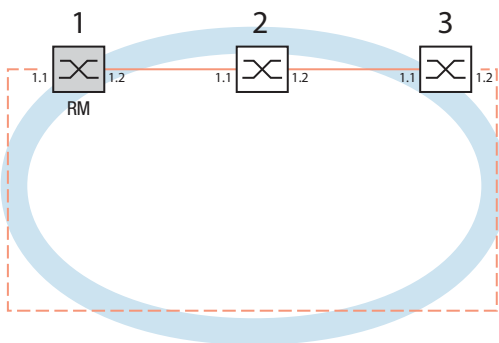


Abb. 30: Beispiel eines MRP-Rings
RM = Ring-Manager
— Hauptleitung
- - - redundante Leitung

Die folgende Beispielkonfiguration beschreibt die Konfiguration des Ring-Manager-Gerätes (1). Die 2 anderen Geräte (2 bis 3) konfigurieren Sie analog, ohne jedoch die Ring-Manager-Funktion zu aktivieren. Dieses Beispiel nutzt kein VLAN. Als Ring-Wiederherstellungszeit legen Sie 200 ms fest. Jedes Gerät unterstützt den Advanced Mode des Ring-Managers.

- Bauen Sie das Netz nach Ihren Erfordernissen auf.
- Konfigurieren Sie alle Ports so, dass die Datenrate und die Duplexeinstellungen der Strecken der folgenden Tabelle entsprechen:

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

Tab. 22: Port-Einstellungen für Ring-Ports

Anmerkung: Optische Ports ohne Unterstützung für Autonegotiation (automatische Konfiguration) konfigurieren Sie mit 100 Mbit/s Vollduplex (FDX) oder 1000 Mbit/s Vollduplex (FDX).

Anmerkung: Optische Ports ohne Unterstützung für Autonegotiation (automatische Konfiguration) konfigurieren Sie mit 100 Mbit/s Vollduplex (FDX).

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

- Deaktivieren Sie die Flusskontrolle auf den beteiligten Ports.
Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt. (Lieferzustand: Flusskontrolle global ausgeschaltet und auf allen Ports eingeschaltet.)
- Schalten Sie Spanning Tree auf allen Geräten im Netz aus:
 - Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
 - Ausschalten der Funktion.
Im Lieferzustand ist Spanning Tree für das Gerät aktiviert.

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
no spanning-tree operation	Schaltet Spanning Tree aus.
show spanning-tree global	Zeigt zur Kontrolle die Parameter an.

- Schalten Sie MRP auf allen Geräten im Netz ein:
 - Öffnen Sie den Dialog *Switching > L2-Redundanz > MRP*.
 - Legen Sie die gewünschten Ring-Ports fest.

Anmerkung: Wenn das Gerät die Software mit Unterstützung für Fast MRP verwendet, können Sie keinen *Link-Aggregation*-Port als Ringport auswählen.

Im Command Line Interface definieren Sie zunächst einen zusätzlichen Parameter, die MRP-DomänenID. Konfigurieren Sie alle Ringteilnehmer mit der gleichen MRP-DomänenID. Die MRP-Domänen-ID ist eine Folge aus 16 Ziffernblöcken (8-Bit-Werten).

Beim Konfigurieren mit der grafischen Benutzeroberfläche verwendet das Gerät den Vorgabewert („default domain“) 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255.

```
mrp domain add default-domain           Erzeugt eine neue MRP-Domäne mit der Default-Domänen-ID.  
mrp domain modify port primary 1/1     Port 1/1 als Ring-Port 1 festlegen.  
mrp domain modify port secondary 1/2   Port 1/2 als Ring-Port 2 festlegen.
```

Schalten Sie den *Fixed backup*-Port ein.

Schalten Sie den Ring-Manager ein.

Bei den anderen Geräten im Ring belassen Sie die Einstellung auf *Aus*.

Um zuzulassen, dass das Gerät nach Wiederherstellung des Rings das Senden der Daten auf dem sekundären Ports fortsetzt, markieren Sie das Kontrollkästchen *Fixed backup*.

Anmerkung: Wenn das Gerät zum primären Port zurückwechselt, wird ggf. die maximal zulässige Ring-Wiederherstellungszeit überschritten.

Wenn Sie die Markierung des Kontrollkästchens *Fixed backup* aufheben und der Ring wiederhergestellt ist, blockiert der Ring-Manager den sekundären Ports und hebt die Blockierung des primären Ports auf.

```
mrp domain modify port secondary 1/2   Aktivieren der Fixed backup-Funktion auf dem sekundären  
fixed-backup enable                    Port. Nach Wiederherstellung des Rings leitet der sekundäre Port  
                                         die Daten weiter.
```

Schalten Sie den Ring-Manager ein.

Bei den anderen Geräten im Ring belassen Sie die Einstellung auf *Aus*.

```
mrp domain modify mode manager         Legt fest, dass das Gerät als Ring-Manager arbeitet.  
                                         Schalten Sie die Ring-Manager-Funktion auf keinem weiteren  
                                         Gerät ein.
```

Markieren Sie das Kontrollkästchen im Feld *Advanced mode*.

```
mrp domain modify advanced-mode enabled Schaltet den Advanced Mode ein.
```

Wählen Sie im Feld *Ring-Rekonfiguration* den Wert 200ms aus.

```
mrp domain modify recovery-delay 200ms Legt den Wert 200ms fest als max. Verzögerungszeit bei der  
                                         Rekonfiguration des Rings.
```

Anmerkung: Wenn bei der Wahl von 200 ms für die Ringrekonfiguration die Stabilität des Rings nicht den Anforderungen an Ihr Netz entspricht, wählen Sie 500 ms.

Aktivieren Sie die Funktion des MRP-Rings.

Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
mrp domain modify operation enable     Schaltet den MRP-Ring ein.
```

Wenn alle Ring-Teilnehmer konfiguriert sind, schließen Sie die Linie zum Ring. Verbinden Sie dazu die Geräte an den Enden der Linie über ihre Ring-Ports.

Kontrollieren Sie die Meldungen des Gerätes:

```
show mrp                               Zeigt zur Kontrolle die Parameter an.
```

Das Feld *Funktion* zeigt den Betriebszustand des Ring-Ports.

Mögliche Werte:

- ▶ forwarding
Der Port ist eingeschaltet, Verbindung vorhanden.
- ▶ blocked
Der Port ist blockiert, Verbindung vorhanden.
- ▶ disabled
Der Port ist ausgeschaltet.
- ▶ not-connected
Keine Verbindung vorhanden.

Das Feld *Information* zeigt Meldungen zur Redundanzkonfiguration und mögliche Fehlerursachen.

Folgende Meldungen sind möglich, wenn das Gerät als Ring-Client oder als Ring-Manager arbeitet:

- ▶ *Redundanz verfügbar*
Die Redundanz ist eingerichtet. Fällt eine Komponente des Rings aus, übernimmt die redundante Leitung deren Funktion.
- ▶ *Konfigurationsfehler: Ring-Port-Verbindung fehlerhaft*
Die Verkabelung der Ring-Ports ist fehlerhaft.

Folgende Meldungen sind möglich, wenn das Gerät als Ring-Manager arbeitet:

- ▶ *Konfigurationsfehler: Pakete eines anderen Ring-Managers empfangen*
Im Ring existiert ein weiteres Gerät, das als Ring-Manager arbeitet.
Aktivieren Sie die Funktion *Ring-Manager* bei genau 1 Gerät im Ring.
- ▶ *Konfigurationsfehler: Verbindung im Ring ist mit falschem Port verbunden*
Eine Leitung des Rings ist anstatt mit einem Ring-Port mit einem anderen Port verbunden.
Das Gerät empfängt Test-Datenpakete ausschließlich auf 1 Ring-Port.

Gliedern Sie den MRP-Ring gegebenenfalls in ein VLAN ein:

- Legen Sie im Feld *VLAN-ID* die MRP-VLAN-ID fest. Die MRP-VLAN-ID bestimmt, in welchem der eingerichteten VLANs das Gerät die MRP-Pakete vermittelt. Um die MRP-VLANID zu setzen, konfigurieren Sie zuerst die VLANs und die zugehörigen Egress-Regeln im Dialog *Switching > VLAN > Konfiguration*.
- ▶ Soll der MRP-Ring keinem VLAN zugewiesen sein (wie in diesem Beispiel), belassen Sie die VLANID auf 0.
Legen Sie im Dialog *Switching > VLAN > Konfiguration* für die Ring-Ports im VLAN \cup die VLAN-Zugehörigkeit 1 (Untagged) fest.
- ▶ Soll der MRP-Ring einem VLAN zugewiesen sein, geben Sie eine VLANID > 0 ein.
Legen Sie im Dialog *Switching > VLAN > Konfiguration* für die Ring-Ports im gewählten VLAN die VLAN-Zugehörigkeit \top (Tagged) fest.

mrp domain modify vlan <0..4042>

Weist die VLAN-ID zu.

12.3 Parallelredundanz-Protokoll (PRP)

(hardwareabhängig)

Im Gegensatz zu Ringredundanz-Protokollen verwendet PRP 2 separate LANs, um eine unterbrechungsfreie Verfügbarkeit sicherzustellen. Auf der Strecke vom Sender zum Empfänger sendet PRP parallel 2 Datenpakete über 2 voneinander unabhängige LANs. Der Empfänger verarbeitet das erste empfangene Datenpaket und verwirft das zweite Datenpaket. Das Parallelredundanz-Protokoll (PRP) ist in der internationalen Norm IEC 62439-3 definiert.

Anmerkung: Wenn PRP aktiv ist, verwendet es die Schnittstellen 1/1 und 1/2. Wie Sie anhand der Dialoge *Switching > VLAN*, *Switching > Lastbegrenzer* und *Switching > Filter für MAC-Adressen* feststellen können, ersetzt die PRP-Funktion die Interfaces 1/1 und 1/2 durch das Interface prp/1. Konfigurieren Sie die VLAN-Mitgliedschaft, die Ratenbegrenzung und die MAC-Filterung für das Interface prp/1.

12.3.1 Implementierung

Senden die höheren Protokollschichten ein Datenpaket, erzeugt die PRP-Schnittstelle aus dem Ursprungspaket ein „Zwillingspaket“. Anschließend überträgt die PRP-Schnittstelle zeitgleich je 1 Datenpaket des Paares an jedes beteiligte LAN. Die Pakete durchqueren unterschiedliche LANs und weisen aus diesem Grund verschiedene Laufzeiten auf.

Die empfangende PRP-Schnittstelle leitet das erste Paket eines Paketpaares an die oberen Protokollschichten weiter und verwirft das zweite Paket. Aus Sicht der Anwendung funktioniert eine PRP-Schnittstelle wie eine reguläre Ethernet-Schnittstelle.

Die PRP-Schnittstelle bzw. eine sog. Redundancy Box (RedBox) fügt jedem Paket einen Redundancy Control Trailer (RCT) an. Beim RCT handelt es sich um ein Identifikationsfeld mit einer Länge von 48 bit, das für die Identifizierung der Zwillingspakete verantwortlich ist. Dieses Feld enthält die Identifizierung des LANs (LAN A oder B), Informationen über die Nutzdatengröße sowie eine fortlaufende Nummer mit einer Länge von 16 bit. Die Zwillingspakete unterscheiden sich also ausschließlich in der LAN-Kennung und als Folge in der FCS-Prüfsumme. Bei jedem gesendeten Paket zählt die PRP-Schnittstelle die fortlaufende Nummer hoch. Unter Verwendung der in jedem Paket enthaltenen eindeutigen Attribute (physikalische MAC-Quell-Adresse, fortlaufende Nummer usw.) werden die Zwillingspakete von der empfangenden RedBox bzw. dem empfangenden Double Attached Node (DAN) identifiziert und verworfen.

Je nach Paketgröße entsteht durch das Hinzufügen des RCT-Trailers mit PRP ein reduzierter Durchsatz der verfügbaren Bandbreite.

12.3.2 LRE-Funktionalität

Jeder DANP (Double Attached Node implementing PRP) verfügt über 2 parallel betriebene LAN-Ports. Die Link Redundancy Entity (Link-Redundanz-Einheit, LRE) verbindet die oberen Protokoll-Schichten mit jedem einzelnen Port.

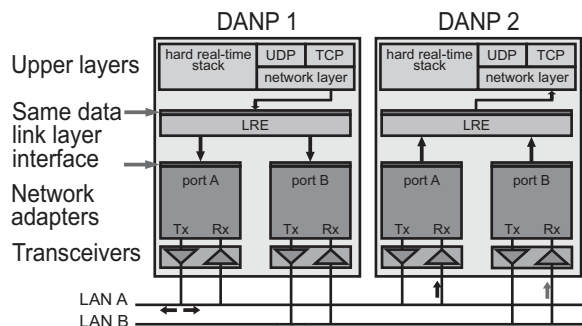


Abb. 31: Ablauf PRP/LRE

Die Link-Redundanz-Einheit (LRE) hat folgende Aufgaben:

- ▶ Zwillingsspaketbehandlung
- ▶ Redundanzverwaltung

Beim Übertragen von Paketen aus den höheren Protokollschichten sendet das LRE diese nahezu zeitgleich von beiden Ports aus. Die beiden Datenpakete durchqueren die LANs mit unterschiedlicher Verzögerung. Empfängt das Gerät das erste Datenpaket, leitet das LRE dieses an die höheren Protokollschichten weiter und verwirft das zweite empfangene Datenpaket.

Für die oberen Protokoll-Schichten verhält sich die LRE wie ein normaler Port.

Zur Identifizierung der Zwillingsspakete fügt das LRE den Paketen einen RCT mit einer fortlaufenden Nummer hinzu. Zudem versendet das LRE regelmäßig Multicast-PRP-Supervision-Pakete und evaluiert die Multicast-PRP-Supervision-Pakete der anderen RedBoxes und DANPs.

Das Gerät bietet Ihnen die Möglichkeit, die empfangenen Supervision-Paket-Einträge anzuzeigen. Die Einträge in der *Switching > L2-Redundanz > PRP > DAN/VDAN-Tabelle* unterstützen die Ermittlung von Redundanz- und Verbindungsproblemen. Dies gilt beispielsweise bei einem Index, wenn der Zeitstempel *Last seen B* zurückgesetzt wird und der Zeitstempel *Last seen A* unverändert bleibt. Die ständige Rücksetzung der Zeitstempel *Last seen A* und *Last seen B* weist auf einen Normalzustand hin.

Anmerkung: Gemäß IEC 62439 beträgt die Entry Forget Time 400 ms. Die Entry Forget Time ist die Zeit, nach der das Gerät einen Eintrag aus der Duplikat-Tabelle entfernt. Wenn das Gerät das 2. Paket eines Paares nach 400 ms oder später empfängt, verarbeitet das Gerät das 2. Paket, anstatt es zu verwerfen. Um dies zu vermeiden, empfiehlt Hirschmann die Verwendung einer maximalen Bandbreite von 90 %.

Anmerkung: Wenn der Abstand zwischen den Paketen (Interframe-Gap) geringer ist als die Latenz zwischen den 2 LANs, sind fehlerhafte Paketfolgen möglich. Fehlerhafte Paketfolgen sind ein Phänomen des PRP-Protokolls. Fehlerhafte Paketfolgen vermeiden Sie, wenn der Abstand zwischen den Paketen größer ist als die Latenz zwischen den LANs.

12.3.3 PRP-Netzstruktur

PRP verwendet 2 unabhängige LANs. Die Topologie jedes dieser LANs ist beliebig, Ring- Stern-, Bus- und Maschen-Topologien sind möglich.

Der Hauptvorteil von PRP liegt darin, dass die Rekonfigurationszeit mit einem aktiven (Transit-) LAN bei null liegt. Wenn das Endgerät von einem der LANs kein Paket erhält, erhält das zweite (Transit-) LAN die Verbindung aufrecht. Solange 1 (Transit-) LAN verfügbar ist, haben Reparaturen oder Wartungsvorgänge am anderen (Transit-) LAN keine Auswirkung auf die Übertragung von Datenpaketen.

Die RedBox (Redundanz-Box) und das DANP („Double Attached Node implementing PRP“) stellen die Basisgeräte eines PRP-Netzes dar. Beide Geräte verfügen jeweils über 1 Verbindung mit den (Transit-) LANs.

Die Geräte im (Transit-) LAN sind herkömmliche Switches. Die Geräte übertragen PRP-Datenpakete auf transparente Weise, ohne die RCT-Informationen zu evaluieren.

Anmerkung: Durch den RCT-Trailer wird das Paket größer. Konfigurieren Sie die MTU-Größe für LAN-A- und LAN-B-Geräte so, dass sie 1524 entspricht oder größer als 1524 ist.

Bei Endgeräten, die eine direkte Verbindung mit einem Gerät im (Transit-) LAN herstellen, handelt es sich um SANs („Single Attached Nodes“). SANs, die mit einem LAN verbunden sind, weisen keine Redundanz auf. Um das redundante PRP-Netz zu verwenden, verbinden Sie das SAN über eine RedBox mit dem PRP-Netz.

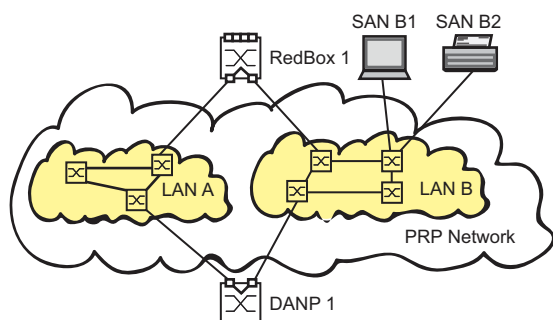


Abb. 32: Netz mit implementiertem Parallelredundanz-Protokoll

12.3.4 RedBoxes und DANPs mit einem PRP-Netz verbinden

DANPs verfügen über 2 Schnittstellen für die Verbindung mit dem PRP-Netz. Bei einer RedBox handelt es sich um ein DANP, das zusätzliche Switch-Ports besitzt. Verwenden Sie die Switch-Ports, um ein oder mehrere SANs redundant in das PRP-Netz zu integrieren.

Die Link-Redundanz-Einheit (LRE) in der RedBox erzeugt beim Senden eines Datenpakets ins PRP-Netz ein Zwillingsspaket. Beim Empfangen leitet die Link-Redundanz-Einheit 1 Datenpaket des Zwillingsspaars weiter, das 2. Datenpaket des Zwillingsspaars verwirft sie.

Anmerkung: Die RedBox unterstützt bis zu 128 Hosts. Beim Versuch, mehr als 128 Hosts mit der RedBox zu unterstützen, verwirft das Gerät Datenpakete.

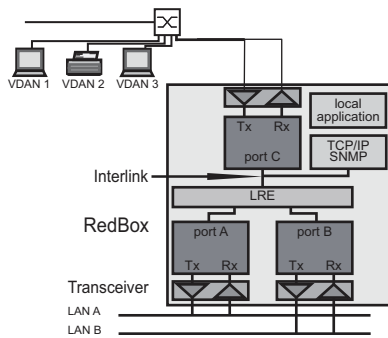


Abb. 33: RedBox-Umwandlung doppeltes auf einfaches LAN

12.3.5 Beispiel-Konfiguration

In dem folgenden Beispiel wird ein einfaches PRP-Netz mit 4 Geräten verwendet. Stellen Sie sicher, dass die Ports in LAN A und LAN B über optische SFP-Schnittstellen (100 Mbit/s) verfügen. Verbinden Sie Port A mit LAN A und Port B mit LAN B.

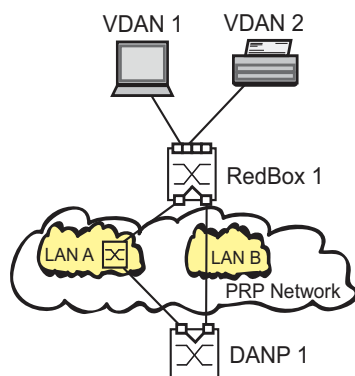


Abb. 34: Beispiel für ein PRP-Netz

Anmerkung: *PRP* ist für Geräte mit FPGA (Hardware für erweiterte Funktionen) verfügbar. Ob Ihr Gerät *PRP* unterstützt, können Sie anhand des Produktcodes feststellen. Um die Funktionen zu nutzen, laden Sie die Geräte-Software mit Unterstützung für *PRP*.

Die PRP-Funktion reserviert die Ports 1/1 und 1/2. Damit entfällt die Möglichkeit, andere Redundanz-Protokolle wie Spanning Tree und MRP parallel auf den Ports 1/1 und 1/2 zu verwenden.

- Wenn Sie Spanning Tree parallel zu PRP verwenden, deaktivieren Sie Spanning Tree auf den Ports 1/1 und 1/2. Deaktivieren Sie auf Port 1/1 und 1/2 außerdem die Funktionen *Root guard*, *TCN guard* und *Loop guard*.
- Wenn Sie MRP parallel zu PRP verwenden, legen Sie als MRP-Ring-Ports andere freie Geräte-Ports fest.




Führen Sie an der RedBox 1 und an den DANP 1-Geräten folgende Schritte aus:

- Öffnen Sie den Dialog *Switching > L2-Redundanz > PRP > Konfiguration*.

Führen Sie im Rahmen *Empfänger Supervision-Paket* die folgenden Schritte aus:

- Aktivieren Sie das Kontrollkästchen *Supervision-Pakete evaluieren*, um die empfangenen PRP-Supervision-Pakete zu analysieren.

Führen Sie im Rahmen *Absender Supervision-Paket* die folgenden Schritte aus:

- Aktivieren Sie *Aktiv*, um PRP-Supervision-Pakete von diesem Gerät zu übertragen.
- Das Gerät sendet entweder ausschließlich seine eigenen PRP-Supervision-Pakete oder sowohl seine eigenen Supervision-Pakete als auch die Pakete der angeschlossenen Geräte. Aktivieren Sie *VDAN-Pakete senden*, um Pakete für die in der *Switching > L2-Redundanz > PRP > DAN/VDAN-Tabelle* gelisteten VDANs zu übertragen. Bei Deaktivierung sendet das Gerät ausschließlich seine eigenen Supervision-Pakete. Deaktivieren Sie diese Funktion nach der Installation von neuen PRP-Geräten, um einen Überblick über die PRP-Supervision-Pakete auf entfernten Geräten zu erhalten.
- Wählen Sie zum Aktivieren der Ports in den Rahmen *Port A* und *Port B* den Wert *An*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
- Klicken Sie die Schaltfläche , um die im flüchtigen Speicher gespeicherte Konfiguration zu laden.
- Öffnen Sie den Dialog *Switching > L2-Redundanz > PRP > Proxy-Node-Tabelle*, um sich einen Überblick über die VDAN-Abschlussgeräte zu verschaffen, für die dieses Gerät die PRP-Umwandlung bereitstellt.
- Um diese Liste zu löschen, klicken Sie *Zurücksetzen*.
- Um die Liste mit aktuell angeschlossenen Geräten zu laden, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Switching > L2-Redundanz > PRP > PRP Statistiken*, um die Qualität des Datenverkehrs zu begutachten, der durch das Gerät läuft. Das Gerät ermittelt Fehler und zeigt diese in Übereinstimmung mit den in der MIB verwalteten Objekten und den jeweiligen Verbindungen an.
- Um die Einträge in der Statistik-Tabelle zu entfernen, klicken Sie *Zurücksetzen*.
- Um die aktuellen Statistiken zu laden, klicken Sie die Schaltfläche .

Das Gerät bietet Ihnen die Möglichkeit, die empfangenen Supervision-Paket-Einträge anzuzeigen. Die Einträge in der *Switching > L2-Redundanz > PRP > DAN/VDAN-Tabelle* unterstützen die Ermittlung von Redundanz- und Verbindungsproblemen. Dies gilt beispielsweise bei einem Index, wenn der Zeitstempel *Last seen B* zurückgesetzt wird und der Zeitstempel *Last seen A* unverändert bleibt. Die ständige Rücksetzung der Zeitstempel *Last seen A* und *Last seen A* weist auf einen Normalzustand hin.

Anmerkung: Wenn Sie die PRP-Funktion deaktivieren, ist die Deaktivierung von Port „A“ oder Port „B“ erforderlich, um Schleifen im Netz zu vermeiden.

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
no mrp operation	Deaktivieren dieser Funktion
no spanning-tree operation	Deaktivieren dieser Funktion
interface 1/1	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
no shutdown	Aktivieren der Schnittstelle
exit	Wechsel in den Konfigurationsmodus.
interface 1/2	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
no shutdown	Aktivieren der Schnittstelle
exit	Wechsel in den Konfigurationsmodus.
prp instance 1 supervision evaluate	Aktivieren der Auswertung empfangener Supervision-Pakete.
prp instance 1 supervision send	Aktivieren der Übertragung von Supervision-Paketen.

