HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

GRS1020-1030 HiOS-2S Rel. 07000

Referenz-Handbücher

Grafische Benutzeroberfläche

Command Line Interface

Anwender-Handbuch

Konfiguration

HIRSCHMANN
A BELDEN BRAND

Referenz-Handbuch

Grafische Benutzeroberfläche
HiOS-2S GRS (Greyhound 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.

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 Module 26
1.3 Netz 28
1.4 Software 31
1.5 Laden/Speichern 33
1.6 Externer Speicher 43
1.7 Port 46
Konfiguration 47
Statistiken 51
Netzlast 53
1.8 Neustart 54

2 Zeit 57

2.1 Grundeinstellungen 58
Global 59
Sommerzeit 60
2.2 SNTP 63
2.2.1 SNTP Client 64
2.2.2 SNTP Server 67

3 Gerätesicherheit 69

3.1 Benutzerverwaltung 70
3.2 Authentifizierungs-Liste 74
3.3 Management-Zugriff 77
3.3.1 Server 78
Information 79
SNMP 81
Telnet 83
SSH 84
HTTP 87
HTTPS 88
3.3.2 IP-Zugriffsbeschränkung 91
3.3.3 Web 93

3.3.4 Command Line Interface 94
Global 95
Login-Banner 96
3.3.5 SNMPv1/v2 Community 97
3.4 Pre-Login-Banner 98

4 Netzsicherheit 99

4.1 Netzsicherheit Übersicht 100
4.2 Port-Sicherheit 101
Wizard : Port-Sicherheit 104
4.3 802.1X Port-Authentifizierung 106
4.3.1 802.1X Global 107
4.3.2 802.1X Port-Konfiguration 109
4.3.3 802.1X Port-Clients 112
4.3.4 802.1X EAPOL-Portstatistiken 113
4.3.5 802.1X Port-Authentifizierung-Historie 114
4.3.6 802.1X Integrierter Authentifikations-Server 116
4.4 RADIUS 117
4.4.1 RADIUS Global 118
4.4.2 RADIUS Authentication-Server 119
4.4.3 RADIUS Accounting-Server 121
4.4.4 RADIUS Authentication Statistiken 122
4.4.5 RADIUS Accounting-Statistiken 123
4.5 DoS 124
4.5.1 DoS-Global 125
4.6 ACL 128
4.6.1 ACL IPv4-Regel 129
4.6.2 ACL MAC-Regel 132
4.6.3 ACL Zuweisung 134

5 Switching 137

5.1 Switching Global 138
5.2 Lastbegrenzer 140
5.3 Filter für MAC-Adressen 142
5.4 IGMP-Snooping 144
5.4.1 IGMP-Snooping Global 145
5.4.2 IGMP-Snooping Konfiguration 146
VLAN-ID 147
Port 148
5.4.3 IGMP-Snooping Erweiterungen 150
Wizard : Selection VLAN/Port 152
5.4.4 IGMP Snooping-Querier 153
5.4.5 IGMP Snooping Multicasts 155

5.5 MRP-IEEE 156
5.5.1 MRP-IEEE Konfiguration 157
5.5.2 MRP-IEEE Multiple MAC Registration Protocol 158
Konfiguration 159
Service-Requirement 161
Statistiken 162
5.5.3 MRP-IEEE Multiple VLAN Registration Protocol 163
Konfiguration 164
Statistiken 166
5.6 GARP 167
5.6.1 GMRP 168
5.6.2 GVRP 170
5.7 QoS/Priorität 171
5.7.1 QoS/Priorität Global 172
5.7.2 QoS/Priorität Port-Konfiguration 173
5.7.3 802.1D/p Zuweisung 174
5.7.4 IP-DSCP-Zuweisung 175
5.7.5 Queue-Management 177
5.8 VLAN 178
5.8.1 VLAN Global 179
5.8.2 VLAN Konfiguration 180
5.8.3 VLAN Port 182
5.8.4 VLAN Voice 183
5.9 L2-Redundanz 185
5.9.1 MRP 186
5.9.2 Spanning Tree 189
5.9.2.1 Spanning Tree Global 190
5.9.2.2 Spanning Tree Port 195
CIST 196
Guards 200
5.9.3 Link-Aggregation 202
5.9.4 Link-Backup 207

6 Diagnose 211

6.1 Statuskonfiguration 212
6.1.1 Gerätestatus 213
Global 214
Port 217
Status 218
6.1.2 Sicherheitsstatus 219
Global 220
Port 224

Status 225
6.1.3 Signalkontakt 226
6.1.3.1 Signalkontakt 1 / Signalkontakt 2 227
Global 228
Port 231
Status 232
6.1.4 MAC-Benachrichtigung 233
6.1.5 Alarme (Traps) 235
6.2 System 236
6.2.1 Systeminformationen 237
6.2.2 Hardware-Zustand 238
6.2.3 Konfigurations-Check 239
6.2.4 IP-Adressen Konflikterkennung 241
6.2.5 ARP 244
6.2.6 Selbsttest 245
6.3 Syslog 247
6.4 Ports 249
6.4.1 SFP 250
6.4.2 TP-Kabeldiagnose 251
6.4.3 Port-Monitor 253
Global 254
Auto-Disable 257
Link-Änderungen 258
CRC/Fragmente 259
Überlast-Erkennung 260
Link-Speed-/Duplex-Mode-Erkennung 261
6.4.4 Auto-Disable 263
Port 263
Status 265
6.4.5 Port-Mirroring 266
6.5 LLDP 269
6.5.1 LLDP Konfiguration 270
6.5.2 LLDP Topologie-Erkennung 273
LLDP 274
LLDP-MED 275
6.6 Bericht 277
6.6.1 Bericht Global 278
6.6.2 Persistentes Ereignisprotokoll 282
6.6.3 System Log 284
6.6.4 Audit Trail 285
7 Erweitert 287

7.1 DHCP-L2-Relay 288
7.1.1 DHCP-L2-Relay Konfiguration 289
Interface 290
VLAN-ID 291
7.1.2 DHCP-L2-Relay Statistiken 292
7.2 DHCP-Server 293
7.2.1 DHCP-Server Global 294
7.2.2 DHCP-Server Pool 295
7.2.3 DHCP-Server Lease-Tabelle 298
7.3 Industrie-Protokolle 299
7.3.1 IEC61850-MMS 300
7.3.2 Modbus TCP 302

A Index 305

B Weitere Unterstützung 307

C Leserkritik 308

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.
`Courier`	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: ▶ *Benutzer:* Bezeichnung des angemeldeten Benutzers ▶ *Gerätename:* Bezeichnung des Geräts Klicken Sie die Schaltfläche, um den Dialog *Gerätesicherheit > Benutzerverwaltung* zu öffnen.
	Wenn Sie den Mauszeiger über der Schaltfläche positionieren, zeigt ein Tooltip die Zusammenfassung des Dialogs *Diagnose > System > Konfigurations-Check*. Klicken Sie die Schaltfläche, um den Dialog *Diagnose > System > Konfigurations-Check* zu öffnen.
	Klicken Sie die Schaltfläche, um den gegenwärtig angemeldeten Benutzer abzumelden und die Login-Seite anzuzeigen.

Schaltfläche	Bedeutung
298	Zeigt die verbleibende Zeit in Sekunden, bis das Gerät einen inaktiven Benutzer automatisch abmeldet. Klicken Sie die Schaltfläche, um den Dialog ***Gerätesicherheit > Management-Zugriff > Web*** zu öffnen. Dort können Sie das Timeout festlegen.
	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. Klicken Sie die Schaltfläche, um den Dialog ***Grundeinstellungen > Laden/Speichern*** zu öffnen. Mit einem Rechtsklick auf die Schaltfläche können Sie die gegenwärtigen Einstellungen im permanenten Speicher (NVM) speichern.
	Wenn Sie den Mauszeiger über der Schaltfläche positionieren, zeigt ein Tooltip die folgenden Informationen: ▶ ***Gerätestatus:*** Dieser Abschnitt zeigt eine komprimierte Ansicht des Rahmens ***Geräte-Status*** im Dialog ***Grundeinstellungen > System***. Der Abschnitt zeigt den zeitlich zuerst aufgetretenen, gegenwärtig noch andauernden Alarm. ▶ ***Sicherheitsstatus:*** Dieser Abschnitt zeigt eine komprimierte Ansicht des Rahmens ***Sicherheits-Status*** im Dialog ***Grundeinstellungen > System***. 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: – Dialog ***Grundeinstellungen > Externer Speicher***, Parameter ***Automatisches Software-Update*** – Dialog ***Grundeinstellungen > Externer Speicher***, Parameter ***Konfigurations-Priorität*** – Dialog ***Gerätesicherheit > Management-Zugriff > Server***, Registerkarte ***SNMP***, Parameter ***UDP-Port*** – Dialog ***Diagnose > System > Selbsttest***, Parameter ***RAM test*** – Dialog ***Diagnose > System > Selbsttest***, Parameter ***SysMon1 ist verfügbar*** – Dialog ***Diagnose > System > Selbsttest***, Parameter ***Bei Fehler Default-Konfiguration laden*** Klicken Sie die Schaltfläche, um den Dialog ***Diagnose > Statuskonfiguration >*** Gerätestatus zu öffnen.

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: ☐ 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***.
	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
- Module
- Netz
- Software
- Laden/Speichern
- Externer Speicher
- 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 ***Diagnose > Statuskonfiguration > Gerätestatus***, Registerkarte ***Status*** zeigt die Alarme im Überblick.

Anmerkung: Das Gerät meldet einen Alarm, wenn Sie an ein Gerät mit mehreren Anschlüssen für die Versorgungsspannung lediglich ein Netzteil anschließen. Um diesen Alarm zu vermeiden, deaktivieren Sie im Dialog ***Diagnose > Statuskonfiguration > Gerätestatus*** das Überwachen der fehlenden Netzteile.

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 ***Diagnose > Statuskonfiguration > Sicherheitsstatus***, Registerkarte ***Status*** zeigt die Alarme im Überblick.

Status Signalkontakt

Die Felder in diesem Rahmen zeigen den Signalkontaktstatus 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 > Signalkontakt > ***Signalkontakt 1***/***Signalkontakt 2***.

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 ***Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 1***/***Signalkontakt 2***, Registerkarte ***Status*** zeigt die Alarme im Überblick.

Systemdaten

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

Parameter	Bedeutung
Systemname	Legt den Namen fest, unter dem das Gerät im Netz bekannt ist. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen Die folgenden Zeichen sind zulässig: – `0..9` – `a..z` – `A..Z` – `!#$%&'()*+,-./:;<=>?@[\]^_`{}~` – `<Gerätename>-<MAC-Adresse>` (Voreinstellung) Beim Erzeugen von HTTPS-X.509-Zertifikaten verwendet die Applikation, die das Zertifikat generiert, den festgelegten Wert als Domain-Namen und als gemeinsamen Namen. 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. ▶ DHCP-Client ▶ ***Syslog*** ▶ ***IEC61850-MMS***
Standort	Legt den Standort des Geräts fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
Ansprechpartner	Legt den Ansprechpartner für dieses Gerät fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
Gerätetyp	Zeigt die Produktbezeichnung des Grundgeräts.
Netzteil 1 Netzteil 2	Zeigt den Status des Netzteils am betreffenden Spannungsversorgungs-Anschluss. Mögliche Werte: ▶ `vorhanden` ▶ `defekt` ▶ `nicht vorhanden` ▶ `unbekannt`
Betriebszeit	Zeigt die Zeit, die seit dem letzten Neustart dieses Geräts vergangen ist. Mögliche Werte: ▶ Zeit im Format `Tag(e), ...h ...m ...s`

Parameter	Bedeutung
Temperatur [°C]	Zeigt die gegenwärtige Temperatur im Gerät in °C. Das Überwachen der Temperaturgrenzen schalten Sie ein im Dialog ***Diagnose*** > Statuskonfiguration > ***Gerätestatus***.
Obere Temp.-Grenze [°C]	Legt die obere Temperaturgrenze in °C fest. Das Anwender-Handbuch „Installation“ enthält ausführliche Informationen zum Festlegen der Temperaturgrenzen. Mögliche Werte: ▶ `-99..99` (ganze Zahl) Überschreitet die Temperatur im Gerät diesen Wert, generiert das Gerät einen Alarm.
Untere Temp.-Grenze [°C]	Legt die untere Temperaturgrenze in °C fest. Das Anwender-Handbuch „Installation“ enthält ausführliche Informationen zum Festlegen der Temperaturgrenzen. Mögliche Werte: ▶ `-99..99` (ganze Zahl) Unterschreitet die Temperatur im Gerät diesen Wert, generiert das Gerät einen Alarm.

LED-Status

Dieser Rahmen zeigt die Zustände der Gerätstatus-LEDs zum Zeitpunkt der letzten Aktualisierung. Das Anwender-Handbuch „Installation“ enthält ausführliche Informationen zu den Gerätstatus-LEDs.

Parameter	Farbe	Bedeutung
Status	●	Gegenwärtig ist kein Alarm vorhanden. Der Gerätstatus ist OK.
	●	Gegenwärtig ist mindestens ein Gerätstatus-Alarm vorhanden. Siehe Rahmen ***Geräte-Status*** oben.
Power	●	Gerätevariante mit 2 Netzteilen: Lediglich eine Versorgungsspannung ist aktiv.
	●	Gerätevariante mit 1 Netzteil: Die Versorgungsspannung ist aktiv. Gerätevariante mit 2 Netzteilen: Beide Versorgungsspannungen sind aktiv.
RM	●	Das Gerät arbeitet weder als ***MRP***-Ringmanager noch als ***DLR***-Supervisor.
	●	Verlust der Redundanz-Reserve. Das Gerät arbeitet als ***MRP***-Ring-Manager.
	●	Die Redundanz-Reserve ist verfügbar. Das Gerät arbeitet als ***MRP***-Ring-Manager.
ACA	●	Kein externer Speicher angeschlossen.
	●	Der externe Speicher ist angeschlossenen, jedoch nicht betriebsbereit.
	●	Der externe Speicher ist angeschlossenen und betriebsbereit.

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 ***Grundeinstellungen > Ports***, Registerkarte ***Konfiguration***.
		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 Module

Das Gerät bietet Ihnen die Möglichkeit, die Module im laufenden Betrieb einzustecken oder zu entfernen (hot plug).

Um den Netzzugriff zu unterbinden, deaktivieren Sie einen Steckplatz. Auf einem deaktivierten Steckplatz werden Module erkannt und die Port-Konfiguration ist möglich. Allerdings stellt das Modul keine Verbindungen ins Netz her, solange der Steckplatz deaktiviert ist.

Anleitung zur Installation eines Moduls

Führen Sie die folgenden Schritte aus:

☐ Stecken Sie das Modul in den Steckplatz.
Das Gerät konfiguriert das Modul automatisch anhand der Voreinstellungen und erkennt die Modul-Parameter.

☐ Klicken Sie die Schaltfläche , um die grafische Benutzeroberfläche zu aktualisieren.
Die Spalte ***Modul-Status*** zeigt für das installierte Modul den Wert `physical`.

☐ Markieren Sie in der Tabelle das installierte Modul.

☐ Um den Zugriff auf das Netz über den Steckplatz zu ermöglichen, aktivieren Sie den Steckplatz:
Heben Sie die Markierung des Kontrollkästchens ***Aktiv*** auf.

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Anleitung zum Entfernen eines Moduls

Das Entfernen eines Moduls aus einem Steckplatz hilft, den Zugriff auf das Netz durch Nutzung eines leeren Steckplatzes zu unterbinden.
Führen Sie die folgenden Schritte aus:

☐ Entfernen Sie das Modul aus dem Steckplatz.

☐ Klicken Sie die Schaltfläche , um die grafische Benutzeroberfläche zu aktualisieren.
Die Spalte ***Modul-Status*** zeigt für das zuvor entfernte Modul den Wert `configurable`.

☐ Markieren Sie in der Tabelle das zuvor entfernte Modul.

☐ Klicken Sie die Schaltfläche und dann den Eintrag ***Modul entfernen***.
Die Spalte ***Modul-Status*** zeigt für das zuvor entfernte Modul den Wert `remove`. Zusätzlich zeigt die Spalte ***Typ*** und einige andere Spalten den Wert `n/a`.
Das markierte Kontrollkästchen ***Aktiv*** weist darauf hin, dass der Steckplatz noch aktiv ist.

☐ Um weitere Zugriffe auf das Netz über den nicht verwendeten Steckplatz zu unterbinden, deaktivieren Sie den Steckplatz.
Heben Sie die Markierung des Kontrollkästchens ***Aktiv*** auf.

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Solange die Spalte ***Modul-Status*** den Wert `configurable` zeigt, können Sie das Modul konfigurieren und seine Einstellungen speichern.

- Wenn Sie das Modul durch ein baugleiches Modul ersetzen, dann wendet das Gerät die Einstellungen sofort auf das neue Modul an.
- Wenn Sie das Modul durch ein Modul anderen Typs ersetzen, dann wendet das Gerät die Werkseinstellungen auf das neue Modul an.
- Wenn Sie ein Modul in einen leeren Steckplatz einschieben, dann konfiguriert das Gerät das Modul mit seinen Voreinstellungen. Wenn der Steckplatz inaktiv ist, bleibt er solange inaktiv, bis Sie das Kontrollkästchen in Spalte ***Aktiv*** markieren. Nachdem die Voreinstellungen des Ports in das Modul geladen wurden, ist der Zugriff auf das Netz möglich.

Tabelle

Schaltfläche	Bedeutung
Modul	Zeigt die Nummer des Steckplatzes, auf den sich der Eintrag bezieht.
Aktiv	Aktiviert/deaktiviert den Steckplatz. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Steckplatz ist aktiv. Das Gerät erkennt ein in diesem Steckplatz installiertes Modul. ▶ `unmarkiert` Der Steckplatz ist inaktiv.
Typ	Zeigt den Typ des im Steckplatz installierten Moduls. Ein Wert von `n/a` weist darauf hin, dass der Steckplatz leer ist.
Beschreibung	Legt eine Kurzbeschreibung für das installierte Modul fest.
Version	Zeigt die Modulversion.
Ports	Zeigt, wie viele Ports am Modul verfügbar sind.
Seriennummer	Zeigt die Seriennummer des Moduls. Ein Wert von `n/a` weist darauf hin, dass der Steckplatz leer ist.
Modul-Status	Zeigt den Status des Steckplatzes. Mögliche Werte: ▶ `physical` Weist darauf hin, dass ein Modul im Steckplatz vorhanden und aktiv ist. ▶ `configurable` Weist darauf hin, dass der Steckplatz leer und für die Konfiguration verfügbar ist. ▶ `remove` Weist darauf hin, dass der Steckplatz leer und deaktiviert ist. ▶ `fix` Weist darauf hin, dass das Modul nicht entfernt werden kann.

Schaltflächen

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

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Modul entfernen	Entfernt das Modul aus der Tabelle.

1.3 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.

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	Legt fest, aus welcher Quelle das Gerät nach dem Starten seine IP-Parameter erhält: Mögliche Werte: ▶ `Lokal` Das Gerät verwendet die IP-Parameter aus dem internen Speicher. Die Einstellungen dafür legen Sie im Rahmen ***IP-Parameter*** 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` (Voreinstellung) 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. **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.
VLAN-ID	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. Mögliche Werte: ▶ `1..4042` (Voreinstellung: `1`) Voraussetzung ist, dass das VLAN bereits eingerichtet ist. Siehe Dialog ***Switching > VLAN >*** Konfiguration . Wenn Sie nach Ändern des Werts die Schaltfläche ☑ klicken, öffnet sich der Dialog ***Information***. Wählen Sie den Port aus, über den Sie die Verbindung zum Gerät zukünftig herstellen. Nach Klicken der Schaltfläche ***Ok*** sind die Einstellungen des neuen Management-VLANs dem Port zugewiesen. – Der Port wird Mitglied des VLANs und vermittelt die Datenpakete ohne VLAN-Tag (untagged). Siehe Dialog ***Switching > VLAN > Konfiguration***. – Das Gerät weist dem Port die Port-VLAN-ID des neuen Management-VLANs zu. Siehe Dialog ***Switching > VLAN > Port***. Nach kurzer Wartezeit ist das Gerät über den neuen Port im neuen Management-VLAN erreichbar.
MAC-Adresse	Zeigt die MAC-Adresse des Geräts. Mit der MAC-Adresse ist das Management des Geräts über das Netz erreichbar.

BOOTP/DHCP

Parameter	Bedeutung
Client-ID	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. Das Gerät sendet als DHCP-Client-ID den Gerätenamen, der im Feld ***Systemname*** im Dialog ***Grundeinstellungen > System*** festgelegt ist.

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	Schaltet die HiDiscovery-Funktion im Gerät ein/aus. Mögliche Werte: ▶ `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	Schaltet den Schreibzugriff auf das Gerät per HiDiscoveryein/aus. Mögliche Werte: ▶ `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. Empfehlung: Ändern Sie erst nach Inbetriebnahme des Geräts die Einstellung auf `readOnly`.
Signal	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. Mögliche Werte: ▶ `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
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
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.

1.4 Software

Dieser Dialog bietet Ihnen die Möglichkeit, die Geräte-Software zu aktualisieren und Informationen über die Geräte-Software anzuzeigen.
Außerdem haben Sie die Möglichkeit, ein im Gerät gespeichertes Backup der Geräte-Software wiederherzustellen.

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.
Backup version	Zeigt Versionsnummer und Erstellungsdatum der als Backup im Flash gespeicherten Geräte-Software. Diese Geräte-Software hat das Gerät beim letzten Software-Update oder nach Klicken der Schaltfläche ***Wiederherstellen*** in den Backup-Bereich kopiert.
Wiederherstellen	Stellt die als Backup gespeicherte Geräte-Software wieder her. Dabei tauscht das Gerät die ***Stored version*** und die ***Backup version*** der Geräte-Software. Das Gerät lädt die ***Stored version*** beim nächsten Neustart.
Bootcode	Zeigt Versionsnummer und Erstellungsdatum des Bootcodes.

Software-Update

Parameter	Bedeutung

URL	Legt Pfad und Dateiname der Image-Datei fest, mit der Sie die Geräte-Software aktualisieren.
	
	Das Gerät bietet Ihnen folgende Möglichkeiten, die Geräte-Software zu aktualisieren:
	▶ 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:
	`ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
	▶ 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:
	`tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
	▶ 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:
	– `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>`

Parameter	Bedeutung
Start	Aktualisiert die Geräte-Software. 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. Die bisher verwendete Geräte-Software kopiert das Gerät in den Backup-Bereich. Um während des Software-Updates im Gerät angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ legen Sie vor dem Software-Update im Dialog ***Gerätesicherheit >*** Management-Zugriff ***> Web***, Feld ***Web-Interface Session-Timeout [min]*** einen ausreichend hohen Wert fest.

Alternativ bietet das Gerät Ihnen die Möglichkeit, die Geräte-Software durch Rechtsklicken in der Tabelle zu aktualisieren, wenn sich die Image-Datei auf dem externen Speicher befindet.

Tabelle

Parameter	Bedeutung
Datei Ort	Zeigt den Speicherort der Geräte-Software. Mögliche Werte: ▶ `ram` Flüchtiger Speicher des Geräts ▶ `flash` Permanenter Speicher (`NVM`) des Geräts ▶ `usb` Externer USB-Speicher (ACA21/ACA22)
Index	Zeigt den Index der Geräte-Software. Für die der Geräte-Software im Flash hat der Index die folgende Bedeutung: ▶ `1` Diese Geräte-Software lädt das Gerät beim Neustart. ▶ `2` Diese Geräte-Software hat das Gerät beim letzten Software-Update in den Backup-Bereich kopiert.
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.

1.5 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.

Externer Speicher

Parameter	Bedeutung
Ausgewählter externer Speicher	Zeigt den Typ des externen Speichers. Mögliche Werte: ▶ `usb` Externer USB-Speicher (ACA21/ACA22)
Status	Zeigt den Betriebszustand des externen Speichers. Mögliche Werte: ▶ `notPresent` Kein externer Speicher angeschlossen. ▶ `removed` Jemand hat den externen Speicher während des Betriebs aus dem Gerät entfernt. ▶ `ok` Der externe Speicher ist angeschlossenen und betriebsbereit. ▶ `outOfMemory` Der Speicherplatz auf dem externen Speicher ist belegt. ▶ `genericErr` Das Gerät hat einen Fehler festgestellt.

Konfigurations-Verschlüsselung

Parameter	Bedeutung
Aktiv	Zeigt, ob die Konfigurations-Verschlüsselung im Gerät aktiv/inaktiv ist. Mögliche Werte: ▶ `markiert` 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. ▶ `unmarkiert` Die Konfigurations-Verschlüsselung ist inaktiv. Das Gerät lädt ein Konfigurationsprofil aus dem permanenten Speicher (`NVM`) ausschließlich dann, wenn dieses unverschlüsselt ist. Wenn im Dialog ***Grundeinstellungen > Externer Speicher*** die Spalte ***Konfigurations-Priorität*** den Wert oder `second` hat und das Konfigurationsprofil unverschlüsselt ist, zeigt der Rahmen ***Sicherheits-Status*** im Dialog ***Grundeinstellungen > System*** einen Alarm. Im Dialog ***Diagnose > Statuskonfiguration > Sicherheitsstatus***, Registerkarte ***Global***, Spalte ***Überwachen*** legen Sie fest, ob das Gerät den Parameter ***Unverschlüsselte Konfiguration vom externen Speicher laden*** überwacht.
Passwort setzen	Öffnet das ***Passwort setzen***-Fenster, das Ihnen beim Festlegen des Passworts hilft, das für die Verschlüsselung des Konfigurationsprofils erforderlich ist. Das Verschlüsseln des Konfigurationsprofils erschwert den unberechtigten Zugriff. ☐ Wenn Sie ein vorhandenes Passwort ändern, geben Sie in das Feld ***Altes Passwort*** das bisherige Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen ***Passwort anzeigen***. ☐ Geben Sie im Feld ***Neues Passwort*** das Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen ***Passwort anzeigen***. ☐ Markieren Sie das Kontrollkästchen ***Konfiguration danach speichern***, um die Verschlüsselung auf das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (`NVM`) und auf dem externen Speicher 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. Wenn Sie ein Gerät mit verschlüsseltem Konfigurationsprofil zum Beispiel wegen eines Defekts ersetzen, gehen Sie wie folgt vor: ☐ Starten Sie das neue Gerät, weisen Sie die IP-Parameter zu. ☐ Öffnen Sie auf dem neuen Gerät den Dialog ***Grundeinstellungen > Laden/Speichern***. ☐ Verschlüsseln Sie im neuen Gerät das Konfigurationsprofil. Siehe oben. Geben Sie dasselbe Passwort ein, das Sie im defekten Gerät verwendet haben. ☐ Installieren Sie im neuen Gerät den externen Speicher aus dem defekten Gerät. ☐ Starten Sie das neue Gerät neu. Beim Neustart lädt das Gerät das Konfigurationsprofil mit den Einstellungen des defekten Geräts vom externen Speicher. Das Gerät kopiert die Einstellungen in den flüchtigen Speicher (`RAM`) und in den permanenten Speicher (`NVM`).
Löschen	Öffnet das ***Löschen***-Fenster, das Ihnen beim Aufheben der Konfigurations-Verschlüsselung im Gerät hilft. ☐ Geben Sie im Feld ***Altes Passwort*** das bisherige Passwort ein. Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen ***Passwort anzeigen***. ☐ Markieren Sie das Kontrollkästchen ***Konfiguration danach speichern***, um die Verschlüsselung auch im „ausgewählten“ Konfigurationsprofil im permanenten Speicher (`NVM`) und auf dem externen Speicher aufzuheben. **Anmerkung:** Wenn Sie weitere Konfigurationsprofile verschlüsselt im Speicher vorhalten, hindert das Gerät Sie anschließend daran, diese Konfigurationsprofile zu aktivieren oder als „ausgewählt“ zu kennzeichnen.

Information

Parameter	Bedeutung
NVM synchron mit running-config	Zeigt, ob das Konfigurationsprofil im flüchtigen Speicher (`RAM`) und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (`NVM`) übereinstimmen. Mögliche Werte: ▶ `markiert` Die Konfigurationsprofile stimmen überein. ▶ `unmarkiert` Die Konfigurationsprofile unterscheiden sich.
Externer Speicher und NVM synchron	Zeigt, ob das „ausgewählte“ Konfigurationsprofil im externen Speicher und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (`NVM`) übereinstimmen. Mögliche Werte: ▶ `markiert` Die Konfigurationsprofile stimmen überein. ▶ `unmarkiert` Die Konfigurationsprofile unterscheiden sich. Mögliche Ursachen: – An das Gerät ist kein externer Speicher angeschlossen. – Im Dialog ***Grundeinstellungen > Externer Speicher*** ist die Funktion ***Sichere Konfiguration beim Speichern*** ausgeschaltet.

Sichere Konfiguration auf Remote-Server beim Speichern

Parameter	Bedeutung
Funktion	Schaltet die ***Sichere Konfiguration auf Remote-Server beim Speichern***-Funktion ein/aus. Mögliche Werte: ▶ `Eingeschaltet` Die ***Sichere Konfiguration auf Remote-Server beim Speichern***-Funktion ist eingeschaltet. Wenn Sie das Konfigurationsprofil im permanenten Speicher (`NVM`) speichern, sichert das Gerät das Konfigurationsprofil automatisch auf dem im Feld ***URL*** festgelegten Remote-Server. ▶ `Ausgeschaltet` (Voreinstellung) Die ***Sichere Konfiguration auf Remote-Server beim Speichern***-Funktion ist ausgeschaltet.
URL	Legt Pfad und Dateiname des zu sichernden Konfigurationsprofils auf dem Remote-Server fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen Beispiel: `tftp://192.9.200.1/cfg/config.xml` Das Gerät unterstützt die folgenden Platzhalter: – `%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	Öffnet das ***Anmeldeinformationen***-Fenster, das Ihnen beim Festlegen des Passworts hilft, das für die Anmeldung auf dem Remote-Server erforderlich ist.
	☐ Geben Sie im Feld ***Benutzername*** den Benutzernamen ein.
	Um anstelle von ***** (Sternchen) den Benutzernamen im Klartext anzuzeigen, markieren Sie das Kontrollkästchen ***Passwort anzeigen***.
	Mögliche Werte:
	– Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
	☐ Geben Sie im Feld ***Passwort*** das Passwort ein.
	Um anstelle von ***** (Sternchen) das Passwort im Klartext anzuzeigen, markieren Sie das Kontrollkästchen ***Passwort anzeigen***.
	Mögliche Werte:
	▶ Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen
	Die folgenden Zeichen sind zulässig:
	`a..z`
	`A..Z`
	`0..9`
	`#$%&'()*+,-./:;<=>?@_```

Konfigurationsänderungen rückgängig machen

Parameter	Bedeutung
Funktion	Schaltet die ***Konfigurationsänderungen rückgängig machen***-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. Mögliche Werte: ▶ `An` Die Funktion ist eingeschaltet. – Die Zeitspanne zwischen Verbindungsabbruch und Laden des Konfigurationsprofils legen Sie fest im Feld ***Timeout [s] für Wiederherstellung nach Verbindungsabbruch***. – Enthält der permanente Speicher (`NVM`) mehrere Konfigurationsprofile, lädt das Gerät das als „ausgewählt“ gekennzeichnete Konfigurationsprofil. ▶ `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. **Anmerkung:** Bevor Sie die Funktion einschalten, speichern Sie die Einstellungen im Konfigurationsprofil. Gegenwärtige Änderungen, die lediglich flüchtig im Gerät gespeichert sind, bleiben somit erhalten.
Timeout [s] für Wiederherstellung nach Verbindungsabbruch	Legt die Zeit in Sekunden fest, nach der das Gerät das „ausgewählte“ Konfigurationsprofil aus dem permanenten Speicher (`NVM`) lädt, wenn die Verbindung abbricht. Mögliche Werte: ▶ `30..600` (Voreinstellung: `600`) 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.
Watchdog IP-Adresse	Zeigt die IP-Adresse des PCs, auf dem Sie die Funktion eingeschaltet haben. Mögliche Werte: ▶ IPv4-Adresse (Voreinstellung: `0.0.0.0`)

Tabelle

Parameter	Bedeutung
Speicher-Typ	Zeigt den Speicherort des Konfigurationsprofils. Mögliche Werte: ▶ `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 ***Konfigurationsänderungen rückgängig machen***. 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: ☐ Markieren Sie in der Tabelle das Konfigurationsprofil. ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag ***Aktivieren***. ▶ `ENVM` (externer Speicher) Auf dem externen Speicher speichert das Gerät eine Sicherungskopie des „ausgewählten“ Konfigurationsprofils. Voraussetzung ist, dass Sie im Dialog ***Grundeinstellungen > Externer Speicher*** das Kontrollkästchen in Spalte ***Sichere Konfiguration beim Speichern*** markieren.
Profilname	Zeigt die Bezeichnung des Konfigurationsprofils. Mögliche Werte: ▶ `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 ***Speichern unter...*** 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 ***Exportieren...***.
Datum der letzten Änderung (UTC)	Zeigt den Zeitpunkt (UTC), zu dem ein Benutzer das Konfigurationsprofil zuletzt gespeichert hat.
Ausgewählt	Zeigt, ob das Konfigurationsprofil als „ausgewählt“ gekennzeichnet ist. Mögliche Werte: ▶ `markiert` Das Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet. – 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 ***Aktivieren***.

Parameter	Bedeutung
Verschlüsselt	Zeigt, ob das Konfigurationsprofil verschlüsselt ist. Mögliche Werte: ▶ `markiert` Das Konfigurationsprofil ist verschlüsselt. ▶ `unmarkiert` Das Konfigurationsprofil ist unverschlüsselt. Die Verschlüsselung des Konfigurationsprofils schalten Sie im Rahmen ***Konfigurations-Verschlüsselung*** ein und aus.
Verschlüsselung verifiziert	Zeigt, ob das Passwort des verschlüsselten Konfigurationsprofils mit dem im Gerät gespeicherten Passwort übereinstimmt. Mögliche Werte: ▶ `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	Zeigt die Versionsnummer der Geräte-Software, die das Gerät beim Speichern des Konfigurationsprofils ausgeführt hat.
Fingerprint	Zeigt die im Konfigurationsprofil gespeicherte Prüfsumme. Das Gerät berechnet die Prüfsumme beim Speichern der Einstellungen und fügt sie in das Konfigurationsprofil ein.
Fingerprint verifiziert	Zeigt, ob die im Konfigurationsprofil gespeicherte Prüfsumme gültig ist. Das Gerät berechnet die Prüfsumme des als „ausgewählt“ gekennzeichneten Konfigurationsprofils und vergleicht diese mit der Prüfsumme, die in diesem Konfigurationsprofil gespeichert ist. Mögliche Werte: ▶ `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: – Die Datei ist beschädigt. – Das Dateisystem auf dem externen Speicher ist inkonsistent. – 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. Das Gerät verifiziert die Prüfsumme ausschließlich dann korrekt, wenn das Konfigurationsprofil zuvor wie folgt gespeichert wurde: – auf einem baugleichen Gerät – mit derselben Software-Version, welche das Gerät derzeit ausführt **Anmerkung:** Diese Funktion kennzeichnet Änderungen an den Einstellungen des Konfigurationsprofils. Die Funktion bietet keinen Schutz davor, das Gerät mit geänderten Einstellungen zu betreiben.

Schaltflächen

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

Schaltfläche	Bedeutung
	Entfernt das in der Tabelle markierte Konfigurationsprofil aus dem permanenten Speicher (NVM) oder vom externen Speicher. Wenn das Konfigurationsprofil als „ausgewählt“ gekennzeichnet ist, hindert das Gerät Sie daran, das Konfigurationsprofil zu entfernen.
	Überträgt die Einstellungen aus dem flüchtigen Speicher (RAM) in das als „ausgewählt“ gekennzeichnete Konfigurationsprofil im permanenten Speicher (NVM). Wenn im Dialog ***Grundeinstellungen > Externer Speicher*** das Kontrollkästchen in Spalte ***Sichere Konfiguration beim Speichern*** markiert ist, erzeugt das Gerät eine Kopie des Konfigurationsprofils auf dem externen Speicher.
	Zeigt ein Untermenü mit folgenden Einträgen.
Speichern unter...	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“. **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. Wenn im Dialog ***Grundeinstellungen > Externer Speicher*** das Kontrollkästchen in Spalte ***Sichere Konfiguration beim Speichern*** markiert ist, kennzeichnet das Gerät auch das gleichnamige Konfigurationsprofil auf dem externen Speicher als „ausgewählt“.
Aktivieren	Lädt die Einstellungen des in der Tabelle markierten Konfigurationsprofils in den flüchtigen Speicher (RAM). ▶ Das Gerät trennt die Verbindung zur grafischen Benutzeroberfläche. ☐ Laden Sie die grafische Benutzeroberfläche neu. ☐ Melden Sie sich erneut an. ▶ Das Gerät verwendet die Einstellungen des Konfigurationsprofils ab sofort im laufenden Betrieb. Schalten Sie die Funktion ***Konfigurationsänderungen rückgängig machen*** 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. 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. 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.

Schaltfläche	Bedeutung
Auswählen	Kennzeichnet das in der Tabelle markierte Konfigurationsprofil als „ausgewählt“. Anschließend ist in Spalte ***Ausgewählt*** das Kontrollkästchen `markiert`. Das Gerät lädt die Einstellungen dieses Konfigurationsprofils beim Neustart oder beim Anwenden der Funktion ***Konfigurationsänderungen rückgängig machen*** in den flüchtigen Speicher (RAM). ▶ 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: – Die Konfigurations-Verschlüsselung im Gerät ist eingeschaltet. – Das Passwort des Konfigurationsprofils stimmt mit dem im Gerät gespeicherten Passwort überein. Andernfalls ist das Gerät außerstande, beim nächsten Neustart die Einstellungen des Konfigurationsprofils zu laden und zu entschlüsseln. Für diesen Fall legen Sie im Dialog ***Diagnose > System > Selbsttest*** fest, ob das Gerät mit Werkseinstellungen startet oder den Neustart abbricht und anhält. **Anmerkung:** Als „ausgewählt“ lassen sich ausschließlich Konfigurationsprofile kennzeichnen, die im permanenten Speicher (`NVM`) gespeichert sind. Wenn im Dialog ***Grundeinstellungen > Externer Speicher*** das Kontrollkästchen in Spalte ***Sichere Konfiguration beim Speichern*** markiert ist, kennzeichnet das Gerät auch das gleichnamige Konfigurationsprofil auf dem externen Speicher als „ausgewählt“.

Schaltfläche	Bedeutung

Importieren...	Öffnet den Dialog ***Importieren...***, um ein Konfigurationsprofile zu importieren.
	Voraussetzung ist, dass Sie das Konfigurationsprofil zuvor mit der Schaltfläche ***Exportieren...*** oder mit dem Link in Spalte ***Profilname*** exportiert haben.
	
	☐ 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.
	▶ `Externer Speicher`
	Das Gerät importiert das Konfigurationsprofil vom externen Speicher.
	☐ Wenn oben `PC/URL` ausgewählt ist, dann legen Sie im Rahmen ***Import profile from PC/URL*** die Datei des zu importierenden Konfigurationsprofils fest.
	– 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:
	`ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
	– Import von einem TFTP-Server
	Befindet sich die Datei auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
	`tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
	– 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:
	`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>`
	☐ Wenn oben `Externer Speicher` ausgewählt ist, dann legen Sie im Rahmen ***Import profile from external memory*** die Datei des zu importierenden Konfigurationsprofils fest.
	Wählen Sie in der Dropdown-Liste ***Profilname*** den Namen des zu importierenden Konfigurationsprofils.
	☐ Im Rahmen ***Ziel*** legen Sie fest, wo das Gerät das importierte Konfigurationsprofil speichert.
	Im Feld ***Profilname*** legen Sie den Namen fest, unter dem das Gerät das Konfigurationsprofil speichert.
	Im Feld ***Speicher-Typ*** legen Sie den Speicherort für das Konfigurationsprofil fest.
	Voraussetzung ist, dass Sie in der Dropdown-Liste ***Select source*** den Wert `PC/URL` ausgewählt haben.
	▶ `RAM`
	Das Gerät speichert das Konfigurationsprofil im flüchtigen Speicher (`RAM`) des Geräts. Dies ersetzt die `running-config`, 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.
	
	Beim Importieren eines Konfigurationsprofils übernimmt das Gerät die Einstellungen wie folgt:
	– 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 Gerät Module verwendet, lesen Sie auch den Hilfetext zum Dialog ***Grundeinstellungen > Module***.
	– 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 `running-config`-Konfigurationsprofil.
	
	Bezüglich Verschlüsselung des Konfigurationsprofil lesen Sie auch den Hilfetext zum Rahmen ***Konfigurations-Verschlüsselung***. Das Gerät importiert das Konfigurationsprofil unter den folgenden Bedingungen:
	– 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...	Exportiert das in der Tabelle markierte Konfigurationsprofil und speichert es als XML-Datei auf einem Remote-Server.
	Um die Datei auf Ihrem PC zu speichern, klicken Sie den Link in Spalte ***Profilname***, um den Speicherort zu wählen und den Dateinamen festzulegen.
	
	Das Gerät bietet Ihnen folgende Möglichkeiten, ein Konfigurationsprofil zu exportieren:
	▶ 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:
	– `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.
	– `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

Auf Lieferzustand zurücksetzen...	Setzt die Einstellungen im Gerät auf die voreingestellten Werte zurück. ▶ 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). ▶ Ist ein externer Speicher angeschlossen, löscht das Gerät die auf dem externen Speicher gespeicherten Konfigurationsprofile. ▶ Nach kurzer Zeit startet das Gerät neu mit den im Lieferzustand voreingestellten Werten.
Auf Default-Zustand zurücksetzen	Löscht die gegenwärtigen Betriebseinstellungen (`running config`) aus dem flüchtigen Speicher (`RAM`).

1.6 Externer Speicher

Dieser Dialog bietet Ihnen die Möglichkeit, Funktionen zu aktivieren, die das Gerät automatisch in Verbindung mit dem externen Speicher ausführt. Der Dialog zeigt außerdem den Betriebszustand sowie Identifizierungsmerkmale des externen Speichers.

Konfiguration

Parameter	Bedeutung
USB mode	Legt den Modus fest für die Kommunikation zwischen Gerät und externem Speichers. Damit Änderungen in diesem Feld wirksam werden, speichern Sie die Einstellungen permanent und starten Sie das Gerät neu. Mögliche Werte: ▶ `normal` (USB 2.0-Modus) Gerät und externer Speicher kommunizieren im High-Speed-Modus (480 Mbit/s). ▶ `compatibility` (USB 1.1-Kompatibilitätsmodus) Gerät und externer Speicher kommunizieren im Full-Speed-Modus (12 Mbit/s). **Anmerkung:** Der externe Speicher ACA21 arbeitet ausschließlich im USB 1.1-Kompatibilitätsmodus. Wenn Sie diesen externen Speicher verwenden, legen Sie den Wert `compatibility` fest.

Information

Parameter	Bedeutung
Momentaner USB-Modus	Zeigt den Modus, den das Gerät für die Kommunikation mit dem externen Speicher gegenwärtig verwendet. Mögliche Werte: ▶ `normal` (USB 2.0-Modus) Gerät und externer Speicher kommunizieren im High-Speed-Modus (480 Mbit/s). ▶ `compatibility` (USB 1.1-Kompatibilitätsmodus) Gerät und externer Speicher kommunizieren im Full-Speed-Modus (12 Mbit/s).

Tabelle

Parameter	Bedeutung
Typ	Zeigt den Typ des externen Speichers. Mögliche Werte: ▶ `usb` Externer USB-Speicher (ACA21/ACA22)

Parameter	Bedeutung
Status	Zeigt den Betriebszustand des externen Speichers. Mögliche Werte: ▶ `notPresent` Kein externer Speicher angeschlossen. ▶ `removed` Jemand hat den externen Speicher während des Betriebs aus dem Gerät entfernt. ▶ `ok` Der externe Speicher ist angeschlossenen und betriebsbereit. ▶ `outOfMemory` Der Speicherplatz auf dem externen Speicher ist belegt. ▶ `genericErr` Das Gerät hat einen Fehler festgestellt.
Beschreibbar	Zeigt, ob das Gerät Schreibzugriff auf den externen Speicher hat. Mögliche Werte: ▶ `markiert` Das Gerät hat Schreibzugriff auf den externen Speicher. ▶ `unmarkiert` Das Gerät hat ausschließlich Lesezugriff auf den externen Speicher. Möglicherweise ist auf den externen Speicher ein Schreibschutz aktiviert.
Automatisches Software-Update	Aktiviert/deaktiviert die automatische Aktualisierung der Geräte-Software während des Neustarts. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die automatische Aktualisierung der Geräte-Software während des Neustarts ist aktiviert. Das Gerät aktualisiert die Geräte-Software, wenn sich folgende Dateien auf dem externen Speicher befinden: – die Image-Datei der Geräte-Software – eine Textdatei „startup.txt“ mit dem Inhalt `autoUpdate=<Name_der_Image-Datei>.bin` ▶ `unmarkiert` Die automatische Aktualisierung der Geräte-Software während des Neustarts ist deaktiviert.

SSH-Key automatisch uploaden	Aktiviert/deaktiviert das Laden des DSA-/RSA-Schlüssels vom externen Speicher beim Neustart.
	
	Mögliche Werte:
	▶ `markiert` (Voreinstellung)
	Das Laden des DSA-/RSA-Schlüssels ist aktiviert.
	Beim Neustart lädt das Gerät den DSA-/RSA-Schlüssel vom externen Speicher, wenn sich auf dem externen Speicher folgende Dateien befinden:
	– SSH-RSA-Schlüssel-Datei
	– SSH-DSA-Schlüssel-Datei
	– eine Textdatei „startup.txt“ mit dem Inhalt
	`autoUpdateRSA=<Dateiname_des_SSH-RSA-Schlüssels>`
	`autoUpdateDSA=<Dateiname_des_SSH-DSA-Schlüssels>`
	Meldungen zeigt das Gerät auf der Systemkonsole an der V.24-Schnittstelle.
	▶ `unmarkiert`
	Das Laden des DSA-/RSA-Schlüssels ist deaktiviert.
	
	Anmerkung: Beim Laden des DSA/RSA-Schlüssels aus dem externen Speicher (`ENVM`) überschreibt das Gerät die im permanenten Speicher (`NVM`) vorhandenen Schlüssel.

Parameter	Bedeutung
Konfigurations-Priorität	Legt fest, von welchem Speicher das Gerät beim Neustart das Konfigurationsprofil lädt. Mögliche Werte: ▶ `disable` Das Gerät lädt das Konfigurationsprofil aus dem permanenten Speicher (`NVM`). ▶ `first` Das Gerät lädt das Konfigurationsprofil vom externen Speicher. Findet das Gerät auf dem externen Speicher kein Konfigurationsprofil, lädt es das Konfigurationsprofil aus dem permanenten Speicher (`NVM`). **Anmerkung:** Beim Laden des Konfigurationsprofils aus dem externen Speicher (`ENVM`) überschreibt das Gerät die Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (`NVM`). Wenn die Spalte ***Konfigurations-Priorität*** den Wert `first` hat und das Konfigurationsprofil unverschlüsselt ist, zeigt der Rahmen ***Sicherheits-Status*** im Dialog ***Grundeinstellungen >*** System einen Alarm. Im Dialog ***Diagnose > Statuskonfiguration > Sicherheitsstatus***, Registerkarte ***Global***, Spalte ***Überwachen***legen Sie fest, ob das Gerät den Parameter ***Unverschlüsselte Konfiguration vom externen Speicher laden*** überwacht.
Sichere Konfiguration beim Speichern	Aktiviert/deaktiviert das Erzeugen einer Kopie auf dem externen Speicher beim Speichern des Konfigurationsprofils. Mögliche Werte: ▶ `markiert` (Voreinstellung) Das Erzeugen einer Kopie ist aktiviert. Wenn Sie im Dialog ***Grundeinstellungen > Laden/ Speichern*** die Schaltfläche ***Speichern*** klicken, erzeugt das Gerät eine Kopie des Konfigurationsprofils auf dem aktiven externen Speicher. ▶ `unmarkiert` Das Erzeugen einer Kopie ist deaktiviert. Das Gerät erzeugt keine Kopie des Konfigurationsprofils.
Hersteller-ID	Zeigt den Namen des Speicher-Herstellers.
Revision	Zeigt die durch den Speicher-Hersteller vorgegebene Revisionsnummer.
Version	Zeigt die durch den Speicher-Hersteller vorgegebene Versionsnummer.
Name	Zeigt die durch den Speicher-Hersteller vorgegebene Produktbezeichnung.
Seriennummer	Zeigt die durch den Speicher-Hersteller vorgegebene Seriennumer.

Schaltflächen

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

1.7 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	Bezeichnung des Ports. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen Die folgenden Zeichen sind zulässig: – `<space>` – `0..9` – `a..z` – `A..Z` – `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`
Port an	Aktiviert/deaktiviert den Port. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der Port ist aktiv. ▶ `unmarkiert` Der Port ist inaktiv. Der Port sendet und empfängt keine Daten.
Zustand	Zeigt, ob der Port gegenwärtig physikalisch eingeschaltet oder ausgeschaltet ist. Mögliche Werte: ▶ `markiert` Der Port ist physikalisch eingeschaltet. ▶ `unmarkiert` Der Port ist physikalisch ausgeschaltet. Wenn die Funktion ***Port an*** aktiv ist, hat die ***Auto-Disable***-Funktion den Port ausgeschaltet. Die Einstellungen der Funktion ***Auto-Disable*** legen Sie im Dialog ***Diagnose > Ports >*** Auto-Disable fest.
Power-State (Port aus)	Legt fest, ob der Port physikalisch eingeschaltet oder ausgeschaltet ist, wenn Sie den Port mit der Funktion ***Port an***deaktivieren. Mögliche Werte: ▶ `markiert` Der Port bleibt physikalisch eingeschaltet. Ein angeschlossenes Gerät empfängt einen aktiven Link. ▶ `unmarkiert` (Voreinstellung) Der Port ist physikalisch ausgeschaltet.
Auto power down	Legt fest, wie sich der Port verhält, wenn kein Kabel angeschlossen ist. Mögliche Werte: ▶ `no-power-save` (Voreinstellung) Der Port bleibt aktiviert. ▶ `auto-power-down` Der Port schaltet in den Energiesparmodus. ▶ `unsupported` Der Port unterstützt diese Funktion nicht und bleibt aktiviert.

Parameter	Bedeutung
Automatische Konfiguration	Aktiviert/deaktiviert die automatische Auswahl des Betriebsmodus für den Port. Mögliche Werte: ▶ `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 ***Manuelle Konfiguration*** und in Spalte ***Manuelles Cable-Crossing (Auto. Konfig. aus)*** festlegen. ▶ Ausgegraute Darstellung Keine automatische Auswahl des Betriebsmodus.
Manuelle Konfiguration	Legt den Betriebsmodus des Ports fest, wenn die ***Automatische Konfiguration***-Funktion ausgeschaltet ist. Mögliche Werte: ▶ `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 **Anmerkung:** Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts und vom verwendeten Modul.
Link/ Aktuelle Betriebsart	Zeigt, welchen Betriebsmodus der Port gegenwärtig verwendet. Mögliche Werte: ▶ `-` 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 **Anmerkung:** Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts und vom verwendeten Modul.

Parameter	Bedeutung
Manuelles Cable-Crossing (Auto. Konfig. aus)	Legt die Belegung der Anschlüsse eines TP-Ports fest. Voraussetzung ist, dass die ***Automatische Konfiguration***-Funktion ausgeschaltet ist. Mögliche Werte: ▶ `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	Aktiviert/deaktiviert die Flusskontrolle auf dem Port. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Flusskontrolle auf dem Port ist aktiv. Auf dem Port ist das Senden und Auswerten von Pause-Paketen (Vollduplex-Betrieb) oder Kollisionen (Halbduplex-Betrieb) aktiviert. ☐ Um die Flusskontrolle im Gerät einzuschalten, aktivieren Sie zusätzlich die Funktion ***Flusskontrolle*** im Dialog ***Switching > Global***. ☐ 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. 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.
Trap senden (Link-Up/Down)	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Link-Status-Änderungen auf dem Port erkennt. Mögliche Werte: ▶ `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. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose > Statuskonfiguration > Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen.
Signal	Aktiviert/deaktiviert das Blinken der Port-LED. Diese Funktion bietet Ihnen die Möglichkeit, den Port im Feld zu identifizieren. Mögliche Werte: ▶ `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	Aktiviert/deaktiviert die ***Link-Überwachung***-Funktion auf dem Interface. Verwenden Sie die ***Link-Überwachung***-Funktion für Endgeräte, die kein Far End Fault Indication (FEFI) auf optischen Links unterstützen. Mögliche Werte: ▶ `markiert` Die ***Link-Überwachung***-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 ***Link-Überwachung***-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`.

[Netzlast]

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

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Netzlast [%]	Zeigt die gegenwärtige Netzlast in Prozent, bezogen auf die in Spalte ***Kontroll-Intervall [s]*** festgelegte Zeitspanne. Die Netzlast ist das Verhältnis der empfangen Datenmenge zur maximal möglichen Datenmenge bei der gegenwärtig konfigurierten Datenrate.
Unterer Grenzwert [%]	Legt einen unteren Grenzwert für die Netzlast fest. Unterschreitet die Netzlast des Ports diesen Wert, zeigt Spalte ***Alarm*** 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 Netzlast fest. Überschreitet die Netzlast des Ports diesen Wert, zeigt Spalte ***Alarm*** 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 Netzlast. Mögliche Werte: ▶ `markiert` Die Netzlast des Ports liegt unter dem in Spalte ***Unterer Grenzwert [%]*** oder über dem in Spalte ***Oberer Grenzwert [%]*** festgelegten Wert. Das Gerät sendet einen SNMP-Trap. ▶ `unmarkiert` Die Netzlast des Ports liegt über dem in Spalte ***Unterer Grenzwert [%]*** und unter dem in Spalte ***Oberer Grenzwert [%]*** festgelegten Wert. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose > Statuskonfiguration > Alarme (Traps)*** 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`.

1.8 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 ***Neustart***, um einen sofortigen oder einen verzögerten Neustart des Geräts auszulösen. Wenn sich das Konfigurationsprofil im flüchtigen Speicher (***Warnung***`RAM`) und das „ausgewählte“ Konfigurationsprofil im permanenten Speicher (NVM) unterscheiden, zeigt das Gerät den Dialog ***Warnung***. ☐ Um die Änderungen permanent zu speichern, klicken Sie im Dialog ***Warnung*** die Schaltfläche ***Ja***. ☐ Um die Änderungen zu verwerfen, klicken Sie im Dialog ***Warnung*** die Schaltfläche ***Nein***. ▶ Im Feld ***Neustart in*** 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 ***Diagnose > System > Selbsttest*** aktiviert ist. ▶ Das Gerät startet die Geräte-Software, die das Feld ***Stored version*** im Dialog ***Grundeinstellungen > Software*** anzeigt. ▶ Das Gerät lädt die Einstellungen aus dem „ausgewählten“ Konfigurationsprofil. Siehe Dialog ***Grundeinstellungen > Laden/Speichern***. **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 ***Switching >*** Filter für MAC-Adressen in Spalte ***Status*** den Wert `learned` haben.
ARP-Tabelle zurücksetzen	Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen. Siehe Dialog ***Diagnose > System > ARP***.
Port-Statistiken leeren	Setzt die Zähler der Portstatistik auf `0`. Siehe Dialog ***Grundeinstellungen > Port***, Registerkarte ***Statistiken***.
IGMP-Snooping-Daten zurücksetzen	Entfernt die IGMP-Snooping-Einträge und setzt den Zähler im Rahmen ***Information*** auf `0`. Siehe Dialog ***Switching > IGMP-Snooping > Global***.
Log-Datei löschen	Entfernt die protokollierten Einträge aus der Log-Datei. Siehe Dialog ***Diagnose > Bericht > System Log***.

Schaltfläche	Bedeutung
Persistente Log-Datei löschen	Entfernt die Log-Dateien vom externen Speicher. Siehe Dialog ***Diagnose > Bericht > Persistentes Ereignisprotokoll***.

2 Zeit

Das Menü enthält die folgenden Dialoge:

- Grundeinstellungen
- SNTP

2.1 Grundeinstellungen

Das Gerät ist mit einer gepufferten Hardware-Uhr ausgestattet. Diese führt die aktuelle Uhrzeit weiter, wenn die Stromversorgung ausfällt oder wenn Sie das Gerät von der Stromversorgung trennen. Nach dem Start des Geräts steht Ihnen die gegenwärtige Uhrzeit zur Verfügung, zum Beispiel für Log-Einträge.

Die Hardware-Uhr überbrückt eine Ausfallzeit der Stromversorgung von 3 Stunden. Voraussetzung dafür ist, dass die Stromversorgung das Gerät vorher mindestens 5 Minuten kontinuierlich gespeist hat. 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: ▶ `lokal` Systemuhr des Geräts. ▶ `sntp` Der SNTP-Client ist aktiviert und das Gerät ist durch einen SNTP-Server synchronisiert.
Lokaler Offset [min]	Legt die Differenz zwischen lokaler Zeit und ***Systemzeit (UTC)*** in Minuten fest: ***Lokaler Offset [min]*** = ***Systemzeit*** − ***Systemzeit (UTC)*** Mögliche Werte: ▶ `-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 ***Sommerzeit***-Modus ein/aus. Mögliche Werte: ▶ `An` Die ***Sommerzeit***-Modus ist eingeschaltet. Das Gerät wechselt automatisch zwischen Sommerzeit und Winterzeit. ▶ `Aus` (Voreinstellung) Die ***Sommerzeit***-Modus ist ausgeschaltet. Die Zeitpunkte, zu denen das Gerät zwischen Sommer- und Winterzeit umschaltet, sind in den Rahmen ***Sommerzeit Beginn*** und ***Sommerzeit Ende*** festgelegt.
Profil...	Öffnet den Dialog ***Profil...***. Dort wählen Sie ein vordefiniertes Profil für Beginn und Ende der Sommerzeit aus. Dieses Profil überschreibt die Einstellungen in den Rahmen ***Sommerzeit Beginn*** und ***Sommerzeit Ende***.

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: ▶ `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`)

Schaltflächen

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

2.2 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

2.2.1 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 ***SNTP Client***-Funktion des Geräts ein/aus. Mögliche Werte: ▶ `An` Die ***SNTP Client***-Funktion ist eingeschaltet. Das Gerät arbeitet als SNTP-Client. ▶ `Aus` (Voreinstellung) Die ***SNTP Client***-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: ▶ `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: ▶ `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 `syncToRemoteServer` zu `notSynchronized` ändert, wenn der Client keine Broadcast-Pakete empfängt. Mögliche Werte: ▶ `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: ▶ `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	Zeigt den Zustand des SNTP-Clients. Mögliche Werte: ▶ `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	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht. Mögliche Werte: ▶ `1..4` 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. 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. 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.
Name	Legt die Bezeichnung des SNTP-Servers fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
Adresse	Legt die IP-Adresse des SNTP-Servers fest. Mögliche Werte: ▶ Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)
Ziel-UDP-Port	Legt den UDP-Port fest, auf dem der SNTP-Server die Zeitinformationen erwartet. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `123`) Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Parameter	Bedeutung
Status	Zeigt den Verbindungsstatus zwischen SNTP-Client und SNTP-Server. Mögliche Werte: ▶ `erfolgreich` Das Gerät hat die Zeit erfolgreich mit dem SNTP-Server synchronisiert. ▶ `badDateEncoded` Die empfangene Zeitinformation enthält Protokollfehler, Synchronisation fehlgeschlagen. ▶ `other` – Für die IP-Adresse des SNTP-Servers ist der Wert `0.0.0.0` eingetragen, Synchronisation fehlgeschlagen. oder – Der SNTP-Client verwendet einen anderen SNTP-Server. ▶ `requestTimedOut` Das Gerät hat keine Antwort vom SNTP-Server erhalten, Synchronisation fehlgeschlagen. ▶ `serverKissOfDeath` 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 ***Request-Intervall [s]*** eingestellt nach, ob der Server noch überlastet ist. ▶ `serverUnsychronized` Der SNTP-Server ist weder auf eine lokale noch auf eine externe Referenzzeitquelle synchronisiert, Synchronisation fehlgeschlagen. ▶ `versionNotSupported` Die SNTP-Versionen auf Client und Server sind zueinander inkompatibel, Synchronisation fehlgeschlagen.
Aktiv	Aktiviert/deaktiviert die Verbindung zum SNTP-Server. Mögliche Werte: ▶ `markiert` Die Verbindung zum SNTP-Server ist aktiviert. Der SNTP-Client hat Zugriff auf den SNTP-Server. ▶ `unmarkiert` (Voreinstellung) 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.

2.2.2 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	Schaltet die ***SNTP Server***-Funktion des Geräts ein/aus. Mögliche Werte: ▶ `An` Die ***SNTP Server***-Funktion ist eingeschaltet. Das Gerät arbeitet als SNTP-Server. ▶ `Aus` (Voreinstellung) Die ***SNTP Server***-Funktion ist ausgeschaltet. Beachten Sie die Einstellung des Kontrollkästchens ***Server deaktivieren bei lokaler Zeitquelle*** im Rahmen ***Konfiguration***.

Konfiguration

Parameter	Bedeutung
UDP-Port	Legt die Nummer des UDP-Ports fest, auf dem der SNTP-Server des Geräts Anfragen anderer Clients entgegennimmt. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `123`) Ausnahme: Port `2222` ist für interne Funktionen reserviert.
Broadcast-Admin-Modus	Aktiviert/deaktiviert den Broadcast-Modus: ▶ `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	Legt die IP-Adresse fest, an die der SNTP-Server des Geräts die SNTP-Pakete im Broadcast-Modus sendet. Mögliche Werte: ▶ Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`) Broadcast- und Multicast-Adressen sind zulässig.
Broadcast-UDP-Port	Legt die Nummer des UDP-Ports fest, auf dem der SNTP-Server die SNTP-Pakete im Broadcast-Modus sendet. Mögliche Werte: ▶ `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: ▶ `0` Der SNTP-Server sendet die SNTP-Pakete im selben VLAN, in dem der Management-Zugriff auf das Gerät möglich ist. Siehe Dialog ***Grundeinstellungen > Netz***. ▶ `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: ▶ `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: ▶ `markiert` 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. ▶ `unmarkiert` (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: ▶ `disabled` Der SNTP-Server ist deaktiviert. ▶ `notSynchronized` Der SNTP-Server ist weder auf eine lokale noch auf eine externe Referenzzeitquelle synchronisiert. ▶ `syncToLocal` Der SNTP-Server ist synchronisiert auf die Hardware-Uhr des Geräts. ▶ `syncToRefclock` Der SNTP-Server ist synchronisiert auf eine externe Referenzzeitquelle, zum Beispiel PTP. ▶ `syncToRemoteServer` 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.

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 `administrator`, 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 ***Richtlinien überprüfen***. 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: ▶ `markiert` Das Benutzerkonto ist aktiv. Das Gerät akzeptiert die Anmeldung eines Benutzers mit dem Benutzernamen. ▶ `unmarkiert` (Voreinstellung) Das Benutzerkonto ist inaktiv. Das Gerät verweigert die Anmeldung eines Benutzers mit dem Benutzernamen. Wenn ausschließlich 1 Benutzerkonto mit der Berechtigung `administrator` 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: – `a..z` – `A..Z` – `0..9` – `#$%&'()*+,-./:;<=>?@_`` Die Mindestlänge des Passworts ist im Rahmen ***Konfiguration*** festgelegt. Das Gerät unterscheidet zwischen Groß- und Kleinschreibung. Wenn das Kontrollkästchen in Spalte ***Richtlinien überprüfen*** markiert ist, prüft das Gerät das Passwort gemäß der im Rahmen ***Passwort-Richtlinien*** festgelegten Richtlinien. Die Mindestlänge des Passwortes prüft das Gerät immer, auch wenn das Kontrollkästchen in Spalte ***Richtlinien überprüfen*** `unmarkiert` ist.