```
prp instance 1 supervision  
redbox-exclusively
```

```
prp operation  
show prp counters  
show prp node-table  
show prp proxy-node-table
```

Sendet Supervision-Pakete ausschließlich für diese RedBox. Verwenden Sie die `no`-Form des Kommandos, um Supervision-Pakete für jeden angeschlossenen VDAN und diese RedBox zu senden. Voraussetzung ist, dass Sie die Funktion zum Senden von Supervision-Paketen aktivieren.

Einschalten der *PRP*-Funktion.

Anzeige der PRP-Zählerdaten.

Anzeige der Knotentabelle.

Anzeige der Proxy-Node-Tabelle.

12.4 High-availability Seamless Redundancy (HSR) (hardwareabhängig)

Ebenso wie bei PRP liegt die Rekonfigurationszeit eines auf HSR basierten Rings bei null. HSR ist für Anwendungen geeignet, die eine hohe Verfügbarkeit und kurze Reaktionszeiten erfordern. Dies sind zum Beispiel Schutzanwendungen für die Automatisierung elektrischer Anlagen oder Steuerungen für Synchronantriebe, die eine konstante Verbindung benötigen.

Anmerkung: Wenn HSR aktiv ist, verwendet es die Schnittstellen 1/1 und 1/2. Wie Sie anhand der Dialoge *Switching > Lastbegrenzer* und *Switching > Filter für MAC-Adressen* feststellen können, ersetzt die HSR-Funktion die Interfaces 1/1 und 1/2 durch das Interface hsr/1. Konfigurieren Sie die VLAN-Mitgliedschaft und die Ratenbegrenzung für das Interface hsr/1.

12.4.1 Implementierung

Eine HSR-Redundanz-Box (RedBox) verwendet 2 parallel arbeitende Ethernet-Ports, um sich mit einem Ring zu verbinden. Bei einer in dieser Konfiguration arbeitenden HSR-RedBox handelt es sich um einen doppelt angebotenen Knoten, welcher das HSR-Protokoll umsetzt (DANH, Double Attached Node implementing HSR). Bei einem Standard Ethernet-Gerät, welches über eine HSR-RedBox an den HSR-Ring angeschlossen ist, spricht man von einem VDANH (Virtual Doubly Attached Node implementing HSR).

Wie bei PRP versendet der übertragende HSR-Knoten bzw. die HSR-RedBox innerhalb des Rings doppelte Pakete, d.h. 1 Paket in jede Richtung. Zur Identifizierung fügt der HSR-Knoten den doppelten Paketen eine HSR-Markierung hinzu. Die HSR-Markierung besteht aus einer Port-Kennung, der Länge der Nutzdaten und einer fortlaufenden Nummer. In einem normal arbeitenden Ring empfängt der Ziel-HSR-Knoten oder die RedBox beide Pakete innerhalb eines gewissen Zeitversatzes. Ein HSR-Knoten leitet das zuerst ankommende Paket weiter und verwirft das zweite Paket bei dessen Ankunft. Eine RedBox hingegen leitet das erste Paket an die VDANHs weiter und verwirft das zweite Paket bei dessen Ankunft.

Die HSR-Knoten und HSR-RedBoxes fügen dem Paket nach der Quell-MAC-Adresse ein HSR-Tag hinzu. Der Vorteil der Platzierung des HSR-Tags besteht darin, dass das Gerät dadurch dazu imstande ist, das Paket direkt nach dem Empfang des HSR-Headers und der Durchführung der doppelten Erkennung weiterzuleiten. Darüber hinaus wird dadurch die Verzögerungszeit innerhalb des Gerätes verkürzt. Im Gegensatz dazu enthält der RCT beim PRP am Ende des Pakets ein PRP-Suffix. Das bedeutet, dass ein PRP-Gerät das Paket vollständig empfängt, bevor es das Paket an den korrekten Port weiterleitet.

HSR-Knoten und HSR-RedBoxes verwenden außerdem die LRE-Funktion wie im Kapitel zum PRP beschrieben. Ebenso wie bei PRP sind die LRE in den HSR-RedBoxes für die Markierung und die doppelte Erkennung zuständig.

Die Anzahl von HSR-Knoten im Ring sollte 50 nicht überschreiten.

Sinnvoll ist, den in den HSR Ring eingespeisten Verkehr zu limitieren. Befinden sich Fremdgeräte mit höheren Latenzzeiten im Ring, reduzieren Sie die Anzahl der Ring-Teilnehmer dementsprechend. Vergewissern Sie sich, dass die Summe der an den HSR-Knoten eingespeisten Bandbreiten unter 84 % liegt.

Anmerkung: *HSR* ist für Geräte mit FPGA (Hardware für erweiterte Funktionen) verfügbar. Ob Ihr Gerät *HSR* unterstützt, können Sie anhand des Produktcodes feststellen. Um die Funktionen zu nutzen, laden Sie die Geräte-Software mit Unterstützung für *HSR*.

12.4.2 HSR-Netzstruktur

Ein HSR-Netz besteht aus einem Ring, in dem jedes HSR-Gerät eine spezifische Funktion im Netz ausführt. Beispielsweise verbindet ein HSR-Gerät Standard-Ethernet-Geräte mit einem HSR-Ring bzw. PRP-LANs mit einem HSR-Ring.

■ SANs mit einem HSR-Netz verbinden

Standard-Ethernet-Geräte, wie Laptops und Drucker besitzen 1 Netzanschlussstelle. Dadurch übertragen Standard-Ethernet-Geräte Datenverkehr über einen HSR-Ring durch eine HSR-RedBox, die als Proxy für die daran angeschlossenen Ethernet-Geräte dient. Die HSR-RedBox-Schnittstellen versenden doppelte Pakete, d. h. je 1 Paket in jede Richtung des Netzes.

Die Host-RedBox leitet ausschließlich das erste Unicast-Paket an den Ziel-VDANH weiter und verwirft das zweite Paket bei dessen Ankunft.

Die HSR-Knoten und RedBoxes leiten Multicast- und Broadcast-Datenverkehr um den Ring herum sowie an die angeschlossenen VDANH-Geräte. Um zu verhindern, dass der Datenverkehr in einer Endlosschleife um den Ring herum kreist, verwirft der Knoten, der ursprünglich den Datenverkehr im Netz überträgt, die übertragenen Rahmen bei deren Empfang.

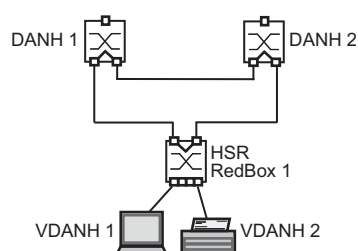


Abb. 35: VDANH mit einem HSR-Netz verbinden

■ Beispielkonfiguration: SAN-Geräte verbinden

Ein einfaches HSR-Netz besteht aus 3 HSR-Geräten (siehe Abbildung oben). In dem folgenden Beispiel wird die Konfiguration einer Host-HSR-RedBox für Standard-Ethernet-Geräte vorgenommen.

Deaktivieren Sie STP auf den PRP-Ports oder global. Deaktivieren Sie außerdem MRP auf den PRP-Ports, oder konfigurieren Sie MRP auf Ports, bei denen es sich nicht um die PRP-Ports handelt.

- Öffnen Sie den Dialog *Switching > L2-Redundanz > MRP*.
- Um die Funktion auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- Vergewissern Sie sich, dass es sich bei den Ports in den Rahmen *Ring-Port 1* und *Ring-Port 2* nicht um dieselben Ports handelt, die von der *HSR*-Funktion verwendet werden.
- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- Um die Funktion auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- Deaktivieren Sie auf der Registerkarte *CIST* in der Spalte *STP aktiv* die für HSR verwendeten Ports.
- Deaktivieren Sie auf der Registerkarte *Guards* in den Spalten *Root guard*, *TCN guard* und *Loop guard* die für HSR verwendeten Ports.

Anmerkung: Wenn Sie die HSR-Funktion deaktivieren, ist die Deaktivierung von Port „A“ oder Port „B“ erforderlich, um Schleifen im Netz zu vermeiden.


Das Gerät sendet entweder ausschließlich seine eigenen HSR-Supervision-Pakete oder sowohl seine eigenen Supervision-Pakete als auch die Pakete der angeschlossenen Geräte. Deaktivieren Sie diese Funktion nach der Installation von neuen HSR-Geräten, um einen Überblick über die HSR-Supervision-Pakete auf entfernten Geräten zu erhalten.



- Öffnen Sie den Dialog *Switching > L2-Redundanz > HSR > HSR > HSR > Konfiguration*.
- Aktivieren Sie für die Analyse der empfangenen HSR-Supervision-Pakete das Kontrollkästchen *Supervision-Pakete evaluieren* im Rahmen *Empfänger Supervision-Paket*.
- Aktivieren Sie *Aktiv* im Rahmen *Absender Supervision-Paket*, um die HSR-Supervision-Pakete aus diesem Gerät zu übertragen.
- Aktivieren Sie *VDAN-Pakete senden*, um Pakete für die im Dialog *Switching > L2-Redundanz > HSR > DAN/VDAN-Tabelle* gelisteten VDANs zu übertragen.

Führen Sie für die Konfiguration von HSR-RedBox 1 die folgenden Schritte aus:


- Setzen Sie den *HSR mode* auf `modeu`, um das Gerät so zu konfigurieren, dass es den Unicast-Datenverkehr um den Ring herum an das Zielgerät weiterleitet.
- Setzen Sie *Switching node type* auf `hsrredboxsan`, um das Gerät als HSR-Host zu konfigurieren.

Anmerkung: Wird *Switching node type* auf `hsrredboxsan` gesetzt, wird die Funktion *Redbox-Identity* deaktiviert.

- Um die Ports einzuschalten, wählen Sie in den Rahmen *Port A* und *Port B* das Optionsfeld *An*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
- Klicken Sie die Schaltfläche , um die im flüchtigen Speicher gespeicherte Konfiguration zu laden.
- Öffnen Sie den Dialog *Switching > L2-Redundanz > HSR > DAN/VDAN-Tabelle*, um den aus dem LAN empfangenen Datenverkehr anzuzeigen. Auf der Grundlage dieser Informationen können Sie feststellen, wie die LANs funktionieren.

- Um diese Liste zu löschen, klicken Sie *Zurücksetzen*.
- Um die Tabelleneinträge zu aktualisieren, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Switching > L2-Redundanz > HSR > Proxy-Node-Tabelle*, um die Abschluss-VDAN-Geräte anzuzeigen, für das dieses Gerät die HSR-Umsetzung bereitstellt.
- Wählen Sie *Zurücksetzen*, um die Einträge aus der Proxy-Tabelle zu entfernen.
- Um die Tabelleneinträge zu aktualisieren, klicken Sie die Schaltfläche .

Das Gerät ermittelt Fehler und zeigt diese in Übereinstimmung mit den in der MIB verwalteten Objekten und den jeweiligen Verbindungen an.

- Öffnen Sie den Dialog *Switching > L2-Redundanz > HSR > HSR Statistiken*, um die Qualität des Datenverkehrs anzuzeigen, der das Gerät durchquert.
- Um die Einträge in der Statistik-Tabelle zu entfernen, klicken Sie *Zurücksetzen*.
- Um die aktuellen Statistiken zu laden, klicken Sie die Schaltfläche .

Eine weitere Möglichkeit ist die Konfiguration der Host-HSR-RedBox 1 über die folgenden CLI-Befehle:

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>configure</code>	Wechsel in den Konfigurationsmodus.
<code>no mrp operation</code>	Deaktivieren dieser Funktion
<code>no spanning-tree operation</code>	Deaktivieren dieser Funktion
<code>interface 1/1</code>	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
<code>no shutdown</code>	Aktivieren der Schnittstelle
<code>exit</code>	Wechsel in den Konfigurationsmodus.
<code>interface 1/2</code>	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
<code>no shutdown</code>	Aktivieren der Schnittstelle
<code>exit</code>	Wechsel in den Konfigurationsmodus.
<code>hsr instance 1 mode modeu</code>	Weiterleiten des Unicast-Datenverkehrs an die verbundenen VDANs und um den Ring herum durch den HSR-Host.
<code>hsr instance 1 port-a</code>	Aktivieren des HSR-Ports A.
<code>hsr instance 1 port-b</code>	Aktivieren des HSR-Ports B.
<code>hsr instance 1 switching-node-type hsrredboxsan</code>	Einrichten des Gerätes dahingehend, dass es den für LAN B des PRP-Netzes bestimmten Datenverkehr verarbeitet.
<code>hsr instance 1 supervision evaluate</code>	Aktivieren der Auswertung empfangener Supervision-Pakete.
<code>hsr instance 1 supervision send</code>	Aktivieren der Übertragung von Supervision-Paketen.
<code>hsr instance 1 supervision redbox-exclusively</code>	Sendet Supervision-Pakete ausschließlich für diese RedBox. Verwenden Sie die <code>no</code> -Form des Kommandos, um Supervision-Pakete für jeden angeschlossenen VDAN und diese RedBox zu senden. Voraussetzung ist, dass Sie die Funktion zum Senden von Supervision-Paketen aktivieren.
<code>hsr operation</code>	Einschalten der <i>HSR</i> -Funktion.

Zeigen Sie über die Anzeigebefehle die Statistik zum Datenverkehr eines Gerätes an.

<code>show hsr counters</code>	Anzeige der HSR-Zählerdaten.
<code>show hsr node-table</code>	Anzeige der Knotentabelle.
<code>show hsr proxy-node-table</code>	Anzeige der Proxy-Node-Tabelle.

■ HSR- und PRP-Netzverbindungen

Beim Verbinden der PRP-Netze mit einem HSR-Netz verwendet das HSR-Gerät 2 Schnittstellen, um die Verbindung mit dem HSR-Ring herzustellen. Das HSR-Gerät verwendet eine dritte Schnittstelle, um die Verbindung mit LAN A oder LAN B des PRP-Netzes herzustellen (siehe folgende Abbildung). Das HSR-Gerät, das den Datenverkehr über den HSR-Ring überträgt, ermittelt den für PRP-Netze bestimmten Datenverkehr mit der entsprechenden Markierung. Die HSR-Geräte leiten anschließend den PRP-Datenverkehr über LAN A oder LAN B weiter. Das PRP-Gerät empfängt den Datenverkehr und verarbeitet ihn wie im Kapitel zum PRP beschrieben.

Die HSR-Geräte identifizieren und markieren den Datenverkehr für bis zu 7 mit 1 HSR-Ring verbundene PRP-Netze.

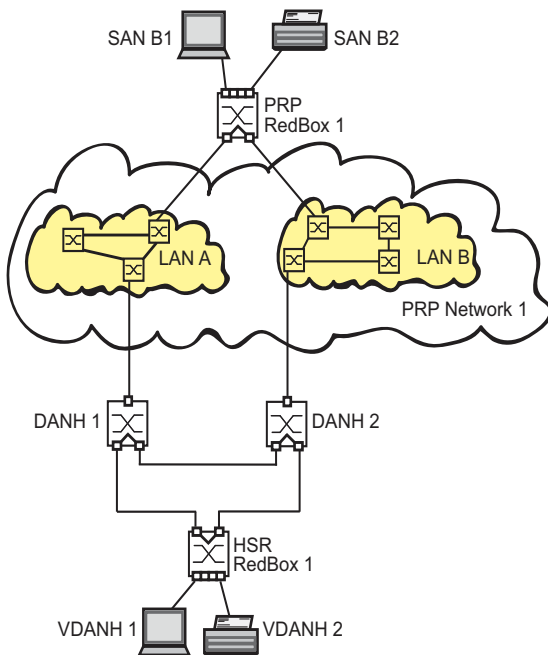


Abb. 36: PRP-Netz mit einem HSR-Netz verbinden

HSR-RedBoxes verwenden 2 Schnittstellen für den HSR-Ring. Sind diese dahingehend konfiguriert, dass sie den PRP-Datenverkehr verwalten, stellt eine dritte Schnittstelle eine Verbindung mit einem LAN des PRP-Netzes her. Die weiteren Schnittstellen stellen einen HSR-Netzzugriff für VDANs bereit. Die HSR-RedBox listet die angeschlossenen VDANs in der *Switching > L2-Redundanz > HSR > Proxy-Node-Tabelle* auf.

■ Beispielkonfiguration: PRP-Netzverbindung

In dem folgenden Beispiel wird ein einfaches HSR-Netz mit 3 HSR-Geräten konfiguriert (siehe Abbildung oben). Verwenden Sie die im vorigen Beispiel konfigurierte HSR-RedBox, um die Standard-Ethernet-Geräte mit einem HSR-Ring zu verbinden. HSR-RedBox 1 sendet 1 doppeltes Paket an DANH 1 und ein doppeltes Gerät an DANH 2. Bei Ankunft des ersten der beiden Pakete sendet DANH 1 das Paket ins PRP-Netz 1, LAN A; DANH 2 sendet das Paket ins PRP-Netz 1, LAN B.

Deaktivieren Sie STP auf den PRP-Ports oder global. Deaktivieren Sie außerdem MRP auf den PRP-Ports, oder konfigurieren Sie MRP auf Ports, bei denen es sich nicht um die PRP-Ports handelt.

Verwenden Sie die im vorigen Beispiel für HSR-RedBox 1 konfigurierte HSR-RedBox. Führen Sie auf DANH 1 und DANH 2 die folgenden Schritte aus.


- Öffnen Sie den Dialog *Switching > L2-Redundanz > MRP*.
- Um die Funktion auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- Vergewissern Sie sich, dass es sich bei den Ports in den Rahmen *Ring-Port 1* und *Ring-Port 2* nicht um dieselben Ports handelt, die von der *HSR*-Funktion verwendet werden.
- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- Um die Funktion auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- Deaktivieren Sie auf der Registerkarte *CIST* in der Spalte *STP aktiv* die für HSR verwendeten Ports.
- Deaktivieren Sie auf der Registerkarte *Guards* in den Spalten *Root guard*, *TCN guard* und *Loop guard* die für HSR verwendeten Ports.

Anmerkung: Wenn Sie die HSR-Funktion deaktivieren, ist die Deaktivierung von Port „A“ oder Port „B“ erforderlich, um Schleifen im Netz zu vermeiden.

Das Gerät sendet entweder ausschließlich seine eigenen HSR-Supervision-Pakete oder sowohl seine eigenen Supervision-Pakete als auch die Pakete der angeschlossenen Geräte. Deaktivieren Sie diese Funktion nach der Installation von neuen HSR-Geräten, um einen Überblick über die HSR-Supervision-Pakete auf entfernten Geräten zu erhalten.


- Öffnen Sie den Dialog *Switching > L2-Redundanz > HSR > HSR > HSR > Konfiguration*.
- Aktivieren Sie für die Analyse der empfangenen HSR-Supervision-Pakete das Kontrollkästchen *Supervision-Pakete evaluieren* im Rahmen *Empfänger Supervision-Paket*.
- Aktivieren Sie *Aktiv* im Rahmen *Absender Supervision-Paket*, um die HSR-Supervision-Pakete aus diesem Gerät zu übertragen.
- Aktivieren Sie *VDAN-Pakete senden*, um Pakete für die im Dialog *Switching > L2-Redundanz > HSR > DAN/VDAN-Tabelle* gelisteten VDANs zu übertragen.

Führen Sie für die Konfiguration von DANH 1 die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > L2-Redundanz > HSR > HSR > HSR > Konfiguration*.
- Setzen Sie den *HSR mode* auf *modeu*, um das Gerät so zu konfigurieren, dass es den Unicast-Datenverkehr um den Ring herum an das Zielgerät weiterleitet.
- Um das Gerät dahingehend zu konfigurieren, dass es Datenverkehr an PRP-LAN A weiterleitet, setzen Sie den *Switching node type* auf *hsrredboxprpa*.
- Um das Gerät dahingehend zu konfigurieren, dass es Datenverkehr an PRP-Netz 1, LAN A weiterleitet, setzen Sie *Redbox-Identity* auf *id1a*.
- Um die Ports einzuschalten, wählen Sie in den Rahmen *Port A* und *Port B* das Optionsfeld *An*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
- Klicken Sie die Schaltfläche , um die im flüchtigen Speicher gespeicherte Konfiguration zu laden.

Führen Sie für die Konfiguration von DANH 2 die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > L2-Redundanz > HSR > HSR > HSR > Konfiguration*.
- Setzen Sie den *HSR mode* auf *modeu*, um das Gerät so zu konfigurieren, dass es den Unicast-Datenverkehr um den Ring herum an das Zielgerät weiterleitet.
- Um das Gerät dahingehend zu konfigurieren, dass es Datenverkehr an PRP-LAN A weiterleitet, setzen Sie den *Switching node type* auf *hsrredboxprpb*.

- Um das Gerät dahingehend zu konfigurieren, dass es Datenverkehr an PRP-Netz 1, LAN B weiterleitet, setzen Sie den *Redbox-Identity* auf `id1b`.
- Um die Ports einzuschalten, wählen Sie in den Rahmen *Port A* und *Port B* das Optionsfeld *An*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
- Klicken Sie die Schaltfläche , um die im flüchtigen Speicher gespeicherte Konfiguration zu laden.

Sie haben außerdem die Möglichkeit, die folgenden CLI-Befehle für die Konfiguration von HSR-Gerät 1 und 2 zu verwenden.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>configure</code>	Wechsel in den Konfigurationsmodus.
<code>no mrp operation</code>	Deaktivieren dieser Funktion
<code>no spanning-tree operation</code>	Deaktivieren dieser Funktion
<code>interface 1/1</code>	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
<code>no shutdown</code>	Aktivieren der Schnittstelle
<code>exit</code>	Wechsel in den Konfigurationsmodus.
<code>interface 1/2</code>	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
<code>no shutdown</code>	Aktivieren der Schnittstelle
<code>exit</code>	Wechsel in den Konfigurationsmodus.

Verwenden Sie die folgenden CLI-Befehle, um DANH 1 so zu konfigurieren, dass er Datenverkehr für PRP-Netz 1, LAN A verarbeitet.

<code>hsr instance 1 mode modeu</code>	Weiterleiten des Unicast-Datenverkehrs an die verbundenen VDANs und um den Ring herum durch den HSR-Host.
<code>hsr instance 1 port-a</code>	Aktivieren des HSR-Ports A.
<code>hsr instance 1 port-b</code>	Aktivieren des HSR-Ports B.
<code>hsr instance 1 switching-node-type hsrredboxprpa</code>	Einrichten des Gerätes dahingehend, dass es den für LAN A des PRP-Netzes bestimmten Datenverkehr verarbeitet.
<code>hsr instance 1 redbox-id id1a</code>	Einrichten des Gerätes dahingehend, dass es den für LAN A des PRP-Netzes 1 bestimmten Datenverkehr verarbeitet.
<code>hsr instance 1 supervision evaluate</code>	Aktivieren der Auswertung empfangener Supervision-Pakete.
<code>hsr instance 1 supervision send</code>	Aktivieren der Übertragung von Supervision-Paketen.
<code>hsr instance 1 supervision redbox-exclusively</code>	Sendet Supervision-Pakete ausschließlich für diese RedBox. Verwenden Sie die <code>no</code> -Form des Kommandos, um Supervision-Pakete für jeden angeschlossenen VDAN und diese RedBox zu senden. Voraussetzung ist, dass Sie die Funktion zum Senden von Supervision-Paketen aktivieren.
<code>hsr operation</code>	Einschalten der <i>HSR</i> -Funktion.

Verwenden Sie die folgenden CLI-Befehle, um DANH 1 so zu konfigurieren, dass er Datenverkehr für PRP-Netz 1, LAN B verarbeitet.

<code>hsr instance 1 mode modeu</code>	Weiterleiten des Unicast-Datenverkehrs an die verbundenen VDANs und um den Ring herum durch den HSR-Host.
<code>hsr instance 1 port-a</code>	Aktivieren des HSR-Ports A.
<code>hsr instance 1 port-b</code>	Aktivieren des HSR-Ports B.
<code>hsr instance 1 switching-node-type hsrredboxprpb</code>	Einrichten des Gerätes dahingehend, dass es den für LAN B des PRP-Netzes bestimmten Datenverkehr verarbeitet.
<code>hsr instance 1 redbox-id id1b</code>	Einrichten des Gerätes dahingehend, dass es den für LAN B des PRP-Netzes 1 bestimmten Datenverkehr verarbeitet.
<code>hsr instance 1 supervision evaluate</code>	Aktivieren der Auswertung empfangener Supervision-Pakete.
<code>hsr instance 1 supervision send</code>	Aktivieren der Übertragung von Supervision-Paketen.

```
hsr instance 1 supervision  
redbox-exclusively
```

Sendet Supervision-Pakete ausschließlich für diese RedBox. Verwenden Sie die `no`-Form des Kommandos, um Supervision-Pakete für jeden angeschlossenen VDAN und diese RedBox zu senden. Voraussetzung ist, dass Sie die Funktion zum Senden von Supervision-Paketen aktivieren.

```
hsr operation
```

Einschalten der **HSR**-Funktion.

Zeigen Sie über die Anzeigebefehle die Statistik zum Datenverkehr eines Gerätes an.

```
show hsr counters  
show hsr node-table  
show hsr proxy-node-table
```

Anzeige der HSR-Zählerdaten.

Anzeige der Knotentabelle.

Anzeige der Proxy-Node-Tabelle.

12.5 Spanning Tree

Anmerkung: Das Spanning-Tree-Protokoll ist ein Protokoll für MAC-Bridges. Daher verwendet die folgende Beschreibung den Begriff Bridge für das Gerät.

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

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

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

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

Anmerkung: RSTP löst eine Schicht-2-Netztopologie mit redundanten Pfaden in eine Baumstruktur (Spanning Tree) auf, die keine redundanten Pfade mehr enthält. Eines der Geräte übernimmt dabei die Rolle der Root-Bridge. Die maximal erlaubte Anzahl der Geräte in einem aktiven Ast von der Root-Bridge bis zur Astspitze können Sie durch die Variable `Max Age` der aktuellen Root-Bridge vorgeben. Der voreingestellte Wert für `Max Age` ist 20, er kann bis auf 40 erhöht werden. Wenn das als Root arbeitende Gerät ausfällt und ein anderes Gerät dessen Funktion übernimmt, bestimmt die neue Root-Bridge die größtmögliche erlaubte Anzahl der Geräte in einem Ast durch ihre `Max Age`-Einstellung.

Anmerkung: Der RSTP-Standard schreibt vor, dass alle Geräte innerhalb eines Netzes mit dem (Rapid-) Spanning-Tree-Algorithmus arbeiten. Bei gleichzeitigem Einsatz von STP und RSTP gehen in den Netz-Segmenten, die gemischt betrieben werden, die Vorteile der schnelleren Rekonfiguration bei RSTP verloren.

Ein Gerät, das lediglich RSTP unterstützt, arbeitet mit MSTP-Geräten zusammen, indem es sich keiner MST-Region, sondern dem CST (Common Spanning Tree) zuweist.

■ Root-Pfadkosten

Jedem Pfad, der 2 Bridges miteinander verbindet, weisen die Bridges Kosten für die Übertragung (Pfadkosten) zu. Das Gerät bestimmt diesen Wert in Abhängigkeit von der Datenrate (siehe [Tabelle 23](#)). Dabei weist sie Pfaden mit niedrigerer Datenrate die höheren Pfadkosten zu.

Alternativ dazu kann auch der Administrator die Pfadkosten festlegen. Dabei weist er - wie das Gerät - Pfaden mit niedrigerer Datenrate die höheren Pfadkosten zu. Da er aber diesen Wert letztendlich frei wählen kann, verfügt er hiermit über ein Werkzeug, bei redundanten Pfaden einem bestimmten Pfad den Vorzug zu geben.

Die Root-Pfadkosten sind die Summe aller Einzelpfadkosten der Pfade, die ein Datenpaket zwischen dem angeschlossenen Port einer Bridge und der Root-Bridge passiert.

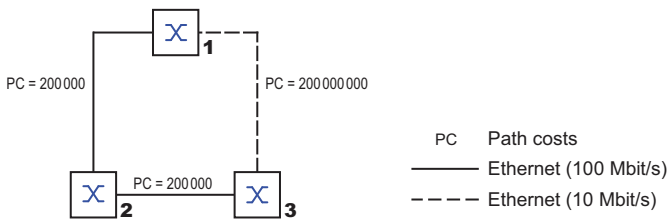


Abb. 38: Pfadkosten

Datenrate	Empfohlener Wert	Empfohlener Bereich	Möglicher Bereich
≤100 Kbit/s	200 000 000 ^a	20000000-200000000	1-200000000
1 Mbit/s	20000000 ^a	2000000-200000000	1-200000000
10 Mbit/s	2000000 ^a	200000-20000000	1-200000000
100 Mbit/s	200000 ^a	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200 000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

Tab. 23: Empfohlene Pfadkosten beim RSTP in Abhängigkeit von der Datenrate.

a. Bridges, die zu IEEE 802.1D 1998 konform sind, und ausschließlich 16 Bit-Werte für Pfadkosten unterstützen, sollten als Pfadkosten den Wert 65.535 (FFFFH) verwenden, wenn Sie sie zusammen mit Bridges benutzen, die 32 Bit-Werte für die Pfadkosten unterstützen.

■ Port-Identifikation

Die Portidentifikation besteht aus 2 Bytes. Ein Teil, das niederwertigste Byte, enthält die physikalischen Portnummer. Dies gewährleistet eine eindeutige Bezeichnung des Port dieser Bridge. Der zweite, höherwertige Teil ist die Port-Priorität, die der Administrator festlegt (Voreinstellung: 128). Auch hier gilt: Der Port mit dem kleinsten Zahlenwert für die Portidentifikation besitzt die höchste Priorität.

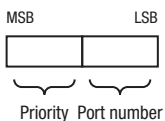


Abb. 39: Port-Identifikation

■ MaxAge und Diameter

Die Größen „MaxAge“ und „Diameter“ bestimmen maßgeblich die maximale Ausdehnung eines Spanning-Tree-Netzes.

■ Diameter

Die Anzahl der Verbindungen zwischen den am weitesten voneinander entfernten Geräten im Netz heißt Netzdurchmesser (Diameter).

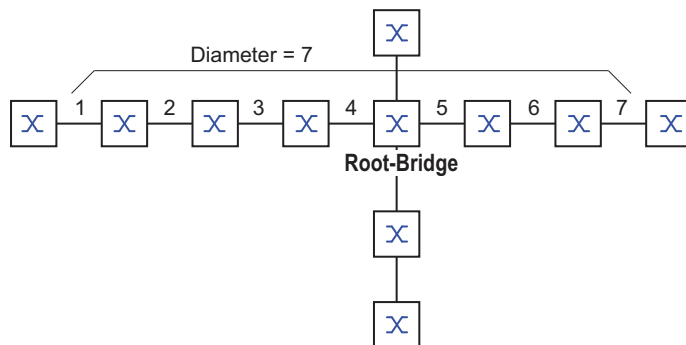


Abb. 40: Definition „Diameter“

Der im Netz erreichbare Netzdurchmesser beträgt $\text{MaxAge}-1$.

Im Lieferzustand ist $\text{MaxAge} = 20$, der maximal erreichbare Diameter = 19. Wenn Sie für MaxAge den Maximalwert 40 einstellen, ist der maximal erreichbare Diameter = 39.

■ MaxAge

Jede STP-BPDU enthält einen Zähler „MessageAge“. Der Zähler erhöht sich beim Durchlaufen einer Bridge um 1.

Die Bridge vergleicht vor dem Weiterleiten einer STP-BPDU den Zähler „MessageAge“ mit dem im Gerät festgelegten Wert „MaxAge“:

- Ist MessageAge < MaxAge, leitet die Bridge die STP-BPDU an die nächste Bridge weiter.
- Ist MessageAge = MaxAge, verwirft die Bridge die STP-BPDU.

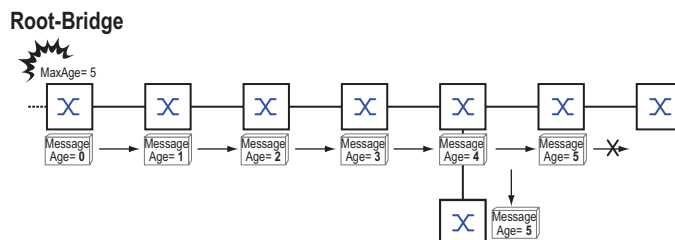


Abb. 41: Übertragung einer STP-BPDU in Abhängigkeit von MaxAge

12.5.2 Regeln für die Erstellung der Baumstruktur

■ Bridge-Information

Zur Berechnung der Baumstruktur benötigen die Bridges nähere Informationen über die anderen Bridges, die sich im Netz befinden.

Um diese Informationen zu erhalten, sendet jede Bridge eine BPDU (Bridge Protocol Data Unit) an andere Bridges.

Bestandteil einer BPDU ist unter anderem:

- ▶ Bridge-Identifikation
- ▶ Root-Pfadkosten
- ▶ Port-Identifikation

(siehe IEEE 802.1D)

■ Aufbauen der Baumstruktur

- ▶ Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation nennt man auch Root-Bridge. Sie bildet die Root (Wurzel) der Baumstruktur
- ▶ Der Aufbau des Baumes hängt von den Root-Pfadkosten ab. Spanning Tree wählt die Struktur so, dass die minimalen Pfadkosten zwischen jeder einzelnen Bridge zur Root-Bridge entstehen.
- ▶ Bei mehreren Pfaden mit gleichen Root-Pfadkosten entscheidet die von der Root weiter entfernte Bridge, welchen Port sie blockiert. Sie verwendet dazu die Bridge-Identifikationen der näher an der Root liegenden Bridges. Die Bridge blockiert den Port, der zu der Bridge mit der numerisch höheren ID führt (eine numerisch höhere ID ist die logisch schlechtere). Haben 2 Bridges die gleiche Priorität, hat die Bridge mit der numerisch größeren MAC-Adresse die numerisch höhere ID, dies ist die logisch schlechtere.
- ▶ Wenn von einer Bridge mehrere Pfade mit den gleichen Root-Pfadkosten zu der selben Bridge führen, zieht die von der Root weiter entfernte Bridge als letztes Kriterium die Port-Identifikation der anderen Bridge heran ([siehe Abbildung 39](#)). Die Bridge blockiert dabei den Port, der zu dem Port mit der schlechteren ID führt. Haben 2 Ports die selbe Priorität, ist die ID mit der höheren Port-Nr. die schlechtere.

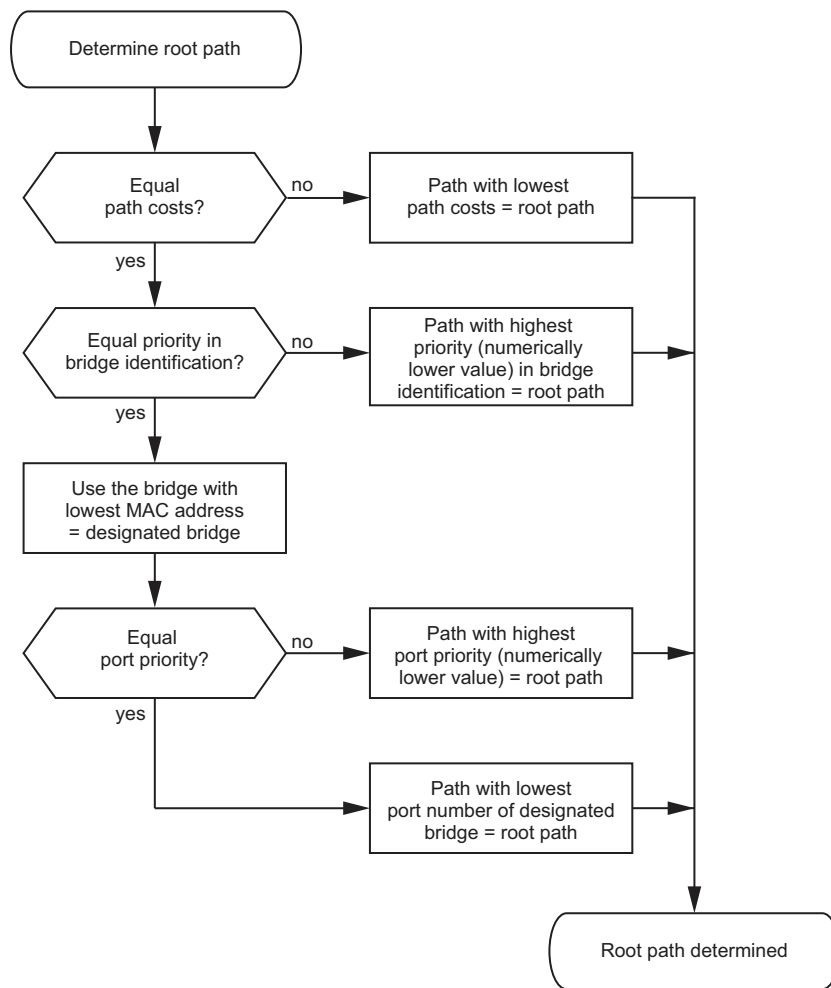
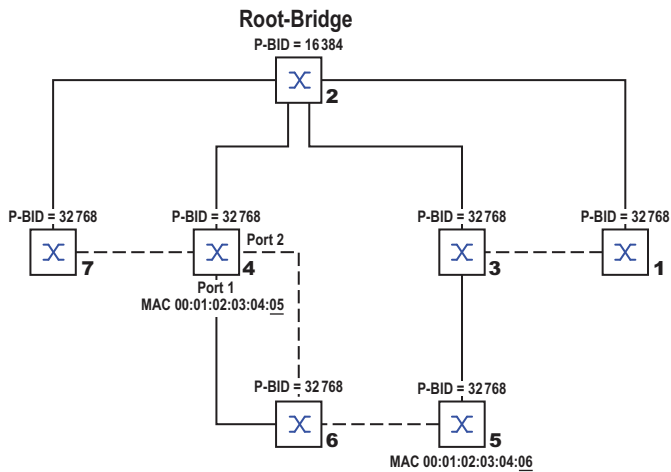


Abb. 42: Flussdiagramm Root-Pfad festlegen

■ Beispiel für die Manipulation der Baumstruktur

Der Management-Administrator des Netzes stellt bald fest, dass diese Konfiguration mit Bridge 1 als Root-Bridge ungünstig ist. Auf den Pfaden zwischen Bridge 1 zu Bridge 2 und Bridge 1 zu Bridge 3 summieren sich die Kontrollpakete, die die Root-Bridge zu allen anderen Bridges sendet. Konfiguriert der Management-Administrator die Bridge 2 als Root-Bridge, dann verteilt sich die Belastung der Teilnetze durch Kontrollpakete wesentlich besser. Hieraus entsteht die dargestellte Konfiguration (siehe Abbildung 45). Die Pfadkosten der meisten Bridges zur Root-Bridge sind kleiner geworden.



P-BID Priority of the bridge identification (BID)
= BID without MAC Address

— Root path
- - - - Interrupted path

Abb. 45: Beispiel für die Manipulation der Baumstruktur

12.5.4 Das Rapid Spanning Tree Protokoll

Das RSTP behält die Berechnung der Baumstruktur vom STP unverändert bei. RSTP ändert lediglich Parameter und fügt neue Parameter und Mechanismen hinzu, die die Rekonfiguration beschleunigen, falls eine Verbindung oder eine Bridge ausfällt.

Eine zentrale Bedeutung erfahren in diesem Zusammenhang die Ports.

■ Port-Rollen

RSTP weist jedem Bridge-Port eine der folgenden Rollen zu ([siehe Abbildung 46](#)):

- ▶ **Root-Port:**
Dies ist der Port, an dem eine Bridge Datenpakete mit den niedrigsten Pfadkosten von der Root-Bridge empfängt.
Existieren mehrere Ports mit gleich niedrigen Pfadkosten, dann entscheidet die Bridge-Identifikation der zur Root führenden Bridge (Designated Bridge), welchem ihrer Ports die weiter von der Root entfernte Bridge die Rolle des Root-Ports gibt.
Hat eine Bridge mehrere Ports mit gleich niedrigen Pfadkosten zur selben Bridge, entscheidet die Bridge anhand der Portidentifikation der zur Root führenden Bridge (Designated Bridge), welchen Port sie lokal als Root-Port wählt ([siehe Abbildung 42](#)).
Die Root-Bridge selbst besitzt keinen Root-Port.
- ▶ **Designierter Port (Designated-Port):**
Die Bridge in einem Netzsegment, die die niedrigsten Root-Pfadkosten hat, ist die designierte Bridge (Designated Bridge).
Haben mehrere Bridges die gleichen Root-Pfadkosten, übernimmt die Bridge mit der zahlenmäßig kleinsten Bridge-Identifikation die Rolle der designierten Bridge. Der designierte Port an dieser Bridge ist der Port, der ein von der Root-Bridge wegführendes Netzsegment verbindet. Ist eine Bridge mit mehr als einem Port mit einem Netzsegment verbunden (zum Beispiel über einen Hub), gibt sie ihrem Port mit der besseren Port-Identifikation die Rolle des Designated Ports.
- ▶ **Edge-Port**
Ein Edge-Port ist ein Endgeräte-Port am „Rand“ (engl. „Edge“) eines geschichteten Netzes. Jedes Netzsegment, in dem sich keine weitere RSTP-Bridge befindet, ist mit genau einem designierten Port verbunden. Dieser designierte Port ist dann gleichzeitig ein Edge-Port, wenn er keine BPDUs (Spanning Tree Bridge Protocol Data Units) empfangen hat.
- ▶ **Alternate-Port**
Dies ist ein blockierter Port, der beim Ausfall der Verbindung zur Root-Bridge die Aufgabe des Root-Ports übernimmt. Der alternative Port stellt die Verbindung der Bridge zur Root-Bridge hin sicher.
- ▶ **Backup-Port**
Dies ist ein blockierter Port, der als Ersatz zur Verfügung steht, falls die Verbindung zum designierten Port dieses Netzsegmentes (ohne RSTP-Bridges, zum Beispiel ein Hub) ausfällt.
- ▶ **Disabled-Port**
Dies ist ein Port, der innerhalb des Spanning-Tree-Protokolls keine Rolle spielt, also abgeschaltet ist oder keine Verbindung hat.

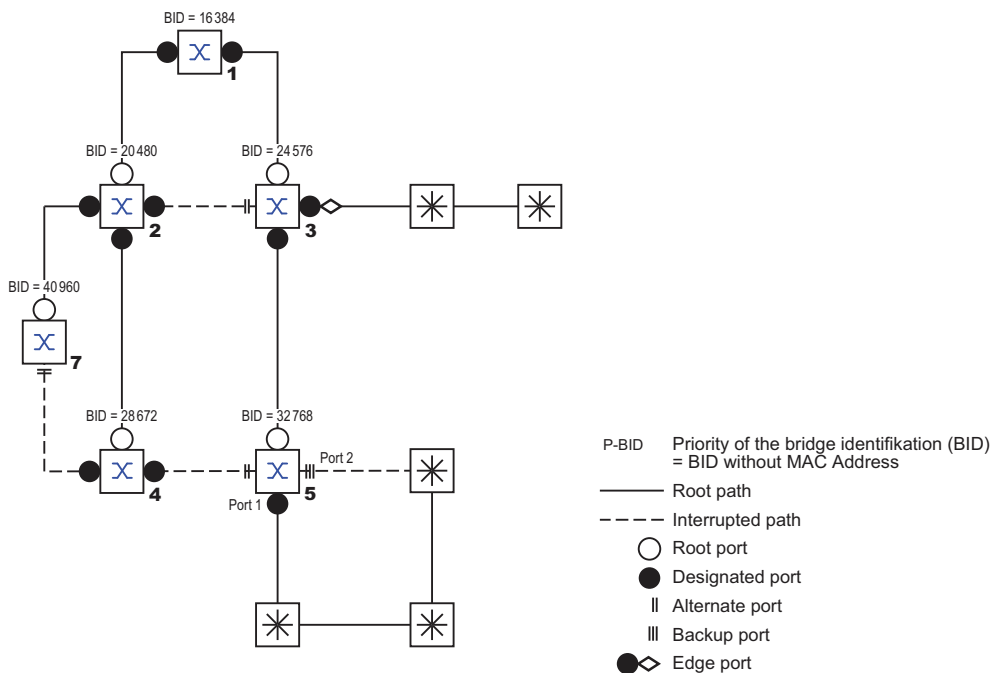


Abb. 46: Port-Rollen-Zuweisung

Port-Status

In Abhängigkeit von der Baumstruktur und dem Status der ausgewählten Verbindungswege weist RSTP den Ports ihren Status zu.

STP Port Status	Administrative Bridge Port-Status	MAC Operational	RSTP Port-Status	Aktive Topologie (Port Rolle)
DISABLED	Ausgeschaltet	FALSE	Die dot1d-MIB zeigt „Disabled“ an	Excluded (Disabled)
DISABLED	Enabled	FALSE	Discarding ^a	Excluded (Disabled)
BLOCKING	Enabled	TRUE	Die dot1d-MIB zeigt „Blocked“ an	Excluded (Alternate, Backup)
LISTENING	Enabled	TRUE	Discarding ^b	Included (Root, Designated)
LEARNING	Enabled	TRUE	Learning	Included (Root, Designated)
FORWARDING	Enabled	TRUE	Forwarding	Included (Root, Designated)

Tab. 24: Beziehung zwischen Port-Status-Werten bei STP und RSTP

Bedeutung der RSTP-Port-Status:

- ▶ Disabled: Port gehört nicht zur aktiven Topologie
- ▶ Discarding: Kein Address Learning in FDB, kein Datenverkehr außer STP-BPDUs
- ▶ Learning: Address Learning aktiv (FDB), kein Datenverkehr außer STPBPDUs
- ▶ Forwarding: Address Learning aktiv (FDB), Senden und Empfangen aller Paket-Typen (nicht ausschließlich STP-BPDUs)

■ Spanning Tree Priority Vector

Um den Ports Rollen zuzuteilen, tauschen die RSTP-Bridges Konfigurationsinformationen untereinander aus. Diese Informationen heißen "Spanning Tree Priority Vector". Sie sind Teil der RST BPDUs und enthalten folgende Informationen:

- ▶ Bridge-Identifikation der Root-Bridge
- ▶ Root-Pfadkosten der sendenden Bridge
- ▶ Bridge-Identifikation der sendenden Bridge
- ▶ Portidentifikation des Ports, durch den die Nachricht gesendet wurde
- ▶ Portidentifikation des Ports, durch den die Nachricht empfangen wurde

Auf Basis dieser Informationen sind die am RSTP beteiligten Bridges in der Lage, selbständig Port-Rollen zu bestimmen und den Port-Status ihrer lokalen Ports zu definieren.

■ Schnelle Rekonfiguration

Warum kann RSTP schneller als STP auf eine Unterbrechung des Root-Pfades reagieren?

- ▶ Einführung von Edge-Ports:
Bei einer Rekonfiguration setzt RSTP einen Edge-Port nach Ablauf von 3 Sekunden (Voreinstellung) in den Vermittlungsmodus und wartet dann "Hello Time" ab, um sich zu vergewissern, dass keine BPDU-sendende Bridge angeschlossen ist.
Wenn der Anwender sicherstellt, dass an diesem Port ein Endgerät angeschlossen ist und bleibt, entstehen im Rekonfigurationsfall an diesem Port keine Wartezeiten
- ▶ Einführung von alternativen Ports:
Da schon im regulären Betrieb die Portrollen verteilt sind, kann eine Bridge sofort nach dem Verlust der Verbindung zur Root-Bridge vom Root-Port zu einem alternativen Port umschalten.
- ▶ Kommunikation mit Nachbar-Bridges (Punkt-zu-Punkt-Verbindungen):
Die dezentrale, direkte Kommunikation zwischen benachbarten Bridges erlaubt ohne Wartezeiten eine Reaktion auf Zustandsänderungen der Spanning-Tree-Topologie.
- ▶ Adresstabelle:
Beim STP bestimmt das Alter der Einträge in der FDB über die Aktualisierung der Kommunikation. Das RSTP löscht sofort und gezielt die Einträge der Ports, die von einer Umkonfiguration betroffen sind.
- ▶ Reaktion auf Ereignisse:
Ohne Zeitvorgaben einhalten zu müssen, reagiert RSTP sofort auf Ereignisse wie Verbindungsunterbrechung, Verbindung vorhanden, u.a.

Anmerkung: Die Kehrseite dieser schnellen Rekonfiguration ist die Möglichkeit, dass Datenpakete während der Rekonfigurationsphase der RSTP-Topologie dupliziert und/oder mit vertauschter Reihenfolge beim Empfänger ankommen können. Wenn Sie dies in Ihrer Anwendung nicht akzeptieren können, dann benutzen Sie das langsamere Spanning Tree Protokoll oder wählen Sie eines der anderen in diesem Buch beschriebenen, schnelleren Redundanzverfahren.

■ STP-Kompatibilitätsmodus

Der STP-Kompatibilitätsmodus bietet Ihnen die Möglichkeit, RSTP-Geräte in Netzen mit Alt-Installationen zu betreiben. Erkennt ein RSTP-Gerät ein älteres STP-Gerät, schaltet es am betreffenden Port den STP-Kompatibilitätsmodus ein.

12.5.5 Gerät konfigurieren

RSTP konfiguriert die Netztopologie komplett selbständig. Das Gerät mit der niedrigsten Bridge-Priorität wird dabei automatisch Root-Bridge. Um dennoch eine bestimmte Netzstruktur vorzugeben, legen Sie ein Gerät als Root-Bridge fest. Im Regelfall übernimmt diese Rolle ein Gerät im Backbone.

- Bauen Sie das Netz nach Ihren Erfordernissen auf, zunächst ohne redundante Strecken.
- Deaktivieren Sie die Flusskontrolle auf den beteiligten Ports.
Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt. (Lieferzustand: Flusskontrolle global ausgeschaltet und auf allen Ports eingeschaltet.)
- Schalten Sie MRP auf allen Geräten aus.
- Schalten Sie Spanning Tree auf allen Geräten im Netz ein.
Im Lieferzustand ist Spanning Tree auf dem Gerät eingeschaltet.
- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- Einschalten der Funktion.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
spanning-tree operation	Schaltet Spanning Tree ein.
show spanning-tree global	Zeigt zur Kontrolle die Parameter an.

- Schließen Sie nun die redundanten Strecken an.
- Legen Sie die Einstellungen für das Gerät fest, das die Rolle der Root-Bridge übernimmt.
- Legen Sie im Feld *Priorität* einen numerisch kleineren Wert fest.
Die Bridge mit der numerisch niedrigsten Bridge-ID hat die höchste Priorität und wird zur Root-Bridge des Netzes.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

spanning-tree mst priority 0 <0..61440 in 4096er-Schritten>	Legt die Bridge-Priorität des Gerätes fest.
--	---

Nach dem Speichern zeigt der Dialog folgende Information:

- Das Kontrollkästchen *Bridge ist Root* ist markiert.
- Das Feld *Root-Port* zeigt den Wert 0.0.
- Das Feld *Root-Pfadkosten* zeigt den Wert 0.

show spanning-tree global	Zeigt zur Kontrolle die Parameter an.
---------------------------	---------------------------------------

- Ändern Sie gegebenenfalls die Werte in den Feldern *Forward-Verzögerung [s]* und *Max age*.
 - Die Root-Bridge übermittelt die geänderten Werte an die anderen Geräte.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

`spanning-tree forward-time <4..30>`

Legt die Verzögerungszeit für Zustandswechsel in Sekunden fest.

`spanning-tree max-age <6..40>`

Legt die maximal zulässige Astlänge fest, d. h. die Anzahl der Geräte bis zur Root-Bridge.

`show spanning-tree global`

Zeigt zur Kontrolle die Parameter an.

Anmerkung: Die Parameter *Forward-Verzögerung [s]* und *Max age* stehen in folgender Beziehung zueinander:

$$\textit{Forward-Verzögerung [s]} \geq (\textit{Max age}/2) + 1$$

Wenn Sie in die Felder einen Wert einfügen, der dieser Beziehung widerspricht, ersetzt das Gerät diese Werte mit den zuletzt gültigen Werten oder mit der Voreinstellung.

Anmerkung: Lassen Sie den Wert im Feld „Hello Time“ möglichst unverändert.

- Prüfen Sie in den anderen Geräten die folgende Werte:
 - Bridge-ID (Bridge-Priorität und MAC-Adresse) des jeweiligen Gerätes sowie der Root-Bridge.
 - Nummer des Geräte-Ports, der zur Root-Bridge führt.
 - Pfadkosten vom Root-Port des Gerätes bis zur Root-Bridge.

`show spanning-tree global`

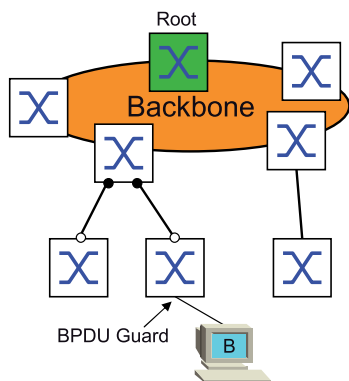
Zeigt zur Kontrolle die Parameter an.

12.5.6 Guards

Das Gerät bietet Ihnen die Möglichkeit, an den Geräte-Ports verschiedene Schutzfunktionen (Guards) zu aktivieren.

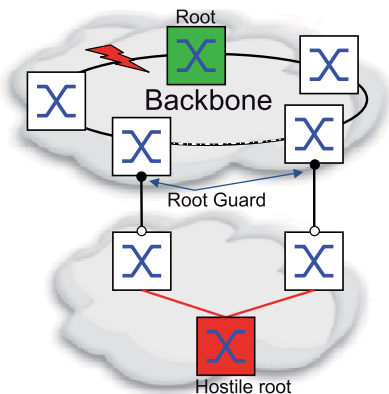
Folgende Schutzfunktionen helfen, Ihr Netz vor Fehlkonfigurationen, Loops und Angriffen mit STP-BPDUs zu schützen:

- ▶ BPDU Guard – für manuell festgelegte Edge-Ports (Endgeräte-Ports)
Diese Schutzfunktion aktivieren Sie global im Gerät.



Endgeräte-Ports empfangen im Normalfall keine STP-BPDUs. Versucht ein Angreifer, auf diesem Port trotzdem STP-BPDUs einzuspeisen, deaktiviert das Gerät den Geräte-Port.

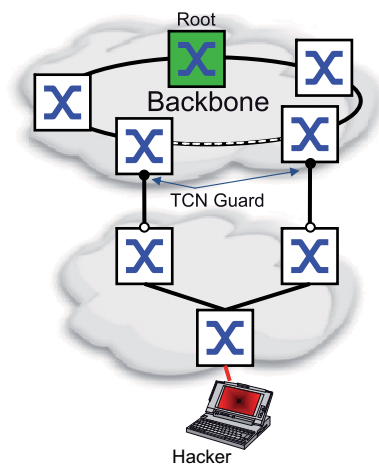
- ▶ Root Guard – für Designated-Ports
Diese Schutzfunktion aktivieren Sie für jeden Geräte-Port separat.



Empfängt ein Designated-Port eine STP-BPDU mit besserer Pfadinformation zur Root-Bridge, verwirft das Gerät die STP-BPDU und setzt den Vermittlungsstatus des Ports auf `discarding` anstatt auf `root`.

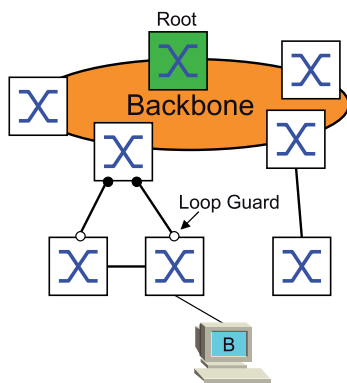
Bleiben die STP-BPDUs mit besserer Pfadinformation zur Root-Bridge aus, setzt das Gerät den Status des Ports nach $2 \times \text{Hello-Time [s]}$ wieder auf einen Wert gemäß Port-Rolle.

- ▶ TCN Guard – für Ports, die STP-BPDUs mit Topology-Change-Flag empfangen
Diese Schutzfunktion aktivieren Sie für jeden Geräte-Port separat.



Bei eingeschalteter Schutzfunktion ignoriert das Gerät Topology-Change-Flags in empfangenem STP-BPDUs. Der Inhalt der Adresstabelle (FDB) des Geräte-Ports bleibt dadurch unverändert. Weitere Informationen in der BPDU, die eine Topologie-Änderung bewirken, verarbeitet das Gerät jedoch.

- ▶ Loop Guard – für Root-, Alternate- und Backup-Ports
Diese Schutzfunktion aktivieren Sie für jeden Geräte-Port separat.



Diese Schutzfunktion verhindert den irrtümlichen Wechsel des Vermittlungsstatus eines Ports auf *forwarding*, falls der Port keine STP-BPDUs mehr empfängt. Tritt dieser Fall ein, kennzeichnet das Gerät den Loop-Status des Ports als inkonsistent, leitet aber keine Datenpakete weiter.

■ BPDU Guard einschalten

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- Markieren Sie das Kontrollkästchen *BPDU-Guard*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
enable
configure
spanning-tree bpdu-guard
show spanning-tree global
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Schaltet den BPDU Guard ein.
Zeigt zur Kontrolle die Parameter an.

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- Wechseln Sie in die Registerkarte *CIST*.
- Markieren Sie für Endgeräte-Ports das Kontrollkästchen in der Spalte *Admin-Edge-Port*.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

interface <x/y>	Wechsel in den Interface-Konfigurationsmodus von Interface <x/y>.
spanning-tree edge-port	Kennzeichnet den Port als Endgeräte-Port (Edge Port).
show spanning-tree port x/y	Zeigt zur Kontrolle die Parameter an.
exit	Verlässt den Interface-Modus.

Empfängt ein Endgeräte-Port eine STP-BPDU, verhält sich das Gerät wie folgt:

- ▶ Das Gerät schaltet diesen Port aus.
Im Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration* ist bei diesem Port das Kontrollkästchen in der Spalte *Port an* unmarkiert.
- ▶ Das Gerät kennzeichnet den Port.

Im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *Guards* ist das Kontrollkästchen in der Spalte *BPDU guard effect* markiert.

show spanning-tree port x/y	Zeigt zur Kontrolle die Parameter des Ports an. Der Wert des Parameters <i>BPDU guard effect</i> ist enabled.
-----------------------------	---

Um den Status des Geräte-Ports wieder auf den Wert *forwarding* zu setzen, verfahren Sie wie folgt:

- Wenn der Port weiterhin BPDUs empfängt:
 - Heben Sie die manuelle Festlegung als Edge-Port (Endgeräte-Port) auf.
oder
 - Deaktivieren Sie den BPDU Guard.
- Schalten Sie den Geräte-Port wieder ein.

■ Root Guard / TCN Guard / Loop Guard einschalten

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- Wechseln Sie in die Registerkarte *Guards*.
- Für Designated-Ports markieren Sie das Kontrollkästchen in der Spalte *Root guard*.
- Für Ports, die STP-BPDUs mit Topology-Change-Flag empfangen, markieren Sie das Kontrollkästchen in der Spalte *TCN guard*.
- Für Root-, Alternate- oder Backup-Ports markieren Sie das Kontrollkästchen in der Spalte *Loop guard*.

Anmerkung: Die Funktionen *Root guard* und *Loop guard* schließen sich gegenseitig aus. Wenn Sie versuchen, die Funktion *Root guard* zu aktivieren, während die Funktion *Loop guard* aktiviert ist, deaktiviert das Gerät die Funktion *Loop guard*.

- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
interface <x/y>	Wechsel in den Interface-Konfigurationsmodus von Interface <x/y>.
spanning-tree guard-root	Schaltet den Root Guard auf dem Designated-Port ein.
spanning-tree guard-tcn	Schaltet den TCN Guard auf dem Port ein, der STP-BPDUs mit Topology-Change-Flag empfängt.
spanning-tree guard-loop	Schaltet den Loop Guard auf einem Root-, Alternate- oder Backup-Port ein.