Parameter	Bedeutung
Rolle	Legt die Benutzer-Rolle fest, die den Zugriff des Benutzers auf die einzelnen Funktionen des Geräts regelt. Mögliche Werte: ▶ `unauthorized` 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. ▶ `guest` (Voreinstellung) Der Benutzer ist berechtigt, das Gerät zu überwachen. ▶ `auditor` Der Benutzer ist berechtigt, das Gerät zu überwachen und im Dialog ***Diagnose > Bericht >*** Audit Trail die Protokoll-Datei zu speichern. ▶ `operator` Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern – mit Ausnahme der Sicherheitseinstellungen für den Zugriff auf das Gerät. ▶ `administrator` Der Benutzer ist berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern. Den in der Antwort eines RADIUS-Servers übertragenen Service-Type weist das Gerät wie folgt einer Benutzer-Rolle zu: – `Administrative-User: administrator` – `Login-User: operator` – `NAS-Prompt-User: guest`
Benutzer gesperrt	Entsperrt das Benutzerkonto. Mögliche Werte: ▶ `markiert` 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. ▶ `unmarkiert` (ausgegraut) (Voreinstellung) Das Benutzerkonto ist entsperrt. Der Benutzer hat Management-Zugriff auf das Gerät.
Richtlinien überprüfen	Aktiviert/deaktiviert das Prüfen des Passworts. Mögliche Werte: ▶ `markiert` Das Prüfen des Passworts ist aktiviert. Beim Einrichten oder Ändern des Passworts prüft das Gerät das Passwort gemäß der im Rahmen ***Passwort-Richtlinien*** festgelegten Richtlinien. ▶ `unmarkiert` (Voreinstellung) Das Prüfen des Passworts ist deaktiviert.
SNMP-Authentifizierung	Legt das Authentifizierungsprotokoll fest, welches das Gerät beim Zugriff des Benutzers per SNMPv3 anwendet. Mögliche Werte: ▶ `hmacmd5` (Voreinstellung) Das Gerät verwendet für dieses Benutzerkonto das Protokoll HMAC-MD5. ▶ `hmacsha` Das Gerät verwendet für dieses Benutzerkonto das Protokoll HMAC-SHA.
SNMP-Verschlüsselung	Legt das Verschlüsselungsprotokoll fest, welches das Gerät beim Zugriff des Benutzers per SNMPv3 anwendet. Mögliche Werte: ▶ `kein` keine Verschlüsselung ▶ `des` (Voreinstellung) DES-Verschlüsselung ▶ `aesCfb128` AES-128-Verschlüsselung

Schaltflächen

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

Schaltfläche	Bedeutung
	Öffnet das Fenster ***Erzeugen***, um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld ***Benutzername*** 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	Legt die Authentifizierungsrichtlinie fest, die das Gerät beim Zugriff über die in Spalte ***Zugeordnete Anwendungen*** festgelegte Anwendung anwendet. 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. Mögliche Werte: ▶ `lokal` (Voreinstellung) Das Gerät authentifiziert die Benutzer mittels der lokalen Benutzerverwaltung. Siehe Dialog ***Gerätesicherheit > Benutzerverwaltung***. Der Authentifizierungliste `defaultDot1x8021AuthList` können Sie diesen Wert nicht zuweisen. ▶ `radius` Das Gerät authentifiziert die Benutzer mit einen RADIUS-Server im Netz. Den RADIUS-Server legen Sie im Dialog ***Netzsicherheit > RADIUS > Authentication-Server*** fest. ▶ `reject` Abhängig von der Richtlinie, die Sie zuerst anwenden, akzeptiert das Gerät die Authentifizierung oder lehnt die Authentifizierung ab. Mögliche Authentifizierungsszenarios sind: – Wenn die erste Richtlinie in der Authentifizierungsliste `lokal` 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 `lokal` 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 `radius` 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 `reject` ist, lehnen die Geräte die Benutzeranmeldung sofort ab, ohne eine andere Richtlinie anzuwenden. – Vergewissern Sie sich, dass die Authentifizierungsliste `defaultV24AuthList` mindestens eine Richtlinie enthält, die vom Wert `reject` abweicht. ▶ `ias` 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 ***Netzsicherheit > 802.1X Port-Authentifizierung > Integrierter Authentifikations-Server***. Der Authentifizierungliste `defaultDot1x8021AuthList` können Sie ausschließlich diesen Wert zuweisen.
Zugeordnete Anwendungen	Zeigt die zugeordneten Anwendungen. Wenn Benutzer mit der betreffenden Anwendung auf das Gerät zugreifen, wendet das Gerät die festgelegten Richtlinien für die Authentifizierung an. Um der Liste eine andere Anwendung zuzuordnen oder die Zuordnung aufzuheben, klicken Sie die Schaltfläche ☰ und dann den Eintrag ***Anwendungen zuordnen***. Jede Anwendung lässt sich immer genau einer Liste zuordnen.
Aktiv	Aktiviert/deaktiviert die Liste. Mögliche Werte: ▶ `markiert` Die Liste ist aktiviert. Das Gerät wendet die Richtlinien dieser Liste an, wenn Benutzer mit der betreffenden Anwendung auf das Gerät zugreifen. ▶ `unmarkiert` (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	Öffnet das Fenster ***Anwendungen zuordnen***. ▶ 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:  : 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. Verschieben Sie keinesfalls den Eintrag `WebInterface` in das linke Feld. Andernfalls bricht die Verbindung zum Gerät ab, sobald Sie die Schaltfläche ***Ok*** klicken.

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	Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 1 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte ***SNMP***. Mögliche Werte: ▶ `markiert` Server-Dienst ist aktiv. ▶ `unmarkiert` Server-Dienst ist inaktiv.
SNMPv2	Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 2 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte ***SNMP***. Mögliche Werte: ▶ `markiert` Server-Dienst ist aktiv. ▶ `unmarkiert` Server-Dienst ist inaktiv.
SNMPv3	Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit SNMP Version 3 ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte ***SNMP***. Mögliche Werte: ▶ `markiert` Server-Dienst ist aktiv. ▶ `unmarkiert` Server-Dienst ist inaktiv.
Telnet server	Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit Telnet ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte ***Telnet***. Mögliche Werte: ▶ `markiert` Server-Dienst ist aktiv. ▶ `unmarkiert` Server-Dienst ist inaktiv.
SSH server	Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit Secure Shell ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte ***SSH***. Mögliche Werte: ▶ `markiert` Server-Dienst ist aktiv. ▶ `unmarkiert` Server-Dienst ist inaktiv.
HTTP server	Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit der grafischen Bedienoberfläche über HTTP ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte ***HTTP***. Mögliche Werte: ▶ `markiert` Server-Dienst ist aktiv. ▶ `unmarkiert` Server-Dienst ist inaktiv.
HTTPS server	Zeigt, ob der Server-Dienst, der den Zugriff auf das Gerät mit der grafischen Bedienoberfläche über HTTPS ermöglicht, aktiv oder inaktiv ist. Siehe Registerkarte ***HTTP***. Mögliche Werte: ▶ `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	Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 1. Mögliche Werte: ▶ `markiert` (Voreinstellung) Zugriff ist aktiviert. ▶ `unmarkiert` Zugriff ist deaktiviert. Die Community-Namen legen Sie fest im Dialog ***Gerätesicherheit > Management-Zugriff >*** SNMPv1/v2 Community.
SNMPv2	Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 2. Mögliche Werte: ▶ `markiert` (Voreinstellung) Zugriff ist aktiviert. ▶ `unmarkiert` Zugriff ist deaktiviert. Die Community-Namen legen Sie fest im Dialog ***Gerätesicherheit > Management-Zugriff >*** SNMPv1/v2 Community.
SNMPv3	Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 3. Mögliche Werte: ▶ `markiert` (Voreinstellung) Zugriff ist aktiviert. ▶ `unmarkiert` Zugriff ist deaktiviert. Netzmanagementsysteme wie Industrial HiVision verwenden dieses Protokoll, um mit dem Gerät zu kommunizieren.
UDP-Port	Legt die Nummer des UDP-Ports fest, auf dem der SNMP-Agent Anfragen von Clients entgegennimmt. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `161`) Ausnahme: Port `2222` ist für interne Funktionen reserviert. Damit der SNMP-Agent nach einer Änderung den neuen Port verwendet, gehen Sie wie folgt vor: ☐ Klicken Sie die Schaltfläche ✔. ☐ Wählen Sie im Dialog ***Grundeinstellungen > Laden/Speichern*** das aktive Konfigurationsprofil. ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag ***Speichern***. ☐ Starten Sie das Gerät neu.
SNMPover802	Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP über IEEE-802. Mögliche Werte: ▶ `markiert` Zugriff ist aktiviert. ▶ `unmarkiert` (Voreinstellung) Zugriff ist deaktiviert. Die HiDiscovery-Software verwendet SNMP über IEEE-802, um Geräte ohne IP-Adresse zu erreichen.

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	Schaltet den Telnet-Server ein/aus. Mögliche Werte: ▶ `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. **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.

Konfiguration

Parameter	Bedeutung
TCP-Port	Legt die Nummer des TCP-Ports fest, auf dem das Gerät Telnet-Anfragen von den Clients entgegennimmt. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `23`) Ausnahme: Port `2222` ist für interne Funktionen reserviert. Nach Ändern des Ports startet der Server automatisch neu. Bestehende Verbindungen bleiben aufgebaut.
Verbindungen	Zeigt, wie viele Telnet-Verbindungen gegenwärtig zum Gerät aufgebaut sind.
Verbindungen (max.)	Legt fest, wie viele gleichzeitige Telnet-Verbindungen zum Gerät maximal möglich sind. Mögliche Werte: ▶ `1..5` (Voreinstellung: `5`)
Session-Timeout [min]	Legt die Timeout-Zeit in Minuten fest. Bei Inaktivität beendet das Gerät nach dieser Zeit die Sitzung des angemeldeten Benutzers. Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers wirksam. Mögliche Werte: ▶ `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.
Alternativ bietet Ihnen das Gerät die Möglichkeit, den DSA-/RSA-Schlüssel (Host Key) beim Neustart vom externen Speicher zu laden. Diese Funktion aktivieren Sie im Dialog ***Grundeinstellungen >*** Externer Speicher, Spalte ***SSH-Key automatisch uploaden***.

Funktion

Parameter	Bedeutung
Funktion	Schaltet den SSH-Server ein/aus. Mögliche Werte: ▶ `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. **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.

Konfiguration

Parameter	Bedeutung
TCP-Port	Legt die Nummer des TCP-Ports fest, auf dem das Gerät SSH-Anfragen von den Clients entgegennimmt. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `22`) Ausnahme: Port `2222` ist für interne Funktionen reserviert. Nach Ändern des Ports startet der Server automatisch neu. Bestehende Verbindungen bleiben aufgebaut.
Sessions	Zeigt, wie viele SSH-Verbindungen gegenwärtig zum Gerät aufgebaut sind.

Parameter	Bedeutung
Sessions (max.)	Legt fest, wie viele gleichzeitige SSH-Verbindungen zum Gerät maximal möglich sind. Mögliche Werte: ▶ `1..5` (Voreinstellung: `5`)
Session-Timeout [min]	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. Mögliche Werte: ▶ `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	Zeigt, ob ein DSA-Host-Key im Gerät vorhanden ist. Mögliche Werte: ▶ `markiert` Schlüssel vorhanden. ▶ `unmarkiert` Kein Schlüssel vorhanden.
RSA vorhanden	Zeigt, ob ein RSA-Host-Key im Gerät vorhanden ist. Mögliche Werte: ▶ `markiert` Schlüssel vorhanden. ▶ `unmarkiert` Kein Schlüssel vorhanden.
Erzeugen	Erzeugt einen Host-Key auf dem Gerät. Voraussetzung ist, dass der ***SSH***-Server ausgeschaltet ist. Länge des erzeugten Schlüssels: ▶ 2048 Bit (RSA) ▶ 1024 Bit (DSA) Damit der Server den generierten Host-Key verwendet, starten Sie den Server neu. Alternativ haben Sie die Möglichkeit, einen eigenen Schlüssel im PEM-Format auf das Gerät zu kopieren. Siehe Rahmen ***Key-Import***.
Löschen	Entfernt den Host-Key aus dem Gerät. Voraussetzung ist, dass der SSH-Server ausgeschaltet ist.

Parameter	Bedeutung
Betriebszustand	Zeigt, ob das Gerät gegenwärtig einen Host-Key erzeugt. Möglicherweise hat ein anderer Benutzer diese Aktion ausgelöst. Mögliche Werte: ▶ `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	Legt Pfad und Dateiname Ihres DSA-/RSA-Host-Keys fest.
	
	Das Gerät akzeptiert den DSA-/RSA-Schlüssel, wenn dieser die folgende Schlüssellänge aufweist:
	– 2048 bit (RSA)
	– 1024 bit (DSA)
	
	Das Gerät bietet Ihnen folgende Möglichkeiten, den Schlüssel in das Gerät zu kopieren:
	▶ 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:
	`ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
	▶ Import von einem TFTP-Server
	Befindet sich der Schlüssel 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 der Schlüssel auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in folgender Form 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>`

Start	Kopiert den im Feld ***URL*** 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	Schaltet für den Webserver das Protokoll ***HTTP*** ein/aus. Mögliche Werte: ▶ `An` (Voreinstellung) Das Protokoll ***HTTP*** ist eingeschaltet. Der Management-Zugriff auf das Gerät ist möglich über eine unverschlüsselte ***HTTP***-Verbindung. Wenn das Protokoll ***HTTPS*** ebenfalls eingeschaltet ist, leitet das Gerät die Anfrage für eine ***HTTP***-Verbindung automatisch auf eine verschlüsselte ***HTTPS***-Verbindung um. ▶ `Aus` Das Protokoll ***HTTP*** ist ausgeschaltet. Wenn das Protokoll ***HTTPS*** eingeschaltet ist, ist der Management-Zugriff auf das Gerät möglich über eine verschlüsselte ***HTTPS***-Verbindung. **Anmerkung:** Wenn die Protokolle ***HTTP*** und ***HTTPS*** ausgeschaltet sind, können Sie das Protokoll ***HTTP*** mit dem CLI-Kommando `http server` einschalten, um die grafische Benutzeroberfläche zu erreichen.

Konfiguration

Parameter	Bedeutung
TCP-Port	Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTP-Anfragen von den Clients entgegennimmt. Mögliche Werte: ▶ `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 ***HTTPS*** ein/aus. Mögliche Werte: ▶ `An` (Voreinstellung) Das Protokoll ***HTTPS*** ist eingeschaltet. Der Management-Zugriff auf das Gerät ist möglich über eine verschlüsselte ***HTTPS***-Verbindung. Wenn kein digitales Zertifikat vorhanden ist, erzeugt das Gerät ein digitales Zertifikat, bevor es das ***HTTPS***-Protokoll einschaltet. ▶ `Aus` Das Protokoll ***HTTPS*** ist ausgeschaltet. Wenn das Protokoll ***HTTP*** eingeschaltet ist, ist der Management-Zugriff auf das Gerät möglich über eine unverschlüsselte ***HTTP***-Verbindung. **Anmerkung:** Wenn die Protokolle ***HTTP*** und ***HTTPS*** ausgeschaltet sind, können Sie das Protokoll ***HTTPS*** mit dem CLI-Kommando `https server` 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 ***Fingerprint*** anzeigt. Mögliche Werte: ▶ `sha1` Das Feld ***Fingerprint*** zeigt den SHA1-Fingerprint des Zertifikats. ▶ `sha256` Das Feld ***Fingerprint*** zeigt den SHA256-Fingerprint des Zertifikats.
Fingerprint	Zeichenfolge des digitalen Zertifikats, das der Server verwendet. Wenn Sie die Einstellung im Feld ***Fingerprint-Typ*** ändern, klicken Sie anschließend die Schaltflächen 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 ***Zertifikat-Import***.
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	Legt Pfad und Dateiname des Zertifikats fest.
	
	Zulässig sind Zertifikate mit folgenden Eigenschaften:
	– X.509-Format
	– `.PEM`Dateinamenserweiterung
	– Base64-kodiert, umschlossen von
	• `-----BEGIN PRIVATE KEY-----` und `-----END PRIVATE KEY-----` sowie
	• `-----BEGIN CERTIFICATE-----` und `-----END CERTIFICATE-----`
	– RSA-Schlüssel mit 2048 bit Länge
	
	Das Gerät bietet Ihnen folgende Möglichkeiten, das Zertifikat in das Gerät zu kopieren:
	▶ 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:
	– `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 ***URL*** 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 ***IP-Zugriffsbeschränkung***-Funktion ein/aus. Mögliche Werte: ▶ `An` Die ***IP-Zugriffsbeschränkung***-Funktion ist eingeschaltet. Der Management-Zugriff auf das Gerät ist beschränkt. ▶ `Aus` (Voreinstellung) Die ***IP-Zugriffsbeschränkung***-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: ▶ `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 ***Netzmaske***. Mögliche Werte: ▶ Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)
Netzmaske	Legt den Bereich des in Spalte ***Adresse*** festgelegten Netzes fest. Mögliche Werte: ▶ 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 *Modbus TCP*-Server. Mögliche Werte: ▶ `markiert` (Voreinstellung) Zugriff ist aktiviert für nebenstehenden IP-Adressbereich. ▶ `unmarkiert` Zugriff ist deaktiviert.
Aktiv	Aktiviert/deaktiviert den Tabelleneintrag. Mögliche Werte: ▶ `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	Legt die Zeichenfolge fest, die das Gerät im Command Line Interface (CLI) am Beginn jeder Kommandozeile anzeigt. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..128 Zeichen (`0x20..0x7E`) inklusive Leerzeichen Wildcards – `%d` Datum – `%i` IP-Adresse – `%m` MAC-Adresse – `%p` Produktname – `%t` Uhrzeit Voreinstellung: `((GRS))` Änderungen an dieser Einstellung sind in aktiven CLI-Sitzungen sofort wirksam.
V.24-Timeout [min]	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. Mögliche Werte: ▶ `0..160` (Voreinstellung: `5`) Der Wert `0` deaktiviert die Funktion, der Benutzer bleibt bei Inaktivität angemeldet. Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers wirksam. Für Telnet und SSH legen Sie das Timeout fest im Dialog ***Gerätesicherheit > Management-Zugriff > Server***.

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	Schaltet die ***Login-Banner***-Funktion ein/aus. Mögliche Werte: ▶ `An` Die ***Login-Banner***-Funktion ist eingeschaltet. Das Gerät zeigt die im Feld ***Banner-Text*** festgelegte Textinformation den Benutzern, die sich mit dem Command Line Interface (CLI) auf dem Gerät anmelden. ▶ `Aus` (Voreinstellung) Die ***Login-Banner***-Funktion ist ausgeschaltet. Der CLI-Startbildschirm zeigt Informationen über das Gerät. Die Textinformation im Feld ***Banner-Text*** bleibt erhalten.

Banner-Text

Parameter	Bedeutung
Banner-Text	Legt die Textinformation fest, die das Gerät zu Beginn jeder Sitzung im Command Line Interface anzeigt. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..1024 Zeichen (`0x20..0x7E`) inklusive Leerzeichen ▶ `<Tabulator>` ▶ `<Zeilenumbruch>`
Verbleibende Zeichen	Zeigt, wie viele Zeichen im Feld ***Banner-Text*** noch für die Textinformation zur Verfügung stehen. Mögliche Werte: ▶ `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: ▶ `Write` Bei Anfragen mit dem nebenstehenden Community-Namen erhält die Anwendung Lese- und Schreibrechte auf dem Gerät. ▶ `Read` 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: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen `private` (Voreinstellung für Lese- und Schreibrechte) `public` (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 ***Pre-Login-Banner***-Funktion ein/aus. Mit der ***Pre-Login-Banner***-Funktion zeigt das Gerät im Login-Dialog der grafischen Benutzeroberfläche und des Command Line Interfaces eine Begrüßung oder einen Hinweis. Mögliche Werte: ▶ `An` Die ***Pre-Login-Banner***-Funktion ist eingeschaltet. Das Gerät zeigt im Login-Dialog den im Feld ***Banner-Text*** festgelegten Text. ▶ `Aus` (Voreinstellung) Die ***Pre-Login-Banner***-Funktion ist ausgeschaltet. Das Gerät zeigt im Login-Dialog keinen Text. Haben Sie im Feld ***Banner-Text*** 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: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..512 Zeichen (`0x20..0x7E`) inklusive Leerzeichen ▶ `<Tabulator>` ▶ `<Zeilenumbruch>`
Verbleibende Zeichen	Zeigt, wie viele Zeichen im Feld ***Banner-Text*** noch zur Verfügung stehen. Mögliche Werte: ▶ `512..0`

Schaltflächen

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

4 Netzsicherheit

Das Menü enthält die folgenden Dialoge:

- Netzsicherheit Übersicht
- Port-Sicherheit
- 802.1X Port-Authentifizierung
- RADIUS
- DoS
- ACL

4.1 Netzsicherheit Übersicht

Dieser Dialog zeigt die im Gerät verwendeten Netzsicherheits-Regeln.

Parameter

Parameter	Bedeutung
Port/VLAN	Legt fest, ob das Gerät VLAN- und/oder portbasierte Regeln anzeigt. Mögliche Werte: ▶ `Alle` (Voreinstellung) Das Gerät zeigt die von Ihnen festgelegten VLAN- und portbasierten Regeln. ▶ `Port: <Port-Nummer>` Das Gerät zeigt portbasierte Regeln für einen bestimmten Port. Diese Auswahl ist verfügbar, wenn Sie für diesen Port eine oder mehrere Regeln festgelegt haben. ▶ `VLAN: <VLAN-ID>` Das Gerät zeigt VLAN-basierte Regeln für ein bestimmtes VLAN. Diese Auswahl ist verfügbar, wenn Sie für dieses VLAN eine oder mehrere Regeln festgelegt haben.
ACL	Zeigt die ACL-Regeln in der Übersicht. Access-Control-Listen bearbeiten Sie im Dialog ***Netzsicherheit > ACL***.
Alle	Markiert die nebenstehenden Kontrollkästchen. Das Gerät zeigt die zugehörigen Regeln in der Übersicht.
Kein	Hebt die Markierung der nebenstehenden Kontrollkästchen auf. Das Gerät zeigt keine Regeln in der Übersicht.

Schaltflächen

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

4.2 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 erfassen 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 unbekannten Absendern. 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 ***Port-Sicherheit***-Funktion ein/aus. Mögliche Werte: ▶ `An` Die ***Port-Sicherheit***-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 ***Port-Sicherheit***-Funktion ist ausgeschaltet. Das Gerät vermittelt jedes empfangene Datenpaket, ohne den Absender zu prüfen.

Konfiguration

Parameter	Bedeutung
Auto-Disable	Aktiviert/deaktiviert die ***Auto-Disable***-Funktion für ***Port-Sicherheit***. Mögliche Werte: ▶ `markiert` Die ***Auto-Disable***-Funktion für ***Port-Sicherheit*** ist aktiv. Markieren Sie zusätzlich das Kontrollkästchen in Spalte ***Auto-Disable*** für die gewünschten Ports. ▶ `unmarkiert` (Voreinstellung) Die ***Auto-Disable***-Funktion für ***Port-Sicherheit*** ist inaktiv.

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Aktiv	Aktiviert/deaktiviert auf dem Port das Prüfen des Absenders. Mögliche Werte: ▶ `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 ***Funktion*** ein. ▶ `unmarkiert` (Voreinstellung) Das Gerät vermittelt jedes auf dem Port empfangene Datenpaket, ohne den Absender zu prüfen. **Anmerkung:** Wenn Sie das Gerät als aktiven Teilnehmer innerhalb eines MRP-Rings betreiben, empfehlen wir, die Markierung des Kontrollkästchens aufzuheben.
Auto-Disable	Aktiviert/deaktiviert die ***Auto-Disable***-Funktion für die Parameter, deren Einhaltung die ***Port-Sicherheit***-Funktion auf dem Port überwacht. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die ***Auto-Disable***-Funktion ist auf dem Port aktiv. Voraussetzung ist, dass im Rahmen ***Konfiguration*** das Kontrollkästchen ***Auto-Disable*** markiert ist. – Das Gerät schaltet den Port aus, wenn der Port unerwünschte Absender oder mehr Absender erfasst als in Spalte ***Dynamisches Limit*** festgelegt ist. Die „Link-Status“-LED des Ports blinkt 3× pro Periode. – Der Dialog ***Diagnose > Ports > Auto-Disable*** zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind. – Die ***Auto-Disable***-Funktion schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog ***Diagnose > Ports > Auto-Disable*** in Spalte ***Reset-Timer [s]*** eine Wartezeit für den betreffenden Port fest. ▶ `unmarkiert` Die ***Auto-Disable***-Funktion auf dem Port ist inaktiv.
Trap senden	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät auf dem Port Datenpakete von einem unerwünschten Absender verwirft. Mögliche Werte: ▶ `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. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose >*** Statuskonfiguration ***> Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen.

Parameter	Bedeutung
Trap-Intervall [s]	Legt die Wartezeit in Sekunden fest, die das Gerät nach Senden eines SNMP-Traps einhält, bis es den nächsten SNMP-Trap sendet. Mögliche Werte: ▶ `0..3600` (Voreinstellung: `0`) Der Wert `0` deaktiviert die Wartezeit.
Dynamisches Limit	Legt die Obergrenze fest für die Anzahl automatisch erfasster Absender (***Dynamische Einträge***). Sobald die Obergrenze erreicht ist, beendet das Gerät das „Lernen“ auf diesem Port. Passen Sie den Wert an die Anzahl der zu erwartenden Absender an. Wenn der Port mehr Absender erfasst als hier festgelegt ist, schaltet die Funktion ***Auto-Disable*** den Port aus. Voraussetzung ist, dass in Spalte ***Auto-Disable*** das Kontrollkästchen markiert ist und im Rahmen ***Konfiguration*** das Kontrollkästchen ***Auto-Disable***markiert ist. Mögliche Werte: ▶ `0` Deaktiviert das automatische Erfassen der Absender auf diesem Port. ▶ `1..600` (Voreinstellung: `600`)
Statisches Limit	Legt die Obergrenze fest für die Anzahl der mit dem Port verknüpften Absender (***Statische Einträge (/)***). Das ***Wizard***-Fenster unterstützt Sie dabei, den Port mit einem oder mehreren erwünschten Absendern zu verknüpfen. Mögliche Werte: ▶ `0..64` (Voreinstellung: `64`) Der Wert `0` verhindert, dass Sie einen Absender mit dem Port verknüpfen.
Dynamische Einträge	Zeigt, wie viele Absender das Gerät automatisch ermittelt hat. Siehe Dialog ***Wizard***, Feld ***Dynamische Einträge***.
Statische Einträge	Zeigt, wie viele Absender mit dem Port verknüpft sind. Siehe Dialog ***Wizard***, Feld ***Statische Einträge (/)***.
Last violating VLAN ID/MAC	Zeigt VLAN-ID und MAC-Adresse eines unerwünschten Absenders, dessen Datenpakete das Gerät an diesem Port zuletzt verworfen hat.
Gesendete Traps	Zeigt die Anzahl der auf diesem Port verworfenen Datenpakete, die das Gerät zum Senden eines SNMP-Traps veranlasst haben.

Schaltflächen

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

Schaltfläche	Bedeutung
	Öffnet den Dialog ***Wizard***. Im Dialog ***Wizard*** weisen Sie einem Port die zulässigen MAC-Adressen zu.

[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 ***Statische Einträge (/)*** zu übernehmen, klicken Sie die Schaltfläche ***Hinzufügen***.
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 ***Statische Einträge (/)*** zu übernehmen, klicken Sie die Schaltfläche ***Hinzufügen***.
Hinzufügen	Übernimmt die in den Feldern ***VLAN-ID*** und ***MAC-Adresse*** festgelegten Werte in das Feld ***Statische Einträge (/)***.
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 ***Statisches Limit***. **Anmerkung:** Eine MAC-Adresse, die sie diesem Port zuweisen, können Sie keinem weiteren Port zuweisen.
Entfernen	Entfernt die im Feld ***Statische Einträge (/)*** markierten Einträge.
	Verschiebt die im Feld ***Dynamische Einträge*** markierten Einträge in das Feld ***Statische Einträge (/)***.

Parameter	Bedeutung
	Verschiebt jeden Eintrag aus dem Feld ***Dynamische Einträge*** in das Feld ***Statische Einträge (/)***. Enthält das Feld ***Dynamische Einträge*** mehr Einträge als im Feld ***Statische Einträge (/)*** erlaubt sind, verschiebt das Gerät die vorderen Einträge, solange bis die Obergrenze erreicht ist.
Dynamische Einträge	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. Die Obergrenze für die Anzahl der Einträge legen Sie fest in der Tabelle, Feld ***Dynamisches Limit***. Die Schaltflächen und bieten Ihnen die Möglichkeit, Einträge aus diesem Feld in das Feld ***Statische Einträge (/)*** zu übernehmen. Damit verknüpfen Sie die betreffenden Absender mit dem Port.

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.

4.3 802.1X 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

4.3.1 802.1X Global

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

Funktion

Parameter	Bedeutung
Funktion	Schaltet die ***802.1X Port-Authentifizierung***-Funktion ein/aus. Mögliche Werte: ▶ `An` Die ***802.1X Port-Authentifizierung***-Funktion ist eingeschaltet. Das Gerät prüft den Zugriff angeschlossener Endgeräte auf das Netz. Die portbasierte Zugriffskontrolle ist eingeschaltet. ▶ `Aus` (Voreinstellung) Die ***802.1X Port-Authentifizierung***-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: ▶ `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 ***Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration***, Spalte ***Zugewiesene VLAN-ID*** festgelegten VLAN zugewiesen.
VLAN dynamisch erzeugen	Aktiviert/deaktiviert das automatische Einrichten des vom RADIUS-Authentication-Server zugewiesenen VLANs, falls dieses nicht existiert. Mögliche Werte: ▶ `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: ▶ `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 ***Monitor-Mode*** im Gerät aktiviert ist. Siehe Rahmen ***Konfiguration***.
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 ***Gerätesicherheit > Authentifizierungs-Liste*** fest. ☐ Um die Endgeräte über einen RADIUS-Server zu authentifizieren, weisen Sie der Liste `radius` die Richtline `8021x` zu. ☐ Um die Endgeräte über den Integrierten Authentifikationsserver (IAS) zu authentifizieren, weisen Sie der Liste `ias` die Richtline `8021x` zu.

Schaltflächen

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

4.3.2 802.1X 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	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 ***Port-Kontrolle*** der Wert `auto` festgelegt ist. Mögliche Werte: ▶ `markiert` Das Initialisieren des Ports ist aktiv. Sobald die Initialisierung abgeschlossen ist, ändert das Gerät den Wert wieder auf `unmarkiert`. ▶ `unmarkiert` (Voreinstellung) Das Initialisieren des Ports ist inaktiv. Das Gerät behält den gegenwärtigen Port-Status bei.
Port-Reauthentifizierung	Aktiviert/deaktiviert die einmalige Authentifizierungsanforderung. Wenden Sie diese Funktion ausschließlich dann an, wenn für den Port in Spalte ***Port-Kontrolle*** der Wert `auto` festgelegt ist. Das Gerät bietet Ihnen außerdem die Möglichkeit, das Endgerät periodisch aufzufordern, sich erneut anzumelden. Siehe Spalte ***Periodische Reauthentifizierung***. Mögliche Werte: ▶ `markiert` Die einmalige Authentifizierungsanforderung ist aktiv. Das Gerät fordert das Endgerät auf, sich erneut anzumelden. Anschließend ändert das Gerät den Wert wieder auf `unmarkiert`. ▶ `unmarkiert` (Voreinstellung) Die einmalige Authentifizierungsanforderung ist inaktiv. Das Gerät behält die Anmeldung des Endgeräts bei.
Authentifizierungs-Vorgang	Zeigt den gegenwärtigen Zustand des Authenticators (`Authenticator PAE state`). Mögliche Werte: ▶ `initialize` ▶ `disconnected` ▶ `connecting` ▶ `authenticating` ▶ `authenticated` ▶ `aborting` ▶ `held` ▶ `forceAuth` ▶ `forceUnauth`
Authentifizierungs-Zustand Backend	Zeigt den gegenwärtigen Zustand der Verbindung zum Authentifizierungs-Server (`Backend Authentication state`). Mögliche Werte: ▶ `request` ▶ `response` ▶ `erfolgreich` ▶ `fail` ▶ `timeout` ▶ `idle` ▶ `initialize`

Parameter	Bedeutung
Authentifizierungs-Zustand	Zeigt den gegenwärtigen Zustand der Authentifizierung auf dem Port (`Controlled Port Status`). Mögliche Werte: ▶ `authorized` Das Endgerät ist erfolgreich angemeldet. ▶ `unauthorized` Das Endgerät ist nicht angemeldet.
Port-Kontrolle	Legt fest, wie das Gerät den Zugriff auf das Netz gewährt (`Port control mode`). Mögliche Werte: ▶ `forceUnauthorized` 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. ▶ `auto` 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. ▶ `forceAuthorized` (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]	Legt die Zeitspanne in Sekunden fest, in welcher der Authenticator nach einem erfolglosen Anmeldeversuch keine erneute Anmeldung des Endgeräts akzeptiert (`Ruheperiode [s]`). Mögliche Werte: ▶ `0..65535` (Voreinstellung: `60`)
Sendeperiode [s]	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. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `30`)
Supplikant-Timeout [s]	Legt die Zeitspanne in Sekunden fest, innerhalb welcher der Authenticator auf die Anmeldung des Endgeräts wartet. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `30`)
Server-Timeout [s]	Legt die Zeitspanne in Sekunden fest, innerhalb welcher der Authenticator auf die Antwort des Authentication-Servers (RADIUS oder IAS) wartet. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `30`)
Requests (max.)	Legt fest, wie viele Male der Authenticator das Endgerät auffordert, sich anzumelden, bis die in Spalte ***Supplikant-Timeout [s]*** festgelegte Zeit erreicht ist. Das Gerät sendet sooft wie hier festgelegt ein EAP-Request/Identity-Datenpaket an das Endgerät. Mögliche Werte: ▶ `0..10` (Voreinstellung: `2`)
Zugewiesene VLAN-ID	Zeigt die ID des VLANs, die der Authenticator dem Port zugewiesen hat. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte ***Port-Kontrolle*** der Wert `auto`festgelegt ist. Mögliche Werte: ▶ `0..4042` (Voreinstellung: `0`) Die VLAN-ID, die der Authenticator den Ports zugewiesen hat, finden Sie im Dialog ***Netzsicherheit > 802.1X Port-Authentifizierung > Port-Clients***. Wenn für den Port in Spalte ***Port-Kontrolle*** der Wert `multiClient` festgelegt ist: Das Gerät weist das VLAN-Tag anhand der MAC-Adresse des Endgeräts zu, wenn es Datenpakete ohne VLAN-Tag empfängt.

Parameter	Bedeutung
Zuweisungsgrund	Zeigt den Grund für die Zuweisung der VLAN-ID. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte ***Port-Kontrolle*** der Wert `auto`festgelegt ist. Mögliche Werte: ▶ `notAssigned` (Voreinstellung) ▶ `radius` ▶ `guestVlan` ▶ `unauthenticatedVlan` Die VLAN-ID, die der Authenticator den Ports zugewiesen hat, finden Sie im Dialog ***Netzsicherheit > 802.1X Port-Authentifizierung > Port-Clients***.
Reauthentifizierungs-Periode [s]	Legt die Zeitspanne in Sekunden fest, nach welcher der Authenticator periodisch das Endgerät auffordert, sich erneut anzumelden. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `3600`)
Periodische Reauthentifizierung	Aktiviert/deaktiviert periodische Authentifizierungsanforderungen. Mögliche Werte: ▶ `markiert` Periodische Authentifizierungsanforderungen sind aktiv. Das Gerät fordert das Endgerät periodisch auf, sich erneut anzumelden. Die Zeitspanne legen Sie fest in Spalte ***Reauthentifizierungs-Periode [s]***. Diese Einstellung ist außer Kraft gesetzt, wenn der Authenticator dem Endgerät die ID eines Voice-, Unauthenticated- oder Gast-VLANs zugewiesen hat. ▶ `unmarkiert` (Voreinstellung) Periodische Authentifizierungsanforderungen sind inaktiv. Das Gerät behält die Anmeldung des Endgeräts bei.
Gast VLAN-ID	Legt die ID des VLANs fest, die der Authenticator dem Port zuweist, wenn sich das Endgerät während der in Spalte ***Gast-VLAN-Intervall*** festgelegten Zeit nicht anmeldet. Dieser Wert gilt ausschließlich dann, wenn für den Port in Spalte ***Port-Kontrolle*** der Wert `auto`festgelegt ist. Diese Funktion bietet Ihnen die Möglichkeit, Endgeräten ohne 802.1X-Unterstützung Zugriff auf ausgewählte Dienste im Netz zu gewähren. Mögliche Werte: ▶ `0` (Voreinstellung) Der Authenticator weist dem Port kein Gast-VLAN zu. ▶ `1..4042` **Anmerkung:** Weisen Sie dem Port ausschließlich ein im Gerät statisch eingerichtetes VLAN zu.
Gast-VLAN-Intervall	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 ***Gast VLAN-ID*** festgelegten Gast-VLAN zu. Mögliche Werte: ▶ `1..300` (Voreinstellung: `90`)
Unauthenticated-VLAN-ID	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 ***Port-Kontrolle*** der Wert `auto`festgelegt ist. Diese Funktion bietet Ihnen die Möglichkeit, Endgeräten ohne gültige Zugangsdaten Zugriff auf ausgewählte Dienste im Netz zu gewähren. Mögliche Werte: ▶ `0..4042` (Voreinstellung: `0`) Der Wert `0` bewirkt, dass der Authenticator dem Port kein Unauthenticated-VLAN zuweist. **Anmerkung:** Weisen Sie dem Port ausschließlich ein im Gerät statisch eingerichtetes VLAN zu.

Schaltflächen

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

4.3.3 802.1X 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	Zeigt den Grund für die Zuweisung des VLANs. Mögliche Werte: ▶ `default` ▶ `radius` ▶ `unauthenticatedVlan` ▶ `guestVlan` ▶ `monitorVlan` ▶ `invalid` Das Feld zeigt ausschließlich dann einen gültigen Wert, solange der Client authentifiziert ist.
Session-Timeout	Zeigt die verbleibende Zeit in Sekunden, bis die Anmeldung des Endgeräts abläuft. Dieser Wert gilt ausschließlich dann, wenn für den Port im Dialog ***Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration***, Spalte ***Port-Kontrolle*** der Wert `auto` festgelegt ist. Der Authentication-Server weist dem Gerät die Timeout-Zeit per RADIUS zu. Der Wert `0` bedeutet, dass der Authentication-Server kein Timeout zugewiesen hat.
Termination action	Zeigt die Aktion, die das Gerät bei Ablauf der Anmeldung ausführt. Mögliche Werte: ▶ `default` ▶ `reauthenticate`

Schaltflächen

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

4.3.4 802.1X 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.

4.3.5 802.1X 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	Zeigt den Zustand der Authentifizierung auf dem Port. Mögliche Werte: ▶ `erfolgreich` Die Authentifizierung war erfolgreich. ▶ `Fehler` Die Authentifizierung war fehlerhaft.
Zugriffs-Status	Zeigt, ob das Gerät dem Endgerät Zugriff auf das Netz gewährt. Mögliche Werte: ▶ `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	Zeigt die Art des VLAN, das der Authenticator dem Port zugewiesen hat. Mögliche Werte: ▶ `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	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. Mögliche Werte: ▶ `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.

4.3.6 802.1X 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: ▶ `markiert` Die Zugangsdaten sind aktiv. Ein Endgerät hat die Möglichkeit, sich mit diesen Zugangsdaten per 802.1x anzumelden. ▶ `unmarkiert` (Voreinstellung) Die Zugangsdaten sind inaktiv.

Schaltflächen

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

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

4.4 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

4.4.1 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 ***Netzsicherheit > RADIUS >*** Accounting-Server 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 ***Netzsicherheit > RADIUS > Authentication-Statistiken*** und die Statistik im Dialog ***Netzsicherheit > RADIUS > Accounting-Statistiken***.

4.4.2 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 ***Gerätesicherheit >*** Authentifizierungs-Liste den Wert `radius` in einer der Spalten ***Richtlinie 1*** bis ***Richtlinie 5*** 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
	Öffnet das Fenster ***Erzeugen***, um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld ***Index*** legen Sie die Index-Nummer fest. ▶ Im Feld ***Adresse***legen Sie die IP-Adresse des Servers fest.

4.4.3 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 ***Erzeugen***, um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld ***Index*** legen Sie die Index-Nummer fest. ▶ Im Feld ***Adresse***legen Sie die IP-Adresse des Servers fest.

4.4.4 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 ***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 (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.
Verworfene 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.
Verworfene 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.

4.4.5 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.
Verworfene 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.

4.5 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

4.5.1 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 vorzubreiten. 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: ▶ `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: ▶ `markiert` Der Filter ist aktiv. ▶ `unmarkiert` (Voreinstellung) Der Filter ist inaktiv.
SYN/FIN-Filter	Aktiviert/deaktiviert den SYN/FIN-Filter. Der SYN/FIN-Fter erkennt eingehende Datenpakete mit gleichzeitig gesetzten TCP-Flags SYN und FIN und verwirft diese. Mögliche Werte: ▶ `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: ▶ `markiert` Der Schutz ist aktiv. ▶ `unmarkiert` (Voreinstellung) Der Schutz ist inaktiv.

Parameter	Bedeutung
TCP-SYN-Protection	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. Mögliche Werte: ▶ `markiert` Der Schutz ist aktiv. ▶ `unmarkiert` (Voreinstellung) Der Schutz ist inaktiv.
L4-Port-Protection	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. Mögliche Werte: ▶ `markiert` Der Schutz ist aktiv. ▶ `unmarkiert` (Voreinstellung) Der Schutz ist inaktiv.
Min.-Header-Size-Filter	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. Mögliche Werte: ▶ `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	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. Mögliche Werte: ▶ `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: ▶ `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 ***Erlaubte Paketgröße [Byte]*** festgelegte Paketgröße überschreitet und verwirft diese. Mögliche Werte: ▶ `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 ***Anhand Paketgröße verwerfen***, wenn das Gerät eingehende Datenpakete verwerfen soll, deren Größe die maximal erlaubte Größe von ICMP-Paketen überschreitet. Mögliche Werte: ▶ `0..1472` (Voreinstellung: `512`)

Schaltflächen

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

4.6 ACL

In diesem Menü legen Sie die Einstellungen für Access-Control-Listen (ACL) fest. Access-Control-Listen enthalten Regeln, die das Gerät nacheinander auf den Datenstrom an seinen Ports oder VLANs anwendet.

Erfüllt ein Datenpaket die Kriterien einer oder mehrerer Regeln, wendet das Gerät die in der 1. zutreffenden Regel festgelegte Aktion auf das Datenpaket an. Die noch folgenden Regeln ignoriert das Gerät. Mögliche Aktionen sind:

- `permit`: Das Gerät vermittelt das Datenpaket an einen Port oder an ein VLAN.
- `deny`: Das Gerät verwirft das Datenpaket.

In der Voreinstellung vermittelt das Gerät jedes Datenpaket. Sobald Sie einem Port oder VLAN eine Access-Control-Liste zuweisen, ändert sich dort dieses Verhalten. An das Ende einer Access-Control-Liste fügt das Gerät eine implizite Deny-All-Regel ein. Demzufolge verwirft das Gerät Datenpakete, die keines der Regel-Kriterien erfüllen. Wenn Sie ein anderes Verhalten wünschen, fügen Sie am Ende Ihrer Access-Control-Listen eine „permit“-Regel ein.

Gehen Sie wie folgt vor, um Access-Control-Listen und Regeln einzurichten:

☐ Erzeugen Sie eine Regel und legen Sie die Einstellungen der Regel fest. Siehe Dialog ***Netzsicherheit > ACL > IPv4-Regel*** oder Dialog ***Netzsicherheit > ACL > MAC-Regel***.

☐ Weisen Sie die Access-Control-Liste den Ports und VLANs des Geräts zu. Siehe Dialog ***Netzsicherheit > ACL > Zuweisung***.

Das Menü enthält die folgenden Dialoge:

- ACL IPv4-Regel
- ACL MAC-Regel
- ACL Zuweisung

4.6.1 ACL IPv4-Regel

In diesem Dialog legen Sie die Regeln fest, die das Gerät auf IP-Datenpakete anwendet.

Eine Access-Control-Liste (Gruppe) enthält eine oder mehrere Regeln. Das Gerät wendet die Regeln einer Access-Control-Liste nacheinander an, zuerst die Regel mit dem kleinsten Wert in Spalte ***Index***.

Das Gerät bietet Ihnen die Möglichkeit, nach folgenden Kriterien zu filtern:
- Quell- oder Ziel-IP-Adresse eines Datenpakets
- Typ des übertragenden Protokolls
- Quell- oder Ziel-Port eines Datenpakets

Tabelle

Parameter	Bedeutung
Gruppenname	Zeigt den Namen der Access-Control-Liste. Die Access-Control-Liste enthält die Regeln.
Index	Zeigt die Nummer der Regel innerhalb der Access-Control-Liste. Enthält die Access-Control-Liste mehrere Regeln, wendet das Gerät die Regel mit dem kleinsten Wert zuerst an.
Alle Pakete filtern	Legt fest, auf welche IP-Datenpakete das Gerät die Regel anwendet. Mögliche Werte: ▶ `markiert` (Voreinstellung) Das Gerät wendet die Regel auf jedes IP-Datenpaket an. ▶ `unmarkiert` Das Gerät wendet die Regel auf IP-Datenpakete an, abhängig vom Wert in den Feldern ***Quell-IP-Adresse***,***Ziel-IP-Adresse*** und ***Protokoll***.
Quell-IP-Adresse	Legt die Quell-Adresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Mögliche Werte: ▶ `?.?.?.?` (Voreinstellung) Das Gerät wendet die Regel auf IP-Datenpakete mit beliebiger Quell-Adresse an. ▶ Gültige IPv4-Adresse Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Quell-Adresse an. Verwenden Sie das Zeichen `?` als Platzhalter. Beispiel `192.?.?.32`: Das Gerät wendet die Regel auf IP-Datenpakete an, deren Quell-Adresse mit `192.` beginnt und mit `.32` endet. ▶ Gültige IPv4-Adresse/Bitmaske Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Quell-Adresse an. Die inverse Bitmaske bietet Ihnen die Möglichkeit, den Adressbereich bitgenau festzulegen. Beispiel `192.168.1.1/0.0.0.127`: Das Gerät wendet die Regel auf IP-Datenpakete mit einer Quell-Adresse im Bereich von `192.168.1.0` bis ….`127`an.
Ziel-IP-Adresse	Legt die Ziel-Adresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Mögliche Werte: ▶ `?.?.?.?` (Voreinstellung) Das Gerät wendet die Regel auf IP-Datenpakete mit beliebiger Ziel-Adresse an. ▶ Gültige IPv4-Adresse Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Ziel-Adresse an. Verwenden Sie das Zeichen `?` als Platzhalter. Beispiel `192.?.?.32`: Das Gerät wendet die Regel auf IP-Datenpakete an, deren Quell-Adresse mit `192.` beginnt und mit `.32` endet. ▶ Gültige IPv4-Adresse/Bitmaske Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Ziel-Adresse an. Die inverse Bitmaske bietet Ihnen die Möglichkeit, den Adressbereich bitgenau festzulegen. Beispiel `192.168.1.1/0.0.0.127`: Das Gerät wendet die Regel auf IP-Datenpakete mit einer Ziel-Adresse im Bereich von `192.168.1.0` bis ….`127`an.

Parameter	Bedeutung
Protokoll	Legt den Protokolltyp der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Mögliche Werte: ▶ `any` (Voreinstellung) Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Protokolltyp zu berücksichtigen. ▶ `icmp` ▶ `igmp` ▶ `ip-in-ip` ▶ `tcp` ▶ `udp` ▶ `ip`
Quell-TCP/UDP-Port	Legt den Quell-Port der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass Sie in Spalte ***Protokoll*** den Wert `TCP` oder `UDP`festlegen. Mögliche Werte: ▶ `any` (Voreinstellung) Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Quell-Port zu berücksichtigen. ▶ `1..65535` Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten Quell-Port enthalten.
Ziel-TCP/UDP-Port	Legt den Ziel-Port der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass Sie in Spalte ***Protokoll*** den Wert `TCP` oder `UDP`festlegen. Mögliche Werte: ▶ `any` (Voreinstellung) Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Ziel-Port zu berücksichtigen. ▶ `1..65535` Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten Ziel-Port enthalten.
Aktion	Legt fest, wie das Gerät die IP-Datenpakete behandelt, wenn es die Regel anwendet. Mögliche Werte: ▶ `permit` (Voreinstellung) Das Gerät vermittelt die IP-Datenpakete. ▶ `deny` Das Gerät verwirft die IP-Datenpakete.
Protokolliere	Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog ***Diagnose > Bericht >*** System Log. Mögliche Werte: ▶ `markiert` Die Protokollierung ist aktiviert. Voraussetzung ist, dass Sie die Access-Control-Liste im Dialog ***Netzsicherheit > ACL >*** Zuweisung einem VLAN oder einem Port zuweisen. Das Gerät protokolliert in der Log-Datei im Intervall von 30 s, wie viele Male es eine Deny-Regel auf IP-Datenpakete angewendet hat. ▶ `unmarkiert` (Voreinstellung) Die Protokollierung ist deaktiviert. Das Gerät bietet Ihnen die Möglichkeit, für bis zu 128 Deny-Regeln diese Funktion zu aktivieren.

Schaltflächen

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

Schaltfläche	Bedeutung
	Öffnet das Fenster ***Erzeugen***, um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld ***Gruppenname*** legen Sie den Namen der Access-Control-Liste fest, der die Regel angehört. ▶ Im Feld ***Index*** legen Sie die Nummer der Regel innerhalb der Access-Control-Liste fest. Enthält die Access-Control-Liste mehrere Regeln, wendet das Gerät die Regel mit dem kleinsten Wert zuerst an.

4.6.2 ACL MAC-Regel

In diesem Dialog legen Sie die Regeln fest, die das Gerät auf MAC-Datenpakete anwendet.

Eine Access-Control-Liste (Gruppe) enthält eine oder mehrere Regeln. Das Gerät wendet die Regeln einer Access-Control-Liste nacheinander an, zuerst die Regel mit dem kleinsten Wert in Spalte ***Index***.

Das Gerät bietet Ihnen die Möglichkeit, nach Quell- oder Ziel-MAC-Adresse eines Datenpakets zu filtern.

Tabelle

Parameter	Bedeutung
Gruppenname	Zeigt den Namen der Access-Control-Liste. Die Access-Control-Liste enthält die Regeln.
Index	Zeigt die Nummer der Regel innerhalb der Access-Control-Liste. Enthält die Access-Control-Liste mehrere Regeln, wendet das Gerät die Regel mit dem kleinsten Wert zuerst an.
Alle Pakete filtern	Legt fest, auf welche MAC-Datenpakete das Gerät die Regel anwendet. Mögliche Werte: ▶ `markiert` (Voreinstellung) Das Gerät wendet die Regel auf jedes MAC-Datenpaket an. ▶ `unmarkiert` Das Gerät wendet die Regel auf MAC-Datenpakete an, abhängig vom Wert in den Feldern ***Quell-MAC-Adresse*** und ***Ziel-MAC-Adresse***.
Quell-MAC-Adresse	Legt die Quell-Adresse der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet. Mögliche Werte: ▶ `??:??:??:??:??:??` (Voreinstellung) Das Gerät wendet die Regel auf MAC-Datenpakete mit beliebiger Quell-Adresse an. ▶ Gültige MAC-Adresse Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quell-Adresse an. Verwenden Sie das Zeichen `?` als Platzhalter. Beispiel `00:11:??:??:??:??`: Das Gerät wendet die Regel auf MAC-Datenpakete an, deren Quell-Adresse mit `00:11` beginnt. ▶ Gültige MAC-Adresse/Bitmaske Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quell-Adresse an. Die Bitmaske bietet Ihnen die Möglichkeit, den Adressbereich bitgenau festzulegen. Beispiel `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: Das Gerät wendet die Regel auf MAC-Datenpakete mit einer Quell-Adresse im Bereich von `00:11:22:33:44:54` bis …`:57`an.
Ziel-MAC-Adresse	Legt die Ziel-Adresse der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet. Mögliche Werte: ▶ `??:??:??:??:??:??` (Voreinstellung) Das Gerät wendet die Regel auf MAC-Datenpakete mit beliebiger Ziel-Adresse an. ▶ Gültige MAC-Adresse Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Ziel-Adresse an. Verwenden Sie das Zeichen `?` als Platzhalter. Beispiel `00:11:??:??:??:??`: Das Gerät wendet die Regel auf MAC-Datenpakete an, deren Ziel-Adresse mit `00:11` beginnt. ▶ Gültige MAC-Adresse/Bitmaske Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quell-Adresse an. Die Bitmaske bietet Ihnen die Möglichkeit, den Adressbereich bitgenau festzulegen. Beispiel `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`: Das Gerät wendet die Regel auf MAC-Datenpakete mit einer Ziel-Adresse im Bereich von `00:11:22:33:44:54` bis …`:57`an.

Parameter	Bedeutung
Aktion	Legt fest, wie das Gerät die MAC-Datenpakete behandelt, wenn es die Regel anwendet. Mögliche Werte: ▶ `permit` (Voreinstellung) Das Gerät vermittelt die MAC-Datenpakete. ▶ `deny` Das Gerät verwirft die MAC-Datenpakete.
Protokolliere	Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog ***Diagnose > Bericht >*** System Log. Mögliche Werte: ▶ `markiert` Die Protokollierung ist aktiviert. Voraussetzung ist, dass Sie die Access-Control-Liste im Dialog ***Netzsicherheit > ACL >*** Zuweisung einem VLAN oder einem Port zuweisen. Das Gerät protokolliert in der Log-Datei im Intervall von 30 s, wie viele Male es eine Deny-Regel auf MAC-Datenpakete angewendet hat. ▶ `unmarkiert` (Voreinstellung) Die Protokollierung ist deaktiviert. Das Gerät bietet Ihnen die Möglichkeit, für bis zu 128 Deny-Regeln diese Funktion zu aktivieren.

Schaltflächen

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

Schaltfläche	Bedeutung
	Öffnet das Fenster ***Erzeugen***, um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld ***Gruppenname*** legen Sie den Namen der Access-Control-Liste fest, der die Regel angehört. ▶ Im Feld ***Index*** legen Sie die Nummer der Regel innerhalb der Access-Control-Liste fest. Enthält die Access-Control-Liste mehrere Regeln, wendet das Gerät die Regel mit dem kleinsten Wert zuerst an.

4.6.3 ACL Zuweisung

Dieser Dialog bietet Ihnen die Möglichkeit, den Ports und VLANs des Geräts eine oder mehrere Access-Control-Listen zuzuweisen. Mit dem Zuweisen einer Priorität legen Sie die Reihenfolge der Abarbeitung fest, sofern Sie einem Port oder VLAN mehrere Access-Control-Listen zugewiesen haben.

Das Gerät wendet die Regeln nacheinander an, und zwar in der durch den Regelindex vorgegebenen Reihenfolge. Die Priorität einer Gruppe legen Sie in Spalte ***Priorität***fest. Je kleiner die Zahl, desto höher die Priorität. Während der Bearbeitung wendet das Gerät die Regeln mit hoher Priorität vor Regeln mit niedriger Priorität an.

Beim Zuweisen der Access-Control-Listen zu Ports und VLANs ergeben sich folgende unterschiedliche ACL-Typen:
- Port-basierte IPv4-ACLs
- Port-basierte MAC-ACLs
- VLAN-basierte IPv4-ACLs
- VLAN-basierte MAC-ACLs

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 Zugriff auf die Management-Funktionen ist dann ausschließlich per CLI über die V.24-Schnittstelle des Geräts möglich.

Tabelle

Parameter	Bedeutung
Gruppenname	Zeigt den Namen der Access-Control-Liste. Die Access-Control-Liste enthält die Regeln.
Typ	Zeigt, ob die Access-Control-Liste MAC-Regeln oder IPv4-Regeln enthält. Mögliche Werte: ▶ `mac` Die Access-Control-Liste enthält MAC-Regeln. ▶ `ip` Die Access-Control-Liste enthält IPv4-Regeln. Access-Control-Listen mit IPv4-Regeln bearbeiten Sie im Dialog ***Netzsicherheit > ACL >*** IPv4-Regel. Access-Control-Listen mit MAC-Regeln bearbeiten Sie im Dialog ***Netzsicherheit >*** ACL ***> IPv4-Regel***.
Port	Zeigt den Port, dem die Access-Control-Liste zugewiesen ist. Das Feld bleibt leer, wenn die Access-Control-Liste einem VLAN zugewiesen ist.
VLAN-ID	Zeigt das VLAN, dem die Access-Control-Liste zugewiesen ist. Das Feld bleibt leer, wenn die Access-Control-Liste einem Port zugewiesen ist.
Richtung	Zeigt, dass das Gerät die Access-Control-Liste auf empfangene Datenpakete anwendet.
Priorität	Zeigt die Priorität der Access-Control-Liste. Anhand der Priorität legen Sie die Reihenfolge fest, in welcher das Gerät die Regeln der Access-Control-Listen auf den Datenstrom anwendet. Das Gerät wendet die Regeln beginnend mit Priorität `1` in aufsteigender Reihenfolge an. Mögliche Werte: ▶ `1..4294967295` Wenn eine Access-Control-Liste mit derselben Priorität einem Port und einem VLAN zugewiesen ist, wendet das Gerät die Regeln zuerst auf dem Port an.

Schaltflächen

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

Schaltfläche	Bedeutung
	Öffnet den Dialog ***Erzeugen***, um einem Port oder einem VLAN eine Regel zuzuweisen. ▶ Im Feld ***Port/VLAN*** legen Sie den Port oder die VLAN-ID fest. ▶ Im Feld ***Priorität*** legen Sie die Quell-MAC-Adresse der ARP-Regel fest. ▶ Im Feld ***Richtung***legen Sie fest, auf welche Datenpakete das Gerät die Regel anwendet. ▶ Im Feld ***Gruppenname*** legen Sie fest, welche Regel das Gerät dem Port oder dem VLAN zuweist.

5 Switching

Das Menü enthält die folgenden Dialoge:

- Switching Global
- Lastbegrenzer
- Filter für MAC-Adressen
- IGMP-Snooping
- MRP-IEEE
- GARP
- 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 ***Switching > Filter für MAC-Adressen***.

Parameter	Bedeutung
Flusskontrolle	Aktiviert/deaktiviert die Flusskontrolle im Gerät. Mögliche Werte: ▶ `markiert` Die Flusskontrolle ist im Gerät aktiviert. Aktivieren Sie die Flusskontrolle zusätzlich auf den erforderlichen Ports. Siehe Dialog ***Grundeinstellungen > Port***, Registerkarte ***Konfiguration***, Kontrollkästchen in Spalte ***Flusskontrolle***. ▶ `unmarkiert` (Voreinstellung) Die Flusskontrolle ist im Gerät deaktiviert. 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.
VLAN-Unaware-Modus	Aktiviert/deaktiviert den VLAN-Unaware-Modus. Mögliche Werte: ▶ `markiert` Der VLAN-Unaware-Modus ist aktiv. Das Gerät arbeitet im Bridging-Modus VLAN-unaware (802.1Q): – 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 ***Switching > VLAN > Konfiguration*** und ***Switching > VLAN > Port*** festgelegten VLAN-Einstellungen. Jeder Port ist VLAN `1` zugewiesen. – Das Gerät wertet die im Datenpaket enthaltene Prioritätsinformation aus. **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. ▶ `unmarkiert` (Voreinstellung) Der VLAN-Unaware-Modus ist inaktiv. Das Gerät arbeitet im Bridging-Modus VLAN-aware (802.1Q): – 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.

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	Legt den Grenzwert fest für Broadcast-, Multicast- und Unicast-Verkehr an diesem Port: Mögliche Werte: ▶ `0` (Voreinstellung) Die ***Lastbegrenzer***-Funktion ist auf diesem Port deaktiviert. ▶ `1..24414` bei 100 MBit/s `1..244140` bei 1000 MBit/s ☐ Wenn in Spalte ***Grenzwert Einheit*** der Wert `Prozent` festgelegt ist, legen Sie einen prozentualen Wert zwischen `1` und `100` fest. ☐ Wenn in Spalte ***Grenzwert Einheit*** der Wert `pps` festgelegt ist, legen Sie einen absoluten Wert fest. Die Lastbegrenzerfunktion berechnet den Grenzwert auf Grundlage von 512 Byte großen Datenpaketen. **Anmerkung:** Die tatsächlich zur Verfügung stehenden Betriebsmodi sind abhängig von der Ausstattung des Geräts und vom verwendeten Modul.
Grenzwert Einheit	Legt die Einheit für den Grenzwert fest: Mögliche Werte: ▶ `Prozent` (Voreinstellung) Der Grenzwert ist festgelegt in Prozent der Datenrate des Ports. ▶ `pps` Der Grenzwert ist festgelegt in Datenpaketen pro Sekunde.
Broadcast-Modus	Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Broadcast-Datenpakete. Mögliche Werte: ▶ `markiert` ▶ `unmarkiert` (Voreinstellung) Bei Überschreiten des Grenzwerts verwirft das Gerät an diesem Port die Überlast an Broadcast-Datenpaketen.
Multicast-Modus	Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Multicast-Datenpakete. Mögliche Werte: ▶ `markiert` ▶ `unmarkiert` (Voreinstellung) Bei Überschreiten des Grenzwerts verwirft das Gerät an diesem Port die Überlast an Multicast-Datenpaketen.

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: ▶ `learned` Adressfilter automatisch durch das Gerät eingerichtet anhand empfangener Datenpakete. ▶ `permanent` Adressfilter manuell eingerichtet. Der Adressfilter bleibt dauerhaft eingerichtet. ▶ `IGMP` Adressfilter automatisch eingerichtet durch IGMP-Snooping. ▶ `mgmt` MAC-Adresse des Geräts. Der Adressfilter ist gegen Veränderungen geschützt. ▶ `invalid` Löscht einen manuell eingerichteten Adressfilter. ▶ `MRP-MMRPMRP-MMRP` Multicast-Adressfilter automatisch eingerichtet durch MMRP.
<Port-Nummer>	Zeigt, wie der betreffende Port Datenpakete vermittelt, die an nebenstehende Zieladresse adressiert sind. Mögliche Werte: ▶ `-` Der Port vermittelt keine Datenpakete an die Zieladresse. ▶ `learned` Der Port vermittelt Datenpakete an die Zieladresse. Das Gerät hat den Filter anhand empfangener Datenpakete automatisch eingerichtet. ▶ `IGMP learned` Der Port vermittelt Datenpakete an die Zieladresse. Das Gerät hat den Filter anhand von IGMP automatisch eingerichtet. ▶ `unicast static` Der Port vermittelt Datenpakete an die Zieladresse. Ein Benutzer hat den Filter erzeugt. ▶ `multicast static` 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
	Öffnet das Fenster ***Erzeugen***, um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld ***Adresse*** legen Sie die Ziel-MAC-Adresse fest. ▶ Im Feld ***VLAN-ID*** legen Sie die ID des VLANs fest. ▶ Im Feld ***Port*** legen Sie den Port fest. – 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 ***Status*** den Wert `learned` 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 ***IGMP-Snooping***-Funktion im Gerät ein/aus. Mögliche Werte: ▶ `An` Die ***IGMP-Snooping***-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 ***IGMP-Snooping***-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: – 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: ▶ `0..`2^{31}`-1` Mit der Schaltfläche ***IGMP-Snooping-Daten zurücksetzen*** im Dialog ***Grundeinstellungen >*** Neustart oder mit dem CLI-Kommando `clear igmp-snooping`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 ***Information*** 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	Aktiviert/deaktiviert die ***IGMP-Snooping***-Funktion für dieses VLAN. Voraussetzung ist, dass die ***IGMP-Snooping***-Funktion global aktiviert ist. Mögliche Werte: ▶ `markiert` IGMP-Snooping ist für dieses VLAN aktiviert. Das VLAN ist am Multicast-Datenstrom angemeldet. ▶ `unmarkiert` (Voreinstellung) IGMP-Snooping ist für dieses VLAN deaktiviert. Das VLAN ist vom Multicast-Datenstrom abgemeldet.
Group-Membership-Intervall	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 ***Max. Antwortzeit***. Mögliche Werte: ▶ `2..3600` (Voreinstellung: `260`)
Max. Antwortzeit	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 ***Group-Membership-Intervall***. Mögliche Werte: ▶ `1..25` (Voreinstellung: `10`)
Fast-Leave-Admin-Modus	Aktiviert/deaktiviert die Fast-Leave-Funktion für dieses VLAN. Mögliche Werte: ▶ `markiert` Erhält das Gerät eine IGMP-Leave-Nachricht aus einer Multicast-Gruppe, entfernt es bei eingeschalteter Fast-Leave-Funktion sofort den Eintrag aus seiner Adresstabelle. ▶ `unmarkiert` (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	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. Mögliche Werte: ▶ `0` unbegrenztes Time-Out, keine Ablaufzeit ▶ `1..3600` (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	Aktiviert/deaktiviert die ***IGMP-Snooping***-Funktion für diesen Port. Voraussetzung ist, dass die ***IGMP-Snooping***-Funktion global aktiviert ist. Mögliche Werte: ▶ `markiert` IGMP-Snooping ist auf diesem Port eingeschaltet. Der Port ist am Multicast-Datenstrom angemeldet. ▶ `unmarkiert` (Voreinstellung) IGMP-Snooping ist auf diesem Port ausgeschaltet. Der Port ist vom Multicast-Datenstrom abgemeldet.
Group-Membership-Intervall	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. Mögliche Werte: ▶ `2..3600` (Voreinstellung: `260`) Wählen Sie den Wert im größer als den Wert in Spalte ***Max. Antwortzeit***.
Max. Antwortzeit	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. Mögliche Werte: ▶ `1..25` (Voreinstellung: `10`) Wählen Sie den Wert kleiner als den Wert in Spalte ***Group-Membership-Intervall***.
MRP-Ablaufzeit	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. Mögliche Werte: ▶ `0` unbegrenztes Time-Out, keine Ablaufzeit ▶ `1..3600` (Voreinstellung: `260`)
Fast-Leave-Admin-Modus	Aktiviert/deaktiviert die Fast-Leave-Funktion für diesen Port. Mögliche Werte: ▶ `markiert` Erhält das Gerät eine IGMP-Leave-Nachricht aus einer Multicast-Gruppe, entfernt es bei eingeschalteter Fast-Leave-Funktion sofort den Eintrag aus seiner Adresstabelle. ▶ `unmarkiert` (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	Aktiviert/deaktiviert den ***Static-Query-Port***-Modus. Mögliche Werte: ▶ `markiert` Der ***Static-Query-Port***-Modus ist aktiv. Der Port ist ein statischer Query-Port in den eingerichteten VLANs. ▶ `unmarkiert` (Voreinstellung) Der ***Static-Query-Port***-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>	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. Mögliche Werte: ▶ `-` 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 `Learn by LLDP` 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: ☐ Öffnet das ***Wizard***-Fenster. ☐ Markieren Sie auf der Seite ***Konfiguration*** das Kontrollkästchen `Static`. ▶ `P` = Learn by LLDP (einstellbar) Ein Benutzer hat den Port als `Learn by LLDP` 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: ☐ Öffnet das ***Wizard***-Fenster. ☐ Markieren Sie auf der Seite ***Konfiguration*** das Kontrollkästchen `Learn by LLDP`. ▶ `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: ☐ Öffnet das ***Wizard***-Fenster. ☐ Markieren Sie auf der Seite ***Konfiguration*** das Kontrollkästchen `Forward all`.

Parameter	Bedeutung
Display categories	Erhöht die Übersichtlichkeit der Anzeige. Die Tabelle hebt Zellen hervor, die den ausgewählten Wert enthalten. Dies erleichtert das bedarfsgerechte Analysieren und Sortieren der Tabelle. ▶ `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 ***Wizard***-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 (`Automatic`) zu senden.
Learn by LLDP	Legt den Status `Learn by LLDP` 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 `Forward all` für den Port fest. Mit der Einstellung `Forward all` 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: ▶ `markiert` Die IGMP-Snooping-Querier-Funktion ist für dieses VLAN aktiv. ▶ `unmarkiert` (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: ▶ `markiert` Der Snooping-Querier ist in diesem VLAN aktiv. ▶ `unmarkiert` 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: `0.0.0.0`)
Protokoll-Version	Zeigt die IGMP-Protokoll-Version der General-Query-Datenpakete. Mögliche Werte: ▶ `1` IGMP v1 ▶ `2` IGMP v2 ▶ `3` 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: ▶ `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: ▶ `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: `≥ (2x 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 exisitert 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: ▶ `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: ▶ `An` Bei global eingeschalteter MMRP-*`Funktion`* 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: ▶ `markiert` (Voreinstellung) Bei global und an diesem Port eingeschaltetem MMRP sendet und empfängt das Gerät MMRP-Nachrichten an diesem Port. ▶ `unmarkiert` 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: ▶ `markiert` Bei eingeschalteter Funktion und vorhandenem statischem MAC-Adressen-Filter im betreffenden VLAN bietet das Gerät die Möglichkeit, die MAC-Adressen-Attribute dynamisch zu registrieren. ▶ `unmarkiert` (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>	Legt die Verarbeitung der Service-Requirements für den Port fest. Mögliche Werte: ▶ `FA` Legt die Einstellung ForwardAll 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 ForwardAll-Ports eingerichtet hat. ▶ `F` Legt die Einstellung Forbidden am Port fest. Das Gerät blockiert die dynamischen MMRP-Service-Requirements für ForwardAll. Bei an diesem Port in diesem VLAN blockierten ForwardAll-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. ▶ `-` (Voreinstellung) Schaltet an diesem Port die Weiterleitungsfunktionen aus. ▶ `Learned` 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 ***Letzte empfangene MAC-Adresse*** 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 exisitert 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: ▶ `An` Normaler Teilnehmer. Die Applicant-State-Machine nimmt am Austausch von MMRP-Nachrichten teil. ▶ `Aus` (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: ▶ `An` Die Periodic-State-Machine ist eingeschaltet. Bei global eingeschalteter MVRP-*`Funktion`* überträgt das Gerät periodische MVRP-Nachrichten im Intervall von 1 Sekunde an die an MVRP teilnehmenden Ports. ▶ `Aus` (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: ▶ `markiert` (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. ▶ `unmarkiert` Schaltet die Teilnahme des Ports an MMRP aus.

Parameter	Bedeutung
Restricted VLAN registration	Aktiviert/deaktiviert die Funktion ***Restricted VLAN registration*** an diesem Port. Mögliche Werte: ▶ `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 ***Restricted VLAN registration*** 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 ***Letzte empfangene MAC-Adresse*** zurück.

5.6 GARP

Das Generic Attribute Registration Protocol (GARP) wurde durch die IEEE definiert, um ein generisches Framework bereitzustellen, in welchem Switches Attributwerte registrieren und de-registrieren, zum Beispiel VLAN-Kennungen und Multicast-Gruppen-Mitgliedschaften.

Wird ein Attribut für einen Teilnehmer gemäß dem GARP registriert oder deregistriert, wird der Teilnehmer auf der Grundlage spezifischer Regeln geändert. Bei den Teilnehmern handelt es sich um eine Reihe erreichbarer Endgeräte und Netzgeräte. Der definierte Satz von Teilnehmern zu einem bestimmten Zeitpunkt zusammen mit den zugehörigen Attributen stellt den Erreichbarkeitsbaum für die Teilmenge der Netztopologie dar. Das Gerät leitet die Datenpakete ausschließlich an die registrierten Endgeräte weiter. Durch die Registrierung von Stationen wird vermieden, dass versucht wird, Daten an nicht erreichbare Endgeräte zu senden.

Anmerkung: Vergewissern Sie sich vor der Aktivierung der GMRP-Funktion, dass die MMRP-Funktion deaktiviert ist.

Das Menü enthält die folgenden Dialoge:

- GMRP
- GVRP

5.6.1 GMRP

Das GARP Multicast Registration Protocol (GMRP) ist ein Generic Attribute Registration Protocol (GARP), das einen Mechanismus für die dynamische Registrierung von Gruppenmitgliedschaften durch Netzgeräte und Endgeräte bereitstellt. Die Geräte registrieren Informationen zur Gruppenmitgliedschaft mit den Geräten, die mit demselben LAN-Segment verbunden sind. GARP bietet den Geräten außerdem die Möglichkeit, die Informationen über Netzgeräte hinweg zu verbreiten, die erweiterte Filterdienste unterstützen.

GMRP und GARP sind durch IEEE 802.1P definierte Industriestandardprotokolle.

Funktion

Parameter	Bedeutung
Funktion	Aktiviert/deaktiviert die globale *GMRP*-Funktion des Geräts. Das Gerät nimmt am Austausch von GMRP-Nachrichten teil. Mögliche Werte: ▶ `An` GMRP ist aktiviert. ▶ `Aus` (Voreinstellung) Das Gerät ignoriert GMRP-Nachrichten.

Multicasts

Parameter	Bedeutung
Unbekannte Multicasts	Aktiviert/deaktiviert die unbekannten Multicast-Daten, die entweder geflutet oder verworfen werden sollen. Mögliche Werte: ▶ `Verwerfen` Das Gerät verwirft unbekannte Multicast-Daten. ▶ `An alle Ports senden` (Voreinstellung) Das Gerät sendet unbekannte Multicast-Daten an jeden Port.

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
GMRP aktiv	Aktiviert/deaktiviert die Teilnahme des Ports an *GMRP*. Voraussetzung ist, dass die *GMRP*-Funktion global aktiviert ist. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Teilnahme des Ports an *GMRP* ist aktiv. ▶ `unmarkiert` Die Teilnahme des Ports an *GMRP* ist inaktiv.

Parameter	Bedeutung
Service-Requirement	Legt die Ports fest, für welche die Multicast-Weiterleitung gilt. Mögliche Werte: ▶ `Alle unregistrierten Gruppen weiterleiten` (Voreinstellung) Das Gerät leitet die an *GMRP*-registrierte Multicast-MAC-Adressen gerichteten Daten an das VLAN weiter. Das Gerät leitet Daten an nicht registrierte Gruppen weiter. ▶ `Alle Gruppen weiterleiten` Das Gerät leitet an jede Gruppe gerichtete Daten weiter, unabhängig davon, ob es sich dabei um registrierte oder nicht registrierte Gruppen handelt.

Schaltflächen

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

5.6.2 GVRP

Das GARP VLAN Registration Protocol (GVRP) oder Generic VLAN Registration Protocol ist ein Protokoll zur Steuerung von Virtual Local Area Networks (VLANs) innerhalb eines größeren Netzes. GVRP ist ein Schicht-2-Netzprotokoll, das für die automatische Konfiguration von Geräten in einem VLAN-Netz verwendet wird.

GVRP ist eine GARP-Anwendung, die IEEE-802.1Q-konformes VLAN-Pruning bereitstellt und dynamische VLANs an 802.1Q-Trunk-Ports erstellt. Mit GVRP tauscht das Gerät Informationen zur VLAN-Konfiguration mit anderen GVRP-Geräten aus. Auf diese Weise reduziert das Gerät unnötigen Broadcast- und unbekannten Unicast-Verkehr. Das Austauschen der VLAN-Konfigurationsinformationen bietet Ihnen außerdem die Möglichkeit, die über 802.1Q-Trunk-Ports verbundene VLANs dynamisch zu erzeugen und zu verwalten.

Funktion

Parameter	Bedeutung
Funktion	Aktiviert/deaktiviert die *GVRP*-Funktion global im Gerät. Das Gerät nimmt am Austausch von *GVRP*-Nachrichten teil. Ist die Funktion deaktiviert, ignoriert das Gerät *GVRP*-Nachrichten. Mögliche Werte: ▶ `An` Die *GVRP*-Funktion ist eingeschaltet. ▶ `Aus` (Voreinstellung) Die *GVRP*-Funktion ist ausgeschaltet.

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
GVRP aktiv	Aktiviert/deaktiviert die Teilnahme des Ports an *GVRP*. Voraussetzung ist, dass die *GVRP*-Funktion global aktiviert ist. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Teilnahme des Ports an *GVRP* ist aktiv. ▶ `unmarkiert` Die Teilnahme des Ports an *GVRP* ist inaktiv.

Schaltflächen

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

5.7 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

5.7.1 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	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. Mögliche Werte: ▶ `0..7` (Voreinstellung: `0`) Im Dialog ***Switching > QoS/Priorität > 802.1D/p Zuweisung*** weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.
IP-DSCP-Wert für Management-Pakete	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. Mögliche Werte: ▶ `0 (be/cs0)..63` (Voreinstellung: `0 (be/cs0)`) 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-Precendence-Modell. Im Dialog ***Switching > QoS/Priorität > IP-DSCP-Zuweisung*** weisen Sie jedem IP-DSCP-Wert eine Verkehrsklasse zu.
Queues je Port	Zeigt die Anzahl der Warteschlangen pro Port. Das Gerät verfügt über 8Warteschlangen pro Port. Jede Warteschlange ist einer bestimmten Verkehrsklasse zugewiesen (Traffic Class nach IEEE 802.1D).

Schaltflächen

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

5.7.2 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	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 *Trust-Mode*. Mögliche Werte: ▶ `0..7` (Voreinstellung: `0`)
Trust-Mode	Legt fest, wie das Gerät ein empfangenes Datenpaket behandelt, wenn das Datenpaket eine Prioritätsinformation enthält. Mögliche Werte: ▶ `untrusted` Das Gerät vermittelt das Datenpaket gemäß der in Spalte *Port-Priorität* festgelegten Priorität. Das Gerät ignoriert die im Datenpaket enthaltene Prioritätsinformation. Im Dialog *Switching > QoS/Priorität > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu. ▶ `trustDot1p` (Voreinstellung) Das Gerät vermittelt das Datenpaket gemäß der Prioritätsinformation im VLAN-Tag. Im Dialog *Switching > QoS/Priorität > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu. ▶ `trustIpDscp` – Wenn das Datenpaket ein IP-Paket ist: Das Gerät vermittelt das Datenpaket gemäß des im Datenpaket enthaltenen IP-DSCP-Werts. Im Dialog *Switching > QoS/Priorität > IP-DSCP-Zuweisung* weisen Sie jedem IP-DSCP-Wert eine Verkehrsklasse zu. – Wenn das Datenpaket kein IP-Paket ist: Das Gerät vermittelt das Datenpaket gemäß der in Spalte *Port-Priorität* festgelegten Priorität. Im Dialog *Switching > QoS/Priorität > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu.
Untrusted-Traffic-Klasse	Zeigt die Verkehrsklasse, welche der in Spalte *Port-Priorität* festgelegten VLAN-Prioritätsinformation zugewiesen ist. Im Dialog *Switching > QoS/Priorität > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine Verkehrsklasse zu. Mögliche Werte: ▶ `0..7`

Schaltflächen

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

5.7.3 802.1D/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..7` `0`ist der Warteschlange mit der niedrigsten Priorität zugewiesen. `7`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`	2	`Best Effort` Normale Daten ohne Priorisierung
`1`	0	`Background` Zeitunkritische Daten und Hintergrunddienste
`2`	1	`Standard` Normale Daten
`3`	3	`Excellent Effort` Wichtige Daten
`4`	4	`Controlled Load` Verzögerungsempfindliche Daten mit hoher Priorität
`5`	5	`Video` Bildübertragung mit Verzögerungen und Jitter < 100 ms
`6`	6	`Voice` Sprachübertragung mit Verzögerungen und Jitter < 10 ms
`7`	7	`Network Control` Daten für Netzmanagement und Redundanzmechanismen

5.7.4 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..7` `0`ist der Warteschlange mit der niedrigsten Priorität zugewiesen. `7`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	2
1-7		2
8	CS1	0
9,11,13,15		0
10,12,14	AF11,AF12,AF13	0
16	CS2	1
17,19,21,23		1
18,20,22	AF21,AF22,AF23	1
24	CS3	3
25,27,29,31		3
26,28,30	AF31,AF32,AF33	3
32	CS4	4
33,35,37,39		4
34,36,38	AF41,AF42,AF43	4
40	CS5	5
41,42,43,44,45,47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7

DSCP-Wert	DSCP-Name	Traffic Class
57-63		7

5.7.5 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	Aktiviert/deaktiviert für diese Verkehrsklasse die Abarbeitung der Port-Warteschlange mit ***Strict priority***. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Abarbeitung der Port-Warteschlange mit ***Strict priority*** ist aktiv. – 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` Die Abarbeitung der Port-Warteschlange mit ***Strict priority*** ist inaktiv. Das Gerät verwendet „Weighted Fair Queuing“/“Weighted Round Robin“ (WRR), um die Port-Warteschlange abzuarbeiten. – 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 [%]	Legt die Mindestbandbreite für diese Verkehrsklasse fest, wenn das Gerät die Warteschlangen der Ports mit „Weighted Fair Queuing“ abarbeitet. Mögliche Werte: ▶ `0..100` (Voreinstellung: `0` = das Gerät reserviert für diese Verkehrsklasse keine Bandbreite) Der festgelegte Wert in Prozent bezieht sich auf die auf dem Port verfügbare Bandbreite. Wenn Sie für jede Verkehrsklasse die Funktion ***Strict priority*** ausschalten, steht auf dem Port die maximale Bandbreite für „Weighted Fair Queuing“ zur Verfügung. Die Summe der zugewiesenen Bandbreiten ist höchstens 100 %.

Schaltflächen

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

5.8 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 Gerät priorisiert den empfangenen Datenstrom in folgender Reihenfolge:

- Voice-VLAN
- Port-basiertes VLAN

Das Menü enthält die folgenden Dialoge:

- VLAN Global
- VLAN Konfiguration
- VLAN Port
- VLAN Voice

5.8.1 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 ***Switching > VLAN > Konfiguration***.
VLANs (max.)	Zeigt die maximale Anzahl der im Gerät einrichtbaren VLANs. Siehe Dialog ***Switching > VLAN > Konfiguration***.
VLANs	Anzahl der VLANs, die im Gerät gegenwärtig eingerichtet sind. Siehe Dialog ***Switching > VLAN > Konfiguration***. 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 ***Grundeinstellungen >*** Netz die VLAN-ID für die Management-Funktionen geändert haben.

5.8.2 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 128gleichzeitig 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 ***802.1X Port-Authentifizierung***. Siehe Dialog ***Netzsicherheit > 802.1X Port-Authentifizierung***. ▶ `permanent` VLAN eingerichtet durch den Benutzer. oder VLAN eingerichtet durch Funktion ***MRP***. Siehe Dialog ***Switching > L2-Redundanz > MRP***. VLANs mit dieser Einstellung bleiben nach einem Neustart eingerichtet, wenn Sie die Änderungen im permanenten Speicher speichern. ▶ `dynamicMvrp` VLAN eingerichtet durch Funktion ***MVRP***. Siehe Dialog ***Switching > MRP-IEEE > MVRP***. 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>	Legt fest, ob der betreffende Port Datenpakete des VLANs vermittelt und ob die Datenpakete eine VLAN-Markierung enthalten. Mögliche Werte: ▶ `-` (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 ***GVRP*** oder ***MVRP*** automatisch eingerichtet. ▶ `F` = Forbidden Der Port ist kein Mitglied des VLANs und vermittelt keine Datenpakete dieses VLANs. Das Gerät verhindert zudem, das der Port durch die Funktion ***MVRP*** 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 ***GVRP*** oder ***MVRP*** automatisch eingerichtet. **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.

Schaltflächen

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

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

5.8.3 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 ***Akzeptierte Datenpakete*** den Wert festlegen. Mögliche Werte: ▶ ID eines bereits eingerichteten VLANs (Voreinstellung: `1`) Wenn Sie die Funktion ***MRP*** 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: ▶ `admitAll` (Voreinstellung) Der Port akzeptiert Datenpakete sowohl mit als auch ohne VLAN-Tag. ▶ `admitOnlyVlanTagged` Der Port akzeptiert ausschließlich Datenpakete, die mit einer VLANID ≥ `1` markiert sind.
Ingress-Filtering	Aktiviert/deaktiviert die Eingangsfilterung. Mögliche Werte: ▶ `markiert` Die Eingangsfilterung ist aktiv. Das Gerät vergleicht die im Datenpaket enthaltene VLAN-ID mit den VLANs, in denen der Port Mitglied ist. Siehe Dialog ***Switching > VLAN > Konfiguration***. Stimmt die VLAN-ID im Datenpaket mit einem dieser VLANs überein, vermittelt das Gerät das Datenpaket. Andernfalls verwirft das Gerät das Datenpaket. ▶ `unmarkiert` (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.

5.8.4 VLAN Voice

Verwenden Sie die Voice-VLAN-Funktion, um den Sprach- und Datenverkehr an einem Port nach VLAN und/oder Priorität zu trennen. Ein wesentlicher Nutzen von Voice-VLAN liegt darin, in Zeiten mit erhöhtem Datenverkehrsaufkommen die Qualität des Sprachverkehrs sicherzustellen.

Das Gerät erkennt VoIP Telefone, die Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) verwenden. Dann fügt das Gerät den entsprechenden Switch-Port zur Mitgliedergruppe des konfigurierten Voice-VLANs hinzu. Die Mitgliedergruppe enthält entweder „getaggte“ oder „ungetaggte“ Mitglieder. Die Markierung hängt vom Schnittstellenmodus des Voice-VLANs ab (VLAN ID, Dot1p, None, Untagged).

Ein weiterer Nutzen der Voice-VLAN-Funktion liegt darin, dass das VoIP-Telefon Informationen zu VLAN-Kennung und Priorität via LLDP-Med vom Gerät erhält. Infolgedessen sendet das VoIP-Telefon die Sprachdaten entweder mit Prioritätsmarkierung oder unmarkiert. Dies ist abhängig vom festgelegten Interface-Modus des Voice-VLANs. Die Voice-VLAN-Funktion aktivieren Sie auf dem Port, an dem Sie das VoIP-Telefon anschließen.

Funktion

Parameter	Bedeutung
Funktion	Schaltet die Voice-VLAN-Funktion des Geräts global ein oder aus. Mögliche Werte: ▶ `An` ▶ `Aus` (Voreinstellung)

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Voice-VLAN-Modus	Legt fest, ob der Port empfangene Datenpakete ohne Voice-VLAN-Tag oder mit Voice-VLAN-Prioritätsinformationen überträgt oder verwirft. Mögliche Werte: ▶ `disabled` (Voreinstellung) Deaktiviert die Voice-VLAN-Funktion für diesen Tabelleneintrag. ▶ `kein` Ermöglicht es dem IP-Telefon, eine eigene Konfiguration zum Senden von unmarkiertem Sprachverkehr zu verwenden. ▶ `vlan/dot1p-priority` Der Port filtert Datenpakete des Voice-VLANs anhand der vlan- und dot1p-Prioritätsmarkierungen. ▶ `untagged` Der Port filtert Datenpakete ohne Voice-VLAN-Tag. ▶ `vlan` Der Port filtert Datenpakete des Voice-VLANs anhand des VLAN-Tags. ▶ `dot1p-priority` Der Port filtert Datenpakete des Voice-VLANs anhand der dot1p-Prioritätsmarkierungen. Wenn Sie diesen Wert auswählen, legen Sie zusätzlich in Spalte ***`Priorität`*** einen geeigneten Wert fest.

Parameter	Bedeutung
Data-Priority-Modus	Legt den Trust-Modus für Datenverkehr am jeweiligen Port fest. Das Gerät setzt diesen Modus für Datenverkehr auf dem Voice-VLAN ein, wenn es zugleich ein VoIP-Telefon wie auch einen PC ermittelt und diese Geräte dasselbe Kabel für die Datenübertragung verwenden. Mögliche Werte: ▶ `trust` (Voreinstellung) Mittels dieser Einstellung kann der Datenverkehr mit normaler Priorität ablaufen, wenn am Interface Sprachverkehr anliegt. ▶ `untrust` Wenn Sprachverkehr anliegt und der ***Voice-VLAN-Modus*** auf `dot1p-priority` gesetzt ist, verwendet der Datenverkehr die Priorität 0. Wenn das Interface ausschließlich Datenverkehr vermittelt, verwendet der Datenverkehr die normale Priorität.
Status	Zeigt den Status des Voice-VLANs am betreffenden Port an. Mögliche Werte: ▶ `markiert` Das Voice-VLAN ist eingeschaltet. ▶ `unmarkiert` Das Voice-VLAN ist ausgeschaltet.
VLAN-ID	Legt die ID des VLANs fest, für das der Tabelleneintrag gilt. Um den Datenverkehr an diese VLAN-ID unter Verwendung dieses Filters weiterzuleiten, legen Sie in Spalte ***Voice-VLAN-Modus*** den Wert `vlan` fest. Mögliche Werte: ▶ `0..4042`
Priorität	Legt die Voice-VLAN-Priorität des Ports fest. Voraussetzung ist, dass Sie in Spalte ***Voice-VLAN-Modus*** den Wert festlegen. Mögliche Werte: ▶ `0..7` ▶ `kein` Deaktiviert die Voice-VLAN-Priorität des Ports.
Bypass-Authentifizierung	Aktiviert den Voice-VLAN-Authentifizierungsmodus. Wenn Sie die Funktion deaktivieren und den Wert in Spalte ***Voice-VLAN-Modus*** auf `dot1p-priority` setzen, benötigen Sprachgeräte eine Authentifizierung. Mögliche Werte: ▶ `markiert` (Voreinstellung) Wenn die Funktion im Dialog ***Netzsicherheit > 802.1X Port-Authentifizierung > Global*** eingeschaltet ist, stellen Sie den Parameter ***Port-Kontrolle*** für diesen Port auf den Wert `multiClient`, bevor Sie diese Funktion aktivieren. Den Parameter ***Port-Kontrolle*** finden Sie im Dialog ***Netzsicherheit > 802.1X Port-Authentifizierung > Global***. ▶ `unmarkiert`

Schaltflächen

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

5.9 L2-Redundanz

Das Menü enthält die folgenden Dialoge:

- MRP
- Spanning Tree
- Link-Aggregation
- Link-Backup

5.9.1 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 ***MRP***-Funktion ein/aus. Wenn alle Parameter für den MRP-Ring konfiguriert sind, schalten Sie hier die Funktion ein. Mögliche Werte: ▶ `An` Die ***MRP***-Funktion ist eingeschaltet. Sind alle Geräte im MRP-Ring konfiguriert, ist die Redundanz aktiv. ▶ `Aus` (Voreinstellung) Die ***MRP***-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: ▶ `<Port-Nummer>` Nummer des Ring-Ports
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. ▶ `nicht verbunden` Keine Verbindung vorhanden.

Parameter	Bedeutung
Fixed backup	Aktiviert/deaktiviert die Backup-Port-Funktion für den ***Ring-Port 2***. **Anmerkung:** Bei der Umschaltung auf den primären Port wird ggf. die maximal zulässige Ring-Wiederherstellungszeit überschritten. Mögliche Werte: ▶ `markiert` Die Backup-Funktion für ***Ring-Port 2*** ist aktiviert. Ist der Ring geschlossen, schaltet der Ring-Manager auf den primären Ring-Port zurück. ▶ `unmarkiert` (Voreinstellung) Die Backup-Funktion für ***Ring-Port 2*** ist deaktiviert. Ist der Ring geschlossen, sendet der Ring-Manager weiterhin Daten an den sekundären Ring-Port.

Konfiguration

Parameter	Bedeutung
Ring-Manager	Schaltet die ***Ring-Manager***-Funktion ein/aus. Aktivieren Sie diese Funktion bei genau einem Gerät an den Enden der Linie. Mögliche Werte: ▶ `An` Die ***Ring-Manager***-Funktion ist eingeschaltet. Das Gerät arbeitet als Ring-Manager. ▶ `Aus` (Voreinstellung) Die ***Ring-Manager***-Funktion ist ausgeschaltet. Das Gerät arbeitet als Ring-Client.
Advanced mode	Aktiviert/deaktiviert den Advanced-Modus für schnelle Umschaltzeiten. Mögliche Werte: ▶ `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	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. Mögliche Werte: ▶ `500ms` ▶ `200ms` (Voreinstellung) 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.
VLAN-ID	Legt die ID des VLANs fest, das den Ring-Ports zugewiesen ist. Mögliche Werte: ▶ `0` (Voreinstellung) Kein VLAN zugewiesen. Weisen Sie im Dialog ***Switching > VLAN > Konfiguration***. den Ring-Ports für VLAN `1` den Wert `U` zu. ▶ `1..4042` VLAN zugewiesen. Wenn Sie den Ring-Ports ein noch nicht eingerichtetes VLAN zuweisen, erzeugt das Gerät das VLAN. Im Dialog ***Switching > VLAN > Konfiguration*** erzeugt das Gerät in der Tabelle einen Eintrag für das VLAN und weist den Ring-Ports den Wert `T`zu.

Information

Parameter	Bedeutung
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 Strecke 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. Schalten Sie die Funktion ***Ring-Manager*** 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.

5.9.2 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

5.9.2.1 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: ▶ `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 ***Spanning Tree***-Funktion verwendete Protokoll: Mögliche Werte: ▶ `rstp` Das Protokoll `RSTP` ist aktiv. Mit `RSTP` (IEEE 802.1Q-2005) ist die ***Spanning Tree***-Funktion in jedem eingerichteten VLAN wirksam.

Traps

Parameter	Bedeutung
Trap senden	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn eines der folgenden Ereignisse eintritt: – Eine andere Bridge übernimmt die Rolle der Root-Bridge. – Die Topologie ändert sich. Ein Port ändert ***Port-Status*** von ***forwarding*** zu ***discarding*** oder von ***discarding*** zu ***forwarding***. Mögliche Werte: ▶ `markiert` Das Senden von SNMP-Traps ist aktiv. ▶ `unmarkiert` (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv.

Bridge-Konfiguration

Parameter	Bedeutung
Bridge-ID	Zeigt die Bridge-ID des Geräts. Das Gerät mit der nummerisch niedrigsten Bridge-ID übernimmt die Rolle der Root-Bridge im Netz. Mögliche Werte: ▶ `<Bridge-Priorität> / <MAC-Adresse>` Wert im Feld ***Priorität*** / MAC-Adresse des Geräts

Parameter	Bedeutung
Priorität	Legt die Bridge-Priorität des Geräts fest. Mögliche Werte: ▶ `0..61440` in 4096er-Schritten (Voreinstellung: `32768`) Weisen Sie dem Gerät die nummerisch niedrigste Priorität im Netz zu, um es zur Root-Bridge zu bestimmen.
Hello-Time [s]	Legt die Zeit in Sekunden fest zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Datenpakete). Mögliche Werte: ▶ `1..2` (Voreinstellung: `2`) 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 ***Root-Information***. Aufgrund der Wechselwirkung mit dem Parameter ***Tx holds*** empfehlen wir, den voreinstellten Wert beizubehalten.
Forward-Verzögerung [s]	Legt die Verzögerungszeit für Zustandswechsel in Sekunden fest. Mögliche Werte: ▶ `4..30` (Voreinstellung: `15`) 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 ***Root-Information***. Im Protokoll RSTP handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus. Das ***Spanning Tree***-Protokoll verwendet den Parameter, um den Wechsel zwischen den Zuständen `disabled`, `discarding`, `learning`, `forwarding` zu verzögern.
Die Parameter ***Forward-Verzögerung [s]*** und ***Max age*** stehen in folgender Beziehung zueinander: ***Forward-Verzögerung [s]*** ≥ (***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.	
Max age	Legt die maximal zulässige Astlänge fest, d. h. die Anzahl der Geräte bis zur Root-Bridge. Mögliche Werte: ▶ `6..40` (Voreinstellung: `20`) 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 ***Root-Information***. Das ***Spanning Tree***-Protokoll verwendet den Parameter, um die Gültigkeit von STP-BPDUs in Sekunden festzulegen.
Tx holds	Begrenzt die maximale Übertragungsrate für das Senden von BPDUs. Mögliche Werte: ▶ `1..40` (Voreinstellung: `10`) 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. Das Gerät dekrementiert den Zähler jede Sekunde um `1`. In der folgenden Sekunde sendet das Gerät maximal `1` neue BPDU.

Parameter	Bedeutung
BPDU-Guard	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. Mögliche Werte: ▶ `markiert` Der ***BPDU-Guard*** ist aktiv. – Das Gerät wendet die Funktion auf manuell festgelegte Edge-Ports an. Bei diesen Ports ist im Dialog ***Switching > L2-Redundanz > Spanning Tree > Port***, Registerkarte ***CIST***, das Kontrollkästchen in Spalte ***Admin-Edge-Port*** markiert. – Empfängt ein Edge-Port eine STP-BPDU, schaltet das Gerät den Port aus. Im Dialog ***Grundeinstellungen > Port***, Registerkarte ***Konfiguration*** ist bei diesem Port das Kontrollkästchen in Spalte ***Port an*** `unmarkiert`. ▶ `unmarkiert` (Voreinstellung) Der ***BPDU-Guard*** ist inaktiv. Um den Status des Ports wieder auf den Wert `forwarding` zu setzen, gehen Sie wie folgt vor: ☐ Wenn der Port weiterhin BPDUs empfängt: – Heben Sie im Dialog ***Switching > L2-Redundanz > Spanning Tree > Port***, Registerkarte ***CIST***, die Markierung des Kontrollkästchens in Spalte ***Admin-Edge-Port*** auf. oder – Heben Sie im Dialog ***Switching > L2-Redundanz > Spanning Tree > Global*** die Markierung des Kontrollkästchen ***BPDU-Guard*** auf. ☐ Um den Port wieder einzuschalten, verwenden Sie die ***Auto-Disable***-Funktion. Alternativ gehen Sie wie folgt vor: – Öffnen Sie den Dialog ***Grundeinstellungen > Port***, Registerkarte ***Konfiguration***. – Markieren Sie das Kontrollkästchen in Spalte ***Port an***.
BPDU-Filter (alle Admin-Edge-Ports)	Aktiviert/deaktiviert die Filterung von STP-BPDUs auf jedem manuell festgelegten Edge-Port. Bei diesen Ports ist im Dialog ***Switching > L2-Redundanz > Spanning Tree > Port***, Registerkarte ***CIST***, das Kontrollkästchen in Spalte ***Admin-Edge-Port*** markiert. Mögliche Werte: ▶ `markiert` Der BPDU-Filter ist auf jedem Edge-Port aktiv. Die Funktion schließt diese Ports von ***Spanning Tree***-Operationen aus. – 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 ***BPDU-Filter Port*** im Dialog ***Switching > L2-Redundanz > Spanning Tree >*** Port.
Auto-Disable	Aktiviert/deaktiviert die ***Auto-Disable***-Funktion für die Parameter, deren Einhaltung der ***BPDU-Guard*** auf dem Port überwacht. Mögliche Werte: ▶ `markiert` Die ***Auto-Disable***-Funktion für den ***BPDU-Guard*** ist aktiv. – 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 ***Diagnose > Ports > Auto-Disable*** zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind. – Die ***Auto-Disable***-Funktion schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog ***Diagnose > Ports > Auto-Disable*** in Spalte ***Reset-Timer [s]*** eine Wartezeit für den betreffenden Port fest. ▶ `unmarkiert` (Voreinstellung) Die ***Auto-Disable***-Funktion für den ***BPDU-Guard*** 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 ***Bridge-Konfiguration***.
Forward-Verzögerung [s]	Zeigt die von der Root-Bridge vorgegebene Verzögerungzeit für Zustandswechsel in Sekunden. Mögliche Werte: ▶ `4..30` Das Gerät verwendet diesen vorgegebenen Wert. Siehe Rahmen ***Bridge-Konfiguration***. Im Protokoll RSTP handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus. Das ***Spanning Tree***-Protokoll verwendet den Parameter, um den Wechsel zwischen den Zuständen `disabled`, `discarding`, `learning`, `forwarding` 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 ***Spanning Tree***-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: ▶ `markiert` Das Gerät übernimmt gegenwärtig die Rolle der Root-Bridge. ▶ `unmarkiert` 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 `forwarding` 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.

5.9.2.2 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: ▶ `markiert` (Voreinstellung) ▶ `unmarkiert` Wenn die ***Spanning Tree***-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: ▶ `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 ***Grundeinstellungen > Port***, Registerkarte ***Konfiguration***. ▶ `manualFwd` Die ***Spanning Tree***-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: ▶ `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 ***Grundeinstellungen > Port***, Registerkarte ***Konfiguration***.
Port-Pfadkosten	Legt die Pfadkosten des Ports fest. Mögliche Werte: ▶ `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	Legt die Priorität des Ports fest. Mögliche Werte: ▶ `16..240` in 16er-Schritten (Voreinstellung: `128`) Der Wert repräsentiert die ersten 4 Bits der Port-ID.
Empfangene Bridge-ID	Zeigt die Bridge-ID des Geräts an, von dem dieser Port zuletzt eine STP-BPDU empfangen hat. Mögliche Werte: ▶ Für Ports mit der Rolle `designated` 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 `alternate`, `backup`, `master` und `root` sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle `designated`. ▶ 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 `designated` senden würde.
Empfangene Port-ID	Zeigt die Port-ID des Geräts an, von dem dieser Port zuletzt eine STP-BPDU empfangen hat. Mögliche Werte: ▶ Für Ports mit der Rolle `designated` 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 `alternate`, `backup`, `master` und `root` sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle `designated`. ▶ 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 `designated` senden würde.
Empfangene Port-Pfadkosten	Zeigt die Pfadkosten an, welche die übergeordnete Bridge von ihrem Root-Port zur Root-Bridge hat. Mögliche Werte: ▶ Für Ports mit der Rolle `designated` 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 `alternate`, `backup`, `master` und `root` sind diese Informationen im stationären Zustand (statische Topologie) identisch mit den Informationen der Port-Rolle `designated`. ▶ 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 `designated` senden würde.
Admin-Edge-Port	Aktiviert/deaktiviert den ***Admin-Edge-Port***-Modus. Verwenden Sie den ***Admin-Edge-Port***-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. Mögliche Werte: ▶ `markiert` Der ***Admin-Edge-Port***-Modus ist aktiv. Der Port ist mit einem Endgerät verbunden. – Nach Aufbau der Verbindung wechselt der Port in den Zustand `forwarding`, ohne zuvor in den Zustand `learning` zu wechseln. – Empfängt der Port eine STP-BPDU, deaktiviert das Gerät den Port, falls die BPDU-Guard-Funktion aktiv ist. Siehe Dialog ***Switching > L2-Redundanz > Spanning Tree >*** Global. ▶ `unmarkiert` (Voreinstellung) Der ***Admin-Edge-Port***-Modus ist inaktiv. Der Port ist mit einer anderen STP-Bridge verbunden. Nach Aufbau der Verbindung wechselt der Port in den Zustand `learning`, bevor er ggf. in den Zustand `forwarding` wechselt.

Parameter	Bedeutung
Auto-Edge-Port	Aktiviert/deaktiviert die automatische Erkennung, ob am Port ein Endgerät angeschlossen ist. Voraussetzung ist, dass das Kontrollkästchen in Spalte ***Admin-Edge-Port*** `unmarkiert` ist. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die automatische Erkennung ist aktiv. Nach Aufbau der Verbindung setzt das Gerät den Port nach 1,5 × ***Hello-Time [s]*** in den Zustand `forwarding` (in der Voreinstellung 1,5 × 2 s), falls der Port währenddessen keine STP-BPDU empfängt. ▶ `unmarkiert` Die automatische Erkennung ist inaktiv. Nach Aufbau der Verbindung setzt das Gerät den Port nach ***Max age*** in den Zustand `forwarding`. (Voreinstellung: 20 s)
Oper-Edge-Port	Zeigt, ob am Port ein Endgerät oder eine STP-Bridge angeschlossen ist. Mögliche Werte: ▶ `markiert` Am Port ist ein Endgerät angeschlossen. Der Port empfängt keine STP-BPDUs. ▶ `unmarkiert` Am Port ist eine STP-Bridge angeschlossen. Der Port empfängt STP-BPDUs.
Oper PointToPoint	Zeigt, ob der Port über eine direkte Vollduplex-Verbindung mit einem STP-Gerät verbunden ist. Mögliche Werte: ▶ `true` Der Port ist über eine Vollduplex-Verbindung direkt mit einem STP-Gerät verbunden. Die direkte, dezentrale Kommunikation zwischen 2 Bridges bewirkt kurze Rekonfigurationszeiten ▶ `false` Der Port ist auf andere Weise verbunden, zum Beispiel über eine Halbduplex-Verbindung oder über einen Hub.
BPDU-Filter Port	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 ***Admin-Edge-Port*** markiert. Mögliche Werte: ▶ `markiert` Der BPDU-Filter ist auf dem Port aktiv. Die Funktion schließt den Port von ***Spanning Tree***-Operationen aus. – Das Gerät sendet keine STP-BPDUs auf dem Port. – Das Gerät verwirft jede STP-BPDU, die es auf dem Port empfängt. ▶ `unmarkiert` (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 ***Switching > L2-Redundanz > Spanning Tree > Global***, Rahmen ***Bridge-Konfiguration***. Wenn das Kontrollkästchen ***BPDU-Filter (alle Admin-Edge-Ports)*** markiert ist, dann ist der BPDU-Filter auf dem Port noch aktiv.
Status BPDU-Filter	Zeigt, ob der BPDU-Filter auf dem Port aktiv ist. Mögliche Werte: ▶ `markiert` Der BPDU-Filter ist auf dem Port aktiv aufgrund der folgenden Einstellungen: – Das Kontrollkästchen in Spalte ***BPDU-Filter Port*** ist markiert. und/oder – Das Kontrollkästchen in Spalte ***BPDU-Filter (alle Admin-Edge-Ports)*** ist markiert. Siehe Dialog ***Switching > L2-Redundanz > Spanning Tree > Global***, Rahmen ***Bridge-Konfiguration***. ▶ `unmarkiert` Der BPDU-Filter ist auf dem Port inaktiv.

Parameter	Bedeutung
BPDU flood	Aktiviert/deaktiviert den ***BPDU flood***-Modus auf dem Port, auch wenn die ***Spanning Tree***-Funktion auf dem Port inaktiv ist. Voraussetzung ist, dass auch der ***BPDU flood***-Modus für diese Ports aktiv ist. Mögliche Werte: ▶ `markiert` Der ***BPDU flood***-Modus ist aktiv. Das Gerät flutet STP-BPDUs, die es auf dem Port empfängt, an die Ports, für die ***Spanning Tree***-Funktion inaktiv ist. ▶ `unmarkiert` (Voreinstellung) Der ***BPDU flood***-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	Schaltet die Überwachung auf STP-BPDUs auf dem Port ein/aus. Voraussetzung ist, dass die Funktion ***Loop guard*** inaktiv ist. 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 `designated`. Mögliche Werte: ▶ `markiert` Überwachung auf STP-BPDUs ist eingeschaltet. – 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 `discarding` anstatt auf `root`. – Bleiben STP-BPDUs mit besserer Pfadinformation zur Root-Bridge aus, setzt das Gerät den Zustand des Ports nach 2 × ***Hello-Time [s]*** ▶ `unmarkiert` (Voreinstellung) Überwachung auf STP-BPDUs ist inaktiv.
TCN guard	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. Mögliche Werte: ▶ `markiert` Überwachung auf ‚Topology Change Notifications‘ ist eingeschaltet. – 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. ▶ `unmarkiert` (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	Schaltet die Überwachung auf Loops auf dem Port ein/aus. Voraussetzung ist, dass die Funktion ***Root guard*** inaktiv ist. 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 `alternate`, `backup` und `root`. Mögliche Werte: ▶ `markiert` 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. – Empfängt der Port eine Zeitlang keine STP-BPDUs, setzt das Gerät den Zustand des Ports auf den Wert `discarding` und den Wert in Spalte ***Loop-Zustand*** auf `true`. – Empfängt der Port anschließend wieder STP-BPDUs, setzt das Gerät den Zustand des Ports auf einen Wert gemäß ***Port-Rolle*** und den Wert in Spalte ***Loop-Zustand*** auf `false`. ▶ `unmarkiert` (Voreinstellung) Überwachung auf Loops ist ausgeschaltet. Empfängt der Port eine Zeitlang keine STP-BPDUs, setzt das Gerät den Zustand des Ports auf den Wert `forwarding`.

Parameter	Bedeutung
Loop-Zustand	Zeigt, ob der Loop-Status des Ports inkonsistent ist. Mögliche Werte: ▶ `true` Der Loop-Status des Ports ist inkonsistent: – Der Port empfängt keine STP-BPDUs und die Funktion ***Loop guard*** ist eingeschaltet. – Das Gerät setzt den Status des Ports auf den Wert `discarding`. Damit verhindert das Gerät mögliche Loops. ▶ `false` 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 ***Loop-Zustand*** von `false` auf `true` gesetzt hat.
Übergänge aus Loop-Zustand	Zeigt, wie viele Male das Gerät den Wert in Spalte ***Loop-Zustand*** von `true` auf `false` gesetzt hat.
BPDU guard effect	Zeigt, ob der Port als Edge-Port eine STP-BPDU empfangen hat. Voraussetzung: – Der Port ist ein manuell festgelegter Edge-Port. Im Dialog ***Port*** ist bei diesem Port das Kontrollkästchen in Spalte ***Admin-Edge-Port*** `markiert`. – Im Dialog ***Switching > L2-Redundanz > Spanning Tree > Global*** ist die BPDU-Guard-Funktion aktiv. Mögliche Werte: ▶ `markiert` Der Port ist Edge-Port und hat eine STP-BPDU empfangen. Das Gerät deaktiviert den Port. Im Dialog ***Grundeinstellungen > Port***, Registerkarte ***Konfiguration*** ist bei diesem Port das Kontrollkästchen in Spalte ***Port an*** `unmarkiert`. ▶ `unmarkiert` Der Port ist Edge-Port und hat keine STP-BPDU empfangen oder der Port ist kein Edge-Port. Um den Status des Ports wieder auf den Wert `forwarding` zu setzen, gehen Sie wie folgt vor: ☐ Wenn der Port weiterhin BPDUs empfängt: – Heben Sie in der Registerkarte ***CIST*** die Markierung des Kontrollkästchens in Spalte ***Admin-Edge-Port*** auf. oder – Heben Sie im Dialog ***Switching > L2-Redundanz > Spanning Tree > Global*** die Markierung des Kontrollkästchen ***BPDU-Guard*** auf. ☐ Um den Port zu aktivieren, gehen Sie wie folgt vor: – Öffnen Sie den Dialog ***Grundeinstellungen > Port***, Registerkarte ***Konfiguration***. – Markieren Sie das Kontrollkästchen in Spalte ***Port an***.

Schaltflächen

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

5.9.3 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: ▶ `markiert` (Voreinstellung) Die LAG-Instanz befindet sich in einem aktiven Zustand und verarbeitet den Datenverkehr entsprechend den festgelegten Werten. ▶ `unmarkiert` 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 ***Spanning Tree***-Protokoll auf diesem LAG-Interface. Nach dem Erzeugen der Link-Aggregation-Instanz in der Tabelle fügt das Gerät den Port automatisch zum Dialog ***Switching > L2-Redundanz > Spanning Tree > Port*** hinzu. Mögliche Werte: ▶ `markiert` (Voreinstellung) Das Aktivieren des STP-Modus in diesem Dialog aktiviert den Port auch im Dialog ***Switching > L2-Redundanz > Spanning Tree > Port***. ▶ `unmarkiert` Das Deaktivieren des STP-Modus in diesem Dialog deaktiviert den Port auch im Dialog ***Switching > L2-Redundanz > Spanning Tree > Port***. Voraussetzung ist, dass Sie die Funktion global im Dialog ***Switching > L2-Redundanz >*** Spanning Tree ***> Global*** einschalten.
Statische Link-Aggregation	Aktiviert/deaktiviert die Funktion ***Statische Link-Aggregation*** auf dem LAG-Interface. Mögliche Werte: ▶ `markiert` Wenn die Funktion ***Statische Link-Aggregation*** eingeschaltet ist, unterstützt sie ein stabiles Netz und der Administrator gibt manuell den Aggregation-Status des Ports weiter. ▶ `unmarkiert` (Voreinstellung) Das Gerät gibt den Aggregation-Status des Ports automatisch weiter.

Parameter	Bedeutung
Aktive Ports (min.)	Legt fest, wie viele aktive Ports das Gerät für die Link-Aggregation-Gruppe verwendet. Mögliche Werte: ▶ `1..2` (Voreinstellung: `2`) ▶ `1..4` (Voreinstellung: `4`) **Anmerkung:** Die tatsächlich zur Verfügung stehende Anzahl an Ports ist abhängig vom Gerät.
Typ	Zeigt den Typ der verwendeten Link-Aggregation-Gruppe. Mögliche Werte: ▶ `static` Das Gerät verwendet statische Aggregation am Port, ***Statische Link-Aggregation*** ist eingeschaltet. ▶ `dynamic` Das Gerät verwendet dynamische Aggregation am Port, ***Statische Link-Aggregation*** ist ausgeschaltet.
Trap senden (Link-Up/Down)	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Link-Status-Änderungen auf dem Interface erkennt. Mögliche Werte: ▶ `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. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose >*** Statuskonfiguration ***> Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen.
LACP admin key	Legt den Administrativ-Wert für den lokalen Schlüssel an dieser LAG fest. 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. Mögliche Werte: ▶ `0..65535` (Voreinstellung: `0`)
LACP-Collector max. Verzögerung [µs]	Legt die maximale Verzögerungszeit für den Datenpaket -Sammler in Mikrosekunden fest. 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. Mögliche Werte: ▶ `0..65535` (Voreinstellung: `0`)
Port	Zeigt die Mitglieder des Ports der LAG-Instanz.
Status	Zeigt den LAG-Status des Ports. Mögliche Werte: ▶ `aktiv` Der Port nimmt aktiv in der LAG-Instanz teil. ▶ `inaktiv` Der Port nimmt nicht in der LAG-Instanz teil.
LACP Aktiv	Aktiviert/deaktiviert LACP an diesem Port. Mögliche Werte: ▶ `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	Legt den Wert des Administrativ-Schlüssels für den Aggregation-Port fest. 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. Mögliche Werte: ▶ `0..65535` (Voreinstellung: `0`) Wenn der Port zu einer LAG gehört, wählen Sie diesen Wert entsprechend dem Operativ-Schlüssel für die LAG.
LACP actor admin state	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. Mögliche Werte: ▶ `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 Übertragungsrate. 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. Wenn der Parameter nicht festgelegt ist, zeigt das Gerät folgende Werte für die LACPDU-Parameter: – `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	Legt die Port-Priorität für den LACP-Actor fest. Mögliche Werte: ▶ `0..65535` (Voreinstellung: `128`) Der Port mit dem niedrigeren Wert hat die höhere Priorität.

Parameter	Bedeutung
LACP partner port admin key	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. Die LAG verwendet Schlüssel, um Partner-Ports die Mitgliedschaft zuzuweisen. Legen Sie für Partner, die in derselben LAG teilnehmen, denselben Schlüsselwert fest. Mögliche Werte: ▶ `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. Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten: – ***LACP Partner-Admin-Port*** – ***LACP partner admin port priority*** – ***LACP partner admin SysID*** – ***LACP partner admin sys priority***
LACP partner admin state	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. Mögliche Werte: ▶ `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 aktiv. ▶ `lacpTimeout` 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. ▶ `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. Mögliche Werte: ▶ `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 Partner empfangenen LACPDUs sind im Status "expired" (verfallen).
LACP Partner-Admin-Port	Legt die Port-Nummer für den Partner-Port fest. Mögliche Werte: ▶ `0..65535` (Voreinstellung: `0`) Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten: – ***LACP partner port admin key*** – ***LACP partner admin port priority*** – ***LACP partner admin SysID*** – ***LACP partner admin sys priority***

Parameter	Bedeutung
LACP partner admin port priority	Legt die Port-Priorität für den Partner-Port fest. Mögliche Werte: ▶ `0..65535` (Voreinstellung: `0`) Der Port mit dem niedrigeren Wert hat die höhere Priorität. Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten: – ***LACP partner port admin key*** – ***LACP Partner-Admin-Port*** – ***LACP partner admin SysID*** – ***LACP partner admin sys priority***
LACP partner admin SysID	Legt einen Wert für die MAC-Adresse fest, die die Partner-System-ID darstellt. Mögliche Werte: ▶ Gültige MAC-Adresse (Voreinstellung: `00:00:00:00:00:00`) Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten: – ***LACP partner port admin key*** – ***LACP Partner-Admin-Port*** – ***LACP partner admin port priority*** – ***LACP partner admin sys priority***
LACP partner admin sys priority	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. Mögliche Werte: ▶ `0..65535` (Voreinstellung: `0`) Der Port mit dem niedrigeren Wert hat die höhere Priorität. Um die Partner-Ports zu verwalten, verwenden Sie den Parameter in Verbindung mit den Einstellungen in den folgenden Spalten: – ***LACP partner port admin key*** – ***LACP Partner-Admin-Port*** – ***LACP partner admin port priority*** – ***LACP partner admin SysID***

Schaltflächen

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

Schaltfläche	Bedeutung
	Öffnet das Fenster ***Erzeugen***, um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ In der Dropdown-Liste ***Trunk-Port*** wählen Sie die Port-Nummer für den Trunk der Link-Aggregation-Gruppe. ▶ In der Dropdown-Liste ***Port*** wählen Sie den Port, der dem Interface zugewiesen wird.

5.9.4 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: ▶ `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: ▶ 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: ▶ 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: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
Status Primärer Port	Zeigt den Status des primären Ports für dieses Link-Backup-Paar. Mögliche Werte: ▶ `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	Zeigt den Status des Backup-Ports für dieses Link-Backup-Paar. Mögliche Werte: ▶ `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	Aktiviert/deaktiviert die automatische Fail-Back-Funktion. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die automatische Fail-Back-Funktion ist aktiv. Nach Ablauf des Verzögerungszeit wechselt der Backup-Port zu `blocking` und der primäre Port wechselt zu `forwarding`. ▶ `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 `shutdown` zu `no shutdown` geändert haben.
Fail-Back-Verzögerung [s]	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 `shutdown` zu `no shutdown`ändern. Nach Ablauf des Verzögerungszeit wechselt der Backup-Port zu `blocking` und der primäre Port wechselt zu `forwarding`. Mögliche Werte: ▶ `0..3600` (Voreinstellung: `30`) Bei `0` wechselt der Backup-Port unmittelbar nachdem der primäre Port einen Link wiederhergestellt hat, zu `blocking` und der primäre Port wechselt zu `forwarding`. Unmittelbar nachdem Sie den Port-Status manuell von `shutdown` zu `no shutdown` ändern, wechselt der Backup-Port zu `blocking` und der primäre Port zu `forwarding`.
Aktiv	Aktiviert/deaktiviert die Konfiguration für das Link-Backup-Paar. Mögliche Werte: ▶ `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	Legt den primären Port des Backup-Interface-Paares fest. Im Normalbetrieb ist dieser Port verantwortlich für die Weiterleitung der Daten. Mögliche Werte: ▶ 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
- Signalkontakt
- MAC-Benachrichtigung
- 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	Zeigt den gegenwärtigen Status des Geräts. Das Gerät bestimmt den Status aus den einzelnen überwachten Parametern. Mögliche Werte: ▶ `error` Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen. ▶ `ok`

Traps

Parameter	Bedeutung
Trap senden	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Änderungen an den überwachten Funktionen erkennt. Mögliche Werte: ▶ `markiert` Das Senden von SNMP-Traps ist aktiv. Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt. ▶ `unmarkiert` (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose >*** Statuskonfiguration ***> Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen.

Tabelle

Parameter	Bedeutung
Temperatur	Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn die Temperatur die festgelegten Grenzwerte überschreitet oder unterschreitet. ▶ `unmarkiert` Die Überwachung ist inaktiv. Die Temperaturgrenzen legen Sie fest im Dialog ***Grundeinstellungen > System***, Feld ***Obere Temp.-Grenze [°C]*** und Feld ***Untere Temp.-Grenze [°C]***.
Ring-Redundanz	Aktiviert/deaktiviert die Überwachung der Ring-Redundanz. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. In folgenden Situationen wechselt der Wert im Rahmen ***Geräte-Status*** auf `error`: – Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve). – Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.

Parameter	Bedeutung
Verbindungsfehler	Aktiviert/deaktiviert die Überwachung des Links auf den Ports/Interfaces. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn der Link auf einem überwachten Port/Interface abbricht. In der Registerkarte ***Port*** haben Sie die Möglichkeit, die zu überwachenden Ports/Interfaces einzeln auszuwählen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Modul entfernen	Aktiviert/deaktiviert die Überwachung der Module. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn Sie ein Modul aus dem Gerät entfernen. Weiter unten haben Sie die Möglichkeit, die zu überwachenden Module einzeln auszuwählen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Externen Speicher entfernen	Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Externer Speicher nicht synchron	Aktiviert/deaktiviert die Überwachung der Konfigurationsprofile im Gerät und auf dem externen Speicher. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. In folgenden Situationen wechselt der Wert im Rahmen ***Geräte-Status*** auf `error`: – Das Konfigurationsprofil existiert ausschließlich im Gerät. – Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil auf dem externen Speicher. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Netzteil	Aktiviert/deaktiviert die Überwachung des Netzteils. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn das Gerät einen Fehler am Netzteil feststellt. ▶ `unmarkiert` Die Überwachung ist inaktiv.
Modul	Aktiviert/deaktiviert die Überwachung dieses Moduls. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn Sie das Modul aus dem Gerät entfernen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv. Die Einstellung ist wirksam, wenn Sie weiter oben das Kontrollkästchen ***Modul entfernen*** markieren.

Schaltflächen

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

[Port]

Tabelle

Parameter	Bedeutung
Verbindungsfehler melden	Aktiviert/deaktiviert die Überwachung des Links auf dem Port/Interface. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn der Link auf einem überwachten Port/Interface abbricht. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv. Die Einstellung ist wirksam, wenn Sie in der Registerkarte ***Global*** das Kontrollkästchen ***Verbindungsfehler*** markieren.

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	Zeigt den gegenwärtigen Status der sicherheitsrelevanten Einstellungen im Gerät. Das Gerät bestimmt den Status aus den einzelnen überwachten Parametern. Mögliche Werte: ▶ `error` Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen. ▶ `ok`

Traps

Parameter	Bedeutung
Trap senden	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Änderungen an den überwachten Funktionen erkennt. Mögliche Werte: ▶ `markiert` Das Senden von SNMP-Traps ist aktiv. Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt. ▶ `unmarkiert` (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose >*** Statuskonfiguration ***> Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen.

Tabelle

Parameter	Bedeutung
Passwort-Voreinstellung unverändert	Aktiviert/deaktiviert die Überwachung des Passworts für die lokal eingerichteten Benutzerkonten `user` und `admin`. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie für die Benutzerkonten `user` oder `admin` das voreingestellte Passwort unverändert verwenden. ▶ `unmarkiert` Die Überwachung ist inaktiv. Das Passwort legen Sie fest im Dialog ***Gerätesicherheit > Benutzerverwaltung***.
Min. Passwort-Länge < 8	Aktiviert/deaktiviert die Überwachung der Richtlinie ***Min. Passwort-Länge***. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn für die Richtlinie ***Min. Passwort-Länge*** ein Wert kleiner als `8` festgelegt ist. ▶ `unmarkiert` Die Überwachung ist inaktiv. Die Richtlinie für die ***Min. Passwort-Länge*** legen Sie fest im Dialog ***Gerätesicherheit >*** Benutzerverwaltung, Rahmen ***Konfiguration***.

Parameter	Bedeutung
Passwort-Richtlinien deaktiviert	Aktiviert/deaktiviert die Überwachung der Passwort-Richtlinien-Einstellungen. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn für die Richtlinie ein Wert kleiner als `1` festgelegt ist. – ***Großbuchstaben (min.)*** – ***Kleinbuchstaben (min.)*** – ***Ziffern (min.)*** – ***Sonderzeichen (min.)*** ▶ `unmarkiert` Die Überwachung ist inaktiv. Die Einstellungen für die Richtlinie legen Sie fest im Dialog ***Gerätesicherheit >*** Benutzerverwaltung, Rahmen ***Passwort-Richtlinien***.
Prüfen der Passwort-Richtlinien im Benutzerkonto deaktiviert	Aktiviert/deaktiviert die Überwachung der ***Richtlinien überprüfen***-Funktion. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn die Funktion ***Richtlinien überprüfen*** bei mindestens 1 Benutzerkonto inaktiv ist. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv. Die Funktion ***Richtlinien überprüfen*** aktivieren Sie im Dialog ***Gerätesicherheit >*** Benutzerverwaltung.
Telnet-Server aktiv	Aktiviert/deaktiviert die Überwachung des Telnet-Servers. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie den Telnet-Server einschalten. ▶ `unmarkiert` Die Überwachung ist inaktiv. Den Telnet-Server schalten Sie ein/aus im Dialog ***Gerätesicherheit > Management-Zugriff > Server***, Registerkarte ***Telnet***.
HTTP-Server aktiv	Aktiviert/deaktiviert die Überwachung des HTTP-Servers. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie den HTTP-Server einschalten. ▶ `unmarkiert` Die Überwachung ist inaktiv. Den HTTP-Server schalten Sie ein/aus im Dialog ***Gerätesicherheit > Management-Zugriff >*** Server, Registerkarte ***HTTP***.

Parameter	Bedeutung
SNMP unverschlüsselt	Aktiviert/deaktiviert die Überwachung des SNMP-Servers. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn mindestens eine der folgenden Bedingungen zutrifft: – Die ***SNMPv1***-Funktion ist eingeschaltet. – Die ***SNMPv2***-Funktion ist eingeschaltet. – Die Verschlüsselung für SNMPv3 ist ausgeschaltet. Die Verschlüsselung schalten Sie ein im Dialog ***Gerätesicherheit > Benutzerverwaltung***, Spalte ***SNMP-Verschlüsselung***. ▶ `unmarkiert` Die Überwachung ist inaktiv. Die Einstellungen für den SNMP-Agenten legen Sie fest im Dialog ***Gerätesicherheit > Management-Zugriff > Server***, Registerkarte ***SNMP***.
Zugriff auf System-Monitor mit V.24 möglich	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. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn der System-Monitor aktiviert ist. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv. Den System-Monitor aktivieren/deaktivieren Sie im Dialog ***Diagnose > System > Selbsttest***.
Speichern des Konfigurationsprofils auf dem externen Speicher möglich	Aktiviert/deaktiviert die Überwachung des Konfigurationsprofils auf dem externen Speicher. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn das Speichern des Konfigurationsprofils auf dem externen Speicher aktiviert ist. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv. Das Speichern des Konfigurationsprofils auf dem externen Speicher aktivieren/deaktivieren Sie im Dialog ***Grundeinstellungen > Externer Speicher***.
Unverschlüsselte Konfiguration vom externen Speicher laden	Aktiviert/deaktiviert die Überwachung des Ladens unverschlüsselter Konfigurationsprofile vom externen Speicher. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn die Einstellungen dem Gerät ermöglichen, ein unverschlüsseltes Konfigurationsprofil vom externen Speicher zu laden. Der Rahmen ***Sicherheits-Status*** im Dialog ***Grundeinstellungen > System*** zeigt einen Alarm, wenn folgende Voraussetzungen erfüllt sind: – Das auf dem externen Speicher gespeicherte Konfigurationsprofil ist unverschlüsselt. und – Die Spalte ***Konfigurations-Priorität*** im Dialog ***Grundeinstellungen > Externer Speicher*** hat den Wert `first`. ▶ `unmarkiert` Die Überwachung ist inaktiv.

Parameter	Bedeutung
Verbindungsabbruch auf eingeschalteten Ports	Aktiviert/deaktiviert die Überwachung des Links auf den aktiven Ports. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn der Link auf einem aktiven Port abbricht. In der Registerkarte ***Port*** haben Sie die Möglichkeit, die zu überwachenden Ports einzeln auszuwählen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Zugriff mit HiDiscovery möglich	Aktiviert/deaktiviert die Überwachung der HiDiscovery-Funktion. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie die HiDiscovery-Funktion einschalten. ▶ `unmarkiert` Die Überwachung ist inaktiv. Die HiDiscovery-Funktion schalten Sie im Dialog ***Grundeinstellungen > Netz*** ein/aus.
IEC61850-MMS aktiv	Aktiviert/deaktiviert die Überwachung der ***IEC61850-MMS***-Funktion. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie die ***IEC61850-MMS***-Funktion einschalten. ▶ `unmarkiert` Die Überwachung ist inaktiv. Die ***IEC61850-MMS***-Funktion schalten Sie im Dialog ***Industrie-Protokolle > IEC61850-MMS***, Rahmen ***Funktion*** ein/aus.
Modbus TCP aktiv	Aktiviert/deaktiviert die Überwachung der ***Modbus TCP***-Funktion. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie die ***Modbus TCP***-Funktion einschalten. ▶ `unmarkiert` Die Überwachung ist inaktiv. Die ***Modbus TCP***-Funktion schalten Sie im Dialog ***Erweitert > Industrie-Protokolle >*** Modbus TCP, Rahmen ***Funktion*** ein/aus.
Self-signed HTTPS-Zertifikat vorhanden	Aktiviert/deaktiviert die Überwachung des HTTPS-Zertifikats. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn der HTTPS-Server ein selbst erzeugtes digitales Zertifikat verwendet. ▶ `unmarkiert` 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	Aktiviert/deaktiviert die Überwachung des Links auf den aktiven Ports. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn der Port eingeschaltet ist (Dialog ***Grundeinstellungen > Port***, Registerkarte ***Konfiguration***, Kontrollkästchen ***Port an*** ist `markiert`) und wenn der Link auf dem Port abbricht. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv. Diese Einstellung ist wirksam, wenn Sie im Dialog ***Diagnose > Statuskonfiguration >*** Sicherheitsstatus, Registerkarte ***Global***, das Kontrollkästchen ***Verbindungsabbruch auf eingeschalteten Ports*** markieren.

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 Signalkontakt

Der Signalkontakt ist ein potentialfreier Relaiskontakt. Das Gerät bietet Ihnen damit die Möglichkeit einer Ferndiagnose. Über den Signalkontakt signalisiert das Gerät das Eintreten von Ereignissen, indem es den Relaiskontakt öffnet und den Ruhestromkreis unterbricht.

Anmerkung: Das Gerät enthält möglicherweise mehrere Signalkontakte. Hierbei enthält jeder einzelne Signalkontakt dieselben Überwachungsfunktionen. Mehrere Signalkontakte bieten Ihnen die Möglichkeit, unterschiedliche Funktionen zu gruppieren, was die Systemüberwachung flexibel macht.

Das Menü enthält die folgenden Dialoge:

- Signalkontakt 1 / Signalkontakt 2

6.1.3.1 Signalkontakt 1 / Signalkontakt 2

In diesem Dialog legen Sie die Auslösebedingungen für den Signalkontakt fest.

Der Signalkontakt bietet Ihnen folgende Möglichkeiten:
- Funktionsüberwachung des Geräts.
- Signalisierung des Gerätstatus des Geräts.
- Signalisierung des Sicherheitsstatus des Geräts.
- Steuerung externer Geräte bei manueller Einstellung des Signalkontakts.