```
exit
show spanning-tree port x/y
```

Verlässt den Interface-Modus.
Zeigt zur Kontrolle die Parameter des Ports an.

12.5.7 Ring only mode

Verwenden Sie die *Ring only mode*-Funktion, um Vollduplex-Konnektivität zu erkennen, und um Ports zu konfigurieren, die mit Endgeräten verbunden sind. Die *Ring only mode*-Funktion ermöglicht dem Gerät, in den Zustand „forwarding“ zu wechseln und forwardings zu unterdrücken.

■ Ring only mode konfigurieren

Wenn Sie die *Ring only mode*-Funktion auf den Ports aktivieren und das Gerät das Alter herkömmlicher BPDUs ignoriert, sendet das Gerät Topology Change-Nachrichten mit dem Nachrichten-Alter 1.

■ Beispiel

Das vorliegende Beispiel beschreibt die Konfiguration der *Ring only mode*-Funktion.

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Spanning Tree Global*.
- Wählen Sie im Rahmen *Ring only mode*, Feld *Erster Port* den Port 1/1.
- Wählen Sie im Rahmen *Ring only mode*, Feld *Zweiter Port* den Port 1/1.
- Um die Funktion zu aktivieren, markieren Sie im Rahmen *Ring only mode* das Kontrollkästchen *Aktiv*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

```
enable                               Wechsel in den Privileged-EXEC-Modus.
configure                             Wechsel in den Konfigurationsmodus.
spanning-tree ring-only-mode operation Einschalten der Ring only mode-Funktion.
spanning-tree ring-only-mode first-port Festlegen von Port 1/1 als erstes Interface.
1/1
spanning-tree ring-only-mode second-port Festlegen von Port 1/2 als zweites Interface.
1/2
```

12.5.8 RSTP over HSR

Die Funktion RSTP over HSR bietet Ihnen die Möglichkeit, ein RSTP-Netz redundant an einen HSR-Ring zu koppeln.

Daraus folgt:

- ▶ Das Gerät verwendet den logischen Port `hsr/1`.
- ▶ Das Gerät leert die Proxy Node Table, wenn der logische Port `hsr/1` den Zustand von RSTP zu 'forwarding' ändert.

■ RSTP over HSR konfigurieren

HSR bietet eine begrenzte Bandbreite. Bei Redundanz wird RSTP in einer Weise konfiguriert, dass der Datenverkehr ausschließlich über den HSR-Ring weitergeleitet wird.

■ Beispiel

Verwenden Sie die Funktion RSTP over HSR, um ein RSTP-Netz redundant an einen HSR-Ring zu koppeln.

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Spanning Tree Port*.
- Legen Sie für Port 240 in Spalte *Port-Priorität* den Wert `hsr/1` fest.
- Legen Sie für Port 240 in Spalte *Port-Pfadkosten* den Wert `hsr/1` fest.
- Schalten Sie die *Spanning Tree*-Funktion auf Port `hsr/1` ein.
Markieren Sie für Port `hsr/1` das Kontrollkästchen in Spalte *STP aktiv*.

12.6 Link-Aggregation

Link-Aggregation mit dem Single-Switch-Verfahren hilft Ihnen 2 Einschränkungen bei Ethernet-Links zu überwinden, und zwar Bandbreite und Redundanz.

Das erste Problem, bei dem Ihnen die Link-Aggregation-Group- (LAG) Funktion hilft, ist die Bandbreitenbegrenzung von einzelnen Ports. LAG bietet Ihnen die Möglichkeit, 2 oder mehr Verbindungen zu 1 logischen Verbindung zwischen 2 Geräten zusammenzufassen. Die parallelen Links erhöhen die Übertragungsbandbreite zwischen den 2 Geräten.

Link Aggregation verwenden sie üblicherweise im Backbone-Netz. Die Funktion bietet Ihnen die Möglichkeit, die Bandbreite schrittweise, kostengünstig zu erhöhen

Des Weiteren bietet Link Aggregation Redundanz mit einer unterbrechungsfreien Umschaltung. Wenn bei 2 oder mehr parallel konfigurierten Links 1 Link ausfällt, leiten die anderen Links in der Gruppe den Datenverkehr weiter.

Die Voreinstellungen für eine neue Link-Aggregation-Instanz sind:

- ▶ In Spalte *Aktiv* ist das Kontrollkästchen markiert.
- ▶ In Spalte *Trap senden (Link-Up/Down)* ist das Kontrollkästchen markiert.
- ▶ In Spalte *Statische Link-Aggregation* ist das Kontrollkästchen unmarkiert.
- ▶ In Spalte *Aktive Ports (min.)* ist der Wert 1.

12.6.1 Funktionsweise

Das Gerät arbeitet mit dem Single-Switch-Verfahren. Das Single-Switch-Verfahren bietet Ihnen eine kostengünstige Möglichkeit, Ihr Netz zu erweitern. Das Single-Switch-Verfahren legt fest, dass Sie 1 Gerät auf jeder Seite des Links benötigen, um die physischen Ports zur Verfügung zu stellen. Das Gerät verteilt die Netzlast auf die Ports der Gruppenmitglieder.

Das Gerät wendet auch das Same-Link-Speed-Verfahren an, bei dem die Ports der Gruppenmitglieder voll-duplex sind und Punkt-zu-Punkt-Links dieselbe Übertragungsrates haben. Der 1. Port, den der Benutzer der Gruppe hinzufügt, ist der Master-Port und bestimmt die Bandbreite für die weiteren Mitglieder der Link-Aggregation-Group.

Das Gerät bietet Ihnen die Möglichkeit, bis zu 2 Link-Aggregation-Gruppen einzurichten. Die Anzahl der verwendbaren Ports je Link-Aggregation-Gruppe ist abhängig vom Gerät.

12.6.2 Link-Aggregation Beispiel

Verbinden Sie mehrere Workstations, indem Sie 1 aggregierte Link-Gruppe zwischen Switch 1 und 2 verwenden. Durch das Aggregieren mehrerer Links können höhere Geschwindigkeiten ohne Hardware-Upgrade erreicht werden.

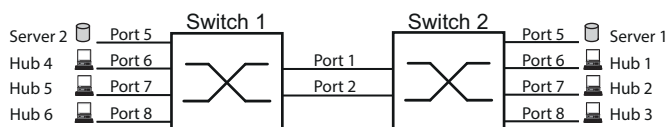


Abb. 47: Link Aggregation Switch-zu-Switch-Netz

Führen Sie folgende Handlungsschritte aus, um Switch 1 und 2 in der grafischen Benutzeroberfläche einzurichten.

- Öffnen Sie den Dialog *Switching* > *L2-Redundanz* > *Link-Aggregation*.
- Klicken Sie die Schaltfläche .
Der Dialog zeigt das Fenster *Erzeugen*.
- Wählen Sie in der Dropdown-Liste *Trunk-Port* die Instanz-Nummer der Link-Aggregation-Gruppe.
- Wählen Sie in der Dropdown-Liste *Port* den Port 1/1.
- Klicken Sie die Schaltfläche .
- Wiederholen Sie die vorherigen Schritte und wählen Sie den Port 1/2.
- Klicken Sie die Schaltfläche .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
link-aggregation add lag/1	Erzeugt eine Link-Aggregation-Gruppe lag/1.
link-aggregation modify lag/1 addport 1/1	Port 1/1 zur Link-Aggregation-Gruppe hinzufügen.
link-aggregation modify lag/1 addport 1/2	Port 1/2 zur Link-Aggregation-Gruppe hinzufügen.

12.7 Link-Backup

Link-Backup bietet einen redundanten Link für Datenverkehr auf Schicht-2-Geräten. Wenn das Gerät einen Fehler auf dem primären Link erkannt hat, leitet das Gerät den Datenverkehr zum Backup-Link um. Sie verwenden Link-Backup üblicherweise in Netzen von Dienst Anbietern oder Unternehmen.

Sie richten die Backup-Links paarweise ein, einen als primären Link und einen als Backup-Link. Wenn Sie beispielsweise Redundanz für Unternehmensnetze zur Verfügung stellen, bietet Ihnen das Gerät die Möglichkeit, mehr als 1 Paar einzurichten. Die maximal Anzahl von Link-Backup-Paaren ist die Gesamtanzahl der physischen Ports / 2. Außerdem sendet das Gerät eine SNMP-Nachricht, wenn der Zustand eines Ports eines Link-Backup-Paares seinen Zustand ändert.

Wenn Sie Link-Backup-Paare einrichten, beachten Sie die folgenden Regeln:

- ▶ Ein Link-Paar besteht aus einer beliebigen Kombination von physischen Ports. Wenn beispielsweise Port 1 ein 100-Mbit-Port und der andere ein 1000-Mbit/s-SFP-Port ist.
- ▶ Ein bestimmter Port ist Teil eines Link-Backup-Paares zu einem beliebigen Zeitpunkt.
- ▶ Vergewissern Sie sich, dass die Ports eines Link-Backup-Paares Mitglieder desselben VLANs mit derselben VLAN-ID sind. Wenn der primäre Port oder der Backup-Port Mitglied eines VLANs sind, weisen Sie dem zweiten Port des Paares dasselbe VLAN zu.

Die Voreinstellung für diese Funktion ist „deaktiviert“ ohne Link-Backup-Paare.

Anmerkung: Vergewissern Sie sich, dass das Spanning-Tree-Protokoll auf den Link-Backup-Ports ausgeschaltet ist.

12.7.1 Beschreibung Fail-Back

Link-Backup bietet Ihnen auch die Möglichkeit, eine Fail-Back-Option einzurichten. Wenn Sie die Fail-Back-Funktion aktivieren und der primäre Link zum normalen Betrieb zurückkehrt, blockiert das Gerät zuerst den Datenverkehr auf dem Backup-Port und überträgt dann den Datenverkehr auf dem primären Port. Dieser Prozess hilft zu vermeiden, dass das Gerät Loops im Netzwerk verursacht.

Wenn der primäre Port zum Link-Up- und aktiven Zustand zurückkehrt, unterstützt das Gerät 2 Betriebsarten:

- ▶ Wenn Sie *Fail back* deaktivieren, bleibt der primäre Port im Blocking-Zustand bis der Backup-Link ausfällt.
- ▶ Wenn Sie *Fail back* aktivieren, und nachdem der *Fail-Back-Verzögerung [s]* Timer abläuft, kehrt der primäre Port in den Forwarding-Zustand zurück und der Backup-Port nimmt den Zustand „Down“ an.

In den oben angeführten Fällen sendet der Port, der seinen Link dazu zwingt, Datenverkehr weiterzuleiten, zuerst ein „Flush-FDB“-Paket zum entfernten Gerät. Das Flush-Paket hilft dem entfernten Gerät dabei, die MAC-Adressen schnell wieder zu lernen.

12.7.2 Beispiel-Konfiguration

Im Beispiel-Netzwerk unten verbinden Sie die Ports 2/3 und 2/4 auf Switch A mit dem Uplink der Switches B und C. Wenn Sie die Ports als Link-Backup-Paar einrichten, leitet 1 Port Datenverkehr weiter, der andere ist im Blocking-Zustand.

Der primäre Port 2/3 auf Switch A ist der aktive Port und leitet Datenverkehr zu Port 1 auf Switch B weiter. Port 2/4 auf Switch A ist der Backup-Port und blockiert den Datenverkehr.

Wenn Switch A Port 2/3 aufgrund eines erkannten Fehlers deaktiviert, beginnt Port 2/4 auf Switch A damit, Datenverkehr zu Port 2 auf Switch C weiterzuleiten.

Wenn Port 2/3 in den aktiven Zustand „no shutdown“ zurückkehrt mit **Fail back** aktiviert und **Fail-Back-Verzögerung [s]** festgelegt auf 30 s. Nachdem der Timer abgelaufen ist, blockiert zuerst Port 2/4 den Datenverkehr, dann fängt Port 2/3 an, den Datenverkehr weiterzuleiten.

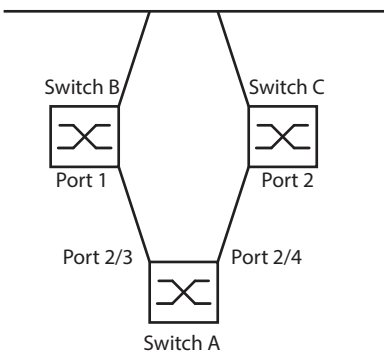


Abb. 48: *Link-Backup* Beispiel-Netzwerk

Die folgenden Tabellen enthalten Beispiele für Parameter für den eingerichteten Switch A.

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Link-Backup*.
- Fügen Sie ein neues Link-Backup-Paar in die Tabelle ein:
 - Klicken Sie die Schaltfläche .
Der Dialog zeigt das Fenster *Erzeugen*.
 - Wählen Sie in der Dropdown-Liste *Primärer Port* den Port 2/3.
Wählen Sie in der Dropdown-Liste *Backup-Port* den Port 2/4.
 - Klicken Sie die Schaltfläche *Ok*.
- Geben Sie im Textfeld *Beschreibung* `Link_Backup_1` als Name für das Backup-Paar ein.
- Um die Fail-Back-Funktion für das Link-Backup-Paar zu aktivieren, markieren Sie das Kontrollkästchen *Fail back*.
- Legen Sie den Fail-Back-Timer für das Link-Backup-Paar fest, geben Sie 30 s ein in *Fail-Back-Verzögerung [s]*.
- Um das Link-Backup-Paar zu aktivieren, markieren Sie das Kontrollkästchen *Aktiv*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
interface 2/3	Wechsel in den Interface-Konfigurationsmodus von Interface 2/3.
link-backup add 2/4	Erzeugt eine Link-Backup-Instanz, bei der Port 2/3 der primäre Port und Port 2/4 der Backup-Port ist.
link-backup modify 2/4 description Link_Backup_1	Legt die Zeichenfolge <code>Link_Backup_1</code> als Name des Backup-Paares fest.
link-backup modify 2/4 failback-status enable	Aktiviert den Fail-Back-Timer.
link-backup modify 2/4 failback-time 30	Legt die Fail-Back-Verzögerungszeit auf 30 s fest.
link-backup modify 2/4 status enable	Aktiviert die Link-Backup-Instanz.

```
exit  
link-backup operation
```

Wechsel in den Konfigurationsmodus.
Aktiviert die *Link-Backup*-Funktion global auf dem Gerät.

13 Funktionsdiagnose

Das Gerät bietet Ihnen folgende Diagnosewerkzeuge:

- ▶ SNMP-Traps senden
- ▶ Gerätestatus überwachen
- ▶ Port-Zustandsanzeige
- ▶ Ereigniszähler auf Portebene
- ▶ Erkennen der Nichtübereinstimmung der Duplex-Modi
- ▶ Auto-Disable
- ▶ SFP-Zustandsanzeige
- ▶ Topologie-Erkennung
- ▶ IP-Adresskonflikte erkennen
- ▶ Erkennen von Schleifen
- ▶ Berichte
- ▶ Datenverkehr eines Ports beobachten (Port Mirroring)
- ▶ Syslog
- ▶ Ereignisprotokoll
- ▶ Ursachen und entsprechende Maßnahmen während des Selbsttests

13.1 SNMP-Traps senden

Das Gerät meldet außergewöhnliche Ereignisse, die während des Normalbetriebs auftreten, sofort an die Netz-Management-Station. Dies geschieht über Nachrichten, sogenannte SNMP-Traps, die das Polling-Verfahren umgehen („Polling“: Abfrage der Datenstationen in regelmäßigen Abständen). SNMP-Traps ermöglichen eine schnelle Reaktion auf außergewöhnliche Ereignisse.

Beispiele für solche Ereignisse sind:

- ▶ Hardware-Reset
- ▶ Änderungen der Konfiguration
- ▶ Segmentierung eines Ports

Das Gerät sendet SNMP-Traps an verschiedene Hosts, um die Übertragungssicherheit für die Nachrichten zu erhöhen. Die nicht quittierte SNMP-Trap-Nachricht besteht aus einem Paket mit Informationen zu einem außergewöhnlichen Ereignis.

Das Gerät sendet SNMP-Traps an jene Hosts, die in der Ziel-Tabelle für SNMP-Traps festgelegt sind. Das Gerät bietet Ihnen die Möglichkeit, die Trap-Ziel-Tabelle mit der Netz-Management-Station über SNMP zu konfigurieren.

13.1.1 Auflistung der SNMP-Traps

Die folgende Tabelle zeigt mögliche vom Gerät gesendete SNMP-Traps:

Bezeichnung des SNMP-Traps	Bedeutung
authenticationFailure	Wird gesendet, falls eine Station versucht, unberechtigt auf einen Agenten zuzugreifen.
coldStart	Wird nach einem Neustart gesendet.
linkDown	Wird gesendet, wenn die Verbindung zu einem Port unterbrochen wird.
linkUp	Wird gesendet, wenn die Verbindung zu einem Port hergestellt ist.
newRoot	Wird gesendet, wenn der sendende Agent zur neuen Wurzel des Spannbaums wird.
topologyChange	Wird gesendet, wenn sich der Port-Zustand von blocking auf forwarding oder von forwarding auf blocking ändert.
alarmRisingThreshold	Wird gesendet, wenn der „RMON input“ seinen oberen Schwellwert überschreitet.
alarmFallingThreshold	Wird gesendet, wenn der „RMON input“ seinen unteren Schwellwert unterschreitet.
hm2AgentPortSecurityViolation	Wird gesendet, wenn eine an diesem Port erkannte MAC-Adresse nicht den aktuellen Einstellungen des Parameters hm2AgentPortSecurityEntry entspricht.
hm2DiagSelftestActionTrap	Wird gesendet, wenn ein Selbsttest gemäß der konfigurierten Einstellungen für die vier Kategorien „Aufgabe“, „Ressource“, „Software“ und „Hardware“ durchgeführt wird.
hm2MrpReconfig	Wird gesendet, wenn sich die Konfiguration des MRP-Rings ändert.
hm2DiagIfaceUtilizationTrap	Wird gesendet, wenn der Schwellwert der Schnittstelle den eingestellten oberen oder unteren Grenzwert über- bzw. unterschreitet.
hm2LogAuditStartNextSector	Wird gesendet, wenn der Audittrail einen Sektor vervollständigt hat und einen neuen beginnt.
hm2PtpSynchronizationChance	Wird gesendet, wenn der Status der PTP-Synchronisation geändert wird.
hm2ConfigurationSavedTrap	Wird gesendet, nachdem das Gerät seine Konfiguration erfolgreich lokal gespeichert hat.
hm2ConfigurationChangedTrap	Wird gesendet, wenn Sie die Konfiguration des Gerätes nach dem lokalen Speichern erstmalig ändern.
hm2PlatformStpInstanceLoopInconsistentStartTrap	Wird gesendet, wenn der Port in dieser STP-Instanz in den Status „loop inconsistent“ geht.
hm2PlatformStpInstanceLoopInconsistentEndTrap	Wird gesendet, wenn der Port in dieser STP-Instanz bei Empfang eines BPDU-Pakets den Status „loop inconsistent“ verlässt.

Tab. 25: Mögliche SNMP-Traps

13.1.2 SNMP-Traps für Konfigurationsaktivitäten



Nachdem Sie eine Konfiguration im Speicher gespeichert haben, sendet das Gerät einen hm2ConfigurationSavedTrap. Dieser SNMP-Trap enthält die Statusvariablen des nichtflüchtigen Speichers (NVM) und des externen nichtflüchtigen Speichers (ENVM), die angeben, ob die aktuelle Konfiguration mit dem NVM und dem ENVM übereinstimmt. Sie können diesen SNMP-Trap auch auslösen, indem Sie eine Konfigurationsdatei in das Gerät kopieren und die aktive gespeicherte Konfiguration ersetzen.

Bei jeder Änderung der Konfiguration sendet das Gerät einen hm2ConfigurationChangedTrap, der angibt, dass die aktuelle und die gespeicherte Konfiguration nicht miteinander übereinstimmen.

13.1.3 SNMP-Trap-Einstellung

Das Gerät bietet Ihnen die Möglichkeit, als Reaktion auf bestimmte Ereignisse einen SNMP-Trap zu senden. Legen Sie mindestens 1 Trap-Ziel fest, das SNMP-Traps empfängt.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)*.
- Klicken Sie die Schaltfläche .
Der Dialog zeigt das Fenster *Erzeugen*.
- Legen Sie im Rahmen *Name* den Namen fest, den das Gerät verwendet, um sich als Quelle des SNMP-Traps auszuweisen.
- Legen Sie im Rahmen *Adresse* die IP-Adresse des Trap-Ziels fest, an welches das Gerät die SNMP-Traps sendet.
- In Spalte *Aktiv* markieren Sie die Einträge, die das Gerät beim Senden von SNMP-Traps berücksichtigen soll.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Das Auslösen eines SNMP-Traps legen Sie zum Beispiel in den folgenden Dialogen fest:

- ▶ Dialog *Grundeinstellungen > Port*
- ▶ Dialog *Netzsicherheit > Port-Sicherheit*
- ▶ Dialog *Switching > L2-Redundanz > Link-Aggregation*
- ▶ Dialog *Diagnose > Statuskonfiguration > Gerätestatus*
- ▶ Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*
- ▶ Dialog *Diagnose > System > IP-Adressen Konflikterkennung*
- ▶ Dialog *Diagnose > System > Selbsttest*
- ▶ Dialog *Diagnose > Ports > Port-Monitor*

13.1.4 ICMP-Messaging

Das Gerät bietet Ihnen die Möglichkeit, das Internet Control Message Protocol (ICMP) für Diagnoseanwendungen zu verwenden, zum Beispiel Ping und Traceroute. Das Gerät verwendet außerdem ICMP für Time-to-Live und das Verwerfen von Nachrichten, in denen das Gerät eine ICMP-Nachricht zurück an das Quellgerät des Paketes weiterleitet.

Verwenden Sie das Ping-Netz-Tool, um den Pfad zu einem bestimmten Host über ein IP-Netz hinweg zu testen. Das Diagnosetool Traceroute zeigt Pfade und Durchgangsverzögerungen von Paketen über ein Netz an.

13.2 Gerätestatus überwachen

Der Gerätestatus gibt einen Überblick über den Gesamtzustand des Gerätes. Viele Prozessvisualisierungssysteme erfassen den Gerätestatus eines Gerätes, um dessen Zustand grafisch darzustellen.

Das Gerät zeigt seinen aktuellen Status als oder im Rahmen *Geräte-Status*. Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät ermöglicht Ihnen:

- ▶ den geänderten Gerätestatus durch Senden eines SNMP-Traps zu signalisieren
- ▶ den Gerätestatus im Dialog *Grundeinstellungen* > *System* der grafischen Benutzeroberfläche zu ermitteln
- ▶ den Gerätestatus im Command Line Interface abzufragen

Die Registerkarte *Global* im Dialog *Diagnose* > *Statuskonfiguration* > *Gerätestatus* bietet Ihnen die Möglichkeit, das Gerät so zu konfigurieren, dass es einen SNMP-Trap an die Netz-Management-Station für die folgenden Ereignisse sendet:

- ▶ Redundanzverlust (im Ring-Manager-Modus)
- ▶ Unterbrechung der Link-Verbindung(en)

Konfigurieren Sie für diese Funktion mindestens einen Port. In der Registerkarte *Port* im Dialog *Diagnose* > *Statuskonfiguration* > *Gerätestatus*, Zeile *Verbindungsfehler melden* legen Sie fest, für welche Ports das Gerät eine Link-Unterbrechung anzeigt.

Entscheiden Sie durch Markieren der entsprechenden Einträge, welche Ereignisse der Gerätestatus erfasst.

13.2.1 Ereignisse, die überwacht werden können

Name	Bedeutung
Ring-Redundanz	Schalten Sie diese Funktion ein, um das Vorhandensein der Ring-Redundanz zu überwachen.
Verbindungsfehler	Aktivieren Sie diese Funktion, um jedes Ereignis in Bezug auf Port-Links zu überwachen, bei dem das Kontrollkästchen <i>Verbindungsfehler melden</i> aktiviert ist.

Tab. 26: *Gerätestatus-Ereignisse*

13.2.2 Gerätestatus konfigurieren

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Global*.
- Markieren Sie für die zu überwachenden Parameter das Kontrollkästchen in Spalte *überwachen*.
- Um einen SNMP-Trap an die Management-Station zu senden, aktivieren Sie die Funktion *Trap senden* im Rahmen *Traps*.
- Legen Sie im Dialog *Diagnose > Statuskonfiguration > Alarmer (Traps)* mindestens 1 Trap-Ziel fest, das SNMP-Traps empfängt.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Grundeinstellungen > System*.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
device-status trap
device-status monitor ring-redundancy
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Senden eines SNMP-Traps, wenn sich der Gerätestatus ändert.
Überwacht die Ring-Redundanz.
In folgenden Situationen wechselt der *Geräte-Status* auf :
– Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve).
– Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen.

Um im Gerät die Überwachung von aktiven Links ohne Verbindung einzuschalten, schalten Sie zuerst die globale Funktion und anschließend die einzelnen Ports ein.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Global*.
- Markieren Sie für den Parameter *Verbindungsfehler* das Kontrollkästchen in Spalte *überwachen*.
- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Port*.
- Markieren Sie für den Parameter *Verbindungsfehler melden* das Kontrollkästchen in der Spalte der zu überwachenden Ports.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
device-status monitor link-failure

interface 1/1

device-status link-alarm
```


Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Überwacht den Link auf den Ports/Interfaces. Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn der Link auf einem überwachten Port/Interface abbricht.
Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
Überwacht den Link auf dem Port/Interface. Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn der Link auf dem Port/Interface abbricht.