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

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Port]
- [Status]

[Global]

Konfiguration

Parameter	Bedeutung
Modus	Legt fest, welche Ereignisse der Signalkontakt signalisiert. Mögliche Werte: ▶ `Manuelle Einstellung` (Voreinstellung für ***Signalkontakt 2***, falls vorhanden) Mit dieser Einstellung schalten Sie den Signalkontakt von Hand, um zum Beispiel ein entferntes Gerät ein- oder auszuschalten. Siehe Optionsfeld ***Kontakt***. ▶ `Funktionsüberwachung` (Voreinstellung) Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der in der Tabelle unten festgelegten Parameter. ▶ `Geräte-Status` Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog ***Diagnose*** > Statuskonfiguration > ***Gerätestatus*** überwachten Parameter. Zusätzlich ist der Zustand im Rahmen ***Signalkontakt-Status*** ablesbar. ▶ `Sicherheits-Status` Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog ***Diagnose*** > Statuskonfiguration > ***Sicherheitsstatus*** überwachten Parameter. Zusätzlich ist der Zustand im Rahmen ***Signalkontakt-Status*** ablesbar. ▶ `Geräte-/Sicherheits-Status` Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog ***Diagnose*** > Statuskonfiguration > ***Gerätestatus*** und im Dialog ***Diagnose*** > ***Statuskonfiguration*** > Sicherheitsstatus überwachten Parameter. Zusätzlich ist der Zustand im Rahmen ***Signalkontakt-Status*** ablesbar.
Kontakt	Schaltet den Signalkontakt von Hand. Voraussetzung ist, dass Sie in der Dropdown-Liste ***Modus*** den Wert `Manuelle Einstellung` auswählen. Mögliche Werte: ▶ `offen` Der Signalkontakt ist geöffnet. ▶ `geschlossen` Der Signalkontakt ist geschlossen.

Signalkontakt-Status

Parameter	Bedeutung
Signalkontakt-Status	Zeigt den gegenwärtigen Zustand des Signalkontakts. Mögliche Werte: ▶ `Offen (Fehler)` Der Signalkontakt ist geöffnet. Der Ruhestromkreis ist unterbrochen. ▶ `Geschlossen (Ok)` Der Signalkontakt ist geschlossen. Der Ruhestromkreis ist geschlossen.

Trap-Konfiguration

Parameter	Bedeutung
Trap senden	Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät Änderungen an den überwachten Funktionen erkennt. Mögliche Werte: ▶ `markiert` Das Senden von SNMP-Traps ist aktiv. Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt. ▶ `unmarkiert` (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose >*** Statuskonfiguration ***> Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen.

Funktionsüberwachung

In dieser Tabelle legen Sie die Parameter fest, die das Gerät überwacht. Das Eintreten eines Ereignisses meldet das Gerät durch Öffnen des Signalkontakts.

Parameter	Bedeutung
Temperatur	Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Signalkontakt öffnet, wenn die Temperatur die Temperaturgrenzen überschreitet oder unterschreitet. ▶ `unmarkiert` Die Überwachung ist inaktiv. Die Temperaturgrenzen legen Sie fest im Dialog ***Grundeinstellungen > System***, Feld ***Obere Temp.-Grenze [°C]*** und Feld ***Untere Temp.-Grenze [°C]***.
Ring-Redundanz	Aktiviert/deaktiviert die Überwachung der Ring-Redundanz. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. In folgenden Situationen öffnet der Signalkontakt: – Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve). – Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Verbindungsfehler	Aktiviert/deaktiviert die Überwachung des Links auf den Ports/Interfaces. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Signalkontakt öffnet, wenn der Link auf einem überwachten Port/Interface abbricht. In der Registerkarte ***Port*** haben Sie die Möglichkeit, die zu überwachenden Ports/Interfaces einzeln auszuwählen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Modul entfernen	Aktiviert/deaktiviert die Überwachung der Module. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Signalkontakt öffnet, wenn Sie ein Modul aus dem Gerät entfernen. Weiter unten haben Sie die Möglichkeit, die zu überwachenden Module einzeln auszuwählen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.

Parameter	Bedeutung
Externer Speicher wurde entfernt	Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Signalkontakt öffnet, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Externer Speicher und NVM nicht synchron	Aktiviert/deaktiviert die Überwachung der Konfigurationsprofile im Gerät und auf dem externen Speicher. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. In folgenden Situationen öffnet der Signalkontakt: – Das Konfigurationsprofil existiert ausschließlich im Gerät. – Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil auf dem externen Speicher. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Netzteil	Aktiviert/deaktiviert die Überwachung des Netzteils. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die Überwachung ist aktiv. Der Signalkontakt öffnet, wenn das Gerät einen Fehler an diesem Netzteil feststellt. ▶ `unmarkiert` Die Überwachung ist inaktiv.
Modul	Aktiviert/deaktiviert die Überwachung dieses Moduls. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Signalkontakt öffnet, wenn Sie dieses Modul aus dem Gerät entfernen. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv. Die Einstellung ist wirksam, wenn Sie weiter oben das Kontrollkästchen ***Modul entfernen*** markieren.

Schaltflächen

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

[Port]

Tabelle

Parameter	Bedeutung
Verbindungsfehler melden	Aktiviert/deaktiviert die Überwachung des Links auf dem Port/Interface. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. Der Signalkontakt öffnet, wenn der Link auf dem ausgewählten Port/Interface abbricht. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv. Die Einstellung ist wirksam, wenn Sie in der Registerkarte ***Global*** das Kontrollkästchen ***Verbindungsfehler*** markieren.

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.

6.1.4 MAC-Benachrichtigung

Das Gerät bietet Ihnen die Möglichkeit, Änderungen im Netz anhand der MAC-Adresse der Geräte zu verfolgen Das Gerät speichert die Kombination aus Port und MAC-Adresse in seiner MAC-Adresstabelle. Wenn das Gerät die MAC-Adresse eines (nicht mehr) angeschlossenen Geräts (ver-)lernt, sendet das Gerät in regelmäßigen Abständen einen SNMP-Trap.

Diese Funktion ist für Ports gedacht, an die Sie Endgeräte anschließen und an denen sich folglich die MAC-Adresse selten ändert.

Funktion

Parameter	Bedeutung
Funktion	Schaltet die ***MAC-Benachrichtigung***-Funktion im Gerät ein/aus. Mögliche Werte: ▶ `An` Die ***MAC-Benachrichtigung***-Funktion ist eingeschaltet. ▶ `Aus` (Voreinstellung) Die ***MAC-Benachrichtigung***-Funktion ist ausgeschaltet.

Konfiguration

Parameter	Bedeutung
Intervall [s]	Legt das Sendeintervall in Sekunden fest. Wenn das Gerät die MAC-Adresse eines (nicht mehr) angeschlossenen Geräts (ver-)lernt, sendet das Gerät nach dieser Zeit einen SNMP-Trap. Mögliche Werte: ▶ `0..2147483647` (Voreinstellung: `30`) Das Gerät erfasst vor dem Senden eines SNMP-Trap bis zu 20 MAC-Adressen. Wenn das Gerät sehr viele Änderungen erkennt, sendet es den SNMP-Trap bereits vor Ablauf des Sendeintervalls.

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Aktiv	Aktiviert/deaktiviert die Funktion ***MAC-Benachrichtigung*** auf dem Port. Mögliche Werte: ▶ `markiert` Die ***MAC-Benachrichtigung***-Funktion ist auf dem Port aktiv. Das Gerät sendet einen SNMP-Trap, wenn eines der folgenden Ereignisse eintritt: – Das Gerät lernt die MAC-Adresse eines neu angeschlossenen Geräts. – Das Gerät verlernt die MAC-Adresse eines nicht mehr angeschlossenen Geräts. ▶ `unmarkiert` (Voreinstellung) Die ***MAC-Benachrichtigung***-Funktion ist auf dem Port inaktiv. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose > Statuskonfiguration > Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen.

Parameter	Bedeutung
Letzte MAC-Adresse	Zeigt die MAC-Adresse des Geräts, das zuletzt an den Port angeschlossen oder vom Port getrennt wurde. Das Gerät erkennt die MAC-Adressen von Geräten, die wie folgt angeschlossen sind: – direkt an den Port angeschlossen – über andere Geräte im Netz mit dem Port verbunden
Letzter MAC-Status	Zeigt den Zustand des Werts ***Letzte MAC-Adresse*** auf dem Port. Mögliche Werte: ▶ `added` Das Gerät hat erkannt, dass ein anderes Gerät an den Port angeschlossen wurde. ▶ `removed` Das Gerät hat erkannt, dass das angeschlossene Gerät vom Port entfernt wurde. ▶ `other` Das Gerät hat keinen Status erkannt.

Schaltflächen

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

6.1.5 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***
- im Dialog ***Diagnose > Statuskonfiguration > MAC-Benachrichtigung***

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 ***Erzeugen***, um der Tabelle einen neuen Eintrag hinzuzufügen. ▶ Im Feld ***Name*** legen Sie eine Bezeichnung für das Trap-Ziel fest. ▶ Im Feld ***Adresse*** 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	Zeigt den Grad der Abweichung zwischen den Einstellungen dieses Geräts und den Einstellungen der erkannten Nachbargeräte. Das Gerät unterscheidet die folgenden Zustände: ▶ `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: Ein Nachbargerät ohne LLDP-Unterstützung, das LLDP-Pakete weiterleitet, kann im Dialog mehrdeutige Meldungen verursachen. Dies tritt auf, wenn das Nachbargerät ein Hub oder ein Switch ohne Management ist, der die Norm IEEE 802.1D-2004 ignoriert.
Der Dialog stellt in dem Fall die am Nachbargerät angeschlossenen und erkannten Geräte als direkt mit dem Gerät verbunden dar, obwohl diese am Nachbargerät angeschlossen sind.

Anmerkung: Wenn im Gerät mehr als 39 VLANseingerichtet 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.

Immer wenn das Gerät einen Adresskonflikt erkennt, blinkt die Status-LED des Geräts 4-mal rot.

Funktion

Parameter	Bedeutung
Funktion	Schaltet die ***IP-Adressen Konflikterkennung***-Funktion ein/aus. Mögliche Werte: ▶ `An` (Voreinstellung) Die ***IP-Adressen Konflikterkennung***-Funktion ist eingeschaltet. Das Gerät prüft, ob ein weiteres Gerät im Netz die eigene IP-Adresse verwendet. ▶ `Aus` Die ***IP-Adressen Konflikterkennung***-Funktion ist ausgeschaltet.

Konfiguration

Parameter	Bedeutung
Erkennungs-Modus	Legt das Verfahren fest, mit dem das Gerät Adresskonflikte erkennt. Mögliche Werte: ▶ `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. – Das Gerät sendet 4 ARP-Probe-Datenpakete mit dem im Feld ***Erkennungs-Verzögerung [ms]*** festgelegten zeitlichen Abstand. Empfängt das Gerät auf diese Datenpakete eine Antwort, liegt ein Addresskonflikt 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 ***Rückfallverzögerung [s]*** 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. – Zur „Verteidigung“ sendet das Gerät Gratuitous-ARP-Datenpakete. Diesen Vorgang wiederholt das Gerät sooft wie im Feld ***Address-Protections*** festgelegt. – Sendet das andere Gerät weiter mit derselben IP-Adresse, prüft das Gerät zyklisch jeweils nach der im Feld ***Rückfallverzögerung [s]*** festgelegten Zeit, ob der Adresskonflikt weiterhin besteht. – Sobald der Adresskonflikt behoben ist, geht das Management des Geräts wieder ans Netz.
Periodische ARP-Überprüfung senden	Schaltet die periodische Adresskonflikt-Erkennung ein/aus. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die periodische Adresskonflikt-Erkennung ist eingeschaltet. – Das Gerät sendet jeweils nach 90 bis 150 Sekunden ein ARP-Probe-Datenpaket und wartet solange wie im Feld ***Erkennungs-Verzögerung [ms]*** festgelegt auf Antwort. – Erkennt das Gerät einen Adresskonflikt, wendet es die Funktionen des passiven Erkennungsmodus an. Wenn die Funktion ***Trap senden*** eingeschaltet ist, sendet das Gerät einen SNMP-Trap. ▶ `unmarkiert` Die periodische Adresskonflikt-Erkennung ist ausgeschaltet.
Erkennungs-Verzögerung [ms]	Legt die Zeitspanne in Millisekunden fest, in der das Gerät nach dem Senden eines ARP-Datenpakets auf Antwort wartet. Mögliche Werte: ▶ `20..500` (Voreinstellung: `200`)
Rückfallverzögerung [s]	Legt die Zeit in Sekunden fest, nach der das Gerät erneut prüft, ob der Adresskonflikt weiterhin besteht. Mögliche Werte: ▶ `3..3600` (Voreinstellung: `15`)
Address-Protections	Legt fest, wie viele Male das Gerät im passiven Erkennungsmodus zum „Verteidigen“ seiner IP-Adresse Gratuitous-ARP-Datenpakete sendet. Mögliche Werte: ▶ `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: ▶ `markiert` Das Senden von SNMP-Traps ist aktiv. Das Gerät sendet einen SNMP-Trap, wenn es einen Adresskonflikt erkennt. ▶ `unmarkiert` (Voreinstellung) Das Senden von SNMP-Traps ist inaktiv. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose >*** Statuskonfiguration ***> Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen.

Information

Parameter	Bedeutung
Konflikt erkannt	Zeigt, ob gegenwärtig ein Adresskonflikt besteht. Mögliche Werte: ▶ `markiert` Das Gerät erkennt einen Adresskonflikt. ▶ `unmarkiert` 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: ▶ `static` Statischer ARP-Eintrag. Der ARP-Eintrag bleibt nach dem Löschen der ARP-Tabelle erhalten. ▶ `dynamic` Dynamischer ARP-Eintrag. Das Gerät löscht den ARP-Eintrag nach Überschreiten der ***Aging-Time [s]***, falls das Gerät während dieser Zeit keine Daten von diesem Gerät empfängt. ▶ `local` 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	Aktiviert/deaktiviert den RAM-Speicher-Test während des Neustarts. Mögliche Werte: ▶ `markiert` (Voreinstellung) Der RAM-Speicher-Test ist aktiviert. Während des Neustarts testet das Gerät den RAM-Speicher. ▶ `unmarkiert` Der RAM-Speicher-Test ist deaktiviert. Dies verkürzt die Startzeit des Geräts.
SysMon1 ist verfügbar	Aktiviert/deaktiviert den Zugang zum System-Monitor während des Neustarts. Mögliche Werte: ▶ `markiert` (Voreinstellung) Das Gerät bietet Ihnen die Möglichkeit, während des Neustarts in den System-Monitor zu wechseln. ▶ `unmarkiert` Das Gerät startet ohne die Möglichkeit, in den System-Monitor zu wechseln. Der System-Monitor bietet Ihnen u. a. die Möglichkeit, die Gerätsoftware zu aktualisieren und gespeicherte Konfigurationsprofile zu löschen.
Bei Fehler Default-Konfiguration laden	Aktiviert/deaktiviert das Laden der Werkseinstellungen, falls das Gerät beim Neustart kein lesbares Konfigurationsprofil findet. Mögliche Werte: ▶ `markiert` (Voreinstellung) Das Gerät lädt die Werkseinstellungen. ▶ `unmarkiert` 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	Fehlerursachen, auf die das Gerät reagiert. Mögliche Werte: ▶ `task` Das Gerät erkennt Fehler in ausgeführten Anwendungen, zum Beispiel wenn eine Task abbricht oder nicht verfügbar ist. ▶ `resource` Das Gerät erkennt Fehler in den verfügbaren Ressourcen, zum Beispiel bei knapp werdendem Speicher. ▶ `software` Das Gerät erkennt Software-Fehler, zum Beispiel Fehler beim Konsistenz-Check. ▶ `hardware` Das Gerät erkennt Hardware-Fehler, zum Beispiel im Chipsatz.
Aktion	Legt das Verhalten des Geräts fest, wenn das nebenstehende Ereignis eintritt. Mögliche Werte: ▶ `reboot` (Voreinstellung) Das Gerät löst einen Neustart aus. ▶ `logOnly` Das Gerät protokolliert den Fehler in der Log-Datei. Siehe Dialog ***Diagnose > Bericht >*** System Log. ▶ `sendTrap` Das Gerät sendet einen SNMP-Trap. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose > Statuskonfiguration > Alarme (Traps)*** 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 ***Ziel-UDP-Port*** 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: ▶ `systemlog` (Voreinstellung) ▶ `audittrail`
Aktiv	Aktiviert bzw. deaktiviert die Übermittlung der Ereignisse zum Syslog-Server: ▶ `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
- TP-Kabeldiagnose
- 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 TP-Kabeldiagnose

Diese Funktion testet ein an das Interface angeschlossene Kabel auf einen Kurzschluss oder eine Unterbrechung. Die Tabelle zeigt den Kabelstatus und die geschätzte Länge an. Das Gerät zeigt auch die einzelnen, an den Port angeschlossenen Kabelpaare an. Wenn das Gerät einen Kurzschluss oder eine Unterbrechung im Kabel ermittelt, zeigt es auch die geschätzte Entfernung zu dem Problem an.

Anmerkung: Dieser Test unterbricht den Datenverkehr am betreffenden Port.

Information

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Status	Status des virtuellen Kabeltesters. Mögliche Werte: ▶ `aktiv` Der Kabeltest ist im Gange. Um den Test zu starten, klicken Sie die Schaltfläche ☰ und dann den Eintrag ***Starte Kabeldiagnose...***. Diese Aktion öffnet den Dialog ***Port auswählen***. ▶ `erfolgreich` Das Gerät zeigt diesen Eintrag nach einem erfolgreichen Test an. ▶ `Fehler` Das Gerät zeigt diesen Eintrag nach einer Unterbrechung des Tests an. ▶ `nicht initialisiert` Das Gerät zeigt diesen Eintrag, während es sich im Standby befindet.

Tabelle

Parameter	Bedeutung
Kabelpaar	Zeigt das Kabelpaar, auf das sich dieser Eintrag bezieht. Das Gerät verwendet das erste unterstützte PHY-Register, um die Werte anzuzeigen.
Ergebnis	Zeigt das Ergebnis des Kabeltests. Mögliche Werte: ▶ `normal` Das Kabel funktioniert ordnungsgemäß. ▶ `offen` Ein Bruch im Kabel verursacht eine Unterbrechung. ▶ `Kurzschluss` Einzelne Adern des Kabels berühren sich und verursachen einen Kurzschluss. ▶ `unbekannt` Das Gerät zeigt diesen Wert bei ungetesteten Kabelpaaren an. **Anmerkung:** In den folgenden Fällen zeigt das Gerät andere Werte an als erwartet: – Wenn kein Kabel am Port angeschlossen ist, zeigt das Gerät den Wert `unbekannt` anstatt `offen`. – Wenn der Port deaktiviert ist, zeigt das Gerät den Wert `Kurzschluss`.
Min. Länge	Zeigt die minimale geschätzte Länge des Kabels in Metern. Das Gerät zeigt den Wert `0`, wenn die Kabellänge unbekannt ist oder wenn das Feld im Rahmen ***Information*** den Wert `aktiv`, `Fehler` oder `nicht initialisiert` zeigt.

Parameter	Bedeutung
Max. Länge	Zeigt die maximale geschätzte Länge des Kabels in Metern. Das Gerät zeigt den Wert `0`, wenn die Kabellänge unbekannt ist oder wenn das Feld im Rahmen ***Information*** den Wert `aktiv`, `Fehler` oder `nicht initialisiert` zeigt.
Distanz [m]	Zeigt die geschätzte Entfernung in Metern vom Kabelende bis zur Position des Fehlers. Das Gerät zeigt den Wert `0`, wenn die Kabellänge unbekannt ist oder wenn das Feld im Rahmen ***Information*** den Wert `aktiv`, `Fehler` oder `nicht initialisiert` zeigt.

Schaltflächen

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

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Starte Kabeldiagnose...	Öffnet den Dialog ***Port auswählen***. In der Dropdown-Liste ***Port*** wählen Sie den zu testenden Port. Wenden Sie den Test ausschließlich bei kupferbasierten Ports an. Um den Kabeltest auf dem ausgewählten Port auszuführen, klicken Sie die Schaltfläche ***Ok***.

6.4.3 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 ***Port-Monitor***-Funktion global ein/aus. Mögliche Werte: ▶ `An` Die ***Port-Monitor***-Funktion ist eingeschaltet. ▶ `Aus` (Voreinstellung) Die ***Port-Monitor***-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: ▶ `markiert` Die Überwachung ist aktiv. – Die ***Port-Monitor***-Funktion überwacht Linkänderungen auf dem Port. – Wenn das Gerät zu viele Linkänderungen erkennt, führt es die in Spalte ***Aktion*** festgelegte Aktion aus. – In der Registerkarte ***Link-Änderungen*** 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: ▶ `markiert` Die Überwachung ist aktiv. – Die ***Port-Monitor***-Funktion überwacht CRC-/Fragmentfehler auf dem Port. – Wenn das Gerät zu viele CRC-/Fragmentfehler erkennt, führt es die in Spalte ***Aktion*** festgelegte Aktion aus. – In der Registerkarte ***CRC/Fragmente*** 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: ▶ `markiert` Die Überwachung ist aktiv. – Die ***Port-Monitor***-Funktion überwacht Duplex-Mismatches auf dem Port. – Wenn das Gerät einen Duplex-Mismatch erkennt, führt es die in Spalte ***Aktion*** festgelegte Aktion aus. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.

Parameter	Bedeutung
Überlast-Erkennung an	Aktiviert/deaktiviert auf dem Port die Überlast-Erkennung. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. – Die ***Port-Monitor***-Funktion überwacht die Last auf dem Port. – Wenn das Gerät Überlast auf dem Port erkennt, führt das Gerät die in Spalte ***Aktion*** festgelegte Aktion aus. – In der Registerkarte ***Überlast-Erkennung*** legen Sie die zu überwachenden Parameter fest. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Link-Speed-/ Duplex-Mode-Erkennung an	Aktiviert/deaktiviert auf dem Port die Überwachung von Verbindungsgeschwindigkeit und Duplex-Modus. Mögliche Werte: ▶ `markiert` Die Überwachung ist aktiv. – Die ***Port-Monitor***-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 ***Aktion*** festgelegte Aktion aus. – In der Registerkarte ***Link-Speed-/Duplex-Mode-Erkennung*** legen Sie die zu überwachenden Parameter fest. ▶ `unmarkiert` (Voreinstellung) Die Überwachung ist inaktiv.
Aktive Bedingung	Zeigt den überwachten Parameter, der zur Aktion auf dem Port geführt hat. Mögliche Werte: ▶ `-` 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	Legt die Aktion fest, die das Gerät ausführt, wenn die ***Port-Monitor***-Funktion eine Überschreitung der Parameter erkennt. Mögliche Werte: ▶ `disable port` Das Gerät schaltet den Port aus und sendet einen SNMP-Trap. Die „Link-Status“-LED des Ports blinkt 3× pro Periode. – Um den Port wieder einzuschalten, markieren Sie den Port und klicken die Schaltfläche ☰ und dann den Eintrag ***Zurücksetzen***. – Die ***Auto-Disable***-Funktion schaltet nach der festgelegten Wartezeit den Port wieder ein, wenn die Überschreitung der Parameter aufgehoben ist. Voraussetzung ist, dass in der Registerkarte ***Auto-Disable*** das Kontrollkästchen für den überwachten Parameter markiert ist. ▶ `send trap` Das Gerät sendet einen SNMP-Trap. Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog ***Diagnose > Statuskonfiguration > Alarme (Traps)*** einschalten und mindestens 1 Trap-Ziel festlegen. ▶ `auto-disable` (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 ***Auto-Disable*** das Kontrollkästchen für den überwachten Parameter markiert ist. – Der Dialog ***Diagnose > Ports > Auto-Disable*** zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind. – Die ***Auto-Disable***-Funktion schaltet den Port automatisch wieder ein. Legen Sie dazu im Dialog ***Diagnose > Ports > Auto-Disable*** in Spalte ***Reset-Timer [s]*** eine Wartezeit für den betreffenden Port fest.
Status Port	Zeigt den Betriebszustand des Ports. Mögliche Werte: ▶ `up` Der Port ist eingeschaltet. ▶ `down` Der Port ist ausgeschaltet. ▶ `notPresent` 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	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: ▶ Dialog ***Diagnose > Ports > Port-Monitor*** – Registerkarte ***Link-Änderungen*** – Registerkarte ***CRC/Fragmente*** – Registerkarte ***Überlast-Erkennung*** ▶ Dialog ***Diagnose > Ports > Auto-Disable***

[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 ***Port-Monitor***-Funktion überwachten Parameter. Markieren Sie das nebenstehende Kontrollkästchen, damit die ***Port-Monitor***-Funktion bei Erkennen einer Überschreitung der überwachten Parameter die Aktion `auto-disable` ausführt.
Auto-Disable	Aktiviert/deaktiviert die ***Auto-Disable***-Funktion für nebenstehende Parameter. Mögliche Werte: ▶ `markiert` Die ***Auto-Disable***-Funktion für nebenstehende Parameter ist aktiv. Bei Überschreiten der nebenstehenden Parameter führt das Gerät die ***Auto-Disable***-Funktion aus, wenn in Spalte ***Aktion*** der Wert `auto-disable` festgelegt ist. ▶ `unmarkiert` (Voreinstellung) Die ***Auto-Disable***-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: ▶ Dialog ***Diagnose > Ports > Port-Monitor*** – Registerkarte ***Link-Änderungen*** – Registerkarte ***CRC/Fragmente*** – Registerkarte ***Überlast-Erkennung*** ▶ Dialog ***Diagnose > Ports > Auto-Disable***

[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 ***Port-Monitor***-Funktion einen Parameter überwacht, um Abweichungen zu erkennen. Mögliche Werte: ▶ `1..180` (Voreinstellung: `10`)
Link-Änderungen	Legt die Anzahl der Linkänderungen fest. Wenn die ***Port-Monitor***-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: ▶ Dialog ***Diagnose > Ports > Port-Monitor*** – Registerkarte ***Link-Änderungen*** – Registerkarte ***CRC/Fragmente*** – Registerkarte ***Überlast-Erkennung*** ▶ Dialog ***Diagnose > Ports > Auto-Disable***

[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 ***Port-Monitor***-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 ***Port-Monitor***-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: ▶ Dialog ***Diagnose > Ports > Port-Monitor*** – Registerkarte ***Link-Änderungen*** – Registerkarte ***CRC/Fragmente*** – Registerkarte ***Überlast-Erkennung*** ▶ Dialog ***Diagnose > Ports > Auto-Disable***

[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 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: ▶ `all` Die ***Port-Monitor***-Funktion überwacht Broadcast-, Multicast- und Unicast-Pakete. ▶ `bc` (Voreinstellung) Die ***Port-Monitor***-Funktion überwacht ausschließlich Broadcast-Pakete. ▶ `bc-mc` Die ***Port-Monitor***-Funktion überwacht ausschließlich Broadcast- und Multicast-Pakete.
Grenzwert-Typ	Legt die Einheit der Datenrate fest. Mögliche Werte: ▶ `pps` (Voreinstellung) Pakete pro Sekunde ▶ `kbps` Kbit pro Sekunde Voraussetzung ist, dass der Wert in Spalte ***Traffic-Typ*** = `all` ist.
Unterer Grenzwert	Legt den unteren Schwellenwert für die Datenrate fest. Die ***Auto-Disable***-Funktion schaltet den Port erst dann wieder ein, wenn die Last auf dem Port niedriger ist als der hier festgelegte Wert. Mögliche Werte: ▶ `0..10000000` (Voreinstellung: `0`)
Oberer Grenzwert	Legt den oberen Schwellenwert für die Datenrate fest. Wenn die ***Port-Monitor***-Funktion diese Last im überwachten Zeitraum erkennt, führt das Gerät die festgelegte Aktion aus. Mögliche Werte: ▶ `0..10000000` (Voreinstellung: `0`))
Intervall [s]	Legt den Zeitraum in Sekunden fest, den die ***Port-Monitor***-Funktion für das Erkennen einer Überschreitung betrachtet. Mögliche Werte: ▶ `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: ▶ Dialog ***Diagnose > Ports > Port-Monitor*** – Registerkarte ***Link-Änderungen*** – Registerkarte ***CRC/Fragmente*** – Registerkarte ***Überlast-Erkennung*** ▶ Dialog ***Diagnose > Ports > Auto-Disable***

[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: ▶ `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 ***Global*** 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: ▶ `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 ***Global*** festgelegte Aktion aus.

Parameter	Bedeutung
100 Mbit/s HDX	Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Halbduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `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 ***Global*** festgelegte Aktion aus.
100 Mbit/s FDX	Aktiviert/deaktiviert das Akzeptieren der Kombination von 100 Mbit/s und Vollduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `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 ***Global*** festgelegte Aktion aus.
1.000 Mbit/s FDX	Aktiviert/deaktiviert das Akzeptieren der Kombination von 1 Gbit/s und Vollduplex auf dem Port durch den Port-Monitor. Mögliche Werte: ▶ `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 ***Global*** 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	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: ▶ Dialog ***Diagnose > Ports > Port-Monitor*** – Registerkarte ***Link-Änderungen*** – Registerkarte ***CRC/Fragmente*** – Registerkarte ***Überlast-Erkennung*** ▶ Dialog ***Diagnose > Ports > Auto-Disable***

6.4.4 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]	Legt die Wartezeit in Sekunden fest, nach der die ***Auto-Disable***-Funktion den Port wieder einschaltet. Mögliche Werte: - `0` (Voreinstellung) Der Timer ist inaktiv. Der Port bleibt ausgeschaltet. - `30..4294967295` Die ***Auto-Disable***-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 ***Auto-Disable***-Funktion den Port wieder einschaltet.

Parameter	Bedeutung
Komponente	Zeigt, welche Software-Komponente im Gerät das Ausschalten des Ports veranlasst hat. Mögliche Werte: ▶ `PORT_MON` ***Port-Monitor*** Siehe Dialog ***Diagnose > Ports > Port-Monitor***. ▶ `PORT_ML` ***Port-Sicherheit*** Siehe Dialog ***Netzsicherheit > Port-Sicherheit***. ▶ `DOT1S` ***BPDU-Guard*** Siehe Dialog ***Switching > L2-Redundanz > Spanning Tree > Global***.
Grund	Zeigt den überwachten Parameter, der zum Ausschalten des Ports geführt hat. Mögliche Werte: ▶ `none` Kein überwachter Parameter. Der Port ist eingeschaltet. ▶ `link-flap` Zu viele Linkänderungen. Siehe Dialog ***Diagnose > Ports > Port-Monitor***, Registerkarte ***Link-Änderungen***. ▶ `crc-error` Zu viele CRC-/Fragmentfehler. Siehe Dialog ***Diagnose > Ports > Port-Monitor***, Registerkarte ***CRC/Fragmente***. ▶ `duplex-mismatch` Duplex-Mismatch erkannt. Siehe Dialog ***Diagnose > Ports > Port-Monitor***, Registerkarte ***Global***. ▶ `bpdu-rate` STP-BPDUs empfangen. Siehe Dialog ***Switching > L2-Redundanz > Spanning Tree >*** Global. ▶ `mac-based-port-security` Zu viele Datenpakete von unerwünschten Absendern. Siehe Dialog ***Netzsicherheit >*** Port-Sicherheit. ▶ `overload-detection` Überlast. Siehe Dialog ***Diagnose > Ports > Port-Monitor***, Registerkarte ***Überlast-Erkennung***. ▶ `speed-duplex` Unerlaubte Kombination von Geschwindigkeit und Duplex-Modus erkannt. Siehe Dialog ***Diagnose > Ports > Port-Monitor***, Registerkarte ***Link-Speed-/Duplex-Mode-Erkennung***.
Aktiv	Zeigt, ob der Port aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet ist. Mögliche Werte: ▶ `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 ***Auto-Disable***-Funktion bei Überschreiten der überwachten Parameter den Port ausschaltet und ggf. wieder einschaltet.
Kategorie	Zeigt, zu welcher Funktion der nebenstehende Parameter gehört. Mögliche Werte: ▶ `port-monitor` Der Parameter gehört zur ***Port-Monitor***-Funktion. Siehe Dialog ***Diagnose > Port > Port-Monitor***. ▶ `network-security` Der Parameter gehört zu den Funktionen im Menü ***Netzsicherheit***. ▶ `l2-redundancy` Der Parameter gehört zu den ***L2-Redundanz***-Funktionen. Siehe Dialog ***Switching > L2-Redundanz***.
Auto-Disable	Zeigt, ob die ***Auto-Disable***-Funktion für den nebenstehenden Parameter aktiviert/deaktiviert ist. Mögliche Werte: ▶ `markiert` Die ***Auto-Disable***-Funktion für nebenstehende Parameter ist aktiv. die ***Auto-Disable***-Funktion schaltet bei Überschreiten der überwachten Parameter den betreffenden Port aus und ggf. wieder ein. ▶ `unmarkiert` (Voreinstellung) Die ***Auto-Disable***-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: ▶ Dialog ***Diagnose > Ports > Port-Monitor*** – Registerkarte ***Link-Änderungen*** – Registerkarte ***CRC/Fragmente*** – Registerkarte ***Überlast-Erkennung*** ▶ Dialog ***Diagnose > Ports > Auto-Disable***

6.4.5 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 ***Port-Mirroring***-Funktion ein/aus. Mögliche Werte: ▶ `An` Die ***Port-Mirroring***-Funktion ist eingeschaltet. Das Gerät kopiert die Datenpakete von den ausgewählten Quell-Ports auf den Ziel-Port. ▶ `Aus` (Voreinstellung) Die ***Port-Mirroring***-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: – Quell-Port – L2-Redundanz-Protokolle Mögliche Werte: ▶ `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.
Sekundärer Port	Legt einen zweiten Ziel-Port fest. Der Port überträgt dieselben Daten wie der oben festgelegte Port. Mögliche Werte: ▶ `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.

Parameter	Bedeutung
Management erlauben	Aktiviert/deaktiviert den Management-Zugriff über den Ziel-Port. Mögliche Werte: ▶ `markiert` 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 ***Port-Mirroring***-Sitzung zu unterbrechen. – 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. ▶ `unmarkiert` (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	Legt die Nummer des Ports fest. Mögliche Werte: ▶ `<Port-Nummer>`
Eingeschaltet	Aktiviert/deaktiviert das Kopieren der Datenpakete von diesem Quell-Port auf den Ziel-Port. Mögliche Werte: ▶ `markiert` Das Kopieren der Datenpakete ist aktiv. Der Port ist als Quell-Port festgelegt. ▶ `unmarkiert` (Voreinstellung) Das Kopieren der Datenpakete ist inaktiv. ▶ (Ausgegraute Darstellung) Das Kopieren der Datenpakete dieses Ports ist nicht möglich. Mögliche Ursachen: – Der Port ist bereits als Ziel-Port festgelegt. – Der Port ist ein logischer Port, kein physischer Port. **Anmerkung:** Das Gerät bietet Ihnen die Möglichkeit, abzüglich des Ziel-Ports jeden physischen Port als Quell-Port zu festzulegen.
Typ	Legt fest, welche Datenpakete das Gerät auf den Ziel-Port kopiert. Mögliche Werte: ▶ `none` (Voreinstellung) Keine Datenpakete. ▶ `tx` Datenpakete, die der Quell-Port sendet. ▶ `rx` Datenpakete, die der Quell-Port empfängt. ▶ `txrx` Datenpakete, die der Quell-Port sendet und empfängt. **Anmerkung:** Mit der Einstellung `txrx` kopiert das Gerät gesendete und empfangene Datenpakete. Der Ziel-Port benötigt mindestens eine Bandbreite, die der Summe aus Sende- und Empfangskanal der Quell-Ports entspricht. Beispielsweise ist bei gleichartigen Ports der Ziel-Port bereits zu 100 % ausgelastet, wenn Sende- und Empfangskanal eines Quell-Ports zu jeweils 50 % ausgelastet sind. 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.

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 ***LLDP***-Funktion ein/aus. Mögliche Werte: ▶ `An` (Voreinstellung) Die ***LLDP***-Funktion ist eingeschaltet. Die Topologie-Erkennung mit LLDP ist auf dem Gerät aktiv. ▶ `Aus` Die ***LLDP***-Funktion ist ausgeschaltet.

Konfiguration

Parameter	Bedeutung
Sende-Intervall [s]	Legt das Intervall in Sekunden fest, in dem das Gerät LLDP-Datenpakete sendet. Mögliche Werte: ▶ `5..32768` (Voreinstellung: `30`)
Sende-Intervall Multiplikator	Legt den Faktor zur Bestimmung des Time-to-live-Werts für die LLDP-Datenpakete fest. Mögliche Werte: ▶ `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 ***Sende-Intervall [s]***.
Reinitialisierungs-Verzögerung [s]	Legt die Verzögerung in Sekunden für die Re-Initialisierung eines Ports fest. Mögliche Werte: ▶ `1..10` (Voreinstellung: `2`) Wenn in Spalte ***Funktion*** der Wert `Aus` 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: ▶ `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: ▶ `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	Legt fest, ob der Port LLDP-Datenpakete sendet und empfängt. Mögliche Werte: ▶ `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.
Benachrichtung	Aktiviert/deaktiviert LLDP-Benachrichtigungen auf dem Port. Mögliche Werte: ▶ `markiert` LLDP-Benachrichtigungen auf dem Port sind aktiv. ▶ `unmarkiert` (Voreinstellung) LLDP-Benachrichtigungen auf dem Port sind inaktiv.
Port-Beschreibung senden	Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit der Port-Beschreibung. Mögliche Werte: ▶ `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	Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit dem Gerätenamen. Mögliche Werte: ▶ `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	Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit der Systembeschreibung. Mögliche Werte: ▶ `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	Aktiviert/deaktiviert das Senden des TLV (Type-Length-Value) mit den System-Ressourcen (Leistungsfähigkeitsdaten). Mögliche Werte: ▶ `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.)	Begrenzt für diesen Port die Anzahl der zu erfassenden benachbarten Geräte. Mögliche Werte: ▶ `1..50` (Voreinstellung: `10`)

Parameter	Bedeutung
FDB-Modus	Legt fest, welche Funktion das Gerät verwendet, um benachbarte Geräte an diesem Port zu erfassen. Mögliche Werte: ▶ `lldpOnly` Das Gerät verwendet ausschließlich LLDP-Datenpakete, um benachbarte Geräte an diesem Port zu erfassen. ▶ `macOnly` 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. ▶ `both` Das Gerät verwendet LLDP-Datenpakete und gelernte MAC-Adressen, um benachbarte Geräte an diesem Port zu erfassen. ▶ `autoDetect` (Voreinstellung) Empfängt das Gerät auf diesem Port LLDP-Datenpakete, arbeitet das Gerät wie mit der Einstellung `lldpOnly`. Andernfalls arbeitet das Gerät wie mit der Einstellung `macOnly`.

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.

Der Dialog enthält die folgenden Registerkarten:

- [LLDP]
- [LLDP-MED]

[LLDP]

Diese Registerkarte 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	Zeigt, ob das angeschlossene Gerät LLDP aktiv unterstützt. Mögliche Werte: ▶ `markiert` Das angeschlossene Gerät unterstützt kein LLDP. Das Gerät verwendet Informationen aus seiner Adresstabelle (FDB, Forwarding Database). ▶ `unmarkiert` (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 Pover over Ethernet (PoE) unterstützt.
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.

[LLDP-MED]

Bei „LLDP for Media Endpoint Devices“ (LLDP-MED) handelt es sich um eine Erweiterung von LLDP, welche zwischen Endgeräten und Netzgeräten arbeitet. Sie bietet insbesondere Unterstützung für VoIP-Anwendungen. Diese unterstützende Richtlinie bietet einen zusätzlichen Satz gebräuchlicher Mitteilungen (d. h. Nachrichten des Typs „Type Length Value“, TLV). Das Gerät nutzt die TLVs, um Funktionsmerkmale wie Netz-Richtlinien, PoE (Power over Ethernet), Bestandsverwaltung und Standortdaten zu ermitteln.

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Geräteklasse	Zeigt die Geräteklasse des über Fernverbindung angeschlossen Geräts. ▶ Der Wert `notDefined` zeigt an, dass das Gerät Funktionsmerkmale aufweist, welche durch keine der ***LLDP-MED***-Klassen abgedeckt sind. ▶ Der Wert `endpointClass1..3` zeigt an, dass das Gerät die Funktionsmerkmale „EndPoint-Klasse 1..3“ aufweist. ▶ Der Wert `networkConnectivity` zeigt an, dass das Gerät die Funktionsmerkmale eines Netzwerkverbindungsgeräts aufweist.
VLAN-ID	Zeigt die Erweiterung für die VLAN-Kennung des entfernten Systems, welches an diesem Port angeschlossen ist (gemäß IEEE 802.3). ▶ Das Gerät verwendet die Werte `1` bis `4042`, um eine gültige Port-VLAN-Kennung zu definieren. ▶ Das Gerät zeigt den Wert `0` für Pakete mit Prioritätsmarkierung. Dies bedeutet, dass ausschließlich die 802.1D-Priorität von Bedeutung ist und das Gerät die voreingestellte VLAN-Kennung des Eingangs-Ports verwendet.
Priorität	Zeigt den Wert der 802.1D-Priorität an, welche dem an diesem Port angeschlossenen entfernten System zugeordnet ist.
DSCP	Zeigt den Wert für den „Differentiated Service Code Point“ an, welcher dem an diesem Port angeschlossenen entfernten System zugeordnet ist.
Status Unknown-Bit	Zeigt den sog. „Unknown Bit Status“ des eingehenden Verkehrs an. ▶ Der Wert `true` zeigt an, dass die Netz-Richtlinie für den angegebenen Anwendungstyp gegenwärtig unbekannt ist. In diesem Fall ignoriert die VLAN-ID die Schicht-2-Priorität und den Wert des Feldes ***DSCP***. ▶ Der Wert `false` zeigt eine definierte Netz-Richtlinie an.
Status Tagged-Bit	Zeigt den sog. „Tagged Bit Status“ an. ▶ Der Wert `true` zeigt an, dass die Anwendung ein markiertes VLAN verwendet. ▶ Der Wert `false` zeigt an, dass das Gerät für die spezifische Anwendung auf einen unmarkierten VLAN-Betrieb zurückgreift. In diesem Fall ignoriert das Gerät sowohl die VLAN-ID wie auch die Schicht-2-Prioritätsfelder. Der DSCP-Wert hingegen ist relevant.
Hardware-Revision	Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Hardware-Revisionskennung an.
Firmware-Revision	Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Firmware-Revisionskennung an.
Software-Revision	Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Software-Revisionskennung an.
Seriennummer	Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Seriennummer an.
Herstellername	Zeigt den vom entfernten Endpunkt mitgeteilten spezifischen Herstellernamen an.
Modellname	Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Modellbezeichnung an.
Asset-ID	Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Kennung zur Produktverfolgung an.

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
- Persistentes Ereignisprotokoll
- 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 ***Console-Logging***-Funktion ein/aus. Mögliche Werte: ▶ `An` Die ***Console-Logging***-Funktion ist eingeschaltet. Das Gerät protokolliert die Ereignisse auf der Konsole. ▶ `Aus` (Voreinstellung) Die ***Console-Logging***-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: ▶ `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	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. Mögliche Werte: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (Voreinstellung) ▶ `notice` ▶ `informational` ▶ `debug`

SNMP-Logging

Parameter	Bedeutung
Protokolliere SNMP-Get-Requests	Schaltet die Protokollierung von SNMP Get requests ein/aus. Mögliche Werte: ▶ `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 ***Schweregrad Get-Request*** aus. ▶ `Aus` (Voreinstellung) Die Protokollierung ist ausgeschaltet.
Protokolliere SNMP-Set-Requests	Schaltet die Protokollierung von SNMP Set requests ein/aus. Mögliche Werte: ▶ `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 ***Schweregrad Set-Request*** aus. ▶ `Aus` (Voreinstellung) Die Protokollierung ist ausgeschaltet.
Schweregrad Get-Request	Legt den Schweregrad des Ereignisses fest, welches das Gerät bei SNMP Get requests protokolliert. Mögliche Werte: ▶ `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: ▶ `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 ***CLI-Logging***-Funktion ein/aus. Mögliche Werte: ▶ `An` Die ***CLI-Logging***-Funktion ist eingeschaltet. Das Gerät protokolliert jeden Befehl, den es über das Command Line Interface (CLI) empfängt. ▶ `Aus` (Voreinstellung) Die ***CLI-Logging***-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 `show running-config script`.
`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 ***Diagnose > Bericht > System Log***.

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 Persistentes Ereignisprotokoll

Das Gerät bietet Ihnen die Möglichkeit, die Log-Einträge in einer Datei auf dem externen Speicher permanent zu speichern. Somit haben Sie auch nach einem Neustart des Geräts Zugriff auf die Log-Einträge.

In diesem Dialog begrenzen Sie die Größe der Log-Datei und legen den Mindest-Schweregrad für zu speichernde Ereignisse fest. Erreicht die Log-Datei die festgelegte Größe, archiviert das Gerät diese Datei und speichert die folgenden Log-Einträge ein einer neu erstellten Datei.

In der Tabelle zeigt das Gerät Ihnen die auf dem externen Speicher vorgehaltenen Log-Dateien. Sobald die festgelegte maximale Anzahl an Dateien erreicht ist, löscht das Gerät die älteste Datei und benennt die verbleibenden Dateien um. Damit bleibt auf dem externen Speicher immer ausreichend Speicherplatz verfügbar.

Funktion

Parameter	Bedeutung
Funktion	Schaltet die ***Persistentes Ereignisprotokoll***-Funktion ein/aus. Aktivieren Sie die Funktion ausschließlich dann, wenn der externe Speicher im Gerät verfügbar ist. Mögliche Werte: ▶ `An` (Voreinstellung) Die ***Persistentes Ereignisprotokoll***-Funktion ist eingeschaltet. Das Gerät speichert die Log-Einträge in einer Datei auf dem externen Speicher. ▶ `Aus` Die ***Persistentes Ereignisprotokoll***-Funktion ist ausgeschaltet.

Konfiguration

Parameter	Bedeutung
Max. Dateigröße [kByte]	Legt die maximale Größe der Log-Datei in KBytes fest. Erreicht die Log-Datei die festgelegte Größe, archiviert das Gerät diese Datei und speichert die folgenden Log-Einträge ein einer neu erstellten Datei. Mögliche Werte: ▶ `0..4096` (Voreinstellung: `1024`) Der Wert `0` deaktiviert das Speichern der Log-Einträge in der Log-Datei.
Dateien (max.)	Legt die Anzahl an Log-Dateien fest, die das Gerät auf dem externen Speicher vorhält. Sobald die festgelegte maximale Anzahl an Dateien erreicht ist, löscht das Gerät die älteste Datei und benennt die verbleibenden Dateien um. Mögliche Werte: ▶ `0..25` (Voreinstellung: `4`) Der Wert `0` deaktiviert das Speichern der Log-Einträge in der Log-Datei.

Parameter	Bedeutung
Schweregrad	Legt den Mindest-Schweregrad der Ereignisse fest. Das Gerät speichert den Log-Eintrag für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden in der Log-Datei auf dem externen Speicher. Mögliche Werte: ▶ `emergency` ▶ `alert` ▶ `critical` ▶ `error` ▶ `warning` (Voreinstellung) ▶ `notice` ▶ `informational` ▶ `debug`
Ziel der Log-Datei	Legt den Typ des externen Speichers für die Protokollierung fest. Mögliche Werte: ▶ `usb` Externer USB-Speicher (ACA21/ACA22)

Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht. Mögliche Werte: ▶ `1..25` Das Gerät legt diese Nummer automatisch fest.
Dateiname	Zeigt den Dateinamen der Log-Datei auf dem externen Speicher. Mögliche Werte: ▶ `messages` ▶ `messages.X`
Dateigröße [Byte]	Zeigt die Größe der Log-Datei auf dem externen Speicher in Bytes.

Schaltflächen

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

Schaltfläche	Bedeutung
	Zeigt ein Untermenü mit folgenden Einträgen.
Persistente Log-Datei löschen	Entfernt die Log-Dateien vom externen Speicher.

6.6.3 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.

6.6.4 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:

- DHCP-L2-Relay
- DHCP-Server
- Industrie-Protokolle

7.1 DHCP-L2-Relay

Ein Netzadministrator verwendet den DHCP-L2-Relay-Agenten, um DHCP-Client-Informationen hinzuzufügen. DHCP-L3-Relay-Agenten und DHCP-Server benötigen diese Informationen, um den Clients eine IP-Adresse und eine Konfiguration zuzuweisen.

Sofern aktiv, fügt das Relais den Paketen die in diesem Dialog konfigurierten Option-82-Informationen hinzu, bevor es die DHCP-Anforderungen von den Clients an die Server übermittelt. Die Option-82-Felder stellen eindeutige Informationen über den Client und das Relais bereit. Diese eindeutige Kennung besteht aus einer Circuit-ID für den Client und einer Remote-ID für das Relais.

Zusätzlich zu den Typ-, Längen- und Multicast-Feldern beinhaltet die Circuit-ID die VLAN-ID, die Gerätenummer, die Steckplatznummer sowie die Port-Nummer für den angeschlossenen Client.

Die Remote-ID besteht aus einem Typ- und einem Längenfeld sowie entweder einer MAC-Adresse, einer IP-Adresse oder einer benutzerdefinierten Gerätebeschreibung. Bei einer Client-Kennung handelt es sich um einen benutzerdefinierten Systemnamen für das Gerät.

Das Menü enthält die folgenden Dialoge:
- DHCP-L2-Relay Konfiguration
- DHCP-L2-Relay Statistiken

7.1.1 DHCP-L2-Relay Konfiguration

Dieser Dialog bietet Ihnen die Möglichkeit, die Relais-Funktion an einem Port und an einem VLAN zu aktivieren. Wenn Sie diese Funktion an einem Port aktivieren, leitet das Gerät die Option-82-Informationen entweder weiter oder verwirft diese Informationen an ungesicherten Ports. Zudem bietet Ihnen das Gerät die Möglichkeit, die Remote-Kennung des VLANs festzulegen.

Der Dialog enthält die folgenden Registerkarten:
- [Interface]
- [VLAN-ID]

Funktion

Parameter	Bedeutung
Funktion	Schaltet die DHCP-L2-Relay-Funktion des Geräts global ein oder aus. Mögliche Werte: ▶ `An` Aktiviert die DHCP-L2-Relay-Funktion des Geräts. ▶ `Aus` (Voreinstellung) Deaktiviert die DHCP-L2-Relay-Funktion des Geräts.

[Interface]

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Aktiv	Aktiviert/deaktiviert die Funktion ***DHCP-L2-Relay*** auf dem Port. Voraussetzung ist, dass Sie die Funktion global aktivieren. Mögliche Werte: ▶ `markiert` Die ***DHCP-L2-Relay***-Funktion ist aktiv. ▶ `unmarkiert` (Voreinstellung) Die ***DHCP-L2-Relay***-Funktion ist inaktiv.
Gesicherter Port	Activiert/deaktiviert den gesicherten ***DHCP-L2-Relay***-Modus für den entsprechenden Port. Mögliche Werte: ▶ `markiert` Das Gerät akzeptiert DHCP-Pakete mit Option-82-Informationen. ▶ `unmarkiert` (Voreinstellung) Das Gerät verwirft die an ungesicherten Ports empfangenen DHCP-Pakete, welche Option-82-Informationen enthalten.

Schaltflächen

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

[VLAN-ID]

Tabelle

Parameter	Bedeutung
VLAN-ID	VLAN, auf das sich der Tabelleneintrag bezieht.
Aktiv	Aktiviert/deaktiviert die DHCP-L2-Relay-Funktion im VLAN. Voraussetzung ist, dass Sie die Funktion global aktivieren. Mögliche Werte: ▶ `markiert` Die DHCP-L2-Relay-Funktion ist aktiv. ▶ `unmarkiert` (Voreinstellung) Die DHCP-L2-Relay-Funktion ist inaktiv.
Circuit-ID	Aktiviert/deaktiviert das Hinzufügen der Circuit-ID zu den Option-82-Informationen. Mögliche Werte: ▶ `markiert` (Voreinstellung) Aktiviert das gemeinsame Senden von Circuit-ID und Remote-ID. ▶ `unmarkiert` Das Gerät sendet ausschließlich die Remote-ID.
Remote-ID-Typ	Legt die Komponenten der Remote-ID für dieses VLAN fest. Mögliche Werte: ▶ `ip` Legt die IP-Adresse des Geräts als Remote-ID fest. ▶ `mac` (Voreinstellung) Legt die MAC-Adresse des Geräts als Remote-ID fest. ▶ `client-id` Legt den Systemnamen des Geräts als Remote-ID fest. ▶ `other` Geben Sie in Spalte ***Remote-ID*** benutzerdefinierte Informationen ein, wenn Sie diesen Wert verwenden.
Remote-ID	Zeigt die Remote-ID für das VLAN an. Legen Sie die ID fest, wenn Sie in Spalte ***Remote-ID-Typ*** den Wert `other` festlegen.

Schaltflächen

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

7.1.2 DHCP-L2-Relay Statistiken

Das Gerät überwacht den Verkehr an den Ports und zeigt die Ergebnisse in tabellarischer Form an.

Die Tabelle ist in unterschiedliche Kategorien unterteilt, um Sie bei der Analyse zu unterstützen.

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
Ungesicherte Server-Nachrichten mit Option 82	Zeigt die Anzahl der Nachrichten vom DHCP-Server, welche mit Option-82-Informationen am ungesicherten Port eingegangen sind.
Ungesicherte Client-Nachrichten mit Option 82	Zeigt die Anzahl der Nachrichten vom DHCP-Client, welche mit Option-82-Informationen am ungesicherten Port eingegangen sind.
Gesicherte Server-Nachrichten ohne Option 82	Zeigt die Anzahl der Nachrichten vom DHCP-Server, welche ohne Option-82-Informationen am gesicherten Port eingegangen sind.
Gesicherte Client-Nachrichten ohne Option 82	Zeigt die Anzahl der Nachrichten vom DHCP-Client, welche ohne Option-82-Informationen am gesicherten Port eingegangen sind.

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.

7.2 DHCP-Server

Mit Hilfe des DHCP-Servers verwalten Sie eine Datenbank, welche die verfügbaren IP-Adressen sowie Konfigurationsdaten enthält. Wenn das Gerät eine Anfrage von einem Client erhält, prüft der DHCP-Server das Netz des DHCP-Clients und vergibt anschließend eine IP-Adresse. Sofern aktiviert, weist der DHCP-Server dem Client auch die entsprechenden Konfigurationsdaten zu. Die Konfigurationsdaten legen beispielsweise fest, welche IP-Adresse, welchen DNS-Server und welche Default-Route ein Client verwendet.

Der DHCP-Server weist einem Client für einen benutzerdefinierten Zeitraum eine bestimmte IP-Adresse zu. Der DHCP-Client ist verantwortlich dafür, die IP-Adresse vor Ablauf des Zeitraums zu verlängern. Falls der DHCP-Client außerstande ist, die Adresse zu verlängern, geht diese für eine anderweitige Zuteilung in den Pool zurück.

Das Menü enthält die folgenden Dialoge:

- DHCP-Server Global
- DHCP-Server Pool
- DHCP-Server Lease-Tabelle

7.2.1 DHCP-Server Global

Aktivieren Sie die Funktion entsprechend Ihren Anforderungen entweder global oder pro Port.

Funktion

Parameter	Bedeutung
Funktion	Schaltet die DHCP-Server-Funktion des Geräts global ein oder aus. Mögliche Werte: ▶ `An` ▶ `Aus` (Voreinstellung)

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports.
DHCP-Server aktiv	Aktiviert/deaktiviert die DHCP-Server-Funktion auf diesem Port. Voraussetzung ist, dass Sie die Funktion global aktivieren. Mögliche Werte: ▶ `markiert` (Voreinstellung) Die DHCP-Server-Funktion ist aktiv. ▶ `unmarkiert` Die DHCP-Server-Funktion ist inaktiv.

Schaltflächen

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

7.2.2 DHCP-Server Pool

Weisen Sie dem mit einem Port verbundenen Endgerät oder Switch eine IP-Adresse zu.

Der DHCP-Server stellt IP-Adress-Pools bereit, aus denen er den Clients IP-Adressen zuweist. Ein Pool besteht aus einer Liste mit Einträgen. Sie können einen Eintrag als statisch definieren, d. h. zu einer bestimmten IP-Adresse gehörend, oder als dynamisch, d. h. zu einem IP-Adressbereich gehörend. Das Gerät kann bis zu 128 Pools erfassen und speichern.

Bei statischer Zuteilung weist der DHCP-Server einem einzelnen Client eine bestimmte IP-Adresse zu. Der DHCP-Server identifiziert den Client über eine eindeutige Hardware-ID. Ein statischer Adresseintrag enthält 1 IP-Adresse. Diese IP-Adresse wenden Sie entweder auf jeden Port oder auf einen bestimmten Port des Geräts an. Für eine statische Zuteilung geben Sie im Feld ***IP-Adresse*** eine zuzuweisende IP-Adresse ein und lassen Spalte ***Letzte IP-Adresse*** frei. Geben Sie eine Hardware-Kennung an, mit welcher der DHCP-Server den Client eindeutig identifiziert. Bei dieser Kennung kann es sich um eine MAC-Adresse, eine Client-ID, eine Remote-ID oder eine Circuit-ID handeln. Wenn ein Client mit einer bekannten Hardware-Kennung das Gerät kontaktiert, weist der DHCP-Server die statische IP-Adresse zu.

Wenn ein DHCP-Client bei dynamischer Zuweisung einen Port kontaktiert, weist der DHCP-Server eine noch freie IP-Adresse aus einem Pool für diesen Port zu. Für eine dynamische Zuteilung erstellen Sie einen Pool für die Ports, indem Sie einen IP-Adressbereich zuweisen. Legen Sie die erste und die letzte IP-Adresse des IP-Adressbereiches fest. Lassen Sie die Felder ***MAC-Adresse***, ***Client-ID***, ***Remote-ID*** und ***Circuit-ID*** frei. Sie haben die Möglichkeit, mehrere Pool-Einträge zu erzeugen. Hierdurch erzeugen Sie einen IP-Adressbereich, der Lücken enthält.

Dieser Dialog zeigt die unterschiedlichen Informationen an, die zur Vergabe einer IP-Adresse für einen Port oder ein VLAN erforderlich sind. Verwenden Sie die Schaltfläche  , um einen Eintrag hinzuzufügen. Das Gerät fügt einen schreib- und lesbaren Eintrag hinzu.

Tabelle

Parameter	Bedeutung
Index	Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.
Aktiv	Aktiviert/deaktiviert die DHCP-Server-Funktion auf diesem Port. Mögliche Werte: ▶ `markiert` Die DHCP-Server-Funktion ist aktiv. ▶ `unmarkiert` (Voreinstellung) Die DHCP-Server-Funktion ist inaktiv.
IP-Adresse	Legt die IP-Adresse für die statische IP-Adresszuweisung fest. Wenn Sie die dynamische IP-Adresszuweisung verwenden, definiert dieser Wert den Beginn des IP-Adressraums. Mögliche Werte: ▶ Gültige IPv4-Adresse
Letzte IP-Adresse	Wenn Sie die dynamische IP-Adresszuweisung verwenden, definiert dieser Wert das Ende des IP-Adressraums. Mögliche Werte: ▶ Gültige IPv4-Adresse
Port	Zeigt die Nummer des Ports.

Parameter	Bedeutung
VLAN-ID	Zeigt das VLAN, auf das sich der Tabelleneintrag bezieht. Der Wert `1` entspricht dem standardmäßigen Management-VLAN. Mögliche Werte: ▶ `1..4042`
MAC-Adresse	Legt die MAC-Adresse des Geräts fest, welches die IP-Adresse vergibt. 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` ▶ `-` Bei der IP-Adresszuweisung ignoriert der Server diese Variable.
DHCP-Relay	Legt die IP-Adresse des DHCP-Relays fest, über das Clients ihre Anfrage an den DHCP-Server senden. Wenn der DHCP-Server die Anfrage eines Clients über ein anderes DHCP-Relay empfängt, ignoriert er diese. Mögliche Werte: ▶ Gültige IPv4-Adresse IP-Adresse des DHCP-Relays. ▶ `-` Zwischen Client und DHCP-Server befindet sich kein DHCP-Relay.
Client-ID	Legt die Kennzeichnung des Client-Geräts fest, welches die IP-Adresse vergibt. Mögliche Werte: ▶ 1..80 Bytes (Format `XX XX .. XX`) ▶ `-` Bei der IP-Adresszuweisung ignoriert der Server diese Variable.
Remote-ID	Legt die Kennzeichnung des entfernten Geräts fest, welches die IP-Adresse vergibt. Mögliche Werte: ▶ 1..80 Bytes (Format `XX XX .. XX`) ▶ `-` Bei der IP-Adresszuweisung ignoriert der Server diese Variable.
Circuit-ID	Legt die Circuit-ID des Geräts fest, welches die IP-Adresse vergibt. Mögliche Werte: ▶ 1..80 Bytes (Format `XX XX .. XX`) ▶ `-` Bei der IP-Adresszuweisung ignoriert der Server diese Variable.
Hirschmann-Gerät	Aktiviert/deaktiviert Hirschmann-Multicasts. Aktivieren Sie diese Funktion, wenn das Gerät in diesem IP-Adressbereich ausschließlich Hirschmann-Geräte bedient. Mögliche Werte: ▶ `markiert` Das Gerät bedient in diesem IP-Adressbereich ausschließlich Hirschmann-Geräte. Hirschmann-Multicasts sind aktiviert. ▶ `unmarkiert` (Voreinstellung) Das Gerät bedient in diesem IP-Adressbereich Geräte unterschiedlicher Hersteller. Hirschmann-Multicasts sind deaktiviert.
Konfigurations-URL	Legt das verwendete Protokoll sowie den Namen und den Pfad zur Konfigurationsdatei fest. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..70 Zeichen Beispiel: `tftp://192.9.200.1/cfg/config.sav` Wenn Sie diesen Eintrag frei lassen, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt.

Parameter	Bedeutung
Lease-Time [s]	Legt die Vergabezeit in Sekunden fest. Mögliche Werte: ▶ `1..4294967294` (Voreinstellung: `86400`) ▶ `4294967295` Verwenden Sie diesen Wert für zeitlich unbegrenzte Vergaben oder für Vergaben über BOOTP.
Default-Gateway	Legt die IP-Adresse des Standard-Gateways fest. Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt. Mögliche Werte: ▶ Gültige IPv4-Adresse
Netzmaske	Legt die Maske des Netzes fest, zu welcher der Client gehört. Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt. Mögliche Werte: ▶ Gültige IPv4-Netzmaske
WINS-Server	Legt die IP-Adresse des Windows Internet Name Servers fest, welcher NetBIOS-Namen konvertiert. Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt. Mögliche Werte: ▶ Gültige IPv4-Adresse
DNS-Server	Legt die IP-Adresse des DNS-Servers fest. Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt. Mögliche Werte: ▶ Gültige IPv4-Adresse
Hostname	Legt den Host-Namen fest. Wenn Sie diesen Eintrag frei lassen, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Schaltflächen

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

7.2.3 DHCP-Server Lease-Tabelle

Dieser Dialog zeigt den Status der IP-Adressvergabe an den einzelnen Ports.

Tabelle

Parameter	Bedeutung
Port	Zeigt die Nummer des Ports, an welchen die Adresse gegenwärtig vergeben ist.
IP-Adresse	Zeigt die vergebene IP-Adresse, auf die sich der Eintrag bezieht.
Status	Zeigt die Phase der Vergabe an. Gemäß DHCP-Standard läuft die Vergabe von IP-Adressen in 4 Schritten ab: Discovery (Client sendet Anfrage an Server), Offer (Server bieten IP-Adresse an), Request (Client fordert IP-Adresse an) sowie Acknowledgement (Server bestätigt Adresse). Mögliche Werte: ▶ `bootp` Ein DHCP-Client versucht gerade, einen DHCP-Server für die IP-Adresszuweisung zu ermitteln. ▶ `offering` Der DHCP-Server prüft gerade, ob die IP-Adresse für den Client geeignet ist. ▶ `requesting` Ein DHCP-Client bezieht gerade die angebotene IP-Adresse. ▶ `bound` Der DHCP-Server vergibt die IP-Adresse an einen Client. ▶ `renewing` Der DHCP-Client fordert eine Verlängerung der Adressvergabe an. ▶ `rebinding` Nach einer erfolgreichen Verlängerung vergibt der DHCP-Server die IP-Adresse an den Client. ▶ `declined` Der DHCP-Server hat die Anfrage nach der IP-Adresse abgelehnt. ▶ `released` Die IP-Adresse steht für andere Clients zur Verfügung.
Verbleibende Lifetime	Zeigt die verbleibende Zeit für die Vergabe der IP-Adresse an.
Vergeben an MAC-Adresse	Zeigt die MAC-Adresse des Geräts, welches die IP-Adresse vergibt.
Gateway	Zeigt die Gateway-IP-Adresse des Geräts, welches die IP-Adresse vergibt.
Client-ID	Zeigt die Client-Kennung des Geräts, welches die IP-Adresse vergibt.
Remote-ID	Zeigt die Remote-Kennung des Geräts, welches die IP-Adresse vergibt.
Circuit-ID	Zeigt die Circuit-ID des Geräts, welches die IP-Adresse vergibt.