Anmerkung: Die obigen CLI-Kommandos schalten Überwachung und Trapping für die unterstützten Komponenten ein. Wenn Sie die Überwachung nur für einzelne Komponenten ein- bzw. ausschalten möchten, finden Sie die entsprechende Syntax im Referenzhandbuch „Command Line Interface“ oder in der Hilfe der CLI-Konsole. (Fügen Sie ein Fragezeichen ? am CLI-Prompt ein.)

13.2.3 Gerätestatus anzeigen

Führen Sie die folgenden Schritte aus:

 Öffnen Sie den Dialog *Grundeinstellungen* > *System*.

 `show device-status all`

Im Privileged-EXEC-Modus: Anzeige des Gerätestatus und der Einstellung zur Ermittlung des Gerätestatus

13.3 Sicherheitsstatus

Der Sicherheitsstatus gibt Überblick über die Gesamtsicherheit des Gerätes. Viele Prozesse dienen als Hilfsmittel für die Systemvisualisierung, indem sie den Sicherheitsstatus des Gerätes erfassen und anschließend seinen Zustand in grafischer Form darstellen. Das Gerät zeigt den Gesamtsicherheitsstatus im Dialog *Grundeinstellungen* > *System*, Rahmen *Sicherheits-Status*.

In der Registerkarte *Global* im Dialog *Diagnose* > *Statuskonfiguration* > *Sicherheitsstatus* zeigt das Gerät im Rahmen *Sicherheits-Status* seinen aktuellen Status als *OK* oder *Warnung*. Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät ermöglicht Ihnen:

- ▶ den geänderten Sicherheitsstatus durch Senden eines SNMP-Traps zu signalisieren
- ▶ den Sicherheitsstatus im Dialog *Grundeinstellungen* > *System* der grafischen Benutzeroberfläche zu ermitteln
- ▶ den Sicherheitsstatus im Command Line Interface abzufragen

13.3.1 Ereignisse, die überwacht werden können

Legen Sie die Ereignisse fest, die das Gerät überwacht.

Markieren Sie für den betreffenden Parameter das Kontrollkästchen in Spalte *Überwachen*.

Name	Bedeutung
Passwort-Voreinstellung unverändert	Um die Sicherheit zu erhöhen, ändern Sie nach der Installation die Passwörter. Das Gerät überwacht, ob die voreingestellten Passwörter unverändert bleiben.
Min. Passwort-Länge < 8	Erzeugen Sie Passwörter mit einer Länge von mehr als 8 Zeichen, um ein hohes Maß an Sicherheit zu erhalten. Bei aktivierter Funktion überwacht das Gerät die Einstellung <i>Min. Passwort-Länge</i> .
Passwort-Richtlinien deaktiviert	Das Gerät überwacht, ob die Einstellungen im Dialog <i>Gerätesicherheit</i> > <i>Benutzerverwaltung</i> die Anforderungen der Passworrichtlinie erfüllen.
Prüfen der Passwort-Richtlinien im Benutzerkonto deaktiviert	Das Gerät überwacht die Einstellungen des Kontrollkästchens <i>Richtlinien überprüfen</i> . Wenn <i>Richtlinien überprüfen</i> inaktiv ist, sendet das Gerät einen SNMP-Trap.
Telnet-Server aktiv	Das Gerät überwacht, wann Sie die Telnet-Funktion einschalten.
HTTP-Server aktiv	Das Gerät überwacht, wann Sie die Funktion für die HTTP-Verbindung einschalten.
SNMP unverschlüsselt	Das Gerät überwacht, wann Sie die Funktion für die SNMPv1- oder SNMPv2-Verbindung einschalten.
Zugriff auf System-Monitor mit V.24 möglich	Das Gerät überwacht den Status des System-Monitors.
Verbindungsabbruch auf eingeschalteten Ports	Das Gerät überwacht den Link-Status der aktiven Ports.
Zugriff mit HiDiscovery möglich	Das Gerät überwacht, wann Sie die Lese-/Schreibfunktion für HiDiscovery einschalten.
IEC61850-MMS aktiv	Das Gerät überwacht, wann Sie das Protokoll IEC 61850-MMS einschalten.

Tab. 27: *Sicherheitsstatus-Ereignisse*

Name	Bedeutung
Modbus TCP aktiv	Das Gerät überwacht, wann Sie das Modbus TCP/IP-Protokoll einschalten.
Self-signed HTTPS-Zertifikat vorhanden	Das Gerät überwacht, ob der HTTPS-Server ein selbst erzeugtes digitales Zertifikat verwendet.

Tab. 27: *Sicherheitsstatus-Ereignisse (Forts.)*

13.3.2 Konfigurieren des Sicherheitsstatus

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*.
- Markieren Sie für die zu überwachenden Parameter das Kontrollkästchen in Spalte *Überwachen*.
- Um einen SNMP-Trap an die Management-Station zu senden, aktivieren Sie die Funktion *Trap senden* im Rahmen *Traps*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
- Legen Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* mindestens 1 Trap-Ziel fest, das SNMP-Traps empfängt.

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
security-status monitor pwd-change	Überwacht das Passwort für die lokal eingerichteten Benutzerkonten <i>user</i> und <i>admin</i> . Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn Sie für die Benutzerkonten <i>user</i> oder <i>admin</i> das voreingestellte Passwort unverändert verwenden.
security-status monitor pwd-min-length	Überwacht den in Richtlinie <i>Min. Passwort-Länge</i> festgelegten Wert. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn für die Richtlinie <i>Min. Passwort-Länge</i> ein Wert kleiner als 8 festgelegt ist.
security-status monitor pwd-policy-config	Überwacht die Passwort-Richtlinien-Einstellungen. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn für mindestens eine der folgenden Richtlinien der Wert 0 festgelegt ist. <ul style="list-style-type: none"> – <i>Großbuchstaben (min.)</i> – <i>Kleinbuchstaben (min.)</i> – <i>Ziffern (min.)</i> – <i>Sonderzeichen (min.)</i>
security-status monitor pwd-policy-inactive	Überwacht die Passwort-Richtlinien-Einstellungen. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn für mindestens eine der folgenden Richtlinien der Wert 0 festgelegt ist.
security-status monitor telnet-enabled	Überwacht den Telnet-Server. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn Sie den Telnet-Server einschalten.
security-status monitor http-enabled	Überwacht den HTTP-Server. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn Sie den HTTP-Server einschalten.

security-status monitor snmp-unsecure	Überwacht den SNMP-Server. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn mindestens eine der folgenden Bedingungen zutrifft: <ul style="list-style-type: none">– Die Funktion <i>SNMPv1</i> ist eingeschaltet.– Die Funktion <i>SNMPv2</i> ist eingeschaltet.– Die Verschlüsselung für SNMPv3 ist ausgeschaltet. Die Verschlüsselung schalten Sie ein im Dialog <i>Gerätesicherheit > Benutzerverwaltung</i> , Feld <i>SNMP-Verschlüsselung</i> .
security-status monitor sysmon-enabled	Überwachen der Aktivierung von System Monitor 1 auf dem Gerät.
security-status monitor iec61850-mms-enabled	Überwacht die <i>IEC61850-MMS</i> -Funktion. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn Sie die <i>IEC61850-MMS</i> -Funktion einschalten.
security-status trap	Senden eines SNMP-Traps, wenn sich der Gerätestatus ändert.

Um im Gerät die Überwachung von aktiven Links ohne Verbindung einzuschalten, schalten Sie zuerst die globale Funktion und anschließend die einzelnen Ports ein.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*.
- Markieren Sie für den Parameter *Verbindungsabbruch auf eingeschalteten Ports* das Kontrollkästchen in Spalte *Überwachen*.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Port*.
- Markieren Sie für den Parameter *Verbindungsabbruch auf eingeschalteten Ports* das Kontrollkästchen in der Spalte der zu überwachenden Ports.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
security-status monitor no-link-enabled	Überwacht den Link auf aktiven Ports. Der Wert im Rahmen <i>Sicherheits-Status</i> wechselt auf <i>error</i> , wenn der Link auf einem aktiven Port abbricht.
interface 1/1	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
security-status monitor no-link	Überwacht den Link auf Interface/Port 1.

13.3.3 Anzeigen des Sicherheitsstatus

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > System*.

show security-status all	Zeigt im EXEC-Privilege-Modus Sicherheitsstatus und die Einstellung zur Ermittlung des Gerätestatus.
--------------------------	--

13.4 Portereignis-Zähler

Die Port-Statistiktablett versetzt den erfahrenen Netzbetreuer in die Lage, erkannte eventuelle Schwachpunkte im Netz zu identifizieren.

Diese Tabelle zeigt Ihnen die Inhalte verschiedener Ereigniszähler an. Die Paketzähler summieren die Ereignisse aus Sende- und Empfangsrichtung. Im Dialog *Grundeinstellungen* > *Neustart* können Sie die Ereigniszähler zurücksetzen.

Zähler	Angabe bekannter möglicher Schwächen
Empfangene Fragmente	<ul style="list-style-type: none"> – Nicht funktionierender Controller des verbundenen Gerätes – Elektromagnetische Einkoppelung im Übertragungsmedium
CRC-Fehler	<ul style="list-style-type: none"> – Nicht funktionierender Controller des verbundenen Gerätes – Elektromagnetische Einkoppelung im Übertragungsmedium – Nicht betriebsbereite Komponente im Netz
Kollisionen	<ul style="list-style-type: none"> – Nicht funktionierender Controller des verbundenen Gerätes – Netzausdehnung zu groß/Zeilen zu lang – Kollision oder Fehler beim Datenpaket ermittelt

Tab. 28: Beispiele für die Angabe bekannter Schwächen

Führen Sie die folgenden Schritte aus:

- Um die Ereigniszähler anzuzeigen, öffnen Sie den Dialog *Grundeinstellungen* > *Port*, Registerkarte *Statistiken*.
- Um die Zähler zurückzusetzen, klicken Sie im Dialog *Grundeinstellungen* > *Neustart* die Schaltfläche *Port-Statistiken leeren*.

13.4.1 Erkennen der Nichtübereinstimmung der Duplex-Modi

Weisen 2 direkt miteinander verbundene Ports nicht übereinstimmende Modi auf, treten Probleme auf. Die Nachverfolgung dieser Probleme ist schwierig. Das automatische Erkennen und Melden dieser Situation hat den Vorteil, dass nicht übereinstimmende Duplex-Modi erkannt werden, bevor Probleme auftreten.

Diese Situation wird durch eine fehlerhafte Konfiguration verursacht, zum Beispiel wenn Sie die automatische Konfiguration am Remote-Port deaktivieren.

Ein typischer Effekt dieser Nichtübereinstimmung ist, dass die Verbindung bei niedriger Datenrate zu funktionieren scheint, das lokale Gerät bei höherem bidirektionalem Verkehrsaufkommen jedoch viele CRC-Fehler zählt und die Verbindung deutlich unter dem Nenndurchsatz bleibt.

Das Gerät bietet Ihnen die Möglichkeit, diese Situation zu erkennen und sie an die Netz-Management-Station zu melden. Das Gerät bewertet dazu die Fehlerzähler des Ports in Abhängigkeit von den Port-Einstellungen.

■ Möglichen Ursachen für Port-Fehlerereignisse

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

- ▶ Kollisionen
Im Halbduplexmodus bedeuten Kollisionen Normalbetrieb.
- ▶ Duplex-Problem
Nicht übereinstimmende Duplex-Modi.
- ▶ EMI
Elektromagnetische Interferenz.
- ▶ Netzausdehnung
Die Netzausdehnung ist zu groß bzw. sind zu viele Kaskadenhubs vorhanden.
- ▶ Kollisionen, Late Collisions
Im Vollduplex-Modus keine Erhöhung der Port-Zähler für Kollisionen oder Late Collisions.
- ▶ CRC-Fehler
Das Gerät bewertet diese Fehler als nicht übereinstimmende Duplex-Modi im manuellen Vollduplex-Modus.

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

Tab. 29: Bewertung des nicht übereinstimmenden Duplex-Modus

13.5 Auto-Disable

Unterschiedliche konfigurationsbedingte Ursachen können bewirken, dass das Gerät einen Port ausschaltet. Jede Ursache führt zur Software-seitigen Abschaltung des Ports. Um die Software-seitige Abschaltung des Ports aufzuheben, können Sie den verursachenden Zustand manuell beseitigen oder einen Timer festlegen, der den Port automatisch wieder einschaltet.

Wenn die Konfiguration einen Port als eingeschaltet zeigt, das Gerät jedoch einen Fehler oder eine Zustandsänderung erkennt, schaltet die Software den betreffenden Port ab. Anders gesagt: Die Geräte-Software schaltet den Port aufgrund eines erkannten Fehlers oder einer erkannten Zustandsänderung aus.

Bei der Auto-Deaktivierung eines Ports schaltet das Gerät den betreffenden Port ab; der Port blockiert den Datenverkehr. Die Port-LED blinkt pro Phase dreimal grün und identifiziert den Grund für das Abschalten. Darüber hinaus erzeugt das Gerät einen Protokolleintrag, der den Grund für die Selbstabschaltung aufführt. Wenn Sie den Port nach einem Timeout mit der *Auto-Disable*-Funktion wieder einschalten, erzeugt das Gerät einen Protokolleintrag.

Die *Auto-Disable*-Funktion stellt eine Wiederherstellungsfunktion bereit, die einen per Selbstabschaltung deaktivierten Port nach einem benutzerdefinierten Zeitraum automatisch wieder aktiviert. Wenn diese Funktion einen Port aktiviert, sendet das Gerät einen SNMP-Trap mit der Port-Nummer, jedoch ohne einen Wert für den Parameter *Grund*.

Die *Auto-Disable*-Funktion hat die folgenden Aufgaben:

- ▶ Sie unterstützt den Netzwerk-Administrator bei der Port-Analyse.
- ▶ Dies verringert die Wahrscheinlichkeit, dass der betreffende Port ein instabiles Netz verursacht.

Die *Auto-Disable*-Funktion steht für folgende Funktionen zur Verfügung:

- ▶ *Link-Änderungen* (*Port-Monitor*-Funktion)
- ▶ *CRC/Fragmente* (*Port-Monitor*-Funktion)
- ▶ Duplex Mismatch-Erkennung (*Port-Monitor*-Funktion)
- ▶ *Spanning Tree*
- ▶ *Port-Sicherheit*
- ▶ *Überlast-Erkennung* (*Port-Monitor*-Funktion)
- ▶ *Link-Speed-/Duplex-Mode-Erkennung* (*Port-Monitor*-Funktion)

Im folgenden Beispiel konfigurieren Sie das Gerät so, dass es einen Port deaktiviert und anschließend automatisch reaktiviert, wenn es eine Überschreitung der in der Registerkarte *Diagnose > Ports > Port-Monitor > CRC/Fragmente* festgelegten Grenzwerte feststellt.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *CRC/Fragmente*.
- Vergewissern Sie sich, dass die in der Tabelle angegebenen Grenzwerte mit Ihren Einstellungen für Port 1/1 übereinstimmen.
- Öffnen Sie den Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Global*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um dem Gerät zu ermöglichen, den Port aufgrund erkannter Fehler auszuschalten, markieren Sie das Kontrollkästchen in Spalte *CRC/Fragmente an* für Port 1/1.

- In Spalte **Aktion** können Sie festlegen, wie das Gerät auf erkannte Fehler reagiert. In diesem Beispiel schaltet das Gerät Port 1/1 aufgrund von Grenzwertüberschreitungen aus und schaltet den Port anschließend wieder ein.

- ▶ Um dem Gerät zu ermöglichen, den Port auszuschalten und anschließend automatisch wieder einzuschalten, wählen Sie den Wert `auto-disable` und konfigurieren die Funktion **Auto-Disable**. Der Wert `auto-disable` funktioniert ausschließlich mit der Funktion `auto-disable`.

Das Gerät ist außerdem in der Lage, einen Port auszuschalten, ohne ihn automatisch wieder einzuschalten.

- ▶ Um dem Gerät zu ermöglichen, den Port ausschließlich auszuschalten, wählen Sie den Wert `disable port`. Um einen ausgeschalteten Port manuell wieder einzuschalten, markieren Sie den Port.

Klicken Sie die Schaltfläche  und dann den Eintrag **Zurücksetzen**.

- ▶ Wenn Sie die Funktion **Auto-Disable** konfigurieren, schaltet der Wert `disable port` den Port ebenfalls automatisch wieder ein.

- Öffnen Sie den Dialog **Diagnose > Ports > Port-Monitor**, Registerkarte **Auto-Disable**.
- Um dem Gerät zu ermöglichen, den Port nach einem Ausschalten wegen erkannter Grenzwertüberschreitungen automatisch wieder einzuschalten, markieren Sie das Kontrollkästchen in Spalte **CRC-/Fragment-Fehler**.
- Öffnen Sie den Dialog **Diagnose > Ports > Port-Monitor**, Registerkarte **Port**.
- Legen Sie in Spalte **Reset-Timer [s]** eine Verzögerungszeit von 120 s für die zu aktivierenden Ports fest.

Anmerkung: Der Eintrag **Zurücksetzen** bietet Ihnen die Möglichkeit, den Port zu aktivieren, bevor die in Spalte **Reset-Timer [s]** festgelegte Zeit abgelaufen ist.

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>configure</code>	Wechsel in den Konfigurationsmodus.
<code>interface 1/1</code>	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
<code>port-monitor condition crc-fragments count 2000</code>	CRC-Fragment-Zähler auf 2000 Teile pro Million festlegen.
<code>port-monitor condition crc-fragments interval 15</code>	Setzt das Messintervall für die CRC-Fragment-Erkennung auf 15 Sekunden.
<code>auto-disable timer 120</code>	Legt eine Wartezeit von 120 Sekunden fest, nach der die Auto-Disable -Funktion den Port wieder einschaltet.
<code>exit</code>	Wechsel in den Konfigurationsmodus.
<code>auto-disable reason crc-error</code>	Aktivieren Sie die die Selbstabschaltfunktion für CRC.
<code>port-monitor condition crc-fragments mode</code>	Um eine Aktion auszulösen, aktivieren Sie die CRC-Fragment-Bedingung.
<code>port-monitor operation</code>	Aktivieren Sie die Port-Monitor -Funktion.

Wenn das Gerät einen Port wegen Grenzwertüberschreitungen ausschaltet, haben Sie die Möglichkeit, den ausgeschalteten Port mit den folgenden CLI-Kommandos manuell zurückzusetzen.

Führen Sie die folgenden Schritte aus:


<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>configure</code>	Wechsel in den Konfigurationsmodus.
<code>interface 1/1</code>	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
<code>auto-disable reset</code>	Bietet Ihnen die Möglichkeit, den Port einzuschalten, bevor der Timer zu zählen beginnt.

13.6 SFP-Zustandsanzeige

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

- ▶ Modultyp,
- ▶ Seriennummer des Medien-Moduls
- ▶ Temperatur in ° C,
- ▶ Sendeleistung in mW,
- ▶ Empfangsleistung in mW.

Führen Sie die folgenden Schritte aus:

-  Öffnen Sie den Dialog *Diagnose > Ports > SFP*.

13.7 Topologie-Erkennung

IEEE 802.1AB beschreibt das Link Layer Discovery Protocol (LLDP). Das LLDP ermöglicht dem Anwender eine automatische Topologie-Erkennung seines LANs.

Geräte mit aktivem LLDP:

- ▶ senden ihre Verbindungs- und Verwaltungsdaten an die angrenzenden Geräte des gemeinsamen LANs. Die Bewertung der Geräte erfolgt, wenn die LLDP-Funktion beim empfangenden Gerät aktiviert ist.
- ▶ empfangen eigene Verbindungs- und Management-Informationen von angrenzenden Geräten des gemeinsamen LANs, sofern diese auch das LLDP aktiviert haben.
- ▶ bauen eine Datenbank mit Verwaltungsdaten und Objektdefinitionen auf, um Informationen zu benachbarten Geräten mit aktivem LLDP zu speichern.

Als zentrales Element enthält die Verbindungsinformation die genaue, eindeutige Kennzeichnung des Verbindungsendpunktes: MAC (Dienstzugangspunkt). Diese setzt sich zusammen aus einer netzweit eindeutigen Geräteerkennung und einer für dieses Gerät eindeutigen Port-Kennung.

- ▶ Chassis-Kennung (dessen MAC-Adresse)
- ▶ Port-Kennung (dessen Port-MAC-Adresse)
- ▶ Beschreibung des Ports
- ▶ Systemname
- ▶ Systembeschreibung
- ▶ Unterstützte Systemfunktionen
- ▶ Momentan aktive Systemfunktionen
- ▶ Interface-ID der Management-Adresse
- ▶ VLAN-ID des Ports
- ▶ Status der Autonegotiation auf dem Port
- ▶ Einstellung für Medium-/Halb- und Voll-Duplex sowie für die Port-Geschwindigkeit
- ▶ Information über die im Gerät installierten VLANs (VLAN-Kennung und VLAN-Namen; unabhängig davon, ob der Port VLAN-Mitglied ist).

Diese Informationen kann eine Netz-Management-Station von Geräten mit aktivem LLDP abrufen. Mit diesen Informationen ist die Netz-Management-Station in der Lage, die Topologie des Netzes darzustellen.

Nicht-LLDP-Geräte blockieren in der Regel die spezielle Multicast-LLDP-IEEE-MAC-Adresse, die zum Informationsaustausch verwendet wird. Nicht-LLDP-Geräte werfen aus diesem Grund LLDP-Pakete. Wird ein nicht-LLDP-fähiges Gerät zwischen 2 LLDP-fähigen Geräten positioniert, lässt das nicht-LLDP-fähige Gerät den Informationsaustausch zwischen 2 LLDP-fähigen Geräten nicht zu.

Die Management Information Base (MIB) für ein LLDP-fähiges Gerät enthält die LLDP-Informationen in der LLDP-MIB und in der privaten HM2-LLDP-EXT-HM-MIB und HM2-LLDP-MIB.

13.7.1 Anzeige der Topologie-Erkennung

So zeigen Sie die Topologie des Netzes an:

- Öffnen Sie den Dialog *Diagnose > LLDP > LLDP Topologie-Erkennung*, Registerkarte *LLDP*.

Wenn Sie an einen Port mehrere Geräte anschließen (zum Beispiel über einen Hub), zeigt die Tabelle für jedes angeschlossenes Gerät je eine Zeile an.

Das Aktivieren der Einstellung „FDB Einträge anzeigen“ am unteren Ende der Tabelle bietet Ihnen die Möglichkeit, Geräte ohne aktive LLDP-Unterstützung in der Tabelle anzuzeigen. Das Gerät nimmt in diesem Fall auch Informationen aus seiner FDB (Forwarding Database) auf.

Wenn Sie den Port mit Geräten mit einer aktiven Topologie-Erkennungsfunktion verbinden, tauschen die Geräte LLDP Data Units (LLDPDU) aus, und die Topologie-Tabelle zeigt diese benachbarten Geräte an.

Sind an einen Port ausschließlich Geräte ohne aktive Topologie-Erkennung angeschlossen, enthält die Tabelle eine Zeile für diesen Port, um die angeschlossenen Geräte darzustellen. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.

Die FDB-Adresstabelle enthält MAC-Adressen von Geräten, die die Topologie-Tabelle aus Gründen der Übersicht ausblendet.

13.8 Erkennen von Schleifen

Schleifen im Netz (sog. Loops) können Verbindungsunterbrechungen oder Datenverlust verursachen. Dies gilt auch dann, wenn sie nur vorübergehend sind. Die automatische Detektion und Meldung dieser Situation bietet Ihnen die Möglichkeit, diese rascher zu entdecken und leichter zu diagnostizieren.

Eine Fehlkonfiguration kann einen Loop verursachen, zum Beispiel wenn Sie Spanning Tree deaktivieren.

Das Gerät bietet Ihnen die Möglichkeit, die Effekte zu erkennen, die Loops typischerweise bewirken, und diese Situation automatisch an die Netz-Management-Station zu melden. Dabei haben Sie die Möglichkeit, einzustellen, ab welchem Ausmaß der Loop-Effekte das Gerät eine Meldung verschickt.

BPDU-Rahmen, die vom ausgewählten Port aus gesendet wurden und innerhalb kurzer Zeit entweder an einem anderen Port desselben Gerätes oder an demselben Port empfangen werden, sind ein typischer Effekt einer Schleife.

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*.
- Prüfen Sie den Wert in den Feldern *Port-Status* und *Port-Rolle*. Wenn das Feld *Port-Status* den Wert `discarding` und das Feld *Port-Rolle* den Wert `backup` zeigt, befindet sich der Port in einem Schleifenstatus.
oder
- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *Guards*.
- Prüfen Sie den Wert in Spalte *Loop-Zustand*. Wenn das Feld den Wert `true` zeigt, befindet sich der Port in einem Schleifenstatus.

13.9 Berichte

Im Folgenden werden die für Diagnosezwecke verfügbaren Berichte und Schaltflächen aufgeführt:

- ▶ System-Log-Datei
Die Logdatei ist eine HTML-Datei, in die das Gerät wichtige geräteinternen Ereignisse schreibt.
- ▶ Audit Trail
Protokolliert erfolgreiche CLI-Kommandos und Kommentare von Benutzern. Die Datei schließt auch das SNMP-Logging ein.
- ▶ Download Support Informationen
Diese Schaltfläche bietet Ihnen die Möglichkeit, Systeminformationen als Dateien in einem ZIP-Archiv herunterzuladen.

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

13.9.1 Globale Einstellungen

Über diesen Dialog aktivieren oder deaktivieren Sie die jeweiligen Ziele, an die das Gerät Berichte sendet, zum Beispiel Konsole, Syslog-Server oder CLI-Verbindung. Ferner legen Sie fest, ab welchem Schweregrad das Gerät Ereignisse in die Berichte schreibt.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Bericht > Bericht Global*.
- Um einen Bericht an die Konsole zu senden, legen Sie im Rahmen *Console-Logging* die gewünschte Stufe im Feld *Schweregrad* fest.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Console-Logging* das Optionsfeld .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

Das Gerät puffert die protokollierten Ereignisse in 2 separaten Speicherbereichen, sodass das Gerät die Protokolleinträge für dringende Ereignisse beibehält. Legen Sie den minimalen Schweregrad für Ereignisse fest, die das Gerät im gepufferten Speicherbereich mit einer höheren Priorität protokolliert.

Führen Sie die folgenden Schritte aus:

- Um Ereignisse an den Puffer zu senden, legen Sie im Rahmen *Buffered-Logging* die gewünschte Stufe im Feld *Schweregrad* fest.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

Wenn Sie die Protokollierung von SNMP-Anfragen aktivieren, protokolliert das Gerät die Anfragen im Syslog als Ereignisse. Die Funktion *Protokolliere SNMP-Get-Requests* protokolliert Benutzeranfragen nach Geräte-Konfigurationsinformationen. Die Funktion *Protokolliere SNMP-Set-Requests* protokolliert Geräte-Konfigurationsereignisse. Legen Sie die Untergrenze für Ereignisse fest, die das Gerät im Syslog einträgt.

Führen Sie die folgenden Schritte aus:

- Um SNMP-Lese-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die *Protokolliere SNMP-Get-Requests*-Funktion ein.
Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld .
- Um SNMP-Schreib-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die *Protokolliere SNMP-Set-Requests*-Funktion ein.
Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld .
- Wählen Sie den gewünschten Schweregrad für die Get- und Set-Anfragen.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Sofern aktiv, protokolliert das Gerät Änderungen an der Konfiguration, die über CLI-Kommandos vorgenommen wurden, im Audit Trail. Diese Funktion liegt der Norm IEEE 1686 für intelligente elektronische Unterstationsgeräte zugrunde.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Bericht > Bericht Global*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *CLI-Logging* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Das Gerät bietet Ihnen die Möglichkeit, die folgenden Systeminformationen in einer ZIP-Datei auf Ihrem PC speichern:

- ▶ `audittrail.html`
- ▶ `CLICommands.txt`
- ▶ `defaultconfig.xml`
- ▶ `script`
- ▶ `runningconfig.xml`
- ▶ `supportinfo.html`
- ▶ `systeminfo.html`
- ▶ `systemlog.html`

Den Dateinamen des ZIP-Archivs erzeugt das Gerät automatisch nach dem Muster `<IP-Adresse>_<Gerätename>.zip`.

Führen Sie die folgenden Schritte aus:



- Klicken Sie die Schaltfläche und dann den Eintrag *Support-Informationen herunterladen*.
- Wählen Sie das Verzeichnis aus, in welchem Sie die Support-Information speichern.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

13.9.2 Syslog

Das Gerät bietet Ihnen die Möglichkeit, Nachrichten zu wichtigen geräteinternen Ereignissen an einen oder mehrere Syslog-Server (bis zu 8) zu senden. Zusätzlich schließen Sie SNMP-Anfragen des Gerätes als Ereignisse in den Syslog ein.


Anmerkung: Zum Anzeigen der protokollierten Ereignisse öffnen Sie den Dialog *Diagnose* > Bericht > *Audit Trail* oder den Dialog *Diagnose* > Bericht > *System Log*.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose* > *Syslog*.
- Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- Fügen Sie in Spalte *IP-Adresse* die IP-Adresse des Syslog-Servers ein.
- Legen Sie in Spalte *Ziel-UDP-Port* den UDP-Port fest, auf dem der Syslog-Server die Log-Einträge erwartet.
- Legen Sie in Spalte *Min. Schweregrad* den Mindest-Schweregrad fest, den ein Ereignis aufweisen muss, damit das Gerät einen Protokolleintrag an diesen Syslog-Server sendet.
- Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Konfigurieren Sie im Rahmen *SNMP-Logging* die folgenden Einstellungen für SNMP-Lese- und Schreibanfragen:

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose* > Bericht > Bericht Global.
- Um SNMP-Lese-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die *Protokollierte SNMP-Get-Requests*-Funktion ein.
Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld .
- Um SNMP-Schreib-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die *Protokollierte SNMP-Set-Requests*-Funktion ein.
Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld .
- Wählen Sie den gewünschten Schweregrad für die Get- und Set-Anfragen.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

```
enable
configure
logging host add 1 addr 10.0.1.159
severity 3

logging syslog operation
exit
show logging host
```

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Fügt der Liste der Syslog-Server einen neuen Empfänger hinzu. Der Wert 3 legt den Schweregrad des Ereignisses fest, welches das Gerät protokolliert. Der Wert 3 bedeutet Fehler.
Einschalten der *Syslog*-Funktion.
Wechsel in den Privileged-EXEC-Modus.
Anzeigen der Syslog-Host-Einstellungen.

No.	Server IP	Port	Max. Severity	Type	Status
1	10.0.1.159	514	error	systemlog	active

```
configure
logging snmp-requests get operation
logging snmp-requests get severity 5
```

Wechsel in den Konfigurationsmodus.
Protokolliert SNMP-Get-Anfragen.
Der Wert 5 legt den Schweregrad des Ereignisses fest, welches das Gerät bei SNMP-GET-Anfragen protokolliert. Der Wert 5 bedeutet Hinweis.


```
logging snmp-requests set operation Protokolliert SNMP-SET-Anfragen.  
logging snmp-requests set severity 5 Der Wert 5 legt den Schweregrad des Ereignisses fest, welches  
das Gerät bei SNMP-SET-Anfragen protokolliert. Der Wert 5  
bedeutet Hinweis.  
exit Wechsel in den Privileged-EXEC-Modus.  
show logging snmp Zeigt die SNMP-Logging-Einstellungen an.
```



```
Log SNMP GET requests : enabled  
Log SNMP GET severity : notice  
Log SNMP SET requests : enabled  
Log SNMP SET severity : notice
```

13.9.3 System-Log

Das Gerät bietet Ihnen die Möglichkeit, ein Protokoll zu den Systemereignissen aufzurufen. In der Tabelle im Dialog *Diagnose > Bericht > System Log* werden die protokollierten Ereignisse aufgeführt.

Führen Sie die folgenden Schritte aus:

- Wählen Sie für die Aktualisierung des Protokollinhaltes „Reload“.
- Um im Protokollinhalt nach einem Schlüsselwort zu suchen, wählen Sie „Search“.
- Wählen Sie „Speichern“, um den Inhalt des Protokolls als HTML-Datei zu archivieren.

Anmerkung: Sie haben die Möglichkeit, auch protokollierte Ereignisse an einen oder mehrere Syslog-Server zu senden.

13.9.4 Audit Trail

Der Dialog *Diagnose > Bericht > Audit Trail* enthält Systeminformationen sowie Änderungen, die über CLI und SNMP an dem Gerät vorgenommen wurden. Bei Änderungen der Gerätekonfiguration zeigt der Dialog an, wer zu welchem Zeitpunkt welche Änderungen vorgenommen hat. Um Änderungen an der Gerätekonfiguration zu protokollieren, verwenden Sie im Dialog *Diagnose > Bericht > Audit Trail* die Funktionen *Protokolliere SNMP-Get-Requests* und *Protokolliere SNMP-Set-Requests*.

Der Dialog *Diagnose > Syslog* gibt Ihnen die Möglichkeit, bis zu 8 Syslog-Server einzustellen, an die das Gerät Audit Trails sendet.

Die folgende Liste enthält Protokollereignisse:

- ▶ Änderungen an Konfigurationsparametern
- ▶ CLI-Kommandos (mit Ausnahme der `show`-Kommandos)
- ▶ CLI-Kommando `logging audit-trail <string>`, das den Kommentar protokolliert
- ▶ Automatische Änderungen der Systemzeit
- ▶ Watchdog-Ereignisse

- ▶ Sperren eines Benutzers nach mehreren fehlgeschlagenen Login-Versuchen
- ▶ Benutzeranmeldung über CLI (lokal oder remote)
- ▶ Manuelle, benutzerinitiierte Abmeldung
- ▶ Zeitlich festgelegte Abmeldung nach einem durch den Benutzer definierten Zeitraum, über den CLI inaktiv ist
- ▶ Dateiübertragung, einschließlich Firmware-Update
- ▶ Konfigurationsänderungen über HiDiscovery
- ▶ Automatische Konfiguration oder Firmware-Updates über den externen Speicher
- ▶ Gesperrter Management-Zugriff aufgrund von ungültigen Anmeldedaten
- ▶ Neustart
- ▶ Öffnen und Schließen von SNMP über HTTPS-Tunnel
- ▶ Ermittelte Stromausfälle

13.10 Netzanalyse mit TCPDump

TCPDump ist ein UNIX-Hilfsprogramm für das Packet-Sniffing, das von Netzadministratoren verwendet wird, um Datenverkehr im Netz aufzuspüren und zu analysieren. Das Aufspüren von Datenverkehr dient unter anderem der Verifizierung der Konnektivität zwischen Hosts und der Analyse des Datenverkehrs, der das Netz durchquert.

TCPDump auf dem Gerät bietet die Möglichkeit, durch die Management-CPU empfangene oder übertragene Pakete zu dekodieren oder zu erfassen. Auf diese Funktion kann über das CLI-Kommando `debug` zugegriffen werden. Weitere Informationen zur TCPDump-Funktion finden Sie im Referenzhandbuch „Command Line Interface“.

13.11 Datenverkehr beobachten

Das Gerät bietet Ihnen die Möglichkeit, Datenpakete, die das Gerät durchlaufen, an einen Zielport weiterzuleiten. Dort können Sie die Datenpakete überwachen und auswerten.

Das Gerät bietet Ihnen folgende Möglichkeiten:

- [Port-Mirroring](#)

13.11.1 Port-Mirroring

Die *Port-Mirroring*-Funktion bietet Ihnen die Möglichkeit, die Datenpakete von physischen Quellports zu einem physischen Zielport zu kopieren.

Mit einem am Zielport angeschlossenen Analysator, zum Beispiel RMON-Probe, überwachen Sie die auf den Quellports gesendeten und empfangenen Datenpakete. Die Funktion hat keine Auswirkungen auf den über die Quellports laufenden Datenstrom.

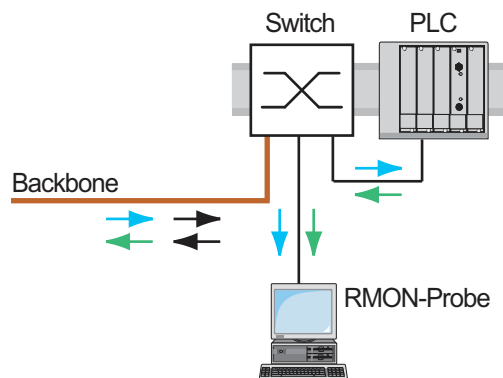


Abb. 49: Beispiel

Das Gerät sendet auf dem Zielport ausschließlich die von den Quellports kopierten Datenpakete.

Um über den Zielport auf die Management-Funktionen zuzugreifen, markieren Sie vor Einschalten der *Port-Mirroring*-Funktion das Kontrollkästchen *Management erlauben*. Das Gerät lässt den Zugriff auf die Management-Funktionen über den Zielport zu, ohne die aktive *Port-Mirroring*-Session zu unterbrechen.

Anmerkung: Das Gerät dupliziert auf dem Zielport Multicasts, Broadcasts und unbekannte Unicasts. Die VLAN-Einstellungen auf dem Zielport bleiben unverändert. Voraussetzung für den Management-Zugriff über den Zielport ist, dass der Zielport Mitglied im Management-VLAN ist.


Für Ports, auf denen folgende Redundanz-Protokolle aktiv sind, gelten Einschränkungen:

- ▶ **Fast MRP (hardwareabhängig)**
Kein Port-Mirroring von vermittelten MRP-Test-Paketen.
- ▶ **HSR, PRP (hardwareabhängig)**
Um den Datenstrom auf HSR-/PRP-Ports zu beobachten, legen Sie den Quellport 1/1 fest. Auf Quellport 1/1 erfasst die *Port-Mirroring*-Funktion:
 - Datenpakete, die von außen durch das Gerät ins HSR-/PRP-Netz gelangen
 - Datenpakete nach Duplikaterkennung, die das HSR-/PRP-Netz durch das Gerät verlassen
 - Keine Link Local-Pakete, mit denen Protokolle wie LLDP arbeiten

■ **Port-Mirroring-Funktion einschalten**

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- Legen Sie die Quellports fest.
Markieren Sie das Kontrollkästchen in Spalte *Eingeschaltet* für die gewünschten Ports.
- Legen Sie den Zielport fest.
Wählen Sie im Rahmen *Ziel-Port*, Dropdown-Liste *Primärer Port* den gewünschten Port. Die Dropdown-Liste zeigt ausschließlich die verfügbaren Ports. Bereits als Quellport festgelegte Ports sind nicht verfügbar.
- Um über den Zielport auf die Management-Funktionen zuzugreifen:
Markieren Sie im Rahmen *Ziel-Port* das Kontrollkästchen *Management erlauben*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

Um die *Port-Mirroring*-Funktion zu deaktivieren und die Voreinstellungen wiederherzustellen, klicken Sie die Schaltfläche  und dann den Eintrag *Konfiguration zurücksetzen*.

13.12 Selbsttest

Das Gerät prüft beim Booten und gelegentlich danach seine Anlagen. Das Gerät prüft die Aufgabenverfügbarkeit oder den Aufgabenabbruch im System sowie den verfügbaren Speicherplatz. Außerdem prüft das Gerät die Funktionalität der Anwendung und prüft, ob der Chipsatz eine Verschlechterung der Hardware aufweist.

Wenn das Gerät einen Integritätsverlust ermittelt, reagiert es auf die Beeinträchtigung mit einer benutzerdefinierten Maßnahme. Für die Konfiguration stehen folgende Kategorien zur Verfügung:

- ▶ `task`
Zu ergreifende Maßnahme, wenn eine Aufgabe missglückt ist.
- ▶ `resource`
Zu ergreifende Maßnahme bei ungenügenden Ressourcen.
- ▶ `software`
Zu ergreifende Maßnahme bei Verlust der Software-Integrität, wie bspw. bei Prüfsummenfehlern in Code-Segmenten oder bei Zugriffsverletzungen.
- ▶ `hardware`
Zu ergreifende Maßnahme aufgrund einer Beeinträchtigung der Hardware.

Legen Sie für jede Kategorie eine entsprechende Maßnahme fest, mit der das Gerät bei Feststellen eines Integritätsverlustes reagiert. Für die Konfiguration stehen folgende Funktionen zur Verfügung:

- ▶ `log only`
Diese Aktion schreibt eine Meldung an die Ereignisprotokolldatei.
- ▶ `send trap`
Sendet einen SNMP-Trap an das Trap-Ziel.
- ▶ `reboot`
Bei Aktivierung führt ein Fehler in dieser Kategorie zu einem Neustart des Gerätes.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Diagnose > System > Selbsttest*.
- Legen Sie für eine Ursache die auszuführende Aktion in Spalte *Aktion* fest.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

<code>enable</code>	Wechsel in den Privileged-EXEC-Modus.
<code>configure</code>	Wechsel in den Konfigurationsmodus.
<code>selftest action task log-only</code>	Senden einer Nachricht an das Ereignisprotokoll, wenn eine Aufgabe missglückt ist.
<code>selftest action resource send-trap</code>	Senden eines SNMP-Traps bei Ressourcen-Mangel.
<code>selftest action software send-trap</code>	Senden eines SNMP-Traps bei Verlust der Software-Integrität.
<code>selftest action hardware reboot</code>	Neustart des Gerätes bei Beeinträchtigung der Hardware

Durch die Deaktivierung dieser Funktionen können Sie die Zeit verkürzen, die zum Neustarten des Gerätes nach einem Kaltstart erforderlich ist. Diese Optionen finden Sie im Dialog *Diagnose > System > Selbsttest*, Rahmen *Konfiguration*.

- ▶ *RAM test*
Aktiviert/deaktiviert die RAM-Test-Funktion während eines Kaltstarts.
- ▶ *SysMon1 ist verfügbar*
Aktiviert/deaktiviert die System-Monitor-Funktion während eines Kaltstarts.
- ▶ *Bei Fehler Default-Konfiguration laden*
Aktiviert/deaktiviert das Laden der Standard-Gerätekonfiguration, falls dem Gerät beim Neustart keine lesbare Konfiguration zur Verfügung steht.

Anmerkung: Die folgenden Einstellungen sperren Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Neustart kein lesbares Konfigurationsprofil findet. Dies ist zum Beispiel dann der Fall, wenn sich das Passwort des zu ladenden Konfigurationsprofils von dem im Gerät festgelegten Passwort unterscheidet.

► Das Kontrollkästchen *SysMon1 ist verfügbar* ist unmarkiert.

► Das Kontrollkästchen *Bei Fehler Default-Konfiguration laden* ist unmarkiert.

Um das Gerät wieder entsperren zu lassen, wenden Sie sich an Ihren Vertriebspartner.

<code>selftest ramtest</code>	Aktivieren des RAM-Selbsttests bei einem Kaltstart
<code>no selftest ramtest</code>	Abschalten der Funktion „ramtest“
<code>selftest system-monitor</code>	Aktivieren der Funktion „SysMon1“
<code>no selftest system-monitor</code>	Abschalten der Funktion „SysMon1“
<code>show selftest action</code>	Statusanzeige der durchzuführenden Maßnahmen bei einer Beeinträchtigung des Gerätes
<code>show selftest settings</code>	Anzeige der Einstellungen für „ramtest“ und SysMon“ bei einem Kaltstart

14 **Erweiterte Funktionen des Gerätes**

14.1 MRP-IEEE

Die Erweiterung IEEE 802.1ak der Norm IEEE 802.1Q führte das Multiple-Registration-Protokoll (MRP) als Ersatz für das Generic-Attribute-Registration-Protokoll (*GARP*) ein. Zudem änderte und ersetzte das IEEE die *GARP*-Anwendungen, das *GARP*-Multicast-Registration-Protokoll (*GMRP*) und das *GARP*-VLAN-Registration-Protokoll (*GVRP*) mit dem Multiple-MAC-Registration-Protokoll (*MMRP*) und dem Multiple-VLAN-Registration-Protokoll (*MVRP*).

Um den Verkehr auf die erforderlichen Bereiche eines Netzes zu begrenzen, verteilen die MRP-Anwendungen Attribut-Werte an Geräte mit eingeschaltetem MRP innerhalb eines LANs. Die MRP-Anwendungen registrieren und deregistrieren Multicast-Gruppenmitgliedschaften und VLAN-Kennungen.

Anmerkung: Das Multiple-Registration-Protokoll (MRP) erfordert ein Loop-freies Netz. Um die Möglichkeit von Loops in Ihrem Netz zu verringern, verwenden Sie ein Netzprotokoll wie das Media-Redundancy-Protokoll, das Spanning-Tree-Protokoll oder das Spanning-Tree-Protokoll mit MRP.

14.1.1 MRP-Funktion

Jeder Teilnehmer enthält eine Anwendungskomponente und eine MRP-Attribute-Declaration(MAD)-Komponente. Die Anwendungskomponente ist verantwortlich für das Bilden der Attribute sowie deren Registrierung und Deregistrierung. Die MAD-Komponente erzeugt MRP-Nachrichten für die Vermittlung und verarbeitet empfangene Nachrichten anderer Teilnehmer. Die MAD-Komponente kodiert und vermittelt die Attribute an andere Teilnehmer in MRP-Dateneinheiten (MRPDU). Im Switch verteilt eine MRP-Attribute-Propagation(MAP)-Komponente die Attribute an teilnehmende Ports.

Für jede MRP-Anwendung und jedes LAN existiert ein Teilnehmer. Zum Beispiel befindet sich eine Teilnehmeranwendung auf einem Endgerät und eine weitere am Port des Switches. Die Applicant-State-Machine erfasst das Attribut und den Port jeder Anmeldung eines MRP-Teilnehmers an einem Endgerät oder Switch. Änderungen von Variablen der Applicant-State-Machine lösen die Vermittlung von MRPDUs aus, um die Anmeldung oder Rücknahme mitzuteilen.

Um eine *MMRP*-Instanz zu erzeugen, sendet ein Endgerät zunächst eine Join-Empty(JointMt)-Nachricht mit den entsprechenden Attributen. Der Switch flutet dann die JoinMt-Nachricht an den teilnehmenden Ports und den benachbarten Switches. Die benachbarten Switches fluten die Nachricht an ihren teilnehmenden Port und so weiter, wodurch ein Pfad für den Gruppen-Verkehr entsteht.

14.1.2 MRP-Timer

Die Timer-Voreinstellungen helfen, unnötige Attribut-Anmeldungen und -rücknahmen zu vermeiden. Die Timer-Einstellungen ermöglichen den Teilnehmern, MRP-Nachrichten vor Ablauf der Leave- oder LeaveAll-Timer zu empfangen und zu verarbeiten.

Erhalten Sie folgende Beziehungen aufrecht, wenn Sie die Timer neu konfigurieren:

- ▶ Für eine erneute Registrierung nach einem Leave- oder LeaveAll-Ereignis – auch im Fall einer verlorenen Nachricht – legen Sie den Wert für LeaveTime wie folgt fest: $\geq (2 \times \text{JoinTime}) + 60$ in 1/100 s
- ▶ Um das Volumen des nach einem LeaveAll-Ereignis neu hinzukommenden Verkehrs zu minimieren, legen Sie für den LeaveAll-Timer einen Wert fest, der höher ist als die LeaveTime.

Die folgende Liste enthält verschiedene vom Gerät übertragene MRP-Ereignisse.

- ▶ Join – Überwacht den Intervall für die nächste Join-Message-Übertragung
- ▶ Leave – Überwacht den Zeitraum, den ein Switch vor dem Wechsel in den Rücknahme-Status im Leave-Status bleibt.
- ▶ LeaveAll – Überwacht die Frequenz, mit welcher der Switch LeaveAll-Nachrichten erzeugt.

Der Periodic-Timer löst nach Ablauf eine MRP-Nachricht mit einem Join-Request aus, die der Switch an LAN-Teilnehmer sendet. Mit dieser Nachricht vermeiden Switches unnötige Rücknahmen.

14.1.3 MMRP

Wenn ein Gerät Broadcast-, Multicast- oder unbekannte Daten an einem Port empfängt, flutet das Gerät die Daten an andere Ports. Dieser Vorgang beansprucht unnötig Bandbreite im LAN.

Das Multiple-MAC-Registration-Protokoll (*MMRP*) bietet Ihnen die Möglichkeit, das Fluten von Daten mit dem Verteilen einer Attribut-Anmeldung an LAN-Teilnehmer zu überwachen. Die Attribut-Werte sind Informationen von Gruppen-Dienst-Anforderungen und 48-Bit-MAC-Adressen und werden von der MAD-Komponente kodiert und über MRP-Nachrichten an das LAN vermittelt.

Der Switch speichert die Attribute in einer Filterdatenbank als MAC-Adressen-Registrierungs-Einträge. Der Weiterleitungsprozess verwendet die Filterdatenbank-Einträge ausschließlich zur Vermittlung von Daten über diejenigen Ports, die zum Erreichen von LANs, die Gruppen-Mitglieder sind, notwendig sind.

Switches ermöglichen Mechanismen zur Verteilung in Gruppen, denen auf der Grundlage des Open-Host-Konzeptes, wobei sie Pakete an den aktiven Ports empfangen und sie ausschließlich an Ports weiterleiten, die Gruppen-Mitglieder sind. Auf diese Weise beantragt jeder *MMRP*-Teilnehmer mit an eine oder mehrere bestimmte Gruppen zu sendenden Paketen die Mitgliedschaft in der Gruppe. Nutzer von MAC-Diensten senden Pakete an eine bestimmte Gruppe von einem beliebigen Punkt im LAN. Eine Gruppe empfängt diese Pakete in den LANs, die an registrierte *MMRP*-Teilnehmer angebunden sind. *MMRP* und die MAC-Address-Registration-Einträge beschränken so die Pakete auf die erforderlichen Segmente eines Loop-freien LANs.

Um Registrierungs- und Deregistrierungsstatus aufrecht zu erhalten und Daten zu empfangen, erklärt ein Port periodisch sein Interesse. Jedes Gerät mit eingeschalteter *MMRP*-Funktion in einem LAN führt eine Filterdatenbank und leitet Daten mit den Gruppen-MAC-Adressen an die aufgeführten Teilnehmer weiter.

■ MMRP-Beispiel

In diesem Beispiel erwartet Host A für die Gruppe G1 bestimmte Daten. Switch A verarbeitet die **MMRP**-Join-Anfrage von Host A und sendet die Anfrage an beide benachbarte Switches. Die Geräte im LAN erkennen nun, dass ein Host auf den Empfang von Daten für Gruppe G1 bereit ist. Wenn Host B beginnt, die für Gruppe G1 bestimmten Daten zu vermitteln, fließen die Daten auf dem registrierten Pfad und Host A empfängt sie.

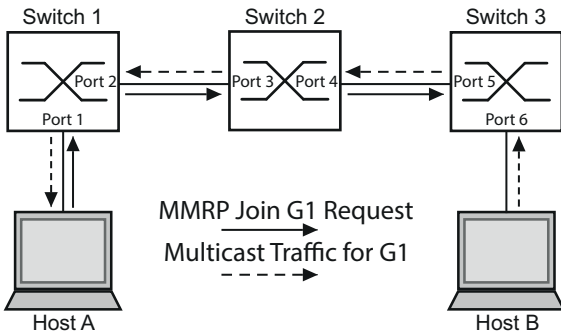


Abb. 50: **MMRP**-Netz für MAC-Adressen-Registrierung

Um die **MMRP**-Funktion auf den Switches einzuschalten, gehen Sie wie folgt vor.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog **Switching > MRP-IEEE > MMRP**, Registerkarte **Konfiguration**.
- Um Port 1 und Port 2 als **MMRP**-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte **MMRP** für Port 2 und Port 1.
- Um Port 3 und Port 4 als **MMRP**-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte **MMRP** für Port 4 und Port 2.
- Um Port 5 und Port 6 als **MMRP**-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte **MMRP** für Port 6 und Port 3.
- Um periodische Ereignisse zu senden, damit das Gerät die Anmeldung der MAC-Adressen-Gruppe aufrecht erhält, schalten Sie **Periodische State-Machine** ein. Wählen Sie im Rahmen **Konfiguration** das Optionsfeld .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

Um die **MMRP**-Ports an Switch 1 einzuschalten, verwenden Sie die folgenden CLI-Kommandos. Schalten Sie die **MMRP**-Funktionen und Ports an den Switches 2 und 3 ein, indem sie in den CLI-Kommandos die entsprechenden Interfaces ersetzen.

<pre>enable</pre>	Wechsel in den Privileged-EXEC-Modus.
<pre>configure</pre>	Wechsel in den Konfigurationsmodus.
<pre>interface 1/1</pre>	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
<pre>mrp-ieee mmrp operation</pre>	Einschalten der MMRP -Funktion auf dem Port.
<pre>interface 1/2</pre>	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
<pre>mrp-ieee mmrp operation</pre>	Einschalten der MMRP -Funktion auf dem Port.
<pre>exit</pre>	Wechsel in den Konfigurationsmodus.
<pre>mrp-ieee mrp periodic-state-machine</pre>	Globales Einschalten der Periodische State-Machine -Funktion.
<pre>mrp-ieee mmrp operation</pre>	Globales Einschalten der MMRP -Funktion.

14.1.4 MVRP

Das Multiple-VLAN-Registration-Protokoll (*MVRP*) ist eine MRP-Anwendung, die Dienste für die dynamische VLAN-Registrierung und -rücknahme bietet.

Die *MVRP*-Funktion bietet einen Mechanismus zur Erhaltung der dynamischen VLAN-Registrierung-Einträge und zur Vermittlung der Information an andere Geräte. Diese Information ermöglicht *MVRP*-fähigen Geräten, Informationen zu Ihrer VLAN-Mitgliedschaft zu erzeugen und zu aktualisieren. Wenn Mitglieder in einem VLAN angemeldet sind, geben diese Informationen Auskunft, über welche Ports der Switch die Daten an diese Mitglieder weiterleitet.

Hauptaufgabe der *MVRP*-Funktion ist, Switches zu ermöglichen, einige der VLAN-Informationen zu ermitteln, die Sie anderenfalls manuell festlegen. Das Ermitteln dieser Informationen ermöglicht Switches, Einschränkungen beim Bandbreitenverbrauch und bei der Konvergenzzeit in großen VLAN-Netzen zu bewältigen.

■ MVRP-Beispiel

Richten Sie ein Netz mit MVRP-fähigen Switches (1 – 4) ein, die in Ring-Topologie mit Endgerätegruppen verbunden sind; A1, A2, B1 und B2 in den 2 verschiedenen VLANs A und B. Zur Vermeidung von Loops Wenn an den Switches STP eingeschaltet ist, sind die Ports, die Switch 1 und Switch 4 verbinden, im „Discarding“-Status.

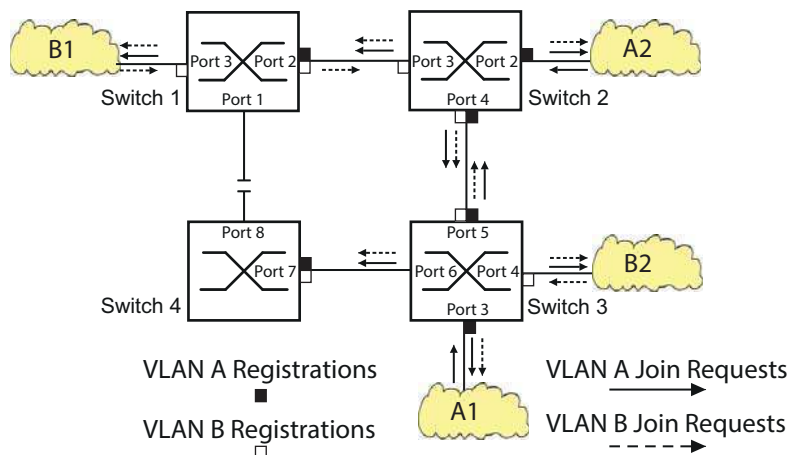


Abb. 51: *MVRP-Beispiel-Netz für VLAN-Registrierung*

Im MVRP-Beispiel-Netz senden die LANs zunächst eine Join-Anfrage an die Switches. Der Switch trägt die VLAN-Registrierung in die Adresstabelle (Forwarding Database) für den Port ein, der die Daten empfängt.

Der Switch verbreitet die Anfrage an die anderen Ports und sendet die Anfrage an die benachbarten LANs und Switches. Dieser Prozess hält an, bis die Switches die VLANs in die Adresstabelle des Empfangs-Ports eingefügt haben.

Um MVRP an den Switches einzuschalten, führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > MRP-IEEE > MVRP*, Registerkarte *Konfiguration*.
- Um die Ports 1 bis 3 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte *MVRP* für die Ports 3 bis 1.
- Um die Ports 2 bis 4 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte *MVRP* für die Ports 4 bis 2.
- Um die Ports 3 bis 6 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte *MVRP* für die Ports 6 bis 3.

- Um Port 7 und Port 8 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte *MVRP* für Port 8 und Port 4.
- Um die Registrierung der VLANs zu aufrecht zu erhalten, schalten Sie die *Periodische State-Machine* ein.
Wählen Sie im Rahmen *Konfiguration* das Optionsfeld .
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Um die *MVRP*-Ports an Switch 1 einzuschalten, verwenden Sie die folgenden CLI-Kommandos. Schalten Sie die *MVRP*-Funktionen und Ports an den Switches 2, 3 und 4 ein, indem sie in den CLI-Kommandos die entsprechenden Interfaces ersetzen.

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
interface 1/1	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
mrp-ieee mvrp operation	Einschalten der <i>MVRP</i> -Funktion auf dem Port.
interface 1/2	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
mrp-ieee mvrp operation	Einschalten der <i>MVRP</i> -Funktion auf dem Port.
exit	Wechsel in den Konfigurationsmodus.
mrp-ieee mvrp periodic-state-machine	Globales Einschalten der <i>Periodische State-Machine</i> -Funktion.
mrp-ieee mvrp operation	Globales Einschalten der <i>MVRP</i> -Funktion.

14.2 CLI Client

Das Gerät unterstützt einen CLI-Client, der direkt eine Verbindung zum SSH-Server über den im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH* festgelegten TCP-Port öffnet. Der CLI-Client bietet Ihnen die Möglichkeit, das Gerät mittels CLI-Kommandos zu konfigurieren.

Voraussetzung für die Verwendung des CLI-Clients ist, dass Sie die Funktion im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH* einschalten.

Detaillierte Informationen zu CLI-Kommandos finden Sie im Referenz-Handbuch „Command Line Interface“.

15 Industrieprotokolle

Lange Zeit gingen die Automatisierungs-Kommunikation und die Büro-Kommunikation getrennte Wege. Die Anforderungen an die Kommunikations-Eigenschaften waren zu unterschiedlich.

Die Büro-Kommunikation bewegt große Datenmengen mit geringen Anforderungen an die Übertragungszeit. Die Automatisierungs-Kommunikation bewegt kleine Datenmengen mit hohen Anforderungen an die Übertragungszeit und Verfügbarkeit.

Während die Vermittlungsgeräte im Büro meist in temperierten, relativ sauberen Räumen stehen, sind die Vermittlungsgeräte in der Automatisierung einem größeren Temperaturbereich ausgesetzt. Verschmutzte, staubige und feuchte Umgebungsbedingungen stellen weitere Anforderungen an die Beschaffenheit der Vermittlungsgeräte.

Mit der Weiterentwicklung der Kommunikations-Technologie näherten sich auch die Anforderungen an die Kommunikations-Eigenschaften an. Mit den heute zur Verfügung stehenden hohen Bandbreiten in der Ethernet-Technologie und den darauf aufsetzenden Protokollen lassen sich große Datenmengen übertragen und genaue Übertragungszeiten definieren.

Mit dem weltweit ersten, aktiven optischen LAN der Welt an der Universität Stuttgart 1984 legte Hirschmann den Grundstein für industriegerechte Büro-Kommunikationsgeräte. Dank der Initiative mit dem weltweit ersten Rail-Hub von Hirschmann in den neunziger Jahren stehen heute Ethernet-Vermittlungsgeräte wie Switches, Router und Firewalls für härteste Automatisierungsbedingungen zur Verfügung.

Der Wunsch nach einheitlichen, durchgängigen Kommunikationsstrukturen veranlasste viele Hersteller von Automatisierungsgeräten, sich zusammenzuschließen, um durch Standards den Fortschritt der Kommunikations-Technologie in der Automatisierung voranzutreiben. So stehen uns heute Protokolle zur Verfügung, die es uns erlauben, vom Büro aus bis in die Feldebene über Ethernet zukommunizieren.

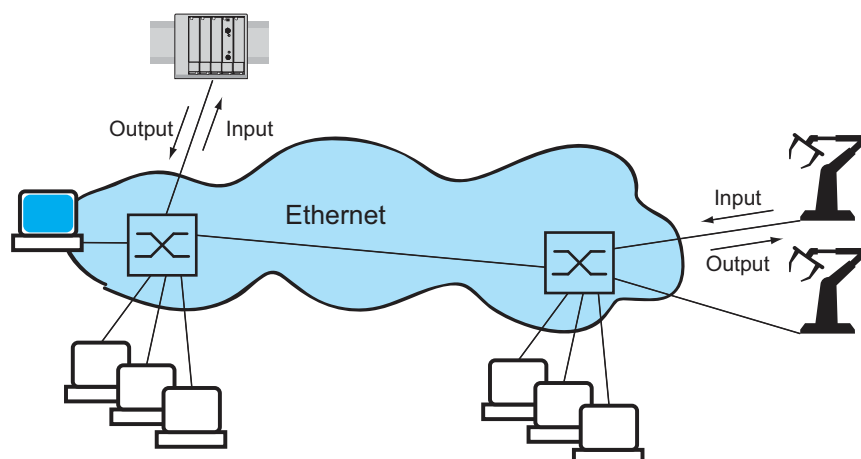


Abb. 52: Beispiel für die Kommunikation.

15.1 IEC 61850/MMS

IEC 61850/MMS ist ein von der International Electrotechnical Commission (IEC) standardisiertes industrielles Kommunikationsprotokoll. Anzutreffen ist das Protokoll in der Schaltanlagenautomatisierung, zum Beispiel in der Leittechnik von Energieversorgern.

Das paketorientiert arbeitende Protokoll basiert auf dem Transportprotokoll TCP/IP und nutzt Manufacturing Messaging Specification (MMS) für die Client-Server-Kommunikation. Das Protokoll ist objektorientiert und definiert eine einheitliche Konfigurationssprache, die u. a. Funktionen für SCADA, Intelligent Electronic Devices (IED) und für die Netzleittechnik umfasst.

Teil 6 der Norm IEC 61850 definiert die Konfigurationssprache SCL (Substation Configuration Language). SCL beschreibt die Eigenschaften des Gerätes sowie die Systemstruktur in maschinell verarbeitbarer Form. Die mit SCL beschriebenen Eigenschaften des Gerätes sind in der ICD-Datei auf dem Gerät gespeichert.

15.1.1 Switch-Modell für IEC 61850

Der Technical Report IEC 61850 90-4 spezifiziert ein Bridge-Modell. Die Funktionen eines Switches bildet das Bridge-Modell als Objekte eines Intelligent Electronic Devices (IED) ab. Ein MMS-Client (zum Beispiel die Leitstellen-Software) verwendet diese Objekte, um das Gerät zu überwachen und zu konfigurieren.

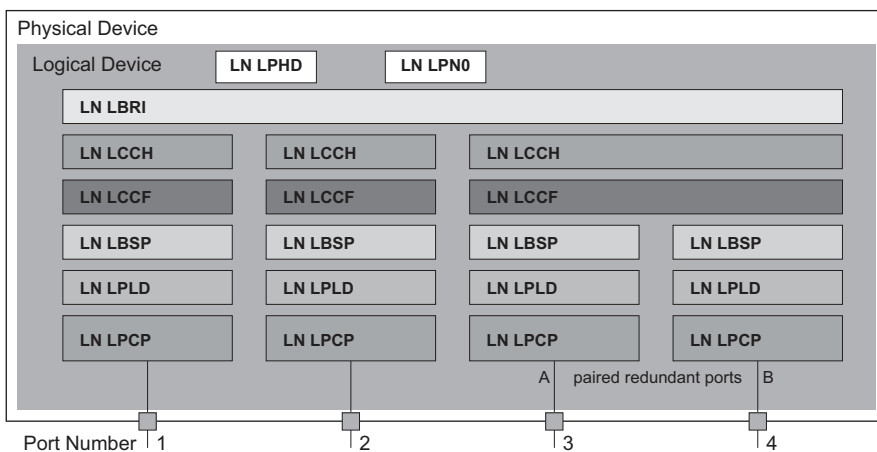


Abb. 53: Bridge-Modell nach Technical Report IEC 61850 90-4

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

Tab. 30: Klassen des Bridge-Modells nach TR IEC61850 90-4

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

Tab. 30: Klassen des Bridge-Modells nach TR IEC61850 90-4 (Forts.)

15.1.2 Integration in ein Steuerungssystem

■ Vorbereitung des Gerätes

- Vergewissern Sie sich, dass dem Gerät eine IP-Adresse zugewiesen ist.
- Öffnen Sie den Dialog *Erweitert* > *Industrie-Protokolle* > *IEC61850-MMS*.
- Um den MMS-Server zu starten, wählen Sie im Rahmen *Funktion* das Optionsfeld und klicken die Schaltfläche *An*.

Anschließend ist ein MMS-Client in der Lage, sich mit dem Gerät zu verbinden sowie die im Bridge-Modell definierten Objekte auszulesen und zu überwachen.


HINWEIS

GEFAHR DES UNAUTORISIERTEN ZUGRIFFS AUF DAS GERÄT

IEC61850/MMS bietet keine Authentifizierungsmechanismen. Ist der Schreibzugriff für IEC61850/MMS eingeschaltet, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Gerätes ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Gerätes und zu Ausfällen im Netz.


Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (zum Beispiel Firewall, VPN etc.) getroffen haben, um das Risiko unautorisierter Zugriffe auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann zu Geräteschäden führen.

- Um dem MMS-Client das Ändern der Einstellungen zu ermöglichen, markieren Sie das Kontrollkästchen *Schreibzugriff* und klicken die Schaltfläche .