Schaltflächen

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

7.3 Industrie-Protokolle

Das Menü enthält die folgenden Dialoge:

- IEC61850-MMS
- Modbus TCP

7.3.1 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 *IEC61850-MMS*-Server ein/aus. Mögliche Werte: ▶ `An` Der *IEC61850-MMS*-Server ist eingeschaltet. ▶ `Aus` (Voreinstellung) Der *IEC61850-MMS*-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	Legt den IED-Namen fest. Der IED-Name ist unabhängig vom System-Namen einstellbar. Mögliche Werte: ▶ Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen Die folgenden Zeichen sind zulässig: – _ – `0..9` – `a..z` – `A..Z` (Voreinstellung: `KEY`) Damit der MMS-Server den IED-Namen verwendet, klicken Sie die Schaltfläche ✓ und starten Sie den MMS-Server neu. Dabei bricht die Verbindung zu verbundenen Clients ab.
TCP-Port	Legt den TCP-Port für den Zugriff auf den MMS-Server fest. Mögliche Werte: ▶ `1..65535` (Voreinstellung: `102`) Ausnahme: Port `2222` ist für interne Funktionen reserviert. **Anmerkung:** Nachdem Sie den Port geändert haben, startet der Server automatisch neu. Offene Verbindungen zum Server beendet das Gerät dabei.
Sessions (max.)	Legt die maximale Anzahl an MMS-Server-Verbindungen fest. Mögliche Werte: ▶ `1..15` (Voreinstellung: `5`)

Information

Parameter	Bedeutung
Status	Zeigt den gegenwärtigen Status des *IEC61850-MMS*-Servers. Mögliche Werte: ▶ `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.

7.3.2 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 ***Modbus TCP***-Server im Gerät ein/aus. Mögliche Werte: ▶ `An` Der ***Modbus TCP***-Server ist eingeschaltet. ▶ `Aus` (Voreinstellung) Der ***Modbus TCP***-Server ist ausgeschaltet.

Konfiguration

Parameter	Bedeutung
Schreibzugriff	Aktiviert/deaktiviert den Schreibzugriff auf die ***Modbus TCP*** 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 ***Modbus TCP***-Server ist aktiv. Dies bietet Ihnen die Möglichkeit, die Geräte-Konfiguration über das ***Modbus TCP***-Protokoll zu ändern. ▶ `unmarkiert` Der Lesezugriff für den ***Modbus TCP***-Server ist aktiv.

Parameter	Bedeutung
TCP-Port	Legt die TCP-Port-Nummer fest, die der *Modbus TCP*-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 *Modbus TCP*-Server zulässt. Mögliche Werte: ▶ `1..5` (Voreinstellung: `5`)

Schaltflächen

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

A Index

1
802.1D/p-Mapping 174
802.1X 74, 106

A
Access-Control-Listen 128
ACL 128
Adresskonflikt-Erkennung 241
Aging Time 138, 244
Alarme 235
Anforderungsintervall 64
ARP 241
ARP-Tabelle 244
Audit-Trail 285
Ausgangs-Lastbegrenzer 140
Authentifizierungs-Historie 114
Authentifizierungs-Liste 74
Auto-Disable 102, 192, 256, 257, 257, 263

B
Benutzerverwaltung 70
Bridge 190

C
CLI 94
Command Line Interface 94
Community-Namen 97

D
DHCP-L2-Relay 288
DHCP-Server 293
DoS 124
DSCP 175

E
EAPOL 113
Eingangs-Lastbegrenzer 140
Einstellungen 33
ENVM 32, 33, 37, 43, 215, 222, 230, 283
Ereignis-Schweregrad 281
Externer Speicher 32, 33, 37, 43, 283

F
FAQ 307
FDB 142
Fingerprint 85, 89
Flash-Speicher 32, 238
Flusskontrolle 138
Forwarding-Tabelle 142

G
GARP 167
Gerätestatus 22, 213
Geräte-Software 31
Geräte-Software Backup 31
GMRP 168
Grenzwerte Netzlast 140
Guards 200
GVRP 170

H
Hardware-Uhr 58
Hardware-Zustand 238
HiDiscovery 28, 29, 81, 223, 285
Host-Key 86
HTML 237, 284
HTTP 87
HTTPS 88
HTTP-Server 221

I
IAS 74, 116
IEC61850 MMS 223, 300
IEEE 802.1X 74
IGMP-Snooping 144
Industrial HiVision 11, 81
Ingress Filtering 182
Integrierter Authentifikations-Server 74, 116
IPv4-Regel 129
IP-Adressen Konflikterkennung 241
IP-DSCP-Mapping 175
IP-Zugriffsbeschränkung 91

K
Kabeldiagnose 251
Konfigurationsprofil 17, 33
Konfigurations-Check 239
Kontextmenü 17

L
L2-Relay 288
Laden/Speichern 33
Lastbegrenzer 140
Link-Aggregation 202
Link-Backup 207
LLDP 269
Logdatei 54, 284
Login-Banner 96, 98
Loops 189

M
Management-VLAN 28
Management-Zugriff 28, 91
Manufacturing Message Specification 300
MAC-Adress-Filter 142
MAC-Adress-Tabelle 142
MAC-Flooding 101
MAC-Regel 132
MAC-Spoofing 101
Media Redundancy Protocol 186
Menü 17
MMRP 158
MMS 300
Modbus TCP 223, 302
Module 215, 229
MRP 186
MRP-IEEE 156
MVRP 163

N

Netzlast 53, 53
Neustart 54
NVM 16, 18, 24, 32, 37

P

Passwort 70, 220, 221
Passwort-Länge 70, 220
Persistentes Ereignisprotokoll 282
Portsicherheit 101
Port-basierte Zugriffskontrolle 106
Port-Clients 112
Port-Konfiguration 109, 173
Port-Mirroring 266
Port-Monitor 263
Port-Priorität 173
Port-Statistiken 113
Port-VLAN 182
Pre-Login-Banner 98

Q

Queues 172
Queue-Management 177

R

RADIUS 74, 117
RAM 37
RAM-Test 245
Relay 288
Ringstruktur 186
Root-Bridge 190
RSTP 189, 190

S

Schulungsangebote 307
Schweregrad 281
Secure Shell 84
Selbsttest 245
SFP-Modul 250
Sicherheitsstatus 22, 219
Signalkontakt 23, 226
Signatur 85
SNMPv1/v2 97
SNMP-Server 81, 222
SNMP-Traps 49, 102, 190, 203, 214, 220, 229, 235, 243, 256
SNTP 63
SNTP-Client 64
SNTP-Server 67
Software-Backup 31
Software-Update 31
Sommerzeit 60
Spanning Tree Protocol 189
SSH-Server 84
Stromversorgung 23, 215, 230
Switch-Dump 281
Syslog 247
Systeminformationen 237
Systemzeit 59
System Log 284
System-Monitor 245

T

Technische Fragen 307
Telnet-Server 83, 221
Temperatur 24, 214, 229
Topologie-Erkennung 273
Traps 49, 102, 190, 203, 214, 220, 229, 235, 243, 256
Trap-Ziel 235
Trust Modus 173
Twisted-Pair-Kabel 251

U

Unaware-Modus 138

V

Verschlüsselung 33
Virtual Local Area Network 178
VLAN 28, 178
VLAN Konfiguration 180
VLAN-Ports 182
VLAN-Unaware-Modus 138
V.24 222

W

Warteschlange (Queue) 172
Watchdog 33, 36
Webserver 87, 88

Z

Zähler-Reset 54
Zertifikat 23, 42, 89, 90, 223
ZIP-Archiv 281
Zugriffsbeschränkung 91
Zugriffskontrolle 106

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	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer +49 (0)7127 14-1600 oder
- per Post an

  Hirschmann Automation and Control GmbH
  Abteilung 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

Reference Manual

Command Line Interface
HiOS-2S GRS (Greyhound 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.

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

Rel. 6.1 - 09/2016 – 10.01.2018

Contents

Safety instructions 26

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 appllists 38
3.1.1 appllists set-authlist 38
3.1.2 appllists enable 38
3.1.3 appllists disable 38

3.2 show 39
3.2.1 show appllists 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 Cabletest 51

6.1 cable-test 52

6.1.1 cable-test 52

7 Class Of Service 53

7.1 classofservice 54
7.1.1 classofservice ip-dscp-mapping 54
7.1.2 classofservice dot1p-mapping 57

7.2 classofservice 58
7.2.1 classofservice trust 58

7.3 cos-queue 59
7.3.1 cos-queue strict 59
7.3.2 cos-queue weighted 59
7.3.3 cos-queue min-bandwidth 59

7.4 show 61
7.4.1 show classofservice ip-dscp-mapping 61
7.4.2 show classofservice dot1p-mapping 61
7.4.3 show classofservice trust 61
7.4.4 show cos-queue 62

8 Command Line Interface (CLI) 63

8.1 cli 64
8.1.1 cli serial-timeout 64
8.1.2 cli prompt 64
8.1.3 cli numlines 65
8.1.4 cli banner operation 65
8.1.5 cli banner text 65

8.2 show 66
8.2.1 show cli global 66
8.2.2 show cli command-tree 66

8.3 logging 67
8.3.1 logging cli-command 67

8.4 show 68
8.4.1 show logging cli-command 68

9 Clock 69

9.1 clock 70
9.1.1 clock set 70
9.1.2 clock timezone offset 70
9.1.3 clock timezone zone 70
9.1.4 clock summer-time mode 71
9.1.5 clock summer-time recurring start 71
9.1.6 clock summer-time recurring end 72
9.1.7 clock summer-time zone 72

9.2 show 73
9.2.1 show clock 73

10 Configuration 75

10.1 save 76
10.1.1 save profile 76

10.2 config 77
10.2.1 config watchdog admin-state 77
10.2.2 config watchdog timeout 77
10.2.3 config encryption password set 78
10.2.4 config encryption password clear 78
10.2.5 config envm auto-update 78
10.2.6 config envm sshkey-auto-update 79
10.2.7 config envm config-save 79

10.2.8 config envm load-priority 80
10.2.9 config envm usb-compatibility 80
10.2.10 config profile select 80
10.2.11 config profile delete 81
10.2.12 config fingerprint verify 81
10.3 copy 82
10.3.1 copy sysinfo system envm 82
10.3.2 copy sysinfoall system envm 82
10.3.3 copy firmware envm 82
10.3.4 copy firmware remote 83
10.3.5 copy config running-config nvm 83
10.3.6 copy config running-config remote 83
10.3.7 copy config nvm 84
10.3.8 copy config envm 84
10.3.9 copy config remote 84
10.3.10 copy sfp-white-list remote 85
10.3.11 copy sfp-white-list envm 85
10.4 clear 86
10.4.1 clear config 86
10.4.2 clear factory 86
10.4.3 clear sfp-white-list 86
10.5 show 87
10.5.1 show running-config xml 87
10.5.2 show running-config script 87
10.6 show 88
10.6.1 show config envm settings 88
10.6.2 show config envm properties 88
10.6.3 show config envm usb-compatibility 88
10.6.4 show config watchdog 89
10.6.5 show config encryption 89
10.6.6 show config profiles 89
10.6.7 show config status 89
10.7 swap 90
10.7.1 swap firmware system backup 90

11 Debugging 91

11.1 debug 92
11.1.1 debug tcpdump help 92
11.1.2 debug tcpdump start cpu 92
11.1.3 debug tcpdump stop 92
11.1.4 debug tcpdump filter show 93
11.1.5 debug tcpdump filter list 93
11.1.6 debug tcpdump filter delete 93
11.2 show 94
11.2.1 show debug logic-modules 94
11.3 copy 95
11.3.1 copy tcpdumpcap nvm envm 95
11.3.2 copy tcpdumpcap nvm remote 95
11.3.3 copy tcpdumpfilter remote 95
11.3.4 copy tcpdumpfilter envm 96
11.3.5 copy tcpdumpfilter nvm 96

12 Device Monitoring 97

12.1 device-status 98
12.1.1 device-status monitor link-failure 98
12.1.2 device-status monitor temperature 98
12.1.3 device-status monitor module-removal 99
12.1.4 device-status monitor envm-removal 99
12.1.5 device-status monitor envm-not-in-sync 99

12.1.6 device-status monitor ring-redundancy 100
12.1.7 device-status monitor power-supply 100
12.1.8 device-status trap 101
12.1.9 device-status module 101
12.2 device-status 102
12.2.1 device-status link-alarm 102
12.3 show 103
12.3.1 show device-status monitor 103
12.3.2 show device-status state 103
12.3.3 show device-status trap 103
12.3.4 show device-status events 104
12.3.5 show device-status link-alarm 104
12.3.6 show device-status module 104
12.3.7 show device-status all 104

13 Device Security 105

13.1 security-status 106
13.1.1 security-status monitor pwd-change 106
13.1.2 security-status monitor pwd-min-length 106
13.1.3 security-status monitor pwd-policy-config 107
13.1.4 security-status monitor pwd-str-not-config 107
13.1.5 security-status monitor pwd-policy-inactive 107
13.1.6 security-status monitor bypass-pwd-strength 108
13.1.7 security-status monitor telnet-enabled 108
13.1.8 security-status monitor http-enabled 109
13.1.9 security-status monitor snmp-unsecure 109
13.1.10 security-status monitor sysmon-enabled 109
13.1.11 security-status monitor extnvm-upd-enabled 110
13.1.12 security-status monitor no-link-enabled 110
13.1.13 security-status monitor hidisc-write-enabled 111
13.1.14 security-status monitor extnvm-load-unsecure 111
13.1.15 security-status monitor iec61850-mms-enabled 111
13.1.16 security-status monitor https-certificate 112
13.1.17 security-status monitor modbus-tcp-enabled 112
13.1.18 security-status trap 113
13.2 security-status 114
13.2.1 security-status no-link 114
13.3 show 115
13.3.1 show security-status monitor 115
13.3.2 show security-status state 115
13.3.3 show security-status no-link 115
13.3.4 show security-status trap 116
13.3.5 show security-status events 116
13.3.6 show security-status all 116

14 Dynamic Host Configuration Protocol (DHCP) 117

14.1 dhcp-server 118
14.1.1 dhcp-server operation 118
14.2 dhcp-server 119
14.2.1 dhcp-server operation 119
14.2.2 dhcp-server pool add 119
14.2.3 dhcp-server pool modify 120
14.2.4 dhcp-server pool mode 121
14.2.5 dhcp-server pool delete 121
14.3 show 122
14.3.1 show dhcp-server operation 122
14.3.2 show dhcp-server pool 122
14.3.3 show dhcp-server interface 122
14.3.4 show dhcp-server lease 123

15 DHCP Layer 2 Relay 125

15.1 dhcp-l2relay 126
15.1.1 dhcp-l2relay mode 126

15.2 dhcp-l2relay 127
15.2.1 dhcp-l2relay mode 127
15.2.2 dhcp-l2relay circuit-id 127
15.2.3 dhcp-l2relay remote-id ip 128
15.2.4 dhcp-l2relay remote-id mac 128
15.2.5 dhcp-l2relay remote-id client-id 128
15.2.6 dhcp-l2relay remote-id other 129

15.3 dhcp-l2relay 130
15.3.1 dhcp-l2relay mode 130
15.3.2 dhcp-l2relay trust 130

15.4 clear 131
15.4.1 clear dhcp-l2relay statistics 131

15.5 show 132
15.5.1 show dhcp-l2relay global 132
15.5.2 show dhcp-l2relay statistics 132
15.5.3 show dhcp-l2relay interfaces 132
15.5.4 show dhcp-l2relay vlan 133

16 DHCP Snooping 135

16.1 ip 136
16.1.1 ip dhcp-snooping verify-mac 136
16.1.2 ip dhcp-snooping mode 136
16.1.3 ip dhcp-snooping database storage 137
16.1.4 ip dhcp-snooping database write-delay 137
16.1.5 ip dhcp-snooping binding add 137
16.1.6 ip dhcp-snooping binding delete all 138
16.1.7 ip dhcp-snooping binding delete interface 138
16.1.8 ip dhcp-snooping binding delete mac 138
16.1.9 ip dhcp-snooping binding mode 139

16.2 clear 140
16.2.1 clear ip dhcp-snooping bindings 140
16.2.2 clear ip dhcp-snooping statistics 140

16.3 ip 141
16.3.1 ip dhcp-snooping trust 141
16.3.2 ip dhcp-snooping log 141
16.3.3 ip dhcp-snooping auto-disable 142
16.3.4 ip dhcp-snooping limit 142

16.4 show 143
16.4.1 show ip dhcp-snooping global 143
16.4.2 show ip dhcp-snooping statistics 143
16.4.3 show ip dhcp-snooping interfaces 143
16.4.4 show ip dhcp-snooping vlan 144
16.4.5 show ip dhcp-snooping bindings 144

17 DoS Mitigation 145

17.1 dos 146
17.1.1 dos tcp-null 146
17.1.2 dos tcp-xmas 146
17.1.3 dos tcp-syn-fin 147
17.1.4 dos tcp-min-header 147
17.1.5 dos icmp-fragmented 147
17.1.6 dos icmp payload-check 148
17.1.7 dos icmp payload-size 148
17.1.8 dos ip-land 149

17.1.9 dos tcp-offset 149
17.1.10 dos tcp-syn 149
17.1.11 dos l4-port 150
17.2 show 151
17.2.1 show dos 151
18 IEEE 802.1x (Dot1x) 153
18.1 dot1x 154
18.1.1 dot1x dynamic-vlan 154
18.1.2 dot1x system-auth-control 154
18.1.3 dot1x monitor 155
18.2 dot1x 156
18.2.1 dot1x guest-vlan 156
18.2.2 dot1x max-req 156
18.2.3 dot1x port-control 156
18.2.4 dot1x re-authentication 157
18.2.5 dot1x unauthenticated-vlan 157
18.2.6 dot1x timeout guest-vlan-period 158
18.2.7 dot1x timeout reauth-period 158
18.2.8 dot1x timeout quiet-period 158
18.2.9 dot1x timeout tx-period 158
18.2.10 dot1x timeout supp-timeout 159
18.2.11 dot1x timeout server-timeout 159
18.2.12 dot1x initialize 159
18.2.13 dot1x re-authenticate 160
18.3 show 161
18.3.1 show dot1x global 161
18.3.2 show dot1x auth-history 161
18.3.3 show dot1x detail 161
18.3.4 show dot1x summary 162
18.3.5 show dot1x clients 162
18.3.6 show dot1x statistics 162
18.4 clear 163
18.4.1 clear dot1x statistics port 163
18.4.2 clear dot1x statistics all 163
18.4.3 clear dot1x auth-history port 163
18.4.4 clear dot1x auth-history all 164
19 IEEE 802.3ad (Dot3ad) 165
19.1 link-aggregation 166
19.1.1 link-aggregation add 166
19.1.2 link-aggregation modify 166
19.1.3 link-aggregation delete 167
19.2 lacp 168
19.2.1 lacp admin-key 168
19.2.2 lacp collector-max-delay 168
19.2.3 lacp lacpmode 168
19.2.4 lacp actor admin key 169
19.2.5 lacp actor admin state lacp-activity 169
19.2.6 lacp actor admin state lacp-timeout 170
19.2.7 lacp actor admin state aggregation 170
19.2.8 lacp actor admin port priority 170
19.2.9 lacp partner admin key 171
19.2.10 lacp partner admin state lacp-activity 171
19.2.11 lacp partner admin state lacp-timeout 171
19.2.12 lacp partner admin state aggregation 172
19.2.13 lacp partner admin port priority 172
19.2.14 lacp partner admin port id 172
19.2.15 lacp partner admin system-priority 173
19.2.16 lacp partner admin system-id 173

19.3 show 174
19.3.1 show link-aggregation port 174
19.3.2 show link-aggregation statistics 174
19.3.3 show link-aggregation members 174
19.3.4 show lacp interface 175
19.3.5 show lacp mode 175
19.3.6 show lacp actor 175
19.3.7 show lacp partner operational 175
19.3.8 show lacp partner admin 176

20 Filtering Database (FDB) 177

20.1 mac-filter 178
20.1.1 mac-filter 178
20.2 bridge 179
20.2.1 bridge aging-time 179
20.3 show 180
20.3.1 show mac-filter-table static 180
20.4 show 181
20.4.1 show bridge aging-time 181
20.5 show 182
20.5.1 show mac-addr-table 182
20.6 clear 183
20.6.1 clear mac-addr-table 183

21 GARP VLAN and Multicast Registration Protocol (GVRP and GMRP) 185

21.1 garp 186
21.1.1 garp gvrp operation 186
21.1.2 garp gmrp operation 186
21.1.3 garp gmrp forward-unknown 187
21.2 garp 188
21.2.1 garp interface join-time 188
21.2.2 garp interface leave-time 188
21.2.3 garp interface leave-all-time 189
21.2.4 garp gvrp operation 189
21.2.5 garp gmrp operation 189
21.2.6 garp gmrp forward-all-groups 190
21.3 show 191
21.3.1 show garp interface 191
21.3.2 show garp gvrp global 191
21.3.3 show garp gvrp interface 191
21.3.4 show garp gvrp statistics interface 192
21.3.5 show garp gmrp global 192
21.3.6 show garp gmrp interface 192
21.3.7 show garp gmrp statistics interface 192
21.4 show 193
21.4.1 show mac-filter-table gmrp 193

22 HiDiscovery 195

22.1 network 196
22.1.1 network hidiscovery operation 196
22.1.2 network hidiscovery mode 196
22.1.3 network hidiscovery blinking 197
22.1.4 network hidiscovery relay 197
22.2 show 198
22.2.1 show network hidiscovery 198

23 Hypertext Transfer Protocol (HTTP) 199

23.1 http 200
23.1.1 http port 200
23.1.2 http server 200

23.2 show 201
23.2.1 show http 201

24 HTTP Secure (HTTPS) 203

24.1 https 204
24.1.1 https server 204
24.1.2 https port 204
24.1.3 https certificate 205

24.2 copy 206
24.2.1 copy httpscert remote 206
24.2.2 copy httpscert envm 206

24.3 show 207
24.3.1 show https 207

25 Integrated Authentification Server (IAS) 209

25.1 ias-users 210
25.1.1 ias-users add 210
25.1.2 ias-users delete 210
25.1.3 ias-users enable 210
25.1.4 ias-users disable 211
25.1.5 ias-users password 211

25.2 show 212
25.2.1 show ias-users 212

26 IEC 61850 MMS Server 213

26.1 iec61850-mms 214
26.1.1 iec61850-mms operation 214
26.1.2 iec61850-mms write-access 214
26.1.3 iec61850-mms port 215
26.1.4 iec61850-mms max-sessions 215
26.1.5 iec61850-mms technical-key 215

26.2 show 216
26.2.1 show iec61850-mms 216

27 Internet Group Management Protocol (IGMP) 217

27.1 ip 218
27.1.1 ip igmp operation 218

27.2 ip 219
27.2.1 ip igmp operation 219
27.2.2 ip igmp version 219
27.2.3 ip igmp robustness 220
27.2.4 ip igmp querier query-interval 220
27.2.5 ip igmp querier last-member-interval 220
27.2.6 ip igmp querier max-response-time 220

27.3 show 222
27.3.1 show ip igmp global 222
27.3.2 show ip igmp interface 222
27.3.3 show ip igmp membership 222
27.3.4 show ip igmp groups 223
27.3.5 show ip igmp statistics 223

28 IGMP Proxy 225

28.1 ip 226
28.1.1 ip igmp-proxy interface 226
28.1.2 ip igmp-proxy report-interval 226

28.2 show 227
28.2.1 show ip igmp-proxy global 227
28.2.2 show ip igmp-proxy groups 227
28.2.3 show ip igmp-proxy source-list 227

29 IGMP Snooping 229

29.1 igmp-snooping 230
29.1.1 igmp-snooping mode 230
29.1.2 igmp-snooping querier mode 230
29.1.3 igmp-snooping querier query-interval 231
29.1.4 igmp-snooping querier timer-expiry 231
29.1.5 igmp-snooping querier version 231
29.1.6 igmp-snooping forward-unknown 232

29.2 igmp-snooping 233
29.2.1 igmp-snooping vlan-id 233

29.3 igmp-snooping 235
29.3.1 igmp-snooping mode 235
29.3.2 igmp-snooping fast-leave 235
29.3.3 igmp-snooping groupmembership-interval 236
29.3.4 igmp-snooping maxresponse 236
29.3.5 igmp-snooping mcrtrexpiretime 236
29.3.6 igmp-snooping static-query-port 236

29.4 show 238
29.4.1 show igmp-snooping global 238
29.4.2 show igmp-snooping interface 238
29.4.3 show igmp-snooping vlan 238
29.4.4 show igmp-snooping querier global 239
29.4.5 show igmp-snooping querier vlan 239
29.4.6 show igmp-snooping enhancements vlan 239
29.4.7 show igmp-snooping enhancements unknown-filtering 239
29.4.8 show igmp-snooping statistics global 240
29.4.9 show igmp-snooping statistics interface 240

29.5 show 241
29.5.1 show mac-filter-table igmp-snooping 241

29.6 clear 242
29.6.1 clear igmp-snooping 242

30 Interface 243

30.1 shutdown 244
30.1.1 shutdown 244

30.2 auto-negotiate 245
30.2.1 auto-negotiate 245

30.3 auto-power-down 246
30.3.1 auto-power-down 246

30.4 cable-crossing 247
30.4.1 cable-crossing 247

30.5 linktraps 248
30.5.1 linktraps 248

30.6 link-loss-alert 249
30.6.1 link-loss-alert operation 249

30.7 speed 250
30.7.1 speed 250
30.8 name 251
30.8.1 name 251
30.9 power-state 252
30.9.1 power-state 252
30.10 mac-filter 253
30.10.1 mac-filter 253
30.11 led-signaling 254
30.11.1 led-signaling operation 254
30.12 show 255
30.12.1 show port 255
30.13 show 256
30.13.1 show link-loss-alert 256
30.14 show 257
30.14.1 show led-signaling operation 257

31 Interface Statistics 259

31.1 utilization 260
31.1.1 utilization control-interval 260
31.1.2 utilization alarm-threshold lower 260
31.1.3 utilization alarm-threshold upper 260
31.2 clear 262
31.2.1 clear port-statistics 262
31.3 show 263
31.3.1 show interface counters 263
31.3.2 show interface layout 263
31.3.3 show interface utilization 263
31.3.4 show interface statistics 264
31.3.5 show interface ether-stats 264

32 Intern 265

32.1 help 266
32.2 logout 267
32.3 history 268
32.4 vlan-mode 269
32.4.1 vlan-mode 269
32.5 exit 270
32.6 end 271
32.7 serviceshell 272
32.7.1 serviceshell deactivate 272
32.8 serviceshell-f 273
32.8.1 serviceshell-f deactivate 273
32.9 traceroute 274
32.9.1 traceroute maxttl 274
32.10 traceroute 275
32.10.1 traceroute source 275
32.11 reboot 276
32.11.1 reboot after 276
32.12 ping 277
32.12.1 ping 277

32.13 ping 278
32.13.1 ping source 278
32.14 show 279
32.14.1 show reboot 279
32.14.2 show serviceshell 279

33 Open Shortest Path First (OSPF) 281

33.1 ip 282
33.1.1 ip ospf area 282
33.1.2 ip ospf trapflags all 284
33.1.3 ip ospf operation 285
33.1.4 ip ospf 1583compatability 285
33.1.5 ip ospf default-metric 286
33.1.6 ip ospf router-id 286
33.1.7 ip ospf external-lsdb-limit 286
33.1.8 ip ospf exit-overflow 287
33.1.9 ip ospf spf-delay 287
33.1.10 ip ospf spf-holdtime 287
33.1.11 ip ospf auto-cost 288
33.1.12 ip ospf distance intra 288
33.1.13 ip ospf distance inter 288
33.1.14 ip ospf distance external 289
33.1.15 ip ospf re-distribute 289
33.1.16 ip ospf distribute-list 290
33.1.17 ip ospf default-info originate 290
33.2 ip 292
33.2.1 ip ospf operation 292
33.2.2 ip ospf area-id 292
33.2.3 ip ospf link-type 293
33.2.4 ip ospf priority 293
33.2.5 ip ospf transmit-delay 293
33.2.6 ip ospf retransmit-interval 294
33.2.7 ip ospf hello-interval 294
33.2.8 ip ospf dead-interval 294
33.2.9 ip ospf cost 295
33.2.10 ip ospf mtu-ignore 295
33.2.11 ip ospf authentication type 296
33.2.12 ip ospf authentication key 296
33.2.13 ip ospf authentication key-id 296
33.3 show 297
33.3.1 show ip ospf global 297
33.3.2 show ip ospf area 297
33.3.3 show ip ospf stub 297
33.3.4 show ip ospf database internal 298
33.3.5 show ip ospf database external 298
33.3.6 show ip ospf range 298
33.3.7 show ip ospf interface 298
33.3.8 show ip ospf virtual-link 299
33.3.9 show ip ospf virtual-neighbor 299
33.3.10 show ip ospf neighbor 299
33.3.11 show ip ospf statistics 299
33.3.12 show ip ospf re-distribute 300
33.3.13 show ip ospf nssa 300
33.3.14 show ip ospf route 300

34 Internet Protocol Version 4 (IPv4) 301

34.1 network 302
34.1.1 network protocol 302
34.1.2 network parms 302
34.2 clear 303

34.2.1 clear arp-table-switch 303
34.3 show 304
34.3.1 show network parms 304
34.4 show 305
34.4.1 show arp 305

35 Link Backup 307

35.1 link-backup 308
35.1.1 link-backup operation 308
35.2 link-backup 309
35.2.1 link-backup add 309
35.2.2 link-backup delete 309
35.2.3 link-backup modify 310
35.3 show 311
35.3.1 show link-backup operation 311
35.3.2 show link-backup pairs 311

36 Link Layer Discovery Protocol (LLDP) 313

36.1 lldp 314
36.1.1 lldp operation 314
36.1.2 lldp config chassis admin-state 314
36.1.3 lldp config chassis notification-interval 315
36.1.4 lldp config chassis re-init-delay 315
36.1.5 lldp config chassis tx-delay 315
36.1.6 lldp config chassis tx-hold-multiplier 316
36.1.7 lldp config chassis tx-interval 316
36.2 show 317
36.2.1 show lldp global 317
36.2.2 show lldp port 317
36.2.3 show lldp remote-data 317
36.3 lldp 318
36.3.1 lldp admin-state 318
36.3.2 lldp fdb-mode 318
36.3.3 lldp max-neighbors 319
36.3.4 lldp notification 319
36.3.5 lldp tlv inline-power 319
36.3.6 lldp tlv link-aggregation 320
36.3.7 lldp tlv mac-phy-config-state 320
36.3.8 lldp tlv max-frame-size 320
36.3.9 lldp tlv mgmt-addr 321
36.3.10 lldp tlv port-desc 321
36.3.11 lldp tlv port-vlan 322
36.3.12 lldp tlv protocol 322
36.3.13 lldp tlv sys-cap 323
36.3.14 lldp tlv sys-desc 323
36.3.15 lldp tlv sys-name 323
36.3.16 lldp tlv vlan-name 324
36.3.17 lldp tlv protocol-based-vlan 324
36.3.18 lldp tlv igmp 325
36.3.19 lldp tlv portsec 325
36.3.20 lldp tlv ptp 325

37 Media Endpoint Discovery LLDP-MED 327

37.1 lldp 328
37.1.1 lldp med confignotification 328
37.1.2 lldp med transmit-tlv capabilities 328
37.1.3 lldp med transmit-tlv network-policy 329
37.2 lldp 330

37.2.1 lldp med faststartrepeatcount 330

37.3 show 331
37.3.1 show lldp med global 331
37.3.2 show lldp med interface 331
37.3.3 show lldp med local-device 331
37.3.4 show lldp med remote-device detail 332
37.3.5 show lldp med remote-device summary 332

38 Logging 333

38.1 logging 334
38.1.1 logging audit-trail 334
38.1.2 logging buffered severity 334
38.1.3 logging host add 335
38.1.4 logging host delete 335
38.1.5 logging host enable 336
38.1.6 logging host disable 336
38.1.7 logging host modify 336
38.1.8 logging syslog operation 337
38.1.9 logging current-console operation 337
38.1.10 logging current-console severity 338
38.1.11 logging console operation 338
38.1.12 logging console severity 339
38.1.13 logging persistent operation 339
38.1.14 logging persistent numfiles 340
38.1.15 logging persistent filesize 340
38.1.16 logging persistent severity-level 340
38.1.17 logging email operation 341
38.1.18 logging email from-addr 341
38.1.19 logging email duration 342
38.1.20 logging email severity urgent 342
38.1.21 logging email severity non-urgent 343
38.1.22 logging email to-addr add 343
38.1.23 logging email to-addr delete 344
38.1.24 logging email to-addr modify 344
38.1.25 logging email mail-server add 344
38.1.26 logging email mail-server delete 345
38.1.27 logging email mail-server modify 345
38.1.28 logging email subject add 346
38.1.29 logging email subject delete 346
38.1.30 logging email subject modify 347
38.1.31 logging email test msgtype 347

38.2 show 348
38.2.1 show logging buffered 348
38.2.2 show logging traplogs 348
38.2.3 show logging console 348
38.2.4 show logging persistent 349
38.2.5 show logging syslog 349
38.2.6 show logging host 349
38.2.7 show logging email statistics 349
38.2.8 show logging email global 350
38.2.9 show logging email to-addr 350
38.2.10 show logging email subject 350
38.2.11 show logging email mail-server 350

38.3 copy 352
38.3.1 copy eventlog buffered envm 352
38.3.2 copy eventlog buffered remote 352
38.3.3 copy eventlog persistent 352
38.3.4 copy traplog system envm 353
38.3.5 copy traplog system remote 353
38.3.6 copy audittrail system envm 353
38.3.7 copy audittrail system remote 354

38.3.8 copy mailcacert remote 354
38.3.9 copy mailcacert envm 354
38.3.10 copy syslogcacert remote 355
38.3.11 copy syslogcacert envm 355
38.4 clear 356
38.4.1 clear logging buffered 356
38.4.2 clear logging persistent 356
38.4.3 clear logging email statistics 356
38.4.4 clear eventlog 357

39 MAC Notification 359

39.1 mac 360
39.1.1 mac notification operation 360
39.1.2 mac notification interval 360
39.2 mac 361
39.2.1 mac notification operation 361
39.3 show 362
39.3.1 show mac notification global 362
39.3.2 show mac notification interface 362

40 Management Access 363

40.1 network 364
40.1.1 network management access web timeout 364
40.1.2 network management access add 364
40.1.3 network management access delete 365
40.1.4 network management access modify 365
40.1.5 network management access operation 366
40.1.6 network management access status 367
40.2 show 368
40.2.1 show network management access global 368
40.2.2 show network management access rules 368

41 Modbus 369

41.1 modbus-tcp 370
41.1.1 modbus-tcp operation 370
41.1.2 modbus-tcp write-access 370
41.1.3 modbus-tcp port 371
41.1.4 modbus-tcp max-sessions 371
41.2 show 372
41.2.1 show modbus-tcp 372

42 Media Redundancy Protocol (MRP) 373

42.1 mrp 374
42.1.1 mrp domain modify advanced-mode 374
42.1.2 mrp domain modify manager-priority 374
42.1.3 mrp domain modify mode 374
42.1.4 mrp domain modify name 375
42.1.5 mrp domain modify operation 375
42.1.6 mrp domain modify port primary 375
42.1.7 mrp domain modify port secondary 376
42.1.8 mrp domain modify recovery-delay 376
42.1.9 mrp domain modify round-trip-delay 376
42.1.10 mrp domain modify vlan 377
42.1.11 mrp domain add default-domain 377
42.1.12 mrp domain add domain-id 377
42.1.13 mrp domain delete 377
42.1.14 mrp operation 378

42.2 show 379
42.2.1 show mrp 379

43 MRP IEEE 381

43.1 mrp-ieee 382
43.1.1 mrp-ieee global join-time 382
43.1.2 mrp-ieee global leave-time 382
43.1.3 mrp-ieee global leave-all-time 383

43.2 show 384
43.2.1 show mrp-ieee global interface 384

44 MRP IEEE MMRP 385

44.1 mrp-ieee 386
44.1.1 mrp-ieee mmrp vlan-id 386

44.2 show 387
44.2.1 show mrp-ieee mmrp global 387
44.2.2 show mrp-ieee mmrp interface 387
44.2.3 show mrp-ieee mmrp statistics global 387
44.2.4 show mrp-ieee mmrp statistics interface 388
44.2.5 show mrp-ieee mmrp service-requirement forward-all vlan 388
44.2.6 show mrp-ieee mmrp service-requirement forbidden vlan 388

44.3 mrp-ieee 389
44.3.1 mrp-ieee mmrp operation 389
44.3.2 mrp-ieee mmrp periodic-machine 389

44.4 clear 390
44.4.1 clear mrp-ieee mmrp 390

44.5 mrp-ieee 391
44.5.1 mrp-ieee mmrp operation 391
44.5.2 mrp-ieee mmrp restrict-register 391

44.6 show 392
44.6.1 show mac-filter-table mmrp 392

45 MRP IEEE MVRP 393

45.1 mrp-ieee 394
45.1.1 mrp-ieee mvrp operation 394
45.1.2 mrp-ieee mvrp periodic-machine 394

45.2 mrp-ieee 395
45.2.1 mrp-ieee mvrp operation 395
45.2.2 mrp-ieee mvrp restrict-register 395

45.3 show 396
45.3.1 show mrp-ieee mvrp global 396
45.3.2 show mrp-ieee mvrp interface 396
45.3.3 show mrp-ieee mvrp statistics global 396
45.3.4 show mrp-ieee mvrp statistics interface 397

45.4 clear 398
45.4.1 clear mrp-ieee mvrp 398

46 Out-of-band Management 399

46.1 network 400
46.1.1 network out-of-band operation 400
46.1.2 network out-of-band protocol 400
46.1.3 network out-of-band parms 401

46.2 show 402

47 Protocol Based VLAN 403

47.1 vlan 404
47.1.1 vlan protocol group add 404
47.1.2 vlan protocol group modify 404
47.1.3 vlan protocol group delete 405

47.2 vlan 406
47.2.1 vlan protocol group add 406
47.2.2 vlan protocol group delete 406

47.3 show 407

48 Port Monitor 409

48.1 port-monitor 410
48.1.1 port-monitor operation 410

48.2 port-monitor 411
48.2.1 port-monitor condition crc-fragments interval 411
48.2.2 port-monitor condition crc-fragments count 411
48.2.3 port-monitor condition crc-fragments mode 411
48.2.4 port-monitor condition link-flap interval 412
48.2.5 port-monitor condition link-flap count 412
48.2.6 port-monitor condition link-flap mode 412
48.2.7 port-monitor condition duplex-mismatch mode 413
48.2.8 port-monitor condition overload-detection traffic-type 413
48.2.9 port-monitor condition overload-detection unit 414
48.2.10 port-monitor condition overload-detection upper-threshold 414
48.2.11 port-monitor condition overload-detection lower-threshold 414
48.2.12 port-monitor condition overload-detection polling-interval 415
48.2.13 port-monitor condition overload-detection mode 415
48.2.14 port-monitor condition speed-duplex mode 415
48.2.15 port-monitor condition speed-duplex speed 416
48.2.16 port-monitor condition speed-duplex clear 416
48.2.17 port-monitor action 416
48.2.18 port-monitor reset 417

48.3 show 418
48.3.1 show port-monitor operation 418
48.3.2 show port-monitor brief 418
48.3.3 show port-monitor overload-detection counters 418
48.3.4 show port-monitor overload-detection port 419
48.3.5 show port-monitor speed-duplex 419
48.3.6 show port-monitor port 419
48.3.7 show port-monitor link-flap 419
48.3.8 show port-monitor crc-fragments 420

49 Port Security 421

49.1 port-security 422
49.1.1 port-security operation 422

49.2 port-security 423
49.2.1 port-security operation 423
49.2.2 port-security max-dynamic 423
49.2.3 port-security max-static 424
49.2.4 port-security mac-address add 424
49.2.5 port-security mac-address move 424
49.2.6 port-security mac-address delete 424
49.2.7 port-security violation-traps 425

49.3 show 426
49.3.1 show port-security global 426
49.3.2 show port-security interface 426
49.3.3 show port-security dynamic 426

49.3.4 show port-security static 427
49.3.5 show port-security violation 427

50 Password Management 429

50.1 passwords 430
50.1.1 passwords min-length 430
50.1.2 passwords max-login-attempts 430
50.1.3 passwords min-uppercase-chars 430
50.1.4 passwords min-lowercase-chars 431
50.1.5 passwords min-numeric-chars 431
50.1.6 passwords min-special-chars 431

50.2 show 432
50.2.1 show passwords 432

51 Radius 433

51.1 authorization 434
51.1.1 authorization network radius 434

51.2 radius 435
51.2.1 radius accounting mode 435
51.2.2 radius server attribute 4 435
51.2.3 radius server acct add 436
51.2.4 radius server acct delete 436
51.2.5 radius server acct modify 436
51.2.6 radius server auth add 437
51.2.7 radius server auth delete 437
51.2.8 radius server auth modify 438
51.2.9 radius server retransmit 438
51.2.10 radius server timeout 439

51.3 show 440
51.3.1 show radius global 440
51.3.2 show radius auth servers 440
51.3.3 show radius auth statistics 440
51.3.4 show radius acct statistics 441
51.3.5 show radius acct servers 441

51.4 clear 442
51.4.1 clear radius 442

52 Remote Monitoring (RMON) 443

52.1 rmon-alarm 444
52.1.1 rmon-alarm add 444
52.1.2 rmon-alarm enable 444
52.1.3 rmon-alarm disable 445
52.1.4 rmon-alarm delete 445
52.1.5 rmon-alarm modify 445

52.2 show 447
52.2.1 show rmon statistics 447
52.2.2 show rmon alarm 447

53 Script File 449

53.1 script 450
53.1.1 script apply 450
53.1.2 script validate 450
53.1.3 script list system 450
53.1.4 script list envm 451
53.1.5 script delete 451

53.2 copy 452
53.2.1 copy script envm 452

53.2.2 copy script remote 452
53.2.3 copy script nvm 453
53.2.4 copy script running-config nvm 453
53.2.5 copy script running-config envm 453
53.2.6 copy script running-config remote 454
53.3 show 455
53.3.1 show script envm 455
53.3.2 show script system 455

54 Selftest 457

54.1 selftest 458
54.1.1 selftest action 458
54.1.2 selftest ramtest 458
54.1.3 selftest system-monitor 459
54.1.4 selftest boot-default-on-error 459
54.2 show 460
54.2.1 show selftest action 460
54.2.2 show selftest settings 460

55 Small Form-factor Pluggable (SFP) 461

55.1 show 462
55.1.1 show sfp 462

56 Signal Contact 463

56.1 signal-contact 464
56.1.1 signal-contact mode 464
56.1.2 signal-contact monitor link-failure 464
56.1.3 signal-contact monitor module-removal 465
56.1.4 signal-contact monitor envm-not-in-sync 465
56.1.5 signal-contact monitor envm-removal 466
56.1.6 signal-contact monitor temperature 466
56.1.7 signal-contact monitor ring-redundancy 466
56.1.8 signal-contact monitor power-supply 467
56.1.9 signal-contact state 467
56.1.10 signal-contact trap 468
56.1.11 signal-contact module 468
56.2 signal-contact 469
56.2.1 signal-contact link-alarm 469
56.3 show 470
56.3.1 show signal-contact 470

57 Slot 471

57.1 slot 472
57.1.1 slot operation 472
57.1.2 slot module 472
57.2 show 473
57.2.1 show slot 473

58 Switched Monitoring (SMON) 475

58.1 monitor 476
58.1.1 monitor session 476
58.2 show 478
58.2.1 show monitor session 478
58.3 clear 479
58.3.1 clear monitor session 479

59 Simple Network Management Protocol (SNMP) 481

59.1 snmp 482
59.1.1 snmp access version v1 482
59.1.2 snmp access version v2 482
59.1.3 snmp access version v3 483
59.1.4 snmp access port 483
59.1.5 snmp access snmp-over-802 483

59.2 show 484
59.2.1 show snmp access 484

60 SNMP Community 485

60.1 snmp 486
60.1.1 snmp community ro 486
60.1.2 snmp community rw 486

60.2 show 487
60.2.1 show snmp community 487

61 SNMP Logging 489

61.1 logging 490
61.1.1 logging snmp-request get operation 490
61.1.2 logging snmp-request get severity 490
61.1.3 logging snmp-request set operation 491
61.1.4 logging snmp-request set severity 492

61.2 show 493
61.2.1 show logging snmp 493

62 Simple Network Time Protocol (SNTP) 495

62.1 sntp 496
62.1.1 sntp client operation 496
62.1.2 sntp client operating-mode 496
62.1.3 sntp client request-interval 497
62.1.4 sntp client broadcast-rcv-timeout 497
62.1.5 sntp client disable-after-sync 497
62.1.6 sntp client server add 498
62.1.7 sntp client server delete 498
62.1.8 sntp client server mode 498
62.1.9 sntp server operation 499
62.1.10 sntp server port 499
62.1.11 sntp server only-if-synchronized 499
62.1.12 sntp server broadcast operation 500
62.1.13 sntp server broadcast address 500
62.1.14 sntp server broadcast port 500
62.1.15 sntp server broadcast interval 501
62.1.16 sntp server broadcast vlan 501

62.2 show 502
62.2.1 show sntp global 502
62.2.2 show sntp client status 502
62.2.3 show sntp client server 502
62.2.4 show sntp server status 503
62.2.5 show sntp server broadcast 503

63 Spanning Tree 505

63.1 spanning-tree 506
63.1.1 spanning-tree operation 506
63.1.2 spanning-tree bpdu-filter 506
63.1.3 spanning-tree bpdu-guard 507

63.1.4 spanning-tree bpdu-migration-check 507
63.1.5 spanning-tree forceversion 507
63.1.6 spanning-tree forward-time 508
63.1.7 spanning-tree hello-time 508
63.1.8 spanning-tree hold-count 508
63.1.9 spanning-tree max-age 508
63.1.10 spanning-tree ring-only-mode operation 509
63.1.11 spanning-tree ring-only-mode first-port 509
63.1.12 spanning-tree ring-only-mode second-port 509
63.1.13 spanning-tree mst 510
63.2 spanning-tree 511
63.2.1 spanning-tree mode 511
63.2.2 spanning-tree bpdu-flood 511
63.2.3 spanning-tree edge-auto 512
63.2.4 spanning-tree edge-port 512
63.2.5 spanning-tree guard-loop 512
63.2.6 spanning-tree guard-root 513
63.2.7 spanning-tree guard-tcn 513
63.2.8 spanning-tree cost 514
63.2.9 spanning-tree priority 514
63.3 show 515
63.3.1 show spanning-tree global 515
63.3.2 show spanning-tree mst instance 515
63.3.3 show spanning-tree mst port 515
63.3.4 show spanning-tree port 516

64 Secure Shell (SSH) 517

64.1 ssh 518
64.1.1 ssh server 518
64.1.2 ssh timeout 518
64.1.3 ssh port 519
64.1.4 ssh max-sessions 519
64.1.5 ssh outbound max-sessions 519
64.1.6 ssh outbound timeout 519
64.1.7 ssh key rsa 520
64.1.8 ssh key dsa 520
64.2 copy 521
64.2.1 copy sshkey remote 521
64.2.2 copy sshkey envm 521
64.3 show 522
64.3.1 show ssh 522

65 Storm Control 523

65.1 storm-control 524
65.1.1 storm-control flow-control 524
65.2 traffic-shape 525
65.2.1 traffic-shape bw 525
65.3 mtu 526
65.3.1 mtu 526
65.4 mtu 527
65.4.1 mtu 527
65.5 storm-control 528
65.5.1 storm-control flow-control 528
65.5.2 storm-control ingress unit 528
65.5.3 storm-control ingress threshold 529
65.5.4 storm-control ingress unicast operation 529
65.5.5 storm-control ingress multicast operation 529
65.5.6 storm-control ingress broadcast operation 530

65.6 show 531
65.6.1 show storm-control flow-control 531
65.6.2 show storm-control ingress 531
65.6.3 show traffic-shape 531
65.6.4 show mtu 532

66 System 533

66.1 system 534
66.1.1 system name 534
66.1.2 system location 534
66.1.3 system contact 534
66.1.4 system port-led-mode 535
66.1.5 system pre-login-banner operation 535
66.1.6 system pre-login-banner text 536
66.1.7 system resources operation 536

66.2 temperature 537
66.2.1 temperature upper-limit 537
66.2.2 temperature lower-limit 537

66.3 show 538
66.3.1 show eventlog 538
66.3.2 show system info 538
66.3.3 show system port-led-mode 538
66.3.4 show system pre-login-banner 539
66.3.5 show system flash-status 539
66.3.6 show system temperature limits 539
66.3.7 show system temperature extremes 539
66.3.8 show system temperature histogram 540
66.3.9 show system temperature counters 540
66.3.10 show system resources 540
66.3.11 show psu slot 540
66.3.12 show psu unit 541

67 Telnet 543

67.1 telnet 544
67.1.1 telnet server 544
67.1.2 telnet timeout 544
67.1.3 telnet port 545
67.1.4 telnet max-sessions 545

67.2 telnet 546
67.2.1 telnet 546

67.3 show 547
67.3.1 show telnet 547

68 Traps 549

68.1 snmp 550
68.1.1 snmp trap operation 550
68.1.2 snmp trap mode 550
68.1.3 snmp trap delete 551
68.1.4 snmp trap add 551

68.2 show 552
68.2.1 show snmp traps 552

69 User Management 553

69.1 show 554
69.1.1 show custom-role global 554
69.1.2 show custom-role commands 554

70 Users 555

70.1 users 556
70.1.1 users add 556
70.1.2 users delete 556
70.1.3 users enable 556
70.1.4 users disable 557
70.1.5 users password 557
70.1.6 users snmpv3 authentication 557
70.1.7 users snmpv3 encryption 558
70.1.8 users access-role 558
70.1.9 users lock-status 558
70.1.10 users password-policy-check 559

70.2 show 560
70.2.1 show users 560

71 Virtual LAN (VLAN) 561

71.1 name 562
71.1.1 name 562

71.2 vlan-unaware-mode 563
71.2.1 vlan-unaware-mode 563

71.3 vlan 564
71.3.1 vlan add 564
71.3.2 vlan delete 564

71.4 vlan 565
71.4.1 vlan acceptframe 565
71.4.2 vlan ingressfilter 565
71.4.3 vlan priority 566
71.4.4 vlan pvid 566
71.4.5 vlan tagging 566
71.4.6 vlan participation include 567
71.4.7 vlan participation exclude 567
71.4.8 vlan participation auto 567

71.5 show 568
71.5.1 show vlan id 568
71.5.2 show vlan brief 568
71.5.3 show vlan port 568
71.5.4 show vlan member current 569
71.5.5 show vlan member static 569

71.6 network 570
71.6.1 network management vlan 570
71.6.2 network management priority dot1p 570
71.6.3 network management priority ip-dscp 570

72 Voice VLAN 571

72.1 voice 572
72.1.1 voice vlan 572

72.2 voice 573
72.2.1 voice vlan vlan-id 573
72.2.2 voice vlan dot1p 573
72.2.3 voice vlan none 574
72.2.4 voice vlan untagged 574
72.2.5 voice vlan disable 574
72.2.6 voice vlan auth 574
72.2.7 voice vlan data priority 575

72.3 show 576
72.3.1 show voice vlan global 576

72.3.2show voice vlan interface 576

A Further Support 577

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>`

Parameter	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>`

Parameter	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>]]]]`

Parameter	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 Cabletest

6.1 cable-test

6.1.1 cable-test

Select port on which to perform the cable test.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `cable-test <P-1>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

7 Class Of Service

7.1 classofservice

Class of service configuration.

7.1.1 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.

7.1.2 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.

7.2 classofservice

Interface classofservice configuration.

7.2.1 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.`

7.3 cos-queue

COS queue configuration

7.3.1 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.`

7.3.2 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.`

7.3.3 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>`

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.

7.4 show

Display device options and settings.

7.4.1 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`

7.4.2 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`

7.4.3 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`

7.4.4 show cos-queue

Show cosqueue parameters

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show cos-queue`

8 Command Line Interface (CLI)

8.1 cli

Set the CLI preferences.

8.1.1 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.`

8.1.2 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`

8.1.3 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.

8.1.4 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`

8.1.5 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).

8.2 show

Display device options and settings.

8.2.1 show cli global

Display CLI preferences.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show cli global`

8.2.2 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`

8.3 logging

Logging configuration.

8.3.1 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`

8.4 show

Display device options and settings.

8.4.1 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`

9 Clock

9.1 clock

Configure local and DST clock settings.

9.1.1 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.

9.1.2 clock timezone offset

Local time offset (in minutes) with respect to UTC (positive values for locations east of\nGreenwich).

- 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).

9.1.3 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).

9.1.4 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.

9.1.5 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).

9.1.6 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).

9.1.7 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).

9.2 show

Display device options and settings.

9.2.1 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.

10 Configuration

10.1 save

Save the configuration to the specified destination.

10.1.1 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.`

10.2 config

Configure the configuration saving settings.

10.2.1 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`

10.2.2 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.`

10.2.3 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.`

10.2.4 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.`

10.2.5 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>`

10.2.6 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>`

10.2.7 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>`

10.2.8 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.

10.2.9 config envm usb-compatibility

Changes the USB compatibility mode. The changes take effect only after saving the settings and rebooting the device.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `config envm usb-compatibility <P-1>`

Parameter	Value	Meaning
P-1	normal	Normal Mode
	compatibility	Compatibility Mode

no config envm usb-compatibility
Disable the option

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `no config envm usb-compatibility <P-1>`

10.2.10 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.

10.2.11 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.

10.2.12 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.

10.3 copy

Copy different kinds of items.

10.3.1 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.`

10.3.2 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`

10.3.3 copy firmware envm

Copy a firmware image to the device from external non-volatile memory.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `copy firmware envm <P-1> system`

`system`: Copy a firmware image to the device from external non-volatile memory.

Parameter	Value	Meaning
`P-1`	string	Filename.

10.3.4 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.`

10.3.5 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.`

10.3.6 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.`

10.3.7 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.`

10.3.8 copy config envm

Copy a configuration from external non-volatile memory to non-volatile memory.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `copy config envm [profile <P-1>] nvm`

`[profile]`: Copy a specfic configuration profile from external non-volatile memory to non-volatile memory.
`nvm`: Copy a specific profile from external non-volatile memory to non-volatile memory.

Parameter	Value	Meaning
`P-1`	string	Filename.

10.3.9 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.`

10.3.10 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.`

10.3.11 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.`

10.4 clear

Clear several items.

10.4.1 clear config

Clear the running configuration.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `clear config`

10.4.2 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).

10.4.3 clear sfp-white-list

Clear the SFP WhiteList.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `clear sfp-white-list`

10.5 show

Display device options and settings.

10.5.1 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`

10.5.2 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).

10.6 show

Display device options and settings.

10.6.1 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`

10.6.2 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`

10.6.3 show config envm usb-compatibility

Show the USB compatibility mode. The admin mode takes effect after saving the settings and rebooting the device.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show config envm usb-compatibility`

10.6.4 show config watchdog

Show the Auto Configuration Undo settings.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show config watchdog`

10.6.5 show config encryption

Show the settings for config encryption.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show config encryption`

10.6.6 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.`

10.6.7 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`

10.7 swap

Swap software images.

10.7.1 swap firmware system backup

Swap the main and backup images.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `swap firmware system backup`

11 Debugging

11.1 debug

Different tools to assist in debugging the device.

11.1.1 debug tcpdump help

Display help file for the tcpdump tool.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `debug tcpdump help`

11.1.2 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).

Parameter	Value	Meaning
`P-1`	string	`<filename> Enter a valid filename.`
`P-2`	string	`Enter a user-defined text, max. 255 characters.`

11.1.3 debug tcpdump stop

Abort capture of network traffic.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `debug tcpdump stop`

11.1.4 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.`

11.1.5 debug tcpdump filter list

Display all available filter files.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `debug tcpdump filter list`

11.1.6 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.`

11.2 show

Display device options and settings.

11.2.1 show debug logic-modules

List logic module information
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `show debug logic-modules`

11.3 copy

Copy different kinds of items.

11.3.1 copy tcpdumpcap nvm envm

Copy the capture file from non-volatile memory to external non-volatile memory.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `copy tcpdumpcap nvm envm [<P-1>]`

Parameter	Value	Meaning
`P-1`	string	`<filename> Enter a valid filename.`

11.3.2 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.`

11.3.3 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.`

Parameter	Value	Meaning
P-2	string	<filename> Enter a valid filename.

11.3.4 copy tcpdumpfilter envm

Copy the capture filter from external non-volatile memory to the specified destination.
- Mode: Privileged Exec Mode
- Privilege Level: Operator
- Format: copy tcpdumpfilter envm <P-1> nvm [<P-2>]

nvm: Copy the capture filter from external non-volatile memory to non-volatile memory.

Parameter	Value	Meaning
P-1	string	<filename> Enter a valid filename.
P-2	string	<filename> Enter a valid filename.

11.3.5 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.

12 Device Monitoring

12.1 device-status

Configure various device conditions to be monitored.

12.1.1 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`

12.1.2 device-status monitor temperature

Enable or disable monitoring of the device temperature.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `device-status monitor temperature`

no device-status monitor temperature
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no device-status monitor temperature`

12.1.3 device-status monitor module-removal

Enable or disable monitoring the presence of modules.

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `device-status monitor module-removal`

no device-status monitor module-removal

Disable the option

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no device-status monitor module-removal`

12.1.4 device-status monitor envm-removal

Enable or disable monitoring the presence of the external non-volatile memory.

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `device-status monitor envm-removal`

no device-status monitor envm-removal

Disable the option

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no device-status monitor envm-removal`

12.1.5 device-status monitor envm-not-in-sync

Enable or disable monitoring synchronization between the external non-volatile memory\n and the running configuration.

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `device-status monitor envm-not-in-sync`

- **no device-status monitor envm-not-in-sync**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Administrator`
  - Format: `no device-status monitor envm-not-in-sync`

12.1.6 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`

12.1.7 device-status monitor power-supply

Enable or disable monitoring the condition of the power supply(s).
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `device-status monitor power-supply <P-1>`

Parameter	Value	Meaning
`P-1`	1..2	`Number of power supply.`

- **no device-status monitor power-supply**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Administrator`
  - Format: `no device-status monitor power-supply <P-1>`

12.1.8 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`

12.1.9 device-status module

Configure the monitoring of the specific module.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `device-status module <P-1>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

no device-status module
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no device-status module <P-1>`

12.2 device-status

Configure various device conditions to be monitored.

12.2.1 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`

12.3 show

Display device options and settings.

12.3.1 show device-status monitor

Display the device monitoring configurations.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show device-status monitor`

12.3.2 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`

12.3.3 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`

12.3.4 show device-status events

Display occurred device status events.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show device-status events`

12.3.5 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`

12.3.6 show device-status module

Display the monitor configurations of the modules.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show device-status module`

12.3.7 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`

13 Device Security

13.1 security-status

Configure the security status settings.

13.1.1 security-status monitor pwd-change

Sets the monitoring of default password change for\n'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`

13.1.2 security-status monitor pwd-min-length

Sets the monitoring of minimum length of the password\n(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`

13.1.3 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`

13.1.4 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`

13.1.5 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`

13.1.6 security-status monitor bypass-pwd-strength

Sets the monitoring whether at least one user is\nconfigured 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`

13.1.7 security-status monitor telnet-enabled

Sets the monitoring of the activation of telnet on\nthe 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`

13.1.8 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`

13.1.9 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`

13.1.10 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`

13.1.11 security-status monitor extnvm-upd-enabled

Sets the monitoring of activation of the configuration\n saving to external non volatile memory.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `security-status monitor extnvm-upd-enabled`

- **no security-status monitor extnvm-upd-enabled**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Administrator`
  - Format: `no security-status monitor extnvm-upd-enabled`

13.1.12 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`

13.1.13 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`

13.1.14 security-status monitor extnvm-load-unsecure

Sets the monitoring of security of the configuration loading from extnvm.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `security-status monitor extnvm-load-unsecure`

no security-status monitor extnvm-load-unsecure
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no security-status monitor extnvm-load-unsecure`

13.1.15 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`

13.1.16 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`

13.1.17 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`

13.1.18 security-status trap

Configure if a trap is sent when the security status\nchanges.

- 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`

13.2 security-status

Configure the security status interface settings.

13.2.1 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`

13.3 show

Display device options and settings.

13.3.1 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`

13.3.2 show security-status state

Display the current security status.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show security-status state`

13.3.3 show security-status no-link

Display the settings of the monitoring of the specific\nnetwork ports.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show security-status no-link`

13.3.4 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`

13.3.5 show security-status events

Display occurred security status events.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show security-status events`

13.3.6 show security-status all

Display all security status settings.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show security-status all`

14 Dynamic Host Configuration Protocol (DHCP)

14.1 dhcp-server

Modify DHCP Server parameters.

14.1.1 dhcp-server operation

Enable or disable the DHCP server on this port.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `dhcp-server operation`

- **no dhcp-server operation**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no dhcp-server operation`

14.2 dhcp-server

Modify DHCP Server parameters.

14.2.1 dhcp-server operation

Enable or disable the DHCP server globally.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `dhcp-server operation`

- **no dhcp-server operation**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no dhcp-server operation`

14.2.2 dhcp-server pool add

Add a pool
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `dhcp-server pool add <P-1> dynamic <P-2> <P-3> static <P-4>`

`dynamic`: Add a dynamic pool (one or more IPs).
`static`: Add a static pool (one IP).

Parameter	Value	Meaning
`P-1`	1..128	`Pool ID.`
`P-2`	A.B.C.D	`IP address.`
`P-3`	A.B.C.D	`IP address.`
`P-4`	A.B.C.D	`IP address.`

14.2.3 dhcp-server pool modify

Modify the dynamic address pool

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `dhcp-server pool modify <-1> mode interface <-2> mac <-3> clientid <-4> remoteid <-5> circuitid <-6> relay <-7> vlan <-8> leasetime <-9> option configpath <-10> gateway <-11> netmask <-12> wins <-13> dns <-14> hostname <-15> hhrschsancsashanhh-device`

`mode`: Pool mode settings.
`interface`: Interface mode.
`mac`: MAC mode.
`clientid`: Clientid mode.
`remoteid`: Remoteid mode.
`circuitid`: Circuitid mode.
`relay`: Relay mode.
`vlan`: VLAN mode.
`leasetime`: Enter the leasetime in seconds.
`option`: Configuration option.
`configpath`: Configpath in 'tftp://<servername>/<file>' format.
`gateway`: Default gateway.
`netmask`: Option netmask.
`wins`: Option wins.
`dns`: Option dns.
`hostname`: Option hostname.
`hhrschsancsashanhh-device`: Set this pool to HHrschsancsashasnHH devices only.

Parameter	Value	Meaning
P-1	1..128	Pool ID.
P-2	slot no./port no.	
P-3	none	Remove MAC mode.
	aa:bb:cc:dd:ee:ff	MAC address.
P-4	none	Remove ID mode.
	xx:xx:...:xx	Enter ID in hexadecimal format.
P-5	none	Remove ID mode.
	xx:xx:...:xx	Enter ID in hexadecimal format.
P-6	none	Remove ID mode.
	xx:xx:...:xx	Enter ID in hexadecimal format.
P-7	none	Remove relay mode.
	ipaddr	Enter IP address of the relay.
P-8	-1..4042	VLAN ID. A value of -1 corresponds to management vlan (the default), any other value (1-4042) represents a specific VLAN
P-9	infinite	Infinite leasetime.
	seconds	Leasetime in seconds.
P-10	tftp://s	tftp://<servername>/<file> Configuration path; empty string ("") to clear value.
P-11	A.B.C.D	IP address.
P-12	a.b.c.d	IP subnet mask.
P-13	A.B.C.D	IP address.
P-14	A.B.C.D	IP address.
P-15	string	Enter a user-defined text, max. 64 characters.

- **no dhcp-server pool modify**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no dhcp-server pool modify mode interface mac clientid remoteid circuitid relay vlan leasetime option configpath gateway netmask wins dns hostname hhrschsancsashanhh-device`

14.2.4 dhcp-server pool mode

Pool enable.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `dhcp-server pool mode <P-1>`

Parameter	Value	Meaning
`P-1`	1..128	`Pool ID.`

- **no dhcp-server pool mode**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no dhcp-server pool mode <P-1>`

14.2.5 dhcp-server pool delete

Pool delete.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `dhcp-server pool delete <P-1>`

Parameter	Value	Meaning
`P-1`	1..128	`Pool ID.`

14.3 show

Display device options and settings.

14.3.1 show dhcp-server operation

Display DHCP Server global information.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show dhcp-server operation`

14.3.2 show dhcp-server pool

Show DHCP Server pool entries.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show dhcp-server pool [<P-1>]`

Parameter	Value	Meaning
`P-1`	1..128	`Pool ID.`

14.3.3 show dhcp-server interface

Show DHCP Server per interface.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show dhcp-server interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

14.3.4 show dhcp-server lease

Show DHCP Server lease entries.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show dhcp-server lease`

15 DHCP Layer 2 Relay

15.1 dhcp-l2relay

Configure DHCP Layer 2 Relay.

15.1.1 dhcp-l2relay mode

Enables or disables DHCP Layer 2 Relay globally.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay mode`

- **no dhcp-l2relay mode**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no dhcp-l2relay mode`

15.2 dhcp-l2relay

Group of commands that configure DHCP Layer 2 Relay on existing VLANs.

15.2.1 dhcp-l2relay mode

Enables or disables DHCP Layer 2 Relay on a VLAN.
- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay mode <P-1>`

Parameter	Value	Meaning
`P-1`	1..4042	`Enter the VLAN ID.`

no dhcp-l2relay mode
Disable the option
- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `no dhcp-l2relay mode`

15.2.2 dhcp-l2relay circuit-id

This commands enables setting the Option-82 Circuit ID in DHCP messages to an interface descriptor.
- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay circuit-id <P-1>`

Parameter	Value	Meaning
`P-1`	1..4042	`Enter the VLAN ID.`

no dhcp-l2relay circuit-id
Disable the option
- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `no dhcp-l2relay circuit-id <P-1>`

15.2.3 dhcp-l2relay remote-id ip

This commands sets the Option-82 Remote ID to the IP address of device (if any assigned, else fails).

- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay remote-id ip <P-1>`

Parameter	Value	Meaning
`P-1`	1..4042	`Enter the VLAN ID.`

15.2.4 dhcp-l2relay remote-id mac

This commands sets the Option-82 Remote ID to the MAC address of device.

- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay remote-id mac <P-1>`

Parameter	Value	Meaning
`P-1`	1..4042	`Enter the VLAN ID.`

15.2.5 dhcp-l2relay remote-id client-id

This commands sets the Option-82 Remote ID to the system name (sysName) of device.

- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay remote-id client-id <P-1>`

Parameter	Value	Meaning
`P-1`	1..4042	`Enter the VLAN ID.`

15.2.6 dhcp-l2relay remote-id other

This commands sets the Option-82 Remote ID manually. If it is omitted then only the Circuit ID is inserted into a relayed DHCP message.

- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay remote-id other <P-1> [<P-2>]`

Parameter	Value	Meaning
`P-1`	1..4042	`Enter the VLAN ID.`
`P-2`	string	`<remote-id> Option 82 Remote ID`

15.3 dhcp-l2relay

Configure DHCP Layer 2 Relay for an interface (list/range)

15.3.1 dhcp-l2relay mode

Enables or disables DHCP Layer 2 Relay on an interface.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay mode`

- **no dhcp-l2relay mode**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no dhcp-l2relay mode`

15.3.2 dhcp-l2relay trust

This command configures an interface as trusted (typically connected to a DHCP server) or untrusted.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `dhcp-l2relay trust`

- **no dhcp-l2relay trust**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no dhcp-l2relay trust`

15.4 clear

Clear several items.

15.4.1 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`

15.5 show

Display device options and settings.

15.5.1 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`

15.5.2 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`

15.5.3 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`

15.5.4 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`

16 DHCP Snooping

16.1 ip

Set IP parameters.

16.1.1 ip dhcp-snooping verify-mac

If enabled verifies the source MAC address in the ethernet packet against the client hardware address in the received DHCP Message. If disabled does not perform this additional security check.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping verify-mac`

- **no ip dhcp-snooping verify-mac**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip dhcp-snooping verify-mac`

16.1.2 ip dhcp-snooping mode

Enable or disable DHCP Snooping.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping mode`

- **no ip dhcp-snooping mode**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip dhcp-snooping mode`

16.1.3 ip dhcp-snooping database storage

This command specifies a location for the persistent DHCP Snooping bindings database. This can be a local file or a remote file on a given host.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping database storage <P-1>`

Parameter	Value	Meaning
P-1	local	Save persistent DHCP Snooping bindings database to a local file.
	tftp-loc	Save persistent DHCP Snooping bindings database to a remote file: <tftp-loc> := tftp://<ip-addr>/<filename>.

16.1.4 ip dhcp-snooping database write-delay

This command configures the interval in seconds at which the DHCP Snooping binding database will be saved (persistent).

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping database write-delay <P-1>`

Parameter	Value	Meaning
P-1	15..86400	Interval in seconds at which the persistent DHCP Snooping binding database will be saved. The interval value ranges from 15 to 86400 seconds.

16.1.5 ip dhcp-snooping binding add

This command creates a new static DHCP Snooping binding (and optionally an associated dynamic IP Source Guard binding) between a MAC address and an IP address, for a specific VLAN at a particular interface.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping binding add <P-1> <P-2> <P-3> <P-4> [<P-5>]`

Parameter	Value	Meaning
P-1	aa:bb:cc:dd:ee:ff	MAC address.
P-2	A.B.C.D	IP address.
P-3	slot no./port no.	
P-4	1..4042	Enter the VLAN ID.
P-5	active	Activate the option.
	inactive	Inactivate the option.

16.1.6 ip dhcp-snooping binding delete all

This command deletes all static DHCP Snooping bindings (and optionally all associated dynamic IP Source Guard bindings) at all interfaces.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping binding delete all`

16.1.7 ip dhcp-snooping binding delete interface

This command deletes all static DHCP Snooping bindings (and optionally all associated dynamic IP Source Guard bindings), associated with a particular interface.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping binding delete interface <P-1>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

16.1.8 ip dhcp-snooping binding delete mac

This command deletes one DHCP Snooping binding (and optionally the associated dynamic IP Source Guard binding), associated with a MAC address.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping binding delete mac <P-1>`

Parameter	Value	Meaning
`P-1`	aa:bb:cc:dd:ee:ff	`MAC address.`

16.1.9 ip dhcp-snooping binding mode

This command activates or deactivates a configured static DHCP Snooping binding, associated with a MAC address.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping binding mode <P-1> <P-2>`

Parameter	Value	Meaning
`P-1`	aa:bb:cc:dd:ee:ff	`MAC address.`
`P-2`	active	`Activate the option.`
	inactive	`Inactivate the option.`

16.2 clear

Clear several items.

16.2.1 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.	

16.2.2 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`

16.3 ip

IP interface commands.

16.3.1 ip dhcp-snooping trust

This command configures an interface as trusted (typically connected to a DHCP server) or un-trusted. DHCP Snooping forwards valid DHCP client messages on trusted interfaces. On un-trusted interfaces the application compares the receive interface with the clients interface in the binding database.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping trust`

- **no ip dhcp-snooping trust**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no ip dhcp-snooping trust`

16.3.2 ip dhcp-snooping log

This command configures an interface to log invalid DHCP messages, or not to log.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping log`

- **no ip dhcp-snooping log**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no ip dhcp-snooping log`

16.3.3 ip dhcp-snooping auto-disable

Enables or disables the auto-disable feature for an interface, applicable when the DHCP packet rate exceeds the limit.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping auto-disable`

- **no ip dhcp-snooping auto-disable**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no ip dhcp-snooping auto-disable`

16.3.4 ip dhcp-snooping limit

This command configures an interface for a maximum DHCP packet rate in a burst interval, or disables it. If the rate of DHCP packets exceed this limit in consecutive intervals then all further packets are dropped. If that happens and additionally the auto-disable feature is enabled, then the port is disabled automatically.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip dhcp-snooping limit <P-1> [<P-2>]`

Parameter	Value	Meaning
`P-1`	-1..150	`Specifies the rate limit value (in packets per seconds, pps) for DHCP snooping purposes. The value -1 switches rate limiting off.`
`P-2`	1..15	`Specifies the burst interval value for DHCP snooping purposes. Because this parameter is optional it leaves unchanged if omitted.`

16.4 show

Display device options and settings.

16.4.1 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`

16.4.2 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`

16.4.3 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`

16.4.4 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`

16.4.5 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.`

17 DoS Mitigation

17.1 dos

Manage DoS Mitigation

17.1.1 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`

17.1.2 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`

17.1.3 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`

17.1.4 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`

17.1.5 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`

17.1.6 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`

17.1.7 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)`

17.1.8 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.`

17.1.9 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`

17.1.10 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`

17.1.11 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`

17.2 show

Display device options and settings.

17.2.1 show dos

Show DoS Mitigation parameters
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show dos`

18 IEEE 802.1x (Dot1x)

18.1 dot1x

Configure 802.1X parameters.

18.1.1 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`

18.1.2 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`

18.1.3 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`

18.2 dot1x

Configure 802.1X interface parameters.

18.2.1 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.`

18.2.2 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).`

18.2.3 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	auto	Port is actually controlled by protocol.
	force-authorized	Port is authorized unconditionally (default).
	force-unauthorized	Port is unauthorized unconditionally.
	multi-client	If more than one client is attached to the port, then each client needs to authenticate separately.

18.2.4 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`

18.2.5 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	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.

18.2.6 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).

18.2.7 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.

18.2.8 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).

18.2.9 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.

18.2.10 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.

18.2.11 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.

18.2.12 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`

18.2.13 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`

18.3 show

Display device options and settings.

18.3.1 show dot1x global

Display global 802.1X configuration.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show dot1x global`

18.3.2 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.\nParameter Usage:[ <slot/port> [index] ]`

18.3.3 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.	

18.3.4 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>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

18.3.5 show dot1x clients

Display 802.1X client information.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show dot1x clients [<P-1>]`

Parameter	Value	Meaning
`P-1`	aa:bb:cc:dd:ee:ff	`MAC address.`

18.3.6 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>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

18.4 clear

Clear several items.

18.4.1 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.	

18.4.2 clear dot1x statistics all

Resets the 802.1X statistics for all ports.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `clear dot1x statistics all`

18.4.3 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.	

18.4.4 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`

19 IEEE 802.3ad (Dot3ad)

19.1 link-aggregation

Configure 802.3ad link aggregation parameters to increase bandwidth and provide redundancy by combining connections.

19.1.1 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>`

Parameter	Value	Meaning
`P-1`	lag/<lagport>	`lag/<lagport>  Enter a lag interface in lag/lagport format.`

19.1.2 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.

Parameter	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`

19.1.3 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.	

19.2 lacp

Configure lacp parameters.

19.2.1 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>`

Parameter	Value	Meaning
`P-1`	0..65535	`Enter a number between 0 and 65535`

19.2.2 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>`

Parameter	Value	Meaning
`P-1`	0..65535	`Enter a number between 0 and 65535`

19.2.3 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`

19.2.4 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`

19.2.5 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`

19.2.6 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`

19.2.7 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`

19.2.8 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`

19.2.9 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`

19.2.10 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`

19.2.11 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`

19.2.12 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`

19.2.13 lacp partner admin port priority

Set LACP partener 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`

19.2.14 lacp partner admin port id

Set LACP partener 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`

19.2.15 lacp partner admin system-priority

Configure the partener 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`

19.2.16 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.`

19.3 show

Display device options and settings.

19.3.1 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.	

19.3.2 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.	

19.3.3 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.	

19.3.4 show lacp interface

Show LAG iterfaces 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.	

19.3.5 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.	

19.3.6 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.	

19.3.7 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.	

19.3.8 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.	

20 Filtering Database (FDB)

20.1 mac-filter

20.1.1 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>`

20.2 bridge

Bridge configuration.

20.2.1 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.`

20.3 show

Display device options and settings.

20.3.1 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`

20.4 show

Display device options and settings.

20.4.1 show bridge aging-time

Address aging time.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show bridge aging-time`

20.5 show

Display device options and settings.

20.5.1 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.`

20.6 clear

Clear several items.

20.6.1 clear mac-addr-table

Clears the MAC address table.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `clear mac-addr-table`

21 GARP VLAN and Multicast Registration Protocol (GVRP and GMRP)

21.1 garp

Configure GARP protocols, GVRP for dynamic VLAN registration and GMRP for dynamic MAC registration.

21.1.1 garp gvrp operation

Enable or disable GVRP globally. When enabled, the device distributes VLAN membership information on GVRP enable active ports. GVRP-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: `garp gvrp operation`

- **no garp gvrp operation**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no garp gvrp operation`

21.1.2 garp gmrp operation

Enable or disable GMRP globally. Devices use GMRP 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: `garp gmrp operation`

- **no garp gmrp operation**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no garp gmrp operation`

21.1.3 garp gmrp forward-unknown

Configure if unknown multicast packets are forwarded. The setting can be discard or flood.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `garp gmrp forward-unknown <P-1>`

Parameter	Value	Meaning
`P-1`	flood	`Unknown multicast frames will be flooded.`
	discard	`Unknown multicast frames will be discarded.`

21.2 garp

Configure GARP parameters and protocols, GVRP for dynamic VLAN registration and GMRP for dynamic MAC registration on a port.

21.2.1 garp interface join-time

Set the GARP 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-GARP participant basis.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `garp interface join-time <P-1>`

Parameter	Value	Meaning
`P-1`	10..100	`Join time-interval in centi-seconds.`

21.2.2 garp interface leave-time

Set the GARP 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: `garp interface leave-time <P-1>`

Parameter	Value	Meaning
`P-1`	20..600	`Leave time-interval in centi-seconds.`

21.2.3 garp interface leave-all-time

Set the GARP 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-GARP Participant basis.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `garp interface leave-all-time <P-1>`

Parameter	Value	Meaning
`P-1`	200..6000	`Leave-All time-interval in centi-seconds.`

21.2.4 garp gvrp operation

Enable or disable GVRP on the port. When enabled, globally and on this port, the device distributes VLAN membership information to GVRP aware devices connected to this port.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `garp gvrp operation`

no garp gvrp operation
Disable the option

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `no garp gvrp operation`

21.2.5 garp gmrp operation

Enable or disable GMRP on the interface, with GMRP enabled globally and on this interface, the device sends and receives GMRP messages on this port.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `garp gmrp operation`

- **no garp gmrp operation**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no garp gmrp operation`

21.2.6 garp gmrp forward-all-groups

Configure forward-all behavior for GMRP on the interface.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `garp gmrp forward-all-groups`

- **no garp gmrp forward-all-groups**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no garp gmrp forward-all-groups`

21.3 show

Display device options and settings.

21.3.1 show garp interface

Show the global configuration of GARP per interface.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show garp interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

21.3.2 show garp gvrp global

Display the GVRP global configuration.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show garp gvrp global`

21.3.3 show garp gvrp interface

Display the GVRP interface configuration.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show garp gvrp interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

21.3.4 show garp gvrp statistics interface

Display the GVRP interface statistics.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show garp gvrp statistics interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

21.3.5 show garp gmrp global

Display the GMRP global configuration.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show garp gmrp global`

21.3.6 show garp gmrp interface

Display the GMRP interface configuration.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show garp gmrp interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

21.3.7 show garp gmrp statistics interface

Display the GMRP interface statistics.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show garp gmrp statistics interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

21.4 show

Display device options and settings.

21.4.1 show mac-filter-table gmrp

Display GMRP entries in the MFDB table.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show mac-filter-table gmrp`

22 HiDiscovery

22.1 network

Configure the inband and outband connectivity.

22.1.1 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>`

22.1.2 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.`

22.1.3 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`

22.1.4 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`

22.2 show

Display device options and settings.

22.2.1 show network hidiscovery

Show the HiDiscovery settings.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show network hidiscovery`

23 Hypertext Transfer Protocol (HTTP)

23.1 http

Set HTTP parameters.

23.1.1 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).`

23.1.2 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`

23.2 show

Display device options and settings.

23.2.1 show http

Show HTTP server information.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show http`

24 HTTP Secure (HTTPS)

24.1 https

Set HTTPS parameters.

24.1.1 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`

24.1.2 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).`

24.1.3 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`

24.2 copy

Copy different kinds of items.

24.2.1 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.`

24.2.2 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.`

24.3 show

Display device options and settings.

24.3.1 show https

Show HTTPS server information.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show https`

25 Integrated Authentification Server (IAS)

25.1 ias-users

Manage IAS Users and User Accounts.

25.1.1 ias-users add

Add a new IAS user.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `ias-users add <P-1>`

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

25.1.2 ias-users delete

Delete an existing IAS user.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `ias-users delete <P-1>`

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

25.1.3 ias-users enable

Enable IAS user.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `ias-users enable <P-1>`

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

25.1.4 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).`

25.1.5 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.`

25.2 show

Display device options and settings.

25.2.1 show ias-users

Display IAS users and user accounts information.

- Mode: `Command is in all modes available.`
- Privilege Level: `Administrator`
- Format: `show ias-users`

26 IEC 61850 MMS Server

26.1 iec61850-mms

Configure the IEC61850 MMS Server settings.

26.1.1 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`

26.1.2 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`

26.1.3 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).

26.1.4 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).

26.1.5 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')

26.2 show

Display device options and settings.

26.2.1 show iec61850-mms

Show the IEC61850 MMS Server settings.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show iec61850-mms`

27 Internet Group Management Protocol (IGMP)

27.1 ip

Set IP parameters.

27.1.1 ip igmp operation

Enable or disable IGMP globally on the device.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip igmp operation`

- **no ip igmp operation**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip igmp operation`

27.2 ip

IP interface commands.

27.2.1 ip igmp operation

Enables or disables IGMP on the interface.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip igmp operation`

- **no ip igmp operation**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no ip igmp operation`

27.2.2 ip igmp version

Configure IGMP version.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip igmp version <P-1>`

Parameter	Value	Meaning
`P-1`	1..3	`Enter igmp version (default: 3).`

27.2.3 ip igmp robustness

Configure IGMP router robustness.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip igmp robustness <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter igmp query robustness (default: 2).

27.2.4 ip igmp querier query-interval

Configure IGMP query interval in seconds.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip igmp querier query-interval <P-1>`

Parameter	Value	Meaning
P-1	1..3600	Enter igmp query interval (default: 125).

27.2.5 ip igmp querier last-member-interval

Configure last member query interval in tenths of seconds.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip igmp querier last-member-interval <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter igmp last member query interval (default: 10).

27.2.6 ip igmp querier max-response-time

Configure maximum response time in tenths of seconds.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip igmp querier max-response-time <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter igmp query maximum response time (default: 100).

27.3 show

Display device options and settings.

27.3.1 show ip igmp global

Display IGMP global configuration.
- Mode: `Command is in all modes available.`
- Privilege Level: `Operator`
- Format: `show ip igmp global`

27.3.2 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.	

27.3.3 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`

27.3.4 show ip igmp groups

Display the subscribed multicast groups.

- Mode: `Command is in all modes available.`
- Privilege Level: `Operator`
- Format: `show ip igmp groups`

27.3.5 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.	

28 IGMP Proxy

28.1 ip

Set IP parameters.

28.1.1 ip igmp-proxy interface

This command enables/disables IGMP Proxy on the router and configures the host interface.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip igmp-proxy interface <P-1>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

- **no ip igmp-proxy interface**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip igmp-proxy interface <P-1>`

28.1.2 ip igmp-proxy report-interval

Sets the unsolicited report interval in seconds.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip igmp-proxy report-interval <P-1>`

Parameter	Value	Meaning
`P-1`	1..260	`Enter a number in the given range.`

28.2 show

Display device options and settings.

28.2.1 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`

28.2.2 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`

28.2.3 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`

29 IGMP Snooping

29.1 igmp-snooping

Configure IGMP snooping.

29.1.1 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`

29.1.2 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`

29.1.3 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.

29.1.4 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.

29.1.5 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).

29.1.6 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.`

29.2 igmp-snooping

Configure IGMP snooping.

29.2.1 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> mcrtrexpiretime <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.
`mcrtrexpiretime`: 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>`

29.3 igmp-snooping

Configure IGMP snooping.

29.3.1 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`

29.3.2 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`

29.3.3 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.

29.3.4 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.

29.3.5 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.

29.3.6 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`

29.4 show

Display device options and settings.

29.4.1 show igmp-snooping global

Show IGMP snooping global information.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show igmp-snooping global`

29.4.2 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.	

29.4.3 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.`

29.4.4 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`

29.4.5 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.`

29.4.6 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.`

29.4.7 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`

29.4.8 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`

29.4.9 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.	

29.5 show

Display device options and settings.

29.5.1 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`

29.6 clear

Clear several items.

29.6.1 clear igmp-snooping

Clear all IGMP snooping entries.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `clear igmp-snooping`

30 Interface

30.1 shutdown

30.1.1 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`

30.2 auto-negotiate

30.2.1 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`

30.3 auto-power-down

30.3.1 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.`

30.4 cable-crossing

30.4.1 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.`

30.5 linktraps

30.5.1 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`

30.6 link-loss-alert

Configure Link Loss Alert on the interface.

30.6.1 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`

30.7 speed

30.7.1 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.`

30.8 name

30.8.1 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.`

30.9 power-state

30.9.1 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`

30.10 mac-filter

30.10.1 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>`

30.11 led-signaling

Enable or disable Port LED signaling.

30.11.1 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`

30.12 show

Display device options and settings.

30.12.1 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.	

30.13 show

Display device options and settings.

30.13.1 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.	

30.14 show

Display device options and settings.

30.14.1 show led-signaling operation

Show Port LED signaling operation.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show led-signaling operation`

31 Interface Statistics

31.1 utilization

Configure the interface utilization parameters.

31.1.1 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.`

31.1.2 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.`

31.1.3 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.

31.2 clear

Clear several items.

31.2.1 clear port-statistics

Clear all statistics counter.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `clear port-statistics`

31.3 show

Display device options and settings.

31.3.1 show interface counters

Show Table with interface counters.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show interface counters`

31.3.2 show interface layout

Show interface layout of the device.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show interface layout`

31.3.3 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.	

31.3.4 show interface statistics

Show summary interface statistics.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show interface statistics [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

31.3.5 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>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

32 Intern

32.1 help

Display help for various special keys.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `help`

32.2 logout

Exit this session.

- Mode: `Command is in all modes available.`
- Privilege Level: `any`
- Format: `logout`

32.3 history

Show a list of previously run commands.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `history`

32.4 vlan-mode

32.4.1 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.`

32.5 exit

Exit from vlan mode.

- Mode: `VLAN Mode`
- Privilege Level: `Operator`
- Format: `exit`

32.6 end

Exit to exec mode.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `end`

32.7 serviceshell

Enter system mode.

32.7.1 serviceshell deactivate

Disable the service shell access permanently (Cannot be undone).

- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `serviceshell deactivate`

32.8 serviceshell-f

Enter system mode.

32.8.1 serviceshell-f deactivate

Disable the service shell access permanently (Cannot be undone).

- Mode: `Factory Mode`
- Privilege Level: `Administrator`
- Format: `serviceshell-f deactivate`

32.9 traceroute

Trace route to a specified host.

32.9.1 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`

32.10 traceroute

Trace route to a specified host.

32.10.1 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.`

32.11 reboot

Reset the device (cold start).

32.11.1 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.`

32.12 ping

32.12.1 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.

32.13 ping

Send ICMP echo packets to a specified host or IP address.

32.13.1 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.`

32.14 show

Display device options and settings.

32.14.1 show reboot

Display Configured reboot in seconds
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show reboot`

32.14.2 show serviceshell

Display the service shell access.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show serviceshell`

33 Open Shortest Path First (OSPF)

33.1 ip

Set IP parameters.

33.1.1 ip ospf area

Configure the OSPF router area. A router area is a sub-division of an OSPF autonomous system and you identify an area by an area-id. OSPF networks, routers, and links that have the same area-id form a logical set.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf area <P-1> range add <P-2> <P-3> <P-4> modify <P-5> <P-6> <P-7> <P-8> delete <P-9> <P-10> <P-11> add delete stub add <P-12> modify <P-13> summarylsa <P-14> default-cost <P-15> delete <P-16> virtual-link add <P-17> delete <P-18> modify <P-19> authentication type <P-20> key <P-21> key-id <P-22> hello-interval <P-23> dead-interval <P-24> transmit-delay <P-25> retransmit-interval <P-26> nssa add <P-27> delete <P-28> modify translator role <P-29> stability-interval <P-30> summary no-redistribute default-info originate [metric <P-31>] [metric-type <P-32>]`

`range`: Configure the range for the area. You summarize the networks within this range into a single routing domain.
`add`: Create a router area.
`modify`: Modify the parameters of a router area.
`delete`: Delete a specific router area.
`add`: Create a new area.
`delete`: Delete a existing area.
`stub`: Configure the preferences for a stub area. You shield stub areas from external route advertisements, but the area receives advertisements from networks that belong to other areas of the same autonomous system.
`add`: Create a stub area. The command also allows you to convert an existing area to a stub area.
`modify`: Modify the stub area parameters.
`summarylsa`: Configure the summary LSA mode for a stub area. When enabled, the router both summarizes and propagates summary LSAs.
`default-cost`: Set the default cost for the stub area.
`delete`: Remove a stub area. After removal, the area receives external route advertisements.
`virtual-link`: Configure a virtual link. You use the virtual link to connect the router to the backbone area (0.0.0.0) through a non-backbone area or to connect two parts of a partitioned backbone area (0.0.0.0) through a non-backbone area.
`add`: Add a virtual neighbor.
`delete`: Delete a virtual neighbor.
`modify`: Modify the parameters of a virtual neighbor.
`authentication`: Configure the authentication type. The device authenticates the OSPF protocol exchanges in the OSPF packet header which includes an authentication type field.
`type`: Configure the authentication type. Authentication types are 0 for null authentication, 1 for simple password authentication, and 2 for cryptographic authentication.
`key`: Configure the authentication key.

key-id: Configure the authentication key-id for md5 authentication. This field identifies the algorithm and secret key used to create the message digest appended to the OSPF packet.
hello-interval: Configure the OSPF hello-interval for the virtual link, in seconds. The hello timer controls the time interval between sending two consecutive hello packets. Set this value to the same hello-interval value of the virtual neighbors.
dead-interval: Configure the OSPF dead-interval for the virtual link, in seconds. If the timer expires without the router receiving hello packets from a virtual neighbor, the router declares the neighbor router as down. Set the timer to at least four times the value of the hello-interval.
transmit-delay: Configure the OSPF transmit-delay for the virtual link, in seconds. Transmit delay is the time that you estimate it takes to transmit a link-state update packet over the virtual link.
retransmit-interval: Configure the OSPF retransmit-interval for the virtual link, in seconds. The retransmit interval is the time between two consecutive link-state advertisement transmissions. Link-state advertisements contain such information as database descriptions and link-state request packets for adjacencies belonging to virtual link.
nssa: Configure a NSSA(Not-So-Stubby-Area).
add: Add a NSSA.
delete: Delete a NSSA.
modify: Modify the parameters of a NSSA.
translator: Configure the NSSA translator related parameters.
role: Configure the NSSA translator role.
stability-interval: Configure the translator stability interval for the NSSA, in seconds.
summary: Configure the import summary for the specified NSSA.
no-redistribute: Configure route redistribution for the specified NSSA.
default-info: Configure the nssa default information origination parameters.
originate: Configuration whether a Type-7 LSA should be originated into the NSSA.
[metric]: Configure the metric for the NSSA.
[metric-type]: Configure the metric type for default information.

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.
P-2	summary-link	Configure summary links LSDB type optional mode.
	nssa-external-link	Configure nssa external link LSDB type optional mode.
P-3	A.B.C.D	IP address.
P-4	a.b.c.d	IP subnet mask.
P-5	summary-link	Configure summary links LSDB type optional mode.
	nssa-external-link	Configure nssa external link LSDB type optional mode.
P-6	A.B.C.D	IP address.
P-7	a.b.c.d	IP subnet mask.
P-8	advertise	Set as advertise.
	do-not-advertise	Set as do-not-advertise.
P-9	summary-link	Configure summary links LSDB type optional mode.
	nssa-external-link	Configure nssa external link LSDB type optional mode.
P-10	A.B.C.D	IP address.
P-11	a.b.c.d	IP subnet mask.
P-12	0	Configure the TOS (0 is for Normal Service).
P-13	0	Configure the TOS (0 is for Normal Service).
P-14	no-area-summary	Disable the router from sending area link state advertisement summaries.
	send-area-summary	Enable the router to send area link state advertisement summaries. The router floods LSAs within the area using multicast. Every topology change starts a new flood of LSAs.
P-15	0..16777215	Configure the default cost.
P-16	0	Configure the TOS (0 is for Normal Service).
P-17	A.B.C.D	IP address.
P-18	A.B.C.D	IP address.
P-19	A.B.C.D	IP address.

Parameter	Value	Meaning
P-20	none	Configure the authentication type as none (Key and key ID is not required).
	simple	Configure the authentication type as simple (Key ID is not required).
	md5	Configure the authentication type as md5 for the interface.
P-21	string	<key> Configure the authentication key.
P-22	0..255	Enter a number in the given range.
P-23	1..65535	Enter a number between 1 and 65535
P-24	1..65535	Enter a number between 1 and 65535
P-25	0..3600	Enter a number in the given range.
P-26	0..3600	Enter a number in the given range.
P-27	import-nssa	Configure the area as NSSA only.
P-28	import-external	Change the area to support external LSAs also.
P-29	always	Configure the NSSA translator role as always. When used as a border router, the router translates LSAs regardless of the translator states of the other NSSA border routers.
	candidate	Configure the NSSA translator role as a candidate. When used as a border router, the router participates in the translator election process. The router maintains a list of reachable NSSA border routers.
P-30	0..65535	Enter a number between 0 and 65535
P-31	1..16777214	Configure the metric value.
P-32	ospf-metric	Set the metric type as ospf Metric.
	comparable-cost	Set the metric type as comparable cost.
	non-comparable	Set the metric type as non-comparable.

- **no ip ospf area**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip ospf area <P-1> range add modify delete add delete stub add modify summarylsa default-cost delete virtual-link add delete modify authentication type key key-id hello-interval dead-interval transmit-delay retransmit-interval nssa add delete modify translator role stability-interval summary no-redistribute default-info originate [metric] [metric-type]`

33.1.2 ip ospf trapflags all

Set all trapflags at once.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf trapflags all <P-1>`

Parameter	Value	Meaning
P-1	[cr]	Enable the Bit.

- **no ip ospf trapflags all**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip ospf trapflags all <P-1>`

33.1.3 ip ospf operation

Enable or disable the OSPF admin mode. When enabled, the device initiates the OSPF process if the OSPF function is active on at least one interface.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf operation`

- **no ip ospf operation**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip ospf operation`

33.1.4 ip ospf 1583compatability

Enable or disable the 1583compatibility for calculating routes external to the autonomous system. When enabled, the router is compatible with the preference rules defined in RFC1583, section 16.4.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf 1583compatability`

- **no ip ospf 1583compatability**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip ospf 1583compatability`

33.1.5 ip ospf default-metric

Configure the default metric for re-distributed routes, when OSPF redistributes routes from other protocols.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf default-metric <P-1>`

Parameter	Value	Meaning
P-1	1..16777214	Configure the default metric for redistributed routes.

- **no ip ospf default-metric**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no ip ospf default-metric <P-1>`

33.1.6 ip ospf router-id

Configure the router ID to uniquely identify this OSPF router in the autonomous system.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf router-id <P-1>`

Parameter	Value	Meaning
P-1	A.B.C.D	IP address.

33.1.7 ip ospf external-lsdb-limit

Configure the OSPF external lsdb limitation, which is the maximum number of non-default AS-external-LSA entries that the router stores in the link-state database. When the value -1 is configured, you disable the limitation.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf external-lsdb-limit <P-1>`

Parameter	Value	Meaning
P-1	-1..2147483647	Configure the external lsdb limit.

33.1.8 ip ospf exit-overflow

Configure the OSPF exit overflow interval, in seconds. After the timer expires the router will attempt to leave the overflow-state. To disable the exit overflow interval function set the value to 0.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf exit-overflow <P-1>`

Parameter	Value	Meaning
P-1	0..2147483647	Configure the exit overflow interval.

33.1.9 ip ospf spf-delay

Configure the SPF delay, in seconds. The Shortest Path First (SPF) delay is the time that the device waits for the network to stabilize before calculating the shortest path tree, after a topology change.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf spf-delay <P-1>`

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

33.1.10 ip ospf spf-holdtime

Configure the minimum time between two consecutive SPF calculations, in seconds.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf spf-holdtime <P-1>`

Parameter	Value	Meaning
P-1	0..65535	Enter a number between 0 and 65535

33.1.11 ip ospf auto-cost

Set the auto cost reference bandwidth of the router interfaces for ospf metric calculations. The default reference bandwidth is 100 Mbps.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf auto-cost <P-1>`

Parameter	Value	Meaning
P-1	1..4294967	Configure the auto cost for OSPF calculation.

33.1.12 ip ospf distance intra

Enter the preference type as intra. Use intra-area routing when the device routes packets solely within an area, such as an internal router.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf distance intra <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter the value.

33.1.13 ip ospf distance inter

Enter the preference type as inter. Use inter-area routing when the device routes packets into or out of an area, such as an area border router.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf distance inter <P-1>`

Parameter	Value	Meaning
P-1	1..255	Enter the value.

33.1.14 ip ospf distance external

Enter the preference type as external. Use external-area routing when the device routes packets into or out of an autonomous system, such as an autonomous system boundary router (ASBR).

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf distance external <P-1>`

Parameter	Value	Meaning
`P-1`	1..255	`Enter the value.`

33.1.15 ip ospf re-distribute

Configure the OSPF route re-distribution. An ASBR is able to translate information from other OSPF processes in separate areas and routes from other sources, such as static routes or other dynamic routing protocols, into the OSPF protocol.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf re-distribute <P-1> [metric <P-2>] [metric-type <P-3>] [tag <P-4>] [subnets <P-5>]`

`[metric]`: Configure the OSPF route re-distribution metric parameters.
`[metric-type]`: Configure the OSPF route redistribution metric-type.
`[tag]`: Configure the OSPF route redistribution tag parameters.
`[subnets]`: Allow the router to redistribute subnets into OSPF.

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.`
`P-2`	0..16777214	`Configure the metric.`
`P-3`	1..2	`Configure the metric type.`
`P-4`	0..4294967295	`Configure the tag.`
`P-5`	enable	`Enable the option.`
	disable	`Disable the option.`

no ip ospf re-distribute

Disable the option

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `no ip ospf re-distribute <P-1> [metric] [metric-type] [tag] [subnets]`

33.1.16 ip ospf distribute-list

Configure the distribute list for the routes from other source protocols.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf distribute-list <P-1> <P-2> <P-3>`

Parameter	Value	Meaning
P-1	out	Configure as out to re-distribute routes with ACL rules
P-2	connected	Select the source protocol as connected.
	static	Select the source protocol as static.
	rip	Select the source protocol as RIP.
P-3	<1000..1099>	Enter the access list number.

no ip ospf distribute-list
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `no ip ospf distribute-list <P-1> <P-2> <P-3>`

33.1.17 ip ospf default-info originate

Originate the OSPF default information.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `ip ospf default-info originate [always] [metric <P-1>] [metric-type <P-2>]`

`[always]`: Always advertise the 0.0.0.0/0.0.0.0 route information.
`[metric]`: Configure the metric for default information.
`[metric-type]`: Configure the metric type for default information.

Parameter	Value	Meaning
P-1	1..16777214	Configure the metric value.
P-2	external-type1	Set the metric type for default information as external type-1. The type 1 value sets the metric to the sum of the internal and external OSPF metrics.
	external-type2	Set the metric type for default information as external type-2. The type 2 value sets the metric to the sum of external OSPF metrics from the source AS to the destination AS.

no ip ospf default-info originate

Disable the option

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `no ip ospf default-info originate [always] [metric <P-1>] [metric-type]`

33.2 ip

IP interface commands.

33.2.1 ip ospf operation

Enable or disable OSPF on port.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf operation`

- **no ip ospf operation**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no ip ospf operation`

33.2.2 ip ospf area-id

Configure the router ID that uniquely identifies the area to which the interface is connected. If a tie occurs during the designated router election the router with the higher router ID is the designated router.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf area-id <P-1>`

Parameter	Value	Meaning
`P-1`	A.B.C.D	`IP address.`

33.2.3 ip ospf link-type

Configure the OSPF link type.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf link-type <P-1>`

Parameter	Value	Meaning
P-1	broadcast	Configure the link-type as broadcast for the interface. In broadcast networks, routers discover their neighbors dynamically using the OSPF hello protocol.
	nbma	Configure the link-type as Non-Broadcast Multi-Access for the interface. The nbma mode, emulates OSPF operation over a broadcast network. The nbma mode is the most efficient way to run OSPF over non-broadcast networks, both in terms of the LSDB size and the amount of routing protocol traffic. However, this mode requires direct communication between every router in the nbma network.
	point-to-point	Configure the link-type as point-to-point for the interface. Use the point-to-point link-type in a network that joins a single pair of routers.
	point-to-multipoint	Configure the link-type as point-to-multipoint for the interface. In the point-to-multipoint mode, OSPF treats each router-to-router link over non-broadcast networks as if they were point-to-point links.

33.2.4 ip ospf priority

Configure the OSPF router priority which the router uses in multi-access networks for the designated router election algorithm. The router with the higher router priority is the designated router. A value of 0 declares the router as ineligible for designated router elections.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf priority <P-1>`

Parameter	Value	Meaning
P-1	0..255	Configure the priority.

33.2.5 ip ospf transmit-delay

Configure the OSPF transmit-delay for the interface, in seconds. The transmit-delay is the time that you estimate it takes to transmit a link-state update packet over the interface.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf transmit-delay <P-1>`

Parameter	Value	Meaning
P-1	0..3600	Enter a number in the given range.

33.2.6 ip ospf retransmit-interval

Configure the OSPF retransmit-interval for the interface, in seconds. The retransmit-interval is the interval after which link-state advertisements containing database description and link-state request packets, are re-transmitted for adjacencies belonging to this interface.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf retransmit-interval <P-1>`

Parameter	Value	Meaning
P-1	0..3600	Enter a number in the given range.

33.2.7 ip ospf hello-interval

Configure the OSPF hello-interval for the interface, in seconds. The hello timer controls the time interval between two consecutive hello packets. Set this value to the same hello-interval value of the neighbor.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf hello-interval <P-1>`

Parameter	Value	Meaning
P-1	1..65535	Enter a number between 1 and 65535

33.2.8 ip ospf dead-interval

Configure the OSPF dead-interval for the interface, in seconds. If the timer expires without the router receiving hello packets from the neighbor, the router declares the neighbor router as down. Set the timer to at least four times the value of the hello-interval.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf dead-interval <P-1>`

Parameter	Value	Meaning
P-1	1..65535	Enter a number between 1 and 65535

33.2.9 ip ospf cost

Configure the OSPF cost for the interface. The cost of a specific interface indicates the overhead required to send packets across the link. If set to 0, OSPF calculates the cost from the reference bandwidth and the interface speed.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf cost <P-1>`

Parameter	Value	Meaning
P-1	<1..65535>	Configure the cost for the specified interface.
	auto	Automatic calculation from reference bandwidth and link speed.

33.2.10 ip ospf mtu-ignore

Enable/Disable OSPF MTU mismatch on interface.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf mtu-ignore`

- **no ip ospf mtu-ignore**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no ip ospf mtu-ignore`

33.2.11 ip ospf authentication type

Configure authentication type.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf authentication type <P-1>`

Parameter	Value	Meaning
P-1	none	Configure the authentication type as none (Key and key ID is not required).
	simple	Configure the authentication type as simple (Key ID is not required).
	md5	Configure the authentication type as md5 for the interface.

33.2.12 ip ospf authentication key

Configure authentication key.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf authentication key <P-1>`

Parameter	Value	Meaning
P-1	string	<key> Configure the authentication key.

33.2.13 ip ospf authentication key-id

Configure authentication key-id for md5 authentication.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `ip ospf authentication key-id <P-1>`

Parameter	Value	Meaning
P-1	0..255	Enter a number in the given range.

33.3 show

Display device options and settings.

33.3.1 show ip ospf global

Display OSPF global configurations.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show ip ospf global`

33.3.2 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.`

33.3.3 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`

33.3.4 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`

33.3.5 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`

33.3.6 show ip ospf range

Display OSPF area range information.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show ip ospf range`

33.3.7 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.	

33.3.8 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.`

33.3.9 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`

33.3.10 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.	

33.3.11 show ip ospf statistics

Display OSPF statistics.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show ip ospf statistics`

33.3.12 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.

33.3.13 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.

33.3.14 show ip ospf route

Display OSPF routes.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show ip ospf route`

34 Internet Protocol Version 4 (IPv4)

34.1 network

Configure the inband and outband connectivity.

34.1.1 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`

34.1.2 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.`

34.2 clear

Clear several items.

34.2.1 clear arp-table-switch

Clear the agent's ARP table (cache).

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `clear arp-table-switch`

34.3 show

Display device options and settings.

34.3.1 show network parms

Show network settings.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show network parms`

34.4 show

Display device options and settings.

34.4.1 show arp

Show ARP table.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show arp`

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 × 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 × 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`

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
	3	Same as error
	4	Same as warning
	5	Same as notice
	6	Same as informational
	7	Same as debug

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
	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

38.1.4 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>`

Parameter	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>`

Parameter	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.

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`

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>`

Parameter	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>`

Parameter	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 persistent

Display persistent logging configurations.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show logging persistent [logfiles]`

`[logfiles]`: List the persistent log files.

38.2.5 show logging syslog

Display current syslog operational setting.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show logging syslog`

38.2.6 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`

38.2.7 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`

38.2.8 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`

38.2.9 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`

38.2.10 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`

38.2.11 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 envm

Copy a buffered log from the device to external non-volatile memory.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `copy eventlog buffered envm <P-1>`

Parameter	Value	Meaning
`P-1`	string	`Enter a user-defined text, max. 32 characters.`

38.3.2 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.`

38.3.3 copy eventlog persistent

Copy the persistent logs from the device to an envm or a file server.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `copy eventlog persistent <P-1> envm <P-2> remote <P-3>`

`envm`: Copy the persistent log from the device to external non-volatile memory.
`remote`: Copy the persistent logs from the device to a file server.

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.
P-2	string	Enter a user-defined text, max. 32 characters.
P-3	string	Enter a user-defined text, max. 128 characters.

38.3.4 copy traplog system envm

Copy the traplog from the device to external non-volatile memory.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator`
- Format: `copy traplog system envm <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

38.3.5 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.

38.3.6 copy audittrail system envm

Copy the audit trail from the device to external non-volatile memory.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Operator, Auditor`
- Format: `copy audittrail system envm <P-1>`

Parameter	Value	Meaning
P-1	string	Enter a user-defined text, max. 32 characters.

38.3.7 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.`

38.3.8 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.`

38.3.9 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.`

38.3.10 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.`

38.3.11 copy syslogcacert envm

Copy CA certificate file (*.pem) from external non-volatile memory to the specified destination.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `copy syslogcacert 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 persistent

Clear persistent log from memory.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `clear logging persistent`

38.4.3 clear logging email statistics

Clear email statistics
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `clear logging email statistics`

38.4.4 clear eventlog

Clear the event log entries from memory.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `clear eventlog`

39 MAC Notification

39.1 mac

Set MAC parameters.

39.1.1 mac notification operation

Enable or disable MAC notification globally.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `mac notification operation`

- **no mac notification operation**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no mac notification operation`

39.1.2 mac notification interval

Set MAC notification interval in seconds.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `mac notification interval <P-1>`

Parameter	Value	Meaning
`P-1`	0..2147483647	`Enter a number in the given range.`

39.2 mac

MAC interface commands.

39.2.1 mac notification operation

Enable or disable MAC notification on this interface.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `mac notification operation`

- **no mac notification operation**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no mac notification operation`

39.3 show

Display device options and settings.

39.3.1 show mac notification global

Displays MAC notification global information.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show mac notification global`

39.3.2 show mac notification interface

Displays MAC notification interface information.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show mac notification interface`

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 Modbus

41.1 modbus-tcp

Configure Modbus TCP/IP server settings.

41.1.1 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`

41.1.2 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`

41.1.3 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`

41.1.4 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).`

41.2 show

Display device options and settings.

41.2.1 show modbus-tcp

Show the Modbus TCP/IP server settings.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show modbus-tcp`

42 Media Redundancy Protocol (MRP)

42.1 mrp

Configure the MRP settings.

42.1.1 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.`

42.1.2 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).`

42.1.3 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).

42.1.4 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.

42.1.5 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.

42.1.6 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.	

42.1.7 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.

Parameter	Value	Meaning
`P-1`	slot no./port no.	
`P-2`	enable	`Enable the option.`
	disable	`Disable the option.`

42.1.8 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>`

Parameter	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.`

42.1.9 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>`

Parameter	Value	Meaning
`P-1`	reset	`Reset the round-trip-delay counters.`

42.1.10 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).`

42.1.11 mrp domain add default-domain

Default MRP domain ID.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `mrp domain add default-domain`

42.1.12 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).`

42.1.13 mrp domain delete

Delete the current MRP domain.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `mrp domain delete`

42.1.14 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`

42.2 show

Display device options and settings.

42.2.1 show mrp

Show MRP settings.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show mrp`

43 MRP IEEE

43.1 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

43.1.1 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.`

43.1.2 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.`

43.1.3 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.`

43.2 show

Display device options and settings.

43.2.1 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.	

44 MRP IEEE MMRP

44.1 mrp-ieee

Configure IEEE MRP protocols.

44.1.1 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>`

44.2 show

Display device options and settings.

44.2.1 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`

44.2.2 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.	

44.2.3 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`

44.2.4 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.	

44.2.5 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.`

44.2.6 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.`

44.3 mrp-ieee

Configure IEEE MRP protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration.

44.3.1 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`

44.3.2 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`

44.4 clear

Clear several items.

44.4.1 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`

44.5 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

44.5.1 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`

44.5.2 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`

44.6 show

Display device options and settings.

44.6.1 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`

45 MRP IEEE MVRP

45.1 mrp-ieee

Configure IEEE MRP protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration.

45.1.1 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`

45.1.2 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`

45.2 mrp-ieee

Configure IEEE MRP parameters and protocols, MVRP for dynamic VLAN registration and MMRP for dynamic MAC registration on a port.

45.2.1 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`

45.2.2 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`

45.3 show

Display device options and settings.

45.3.1 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`

45.3.2 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.	

45.3.3 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`

45.3.4 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.	

45.4 clear

Clear several items.

45.4.1 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`

46 Out-of-band Management

46.1 network

Configure the inband and outband connectivity.

46.1.1 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`

46.1.2 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`

46.1.3 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.`

46.2 show

Display device options and settings.

47 Protocol Based VLAN

47.1 vlan

Creation and configuration of VLANS.

47.1.1 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>`

47.1.2 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.

47.1.3 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.

47.2 vlan

Configure 802.1Q port parameters for VLANs.

47.2.1 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.`

47.2.2 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.`

47.3 show

Display device options and settings.

48 Port Monitor

48.1 port-monitor

Configure the Port Monitor condition settings.

48.1.1 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`

48.2 port-monitor

Configure the Port Monitor condition settings.

48.2.1 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.`

48.2.2 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.`

48.2.3 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`

48.2.4 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>`

Parameter	Value	Meaning
`P-1`	1..180	`Enter a number in the given range.`

48.2.5 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>`

Parameter	Value	Meaning
`P-1`	1..100	`Enter a number in the given range.`

48.2.6 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`

48.2.7 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`

48.2.8 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.`

48.2.9 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.

48.2.10 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.

48.2.11 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.

48.2.12 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.

48.2.13 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`

48.2.14 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`

48.2.15 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

48.2.16 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`

48.2.17 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.`

48.2.18 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>]`

48.3 show

Display device options and settings.

48.3.1 show port-monitor operation

Display the Port Monitor operation.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show port-monitor operation`

48.3.2 show port-monitor brief

Display the Port Monitor summary.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show port-monitor brief`

48.3.3 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`

48.3.4 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.	

48.3.5 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.	

48.3.6 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.	

48.3.7 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>`

Parameter	Value	Meaning
P-1	slot no./port no.	

48.3.8 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>`

Parameter	Value	Meaning
P-1	slot no./port no.	

49 Port Security

49.1 port-security

Port MAC locking/security

49.1.1 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`

49.2 port-security

Port MAC locking/security

49.2.1 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`

49.2.2 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`

49.2.3 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`

49.2.4 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`

49.2.5 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`

49.2.6 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

49.2.7 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]

49.3 show

Display device options and settings.

49.3.1 show port-security global

Port Security global status
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show port-security global`

49.3.2 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.	

49.3.3 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.	

49.3.4 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.	

49.3.5 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.	

50 Password Management

50.1 passwords

Manage password policies and options.

50.1.1 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.

50.1.2 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.

50.1.3 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.

50.1.4 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.`

50.1.5 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.`

50.1.6 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.`

50.2 show

Display device options and settings.

50.2.1 show passwords

Display password policies and options.

- Mode: `Command is in all modes available.`
- Privilege Level: `Administrator`
- Format: `show passwords`

51 Radius

51.1 authorization

Configure authorization parameters.

51.1.1 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`

51.2 radius

Configure RADIUS parameters.

51.2.1 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`

51.2.2 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.`

51.2.3 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

51.2.4 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.

51.2.5 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.

51.2.6 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

51.2.7 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.

51.2.8 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	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	string	Enter a user-defined text, max. 128 characters.
P-8	string	Enter a user-defined text, max. 128 characters.

51.2.9 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).

51.2.10 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).`

51.3 show

Display device options and settings.

51.3.1 show radius global

Display global RADIUS configuration.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show radius global`

51.3.2 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.`

51.3.3 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.`

51.3.4 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.`

51.3.5 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.`

51.4 clear

Clear several items.

51.4.1 clear radius

Clear the RADIUS statistics.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `clear radius <P-1>`

Parameter	Value	Meaning
`P-1`	statistics	`Clear the RADIUS statistics.`

52 Remote Monitoring (RMON)

52.1 rmon-alarm

Create a RMON alarm action.

52.1.1 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.`

52.1.2 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.`

52.1.3 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.`

52.1.4 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.`

52.1.5 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.

52.2 show

Display device options and settings.

52.2.1 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.	

52.2.2 show rmon alarm

Display configuration on RMON alarms.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show rmon alarm`

53 Script File

53.1 script

CLI Script File.

53.1.1 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.

53.1.2 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.

53.1.3 script list system

List all the script files available in the device memory.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `script list system`

53.1.4 script list envm

List all the script files available in external non-volatile memory.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `script list envm`

53.1.5 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.

53.2 copy

Copy different kinds of items.

53.2.1 copy script envm

Copy script file from external non-volatile memory to specified destination.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `copy script envm <P-1> running-config nvm <P-2>`

`running-config`: Copy script file from external non-volatile memory to the running-config.
`nvm`: Copy script file from external non-volatile memory to the non-volatile memory.

Parameter	Value	Meaning
`P-1`	string	Filename.
`P-2`	string	`Enter a user-defined text, max. 32 characters.`

53.2.2 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.`

53.2.3 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.`

53.2.4 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.`

53.2.5 copy script running-config envm

Copy running configuration to external non-volatile memory device.
- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `copy script running-config envm <P-1> [all]`

`[all]`: Copy all running configuration to external non-volatile memory.

Parameter	Value	Meaning
`P-1`	string	`Enter a user-defined text, max. 32 characters.`

53.2.6 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.`

53.3 show

Display device options and settings.

53.3.1 show script envm

Displays the content of the CLI script file present in the envm.
- Mode: `Command is in all modes available.`
- Privilege Level: `Administrator`
- Format: `show script envm <P-1>`

Parameter	Value	Meaning
`P-1`	string	Filename.

53.3.2 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.

54 Selftest

54.1 selftest

Configure the selftest settings.

54.1.1 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.`

54.1.2 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`

54.1.3 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`

54.1.4 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`

54.2 show

Display device options and settings.

54.2.1 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`

54.2.2 show selftest settings

Displays the selftest settings.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show selftest settings`

55 Small Form-factor Pluggable (SFP)

55.1 show

Display device options and settings.

55.1.1 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.	

56 Signal Contact

56.1 signal-contact

Configure the signal contact settings.

56.1.1 signal-contact mode

Configure the Signal Contact mode setting.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> mode <P-2>`

Parameter	Value	Meaning
`P-1`	signal contact no.	
`P-2`	manual	`The signal contact's status is determined by the\nassociated manual setting (subcommand 'state').`
	monitor	`The signal contact's status is determined by the\nassociated monitor settings.`
	device-status	`The signal contact's status is determined by the\ndevice status.`
	security-status	`The signal contact's status is determined by the\nsecurity status.`
	dev-sec-status	`The signal contact's status is determined by the\ndevice status and security status.`

56.1.2 signal-contact monitor link-failure

Sets the monitoring of the network connection(s).
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> monitor link-failure`

Parameter	Value	Meaning
`P-1`	signal contact no.	

no signal-contact monitor link-failure
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> monitor link-failure`

56.1.3 signal-contact monitor module-removal

Sets the monitoring of the module removal.

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> monitor module-removal`

Parameter	Value	Meaning
`P-1`	signal contact no.	

no signal-contact monitor module-removal

Disable the option

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> monitor module-removal`

56.1.4 signal-contact monitor envm-not-in-sync

Sets the monitoring whether the external non-volatile memory device\nis in sync with the running configuration.

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> monitor envm-not-in-sync`

Parameter	Value	Meaning
`P-1`	signal contact no.	

no signal-contact monitor envm-not-in-sync

Disable the option

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> monitor envm-not-in-sync`

56.1.5 signal-contact monitor envm-removal

Sets the monitoring of the external non-volatile memory device removal.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> monitor envm-removal`

Parameter	Value	Meaning
`P-1`	signal contact no.	

no signal-contact monitor envm-removal
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> monitor envm-removal`

56.1.6 signal-contact monitor temperature

Sets the monitoring of the device temperature.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> monitor temperature`

Parameter	Value	Meaning
`P-1`	signal contact no.	

no signal-contact monitor temperature
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> monitor temperature`

56.1.7 signal-contact monitor ring-redundancy

Sets the monitoring of the ring-redundancy.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> monitor ring-redundancy`

Parameter	Value	Meaning
P-1	signal contact no.	

■ **no signal-contact monitor ring-redundancy**
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> monitor ring-redundancy`

56.1.8 signal-contact monitor power-supply

Sets the monitoring of the power supply(s).
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> monitor power-supply <P-2>`

Parameter	Value	Meaning
P-1	signal contact no.	
P-2	1..2	`Number of power supply.`

■ **no signal-contact monitor power-supply**
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> monitor power-supply <P-2>`

56.1.9 signal-contact state

Configure the Signal Contact manual state (only takes\nimmediate effect in manual mode).
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> state <P-2>`

Parameter	Value	Meaning
P-1	signal contact no.	
P-2	open	`Open the signal contact (only takes effect\nin the manual mode).`
	close	`Close the signal contact (only takes effect\nin the manual mode).`

56.1.10 signal-contact trap

Configure if a trap is sent when the Signal Contact\nchanges state (in monitor mode).
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> trap`

Parameter	Value	Meaning
`P-1`	signal contact no.	

no signal-contact trap
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> trap`

56.1.11 signal-contact module

Configure the monitoring of the specific module.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> module <P-2>`

Parameter	Value	Meaning
`P-1`	signal contact no.	
`P-2`	slot no./port no.	

no signal-contact module
Disable the option
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `no signal-contact <P-1> module <P-2>`

56.2 signal-contact

Configure the signal contact interface settings.

56.2.1 signal-contact link-alarm

Configure the monitoring of the specific network ports.
- Mode: `Interface Range Mode`
- Privilege Level: `Administrator`
- Format: `signal-contact <P-1> link-alarm`

Parameter	Value	Meaning
`P-1`	signal contact no.	

- **no signal-contact link-alarm**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Administrator`
  - Format: `no signal-contact <P-1> link-alarm`

56.3 show

Display device options and settings.

56.3.1 show signal-contact

Display signal contact settings.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show signal-contact <P-1> mode monitor state trap link-alarm module events all`

`mode`: Display the signal contact mode.
`monitor`: Display the signal contact monitor settings.
`state`: Display the signal contact state (open/close).\nNote: This covers the signal contact`s administrative\nsetting as well as its actual state.
`trap`: Display the signal contact trap information and settings.
`link-alarm`: Display the settings of the monitoring of the specific\nnetwork ports.
`module`: Display the settings of the monitoring of the specific\nmodules.
`events`: Display occurred device status events.
`all`: Display all signal contact settings for the specified\nsignal contact.

Parameter	Value	Meaning
`P-1`	signal contact no.	

57 Slot

57.1 slot

Configure module status.

57.1.1 slot operation

Enable or disable slot
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `slot <P-1> operation`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

- **no slot operation**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no slot <P-1> operation`

57.1.2 slot module

Remove a virtual module
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `slot <P-1> module <P-2>`

Parameter	Value	Meaning
`P-1`	slot no./port no.	
`P-2`	remove-virtual	`Remove a virtual module`

57.2 show

Display device options and settings.

57.2.1 show slot

Show module parameters.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show slot [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

58 Switched Monitoring (SMON)

58.1 monitor

Configure port mirroring.

58.1.1 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\nnot 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`

58.2 show

Display device options and settings.

58.2.1 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.`

58.3 clear

Clear several items.

58.3.1 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.`

59 Simple Network Management Protocol (SNMP)

59.1 snmp

Configure of SNMP versions and traps.

59.1.1 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`

59.1.2 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`

59.1.3 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`

59.1.4 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).`

59.1.5 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`

59.2 show

Display device options and settings.

59.2.1 show snmp access

Show SNMP access configuration settings.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show snmp access`

60 SNMP Community

60.1 snmp

Configure of SNMP versions and traps.

60.1.1 snmp community ro

SNMP v1/v2 read-only community.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `snmp community ro`

60.1.2 snmp community rw

SNMP v1/v2 read-write community.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `snmp community rw`

60.2 show

Display device options and settings.

60.2.1 show snmp community

Display SNMP v1/2 community.

- Mode: `Command is in all modes available.`
- Privilege Level: `Administrator`
- Format: `show snmp community`

61 SNMP Logging

61.1 logging

Logging configuration.

61.1.1 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>`

61.1.2 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

61.1.3 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>`

61.1.4 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`

61.2 show

Display device options and settings.

61.2.1 show logging snmp

Show the SNMP logging settings.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show logging snmp`

62 Simple Network Time Protocol (SNTP)

62.1 sntp

Configure SNTP settings.

62.1.1 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`

62.1.2 sntp client operating-mode

Set the operating mode of the SNTP client. \nIn unicast-mode, the client sends a request to the SNTP Server. \nIn 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.`

62.1.3 sntp client request-interval

Set the SNTP client request interval in seconds. \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.

62.1.4 sntp client broadcast-rcv-timeout

Set the SNTP client broadcast receive timeout in seconds. \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.

62.1.5 sntp client disable-after-sync

If this option is activated, the SNTP client disables itself \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`

62.1.6 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.`

62.1.7 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.`

62.1.8 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>`

62.1.9 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`

62.1.10 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).`

62.1.11 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`

62.1.12 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`

62.1.13 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.

62.1.14 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).`

62.1.15 sntp server broadcast interval

Set the SNTP server's interval in seconds for sending\nbroadcast 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.`

62.1.16 sntp server broadcast vlan

Set the SNTP server's broadcast VLAN ID used for sending\nbroadcast 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.`

62.2 show

Display device options and settings.

62.2.1 show sntp global

Show SNTP configuration parameters and information.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show sntp global`

62.2.2 show sntp client status

Show SNTP client status.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show sntp client status`

62.2.3 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.

62.2.4 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`

62.2.5 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`

63 Spanning Tree

63.1 spanning-tree

Enable or disable the Spanning Tree protocol.

63.1.1 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`

63.1.2 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`

63.1.3 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`

63.1.4 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.	

63.1.5 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).`

63.1.6 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>`

Parameter	Value	Meaning
P-1	4..30	Enter the bridge forward delay as an integer.

63.1.7 spanning-tree hello-time

Set the Hello Time parameter [s].

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `spanning-tree hello-time <P-1>`

Parameter	Value	Meaning
P-1	1..2	Set the Hello Time parameter (unit: seconds).

63.1.8 spanning-tree hold-count

Set the bridge hold count parameter.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `spanning-tree hold-count <P-1>`

Parameter	Value	Meaning
P-1	1..40	Set bridge hold count parameter.

63.1.9 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.

63.1.10 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

63.1.11 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.	

63.1.12 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.	

63.1.13 spanning-tree mst

MST instance related configuration.

- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `spanning-tree mst`

63.2 spanning-tree

Enable or disable the Spanning Tree protocol on a port.

63.2.1 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`

63.2.2 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`

63.2.3 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`

63.2.4 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`

63.2.5 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`

63.2.6 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`

63.2.7 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`

63.2.8 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.`

63.2.9 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.`

63.3 show

Display device options and settings.

63.3.1 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`

63.3.2 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`

63.3.3 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.	

63.3.4 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.	

64 Secure Shell (SSH)

64.1 ssh

Set SSH parameters.

64.1.1 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`

64.1.2 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).`

64.1.3 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).`

64.1.4 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.`

64.1.5 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.`

64.1.6 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>`

Parameter	Value	Meaning
P-1	0..160	Idle timeout of a session in minutes (default: 5).

64.1.7 ssh key rsa

Generate or delete RSA key

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ssh key rsa <P-1>

Parameter	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

64.1.8 ssh key dsa

Generate or delete DSA key

- Mode: Global Config Mode
- Privilege Level: Administrator
- Format: ssh key dsa <P-1>

Parameter	Value	Meaning
P-1	generate	Generates the item
	delete	Deletes the item

64.2 copy

Copy different kinds of items.

64.2.1 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.`

64.2.2 copy sshkey envm

Copy the SSH key from external non-volatile memory to the specified destination.

- Mode: `Privileged Exec Mode`
- Privilege Level: `Administrator`
- Format: `copy sshkey envm <P-1> nvm`

`nvm`: Copy the SSH key from external non-volatile memory to non-volatile memory.

Parameter	Value	Meaning
`P-1`	string	`Enter a user-defined text, max. 128 characters.`

64.3 show

Display device options and settings.

64.3.1 show ssh

Show SSH server and client information.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show ssh`

65 Storm Control

65.1 storm-control

Configure the global storm-control settings.

65.1.1 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`

65.2 traffic-shape

Traffic shape commands.

65.2.1 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.`

65.3 mtu

65.3.1 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.`

65.4 mtu

65.4.1 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..12288	`Enter a number in the given range.`

65.5 storm-control

Storm control commands

65.5.1 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`

65.5.2 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.`

65.5.3 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.`

65.5.4 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`

65.5.5 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`

65.5.6 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`

65.6 show

Display device options and settings.

65.6.1 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`

65.6.2 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>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

65.6.3 show traffic-shape

Show Traffic Shape Parameters.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show traffic-shape`

65.6.4 show mtu

Show mtu Parameters.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show mtu`

66 System

66.1 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.

66.1.1 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>`

Parameter	Value	Meaning
`P-1`	string	`Enter a user-defined text, max. 255 characters.`

66.1.2 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>`

Parameter	Value	Meaning
`P-1`	string	`Enter a user-defined text, max. 255 characters.`

66.1.3 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.

66.1.4 system port-led-mode

Configure the port led signalling (frontpanel or servicepanel).

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `system port-led-mode <P-1>`

Parameter	Value	Meaning
P-1	portpanel	Set LED control to portpanel.
	servicepanel	Set LED control to servicepanel.

66.1.5 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`

66.1.6 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).`

66.1.7 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`

66.2 temperature

Configure the upper and lower temperature limits of the device. The device allows you to set the threshold as an integer from -99 through 99. You configure the temperatures in degrees Celsius.

66.2.1 temperature upper-limit

Configure the upper temperature limit.

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `temperature upper-limit <P-1>`

Parameter	Value	Meaning
`P-1`	-99..99	`Upper temperature threshold ([C], default 70).`

66.2.2 temperature lower-limit

Configure the lower temperature limit.

- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `temperature lower-limit <P-1>`

Parameter	Value	Meaning
`P-1`	-99..99	`Lower temperature threshold ([C], default 0).`

66.3 show

Display device options and settings.

66.3.1 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`

66.3.2 show system info

Show system related information.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show system info`

66.3.3 show system port-led-mode

Display led control settings.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show system port-led-mode`

66.3.4 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`

66.3.5 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`

66.3.6 show system temperature limits

Show temperature limits.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show system temperature limits`

66.3.7 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`

66.3.8 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`

66.3.9 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`

66.3.10 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`

66.3.11 show psu slot

Display power supply slots
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show psu slot`

66.3.12 show psu unit

Display information for power supply units.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show psu unit`

67 Telnet

67.1 telnet

Set Telnet parameters.

67.1.1 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`

67.1.2 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).`

67.1.3 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.`

67.1.4 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.`

67.2 telnet

67.2.1 telnet

Establish a telnet connection to a remote host.

- Mode: `"User Mode" and "Privileged Exec Mode"`
- Privilege Level: `Guest`
- Format: `telnet <P-1> [<P-2>] [<P-3>] [<P-4>] [<P-5>]`

Parameter	Value	Meaning
`P-1`	string	Hostname or IP address.
`P-2`	1..65535	`Enter port number between 1 and 65535`
`P-3`	debug	`Display the current Telnet options.`
`P-4`	line	`Set the outbound Telnet operational mode as linemode (only takes effect for the serial connection).`
`P-5`	echo	`Enable local echo (only takes effect for the serial connection).`

67.3 show

Display device options and settings.

67.3.1 show telnet

Show telnet server information.

- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show telnet`

68 Traps

68.1 snmp

Configure of SNMP versions and traps.

68.1.1 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`

68.1.2 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>`

68.1.3 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)

68.1.4 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.

68.2 show

Display device options and settings.

68.2.1 show snmp traps

Display SNMP traps.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show snmp traps`

69 User Management

69.1 show

Display device options and settings.

69.1.1 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>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

69.1.2 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>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

70 Users

70.1 users

Manage Users and User Accounts.