■ Offline-Konfiguration

Das Gerät bietet Ihnen die Möglichkeit, mit Hilfe der grafischen Benutzeroberfläche die ICD-Datei herunterzuladen. Diese Datei enthält die mit SCL beschriebenen Eigenschaften des Gerätes und ermöglicht Ihnen, die Substation ohne direkte Verbindung zum Gerät zu konfigurieren.

- Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > IEC61850-MMS*.
- Um die ICD-Datei auf Ihren PC zu laden, klicken Sie die Schaltfläche  und dann den Eintrag *Download*.

■ Gerät überwachen

Der im Gerät integrierte IEC61850/MMS-Server bietet die Möglichkeit, mehrere Stati des Gerätes per Report Control Block (RCB) zu überwachen. Bis zu 5 MMS-Clients können sich gleichzeitig für einen Report Control Block anmelden.

Das Gerät ermöglicht das Überwachen der folgenden Stati:

Klasse	RCB-Objekt	Beschreibung
LN LBRI	RstpRoot	Ändert sich, wenn das Gerät die Rolle der Root-Bridge übernimmt oder abgibt.
	RstpTopoCnt	Ändert sich, wenn sich die Topologie auf Grund eines Wechsels der Root-Bridge ändert.
LN LCCH	ChLiv	Ändert sich, wenn sich der Link-Status des physischen Ports ändert.
LN LPCP	PhyHealth	Ändert sich, wenn sich der Link-Status des physischen Ports ändert.

Tab. 31: Mit IEC 61850/MMS überwachbare Stati des Gerätes

15.2 Modbus TCP

Modbus TCP ist ein Nachrichtenprotokoll auf der Anwendungsschicht, das eine Client-/Server-Kommunikation zwischen dem Client und den in Ethernet-TCP/IP-Netzen verbundenen Geräten herstellt.

Die *Modbus TCP*-Funktion bietet Ihnen die Möglichkeit, das Gerät in Netzen zu installieren, die bereits *Modbus TCP* verwenden, und die in den Registern auf dem Gerät gespeicherten Informationen abzurufen.

15.2.1 Modbus TCP/IP Client/Server-Modus

Das Gerät unterstützt das Modbus TCP/IP Client/Server-Modell. Das Gerät arbeitet in dieser Konstellation als Server und antwortet auf Anfragen eines Clients zu in den Registern gespeicherten Informationen. Um Daten zwischen dem Client und dem Server auszutauschen, verwendet das Client/Server-Modell 4 Nachrichtentypen:

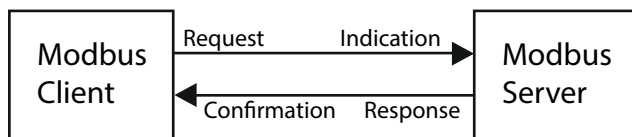


Abb. 54: Modbus TCP/IP Client/Server-Modus

- ▶ Modbus TCP/IP-Anfrage; der Client erzeugt eine Informationsanforderung und sendet sie an den Server.
- ▶ Modbus TCP/IP-Hinweis; der Server empfängt eine Anfrage als Hinweis, dass ein Client Informationen anfordert.
- ▶ Modbus TCP/IP-Antwort; wenn die angeforderten Informationen verfügbar sind, sendet der Server eine Antwort mit den angeforderten Informationen. Wenn die angeforderten Informationen nicht verfügbar sind, sendet der Server eine Ausnahmeantwort, um den Client über den während der Verarbeitung erkannten Fehler zu benachrichtigen. Die Ausnahmeantwort enthält einen Ausnahmecode, der die Ursache des erkannten Fehlers angibt.
- ▶ Modbus TCP/IP-Bestätigung; der Client empfängt eine Antwort vom Server mit den angeforderten Informationen.

15.2.2 Unterstützte Funktionen und Speicherzuordnung

Das Gerät unterstützt Funktionen mit den öffentlichen Codes `0x03` `Read Holding Registers` und `0x05` `Write Single Coil`. Die Codes ermöglichen dem Benutzer, in den Registern gespeicherte Informationen zu lesen, zum Beispiel Systeminformationen einschließlich Systemname, Systemstandort, Software-Version, IP-Adresse und MAC-Adresse. Die Codes ermöglichen dem Benutzer außerdem, die Port-Informationen und die Port-Statistik zu lesen. Der Code `0x05` bietet dem Benutzer die Möglichkeit, die Port-Zähler einzeln oder global zurückzusetzen.

Die folgende Liste enthält Informationen zu den in die Spalte `Format` eingetragenen Werten:

- ▶ **Bitmap:** Eine Gruppe von 32 Bits, verschlüsselt in der Big-Endian-Byte-Reihenfolge und gespeichert in 2 Registern. Big-Endian-Systeme speichern das höchstwertige Byte eines Wortes in der kleinsten Adresse und das niedrigstwertige Byte in der größten Adresse.
- ▶ **F1:** 16-bit unsigned integer
- ▶ **F2:** Enumeration - power supply alarm
 - 0 = power supply good
 - 1 = power supply failure detected
- ▶ **F3:** Enumeration - OFF/ON
 - 0 = Off
 - 1 = On
- ▶ **F4:** Enumeration - port type
 - 0 = Giga - Gigabit Interface Converter (GBIC)
 - 1 = Copper - Twisted Pair (TP)
 - 2 = Fiber - 10 Mb/s
 - 3 = Fiber - 100 Mb/s
 - 4 = Giga - 10/100/1000 Mb/s (triple speed)
 - 5 = Giga - Copper 1000 Mb/s TP
 - 6 = Giga - Small Form-factor Pluggable (SFP)
- ▶ **F9:** 32-bit unsigned long
- ▶ **Zeichenfolge:** Oktette, in Sequenz gespeichert, 2 Oktette je Register.

■ Modbus TCP/IP-Codes

Die folgende Tabelle enthält Adressen, die dem Client ermöglichen, Port-Zähler zurückzusetzen und spezifische Informationen aus den Geräteregistern abzurufen.

■ Port-Informationen

Adresse	Menge	Beschreibung	Min	Max	Schritt	Einheit	Format
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1

Tab. 32: Port-Informationen

Adresse	Menge	Beschreibung	Min	Max	Schritt	Einheit	Format
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

Tab. 32: Port-Informationen

■ Port-Statistik

Adresse	Menge	Beschreibung	Min	Max	Schritt	Einheit	Format
0800	1	Port1 - Number of bytes received	0	4294967295	1	-	F9
0802	1	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	1	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	1	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	1	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	1	Port1 - Total frames received	0	4294967295	1	-	F9
080C	1	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	1	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	1	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	1	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	1	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	1	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	1	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	1	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	1	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	1	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	1	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	1	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	1	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	1	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	1	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	1	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	1	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9

Tab. 33: Port-Statistik

Adresse	Menge	Beschreibung	Min	Max	Schritt	Einheit	Format
082E	1	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	1	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
147E	1	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

Tab. 33: Port-Statistik

15.2.3 Beispiel-Konfiguration

In diesem Beispiel konfigurieren Sie das Gerät so, dass es auf Client-Anfragen antwortet. Voraussetzung für diese Konfiguration ist, dass das Client-Gerät mit einer IP-Adresse aus dem angegebenen Bereich konfiguriert ist. In diesem Beispiel bleibt die Funktion *Schreibzugriff* deaktiviert. Wenn Sie die Funktion *Schreibzugriff* aktivieren, ermöglicht das Gerät Ihnen ausschließlich, die Port-Zähler zurückzusetzen. In der Standardkonfiguration sind die Funktionen *Modbus TCP* und *Schreibzugriff* inaktiv.


HINWEIS

GEFAHR DES UNAUTORISIERTEN ZUGRIFFS AUF DAS GERÄT

Das *Modbus TCP*-Protokoll bietet keine Authentifizierungsmechanismen. Ist der Schreibzugriff für *Modbus TCP* eingeschaltet, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Gerätes ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Gerätes und zu Ausfällen im Netz.

Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (zum Beispiel Firewall, VPN etc.) getroffen haben, um das Risiko unautorisierter Zugriffe auszuschließen.

Die Nichtbeachtung dieser Anweisungen kann zu Geräteschäden führen.

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung*.
- Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche  .
- Legen Sie den IP-Adressbereich in Zeile *Index 2* fest, indem Sie 10.17.1.0/29 in die Spalte *IP-Adressbereich* eingeben.
- Vergewissern Sie sich, dass die *Modbus TCP*-Funktion aktiviert ist.
- Um den Bereich zu aktivieren, markieren Sie das Kontrollkästchen *Aktiv*.
- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus > Global*.
- Vergewissern Sie sich, dass das Kontrollkästchen *Modbus TCP aktiv* markiert ist.
- Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > Modbus TCP*.
- Voreingestellt ist der standardmäßige *Modbus TCP*-Lausch-Port, Port 502. Wenn Sie an einem anderen TCP-Port lauschen möchten, geben Sie den Wert für den Lausch-Port in das Feld *TCP-Port* ein.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
Wenn Sie die *Modbus TCP*-Funktion einschalten, erkennt die *Sicherheitsstatus*-Funktion die Aktivierung und zeigt einen Alarm im Dialog *Grundeinstellungen > System*, Rahmen *Sicherheits-Status*.

<pre>enable network management access add 2 network management access modify 2 ip 10.17.1.0 network management access modify 2 mask 29 network management access modify 2 modbus-tcp enable network management access operation configure security-status monitor modbus-tcp- enabled modbus-tcp operation modbus-tcp port <1..65535> show modbus-tcp Modbus TCP/IP server settings ----- Modbus TCP/IP server operation.....enabled Write-access.....disabled Listening port.....502 Max number of sessions.....5 Active sessions.....0 show security-status monitor Device Security Settings Monitor ----- Password default settings unchanged.....monitored ... Write access using HiDiscovery is possible...monitored Loading unencrypted configuration from ENVM...monitored IEC 61850 MMS is enabled.....monitored Modbus TCP/IP server active.....monitored show security-status event</pre>	<p>Wechsel in den Privileged-EXEC-Modus. Erzeugt den Eintrag für den Adressbereich im Netz. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: 2. Legt die IP-Adresse fest.</p> <p>Legt die Netzmaske fest.</p> <p>Legt fest, dass <i>Modbus TCP</i> Verwaltungszugriff hat.</p> <p>Schaltet die IP-Zugriffsbeschränkung ein. Wechsel in den Konfigurationsmodus. Legt fest, dass das Gerät die Aktivierung des <i>Modbus TCP</i>-Servers überwacht.</p> <p>Schaltet den <i>Modbus TCP</i>-Server ein. Den TCP-Port für die <i>Modbus TCP</i>-Kommunikation festlegen (optional). Voreingestellt ist Port 502. Die <i>Modbus TCP</i>-Server-Einstellungen anzeigen.</p> <p>Zeigen Sie alle Sicherheitsstatus-Einstellungen.</p> <p>Die aufgetretenen Sicherheitsstatus-Ereignisse anzeigen.</p>
---	--


```
Time stamp          Event          Info
-----
2014-01-01 01:00:39 password-change(10) -
.....
2014-01-01 01:00:39 ext-nvm-load-unsecure(21) -
2014-01-01 23:47:40 modbus-tcp-enabled(23) -
```

```
show network management access rules 1 Zeigen Sie die Regeln für den eingeschränkten Management-Zugriff für Index 1.
```

```
Restricted management access settings
```

```
-----
Index.....1
IP Address.....10.17.1.0
Prefix Length.....29
HTTP.....yes
SNMP.....yes
Telnet.....yes
SSH.....yes
HTTPS.....yes
IEC61850-MMS.....yes
Modbus TCP/IP.....yes
Active.....[x]
```

15.3 EtherNet/IP

EtherNet/IP ist ein weltweit akzeptiertes, standardisiertes industrielles Kommunikationsprotokoll, das von der Open DeviceNet Vendor Association (ODVA) gepflegt wird. Das Protokoll basiert auf den weit verbreiteten Standard-Ethernet-Übertragungsprotokollen TCP/IP und UDP/IP. *EtherNet/IP* wird von führenden Herstellern unterstützt und bietet daher eine breite Grundlage für den effektiven Datenverkehr im Industriebereich.

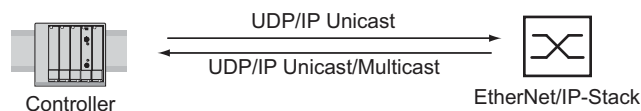


Abb. 55: *EtherNet/IP*-Netz

EtherNet/IP erweitert die Standard-Ethernet-Protokolle um das Industrieprotokoll CIP (Common Industrial Protocol). *EtherNet/IP* implementiert CIP in der Sitzungsschicht und darüber und passt CIP der spezifischen *EtherNet/IP*-Technologie in der Transportschicht und darunter an. Bei Automationsanwendungen implementiert *EtherNet/IP* CIP auf Anwendungsebene. Daher ist *EtherNet/IP* optimal für den Bereich der industriellen Steuerungstechnik geeignet.

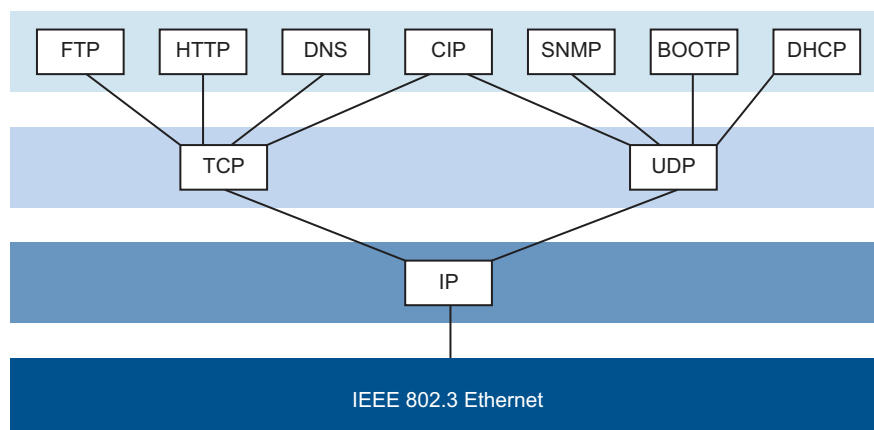


Abb. 56: IEEE802.3 *EtherNet/IP*

EtherNet/IP treffen Sie insbesondere in den USA und im Verbindung mit Rockwell-Steuerungen an.

Ausführliche Informationen zu *EtherNet/IP* finden Sie auf der ODVA-Startseite unter www.odva.org/Home/ODVATECHNOLOGIES/EtherNetIP.aspx.

15.3.1 Integration in ein Steuerungssystem

Um das Gerät in ein Steuerungssystem zu integrieren, führen Sie folgende Schritte aus:

- Öffnen Sie den Dialog *Switching > IGMP-Snooping > IGMP-Snooping Global*.
- Vergewissern Sie sich, dass die IGMP-Snooping-Funktion aktiviert ist.
- Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > EtherNet/IP*. Vergewissern Sie sich, dass die *EtherNet/IP*-Funktion aktiviert ist.
- Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > EtherNet/IP*.
- Um das EDS als ZIP-Datei auf Ihrem PC zu speichern, klicken Sie *Download*. Die ZIP-Datei enthält die *EtherNet/IP*-Konfigurationsdatei und das Symbol, über das eine Verbindung zwischen der Steuerung und dem Gerät konfiguriert wird.

Anmerkung: Wenn *EtherNet/IP* und die Routing-Funktion gleichzeitig aktiviert sind, können Funktionsstörungen in Bezug auf *EtherNet/IP* auftreten, zum Beispiel im Zusammenhang mit „RS Who“. Wenn die Routing-Funktion aktiv ist, deaktivieren Sie die Routing-Funktion des Gerätes.

- Um die Routing-Funktion des Gerätes zu deaktivieren, öffnen Sie den Dialog *Routing > Routing Global*, und klicken Sie im Rahmen *Funktion* das Optionsfeld .

Um die *Routing*-Funktion zu deaktivieren, führen Sie die folgenden Schritte aus:

- | | |
|---------------|--|
| enable | Wechsel in den Privileged-EXEC-Modus. |
| configure | Wechsel in den Konfigurationsmodus. |
| no ip routing | Routing-Funktion auf dem Gerät deaktivieren. |

■ Konfiguration einer SPS am Beispiel der Rockwell-Software

- Öffnen Sie das „EDS Hardware Installation Tool“ von RSLinx.
- Fügen Sie mit dem „EDS Hardware Installation Tool“ die EDS-Datei hinzu.
- Starten Sie den Dienst „RSLinx“ neu, damit RSLinx die EDS-Datei des Geräts übernimmt.
- Prüfen Sie mit RSLinx, ob RSLinx das Gerät erkannt hat.
- Öffnen Sie Ihr Logix 5000 - Projekt.
- Binden Sie das Gerät als neues Modul (Generic Ethernet Module) am Ethernet-Port des Controllers ein.

Einstellung	I/O-Verbindung	Input only	Listen only
Comm Format	Data - DINT	Data - DINT	Input data - DINT - Run/ Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	2	2	2
Input Size	7	7	7
Input Size	7	7	7
Output Assembly Instance	1	254	255
Output Size	1	0	0
Output Size	1	0	0
Configuration Assembly Instance	3	3	3
Configuration Size	0	0	0

Tab. 34: Einstellungen zum Einbinden eines Generic Ethernet Module

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

Anmerkung: Die Überwachung der I/O-Verbindung zur CPU als Ausfallkriterium kann zum Anlagenausfall führen. Daher ist die Überwachung der I/O-Verbindung als Ausfallkriterium weniger geeignet.

Die I/O-Verbindung zwischen der speicherprogrammierbaren Steuerung (SPS) und dem Gerät kann durch ein Management-Programm unterbrochen werden. Beispielsweise kann eine Netzmanagementstation die CPU des Gerätes mit Echtzeitdaten (RT-Daten) mit einer höheren Priorität auslasten. In diesem Fall kann das Gerät weiterhin Datenpakete senden oder empfangen, und das System bleibt betriebsbereit.

■ Beispiel zur Integration aus der Sample Code Library

Die Sample Code Library ist eine Web-Seite von Rockwell. Sie hat das Ziel, den Anwendern einen Platz zu bieten, an welchem sie ihre besten Architekturintegrations-Anwendungen austauschen können.

Suchen Sie in der Web-Seite <http://samplecode.rockwellautomation.com> nach der „Catalog Number“ 9701. Das ist die Katalognummer für ein Beispiel zur Integration des Hirschmann-Geräts in RS Logix 5000 Rel. 16, SPS-Firmware Release 16.

15.3.2 EtherNet/IP -Entity-Parameter

Die folgenden Absätze identifizieren die Objekte, die das Gerät unterstützt.

Speichern Sie die gesamte Gerätekonfiguration. Wenn das Gerät einen Set-Request empfängt, antwortet es darauf beim Speichern der Gerätekonfiguration. Die LEDs blinken, bis das Gerät das Speichern der Gerätekonfiguration beendet.

■ Identity-Objekt

Das Gerät unterstützt das Identity-Objekt (Class Code 0x01) von *EtherNet/IP*. Die Hersteller-ID von Hirschmann lautet 634. Zur Kennzeichnung des Produkttyps „Hirschmann“ verwendet 44 (0x2C) die ID Managed Ethernet Switch.

Die folgende Tabelle listet die Instanzattribute auf. Ausschließlich Instanz 1 ist verfügbar:

Id	Attribute	Access Rule	Data type	Description
1	Vendor ID	Get	UINT	Hirschmann634
2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
3	Product Code	Get	UINT	Product Code: mapping is defined for every device type
4	Revision	Get	STRUCT of: USINT MajorUSINT Minor	Revision of the EtherNet/IP implementation, 2.1.
5	Status	Get	WORD	Support for the following Bit status only: Bit 0: Owned (always 1) Bit 2: Configured (always 1) Bit 4 -7: Extend Device Status value 3: No I/O connection established, value 7: At least one I/O connection established, all in idle mode.
6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
7	Product name	Get	Short String (max. 32 Byte)	Displayed as "Hirschmann" + product family + product ID + software variant.

■ TCP/IP Interface Object

Das Gerät unterstützt ausschließlich Instanz 1 des TCP/IP-Objektes (Class Code 0xf5, F5_H, 245) von *EtherNet/IP*.

In Abhängigkeit vom Schreibzugriff-Status speichert das Gerät die vollständige Konfiguration im Flash-Speicher des Gerätes. Das Speichern der Konfigurationsdatei kann bis zu 10 Sekunden in Anspruch nehmen. Wird der Speichervorgang beispielsweise durch einen Ausfall der Stromversorgung unterbrochen, ist der Betrieb des Gerätes ggf. nicht möglich.

Anmerkung: Das Gerät reagiert auf die Konfigurationsänderung `Get Request` mit einer `Response`, selbst wenn der Speichervorgang für die Konfiguration noch nicht abgeschlossen ist.

Die folgende Tabelle listet die Klassenattribute auf:

Id	Attribute	Access Rule	Data type	Description
1	Revision	Get	UINT	Revision of this object: 3
2	Max Instance	Get	UINT	Maximum instance number: 1
3	Number of instance	Get	UINT	Number of object instances currently created: 1

Die folgende Tabelle listet die Attribute von Instanz 1 auf:

Id	Attribute	Access Rule	Data type	Description
1	Status	Get	DWORD	Interface Status: Bit 0-3: 0 Interface not configured, 1 Interface contains valid config Bit 6: AcdStatus (default 0) Bit 7: AcdFault (default 0)
2	Interface Capability flags	Get	DWORD	Bit 0: BOOTP Client Bit 1: DNS Client Bit 2: DHCP Client Bit 3: DHCP-DNS Update Bit 4: Configuration settable (within CIP), Other bits reserved (0). Bit 7: AcdCapable (TRUE shall indicate that the device is ACD capable)
3	Config Control	Set/Get	DWORD	Bit 0-3: Value 0 using stored config Value 1 using BOOTP Value 2 using DHCP Bit 4: 1 device uses DNS for name lookup (always 0 because not supp.) Other bits reserved (0)
4	Physical Link Object	Get	STRUCT of:UINT Path sizeEPATH Path	Path to the Physical Link Object, always {0x20,0xF6,0x24,0x01} describing instance 1 of the Ethernet Link Object.
5	Interface Configuration	Set/Get	STRUCT of:UDINT IP addressUDINT NetmaskUDINT Gateway addressUDINT Name server 1UDINTName server 2STRING Domain name	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
6	Host Name	Set/Get	STRING	Host Name (for DHCP DNS Update).
7	Safety Network Number			Not supported
8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets. (1–255) The default values: TTL = 1
9	Mcast Config	Get/Set	STRUCT of:USINT Alloc control, USINT reserved, UINT Num Mcast, UDINT Mcast Start Addr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0

Id	Attribute	Access Rule	Data type	Description
10	SelectedAcid	Get/Set	BOOL	Enable ACD (1 default).Disable ACD (0)
11	LastConflictDetected	Get	STRUCT of:USINT AcidActivity,Array of 6 USINT, RemoteMAC Array of 28 USINT ArpPdu	ACD Diagnostic Parameters

Die folgende Tabelle listet die Hirschmann-Erweiterungen zum TCP/IP Interface Object auf:

Id	Attribute	Access Rule	Data type	Description
100=0x64	Cable Test	Set/Get	STRUCT of:USINT Interface,USINT Status	STRUCT of: USINT Interface USINT Status (active (1) Success (2) Failure (3) Uninitialized (4)
101=0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of:2 Pair for 100BASE4 Pair for 1000BASE
102=0x66	Cable Test Result	Get	STRUCT of: USINT Interface,USINT CablePair,USINT CableStatus,USINT CableMinLength, USINT CableMaxLengthUSINTCableF ailureLocation	100BASE:{ {Interface,CablePair1,CableStatus, CableMinLength, CableMaxLength, CableFailureLocation} {Interface,CablePair2,CableStatus, CableMinLength, CableMaxLength, CableFailureLocation} } 1000BASE:{ {Interface,CablePair1,CableStatus, CableMinLength, CableMaxLength, CableFailureLocation} {Interface,CablePair2,CableStatus, CableMinLength, CableMaxLength, CableFailureLocation} {Interface,CablePair3,CableStatus, CableMinLength, CableMaxLength, CableFailureLocation} {Interface,CablePair4,CableStatus, CableMinLength, CableMaxLength, CableFailureLocation} }

■ Ethernet-Verbindungsobjekt

Legen Sie mindestens 1 Instanz für das Gerät fest, zum Beispiel Instanz 1 als CPU-Ethernet-Schnittstelleninstanz (Class Code 0xf6, F6_H, 246) von *EtherNet/IP*.

Id	Attribute	Access Rule	Data type	Description
1	Interface Speed	Get	UDINT	Used interface speed in Mbits/s (10, 100, 1000, ...). 0 is used when the speed has not been determined or is invalid because of errors.
2	Interface Flags	Get	DWORD	Interface Status Flags: Bit 0: Link State (1=Link) Bit 1: Halfduplex(0)/Fullduplex(1) Bits 2-4: Autoneg Status 0 Autoneg in Progress 1 Autoneg failed 2 failed but Speed detected 3 Autoneg success 4 No Autoneg Bit 5: manual configuration require reset (always 0 because not needed) Bit 6: hardware error.

Id	Attribute	Access Rule	Data type	Description
3	Physical Address	Get	ARRAY of 6 USINTs	MAC address of physical interface.
4	Interface Counters	Get	STRUCT of: MIB II CountersEach UDINT	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors.
5	Media Counters	Get	STRUCT of: Ethernet MIB CountersEachUDINT	Alignment Errors, FCS Errors, Single Collision, Multiple Collision, SQE Test Errors, Deferred Transmissions, Late Collisions, Excessive Collisions, MAC TX Errors, Carrier Sense Errors, Frame Too Long, MAC RX Errors.
6	Interface Control	Get/Set	STRUCT of: WORD Control Bits Forced lface Speed	Control Bits: Autoneg enable/disable (Bit 0, enable=1) Duplex mode (Bit 1, full duplex=1), if Autoneg disabled (Bit 0 set to 0). Interface speed in Mbits/s: 10,100,..., if Autoneg disabled (Control Bit 0 set to 0).
7	Interface type	Get	USINT	Type of interface: Value 0: Unknown interface type, Value 1: The interface is internal, Value 2: Twisted-pair, Value 3: Optical fiber.
3	Interface state	Get	USINT	Current state of the interface: Value 0: Unknown interface state, Value 1: The interface is enabled, Value 2: The interface is disabled, Value 3: The interface is testing
9	Admin State	Set/Get	USINT	Administrative state: Value 1: Enable the interface, Value 2: Disable the interface.
10	Interface label	Get	SHORT-STRING	Human readable ID

Die folgende Tabelle listet die Hirschmann-Erweiterungen zum Ethernet Link Object auf:

Id	Attribute	Access Rule	Data type	Description
100=0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
101=0x65	Port Control	Get/Set	DWORD	Bit 0 (RO): Link state 0 link down 1 link up Bit 1 (R/W): Link admin state 0 disabled 1 enabled Bit 8 (RO): Access violation alarm Bit 9 (RO): Utilization alarm
102=0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2DiagfaceUtilization is used. Utilization in percentage (Unit 1% = 100, %/100). RX Interface Utilization.
103=0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagfaceUtilizationAlarmUpperThresh old can be accessed. Utilization in percentage (Unit 1% = 100). RX Interface Utilization Upper Limit.
104=0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagfaceUtilizationAlarmLowerThresh old can be accessed. Utilization in percentage (Unit 1% = 100). RX Interface Utilization Lower Limit.
105=0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0 = disabled), Frames/ second

Id	Attribute	Access Rule	Data type	Description
106=0x6A	Ethernet Interface Description	Get/Set	STRING [max. 64 Bytes] even number of Bytes	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX", or "unavailable", max. 64 Bytes.
107=0x6B	Port Monitor	Get/Set	DWORD	Bit 0: Link Flap 1 ON 0 OFF Bit 1: CRC/Fragment 1 ON 0 OFF Bit 2: Duplex Mismatch 1 ON 0 OFF Bit 3: Overload-Detection 1 ON 0 OFF Bit 4: Link-Speed/ Duplex Mode 1 ON 0 OFF Bit 5-6: Action (to be performed in the event) Bit 01: Deactivate Port Bit 10: Send Trap Bit 7-11: Active Condition (displays which condition caused an action to occur) Bit 00001: Link Flap Bit 00010: CRC/Fragments Bit 00100: Duplex Mismatch Bit 01000: Overload-Detection Bit 10000: Link-Speed/ Duplex mode) Bit 12-15: Reserved (always 0)
108=0x6C	Quick Connect	Get/Set	USINT	Enable /disable Quick Connect on the interface. If you enable Quick Connect, then the device sets the port speed to 100FD, disables auto-negotiation, and spanning tree on the interface. Quick Connect (1 ON, 0 OFF)
109=0x6D	SFP Diagnostics Get	Get	STRUCT of: STRING Module type SHORT-STRING Serial Number USINT Connector USINT Supported DINT Temperature °C DINT Tx Power in mW DINT Rx Power in mW DINT Tx Power in dBm DINT Rx Power in dBm	STRUCT of: { STRING Module type UDINT Serial Number USINT Connector USINT Supported DINT Temperature °C DINT Tx Power in mW DINT Rx Power in mW DINT Tx Power in dBm DINT Rx Power in dBm

■ Switch-Agent-Objekt

Das Gerät unterstützt das herstellerspezifische Ethernet-Switch-Agent-Objekt von Hirschmann (Class Code 0x95, 95_H, 149) für die Gerätekonfigurations- und Informationsparameter mit Instanz 1.

Die folgende Tabelle listet die Instanzattribute des Ethernet-Switch-Agent-Objektes auf:

Switch Status	Id 0x1	DWORD (32 Bit) RO
	Bit 0	Like the signal contact, the value indicates the Device Overall state (0 ok, 1 failed).
	Bit 1	Device Security Status (0 ok, 1 failed)
	Bit 2	Power Supply 1 (0 ok, 1 failed or not existing)
	Bit 3	Power Supply 2 (0 ok, 1 failed or not existing)

Switch Status	Id 0x1	DWORD (32 Bit) RO
	Bit 4	Reserved
	Bit 5	Reserved
	Bit 6	Signal Contact 1 (0 closed, 1 open)
	Bit 7	Signal Contact 2 (0 closed, 1 open or not existing)
	Bit 8	Reserved
	Bit 9	Temperature (0 ok, 1 Failure)
	Bit 10	Module removed (1 removed)
	Bit 11	ACA21/ACA22 removed (1 removed)
	Bit 12	ACA31 removed (1 removed)
	Bit 13	Reserved
	Bit 14	Reserved
	Bit 15	Reserved
	Bit 16	Reserved
	Bit 17	Reserved
	Bit 18	Reserved
	Bit 19	Reserved
	Bit 20	Reserved
	Bit 21	Reserved
	Bit 22	Reserved
	Bit 23 - 30	Network Redundancy: Bit 23: MRP Bit 24: PRP Bit 25: HSR Bit 26: RSTP Bit 27: LAG Bit 28: DLR Bit 29-30: Reserved No Network Redundancy: (0 enabled)
	Bit 31	Connection Error: (1 Failure)

Switch Temperature	Id 0x2	Struct{INT RO Temperature °F INT RO Temperature °C}
--------------------	--------	---

Reserved	Id 0x3	UDINT (unsigned 32 Bit int) RO
		Always 0, attribute is reserved for future use.

Switch Max Ports	Id 0x4	UINT (16 Bit) RO Maximum number of Ethernet Switch Ports
------------------	--------	--

Multicast Settings (IGMP Snooping)	Id 0x5	WORD (16Bit) RW
	Bit 0 RW	IGMP Snooping (1 enabled, 0 disabled)
	Bit 1 RW	IGMP Querier (1 enabled, 0 disabled)
	Bit 2 RO	IGMP Querier Mode (1 Querier, 0=Non-Querier)
	Bit 4 - 6 RW	IGMP Querier Packet Version V1 = 1 V2 = 2 V3 = 3 Off = 0 IGMP Querier disabled
	Bit 8 - 10 RW	Treatment of Unknown Multicasts (Railswitch only): 0 = Send To All Ports 1 = Send To Query Ports 2 = Discard

Switch Existing Ports	Id 0x6 Per Bit starting with Bit 0 (=Port 1)	ARRAY OF DWORD (32 bit) RO Bitmask of existing Switch Ports 1=Port existing 0=Port not available. Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for example max. 28 Ports => 1 DWORD is used (32 Bit)).
Switch Port Control	Id 0x7 Per Bit starting with Bit 0 (=Port 1)	ARRAY OF DWORD (32 bit) RW Bitmask Link Admin Status Switch Ports 0=Port enabled 1=Port disabled Array (bit mask) size is adjusted to the size of maximum number of Switch ports (e.g. max. 28 Ports => 1 DWORD is used (32 Bit)).
Switch Ports Mapping	Id 0x8 Starting with Index 0 (=Port 1)	ARRAY OF USINT (BYTE, 8 bit) RO Instance number of the Ethernet-Link-Object All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist
Switch Action Status	Id 0x9	DWORD (32 Bit) RO, Status of the last executed action (for example config save, software update, etc.)
	Bit 0	Flash Save Configuration In Progress/Flash Write In Progress
	Bit 1	Flash Save Configuration Failed/Flash Write Failed
	Bit 4	Configuration changed (configuration not in sync. between running configuration

Das Hirschmann-spezifische Ethernet-Switch-Agent-Objekt bietet Ihnen den zusätzlichen herstellerspezifischen Dienst mit dem Service-Code 35H zum Speichern der Switch-Konfiguration. Wenn Sie über Ihren PC eine Anfrage zum Speichern einer Gerätekonfiguration senden, sendet das Gerät nach dem Speichern der Konfiguration im Flash-Speicher eine Antwort.

■ Basis-Switch-Objekt (0x51)

Das Basis-Switch-Objekt stellt die Schnittstelle auf CIP-Anwendungsebene zu grundlegenden Statusinformationen für einen Managed Ethernet Switch (Revision 1) bereit.

Ausschließlich Instanz 1 des Basis-Switch (Class Code 0x51) ist verfügbar.

Die folgende Tabelle listet die Instanzattribute auf:

Id	Attribute	Access Rule	Data type	Description
1	Device Up Time	Get	UDINT	Time since the device powered up
2	Total port count	Get	UDINT	Number of physical ports
3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
4	Power source	Get	WORD	Status of switch power source
5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
6	Existing ports	Get	Array of DWORD	Port Mask
7	Global Port Admin State	Get	Array of DWORD	Port Admin Status
8	Global Port link Status	Get	Array of DWORD	Port Link Status
9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version

Id	Attribute	Access Rule	Data type	Description
10	Contact Status	Get	UDINT	Switch Contact Closure
11	Aging Time	Get	UDINT	Range 10...1000000 0= Learning off Default = 300
12	Temperature C	Get	UINT	Switch temperature in degrees Celsius
13	Temperature F	Get	UINT	Switch temperature in degrees Fahrenheit

■ Dienste, Verbindungen, I/O-Daten

Das Gerät unterstützt die folgenden Verbindungstypen und Parameter.

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/ Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

Tab. 35: Einstellungen für die Integration eines neuen Moduls

Die folgende Tabelle bietet eine Übersicht über die unterstützten Ethernets/IP-Requests für die Objektinstanzen.

Service code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object	DLR
Get Attribute All (0x01)	All attributes	All attributes	All attributes	All attributes	All attributes	All attributes
Set Attribute All (0x02)	-	Settable attributes (3,5,6,8,9,10)	Settable attributes (6,9)	-	-	Settable attributes (4,5)
Get Attribute Single (0x0e)	All attributes	All attributes	All attributes	All attributes	All attributes	All attributes
Set Attribute Single (0x10)	-	Settable attributes (3,5,6,8,9,10,0x64)	Settable attributes (6,9,0x65,0x67,0x68,0x69,6C)	Settable attributes (7)	-	Settable attributes (4,5)
Reset (0x05)	Parameter(0,1)	-	-	-	-	-
Save Configuration (0x35) Vendor specific	-	-	-	Save switch configuration	-	-
Mac Filter(0x36) Vendor Specific	-	-	-	Add mac-filterSTRUCT of:{ USINT VLAN-IDARRAY of 6 USINT MAC DWORD Port Mask}	-	-
Verify Fault Location (0x4B)						Verify Fault Location
Clear Rapid Faults (0x4C)						Clear Rapid Faults

Service code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object	DLR
Restart Sign On (0x4D)						Restart Sign On
Clear Gateway Partial Fault (0x04E)						Clear Gateway Partial Fault

I/O Data	Value (data types and sizes to be defined)	Direction
Device Status	Bitmask (see Switch Agent Attribute 1)	Input, DWORD 32 Bit
Link Status	Bitmask, 1 Bit per port 0 = No link 1 = Link up	Input (DWORD 32 Bit *)
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. 0 = Port enabled 1 = Port disabled	Input (DWORD 32 Bit *)
Utilization Alarm	Bitmask, 1 Bit per port 0 = No alarm 1 = Alarm on port	Input (DWORD 32 Bit *)
Access Violation Alarm	Bitmask, 1 Bit per port 0 = No alarm 1 = Alarm on port	Input (DWORD 32 Bit *)
Multicast Connections	Integer, number of connections	Input (1 DINT 32 Bit)
TCP/IP Connections	Integer, number of connections	Input (1 DINT 32 Bit)
Quick Connect Mask	Bitmask (1 Bit per port) 0 = Quick Connect is disabled 1 = Quick Connect is enabled	Input (1 DINT 32 Bit *)
Link Admin State	Bitmask, 1 Bit per port 0 = Port enabled 1 = Port disabled	Output, DWORDa

■ Mapping von Ethernet-Verbindungsobjektinstanzen

Die Tabelle zeigt die Zuweisung der Ports zu den Ethernet-Verbindungsobjektinstanzen.

Ethernet Port	Ethernet Link Object Instance
CPU	1
1	2
2	3
3	4
4	5
...	...

Die Anzahl der Ports ist von der verwendeten Hardware abhängig. Das Ethernet-Verbindungsobjekt existiert nur, wenn der Port angeschlossen ist.

15.4 PROFINET

PROFINET ist ein weltweit akzeptiertes industrielles Kommunikationsnetz auf Basis von Ethernet. Es baut auf den weit verbreiteten Transportprotokollen TCP/IP und UDP/IP (Standard) auf. Dies ist ein wichtiger Aspekt, um die Anforderungen an die Konsistenz von der Management-Ebene bis in die Feldebene zu erfüllen.

PROFINET ergänzt die bewährte Profibus-Technologie für solche Anwendungen, die eine schnelle Datenkommunikation und die Nutzung industrieller IT-Funktionen erfordern.

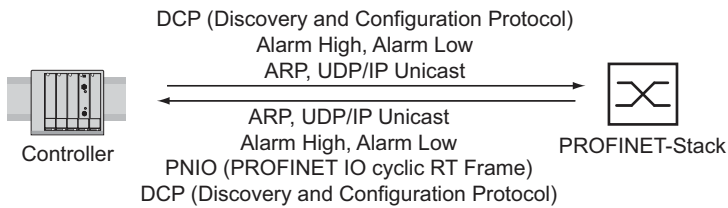


Abb. 57: Kommunikation zwischen Controller und dem Gerät

PROFINET treffen Sie insbesondere in Europa und im Umfeld von Siemens-Steuerungen an. **PROFINET** benutzt die Gerätebeschreibungssprache GSDML (Generic Station Description Markup Language, auf XML basierend), um Geräte und deren Eigenschaften maschinell verarbeitbar zu beschreiben. Die Gerätebeschreibung finden Sie in der GSD(ML)-Datei des Gerätes.

Ausführliche Informationen zu **PROFINET** finden Sie auf der Internetseite der PROFIBUS-Organisation unter <http://www.profibus.com>.

Die Geräte sind konform zur Konformitätsklasse Class B bei **PROFINET**.

■ Gerätemodelle für PROFINET GSDML Version 2.3

Das Gerät erzeugt GSDML-Dateien im Format GSDML V.2.3. In der GSDML-Datei ist das Gerät gemäß GSDML-Norm V.2.2 modelliert.

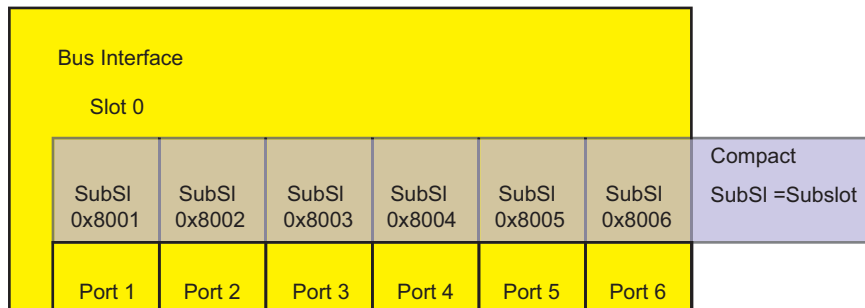


Abb. 58: Kompaktes Gerät

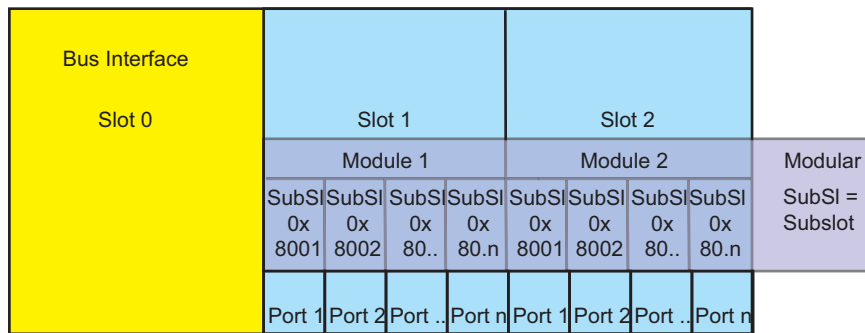


Abb. 59: Modulares Gerät

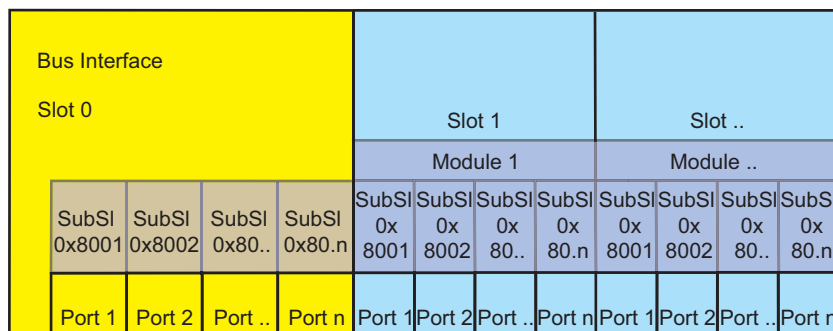


Abb. 60: Kombigerät

■ Grafische Benutzeroberfläche und CLI

In *PROFINET*-Umgebungen stellt der Automationsprozess eine Anwendungsrelation (AR) zu dem Gerät her, wenn das Gerät erfolgreich eingerichtet wurde.

Nach der Anmeldung eines Benutzers zeigt das Gerät über die grafische Benutzeroberfläche und das CLI eine entsprechende Meldung an.

15.4.1 Integration in ein Steuerungssystem

■ Gerät vorbereiten

Nach Installation, Verbindung und Konfiguration des Geräts führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > System*.
- Vergewissern Sie sich, dass im Feld *Systemname* ein gültiger Name für das Gerät festgelegt ist.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Grundeinstellungen > Netz*.
- Wählen Sie im Rahmen *Management-Schnittstelle* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Switching > Switching Global* und markieren Sie das Kontrollkästchen *VLAN-Unaware-Modus*.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarten *Global* und *Port*.
- Konfigurieren Sie die Alarmeinrichtung und den Schwellwert für die Alarme, die Sie überwachen wollen.
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
- Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > PROFINET*.
- Laden Sie die GSD(ML)-Datei zusammen mit dem Symbol auf Ihren lokalen Rechner.
Um die GSD(ML)-Datei und das Symbol abzurufen, gehen Sie folgendermaßen vor:
 - Laden Sie die Datei aus dem Dialog *Erweitert > Industrie-Protokolle > PROFINET* herunter.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

■ Ändern voreingestellter Werte

Funktionen mit direktem Einfluss auf die *PROFINET*-Funktion erfordern das Ändern folgender voreingestellter Werte. Wenn Sie das Gerät in einer speziell erhältlichen *PROFINET*-Variante erworben haben, sind diese Werte bereits voreingestellt:

PROFINET	Dialog <i>Erweitert > Industrie-Protokolle > PROFINET</i> <ul style="list-style-type: none">- <i>Funktion</i> = An- <i>Stationsname</i> = <leer>
Netz	Dialog <i>Grundeinstellungen > Netz</i> <ul style="list-style-type: none">- <i>Zuweisung IP-Adresse</i> = Lokal- <i>Zugriff</i> = readOnly- <i>IP-Adresse</i> = 0.0.0.0- <i>Netzmaske</i> = 0.0.0.0- <i>Gateway-Adresse</i> = 0.0.0.0
VLAN	Dialog <i>Switching > Global</i> <ul style="list-style-type: none">- <i>VLAN-Unaware-Modus</i> = markiert
LLDP	Dialog <i>Diagnose > LLDP</i> <ul style="list-style-type: none">- <i>Sende-Intervall [s]</i> = 5- <i>Sende-Verzögerung [s]</i> = 1

■ Konfiguration der SPS

Die folgende Ausführung bezieht sich auf die Konfiguration der SPS am Beispiel der Software Simatic S7 von Siemens und setzt voraus, dass Sie mit der Bedienung der Software vertraut sind. Das Gerät unterstützt auch Engineering-Stationen anderer Hersteller, wie PC Worx von Phönix.

In der Voreinstellung der SPS erkennt die SPS die Unterbrechung der I/O-Verbindung zum Gerät als Fehler. Die SPS betrachtet 3 Echtzeitpakete, die nacheinander in der SPS oder im Gerät fehlen, als Unterbrechung. Dies führt laut Voreinstellung zum Anlagenausfall. Um diese Voreinstellung zu ändern, führen Sie Step7-Programmierungsmaßnahmen durch.

Anmerkung: Die Überwachung der I/O-Verbindung zur CPU als Ausfallkriterium kann zum Anlagenausfall führen. Daher ist die Überwachung der I/O-Verbindung als Ausfallkriterium weniger geeignet.

Die I/O-Verbindung zwischen der speicherprogrammierbaren Steuerung (SPS) und dem Gerät kann durch ein Management-Programm unterbrochen werden. Beispielsweise kann eine Netzmanagementstation die CPU des Gerätes mit Echtzeitdaten (RT-Daten) mit einer höheren Priorität auslasten. In diesem Fall kann das Gerät weiterhin Datenpakete senden oder empfangen, und das System bleibt betriebsbereit.

■ GDSML-Datei bereitstellen

Zum Erzeugen von GDSML-Dateien und der Symbole bietet Ihnen das Hirschmann-Gerät folgende Möglichkeiten:

- ▶ Sie können die grafische Benutzeroberfläche im Dialog *Erweitert > Industrie-Protokolle > PROFINET* verwenden, um die GSDML-Datei und das Symbol des Gerätes herunterzuladen.

■ Gerät in die Konfiguration aufnehmen

- Öffnen Sie die Anwendung *Simatic Manager* über Simatic S7.
- Öffnen Sie Ihr Projekt.
- Wechseln Sie in die Hardware-Konfiguration.
- Installieren Sie die GSD(ML)-Datei:

Klicken Sie in der Menüleiste *Extras > GSD-Dateien installieren...*

Wählen Sie die zuvor auf Ihrem PC gespeicherte GSD-Datei aus.

Simatic S7 installiert die Datei zusammen mit dem Symbol.

Sie finden das neue Gerät unter:

PROFINET IO > Weitere FELDGERÄTE > Schaltgeräte > Hirschmann..

oder unter

PROFINET IO > Weitere FELDGERÄTE > Network Components > Hirschmann..

- Ziehen Sie das Gerät per Drag-and-Drop auf das Buskabel.

Um das Gerät umzubenennen, führen Sie die folgenden Schritte aus:

- Markieren Sie das Gerät.
- Klicken Sie in der Menüleiste *PLC > Ethernet > Edit Ethernet Node*.
- Fügen Sie im Dialog *Ethernet-Teilnehmer bearbeiten*, Rahmen *Gerätename vergeben* den Namen des Geräts in Feld *Gerätename* ein.
- Klicken Sie die Schaltfläche *Durchsuchen...*
Wählen Sie das Gerät.
Klicken Sie die Schaltfläche *OK*.
- Legen Sie den Namen des Geräts fest.
Klicken Sie die Schaltfläche *Name zuweisen*.
- Klicken Sie die Schaltfläche *Schließen*.

- Rechtsklicken Sie in der Hardware-Konfiguration das Gerät und wählen Sie in der Dropdown-Liste *Objekteigenschaften*.
- Fügen Sie denselben Namen ein, der im Dialog *Ethernet-Teilnehmer bearbeiten* angegeben ist.
- Klicken Sie die Schaltfläche *Ethernet*.
Fügen Sie die IP-Parameter ein.
Um das Fenster *Properties - Ethernet interface...* zu schließen, klicken Sie die Schaltfläche *OK*.
- Um das Fenster *Properties* zu schließen, klicken Sie die Schaltfläche *OK*.

Das Gerät wurde in die Konfiguration aufgenommen.

IO-Zyklus konfigurieren

- Klicken Sie das Gerät in der Hardware-Konfiguration.
- Rechtsklicken Sie im Dialog *Steckplatz/Baugruppe Ansicht* die Zeile X1 //PN-IO.
- Wählen Sie in der Dropdown-Liste *Objekteigenschaften* aus.
- Öffnen Sie im Fenster *Eigenschaften* die Registerkarte *IO-Zyklus*.
- Wählen Sie im Rahmen *Aktualisierungszeit*, Feld *Aktualisierungszeit[ms]*, die erforderliche Aktualisierungszeit in ms für den IO-Zyklus aus.
- Wählen Sie im Rahmen *Ansprechüberwachungszeit*, Feld *Anzahl akzeptierter Aktualisierungszyklen mit fehlenden IO Daten*, die erforderliche Anzahl für den I/O-Zyklus aus.
- Um das Fenster *Eigenschaften* zu schließen, klicken Sie die Schaltfläche *OK*.

Medienredundanz konfigurieren

- Linksklicken Sie das Gerät in der Hardware-Konfigurationen.
- Rechtsklicken Sie im Dialog *Steckplatz/Baugruppe Ansicht* die Zeile X1 //PN-IO.
- Wählen Sie in der Dropdown-Liste *Objekteigenschaften* aus.
- Öffnen Sie im Fenster *Eigenschaften* die Registerkarte *Medienredundanz*.
- Wählen Sie im Rahmen *MRP-Konfiguration*, Feld *Domain*, die erforderliche MRP-Domäne für den Knoten.
- Wählen Sie im Rahmen *MRP-Konfiguration* im Feld *Rolle* die erforderliche Rolle des Knotens im Ring.
- Wählen Sie in den Feldern *Ringport 1* und *Ringport 2* die aktiven MRP-Ring-Ports aus.
- Um das Fenster *Eigenschaften* zu schließen, klicken Sie die Schaltfläche *OK*.

■ Module für modulare Geräte hinzufügen

- Ziehen Sie per Drag-and-Drop ein Modul aus der Bibliothek zu einem Steckplatz (Slot).
Simatic S7 fügt die Ports über die Moduleigenschaften hinzu.

■ **Geräteeigenschaft konfigurieren**

In Steckplatz 0 fügen Sie die Einstellungen für das gesamte Gerät ein.

- Wählen Sie das Gerät.
- Rechtsklicken Sie Steckplatz 0.
Um das gesamte Gerät zu konfigurieren, wählen Sie *Objekteigenschaften*.
- Öffnen Sie im Fenster *Eigenschaften* die Registerkarte *Parameter*.

■ **Port-Eigenschaften konfigurieren**

Bei den modularen Geräten stellen die Steckplätze 1 bis n die Module dar. Die Ports werden als Untersteckplätze/Untermodule dargestellt.

Bei den nichtmodularen Geräten stellen die Untersteckplätze 1 bis n in Steckplatz 0 die Ports dar.

Port-Alarme konfigurieren

- Rechtsklicken Sie einen Port, 1 bis n, und wählen Sie *Objekteigenschaften*.
- Öffnen Sie im Fenster *Eigenschaften* die Registerkarte *Parameter*.
- Wählen Sie die gewünschten Alarme und schließen Sie das Fenster.

Sonderfall: „LinkDown“-Alarm:

Der LinkDown-Alarm setzt sich zusammen aus der UND-Verknüpfung

- des Hirschmann-spezifischen Status für Verbindungsfehler und
- der Simatic S7-spezifischen Option für die Verbindung.

Aktivierung des LinkDown-Alarms:

- Öffnen Sie im Dialog *Eigenschaften* die Registerkarte *Parameter* (Hirschmann-spezifisch).
- Um den Parameter *Alarme* einzuschalten, wählen Sie in Spalte *Wert* den Wert *On*.
- Schalten Sie den Parameter *Überwachung Linkstatus* ein und wählen Sie in der Spalte *Wert* die Option *Generate diagnosis alarm when link goes down*.
- Öffnen Sie die Registerkarte *Optionen*.
- Um die Link-Überwachung zu aktivieren, wählen Sie eine feste Einstellung für den Port im Rahmen *Verbindung*, Feld *Übertragungsmedium/Duplex*.

■ **Verbindungs-Optionen konfigurieren**

- Rechtsklicken Sie einen Port, 1 bis n, und wählen Sie *Objekteigenschaften*.
- Öffnen Sie im Dialog *Eigenschaften* die Registerkarte *Optionen*.
- Wählen Sie im Rahmen *Verbindung*, Feld *Übertragungsmedium/Duplex*, die gewünschte Einstellung für den Port.
- Um das Fenster *Eigenschaften* zu schließen, klicken Sie die Schaltfläche *OK*.

Wenn Sie die Port-Einstellung in einen anderen Wert als *Automatic settings* ändern, schaltet das Gerät den Port über einen kurzen Zeitraum aus. Befindet sich der Port auf einem Pfad zwischen dem I/O-Controller und dem I/O-Gerät, kann die Unterbrechung unter Umständen zu einem Fehler bei der Herstellung einer Application Relation führen. Treffen Sie die folgenden Vorkehrungen, bevor Sie die Port-Einstellung ändern:

Anmerkung: Achten Sie auf Schleifen. Deaktivieren Sie das Rapid-Spanning-Tree-Protokoll (RSTP) an den Geräteports zwischen dem I/O-Controller und dem I/O-Gerät.

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Spanning Tree Port*, Registerkarte *CIST*.
- Entfernen Sie die Markierung im Kontrollkästchen *STP aktiv* für die betreffenden Ports.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

Topologie konfigurieren

- Rechtsklicken Sie einen Port, 1 bis n, und wählen Sie *Objekteigenschaften*.
- Öffnen Sie im Dialog *Eigenschaften* die Registerkarte *Topologie*.
- Wählen Sie im Rahmen *Partner*, Feld *Partner-Port*, die gewünschte Einstellung für den Partner-Port.
- Um das Fenster *Eigenschaften* zu schließen, klicken Sie die Schaltfläche *OK*.

■ Tauschen von Geräten

Hirschmann-Geräte unterstützen die Funktion des Gerätetausches mit einer Engineering-Station. Beim Tauschen gleicher Geräte weist die Engineering-Station dem Austauschgerät die Parameter des ursprünglichen Gerätes zu.

Die Funktion des Gerätetausches mit Simatic S7 erfordert folgende Voraussetzungen:

- ▶ S7 300 mit SW Stand ab V2.7 (z.Zt. für CPU 319 verfügbar) oder S7 400 mit SW Stand ab V5.2
- ▶ Hirschmann-Gerät mit SW Release ab 05.0.00
- ▶ Nachbargerät(e) unterstützen LLDP
- ▶ Topologie (=Nachbarschaftsbeziehungen) ist konfiguriert und auf SPS geladen

Der Gerätetausch erfordert folgende Voraussetzungen:

- ▶ Das Ersatzgerät ist genau vom gleichen Typ wie das zu ersetzende Gerät.
- ▶ Das Ersatzgerät ist genau an der gleichen Stelle im Netz (gleiche Ports und Nachbargeräte) angeschlossen.
- ▶ Das Ersatzgerät verfügt über eine *PROFINET*-Standardkonfiguration. Setzen Sie den Gerätenamen auf "" (Null-String).

Wenn alle diese Voraussetzungen erfüllt sind, weist die Netzmanagementstation dem Ersatzgerät automatisch die Parameter des ursprünglichen Gerätes (Gerätename, IP-Parameter und Konfigurationsdaten) zu.

Vorgehensweise beim Gerätetausch:

- Systemname "" (= Null-String)
 - IP-Adresse = 0.0.0.0 oder DHCP
 - *PROFINET* aktiviert
- Notieren Sie sich die Port-Belegung des ursprünglichen Gerätes, und entfernen Sie das ursprüngliche Gerät aus dem System.
Daraufhin erkennt die SPS einen Fehler.
- Setzen Sie das Ersatzgerät nun an der gleichen Stelle im Netz wieder ein. Vergewissern Sie sich, dass die Port-Belegung der des ursprünglichen Gerätes entspricht.

Die SPS findet das Ersatzgerät und konfiguriert es wie das ursprüngliche Gerät.

Die SPS erkennt den ordnungsgemäßen Betrieb.

Setzen Sie gegebenenfalls die SPS wieder auf „Run“.

■ Module tauschen

Der *PROFINET*-Stack im Gerät erkennt eine Änderung der angeschlossenen Module und meldet die Änderung an die Netzmanagementstation. Wenn ein zuvor konfiguriertes Modul aus dem Gerät entfernt wird, meldet die Netzmanagementstation einen Fehler. Wenn ein konfiguriertes Modul, das gefehlt hat, angeschlossen wird, beseitigt die Netzmanagementstation die Fehlermeldung.

■ **Topologie-Erkennung**

Nach der Initiierung der Topologie-Erkennung durch den Anwender sucht die Netzmanagementstation nach angeschlossenen Geräten.

■ **Projektierung der Topologie**

Simatic S7 bietet dem Anwender die Möglichkeit, die Topologie zu konfigurieren und entsprechend zu überwachen.

Simatic S7 stellt Verbindungsparameter (Qualität und Einstellungen) in einer farbigen Grafik dar.

■ **Kommunikationsdiagnose**

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

■ **Portstatistiken ausgeben**

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

15.4.2 PROFINET-Parameter

■ Alarme

Das Gerät unterstützt Alarme auf Geräte- und Port-Ebene.

Alarme auf Geräteebene	Änderung des Gerätestatus Ausfall der redundanten Spannungsversorgung Ausfall/Entfernen des ACA
Alarme auf Port-Ebene	Änderung des Link-Status Überschreiten einer vorgegebenen Übertragungsrate.

Tab. 36: Unterstützte Alarme

■ Record-Parameter

Das Gerät bietet Datensätze für:

- ▶ Geräte-Parameter
- ▶ Gerätestatus
- ▶ Port-Status/Port-Parameter

Byte	Content	Access	Value	Meaning
0	Send alarm if status changes	rw	0	Do not send alarm
			1	Send alarm if one of the following alarm reasons occurs.
1	Power Alarm	rw	0	Do not send alarm
			1	Send alarm if a power supply fails.
2	ACA Alarm	rw	0	Do not send alarm
			1	Send alarm if the ACA is removed.
3	Module Alarm	rw	0	Do not send alarm
			1	Send alarm if the module connections are changed.

Tab. 37: Geräte-Parameter

Byte	Content	Access	Value	Meaning
0	Device status	ro	0	Unavailable
			1	OK
			2	Error
1	Power supply unit 1	ro	0	Unavailable
			1	OK
			2	Error
2	Power supply unit 2	ro	0	Unavailable
			1	OK
			2	Error
3	Power supply unit 3	ro	0	Unavailable
			1	OK
			2	Error
4	Power supply unit 4	ro	0	Unavailable
			1	OK
			2	Error
5	Power supply unit 5	ro	0	Unavailable
			1	OK
			2	Error
6	Power supply unit 6	ro	0	Unavailable
			1	OK
			2	Error

Tab. 38: Gerätestatus

Byte	Content	Access	Value	Meaning
7	Power supply unit 7	ro	0	Unavailable
			1	OK
			2	Error
8	Power supply unit 8	ro	0	Unavailable
			1	OK
			2	Error
9	Signal contact 1	ro	0	Unavailable
			1	Closed
			2	Open
10	Signal contact 2	ro	0	Unavailable
			1	Closed
			2	Open
11	Temperature	ro	0	Unavailable
			1	OK
			2	Threshold value for temperature exceeded or not reached
12	Fan	ro	0	Unavailable
			1	OK
			2	Fan failure
13	Module removal	ro	0	Unavailable
			1	OK
			2	A module has been removed.
14	ACA Removed	ro	0	Unavailable
			1	OK
			2	The ACA has been removed.
15	Not used		0	
			1	
			2	
16	Not used		0	
			1	
			2	
17	Connection	ro	0	Unavailable
			1	OK
			2	Connection failure.

Tab. 38: Gerätestatus

Byte	Content	Access	Value	Meaning
0	Report port error	rw	0	Do not send alarm
			1	Send alarm if one of the following alarm reasons occurs.
1	Report connection error	rw	0	Do not send alarm
			1	Send alarm if the connection has failed.
2	Transmission rate too high	rw	0	Do not send alarm
			1	Send alarm if the threshold value for the temperature has been exceeded.
3	Port on	rw	0	Unavailable
			1	Switched on
			2	Switched off
4	Link status	ro	0	Unavailable
			1	Connection exists
			2	Connection interrupted
5	Bit rate	ro	0	Unavailable
			1	Unknown
			2	10 MBit/s
			2	100 MBit/s
			2	1000 MBit/s
6	Duplex	ro	0	Half duplex
			1	Full duplex
			2	Full duplex
7	Autonegotiation	ro	0	Unavailable
			1	off
			2	on

Tab. 39: Port-Status/Port-Parameter

■ I/O Data

Die Zuweisung der Bits der übertragenen I/O-Daten entnehmen Sie der folgenden Tabelle.

Direction	Byte	Bit	Meaning
Input	0		General
		0	Device status
		1	Signal contact 1
		2	Signal contact 2
		3	Temperature
		4	Fan
		5	Module removal
		6	ACA Removed
	7	Not used	
Input	1		Power supply status
		0	Power supply unit 1
		1	Power supply unit 2
		2	Power supply unit 3
		3	Power supply unit 4
		4	Power supply unit 5
		5	Power supply unit 6
		6	Power supply unit 7
	7	Power supply unit 8	
Input	2		Supply voltage status
		0	Not used
		1	Not used
		2	Connection error
		3	Not used
		4	Not used
		5	Not used
		6	Not used
	7	Not used	
Output			Not defined

Meaning of the bit content:
0: OK or unavailable
1: Reason for report exists

Tab. 40: Geräte-I/O-Daten

Direction	Byte	Bit	Meaning
Input	0		Connection status for ports 1 to 8
		0	Port 1
		1	Port 2
		2	Port 3
		3	Port 4
		4	Port 5
		5	Port 6
		6	Port 7
	7	Port 8	
Input	1		Connection status for ports 9 to 16
		0	Port 9
		1	Port 10
		2	Port 11
		3	Port 12
		4	Port 13
		5	Port 14
		6	Port 15
	7	Port 16	

Tab. 41: Port-I/O-Daten

Direction	Byte	Bit	Meaning
Input	n		Connection for port (n * 8) + 1 to port (n * 8) + 8
		0	Port (n * 8) + 1
		1	Port (n * 8) + 2
		2	Port (n * 8) + 3
		3	Port (n * 8) + 4
		4	Port (n * 8) + 5
		5	Port (n * 8) + 6
		6	Port (n * 8) + 7
	7	Port (n * 8) + 8	
Means the Input Bit contains:			
– 0: no connection			
– 1: active connection			
Output	0		"Port activated" for ports 1 to 8
		0	Port 1 activated
		1	Port 2 activated
		2	Port 3 activated
		3	Port 4 activated
		4	Port 5 activated
		5	Port 6 activated
		6	Port 7 activated
	7	Port 8 activated	
Output	1		"Port activated" for ports 9 to 16
		0	Port 9 activated
		1	Port 10 activated
		2	Port 11 activated
		3	Port 12 activated
		4	Port 13 activated
		5	Port 14 activated
		6	Port 15 activated
	7	Port 16 activated	
Output	n		"Port activated" for port (n * 8) + 1 to port (n * 8) + 8
		0	Port (n * 8) + 1 activated
		1	Port (n * 8) + 2 activated
		2	Port (n * 8) + 3 activated
		3	Port (n * 8) + 4 activated
		4	Port (n * 8) + 5 activated
		5	Port (n * 8) + 6 activated
		6	Port (n * 8) + 7 activated
	7	Port (n * 8) + 8 activated	

Means the Output Bit contains:

- 0: no port active
- 1: active active

Tab. 41: Port-I/O-Daten

A Konfigurationsumgebung einrichten

A.1 DHCP/BOOTP-Server einrichten

Das folgende Beispiel beschreibt die Konfiguration eines DHCP-Servers mit Hilfe der Software haneWIN DHCP Server. Diese Shareware-Software ist ein Produkt von IT-Consulting Dr. Herbert Hanewinkel. Sie können die Software von <https://www.hanewin.net> herunterladen. Sie können die Software bis zu 30 Kalendertage nach dem Datum der ersten Installation testen, um zu entscheiden, ob Sie eine Lizenz erwerben wollen.

- Zur Installation des DHCP-Servers auf Ihrem PC legen Sie die Produkt-CD in das CD-Laufwerk Ihres PCs und wählen Sie unter Zusatzsoftware *haneWIN DHCP-Server*. Führen Sie die Installation gemäß des Installationsassistenten durch.
- Starten Sie das Programm *haneWIN DHCP-Server*.

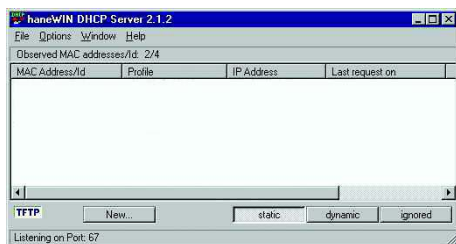


Abb. 61: Startfenster des Programms *haneWIN DHCP-Server*

Anmerkung: Die Installation beinhaltet einen Dienst, der in der Grundkonfiguration automatisch beim Einschalten von Windows gestartet wird. Dieser Dienst ist auch aktiv, wenn das Programm selbst nicht gestartet ist. Der gestartete Dienst beantwortet DHCP-Anfragen.

- Öffnen Sie das Fenster für die Programmeinstellungen im Menü *Optionen > Einstellungen* und wählen Sie die Registerkarte *DHCP*.
- Legen Sie die in der Abbildung dargestellten Einstellungen fest.
- Klicken Sie die Schaltfläche *OK*.

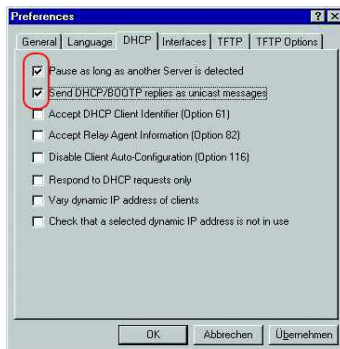


Abb. 62: DHCP-Einstellung

- Zur Eingabe der Konfigurationsprofile wählen Sie im Menü *Optionen > Konfigurationsprofile verwalten*.
- Legen Sie den Namen für das neue Konfigurationsprofil fest.
- Klicken Sie die Schaltfläche *Hinzufügen*.

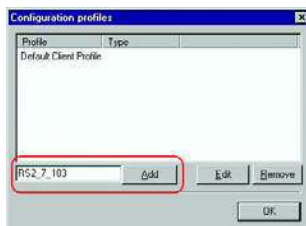


Abb. 63: Konfigurationsprofile hinzufügen

- Legen Sie die Netzmaske fest.
- Klicken Sie die Schaltfläche *Übernehmen*.

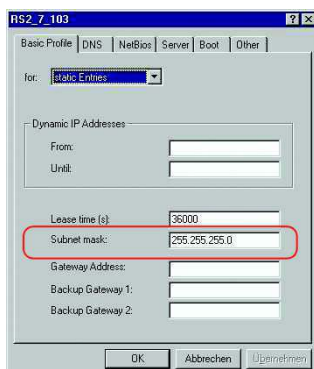


Abb. 64: Netzmaske im Konfigurationsprofil

- Wählen Sie die Registerkarte *Boot*.
- Geben Sie die IP-Adresse Ihres tftp-Servers.

Konfigurationsumgebung einrichten

A.1 DHCP/BOOTP-Server einrichten

- Geben Sie den Pfad und den Dateinamen für die Konfigurationsdatei ein.
- Klicken Sie die Schaltfläche *übernehmen* und dann den Eintrag *OK*.

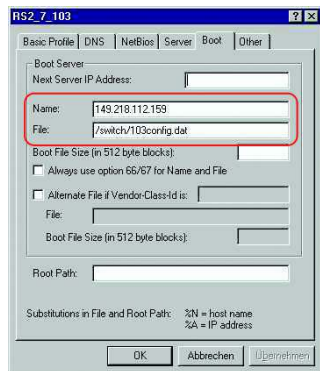


Abb. 65: Konfigurationsdatei auf dem tftp-Server

- Fügen Sie für jeden Gerätetyp ein Profil hinzu.
Haben Geräte des gleichen Typs unterschiedliche Konfigurationen, dann fügen Sie für jede Konfiguration ein Profil hinzu.
- Zum Beenden des Hinzufügens der Konfigurationsprofile klicken Sie die Schaltfläche *OK*.

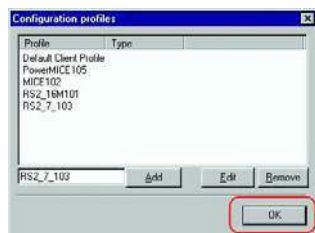


Abb. 66: Konfigurationsprofile verwalten

- Zur Eingabe der statischen Adressen klicken Sie im Hauptfenster die Schaltfläche *Statisch*.



Abb. 67: Statische Adresseingabe

- Klicken Sie die Schaltfläche *Hinzufügen*.