70.1.1 users add

Add a new user.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `users add <P-1>`

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

70.1.2 users delete

Delete an existing user.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `users delete <P-1>`

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

70.1.3 users enable

Enable user.
- Mode: `Global Config Mode`
- Privilege Level: `Administrator`
- Format: `users enable <P-1>`

Parameter	Value	Meaning
P-1	string	<user> User name (up to 32 characters).

70.1.4 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).

70.1.5 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.

70.1.6 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.

70.1.7 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.
	aescfb128	AES-128 as SNMPv3 encryption method.

70.1.8 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.	

70.1.9 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.

70.1.10 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.`

70.2 show

Display device options and settings.

70.2.1 show users

Display users and user accounts information.
- Mode: `Command is in all modes available.`
- Privilege Level: `Administrator`
- Format: `show users`

71 Virtual LAN (VLAN)

71.1 name

71.1.1 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.`

71.2 vlan-unaware-mode

71.2.1 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`

71.3 vlan

Creation and configuration of VLANS.

71.3.1 vlan add

Create a VLAN
- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `vlan add <P-1>`

Parameter	Value	Meaning
`P-1`	1..4042	`Enter the VLAN ID.`

71.3.2 vlan delete

Delete a VLAN
- Mode: `VLAN Database Mode`
- Privilege Level: `Operator`
- Format: `vlan delete <P-1>`

Parameter	Value	Meaning
`P-1`	2..4042	`Enter VLAN ID. VLAN ID 1 can not be deleted or created`

71.4 vlan

Configure 802.1Q port parameters for VLANs.

71.4.1 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.`

71.4.2 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`

71.4.3 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.`

71.4.4 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.`

71.4.5 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>`

71.4.6 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.`

71.4.7 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.`

71.4.8 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.`

71.5 show

Display device options and settings.

71.5.1 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.`

71.5.2 show vlan brief

Show general VLAN parameters.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show vlan brief`

71.5.3 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.	

71.5.4 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`

71.5.5 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`

71.6 network

Configure the inband and outband connectivity.

71.6.1 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.`

71.6.2 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.`

71.6.3 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.`

72 Voice VLAN

72.1 voice

Configure voice VLAN.

72.1.1 voice vlan

Enable or disable the voice VLAN feature.
- Mode: `Global Config Mode`
- Privilege Level: `Operator`
- Format: `voice vlan`

- **no voice vlan**
  Disable the option
  - Mode: `Global Config Mode`
  - Privilege Level: `Operator`
  - Format: `no voice vlan`

72.2 voice

Configure voice VLAN.

72.2.1 voice vlan vlan-id

Set and configure the vlan-id interface mode.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `voice vlan vlan-id <P-1> [dot1p <P-2>]`

`[dot1p]`: Set and configure the vlan id and dot1p interface mode.

Parameter	Value	Meaning
P-1	0..4042	Enter the VLAN ID. Entering of ID 0 disables the feature.
P-2	0	priority 0
	1	priority 1
	2	priority 2
	3	priority 3
	4	priority 4
	5	priority 5
	6	priority 6
	7	priority 7
	255	default

72.2.2 voice vlan dot1p

Set and configure the dot1p voice vlan interface mode.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `voice vlan dot1p <P-1>`

Parameter	Value	Meaning
P-1	0	priority 0
	1	priority 1
	2	priority 2
	3	priority 3
	4	priority 4
	5	priority 5
	6	priority 6
	7	priority 7
	255	default

72.2.3 voice vlan none

Configure the none voice VLAN interface mode.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `voice vlan none`

72.2.4 voice vlan untagged

Configure the untagged voice VLAN interface mode.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `voice vlan untagged`

72.2.5 voice vlan disable

Disable voice VLAN on the interface.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `voice vlan disable`

72.2.6 voice vlan auth

Set voice VLAN Authentication Mode on the interface.
- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `voice vlan auth`

- **no voice vlan auth**
  Disable the option
  - Mode: `Interface Range Mode`
  - Privilege Level: `Operator`
  - Format: `no voice vlan auth`

72.2.7 voice vlan data priority

Trust/Untrust data traffic on the interface.

- Mode: `Interface Range Mode`
- Privilege Level: `Operator`
- Format: `voice vlan data priority <P-1>`

Parameter	Value	Meaning
`P-1`	trust	`Trust data traffic on an interface.`
	untrust	`Untrust data traffic on an interface.`

72.3 show

Display device options and settings.

72.3.1 show voice vlan global

Display the current global Voice VLAN admin mode.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show voice vlan global`

72.3.2 show voice vlan interface

Display a summary of the current Voice VLAN configuration for a specific port or for all ports.
- Mode: `Command is in all modes available.`
- Privilege Level: `Guest`
- Format: `show voice vlan interface [<P-1>]`

Parameter	Value	Meaning
`P-1`	slot no./port no.	

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-2S GRS (Greyhound 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.

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 auf externem Speicher speichern 63
4.2.4 Konfigurationsprofil exportieren 64

4.3 Einstellungen laden 66
4.3.1 Konfigurationsprofil aktivieren 66
4.3.2 Konfigurationsprofil aus dem externen Speicher laden 67
4.3.3 Konfigurationsprofil importieren 68

4.4 Gerät auf Lieferzustand zurücksetzen 70
4.4.1 Mit grafischer Benutzeroberfläche oder CLI 70
4.4.2 System-Monitor starten 70

5 Neueste Software laden 73

5.1 Software-Update vom PC 74

5.2 Software-Update von einem Server 75

5.3 Software-Update vom externen Speicher 76
5.3.1 Manuell – durch den Administrator initiiert 76
5.3.2 Automatisch – durch das Gerät initiiert 76

5.4 Ältere Software laden 78

6 Ports konfigurieren 79

6.1 Port ein-/ausschalten 80

6.2 Betriebsart wählen 81

6.3 Modulsteckplätze deaktivieren 82

7 Unterstützung beim Schutz vor unberechtigtem Zugriff 83

7.1 SNMPv1/v2-Community ändern 84

7.2 SNMPv1/v2 ausschalten 85

7.3 HTTP ausschalten 86

7.4 Telnet ausschalten 87

7.5 HiDiscovery-Zugriff ausschalten 88

7.6 IP-Zugriffsbeschränkung aktivieren 89

7.7 Session-Timeouts anpassen 91

8 Datenverkehr kontrollieren 93

8.1 Unterstützung beim Schutz vor Denial of Service (DoS) 94

8.2 ACL 95
8.2.1 Erzeugen und Bearbeiten von IPv4 -Regeln 96
8.2.2 Erzeugen und Konfigurieren einer IP-ACL im CLI 97
8.2.3 Erzeugen und Bearbeiten von MAC -Regeln 98
8.2.4 Erzeugen und Konfigurieren einer MAC-ACL im CLI 99
8.2.5 Zuweisen von ACL-Gruppen zu Ports oder VLANs 99

9 Die Systemzeit im Netz synchronisieren 101

9.1 Grundeinstellungen 102
9.1.1 Uhrzeit einstellen 102
9.1.2 Automatische Sommerzeitumschaltung 103

9.2 SNTP 104
9.2.1 Vorbereitung 105
9.2.2 Einstellungen des SNTP-Clients festlegen 106
9.2.3 Einstellungen des SNTP-Servers festlegen 106

10 Netzlaststeuerung 109

10.1 Gezielte Paketvermittlung 110
10.1.1 Lernen der MAC-Adressen 111
10.1.2 Aging gelernter MAC-Adressen 111
10.1.3 Statische Adresseinträge 111

10.2 Multicasts 113
10.2.1 Beispiel für eine Multicast-Anwendung 113
10.2.2 IGMP-Snooping 113

10.3 Lastbegrenzung 118

10.4 QoS/Priorität 119
10.4.1 Beschreibung Priorisierung 119
10.4.2 Behandlung empfangener Prioritätsinformationen 120
10.4.3 VLAN-Tagging 121
10.4.4 IP ToS (Type of Service) 122
10.4.5 Handhabung der Verkehrsklassen 122
10.4.6 Queue-Management 123
10.4.7 Management-Priorisierung 124
10.4.8 Priorisierung einstellen 125

10.5 Flusskontrolle 128
10.5.1 Halbduplex- oder Vollduplex-Verbindung 129
10.5.2 Flusskontrolle einrichten 129

11 VLANs 131

11.1 Beispiele für ein VLAN 132
11.1.1 Beispiel 1 132
11.1.2 Beispiel 2 135

11.2 Gast-VLAN / Unauthentifiziertes VLAN 139

11.3 RADIUS-VLAN-Zuordnung 141

11.4 Voice-VLAN erzeugen 142

11.5 VLAN-Unaware-Modus 143

12 Redundanz 145

12.1 Netz-Topologie vs. Redundanzprotokolle 146
12.1.1 Netz-Topologien 147
12.1.2 Redundanzprotokolle 148
12.1.3 Redundanzkombinationen 148

12.2 Media Redundancy Protocol (MRP) 149
12.2.1 Netzstruktur 149
12.2.2 Rekonfigurationszeit 150
12.2.3 Advanced Mode 150
12.2.4 Voraussetzungen für MRP 150
12.2.5 Beispiel-Konfiguration 151

12.3 Spanning Tree 155
12.3.1 Grundlagen 156
12.3.2 Regeln für die Erstellung der Baumstruktur 159
12.3.3 Beispiele 161
12.3.4 Das Rapid Spanning Tree Protokoll 164
12.3.5 Gerät konfigurieren 167
12.3.6 Guards 169
12.3.7 Ring only mode 172

12.4 Link-Aggregation 173
12.4.1 Funktionsweise 173
12.4.2 Link-Aggregation Beispiel 174
12.5 Link-Backup 175
12.5.1 Beschreibung Fail-Back 175
12.5.2 Beispiel-Konfiguration 176

13 Funktionsdiagnose 179

13.1 SNMP-Traps senden 180
13.1.1 Auflistung der SNMP-Traps 181
13.1.2 SNMP-Traps für Konfigurationsaktivitäten 182
13.1.3 SNMP-Trap-Einstellung 183
13.1.4 ICMP-Messaging 183
13.2 Gerätestatus überwachen 184
13.2.1 Ereignisse, die überwacht werden können 185
13.2.2 Gerätestatus konfigurieren 185
13.2.3 Gerätestatus anzeigen 186
13.3 Sicherheitsstatus 188
13.3.1 Ereignisse, die überwacht werden können 188
13.3.2 Konfigurieren des Sicherheitsstatus 189
13.3.3 Anzeigen des Sicherheitsstatus 190
13.4 Out-of-Band-Signalisierung 191
13.4.1 Signalkontakt steuern 191
13.4.2 Gerätestatus und Sicherheitsstatus überwachen 192
13.5 Port-Zustandsanzeige 195
13.6 Portereignis-Zähler 196
13.6.1 Erkennen der Nichtübereinstimmung der Duplex-Modi 196
13.7 Auto-Disable 198
13.8 SFP-Zustandsanzeige 200
13.9 Topologie-Erkennung 201
13.9.1 Anzeige der Topologie-Erkennung 202
13.9.2 LLDP-MED 202
13.10 Erkennen von Schleifen 204
13.11 Berichte 205
13.11.1 Globale Einstellungen 205
13.11.2 Syslog 207
13.11.3 System-Log 208
13.11.4 Audit Trail 208
13.12 Netzanalyse mit TCPDump 210
13.13 Datenverkehr beobachten 211
13.13.1 Port-Mirroring 211
13.14 Selbsttest 213
13.15 Kupferkabeltest 215

14 Erweiterte Funktionen des Gerätes 217

14.1 Gerät als DHCP-Server verwenden 218
14.1.1 Pro Port oder pro VLAN zugewiesene IP-Adressen 218
14.1.2 Beispiel: DHCP-Server – Statische IP-Adresse 219
14.1.3 Beispiel: DHCP-Server – Dynamischer IP-Adressbereich 219
14.2 DHCP-L2-Relay 221
14.2.1 Circuit- und Remote-IDs 221
14.2.2 DHCP-L2-Relay-Konfiguration 222
14.3 GARP 224

14.3.1 GMRP konfigurieren 224
14.3.2 GVRP konfigurieren 225
14.4 MRP-IEEE 226
14.4.1 MRP-Funktion 226
14.4.2 MRP-Timer 227
14.4.3 MMRP 227
14.4.4 MVRP 229
14.5 CLI Client 231

15 Industrieprotokolle 233

15.1 IEC 61850/MMS 234
15.1.1 Switch-Modell für IEC 61850 234
15.1.2 Integration in ein Steuerungssystem 235
15.2 Modbus TCP 237
15.2.1 Modbus TCP/IP Client/Server-Modus 237
15.2.2 Unterstützte Funktionen und Speicherzuordnung 238
15.2.3 Beispiel-Konfiguration 240

A Konfigurationsumgebung einrichten 243

A.1 DHCP/BOOTP-Server einrichten 244
A.2 DHCP-Server Option 82 einrichten 248
A.3 SSH-Zugriff vorbereiten 251
A.3.1 Schlüssel auf dem Gerät erzeugen 251
A.3.2 Eigenen Schlüssel in das Gerät laden 251
A.3.3 SSH-Client-Programm vorbereiten 253
A.4 HTTPS-Zertifikat 255
A.4.1 HTTPS-Zertifikatsverwaltung 255
A.4.2 Zugang über HTTPS 256

B Anhang 257

B.1 Literaturhinweise 258
B.2 Wartung 259
B.3 Management Information BASE (MIB) 260
B.4 Liste der RFCs 262
B.5 Zugrundeliegende IEEE-Normen 264
B.6 Zugrundeliegende IEC-Normen 265
B.7 Zugrundeliegende ANSI-Normen 266
B.8 Technische Daten 267
B.9 Copyright integrierter Software 268
B.10 Verwendete Abkürzungen 269

C Index 271

D Weitere Unterstützung 273

E Leserkritik 274

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 Gerätes 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.
`Courier`	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.

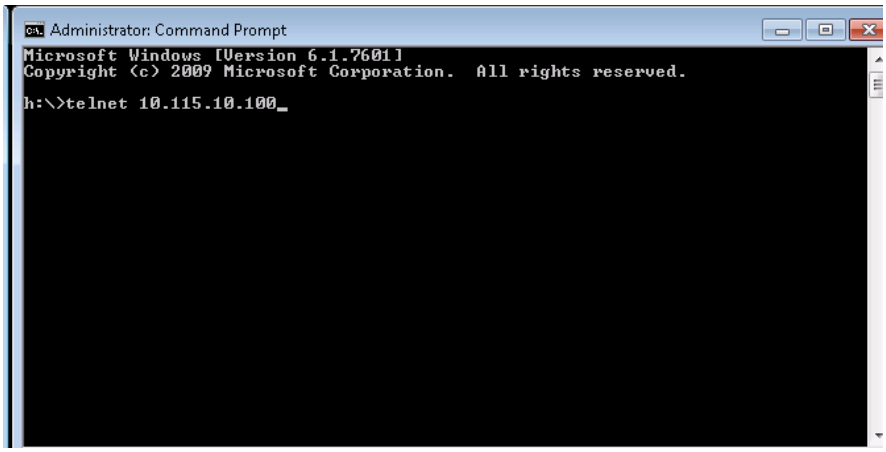


Abb. 1: `Eingabeaufforderung`: Telnet-Verbindung zum Gerät herstellen

Telnet-Verbindung über PuTTY

☐ Starten Sie auf Ihrem Rechner das Programm ***`PuTTY`***.

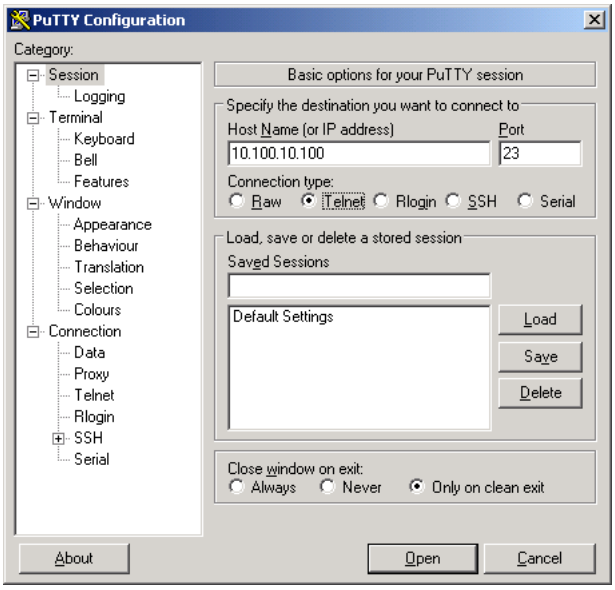


Abb. 2: `PuTTY`-Eingabemaske

☐ 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 5 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:

```
(GRS) >
```

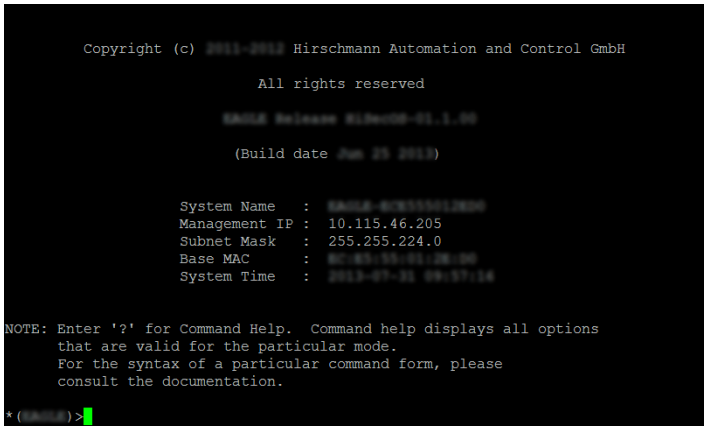


Abb. 4: Start-Bildschirm des CLI

1.2.3 CLI über SSH (Secure Shell)

☐ Starten Sie auf Ihrem Rechner das Programm *PuTTY*.

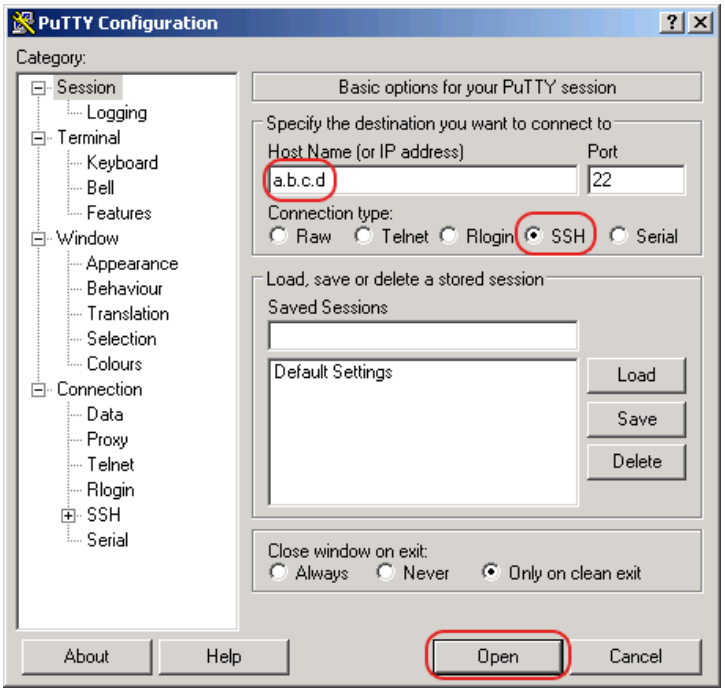


Abb. 5: PuTTY-Eingabemaske

☐ 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 5 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.

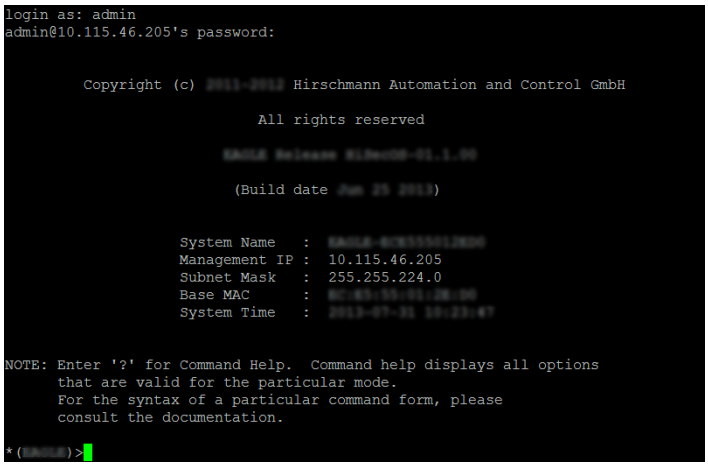


Abb. 7: Start-Bildschirm des CLI

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.

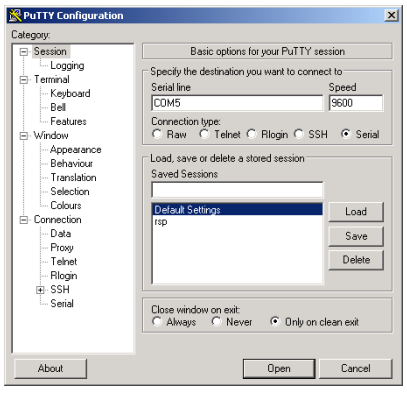


*Abb. 8: Serielle Datenverbindung über V.24 mit dem Programm **PuTTY***

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.

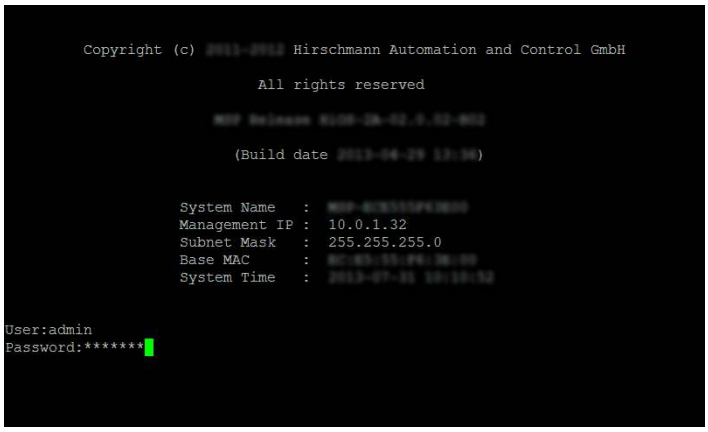


Abb. 9: Einloggen in das Command Line Interface Programm

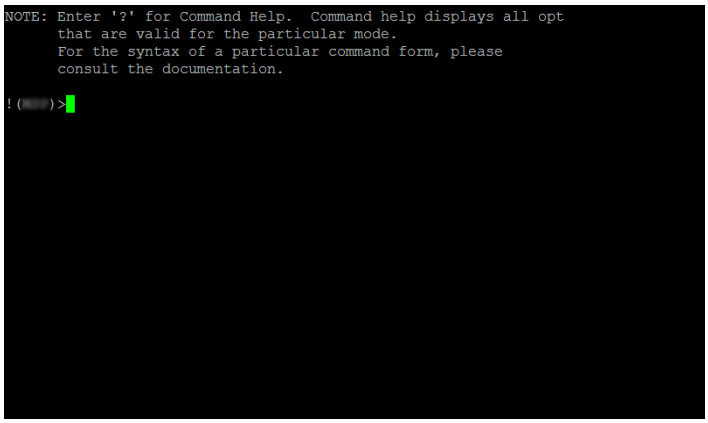


Abb. 10: CLI-Bildschirm nach dem Einloggen

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 verwalten und Software-Image prüfen
- 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: Bildschirmansicht 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.
- Konfiguration über den externen Speicher.
  Wählen Sie diese Methode, wenn Sie ein Gerät durch ein Gerät desselben Typs ersetzen und Sie die Konfiguration bereits in einem externen Speicher gespeichert haben.
- 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

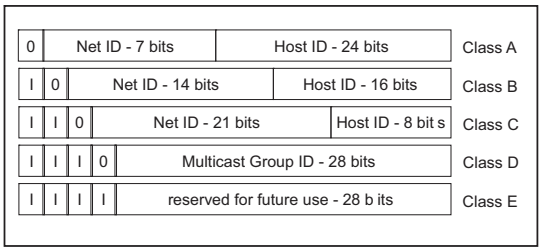


Abb. 12: Bitdarstellung der IP-Adresse

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.

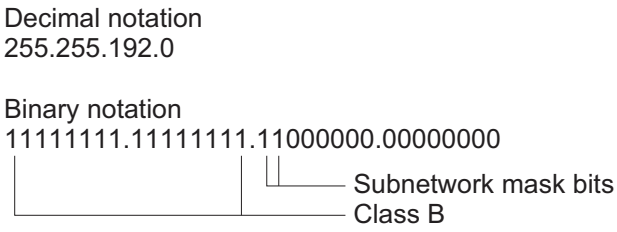
2.1.2 Netzmaske

Router und Gateways unterteilen große Netze in Subnetze. Die Netzmaske ordnet die IP-Adressen der einzelnen Geräte einem bestimmten Subnetz zu.

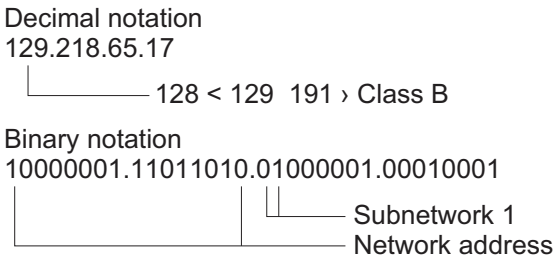
Die Einteilung in Subnetze erfolgt über die Netzmaske analog zu der Einteilung der Netzadresse (net id) in die Klassen A bis C.

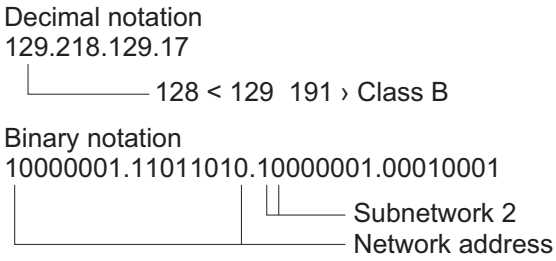
Setzen Sie die Bits der Hostadresse (host id), die die Maske darstellen, auf Eins. Setzen Sie die restlichen Bits der Hostadresse auf Null (vgl. folgende Beispiele).

Beispiel für eine Subnetzmaske:



Beispiel für IP-Adressen mit Subnetzzuordnung gemäß der Netzmaske:





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?

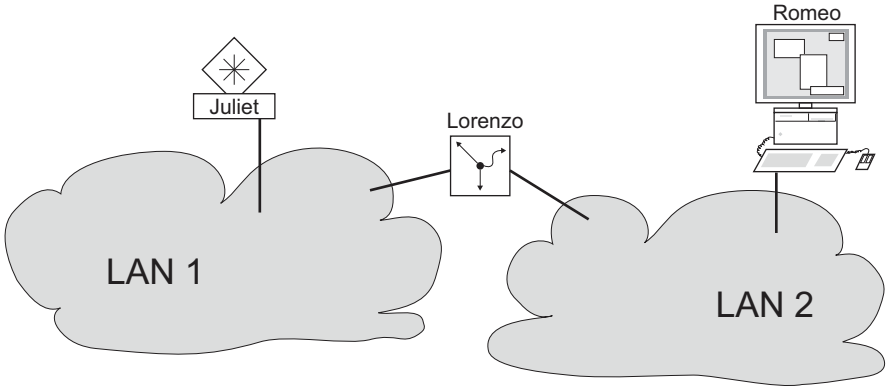


Abb. 13: Management-Agent durch Router von der Netz-Management-Station getrennt

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 Umschlags bei Lorenzo zurück.

Julia findet in der MIB unter der Variablen `hmNetGatewayIPAddr` Lorenzo als Vermittler zu Romeo. So steckt sie den Umschlag mit den IP-Adressen in einen weiteren Umschlag mit der MAC-Zieladresse von Lorenzo.

Nun findet der Brief den gleichen Weg über Lorenzo zu Romeo, so wie der Brief von Romeo zu Julia fand.

2.1.3 Classless Inter-Domain Routing

Die Klasse C mit maximal 254 Adressen war zu klein, und die Klasse B mit maximal 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

Bei der Eingabe der Systemkonfiguration können Sie nach mehreren Methoden vorgehen: entweder über BOOTP/DHCP, das Protokoll HiDiscovery, den externen Speicher. Sie haben die Möglichkeit, die Konfiguration über die V.24-Schnittstelle mithilfe des CLI vorzunehmen.

Das Gerät bietet Ihnen die Möglichkeit, die IP-Parameter über das HiDiscovery-Protokoll oder über die V.24-Schnittstelle mit Hilfe des CLI festzulegen.

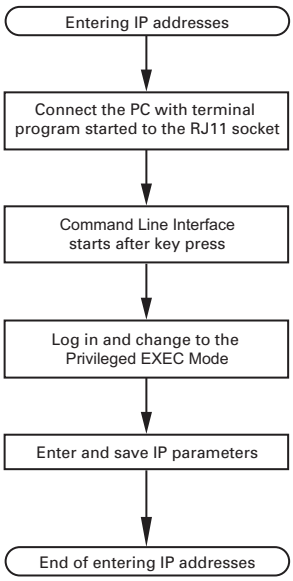
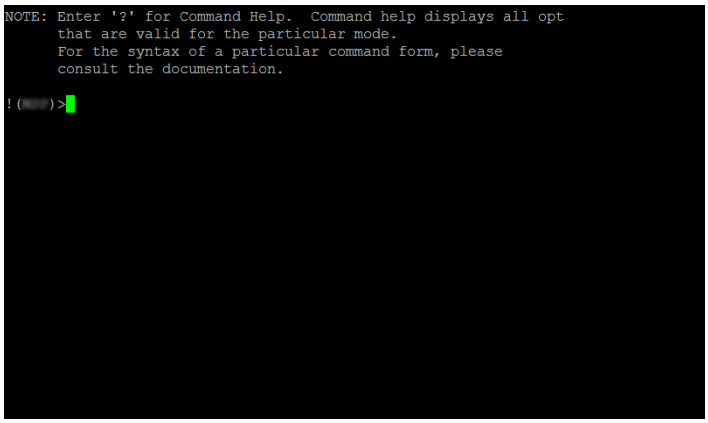


Abb. 14: Ablaufdiagramm Eintragen der IP-Adressen

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.



☐ 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 nvm`.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network protocol none`	DHCP ausschalten.
`network parms 10.0.1.23 255.255.255.0`	Dem Gerät die IP-Adresse `10.0.1.23` und die Netzmaske `255.255.255.0` zuweisen. Optional können Sie zusätzlich eine Gateway-Adresse zuweisen.
`copy config running-config nvm`	Speichern der aktuellen Einstellungen im „ausgewählten” Konfigurationsprofil im permanenten Speicher (`nvm`).

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 .

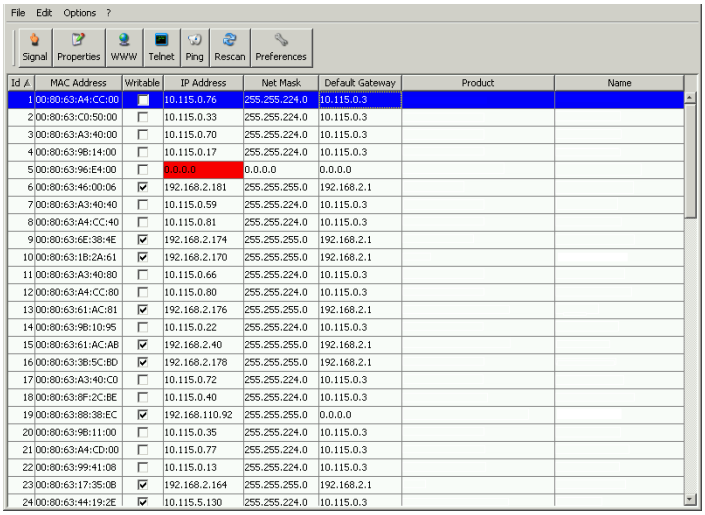


Abb. 15: HiDiscovery

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.

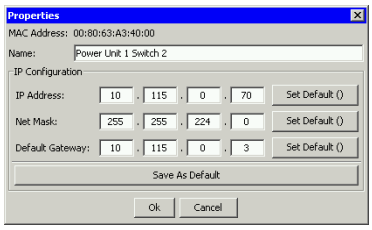


Abb. 16: HiDiscovery – IP-Parameter-Zuweisung

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 Netzschnittstelle 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-Decline-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 zwischenzuspeichern, 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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`authlists add loginGUI`	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`	Weist die Richtlinien `radius`, `local` und `reject` der Authentifizierungs-Liste `loginGUI` zu.
`show authlists`	Zeigt die eingerichteten Authentifizierungs-Listen.
`authlists enable loginGUI`	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 applists`	Zeigt die Anwendungen und die zugewiesenen Listen.
`applists set-authlist WebInterface loginGUI`	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: ▶ 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 ▶ Externen Speicher aktivieren und deaktivieren ▶ 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 ***Diagnose > Bericht >*** 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	`admin`	`user`
Passwort	`private`	`public`
Rolle	`administrator`	`guest`
Benutzer gesperrt	`unmarkiert`	`unmarkiert`
Richtlinien überprüfen	`unmarkiert`	`unmarkiert`
SNMP-Authentifizierung	`hmacmd5`	`hmacmd5`
SNMP-Verschlüsselung	`des`	`des`

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 Passworts 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 Passworts ist im Rahmen ***Konfiguration*** festgelegt. Die Mindestlänge des Passwortes prüft das Gerät immer.

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`users password-policy-check <user> enable`	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 Passworts 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 Passworts 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 zwischenzuspeichern, klicken Sie die Schaltfläche .
Der Dialog zeigt die eingerichteten Benutzerkonten.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`users add USER`	Erzeugt das Benutzerkonto `USER`.
`users password-policy-check USER enable`	Aktiviert für das Benutzerkonto `USER` das Prüfen des Passwortes anhand der festgelegten Richtlinien. Damit erzielen Sie eine höhere Komplexität des Passwortes.
`users password USER SECRET`	Legt für das Benutzerkonto `USER` das Passwort `SECRET` fest. Fügen Sie mindestens 6 Zeichen ein.
`users access-role USER operator`	Weist die Rolle `operator` dem Benutzerkonto `USER` zu.
`users enable USER`	Aktiviert das Benutzerkonto `USER`.
`show users`	Zeigt die eingerichteten Benutzerkonten.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) 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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`users disable <user>`	Deaktivieren eines Benutzerkontos.
`show users`	Zeigt die eingerichteten Benutzerkonten.
`save`	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>`	Löscht das Benutzerkonto `<user>`.
`show users`	Zeigt die eingerichteten Benutzerkonten.
`save`	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 (`nvm`) 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 zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`users snmpv3 authentication <user> md5 | sha1`	Protokoll HMAC-MD5 oder HMAC-SHA dem Benutzerkonto `<user>` für Authentifizierungsanfragen zuweisen.
`users snmpv3 encryption <user> des | aescfb128 | none`	Algorithmus DES oder AES-128 dem Benutzerkonto `<user>` zuweisen. Mit dem Algorithmus verschlüsselt das Gerät Authentifizierungsanfragen. Der Wert `none` hebt die Verschlüsselung auf.
`show users`	Eingerichtete Benutzerkonten anzeigen.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

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 <?>.

```
!(GRS) >enable

!(GRS) #?
  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.

!(GRS) #serviceshell

-> exit
Au revoir!

!*(GRS) #
```

☐ 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.

```
!(GRS) >enable

!(GRS) #serviceshell?
 [deactivate]          Disable the service shell access permanently
                       (Cannot be undone).
  <cr>                 Press Enter to execute the command.

!(GRS) #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.

Wenn ein externer Speicher angeschlossen ist, erzeugt das Gerät automatisch eine Kopie des Konfigurationsprofils auf dem externen Speicher. Diese Funktion lässt sich deaktivieren.

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
...
```

Wenn sich die Kopie auf dem externen Speicher vom Konfigurationsprofil im permanenten Speicher unterscheidet, erkennen Sie diesen Unterschied an den folgenden Kriterien:

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
--------------------------------
...
NV to ACA..................................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 zwischenzuspeichern, 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 auf externem Speicher speichern

Beim Speichern eines Konfigurationsprofils erzeugt das Gerät automatisch eine Kopie auf dem externen Speicher, wenn der externe Speicher angeschlossen ist. In der Voreinstellung ist die Funktion eingeschaltet. Diese Funktion lässt sich wie folgt einschalten oder ausschalten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Grundeinstellungen > Externer Speicher***.

- ☐ Damit das Gerät beim Speichern automatisch eine Kopie im externen Speicher erzeugt, markieren Sie das Kontrollkästchen in Spalte ***Sichere Konfiguration beim Speichern***.
- ☐ Um die Funktion auszuschalten, heben Sie in Spalte ***Sichere Konfiguration beim Speichern*** die Markierung des Kontrollkästchens auf.
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`config envm config-save usb`	Einschalten der Funktion. Beim Speichern eines Konfigurationsprofils erzeugt das Gerät eine Kopie im externen Speicher. `usb` = Externer USB-Speicher

`no config envm config-save usb`	Ausschalten der Funktion. Das Gerät erzeugt keine Kopie im externen Speicher. `usb` = Externer USB-Speicher
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

4.2.4 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 Benutzername 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 aus dem externen Speicher laden

Wenn der externe Speicher angeschlossen ist, lädt das Gerät beim Neustart automatisch ein Konfigurationsprofil aus dem externen Speicher. Das Gerät bietet Ihnen die Möglichkeit, diese Einstellungen wieder in einem Konfigurationsprofil im permanenten Speicher zu speichern.

Enthält der externe Speicher das Konfigurationsprofil eines baugleichen Gerätes, haben Sie die Möglichkeit, auf diese Weise die Einstellungen von einem Gerät in ein anderes zu übertragen.

Führen Sie die folgenden Schritte aus:

☐ Vergewissern Sie sich, dass das Gerät beim Neustart ein Konfigurationsprofil aus dem externen Speicher lädt.

In der Voreinstellung ist die Funktion eingeschaltet. Wenn die Funktion ausgeschaltet ist, schalten Sie sie wie folgt wieder ein:

☐ Öffnen Sie den Dialog ***Grundeinstellungen > Externer Speicher***.
☐ Markieren Sie in Spalte ***Konfigurations-Priorität*** den Wert `first`.
☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`config envm load-priority usb first`	Einschalten der Funktion. Beim Neustart lädt das Gerät ein Konfigurationsprofil aus dem externen Speicher. `usb` = Externer USB-Speicher
`show config envm settings`	Zeigt die Einstellungen des externen Speichers (`envm`).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
```

`save`	Speichern Sie die Einstellungen in einem Konfigurationsprofil im permanenten Speicher (`NVM`) des Geräts.

Das Gerät bietet Ihnen im CLI die Möglichkeit, die Einstellungen aus dem externen Speicher direkt in den permanenten Speicher zu kopieren.

`show config profiles nvm`	Zeigt die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile.
`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy config envm profile config3 nvm`	Kopieren des Konfigurationsprofils `config3` aus dem externen Speicher (`envm`) in den permanenten Speicher (`nvm`).

4.3.3 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 Benutzername 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.
  - `Externer Speicher`
    Das Gerät importiert das Konfigurationsprofil vom externen Speicher.

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.

Um das Konfigurationsprofil vom externen Speicher zu importieren, führen Sie die folgenden Schritte aus:

- ☐ Wählen Sie im Rahmen ***Import profile from external memory***, Dropdown-Liste ***Profilname*** den Namen des zu importierenden Konfigurationsprofils.
  Voraussetzung ist, dass der externe Speicher ein exportiertes Konfigurationsprofil enthält.
- ☐ 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.
- ☐ Klicken Sie die Schaltfläche ***Ok***.

Das Gerät kopiert das Konfigurationsprofil in den permanenten Speicher (`NVM`) des Geräts.
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`	Wechsel in den Privileged-EXEC-Modus.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> running-config`	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.

Ist ein externer Speicher angeschlossen, löscht das Gerät auch die auf dem externen Speicher gespeicherten Konfigurationsprofile.

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`).
Ist ein externer Speicher angeschlossen, löscht das Gerät auch die auf dem externen Speicher gespeicherten Konfigurationsprofile.
Nach kurzer Zeit startet das Gerät neu und lädt die Werkseinstellungen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`clear factory`	Löscht die Konfigurationsprofile im flüchtigen Speicher und im permanenten Speicher. Ist ein externer Speicher angeschlossen, löscht das Gerät auch die auf dem externen Speicher gespeicherten Konfigurationsprofile. 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
- Software-Update vom externen Speicher
- 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 anzeigen:

☐ 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`	Wechsel in den Privileged-EXEC-Modus.
`show system info`	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***.
Die aktuell ausgeführte Geräte-Software kopiert das Gerät in den Backup-Bereich.
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`	Wechsel in den Privileged-EXEC-Modus.
`copy firmware remote tftp://10.0.1.159/product.bin system`	Übertragen der Datei `product.bin` vom TFTP-Server mit der IP-Adresse `10.0.1.159` auf das Gerät.

5.3 Software-Update vom externen Speicher

5.3.1 Manuell – durch den Administrator initiiert

Das Gerät bietet Ihnen die Möglichkeit, die Geräte-Software mit wenigen Mausklicks zu aktualisieren. Voraussetzung ist, dass sich die Image-Datei der Geräte-Software auf dem externen Speicher befindet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Grundeinstellungen > Software***.
- ☐ Markieren Sie in der Tabelle die Zeile, die den Namen der gewünschten Image-Datei auf dem externen Speicher zeigt.
- ☐ Rechtsklicken Sie, um das Kontextmenü anzuzeigen.
- ☐ Um den Update-Vorgang zu starten, klicken Sie im Kontextmenü den Eintrag ***Update***.

  Die aktuell ausgeführte Geräte-Software kopiert das Gerät in den Backup-Bereich.
  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.

5.3.2 Automatisch – durch das Gerät initiiert

Das Gerät aktualisiert beim Neustart die Geräte-Software automatisch, wenn sich folgende Dateien auf dem externen Speicher befinden:

- die Image-Datei der Geräte-Software
- eine Textdatei `startup.txt` mit dem Inhalt `autoUpdate=<Name_der_Image-Datei>.bin`

Voraussetzung ist, dass im Dialog ***Grundeinstellungen > Externer Speicher*** das Kontrollkästchen in Spalte ***Automatisches Software-Update*** markiert ist. Dies ist die Voreinstellung im Gerät.

Führen Sie die folgenden Schritte aus:

- ☐ Kopieren Sie die Image-Datei der neuen Geräte-Software in das Hauptverzeichnis des externen Speichers. Verwenden Sie ausschließlich eine für das Gerät bestimmte Image-Datei.
- ☐ Erzeugen Sie eine Textdatei mit dem Namen `startup.txt` im Hauptverzeichnis des externen Speichers.
- ☐ Öffnen Sie die Datei `startup.txt` im Texteditor und fügen Sie folgende Zeile ein:
  `autoUpdate=<Name_der_Image-Datei>.bin`
- ☐ Installieren Sie den externen Speicher im Gerät.
- ☐ Starten Sie das Gerät neu.
  Während des Boot-Vorgangs prüft das Gerät automatisch folgende Kriterien:
  – Ist ein externer Speicher angeschlossen?
  – Befindet sich im Hauptverzeichnis des externen Speichers eine Datei `startup.txt`?

– Existiert die Image-Datei, die in der Datei `startup.txt` angegeben ist?
– Ist die Software-Version der Image-Datei aktueller als die aktuell im Gerät ausgeführte Software?

Wenn die Kriterien erfüllt sind, startet das Gerät den Update-Vorgang.
Die aktuell ausgeführte Geräte-Software kopiert das Gerät in den Backup-Bereich.
Sobald der Update-Vorgang erfolgreich beendet ist, startet das Gerät selbständig neu und lädt die neue Software-Version.

Kontrollieren Sie das Ergebnis des Update-Vorgangs. Die Log-Datei im Dialog ***Diagnose > Bericht >*** System Log enthält eine der folgenden Meldungen:

- `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
  Software-Update erfolgreich beendet
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
  Software-Update abgebrochen
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
  Software-Update aufgrund falscher Image-Datei abgebrochen
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Software-Update abgebrochen, weil das Speichern der Image-Datei im Gerät missglückt ist.

5.4 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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`no shutdown`	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 zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`no auto-negotiate`	Ausschalten des Modus für die automatische Konfiguration.
`speed 10 full`	Portgeschwindigkeit 10 MBit/s, Vollduplex

6.3 Modulsteckplätze deaktivieren

Wenn Sie ein Modul an einen leeren Steckplatz eines modularen Gerätes anschließen, konfiguriert das Gerät das Modul mit den Voreinstellungen. Die Voreinstellungen ermöglichen den Zugriff auf das Netz. Um unbefugten Netzzugriff zu vermeiden, deaktivieren Sie nicht verwendete Steckplätze.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Grundeinstellungen > Module***.
- ☐ Um nicht verwendete Steckplätze zu deaktivieren, heben Sie die Markierung des Kontrollkästchens ***Aktiv*** auf.

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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`snmp community rw <community name>`	Community für Lese-/Schreibzugriffe festlegen.
`show snmp community`	Eingerichtete Communities anzeigen.
`save`	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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`no snmp access version v1`	Deaktivieren des Protokolls SNMPv1.
`no snmp access version v2`	Deaktivieren des Protokolls SNMPv2.
`show snmp access`	Einstellungen des SNMP-Servers anzeigen.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) 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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`no http server`	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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`https server`	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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`no telnet server`	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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ssh server`	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 zwischenzuspeichern, klicken Sie die Schaltfläche ☑ .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network hidiscovery mode read-only`	Der HiDiscovery-Software die Schreibrechte entziehen.
`no network hidiscovery operation`	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 zwischenzuspeichern, klicken Sie die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`show network management access global`	Zeigt, ob die IP-Zugriffsbeschränkung eingeschaltet oder ausgeschaltet ist.
`show network management access rules`	Eingerichtete Einträge anzeigen.
`no network management access operation`	IP-Zugriffsbeschränkung ausschalten.
`network management access add 2`	Eintrag für den Adressbereich des Firmennetzes erzeugen. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: `2`.
`network management access modify 2 ip 192.168.1.0`	IP-Adresse des Firmennetzes festlegen.
`network management access modify 2 mask 24`	Netzmaske des Firmennetzes festlegen.
`network management access modify 2 ssh disable`	SSH für den Adressbereich des Firmennetzes deaktivieren. Schritt für sämtliche ungewünschten Protokolle wiederholen.
`network management access add 3`	Eintrag für den Adressbereich des Mobilfunknetzes erzeugen. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: `3`.
`network management access modify 3 ip 109.237.176.0`	IP-Adresse des Mobilfunknetzes festlegen.
`network management access modify 3 mask 24`	Netzmaske des Mobilfunknetzes festlegen.
`network management access modify 3 snmp disable`	SNMP für den Adressbereich des Mobilfunknetzes deaktivieren. Schritt für sämtliche ungewünschten Protokolle wiederholen.
`no network management access status 1`	Voreingestellten Eintrag deaktivieren. Dieser Eintrag ermöglicht den Zugriff auf das Gerät von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle.
`network management access status 2`	Eintrag für den Adressbereich des Firmennetzes aktivieren.
`network management access status 3`	Eintrag für den Adressbereich des Mobilfunknetzes aktivieren.
`show network management access rules`	Eingerichtete Einträge anzeigen.
`network management access operation`	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 zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ssh timeout <0..160>`	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 zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`telnet timeout <0..160>`	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`	Wechsel in den Privileged-EXEC-Modus.
`cli serial-timeout <0..160>`	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`	Wechsel in den Privileged-EXEC-Modus.
`network management access web timeout <0..160>`	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)
- Verweigern des Zugriffes auf Geräte auf der Grundlage ihrer IP- oder MAC-Adresse (Zugriffkontrollliste)

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.

Die Datenpakete durchlaufen die Filter-Funktionen des Gerätes in folgender Reihenfolge:
- DoS … wenn `permit` oder `accept`, dann weiter zur nächsten Regel
- ACL … wenn `permit` oder `accept`, dann weiter zur nächsten Regel

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.

8.2 ACL

In diesem Menü haben Sie die Möglichkeit, die Einstellungen für die Access-Control-Listen (Zugriffssteuerungslisten, ACL) vorzunehmen.

Das Gerät verwendet Access-Control-Listen für die Filterung von Datenpaketen, die an einzelnen oder mehreren Ports oder an VLANs eingehen. Hierfür erzeugen Sie Regeln in der jeweiligen ACL, anhand derer das Gerät eine Filterung vornimmt. Wenn eine solche Regel auf ein Paket zutrifft, wendet das Gerät die in der Regel definierten Aktionen auf das Paket an. Hierbei stehen Ihnen folgende Aktionen zur Verfügung:

- zulassen (`permit`)
- verwerfen (`deny`)
- umleiten an einen bestimmten Port (siehe Feld ***Redirection-Port***)
- spiegeln (siehe Feld ***Mirror-Port***)

Sie können empfangene Datenpakete nach folgenden Kriterien filtern:

- Quell- oder Zieladresse eines Pakets (MAC)
- Quell- oder Zieladresse eines Datenpakets (IPv4)
- Quell- oder Zielport eines Datenpakets (IPv4)

Aus der Zuweisung von IP-ACLs und MAC-ACLs zu den Ports und VLANs ergeben sich folgende unterschiedliche ACL-Typen:

- IP-ACLs für VLANs
- IP-ACLs für Ports
- MAC-ACLs für VLANs
- MAC-ACLs für Ports

Wenn Sie einem Port sowohl eine IP-ACL als auch eine MAC-ACL zuweisen, verwendet das Gerät bei der Filterung die IP-ACL zuerst. Um den Datenstrom unter Verwendung der MAC-ACL zu filtern, erzeugen Sie am Ende der IP-ACL eine `permit all`-Regel („alle zulassen“).

Innerhalb eines ACL-Typs arbeitet das Gerät die Regeln der Reihe nach ab, wobei der Index der jeweiligen Regel die entsprechende Reihenfolge bestimmt. Sie können also die Priorität einer Regel über die Index- oder Folgenummer festlegen, wenn Sie eine ACL einem Port oder einem VLAN zuweisen. Grundsätzlich gilt: je niedriger die Folgenummer, desto höher die Priorität. Beim Abarbeiten der Regeln wendet das Gerät die Regel mit der höheren Priorität zuerst an.

Wenn mehrere ACL-Typen Regeln enthalten, die auf ein Datenpaket zutreffen, entscheidet die Priorität des ACL-Typs darüber, welche Regel das Gerät zuerst anwendet. Bitte beachten Sie, dass die Priorität eines ACL-Typs unabhängig ist von der Index- oder Folgenummer einer Regel. Grundsätzlich gilt, dass IP-ACLs eine höhere Priorität haben als MAC-ACLs. Das Gerät bevorzugt also IP-ACLs gegenüber MAC-ACLs.

Sie können bis zu 128 MAC-ACLs und bis zu 128 IP-ACLs erzeugen. Jede ACL kann bis zu 239 Regeln beinhalten, wobei das Gerät unabhängig vom ACL-Typ eine maximale Anzahl von 956 Regeln erlaubt. Dies entspricht 4 vollständig ausgefüllten ACLs mit je 239 Regeln.

Unabhängig vom ACL-Typ können Sie einem einzelnen Port maximal 239 Regeln zuweisen.

Sie können einem einzelnen Port maximal 128 MAC-ACLs und 128 IP-ACLs gleichzeitig zuweisen.

Unabhängig vom ACL-Typ können Sie einem einzelnen VLAN maximal 176 Regeln zuweisen.

Anmerkung: Eine einzelne ACL können Sie beliebig vielen Port oder VLANs zuweisen.

Wenn Sie einem Port oder VLAN eine oder mehrere ACLs zuweisen, verarbeitet das Gerät die ACLs entsprechend ihrer Priorität, wenn ein Interface Datenpakete empfängt. Wenn keine der in den ACLs enthaltenen Regeln einem empfangenen Datenpaket entspricht, wird die implizite `deny`-Regel („Ablehnen“) angewendet. Infolgedessen verwirft das Paket empfangene Datenpakete.

Beachten Sie, dass das Gerät die implizite `deny`-Regel direkt implementiert.

Das Menü ***ACL*** enthält die folgenden Dialoge:
- ***ACL IPv4-Regel***
- ***ACL MAC-Regel***
- ***ACL Zuweisung***

In diesen Dialogen können Sie die Regeln für die unterschiedlichen ACL-Typen benennen, konfigurieren und mit den gewünschten Prioritäten versehen. Zudem nehmen Sie hier die Zuweisung der Regeln zu bestimmten Ports oder VLANs vor.

8.2.1 Erzeugen und Bearbeiten von IPv4-Regeln

Beim Filtern von IPv4-Datenpaketen bietet Ihnen das Gerät die folgenden Funktionen:
- Erzeugen von neuen Gruppen und Regeln
- Hinzufügen von neuen Regeln zu vorhandenen Gruppen
- Bearbeiten einer vorhandenen Regel
- Aktivieren und Deaktivieren von Gruppen und Regeln
- Löschen von vorhandenen Gruppen und Regeln
- Ändern der Reihenfolge der vorhandenen Regeln

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Netzsicherheit > ACL > IPv4-Regel***.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster ***Erzeugen***.
- ☐ Um eine Gruppe zu erzeugen, legen Sie im Feld ***Gruppenname*** einen aussagekräftigen Namen fest. In einer Gruppe können Sie mehrere Regeln zusammenfassen.
- ☐ Um die Regel einer vorhandenen Gruppe hinzuzufügen, wählen Sie im Feld ***Gruppenname*** den Namen der Gruppe aus.
- ☐ Legen Sie im Feld ***Index*** einen Wert im Bereich `1..239` fest.
  Dieser Wert bestimmt die Priorität der Regel.
- ☐ Klicken Sie die Schaltfläche ***Ok***.
  Das Gerät fügt die Regel der Tabelle hinzu.
  Gruppe und Regel sind sofort aktiv.
  Um Gruppe oder Regel zu deaktivieren, heben Sie in Spalte ***Aktiv*** die Markierung des Kontrollkästchens auf.
  Um eine Regel zu entfernen, markieren Sie den betreffenden Tabelleneintrag und klicken die Schaltfläche .
- ☐ Bearbeiten Sie die Parameter der Regel in der Tabelle.
  Um einen Wert zu ändern, doppelklicken Sie in das betreffende Feld.

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

Anmerkung: Das Gerät bietet Ihnen die Möglichkeit, in den Parametern ***Quell-IP-Adresse*** und ***Ziel-IP-Adresse*** Platzhalter zu verwenden. Wenn Sie beispielsweise `192.168.?.?` einfügen, lässt das Gerät Adressen zu, deren erste beide Oktetts mit `192.168` beginnen.

Anmerkung: Voraussetzung zum Ändern der Werte in Spalte ***Quell-TCP/UDP-Port*** und ***Ziel-TCP/UDP-Port*** ist, dass Sie in Spalte ***Protokoll*** den Wert `tcp` oder udp festlegen.

Anmerkung: Voraussetzung zum Ändern des Werts in Spalte ***Redirection-Port*** und ***Mirror-Port*** ist, dass Sie in Spalte ***Aktion*** den Wert `permit` festlegen.

8.2.2 Erzeugen und Konfigurieren einer IP-ACL im CLI

In dem folgenden Beispiel konfigurieren Sie ACLs dahingehend, dass sie Kommunikation von Rechnern B und C zu Rechner A über IP (TCP, UDP usw.) blockieren.

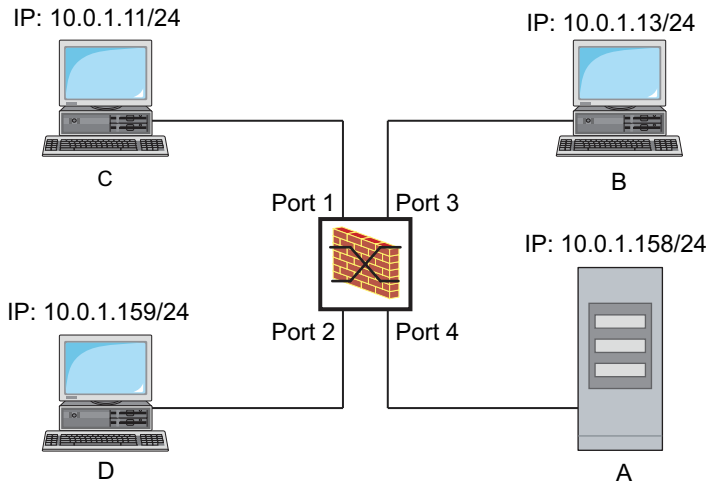


Abb. 17: Beispiel einer IP-ACL

Führen Sie die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip acl add 1 filter`	Fügt eine IP-ACL mit ID `1` und dem Namen `filter` ein.
`ip acl rule add 1 1 deny src 10.0.1.11 0.0.0.0 dst 10.0.1.158 0.0.0.0`	Fügt eine Regel an Position `1` in der IP-ACL mit ID `1` ein, die IP-Datenpakete von `10.0.1.11` nach `10.0.1.158` verbietet.
`ip acl rule add 1 2 permit src any any dst any any`	Fügt eine Regel an Position `2` in der IP-ACL mit ID `1` ein, die IP-Datenpakete erlaubt.
`show acl ip rules 1`	Zeigt die Regeln für die IP-ACL mit ID `1` an.
`ip acl add 2 filter2`	Fügt eine IP-ACL mit ID `2` und dem Namen `filter2` ein.
`ip acl rule add 2 1 deny src 10.0.1.13 0.0.0.0 dst 10.0.1.158 0.0.0.0`	Fügt eine Regel an Position `1` in der IP-ACL mit ID `2` ein, die IP-Datenpakete von `10.0.1.13` nach `10.0.1.158` verbietet.
`ip acl rule add 2 2 permit src any any dst any any`	Fügt eine Regel an Position `2` in der IP-ACL mit ID `2` ein, die IP-Datenpakete erlaubt.
`show acl ip rules 2`	Zeigt die Regeln für die IP-ACL mit ID `2` an.

`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`acl ip assign 1 in 1`	Weist die IP-ACL mit ID `1` an Interface `in` mit Priorität `1/1` (höchste Priorität) für empfangene Datenpakete (`1`) zu.
`exit`	Verlässt den Interface-Modus.
`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/3`.
`acl ip assign 2 in 1`	Weist die IP-ACL mit ID `2` an Interface `in` mit Priorität `1/3` (höchste Priorität) für empfangene Datenpakete (`1`) zu.
`exit`	Verlässt den Interface-Modus.
`show acl ip assignment 1`	Zeigt die Zuweisung der IP-ACL mit ID `1`.
`show acl ip assignment 2`	Zeigt die Zuweisung der IP-ACL mit ID `2`.

8.2.3 Erzeugen und Bearbeiten von MAC-Regeln

Beim Filtern von MAC-Datenpaketen bietet Ihnen das Gerät die folgenden Funktionen:
- Erzeugen von neuen Gruppen und Regeln
- Hinzufügen von neuen Regeln zu vorhandenen Gruppen
- Bearbeiten einer vorhandenen Regel
- Aktivieren und Deaktivieren von Gruppen und Regeln
- Löschen von vorhandenen Gruppen und Regeln
- Ändern der Reihenfolge der vorhandenen Regeln

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Netzsicherheit > ACL > MAC-Regel***.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster ***Erzeugen***.
- ☐ Um eine Gruppe zu erzeugen, legen Sie im Feld ***Gruppenname*** einen aussagekräftigen Namen fest. In einer Gruppe können Sie mehrere Regeln zusammenfassen.
- ☐ Um die Regel einer vorhandenen Gruppe hinzuzufügen, wählen Sie im Feld ***Gruppenname*** den Namen der Gruppe aus.
- ☐ Legen Sie im Feld ***Index*** einen Wert im Bereich `1..239` fest.
  Dieser Wert bestimmt die Priorität der Regel.
- ☐ Klicken Sie die Schaltfläche ***Ok***.
  Das Gerät fügt die Regel der Tabelle hinzu.
  Gruppe und Regel sind sofort aktiv.
  Um Gruppe oder Regel zu deaktivieren, heben Sie in Spalte ***Aktiv*** die Markierung des Kontrollkästchens auf.
  Um eine Regel zu entfernen, markieren Sie den betreffenden Tabelleneintrag und klicken die Schaltfläche .
- ☐ Bearbeiten Sie die Parameter der Regel in der Tabelle.
  Um einen Wert zu ändern, doppelklicken Sie in das betreffende Feld.
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Anmerkung: In den Feldern ***Quell-MAC-Adresse*** und ***Ziel-MAC-Adresse*** können Sie Platzhalter in der Form `FF:??:??:??:??:??` oder `??:??:??:??:00:01` verwenden. Verwenden Sie hier Großbuchstaben.

8.2.4 Erzeugen und Konfigurieren einer MAC-ACL im CLI

Das Beispiel sieht vor, dass AppleTalk und IPX aus dem gesamten Netz gefiltert werden.

Führen Sie die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mac acl add 1 macfilter`	Fügt eine MAC-ACL mit ID `1` und dem Namen `macfilter` ein.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	Fügt eine Regel an Position `1` in der MAC-ACL mit ID `1` ein, die Pakete mit Ethertype `0x809B (AppleTalk)` abweist.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	Fügt eine Regel an Position `2` in der MAC-ACL mit ID `1` ein, die Pakete mit Ethertype `0x8137 (IPX alt)` abweist.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	Fügt eine Regel an Position `3` in der MAC-ACL mit ID `1` ein, die Pakete mit Ethertype `0x8138 (IPX)` abweist.
`mac acl rule add 1 4 permit src any any dst any any`	Fügt eine Regel an Position `4` in der MAC-ACL mit ID `1` ein, die Pakete weiterleitet.
`show acl mac rules 1`	Zeigt die Regeln der MAC-ACL mit ID `1`.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	Wechsel in den Interface-Konfigurationsmodus der Interfaces `1/1` bis `1/6`.
`acl mac assign 1 in 1`	Weist die MAC-ACL mit ID `1` den auf den Interfaces `1/1` bis `1/6` empfangenen Datenpaketen (`in`) zu.
`exit`	Verlässt den Interface-Modus.
`show acl mac assignment 1`	Zeigt die Zuweisung von Interfaces/VLANS der MAC-ACL mit ID `1` an.

8.2.5 Zuweisen von ACL-Gruppen zu Ports oder VLANs

Für die Zuweisung von Gruppenregeln zu Ports oder VLANs bietet Ihnen das Gerät die folgenden Funktionen:

- Zuweisen von ACL-Gruppen zu Ports oder VLANs
- Festlegen der Priorität der Regel
- Zuweisen der ACL über den Gruppennamen

Führen Sie die folgenden Schritte aus:

☐ Öffnen Sie den Dialog ***Netzsicherheit > ACL > Zuweisung***.

☐ Klicken Sie die Schaltfläche .

Der Dialog zeigt das Fenster ***Erzeugen***.

- ☐ Legen Sie im Feld ***Port/VLAN*** den gewünschten Port oder das gewünschte VLAN fest.
- ☐ Legen Sie im Feld ***Priorität*** die Priorität der Zuweisung fest.
- ☐ Legen Sie im Feld ***Richtung*** fest, auf welche Datenpakete das Gerät die Regel anwendet.
- ☐ Legen Sie im Feld ***Gruppenname*** fest, welche Regel das Gerät dem Port oder dem VLAN zuweist.

☐ Klicken Sie die Schaltfläche ***Ok***.

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche  .

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.

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.

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 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`.

▶ 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 zwischenzuspeichern, klicken Sie die Schaltfläche ☑ .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	Einstellen der Systemzeit des Gerätes.
`clock timezone offset <-780..840>`	Eingabe der Zeitdifferenz zwischen der lokalen Zeit und der empfangenen UTC-Zeit in Minuten.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) 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 eine 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 zwischenzuspeichern, klicken Sie die Schaltfläche ☑ .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`clock summer-time mode <disable|recurring|eu|usa>`	Konfigurieren der automatischen Sommerzeitumstellung: einschalten, ausschalten oder mit Profil aktivieren.
`clock summer-time recurring start`	Eingabe des Startzeitpunkts für die Umschaltung.
`clock summer-time recurring end`	Eingabe des Endzeitpunkts für die Umschaltung.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) 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.

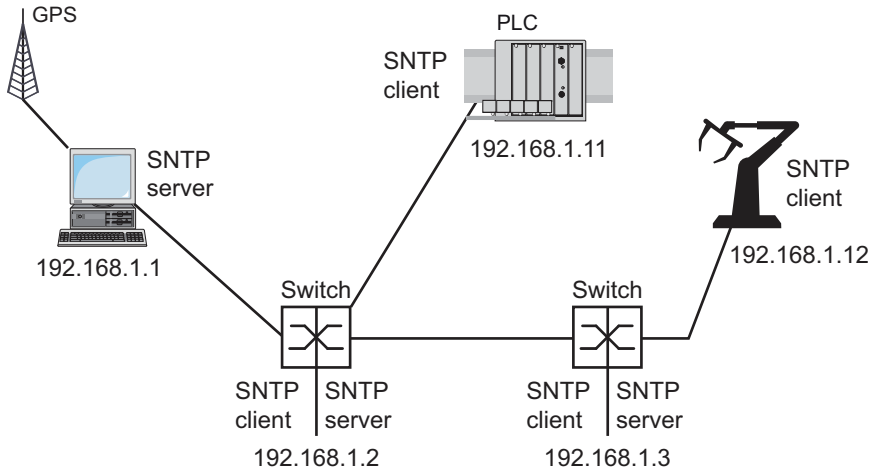


Abb. 18: Beispiel SNTP-Kaskade

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: ***Modus***	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 zwischenzuspeichern, 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

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 ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mac-filter <MAC address> <VLAN ID>`	Erzeugen des MAC-Adressfilters, bestehend aus MAC-Adresse und VLAN-ID.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`mac-filter <MAC address> <VLAN ID>`	Weist dem Port einen bereits erzeugten MAC-Adressfilter zu.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

☐ 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 ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`no mac-filter <MAC address> <VLAN ID>`	Hebt auf dem Port die Zuweisung des MAC-Adressfilters auf.
`exit`	Wechsel in den Konfigurationsmodus.
`no mac-filter <MAC address> <VLAN ID>`	Löschen des MAC-Adressfilters, bestehend aus MAC-Adresse und VLAN-ID.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

☐ 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***.

`clear mac-addr-table`	Löschen der gelernten MAC-Adressen aus der MAC-Adresstabelle (FDB).

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 angeschlossenen 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 gewonnen MAC-Adressen der Multicast-Empfänger als erkannte Multicast-Adressen in seiner MAC-Adresstabelle (FDB). Außerdem kenzeichnet 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 unbekannten 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`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`igmp-snooping vlan-id 1 forward-all 1/1`	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 zwischenzuspeichern, 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“).

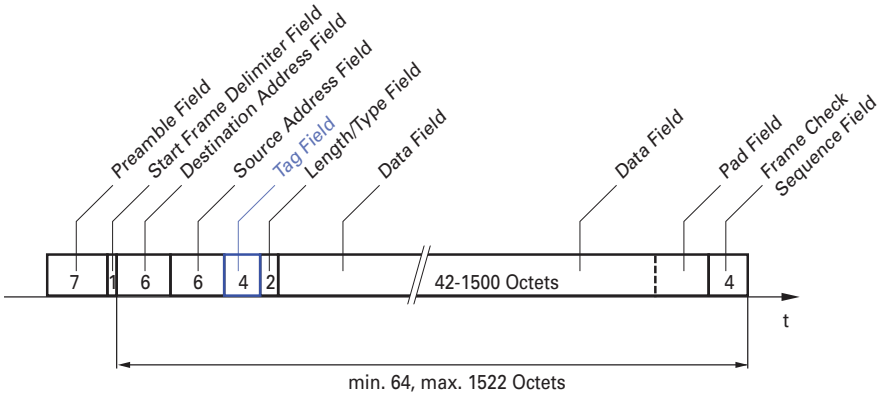


Abb. 19: Ethernet-Datenpaket mit Tag

Das Gerät wertet bei Datenpaketen mit VLAN-Tags folgende Informationen aus:

- Prioritätsinformation
- VLAN-Tag, sofern VLANs eingerichtet sind

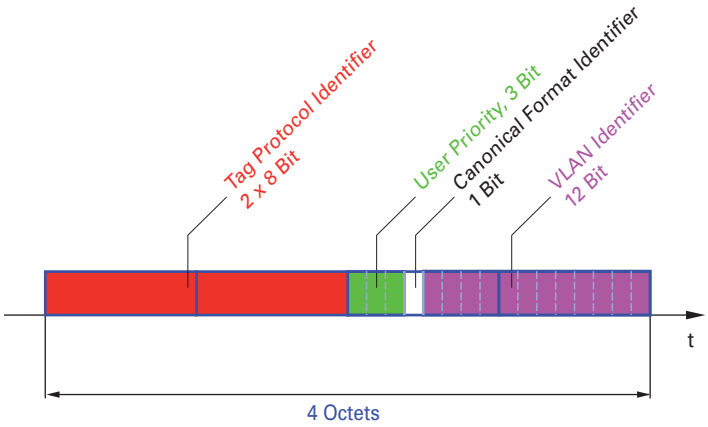


Abb. 20: Aufbau des VLAN-Tag

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 Dienstgüten in IP-Netzen vorgesehen. Schon damals machte man sich aufgrund der geringen zur Verfügung stehenden Bandbreiten und der unzuverlässigen Verbindungswege Gedanken um eine differenzierte Behandlung von IP-Paketen. Durch die kontinuierliche Steigerung der zur Verfügung stehenden Bandbreiten bestand keine Notwendigkeit, das ToS-Feld zu nutzen.

Erst die Echtzeitanforderungen an heutige Netze rücken das ToS-Feld in den Blickpunkt. Eine Markierung im ToS-Byte des IP-Headers ermöglicht eine Unterscheidung unterschiedlicher Dienstgüten. In der Praxis hat sich die Nutzung dieses Feldes jedoch nicht durchgesetzt.

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Must be zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

Tab. 11: 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 höherpriorem 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                                  Wechsel in den Privileged-EXEC-Modus.
configure                               Wechsel in den Konfigurationsmodus.
cos-queue weighted 0                    Weighted Fair Queuing für die Verkehrsklasse 0 einschalten.
cos-queue min-bandwidth: 0 5            Gewichtung 5 % der Verkehrsklasse 0 zuweisen.
cos-queue weighted 1                    Weighted Fair Queuing für die Verkehrsklasse 1 einschalten.
cos-queue min-bandwidth: 1 20           Gewichtung 20 % der Verkehrsklasse 1 zuweisen.
cos-queue weighted 2                    Weighted Fair Queuing für die Verkehrsklasse 2 einschalten.
cos-queue min-bandwidth: 2 30           Gewichtung 30 % der Verkehrsklasse 2 zuweisen.
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
```

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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`vlan priority 3`	Interface `1/1` die Port-Priorität `3` zuweisen.
`exit`	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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`classofservice dot1p-mapping 0 2`	Der VLAN-Priorität `0` die Verkehrsklasse `2` zuweisen.
`classofservice dot1p-mapping 1 2`	Der VLAN-Priorität `1` die Verkehrsklasse `2` zuweisen.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show classofservice dot1p-mapping`	Zeigt die Zuordnung an.