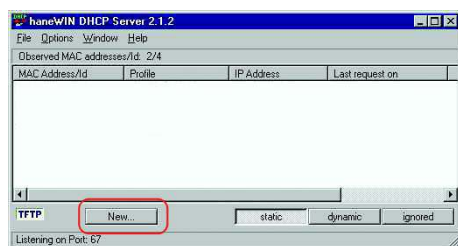


Abb. 68: Statische Adressen hinzufügen

- Geben Sie die MAC-Adresse des Gerätes ein.
- Geben Sie die IP-Adresse des Gerätes ein.

- Wählen Sie das Konfigurationsprofil des Gerätes.
- Klicken Sie die Schaltfläche *übernehmen* und dann den Eintrag *OK*.

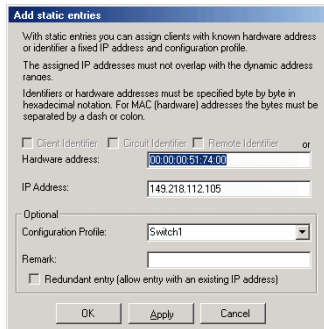


Abb. 69: Einträge für statische Adressen

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

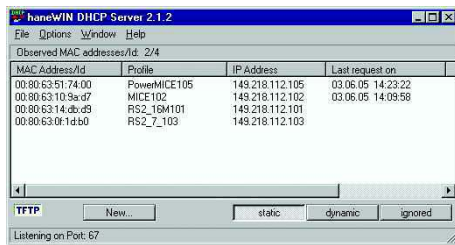


Abb. 70: DHCP-Server mit Einträgen

A.2 DHCP-Server Option 82 einrichten

Das folgende Beispiel beschreibt die Konfiguration eines DHCP-Servers mit Hilfe der Software haneWIN DHCP Server. Diese Shareware-Software ist ein Produkt von IT-Consulting Dr. Herbert Hanewinkel. Sie können die Software von <https://www.hanewin.net> herunterladen. Sie können die Software bis zu 30 Kalendertage nach dem Datum der ersten Installation testen, um zu entscheiden, ob Sie eine Lizenz erwerben wollen.

- Zur Installation des DHCP-Servers auf Ihrem PC legen Sie die Produkt-CD in das CD-Laufwerk Ihres PCs und wählen Sie unter Zusatzsoftware *haneWIN DHCP-Server*. Führen Sie die Installation gemäß des Installationsassistenten durch.
- Starten Sie das Programm *haneWIN DHCP-Server*.



Abb. 71: Startfenster des Programms *haneWIN DHCP-Server*

Anmerkung: Die Installation beinhaltet einen Dienst, der in der Grundkonfiguration automatisch beim Einschalten von Windows gestartet wird. Dieser Dienst ist auch aktiv, wenn das Programm selbst nicht gestartet ist. Der gestartete Dienst beantwortet DHCP-Anfragen.

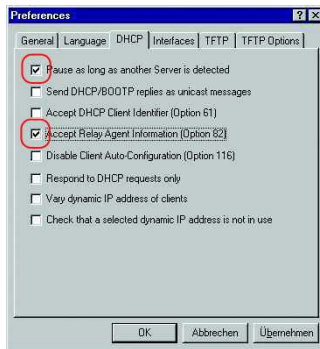


Abb. 72: DHCP-Einstellung

- Zur Eingabe der statischen Adressen klicken Sie die Schaltfläche *Hinzufügen*.

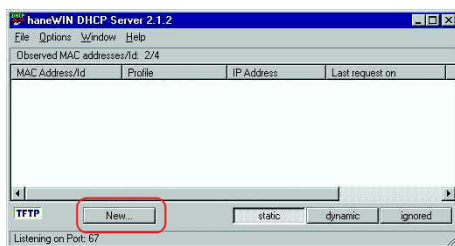


Abb. 73: Statische Adressen hinzufügen

- Markieren Sie das Kontrollkästchen *Circuit Identifier*.
- Markieren Sie das Kontrollkästchen *Remote Identifier*.

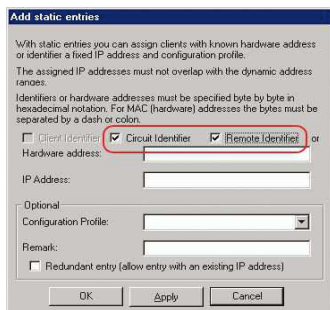


Abb. 74: Voreinstellung für die feste Adresszuweisung

- Legen Sie im Feld *Hardwareadresse* den Wert *Circuit Identifier* und den Wert *Remote Identifier* für Switch und Port fest.
Der DHCP-Server weist dem Gerät, das Sie an den im Feld *Hardwareadresse* festgelegten Port anschließen, die im Feld *IP-Adresse* festgelegte IP-Adresse zu.

Die Hardwareadresse hat folgende Form:

ci cl hh vvvv ssmpprirlxxxxxxxxxxxx

- ▶ ci
Subidentifizier für den Typ der Circuit-ID.
- ▶ cl
Länge der Circuit-ID.
- ▶ hh
Hirschmann-Identifizier:
01, wenn an den Port ein Hirschmann-Gerät angeschlossen wird, sonst 00.
- ▶ vvvv
VLAN-ID der DHCP-Anfrage.
Voreinstellung: 0001 = VLAN 1

- ▶ `ss`
Steckplatz im Gerät, auf dem sich das Modul mit dem Port befindet, an dem das Gerät angeschlossen wird. Legen Sie den Wert `00` fest.
- ▶ `mm`
Modul mit dem Port, an dem das Gerät angeschlossen wird.
- ▶ `pp`
Port, an dem das Gerät angeschlossen wird.
- ▶ `ri`
Subidentifizierer für den Typ der Remote-ID.
- ▶ `rl`
Länge der Remote-ID.
- ▶ `xxxxxxxxxxxx`
Remote-ID des Gerätes (zum Beispiel MAC-Adresse), an dem ein Gerät angeschlossen wird.



Abb. 75: Festlegen der Adressen

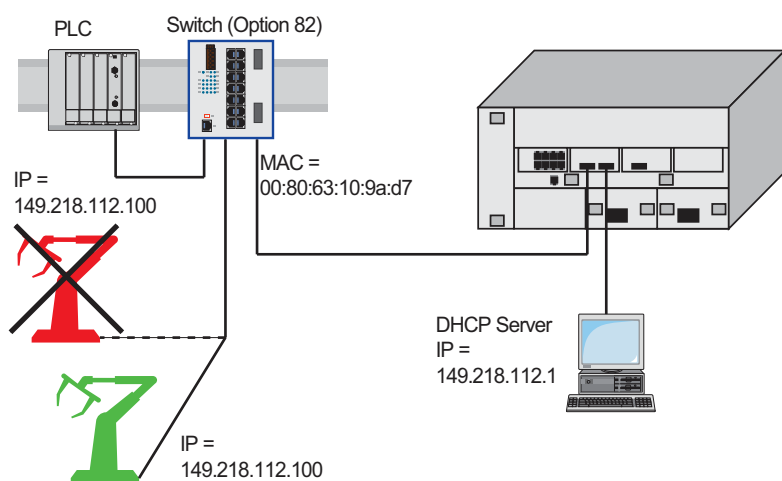


Abb. 76: Anwendungsbeispiel für den Einsatz von Option 82

A.3 MAC-Adresse ändern

Das Gerät bietet Ihnen die Möglichkeit, anstatt der „eingebrennten“ MAC-Adresse eine benutzerdefinierte MAC-Adresse zu verwenden. Die benutzerdefinierte MAC-Adresse:

- ▶ kann mittels CLI oder über die Benutzeroberfläche konfiguriert werden;
- ▶ wird im internen Boot-Parameter-Block gespeichert;
- ▶ wird während der Boot-Phase abgerufen.

Die benutzerdefinierte MAC-Adresse wird entweder über das Web-Interface oder mittels CLI konfiguriert.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen* > *Netz*, Registerkarte *MAC-Konfiguration*.
- Legen Sie im Rahmen *Konfiguration*, Feld *Lokale Administrator-MAC-Adresse* die benutzerdefinierte MAC-Adresse fest.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

Das Gerät übernimmt die Änderung nach einem Neustart.

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
network management mac <local-addr>	Konfigurieren der lokal verwalteten MAC-Adresse
show network management mac	Anzeige der MAC-Adresseinstellungen des Gerätes

Anmerkung: Bei Änderungen an der MAC-Adresse ist ein Neustart des Gerätes erforderlich, damit die geänderte Adresse zugewiesen wird.

A.4 Management-Port festlegen

Sie können das Gerät so konfigurieren, dass der Zugriff auf das Management des Gerätes auf einen Port beschränkt oder über jeden Port möglich ist.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Netz*, Registerkarte *MAC-Konfiguration*.
- Um den Zugriff auf das Management des Gerätes über genau einen Port zu ermöglichen, legen Sie im Rahmen *Konfiguration*, Feld *Management-Port* den zu verwendenden Port fest.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

`network management port <port>`

`show network management port`

Legt die Ports fest, die Zugriff auf das Management des Geräts erhalten. Der Wert `all` erlaubt jedem Port den Zugriff.

Anzeigen der Ports, über die Zugriff auf das Management des Gerätes möglich ist

A.5 SSH-Zugriff vorbereiten

Um über SSH auf das Gerät zuzugreifen, führen Sie die folgenden Schritte aus:

- ▶ Erzeugen Sie einen Schlüssel auf dem Gerät.
oder
- ▶ Laden Sie einen eigenen Schlüssel auf das Gerät.
- ▶ Bereiten Sie den Zugriff auf das Gerät im SSH-Client-Programm vor.

Anmerkung: In der Voreinstellung ist der Schlüssel bereits vorhanden und der SSH-Zugriff freigegeben.

A.5.1 Schlüssel auf dem Gerät erzeugen

Das Gerät bietet Ihnen die Möglichkeit, einen Schlüssel direkt auf dem Gerät zu erzeugen.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- Schalten Sie den SSH-Server aus.
Um die Funktion auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
- Um einen DSA- oder RSA-Schlüssel zu erzeugen, klicken Sie im Rahmen *Signatur* die Schaltfläche *Erzeugen*.
- Schalten Sie den SSH-Server ein.
Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

enable
configure
ssh key dsa generate

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Erzeugen eines neuen DSA-Schlüssels.


A.5.2 Eigenen Schlüssel in das Gerät laden

Erfahrenen Netzadministratoren bietet OpenSSH die Möglichkeit, einen eigenen Schlüssel zu erzeugen. Zum Erzeugen des Schlüssels fügen Sie auf Ihrem PC die folgenden Kommandos ein:

```
ssh-keygen(.exe) -q -t rsa1 -f rsa1.key -C '' -N ''  
dsaparam -out dsaparam.pem 1024
```

Das Gerät bietet Ihnen die Möglichkeit, einen eigenen Schlüssel in das Gerät zu laden.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
 - Schalten Sie den SSH-Server aus.
Um die Funktion auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
 - Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
 - Befindet sich der Host-Key auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie die Datei, die den Host-Key enthält, in den  -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.
 - Klicken Sie im Rahmen *Key-Import* die Schaltfläche *Start*, um den Schlüssel in das Gerät zu laden.
 - Schalten Sie den SSH-Server ein.
Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
 - Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .
-
- Kopieren Sie den selbst erzeugten Schlüssel von Ihrem PC auf den externen Speicher.
 - Kopieren Sie den Schlüssel vom externen Speicher in das Gerät.

enable

copy sshkey envm <file name>

Wechsel in den Privileged-EXEC-Modus.

Eigenen Schlüssel vom externen Speicher in das Gerät laden.

A.5.3 SSH-Client-Programm vorbereiten

Das Programm *PuTTY* bietet Ihnen die Möglichkeit, auf das Gerät mit SSH zuzugreifen. Dieses Programm finden Sie auf der Produkt-CD.

Führen Sie die folgenden Schritte aus:

- Starten Sie das Programm mit einem Doppelklick.

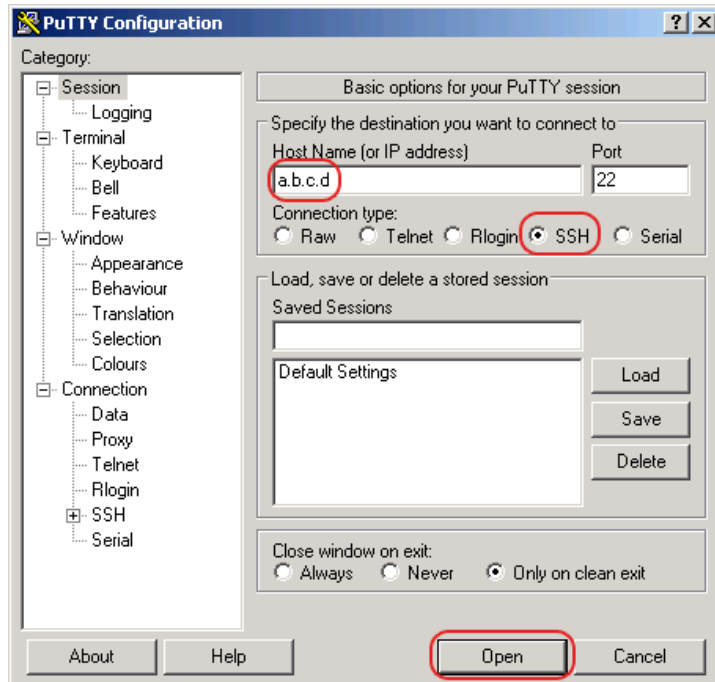


Abb. 77: PuTTY-Eingabemaske

- In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Gerätes ein. Die IP-Adresse (a.b.c.d) besteht aus 4 Dezimalzahlen im Wert von 0 bis 255. Die 4 Dezimalzahlen sind durch einen Punkt getrennt.
- Um den Verbindungstyp auszuwählen, wählen Sie unter *Connection type* das Optionsfeld *SSH*.
- Klicken Sie die Schaltfläche *Open*, um die Datenverbindung zu Ihrem Gerät aufzubauen.

Gegen Ende des Verbindungsaufbaus zeigt das Programm *PuTTY* eine Sicherheitsalarmmeldung an und bietet Ihnen die Möglichkeit, den Fingerabdruck des Schlüssels zu prüfen.



Abb. 78: Sicherheitsabfrage für den Fingerabdruck

- Prüfen Sie den Fingerabdruck des Schlüssels, um sicherzustellen, dass Sie sich tatsächlich mit dem gewünschten Gerät verbunden haben.
- Stimmt der Fingerabdruck mit dem Ihres Schlüssels überein, dann klicken Sie die Schaltfläche *Yes*.

Das Programm *PuTTY* zeigt eine weitere Sicherheitsalarmmeldung zur eingestellten Warnschwelle an.

Erfahrenen Netzadministratoren bietet die OpenSSH-Suite eine weitere Möglichkeit, mittels SSH auf Ihr Gerät zuzugreifen. Zum Einrichten der Datenverbindung fügen Sie das folgende Kommando ein:

```
ssh admin@10.0.112.53
```

`admin` ist der Benutzername.

`10.0.112.53` ist die IP-Adresse Ihres Gerätes.

A.6 HTTPS-Zertifikat

Ihr Web-Browser stellt mit dem HTTPS-Protokoll die Verbindung zum Gerät her. Voraussetzung ist, dass Sie die Funktion *HTTPS server* im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS* einschalten.

Anmerkung: Software von Drittanbietern wie Web-Browser validieren Zertifikate anhand von Kriterien wie Verfallsdatum und aktuellen kryptografischen Parameter-Empfehlungen. Alte Zertifikate können Fehler verursachen, zum Beispiel wenn sie verfallen oder sich kryptographische Empfehlungen ändern. Laden Sie Ihr eigenes, aktuelles Zertifikat hoch oder erzeugen Sie das Zertifikat mit der neuesten Firmware neu, um Validierungskonflikte mit Software von Drittanbietern zu beheben.


A.6.1 HTTPS-Zertifikatsverwaltung

Für die Verschlüsselung ist ein Standardzertifikat nach X.509/PEM (Public-Key-Infrastruktur) erforderlich. In der Voreinstellung befindet sich ein selbst generiertes Zertifikat auf dem Gerät.

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS*.
- Um ein X509/PEM-Zertifikat zu erzeugen, klicken Sie im Rahmen *Zertifikat* die Schaltfläche *Erzeugen*.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .
- Starten Sie den HTTPS-Server neu, um den Schlüssel zu aktivieren. Führen Sie den Neustart des Servers über das Command Line Interface (CLI) durch.

enable	Wechsel in den Privileged-EXEC-Modus.
configure	Wechsel in den Konfigurationsmodus.
https certificate generate	Erzeugen eines HTTPS-Zertifikats (X509/PEM)
no https server	Ausschalten der <i>HTTPS</i> -Funktion.
https server	Einschalten der <i>HTTPS</i> -Funktion.

- Sie haben auch die Möglichkeit, ein extern generiertes Standardzertifikat nach X509/PEM auf das Gerät zu laden:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS*.
- Befindet sich das Zertifikat auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie das Zertifikat in den -Bereich. Alternativ klicken Sie in den Bereich, um das Zertifikat auszuwählen.
- Klicken Sie die Schaltfläche *Start*, um das Zertifikat in das Gerät zu kopieren.
- Um die Änderungen zwischenspeichern, klicken Sie die Schaltfläche .

enable	Wechsel in den Privileged-EXEC-Modus.
copy httpscert envm <file name>	Kopieren des HTTPS-Zertifikats von einem externen nichtflüchtigen Speicher.
configure	Wechsel in den Konfigurationsmodus.

no https server
https server

Ausschalten der *HTTPS*-Funktion.
Einschalten der *HTTPS*-Funktion.

Anmerkung: Wenn Sie ein Zertifikat hochladen oder erzeugen, stellen Sie sicher, dass Sie das Gerät oder den HTTPS-Server neu starten, damit das Zertifikat aktiv wird. Führen Sie den Neustart des Servers über das Command Line Interface (CLI) durch.

A.6.2 Zugang über HTTPS

Die Voreinstellung für HTTPS-Datenverbindungen ist der TCP-Port 443. Wenn Sie die Portnummer ändern, starten Sie anschließend das Gerät oder den HTTPS-Server neu. Damit wird die Änderung wirksam.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld .
- Um über HTTPS auf das Gerät zuzugreifen, geben Sie in Ihrem Browser HTTPS statt HTTP und die IP-Adresse des Gerätes ein.

enable
configure
https port 443

https server
show https

Wechsel in den Privileged-EXEC-Modus.
Wechsel in den Konfigurationsmodus.
Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTPS-Anfragen von den Clients entgegennimmt.
Einschalten der *HTTPS*-Funktion.
Zeigt den Status des *HTTPS*-Servers und die Portnummer.

Wenn Sie die HTTPS-Portnummer ändern, schalten Sie den HTTPS-Server aus- und wieder ein, damit die Änderung wirksam wird.

Das Gerät verwendet das HTTPS-Protokoll und baut eine neue Datenverbindung auf. Am Ende der Sitzung, nach dem Logout des Users, beendet das Gerät die Datenverbindung.

B Anhang

B.1 Literaturhinweise

- ▶ „Optische Übertragungstechnik in industrieller Praxis“
Christoph Wrobel (ed.)
Hüthig Buch Verlag Heidelberg
ISBN 3-7785-2262-0

- ▶ Hirschmann-Handbuch
„Basics of Industrial ETHERNET and TCP/IP“
280 710-834

- ▶ „TCP/IP Illustrated“, Band 1
W.R. Stevens
Addison Wesley 1994
ISBN 0-201-63346-9

B.2 Wartung

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

B.3 Management Information BASE (MIB)

Die Management Information Base (MIB) ist als abstrakte Baumstruktur angelegt.

Die Verzweigungspunkte sind die Objektklassen. Die „Blätter“ der MIB tragen die Bezeichnung generische Objektklassen.

Die Instanzierung der generischen Objektklassen, das heißt, die abstrakte Struktur auf die Realität abzubilden, erfolgt zum Beispiel durch die Angabe des Ports oder der Quelladresse (Source Address), soweit dies zur eindeutigen Identifizierung nötig ist.

Diesen Instanzen sind Werte (Integer, TimeTicks, Counter oder Octet String) zugewiesen, die gelesen und teilweise auch verändert werden können. Die Object Description oder der Object-ID (OID) bezeichnet die Objektklasse. Mit dem Subidentifizier (SID) werden sie instanziiert.

Beispiel:

Die generische Objektklasse `hm2PSState` (OID = 1.3.6.1.4.1.248.11.11.1.1.1.1.2) ist die Beschreibung der abstrakten Information `Netzteilstatus`. Es lässt sich daraus noch kein Wert auslesen, es ist ja auch noch nicht bekannt, welches Netzteil gemeint ist.

Durch die Angabe des Subidentifiziers 2 wird diese abstrakte Information auf die Wirklichkeit abgebildet, instanziiert, und bezeichnet so den Betriebszustand des Netzteils 2. Diese Instanz bekommt einen Wert zugewiesen, der gelesen werden kann. Damit liefert die Instanz `get`

1.3.6.1.4.1.248.11.11.1.1.1.1.2.1 als Antwort 1, das heißt, das Netzteil ist betriebsbereit.

Definition der verwendeten Syntaxbegriffe:

Integer	Ganze Zahl im Bereich von -2^{31} - $2^{31}-1$
IP-Adresse	xxx.xxx.xxx.xxx (xxx = ganze Zahl im Bereich von 0..255)
MAC-Adresse	12-stellige Hexzahl nach ISO/IEC 8802-3
Object Identifier	x.x.x.x... (zum Beispiel 1.3.6.1.1.4.1.248...)
Octet String	ASCII-Zeichen-Kette
PSID	Identifikation der Spannungsversorgung (Nummer des Netzteils)
TimeTicks	Stop-Uhr, verronnene Zeit = Zahlenwert/100 in Sekunden Zahlenwert = ganze Zahl im Bereich von $0-2^{32}-1$
Timeout	Zeitwert in hundertstel Sekunden Zeitwert = ganze Zahl im Bereich von $0-2^{32}-1$
Typfeld	4-stellige Hexzahl nach ISO/IEC 8802-3
Zähler	Ganze Zahl ($0-2^{32}-1$), deren Wert beim Auftreten bestimmter Ereignisse um 1 erhöht wird.

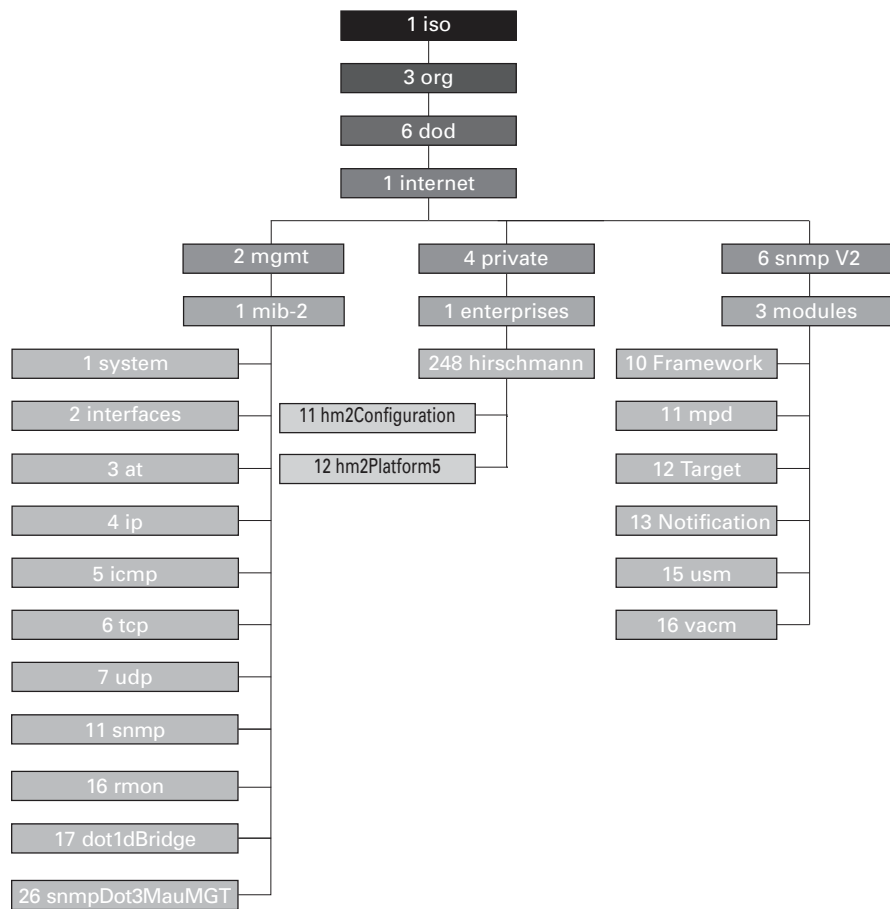


Abb. 79: Baumstruktur der Hirschmann-MIB

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

B.4 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 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 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 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
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 2863	The Interfaces Group 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
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)

B.5 Zugrundeliegende IEEE-Normen

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

B.6 Zugrundeliegende IEC-Normen

IEC 62439	High availability automation networks HSR – High-availability Seamless Redundancy MRP – Media Redundancy Protocol based on a ring topology PRP – Parallel Redundancy Protocol
-----------	--

B.7 Zugrundeliegende ANSI-Normen

ANSI/TIA-1057 Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.8 Technische Daten

Switching	
Größe der MAC-Adress-Tabelle (inkl. statische Filter)	2048
Max. Anzahl statisch konfigurierter MAC-Adressfilter	100
Max. Anzahl der mit IGMP-Snooping lernbaren MAC-Adressfilter	256
Max. Anzahl der MAC-Adresseinträge (MMRP)	64
Anzahl Warteschlangen	4 Queues
Einstellbare Port-Prioritäten	0..3
VLAN	
VLAN-ID-Bereich	1..4042
Anzahl der VLANs	max. 16 gleichzeitig pro Gerät max. 16 gleichzeitig pro Port

B.9 Copyright integrierter Software

Das Produkt enthält unter anderem Open-Source-Software-Dateien, die von Dritten entwickelt und unter einer Open-Source-Software-Lizenz lizenziert wurden.

Die Lizenzbedingungen finden Sie in der grafischen Benutzeroberfläche im Dialog *Hilfe* > *Lizenzen*.

B.10 Verwendete Abkürzungen

ACA	AutoConfiguration Adapter
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
MSTP	Multiple Spanning Tree Protocol
NMS	Network Management System
NTP	Network Time Protocol
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Index

1

802.1X 46

A

ACA 254, 254, 287
 Advanced Mode 145, 147
 Aging-Time 110
 Alarm 192, 254
 Alarmeinstellung 248
 Alarmnachrichten 190
 Alternate-Port 173, 179
 APNIC 30
 ARIN 30
 ARP 32
 Authentifizierungs-Liste 46
 Automatische Konfiguration 77

B

Backup-Port 173, 179
 Bandbreite 124
 Baumstruktur (Spanning Tree) 168, 172
 Benutzernamen 21, 23, 25
 Berechtigungen 49
 Bericht 207
 Best-Master-Clock-Algorithmus 99
 Boundary-Clock (PTP) 98
 BOOTP 29
 BPDU 168
 BPDU Guard 178, 179
 Bridge Identifier 165
 Bridge Protocol Data Unit 168

C

CDROM 260, 264
 CIDR 33
 CIP 235
 Classless Inter Domain Routing 33
 Command Line Interface 19
 Common Industrial Protocol 235

D

Datenpaketerfordernungsintervall 236
 Datensatz 251, 254
 Datenverkehr 89
 DAN (hardwareabhängig) 152
 Delay (PTP) 100
 Denial of Service 90
 Denial-of-Service 89
 Designated Bridge 173
 Designated Port 173, 178
 Device Description Language (Gerätebeschreibungs-
 sprache) 246
 DHCP 29
 DHCP-Server 93, 95, 260, 264
 Diameter (Spanning Tree) 167
 DiffServ 115
 Disabled-Port 173
 DoS 89, 90
 DSCP 115, 122

E

Echtzeit 115
 Edge-Port 173, 178
 EDS 236, 236
 Engineering-Station 252
 Engineering-System 249
 Ereignisprotokoll 210
 Erstinstallation 29
 EtherNet/IP-Website 235

F

Fast\ MRP 142, 142, 145, 147, 214
 FAQ 293
 Flusskontrolle 124
 Flüchtiger Speicher (RAM) 59

G

Gateway 31, 35
 Generic Ethernet Module 236
 Generische Objektklassen 278
 Gerätestatus 193
 Grafische Benutzeroberfläche starten 18
 Grandmaster (PTP) 99
 Grenzwert 248
 GSD 248, 249
 GSDML 246
 GSD-Datei 249

H

HaneWin 260, 264
 Hardware-Reset 190
 HiDiscovery 29, 34, 36, 38, 79, 84, 196, 211, 233
 Hostadresse 30
 HSR- und PRP-Netzverbindungen (hardwareabhängig)
 160
 HSR (hardwareabhängig) 141, 142, 156
 HSR-Netzstruktur (hardwareabhängig) 157

I

IANA 30
 IAS 46
 IEC 61850 226
 IEEE 802.1X 46
 IEEE-MAC-Adresse 204
 IGMP-Snooping 109, 109, 236
 Industrial HiVision 11, 40, 56
 Instanziierung 278
 Integrated authentication server 46
 IP-Adresse 30, 35, 40
 IP-Header 115, 118
 IRIG-B 103
 ISO/OSI-Schichtenmodell 32

K

Kompatibilität (STP) 176
 Konfigurationsänderungen 190
 Konfigurationsdatei 40
 Konformitätsklasse 246

L			
Laufzeitmessung (PTP)		100	
LACNIC		30	
Leave-Nachricht		110	
Link Aggration		142	
Link-Überwachung		193	
Login-Seite		18	
Loop Guard		179, 180	
LRE-Funktionalität (hardwareabhängig)		151	
M			
MaxAge		167	
MAC-Adressen-Filter		106	
MAC-Zieladresse		32	
MMS		226	
Moduleigenschaften		250	
Modus		77	
MRP		141, 142, 144, 145	
Multicast		109	
N			
Nachricht		190	
Netzlast		164, 165	
Netzmanagement		40	
Netzmanagementstation		252	
Netzmaske		31, 35	
Netzstruktur (PRP) (hardwareabhängig)		152	
NVM (permanenter Speicher)		59	
O			
Object Description		278	
Object-ID		278	
Objektklassen		278	
ODVA		235	
ODVA-Website		235	
OpenSSH-Suite		23	
Option 82		264	
Ordinary-Clock (PTP)		99	
P			
Passwort		21, 23, 25	
PC Worx		249	
Permanenter Speicher (NVM)		59	
Pfadkosten		166, 168	
Polling		190	
Portnummer		166	
Port-Identifikation		165, 166	
Port-Mirroring		213	
Port-Priorität		121	
Port-Priorität (Spanning Tree)		166	
Port-Rollen (RSTP)		173	
Port-Status		174	
PPS		103	
PPS (Pulse per Second)		103	
Priorität		117	
Priority Tagged Frames		117	
PROFIBUS-Organisation		246	
PRP (hardwareabhängig)		142, 150	
PRP-Beispielkonfiguration (hardwareabhängig)		153	
PRP-Netzstruktur (hardwareabhängig)		152	
PRP-RedBox (HSR-Beispiel) (hardwareabhängig)		160	
PTP		91	
PTP-Domäne		101	
PuTTY		19	
Q			
QoS		116	
Query		109	
R			
Rapid Spanning Tree		141, 141, 142, 173	
RADIUS		46	
RAM (flüchtiger Speicher)		59	
RedBox (hardwareabhängig)		152	
Redundanz		164	
Referenzzeitquelle		92, 95, 99	
Rekonfiguration		165	
Rekonfigurationszeit (MRP)		145	
Report-Nachricht		109	
RFC		280	
Ring		144	
Ring-Manager		144	
RIPE NCC		30	
RMON-Probe		213	
RM-Funktion		144	
Root Bridge		168	
Root Guard		178, 180	
Root-Pfad		170, 171	
Root-Pfadkosten		165	
Root-Port		173, 179	
Router		31	
Routing-Funktion		236	
RPI		236	
RSTP		176	
RST BPDU		173, 175	
RS Who		236	
S			
SAN (für HSR) (hardwareabhängig)		157	
SAN-RedBox (HSR-Beispiel) (hardwareabhängig)		158	
Schulungsangebote		293	
Schutzfunktionen (Guards)		178	
Secure Shell		19, 22	
Secure Shell		19	
Segmentierung		190	
Service		207	
Service-Shell-Funktion reaktivieren		58	
SFP-Modul		203	
Simatic S7		249	
SNMP		190	
SNMP-Trap		190, 192	
SNTP		91	
Software-Version		71	
Sommerzeitumschaltung		93	
SSH		19, 19, 22	
STP-BPDU		168	
STP-Kompatibilität		176	
Store and Forward		106	
Strict-Priority		118	
Subidentifier		278	
Subnetz		35	
Symbol		236, 236, 248, 249	
Systemanforderungen (GUI)		18	
T			
TCN Guard		178, 180	
TCP/IP		235, 246	
Technische Fragen		293	
Topology-Change-Flag		178	

ToS	115, 118
Transparent-Clock (PTP)	99
Trap	190, 192
Trap-Ziel-Tabelle	190
Type of Service	118
U	
UDP/IP	235, 246
Uhrzeit einstellen	92
Update	26
Übertragungssicherheit	190
V	
Verkehrsklasse	118, 122
Verzögerungszeit (MRP)	145
Video	118
VLAN	127
VLAN-Priorität	121
VLAN-Tag	117, 127
VoIP	118
VT100	24
V.24	19, 24
W	
Warteschlange	118
Weighted Fair Queuing	119
Weighted Round Robin	119
Z	
Zeitsignal (IRIG-B/PPS)	103
Ziel-Tabelle	190
Zugangsschutz	76

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>.

Eine Liste von Telefonnummern und E-Mail-Adressen für direkten technischen Support durch Hirschmann finden Sie unter <https://hirschmann-support.belden.eu.com>.

Sie finden auf dieser Website außerdem eine kostenfreie Wissensdatenbank sowie einen Download-Bereich für Software.

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.hicom-center.com>.
- ▶ Der Support reicht von der Inbetriebnahme über den Bereitschaftsservice 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>

E Leserkritik

Wie denken Sie über dieses Handbuch? Wir sind stets bemüht, in unseren Handbüchern das betreffende Produkt vollständig zu beschreiben und wichtiges Hintergrundwissen zu vermitteln, um Sie beim Einsatz dieses Produkts zu unterstützen. Ihre Kommentare und Anregungen helfen uns dabei, die Qualität und den Informationsgrad dieser Dokumentation weiter zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	gut	befriedigend	mäßig	schlecht
Exakte Beschreibung	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Lesbarkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Verständlichkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Beispiele	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Aufbau	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vollständigkeit	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Grafiken	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Zeichnungen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Tabellen	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Haben Sie in diesem Handbuch Fehler entdeckt?

Wenn ja, welche auf welcher Seite?

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- ▶ als Fax an die Nummer +49 (0)7127 14-1600 oder
- ▶ per Post an

Hirschmann Automation and Control GmbH
Abteilung 01RD-NT
Stuttgarter Str. 45-51
72654 Neckartenzlingen



HIRSCHMANN

A **BELDEN** BRAND