Empfangenen Datenpaketen die Port-Priorität zuweisen

Führen Sie die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`classofservice trust untrusted`	Dem Interface den Modus `untrusted` zuweisen.
`classofservice dot1p-mapping 0 2`	Der VLAN-Priorität `0` die Verkehrsklasse `2` zuweisen.
`classofservice dot1p-mapping 1 2`	Der VLAN-Priorität `1` die Verkehrsklasse `2` zuweisen.
`vlan priority 1`	Für die Port-Priorität den Wert `1` festlegen.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show classofservice trust`	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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`classofservice ip-dscp-mapping cs1 1`	Dem DSCP `CS1` die Verkehrsklasse `1` zuweisen.
`show classofservice ip-dscp-mapping`	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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`classofservice trust ip-dscp`	Den Modus `trust ip-dscp` global zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`show classofservice trust`	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`	Wechsel in den Privileged-EXEC-Modus.
`network management priority dot1p 7`	Management-Paketen die VLAN-Priorität `7` zuweisen. Das Gerät sendet Management-Pakete mit höchster Priorität.
`show network parms`	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`	Wechsel in den Privileged-EXEC-Modus.
`network management priority ip-dscp 56`	Management-Paketen den DSCP-Wert `56` zuweisen. Das Gerät sendet Management-Pakete mit höchster Priorität.
`show network parms`	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.

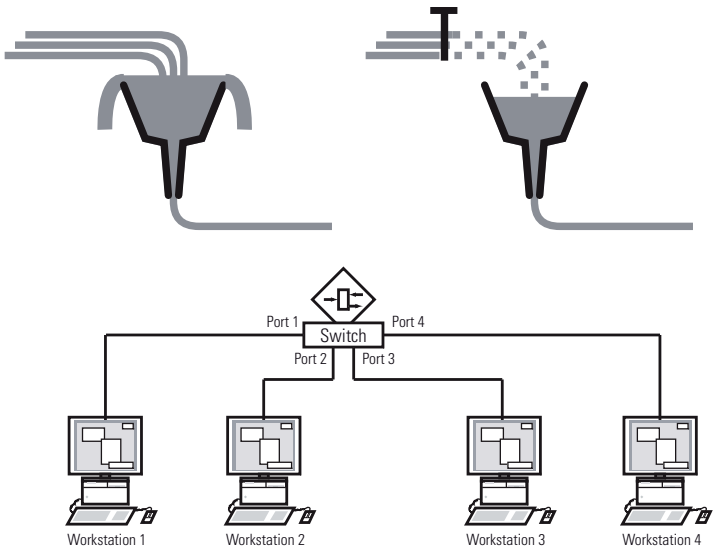


Abb. 21: Beispiel für Flusskontrolle

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 zwischenzuspeichern, 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 unbekannten (nicht gelernten) Zieladressen ausschließlich innerhalb des virtuellen LANs vermitteln. Der Rest des Datennetzes übermittelt 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.

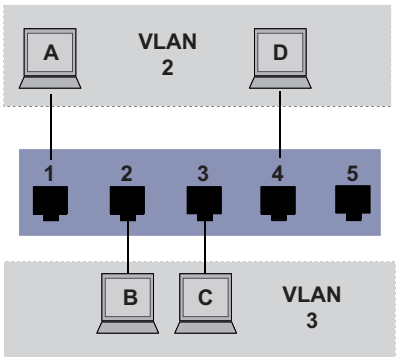


Abb. 22: Beispiel für ein einfaches Port-basiertes VLAN

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 Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Tab. 12: Ingress-Tabelle

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Tab. 13: 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                                  Wechsel in den Privileged-EXEC-Modus.
vlan database                           Wechsel in den VLAN-Konfigurationsmodus.
vlan add 2                              Erzeugt ein neues VLAN mit VLAN-ID 2.
name 2 VLAN2                            Dem VLAN 2 den Namen VLAN2 zuweisen.
vlan add 3                              Erzeugt ein neues VLAN mit VLAN-ID 3.
name 3 VLAN3                            Dem VLAN 3 den Namen VLAN3 zuweisen.
name 1 VLAN1                            Dem VLAN 1 den Namen VLAN1 zuweisen.
exit                                    Wechsel in den Privileged-EXEC-Modus.
show vlan brief                         Zeigt die aktuelle VLAN Konfiguration an.
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
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.
  Änderungen durch die ***GVRP***-Funktion sind gesperrt.
- `-` = Der Port ist kein Mitglied in diesem VLAN.
  Änderungen durch die ***GVRP***-Funktion sind erlaubt.

Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie den Wert `U` 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: `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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`vlan participation include 2`	Port `1/1` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port `1/1` die Port-VLAN-ID `2` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`vlan participation include 3`	Port `1/2` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port `1/2` die Port-VLAN-ID `3` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/3`.
`vlan participation include 3`	Port `1/3` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port `1/3` die Port-VLAN-ID `3` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/4`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/4`.
`vlan participation include 2`	Port `1/4` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port `1/4` die Port-VLAN-ID `2` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show vlan id 3`	Details zu VLAN `3` anzeigen.

```
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
```

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).

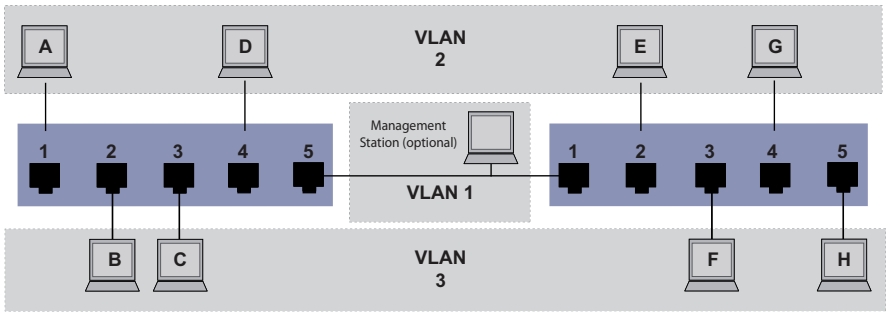


Abb. 23: Beispiel für eine komplexere VLAN-Konfiguration

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 Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Tab. 14: Ingress-Tabelle Gerät links

Endgerät	Port	Port VLAN Identifer (PVID)
Uplink	1	1
E	2	2
F	3	3

Tab. 15: Ingress-Tabelle Gerät rechts

Endgerät	Port	Port VLAN Identifer (PVID)
G	4	2
H	5	3

Tab. 15: Ingress-Tabelle Gerät rechts

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tab. 16: Egress-Tabelle Gerät links

VLAN-ID	Port				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Tab. 17: 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                                  Wechsel in den Privileged-EXEC-Modus.
vlan database                           Wechsel in den VLAN-Konfigurationsmodus.
vlan add 2                              Erzeugt ein neues VLAN mit VLAN-ID 2.
name 2 VLAN2                            Dem VLAN 2 den Namen VLAN2 zuweisen.
vlan add 3                              Erzeugt ein neues VLAN mit VLAN-ID 3.
name 3 VLAN3                            Dem VLAN 3 den Namen VLAN3 zuweisen.
name 1 VLAN1                            Dem VLAN 1 den Namen VLAN1 zuweisen.
exit                                    Wechsel in den Privileged-EXEC-Modus.
show vlan brief                         Zeigt die aktuelle VLAN Konfiguration an.
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
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.
  Änderungen durch die ***GVRP***-Funktion sind gesperrt.
- `-` = Der Port ist kein Mitglied in diesem VLAN.
  Änderungen durch die ***GVRP***-Funktion sind gesperrt.

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                                  Wechsel in den Privileged-EXEC-Modus.
configure                               Wechsel in den Konfigurationsmodus.
interface 1/1                           Wechsel in den Interface-Konfigurationsmodus von Interface 1/
                                        1.
vlan participation include 1            Port 1/1 wird Mitglied des VLANs 1 und vermittelt die
                                        Datenpakete ohne VLAN-Tag.
vlan participation include 2            Port 1/1 wird Mitglied des VLANs 2 und vermittelt die
                                        Datenpakete ohne VLAN-Tag.
```

`vlan tagging 2 enable`	Port `1/1` wird Mitglied des VLANs `2` und vermittelt die Datenpakete mit VLAN-Tag.
`vlan participation include 3`	Port `1/1` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan tagging 3 enable`	Port `1/1` wird Mitglied des VLANs `3` und vermittelt die Datenpakete mit VLAN-Tag.
`vlan pvid 1`	Port-VLAN-ID `1` dem Port `1/1` zuweisen.
`vlan ingressfilter`	Aktivieren von Ingress Filtering auf Port `1/1`.
`vlan acceptframe vlanonly`	Port `1/1` überträgt ausschließlich Pakete mit VLAN Tag.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`vlan participation include 2`	Port `1/2` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port-VLAN-ID `2` dem Port `1/2` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/3`.
`vlan participation include 3`	Port `1/3` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port-VLAN-ID `3` dem Port `1/3` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/4`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/4`.
`vlan participation include 2`	Port `1/4` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port-VLAN-ID `2` dem Port `1/4` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/5`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/5`.
`vlan participation include 3`	Port `1/5` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port-VLAN-ID `3` dem Port `1/5` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show vlan id 3`	Details zu VLAN `3` anzeigen.

```
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time..........0 days, 00:07:47 (System Uptime)
VLAN Routing................disabled

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 / Unauthentifiziertes VLAN

Die Gast-VLAN-Funktion ermöglicht einem Gerät die Bereitstellung einer Port-basierten Netzzugriffssteuerung (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 ***Netzsicherheit > 802.1X Port-Authentifizierung > Global***.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen ***Funktion*** das Optionsfeld .
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

☐ Öffnen Sie den Dialog ***Netzsicherheit > 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`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`vlan add 10`	Erzeugt VLAN `10`.
`vlan add 20`	Erzeugt VLAN `20`.
`name 10 Guest`	Benennt VLAN `10` um in `Guest`.
`name 20 Unauth`	Benennt VLAN `20` um in `Unauth`.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dot1x system-auth-control enable`	Schalten Sie die Funktion 802.1X global ein.
`dot1x port-control auto`	Schaltet die Port-Kontrolle auf Port `1/4` ein.
`interface 1/4`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/4`.
`dot1x guest-vlan 10`	Weist Port `1/4` das Gast-VLAN zu.
`dot1x unauthenticated-vlan 20`	Weist Port `1/4` das nicht autorisierte VLAN zu.
`exit`	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 Voice-VLAN erzeugen

Verwenden Sie die Voice-VLAN-Funktion, um den Sprach- und Datenverkehr an einem Port nach VLAN und/oder Priorität zu trennen. Ein wesentlicher Nutzen bei der Verwendung eines Voice-VLANs liegt darin, in Zeiten mit erhöhtem Datenverkehrsaufkommen die Sprachqualität bei einem IP-Telefon sicherzustellen.

Das Gerät verwendet die Quell-MAC-Adresse zur Identifizierung und Priorisierung des Sprachdatenstroms. Durch die Verwendung einer MAC-Adresse zur Geräte-Identifizierung verhindert das Gerät, dass sich ein bösartiger Client mit demselben Port verbindet und dadurch eine Verschlechterung des Sprachverkehrs verursacht.

Ein weiterer Nutzen der Voice-VLAN-Funktion liegt darin, dass das VoIP-Telefon durch die Verwendung von LLDP-Med eine VLAN-Kennung oder Prioritätsinformationen erhält. Infolgedessen sendet das Telefon die Sprachdaten entweder mit Markierung, mit Prioritätsmarkierung oder ohne Markierung. Dieses hängt von der Konfiguration des Voice-VLAN-Interfaces ab.

Nachstehend finden Sie eine Auflistung der möglichen Modi für das Voice-VLAN-Interface. Die ersten 3 Methoden trennen Sprach- und Datenverkehr und versehen beide mit einer Priorisierung. Die Trennung des Verkehrs führt zu einer besseren Qualität des Sprachverkehrs in Zeiten erhöhten Verkehrsaufkommens.

- Wenn Sie bei dem Port den Modus `vlan` konfigurieren, hat das Gerät die Möglichkeit, die von einem VoIP-Telefon kommenden Sprachdaten mit der benutzerdefinierten Voice-VLAN-ID zu markieren. Das Gerät weist reguläre Daten dann der voreingestellten Port-VLAN-ID zu.
- Wenn Sie bei dem Port den Modus `dot1p-priority` konfigurieren, hat das Gerät die Möglichkeit, die von einem VoIP-Telefon kommenden Daten mit VLAN 0 und der benutzerdefinierten Priorität zu markieren. Das Gerät weist regulären Daten dann die Standardpriorität des Ports zu.
- Sie konfigurieren sowohl die Voice-VLAN-ID wie auch die Priorität auf den Modus `vlan/dot1p-priority`. In diesem Modus sendet das VoIP-Telefon Sprachdaten mit der benutzerdefinierten Voice-VLAN-ID und den benutzerdefinierten Prioritätsinformationen. Das Gerät weist regulären Daten dann die Standard-PVID und die Standardpriorität des Ports zu.
- Wenn Sie das Telefon mit dem Wert `untagged` konfigurieren, sendet dieses unmarkierte Pakete.
- Wenn Sie das Telefon mit dem Wert `none` konfigurieren, verwendet dieses seine eigene Konfiguration zum Senden von Sprachverkehr.

11.5 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 (eineindeutigen) Weg vom Absender zum Empfänger gelangen. Die folgenden Netz-Topologien unterstützen diese Voraussetzung:

- Linien-Topologie
- Stern-Topologie
- Baum-Topologie

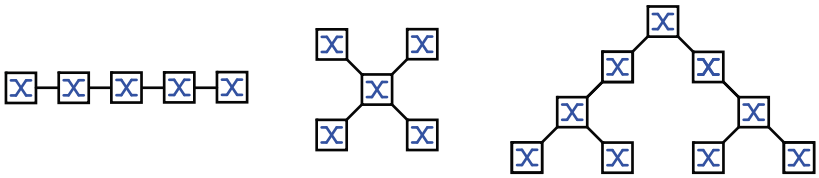


Abb. 24: Netz mit Linien-, Stern- und Baum-Topologie

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.

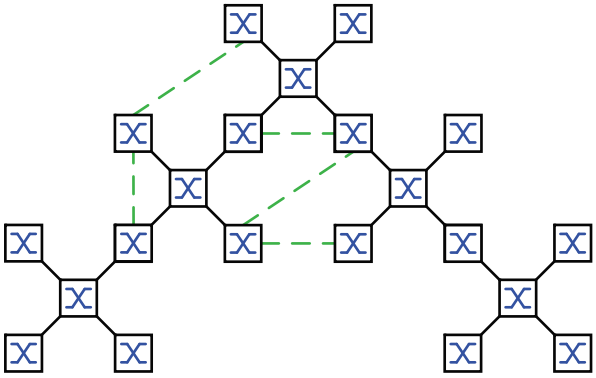


Abb. 25: Maschen-Topologie: Baum-Topologie mit physikalischen Schleifen

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.

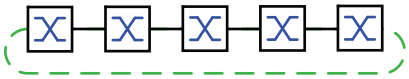


Abb. 26: Ring-Topologie: Linien-Topologie mit verbundenen Enden

Für den Betrieb in dieser Netz-Topologie stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:

- Media Redundancy Protocol (MRP)
- 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.
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 Dienstanbietern oder Unternehmen.

Tab. 18: 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	✓	✓	✓	✓						

Tab. 19: Redundanzprotokolle im Überblick

Symbol	Bedeutung
✓	Kombinierbar
1)	Eine redundante Kopplung zwischen diesen Netztopologien führt möglicherweise zu Datenvervielfachungen.
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.

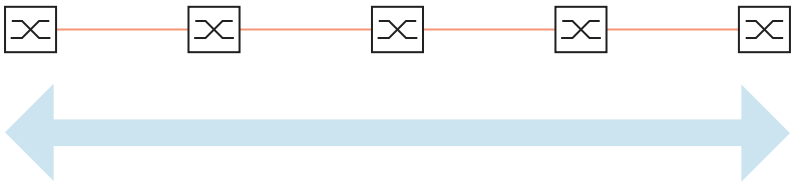


Abb. 27: Linienstruktur

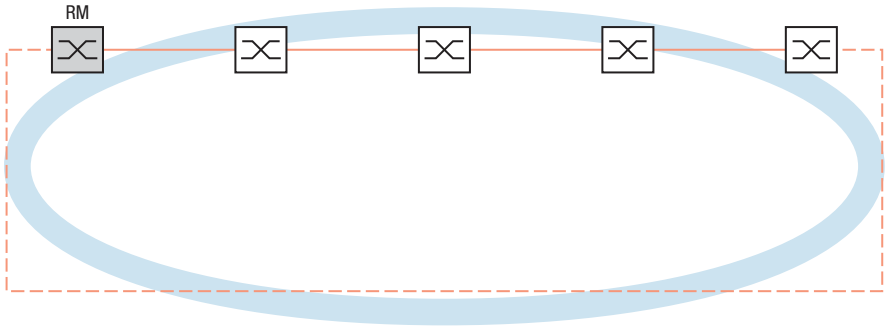


Abb. 28: Redundante Ringstruktur
RM = Ring-Manager
—— Hauptleitung
- - - redundante Leitung

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

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.

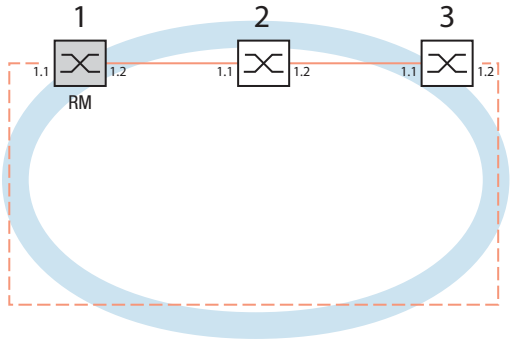


Abb. 29: Beispiel eines MRP-Rings
RM = Ring-Manager
—— Hauptleitung
- - - redundante Leitung

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. 20: 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.

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“) `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

`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 fixed-backup enable`	Aktivieren der ***Fixed backup***-Funktion auf dem sekundären 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 `U` 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 `T` (Tagged) fest.

`mrp domain modify vlan <0..4042>`	Weist die VLAN-ID zu.

12.3 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 benötigte bei Betriebsunfähigkeit einer Verbindung oder einer Bridge eine Rekonfigurationszeit von max. 30 s. Dies ist für zeitkritische Anwendungen nicht mehr akzeptabel. RSTP erreicht durchschnittliche Rekonfigurationszeiten von unter einer Sekunde. Wenn Sie RSTP in einer Ringtopologie mit 10 bis 20 Geräten einsetzen, können Sie auch Rekonfigurationszeiten im Millisekundenbereich erreichen.

Anmerkung: RSTP löst eine 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 erhöhtwerden.
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.

12.3.1 Grundlagen

Da RSTP eine Weiterentwicklung des STP ist, gelten alle folgenden Beschreibungen des STP auch für das RSTP.

Die Aufgaben des STP

Der Spanning Tree-Algorithmus reduziert Netztopologien, die mit Bridges aufgebaut sind und Ringstrukturen durch redundante Verbindungen aufweisen, auf eine Baumstruktur. Dabei trennt STP die Ringstrukturen nach vorgegebenen Regeln auf, indem es redundante Pfade deaktiviert. Wird ein Pfad unterbrochen, weil eine Netzkomponente betriebsunfähig wird, aktiviert das STP den zuvor deaktivierten Pfad wieder. Dies erlaubt redundante Verbindungen zur Erhöhung der Kommunikationsverfügbarkeit.
Das STP ermittelt bei der Bildung der Baumstruktur eine Bridge, die die Basis der STP-Baumstruktur repräsentiert. Diese Bridge heißt Root-Bridge.

Merkmale des STP-Algorithmus:

- automatische Rekonfiguration der Baumstruktur bei Bridge-Ausfällen oder Unterbrechung eines Datenpfades,
- Stabilisierung der Baumstruktur bis zur maximalen Netzausdehnung,
- Stabilisierung der Topologie innerhalb einer vorhersehbaren Zeit,
- durch den Administrator vorbestimmbare und reproduzierbare Topologie,
- Transparenz für die Endgeräte,
- geringe Netzlast gegenüber der verfügbaren Übertragungskapazität durch Einrichtung der Baumstruktur.

Die Bridge-Parameter

Jede Bridge und ihre Verbindungen werden im Kontext von Spanning Tree eindeutig durch die folgenden Parameter beschrieben:

- Bridge Identifier
- Root-Pfadkosten der Bridge-Ports,
- Port-Identifikation

Bridge Identifier

Die Bridge-Identifikation besteht aus 8 Bytes. Die 2 höchstwertigen Bytes sind die Priorität. Die Voreinstellung für die Prioritätszahl ist 32.768 (8000H), jedoch kann der Management-Administrator diese zur Konfiguration des Netzes verändern. Die 6 niederwertigen Bytes der Bridge-Identifikation sind die MAC-Adresse der Bridge. Die MAC-Adresse ermöglicht, dass alle Bridges eine eindeutige Bridge-Identifikation besitzen.
Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation besitzt die höchste Priorität.

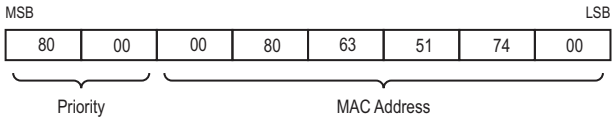


Abb. 30: Bridge-Identifikation, Beispiel (Werte in Hexadezimalschreibweise)

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 21). 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.

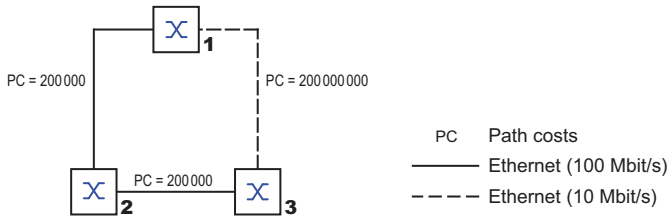


Abb. 31: Pfadkosten

Datenrate	Empfohlener Wert	Empfohlener Bereich	Möglicher Bereich
≤100 Kbit/s	200 000000[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	1-200000000
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. 21: 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.

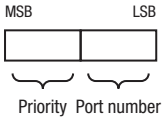


Abb. 32: Port-Identifikation

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).

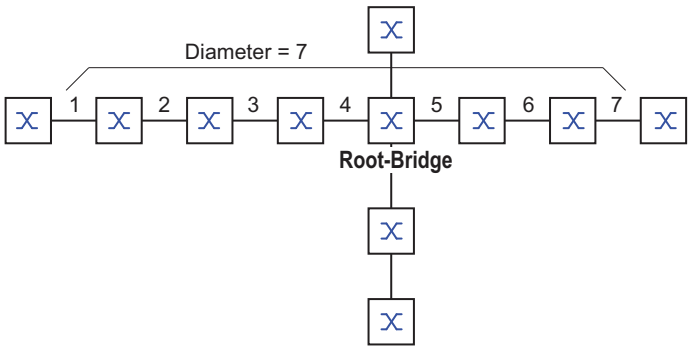


Abb. 33: Definition „Diameter“

Der im Netz erreichbare Netzdurchmesser beträgt MaxAge-1..
Im Lieferzustand ist 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.

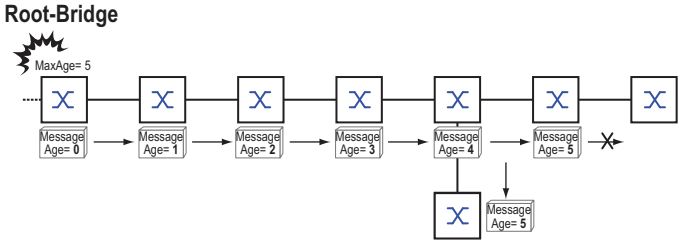


Abb. 34: Übertragung einer STP-BPDU in Abhängigkeit von MaxAge

12.3.2 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 32). 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.

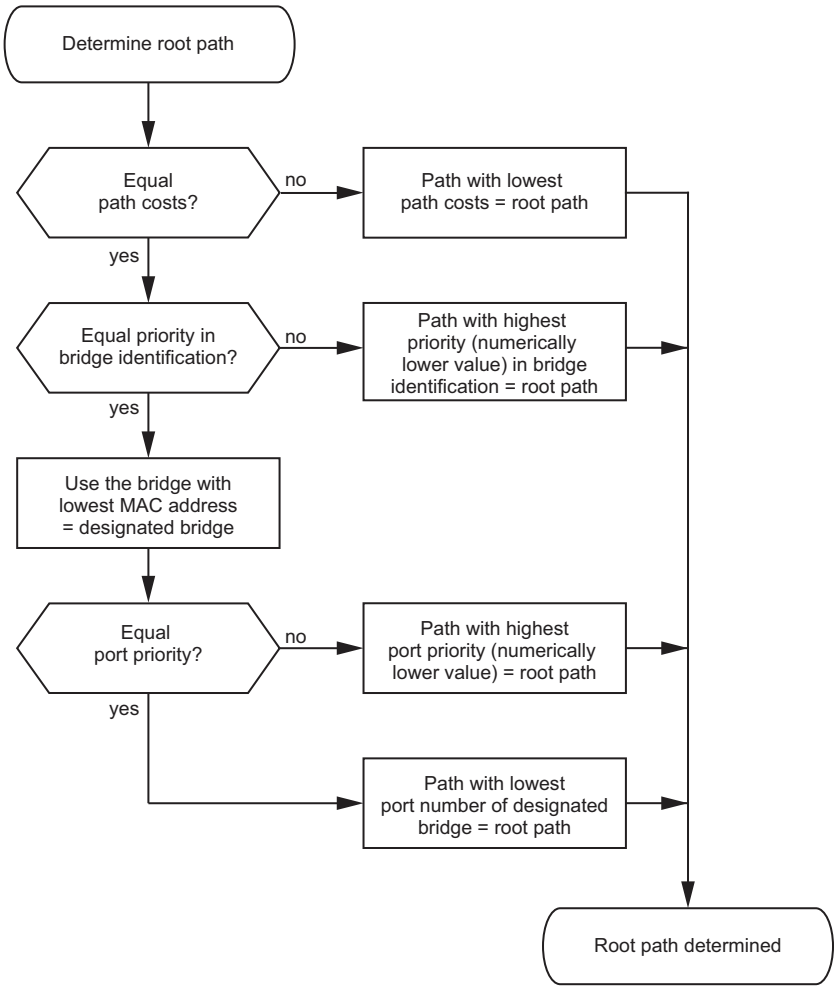


Abb. 35: Flussdiagramm Root-Pfad festlegen

12.3.3 Beispiele

Beispiel für die Bestimmung des Root-Pfads

Anhand des Netzplanes (siehe Abbildung 36) kann man das Flussdiagramm (siehe Abbildung 35) zur Festlegung des Root-Paths nachvollziehen. Der Administrator hat für jede Bridge eine Priorität in der Bridge-Identifikation festgelegt. Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation übernimmt die Rolle der Root-Bridge, in diesem Fall die Bridge 1. Im Beispiel belasten alle Teilpfade die gleichen Pfadkosten. Das Protokoll blockiert den Pfad zwischen Bridge 2 und Bridge 3, da eine Verbindung von Bridge 3 über Bridge 2 zur Root-Bridge höhere Pfadkosten verursachenwürde.

Interessant ist der Pfad von der Bridge 6 zur Root-Bridge:

- Der Pfad über Bridge 5 und Bridge 3 verursacht die gleichen Root-Pfadkosten wie der Pfad über Bridge 4 und Bridge 2.
- STP wählt den Pfad über die Bridge, die in der Bridge-Identifikation die niedrigere MAC-Adresse hat (im Bild dargestellt Bridge 4).
- Zwischen Bridge 6 und Bridge 4 gibt es ebenfalls 2 Pfade.
  Hier entscheidet die Portidentifikation (Port 1 < Port 3).

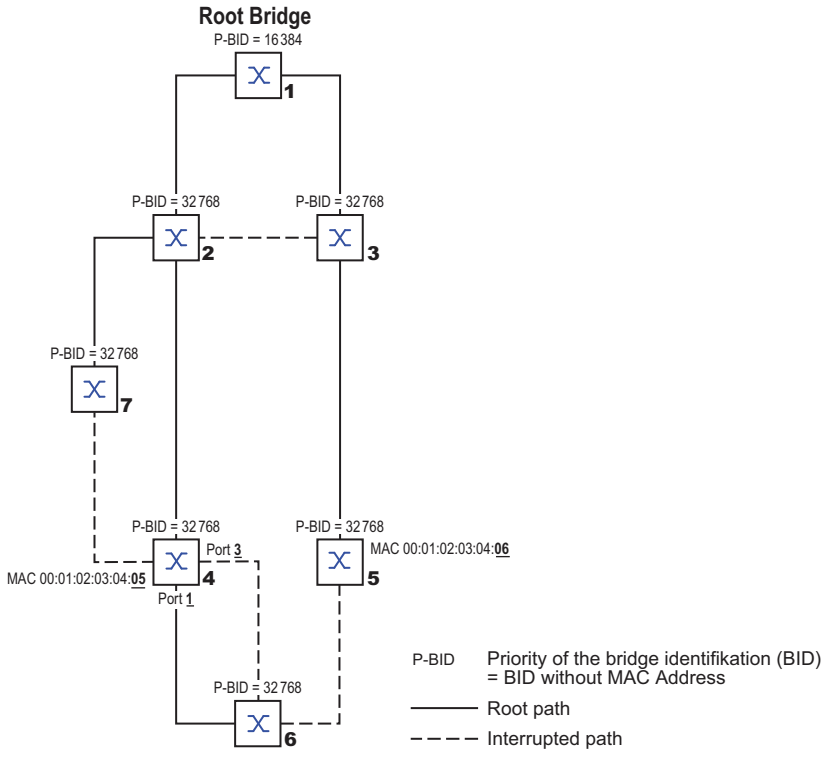


Abb. 36: Beispiel für die Bestimmung des Root-Pfads

Anmerkung: Indem der Administrator für jede Bridge außer der Root-Bridge den im Lieferzustand voreingestellten Wert der Priorität in der Bridge-Identifikation belässt, bestimmt allein die MAC-Adresse in der Bridge-Identifikation, welche Bridge bei Ausfall der momentanen Root-Bridge die Rolle der neuen Root-Bridge übernimmt.

Beispiel für die Manipulation des Root-Pfads

Anhand des Netzplanes (siehe Abbildung 37) kann man das Flussdiagramm (siehe Abbildung 35) zur Festlegung des Root-Paths nachvollziehen. Der Administrator hat folgendes getan:

– Für jede Bridge außer Bridge 1 und Bridge 5 hat er den im Lieferzustand voreingestellten Wert von 32768 (8000H) belassen und
– der Bridge 1 hat er den Wert 16384 (4000H) zugewiesen und damit zur Root-Bridge bestimmt.
– Der Bridge 5 hat er den Wert 28672 (7000H) zugewiesen.

Das Protokoll blockiert den Pfad zwischen Bridge 2 und Bridge 3, da eine Verbindung von Bridge 3 über Bridge 2 zur Root-Bridge höhere Pfadkosten bedeutet.

Interessant ist der Pfad von der Bridge 6 zur Root-Bridge:

▶ Die Bridges wählen den Pfad über Bridge 5, da der Zahlenwert 28672 für ihre Priorität in der Bridge-Identifikation kleiner ist als der Zahlenwert 32768.

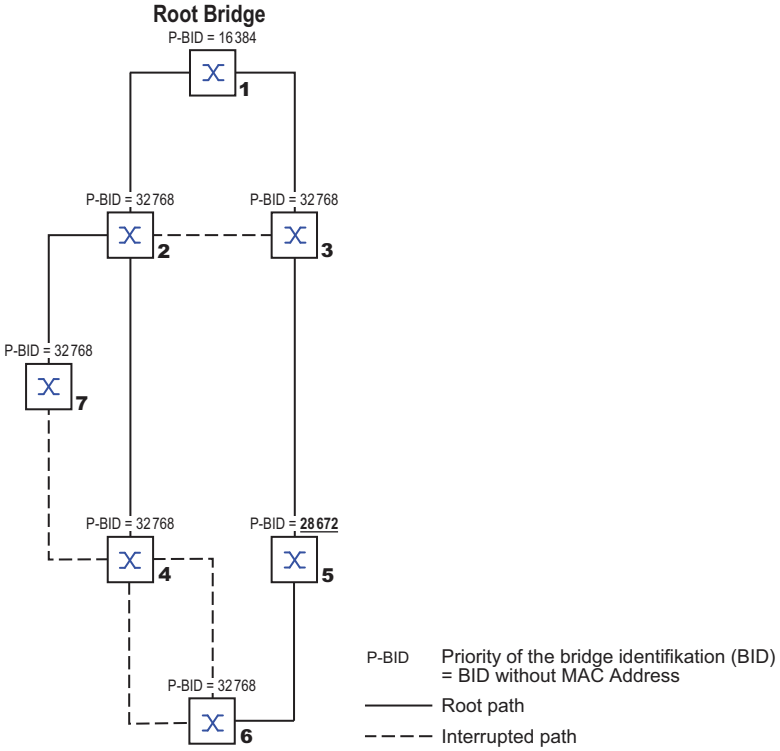


Abb. 37: Beispiel für die Manipulation des Root-Pfads

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 38). Die Pfadkosten der meisten Bridges zur Root-Bridge sind kleiner geworden.

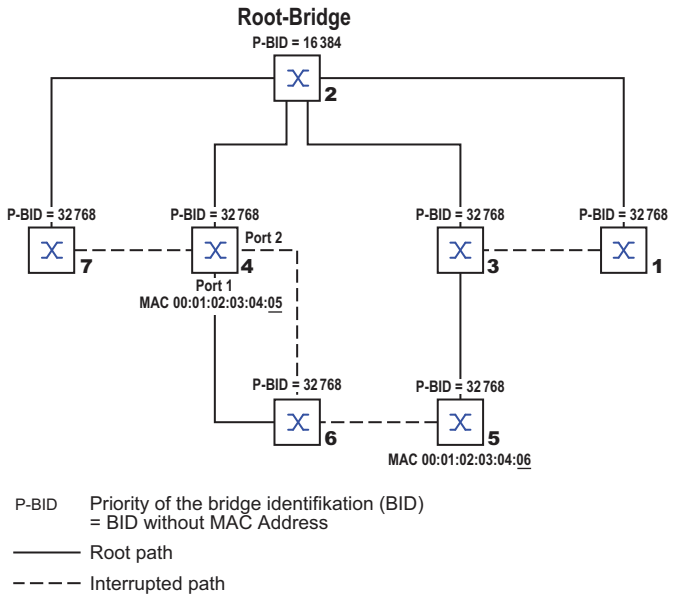


Abb. 38: Beispiel für die Manipulation der Baumstruktur

12.3.4 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 39):

- 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 35).
  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 geswitchten 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.

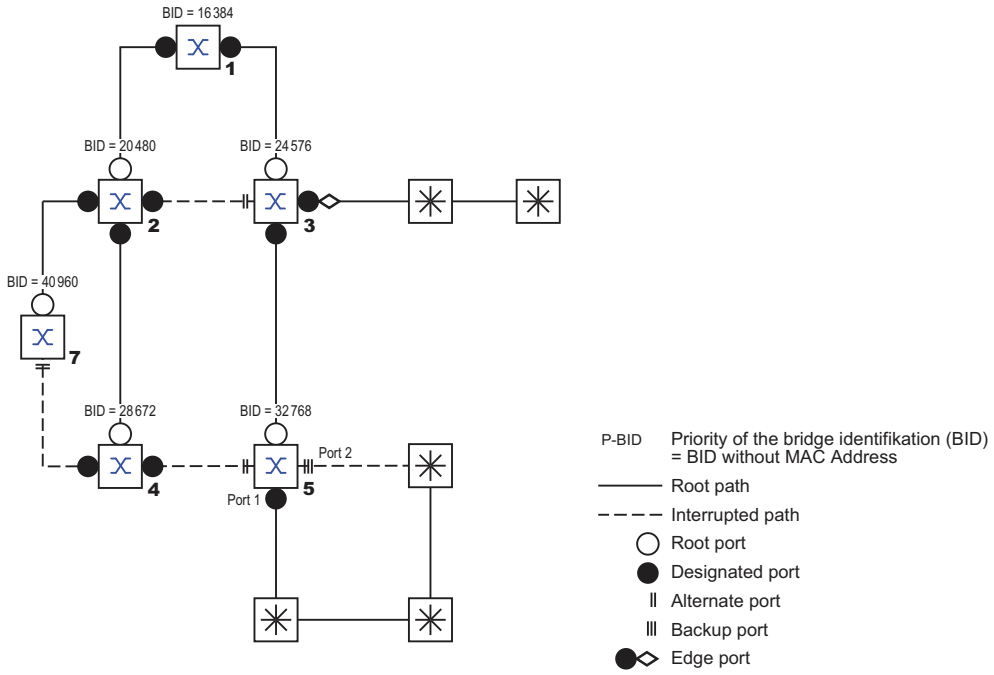


Abb. 39: Port-Rollen-Zuweisung

Port-Stati

In Abhängigkeit von der Baumstruktur und dem Status der ausgewählten Verbindungswege weist RSTP den Ports ihren Status zu.

STP Port Status	Administrative Bridge Port-Status	MAC Operational	RSTP Port-Status	Aktive Topology (Port Rolle)
DISABLED	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. 22: Beziehung zwischen Port-Status-Werten bei STP und RSTP

Bedeutung der RSTP-Port-Stati:

- Disabled: Port gehört nicht zur aktiven Topologie
- Discarding: Kein Addess Learning in FDB, kein Datenverkehr außer STP-BPDUs
- Learning: Address Learning aktiv (FDB), kein Datenverkehr außer 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.

12.3.5 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 nummerisch kleineren Wert fest.
Die Bridge mit der nummerisch 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:
Forward-Verzögerung [s] ≥ (***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.

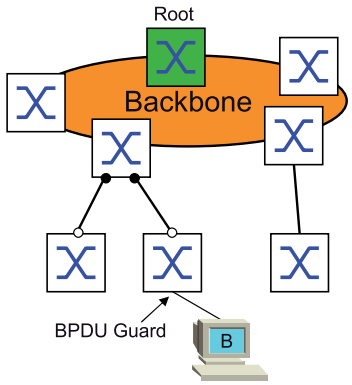
☐ Prüfen Sie in den anderen Geräten die folgende Werte:
– Bridge-ID (Bridge-Priorität und MAC-Adresse) des jeweiligen Gerätes sowie der Root-Bridge.
– Nummer des Geräte-Ports, der zur Root-Bridge führt.
– Pfadkosten vom Root-Port des Gerätes bis zur Root-Bridge.

`show spanning-tree global`	Zeigt zur Kontrolle die Parameter an.

12.3.6 Guards

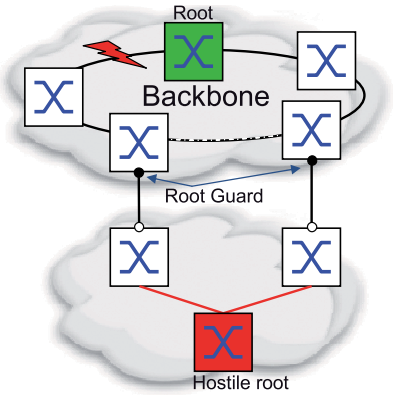
Das Gerät bietet Ihnen die Möglichkeit, an den Geräte-Ports verschiedene Schutzfunktionen (Guards) zu aktivieren.
Folgende Schutzfunktionen helfen, Ihr Netz vor Fehlkonfigurationen, Loops und Angriffen mit STP-BPDUs zu schützen:

- BPDU Guard – für manuell festgelegte Edge-Ports (Endgeräte-Ports)
  Diese Schutzfunktion aktivieren Sie global im Gerät.



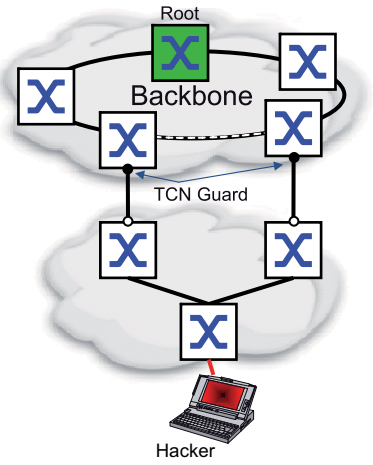
  Endgeräte-Ports empfangen im Normalfall keine STP-BPDUs. Versucht ein Angreifer, auf diesem Port trotzdem STP-BPDUs einzuspeisen, deaktiviert das Gerät den Geräte-Port.

- Root Guard – für Designated-Ports
  Diese Schutzfunktion aktivieren Sie für jeden Geräte-Port separat.



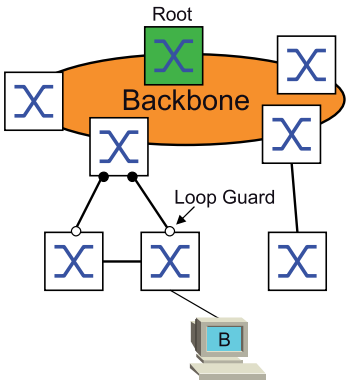
  Empfängt ein Designated-Port eine STP-BPDU mit besserer Pfadinformation zur Root-Bridge, verwirft das Gerät die STP-BPDU und setzt den Vermittlungsstatus des Ports auf `discarding` anstatt auf `root`.
  Bleiben die STP-BPDUs mit besserer Pfadinformation zur Root-Bridge aus, setzt das Gerät den Status des Ports nach 2 × ***`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 zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`spanning-tree bpdu-guard`	Schaltet den BPDU Guard ein.
`show spanning-tree global`	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 ***BPDU guard effect*** 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`	Verlässt den Interface-Modus.
`show spanning-tree port x/y`	Zeigt zur Kontrolle die Parameter des Ports an.

12.3.7 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 zwischenzuspeichern, 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 1/1`	Festlegen von Port `1/1` als erstes Interface.
`spanning-tree ring-only-mode second-port 1/2`	Festlegen von Port `1/2` als zweites Interface.

12.4 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`.

12.4.1 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 Übertragungsrate 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.

12.4.2 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.

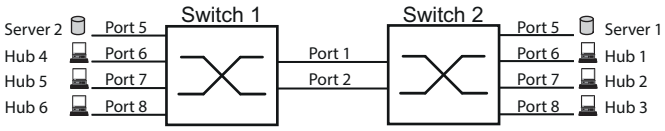


Abb. 40: Link Aggregation Switch-zu-Switch-Netz

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 zwischenzuspeichern, 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.

12.5 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 Dienstanbietern 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.

12.5.1 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.

12.5.2 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.

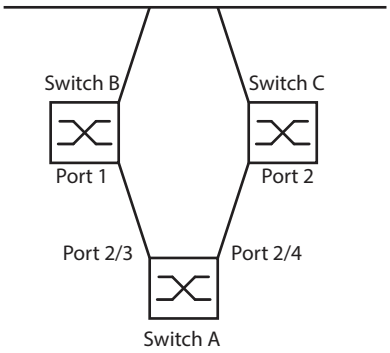


*Abb. 41: **Link-Backup** Beispiel-Netzwerk*

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-Pair 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 `Link_Backup_1` 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`	Wechsel in den Konfigurationsmodus.
`link-backup operation`	Aktiviert die ***Link-Backup***-Funktion global auf dem Gerät.

13 Funktionsdiagnose

Das Gerät bietet Ihnen folgende Diagnosewerkzeuge:

- SNMP-Traps senden
- Gerätestatus überwachen
- Out-of-Band-Signalisierung durch Signalkontakt
- 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.
`hm2DevMonSenseExtNvmRemoval`	Wird gesendet, wenn der externe Speicher entfernt worden ist.
`linkDown`	Wird gesendet, wenn die Verbindung zu einem Port unterbrochen wird.
`linkUp`	Wird gesendet, wenn die Verbindung zu einem Port hergestellt ist.
`hm2DevMonSensePSState`	Wird gesendet, wenn sich der Netzteilstatus ändert.
`hm2SigConStateChange`	Wird gesendet, wenn sich der Zustand des Signalkontaktes bei der Funktionsüberwachung ändert.
`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-Adressse 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. 23: 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 > Statuskonfiguration > Signalkontakt***
- Dialog ***Diagnose > Statuskonfiguration > MAC-Benachrichtigung***
- 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:

- über einen Signalkontakt Out-of-Band zu signalisieren
- 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:

- Inkorrekte Versorgungsspannung
  - mindestens eine der 2 Versorgungsspannungen ist außer Betrieb
  - die interne Versorgungsspannung ist außer Betrieb
- Das Gerät arbeitet außerhalb der benutzerdefinierten Temperaturschwelle.
- 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.
- Entfernen des externen Speichers
- Die Konfiguration des externen Speichers stimmt nicht mit der Konfiguration des Gerätes überein.
- Entfernen eines Moduls

Entscheiden Sie durch Markieren der entsprechenden Einträge, welche Ereignisse der Gerätestatus erfasst.

Anmerkung: Bei einer nichtredundanten Spannungsversorgung meldet das Gerät das Fehlen der Versorgungsspannung. Um diese Meldung zu deaktivieren, speisen Sie die Versorgungsspannung über beide Eingänge ein, oder ignorieren Sie die Überwachung, indem Sie die entsprechenden Kontrollkästchen deaktivieren.

13.2.1 Ereignisse, die überwacht werden können

Name	Bedeutung
Temperatur	Wenn die Temperatur den festgelegten Wert über- oder unterschreitet.
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 ***Verbindungsfehler melden*** aktiviert ist.
Modul entfernen	Schalten Sie diese globale Funktion ein, um das Entfernen eines Moduls überwachen. Schalten Sie außerdem das jeweilige zu überwachende Modul ein.
Externen Speicher entfernen	Aktivieren Sie diese Funktion, um das Vorhandensein eines externen Speichergerätes zu überwachen.
Externer Speicher nicht synchron	Das Gerät überwacht die Synchronisation zwischen der Gerätekonfiguration und der auf dem externen Speicher gespeicherten Konfiguration.
Netzteil	Schalten Sie diese Funktion ein, um die Spannungsversorgung zu überwachen.

*Tab. 24: **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 > Alarme (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 Temperatur zu überwachen, legen Sie im unteren Bereich des Rahmens ***Systemdaten*** die Temperaturschwellen fest.
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`device-status trap`	Senden eines SNMP-Traps, wenn sich der Gerätestatus ändert.
`device-status monitor envm-not-in-sync`	Überwacht die Konfigurationsprofile im Gerät und auf dem externen Speicher. In folgenden Situationen wechselt der ***Geräte-Status*** auf : – Das Konfigurationsprofil existiert ausschließlich im Gerät. – Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil auf dem externen Speicher.
`device-status monitor envm-removal`	Überwacht den aktiven externen Speicher. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen.
`device-status monitor power-supply 1`	Überwacht das Netzteil `1`. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn das Gerät einen Fehler an diesem Netzteil feststellt.

`device-status monitor ring-redundancy`	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.
`device-status monitor temperature`	Überwacht die Temperatur im Gerät. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn die Temperatur die festgelegten Grenzwerte überschreitet oder unterschreitet.
`device-status monitor module-removal`	Überwacht die Module. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn Sie ein Modul aus dem Gerät entfernen.
`device-status module 1`	Überwacht das Modul `1`. Der Wert im Rahmen ***Geräte-Status*** wechselt auf `error`, wenn Sie das Modul `1` aus dem Gerät entfernen.

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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`device-status monitor link-failure`	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.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`device-status link-alarm`	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 oder . Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät ermöglicht Ihnen:

- über einen Signalkontakt Out-of-Band zu signalisieren
- 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 *Min. Passwort-Länge*.
Passwort-Richtlinien deaktiviert	Das Gerät überwacht, ob die Einstellungen im Dialog *Gerätesicherheit >* Benutzerverwaltung die Anforderungen der Passwortrichtlinie erfüllen.
Prüfen der Passwort-Richtlinien im Benutzerkonto deaktiviert	Das Gerät überwacht die Einstellungen des Kontrollkästchens *Richtlinien überprüfen*. Wenn *Richtlinien überprüfen* 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.
Speichern des Konfigurationsprofils auf dem externen Speicher möglich	Das Gerät überwacht die Möglichkeit, Konfigurationen im externen permanenten Speicher zu speichern.
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.

Tab. 25: Sicherheitsstatus-Ereignisse

Name	Bedeutung
Unverschlüsselte Konfiguration vom externen Speicher laden	Das Gerät überwacht die Sicherheitseinstellungen für das Laden der Konfiguration von einem externen permanenten Speicher.
IEC61850-MMS aktiv	Das Gerät überwacht, wann Sie das Protokoll IEC 61850-MMS einschalten.
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. 25: `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 zwischenzuspeichern, 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 `user` und `admin`. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie für die Benutzerkonten `user` oder `admin` das voreingestellte Passwort unverändert verwenden.
`security-status monitor pwd-min-length`	Überwacht den in Richtlinie ***Min. Passwort-Länge*** festgelegten Wert. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn für die Richtlinie ***Min. Passwort-Länge*** ein Wert kleiner als `8` festgelegt ist.
`security-status monitor pwd-policy-config`	Überwacht die Passwort-Richtlinien-Einstellungen. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn für mindestens eine der folgenden Richtlinien der Wert `0` festgelegt ist. – ***Großbuchstaben (min.)*** – ***Kleinbuchstaben (min.)*** – ***Ziffern (min.)*** – ***Sonderzeichen (min.)***
`security-status monitor pwd-policy-inactive`	Überwacht die Passwort-Richtlinien-Einstellungen. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, 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 ***Sicherheits-Status*** wechselt auf `error`, wenn Sie den Telnet-Server einschalten.
`security-status monitor http-enabled`	Überwacht den HTTP-Server. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie den HTTP-Server einschalten.

`security-status monitor snmp-unsecure`	Überwacht den SNMP-Server. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn mindestens eine der folgenden Bedingungen zutrifft: – Die Funktion ***SNMPv1*** ist eingeschaltet. – Die Funktion ***SNMPv2*** ist eingeschaltet. – Die Verschlüsselung für SNMPv3 ist ausgeschaltet. Die Verschlüsselung schalten Sie ein im Dialog ***Gerätesicherheit > Benutzerverwaltung***, Feld ***SNMP-Verschlüsselung***.
`security-status monitor sysmon-enabled`	Überwachen der Aktivierung von System Monitor 1 auf dem Gerät.
`security-status monitor extnvm-upd-enabled`	Überwachen der Aktivierung der Aktualisierung des externen nichtflüchtigen Speichers.
`security-status monitor iec61850-mms-enabled`	Überwacht die ***IEC61850-MMS***-Funktion. Der Wert im Rahmen ***Sicherheits-Status*** wechselt auf `error`, wenn Sie die ***IEC61850-MMS***-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 ***Sicherheits-Status*** wechselt auf `error`, 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 Out-of-Band-Signalisierung

Das Gerät verwendet den Signalkontakt zur Steuerung von externen Geräten und zur Überwachung der Gerätefunktionen. Die Funktionsüberwachung ermöglicht die Durchführung einer Ferndiagnose.
Das Gerät meldet den Funktionsstatus über eine Unterbrechung des potentialfreien Signalkontaktes (Relaiskontakt, Ruhestromschaltung) für den gewählten Modus. Das Gerät überwacht folgende Funktionen:

- Inkorrekte Versorgungsspannung
  - mindestens eine der 2 Versorgungsspannungen ist außer Betrieb
  - die interne Versorgungsspannung ist außer Betrieb
- Das Gerät arbeitet außerhalb der benutzerdefinierten Temperaturschwelle.
- Ereignisse der Ring-Redundanz
  Redundanzverlust (im Ring-Manager-Modus)
  In der Voreinstellung ist die Ring-Redundanz-Überwachung inaktiv. Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in der lokalen Konfiguration.
- Unterbrechung der Link-Verbindung(en)
  Konfigurieren Sie für diese Funktion mindestens einen Port. Im Rahmen ***Verbindungsfehler melden*** legen Sie fest, welche Ports das Gerät bei fehlendem Link meldet. In der Voreinstellung ist die Link-Überwachung inaktiv.
- Entfernen des externen Speichers
- Die Konfiguration auf dem externer Speicher stimmt nicht mit der im Gerät überein.
- Entfernen eines Moduls

Entscheiden Sie durch Markieren der entsprechenden Einträge, welche Ereignisse der Gerätestatus erfasst.

Anmerkung: Bei einer nichtredundanten Spannungsversorgung meldet das Gerät das Fehlen der Versorgungsspannung. Um diese Meldung zu deaktivieren, speisen Sie die Versorgungsspannung über beide Eingänge ein, oder ignorieren Sie die Überwachung, indem Sie die entsprechenden Kontrollkästchen deaktivieren.

13.4.1 Signalkontakt steuern

Der Modus dient der Fernsteuerung des Signalkontaktes.

Anwendungsmöglichkeiten:
- Simulation eines bei einer SPS-Fehlerüberwachung erkannten Fehlers.
- Fernbedienen eines Gerätes über SNMP, zum Beispiel Einschalten einer Kamera.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Diagnose > Statuskonfiguration > Signalkontakt***, Registerkarte ***Global***.
- ☐ Um den Signalkontakt manuell zu steuern, wählen Sie im Rahmen ***Konfiguration***, Dropdown-Liste ***Modus*** den Wert `Manuelle Einstellung`.
- ☐ Um den Signalkontakt zu öffnen, wählen Sie im Rahmen ***Konfiguration*** das Optionsfeld `offen`.

☐ Um den Signalkontakt zu schließen, wählen Sie im Rahmen ***Konfiguration*** das Optionsfeld `geschlossen`.

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`signal-contact 1 mode manual`	Auswählen des manuellen Einstellungsmodus für Signalkontakt `1`.
`signal-contact 1 state open`	Öffnen des Signalkontaktes `1`.
`signal-contact 1 state closed`	Schließen des Signalkontaktes `1`.

13.4.2 Gerätestatus und Sicherheitsstatus überwachen

Im Rahmen ***Konfiguration*** legen Sie fest, welche Ereignisse der Signalkontakt signalisiert:

- `Geräte-Status`
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog ***Diagnose > Statuskonfiguration > Gerätestatus*** überwachten Parameter.
- `Sicherheits-Status`
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog ***Diagnose > Statuskonfiguration > Sicherheitsstatus*** überwachten Parameter.
- `Geräte-/Sicherheits-Status`
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog ***Diagnose > Statuskonfiguration > Gerätestatus*** und im Dialog ***Diagnose > Statuskonfiguration > Sicherheitsstatus*** überwachten Parameter.

Funktionsüberwachung konfigurieren

Führen Sie die folgenden Schritte aus:

☐ Öffnen Sie den Dialog ***Diagnose > Statuskonfiguration > Signalkontakt***, Registerkarte ***Global***.

☐ Um mit dem Signalkontakt die Gerätefunktionen zu überwachen, legen Sie im Rahmen ***Konfiguration***, Feld ***Modus*** den Wert fest.

☐ 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 zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

☐ Legen Sie im Dialog ***Diagnose > Statuskonfiguration > Alarme (Traps)*** mindestens 1 Trap-Ziel fest, das SNMP-Traps empfängt.

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

☐ Die Temperaturschwellen für die Temperaturüberwachung legen Sie im Dialog ***Grundeinstellungen > System*** fest.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`signal-contact 1 monitor temperature`	Überwacht die Temperatur im Gerät. Der Signalkontakt öffnet, wenn die Temperatur die Temperaturschwellen überschreitet oder unterschreitet.
`signal-contact 1 monitor ring-redundancy`	Überwacht die Ring-Redundanz. In folgenden Situationen öffnet der Signalkontakt: – Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve). – Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen.
`signal-contact 1 monitor link-failure`	Überwacht den Link auf den Ports/Interfaces. Der Signalkontakt öffnet, wenn der Link auf einem überwachten Port/Interface abbricht.
`signal-contact 1 monitor envm-removal`	Überwacht den aktiven externen Speicher. Der Signalkontakt öffnet, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen.
`signal-contact 1 monitor envm-not-in-sync`	Überwacht die Konfigurationsprofile im Gerät und auf dem externen Speicher. In folgenden Situationen öffnet der Signalkontakt: – Das Konfigurationsprofil existiert ausschließlich im Gerät. – Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil auf dem externen Speicher.
`signal-contact 1 monitor power-supply 1`	Überwacht das Netzteil `1`. Der Signalkontakt öffnet, wenn das Gerät einen Fehler an diesem Netzteil feststellt.
`signal-contact 1 monitor module-removal 1`	Überwacht das Modul `1`. Der Signalkontakt öffnet, wenn Sie Modul `1` aus dem Gerät entfernen.
`signal-contact 1 trap`	Freigabe des Gerätes zum Senden eines SNMP-Traps bei Änderung des Status der Funktionsüberwachung.
`no signal-contact 1 trap`	Deaktivieren des SNMP-Traps

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:

☐ Aktivieren Sie in Spalte ***Überwachen*** die Funktion ***Verbindungsabbruch auf eingeschalteten Ports***.

☐ Öffnen Sie den Dialog ***Diagnose > Statuskonfiguration > Gerätestatus***, Registerkarte ***Port***.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`signal-contact 1 monitor link-failure`	Überwacht den Link auf den Ports/Interfaces. Der Signalkontakt öffnet, wenn der Link auf einem überwachten Port/Interface abbricht.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`signal-contact 1 link-alarm`	Überwacht den Link auf dem Port/Interface. Der Signalkontakt öffnet, wenn der Link auf dem Port/Interface abbricht.

Ereignisse, die überwacht werden können

Name	Bedeutung
Temperatur	Wenn die Temperatur den festgelegten Wert über- oder unterschreitet.
Ring-Redundanz	Schalten Sie diese Funktion ein, um das Vorhandensein der Ring-Redundanz zu überwachen.

Tab. 26: `Gerätestatus`-Ereignisse

Name	Bedeutung
Verbindungsfehler	Aktivieren Sie diese Funktion, um jedes Ereignis in Bezug auf Port-Links zu überwachen, bei dem das Kontrollkästchen ***Verbindungsfehler melden*** aktiviert ist.
Modul entfernen	Schalten Sie diese globale Funktion ein, um das Entfernen eines Moduls überwachen. Schalten Sie außerdem das jeweilige zu überwachende Modul ein.
Externer Speicher und NVM nicht synchron	Das Gerät überwacht die Synchronisation zwischen der Gerätekonfiguration und der auf dem externen Speicher gespeicherten Konfiguration.
Externer Speicher wurde entfernt	Aktivieren Sie diese Funktion, um das Vorhandensein eines externen Speichergerätes zu überwachen.
Netzteil	Schalten Sie diese Funktion ein, um die Spannungsversorgung zu überwachen.

Tab. 26: `Gerätestatus`-Ereignisse (Forts.)

Signalkontakt-Anzeige

Das Gerät bietet Ihnen weitere Möglichkeiten, den Zustand des Signalkontaktes darzustellen:

- Anzeige in der grafische Benutzeroberfläche
- Abfrage im Command Line Interface

☐ Öffnen Sie den Dialog ***Grundeinstellungen > System***.
Der Rahmen ***Status Signalkontakt*** zeigt den Signalkontaktstatus und informiert über aufgetretene Alarme. Der Rahmen ist hervorgehoben, wenn gegenwärtig ein Alarm vorhanden ist.

```
show signal-contact 1 all
```
Anzeige der Einstellungen für den angegebenen Signalkontakt

13.5 Port-Zustandsanzeige

Führen Sie die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.

Der Dialog zeigt das Gerät mit der aktuellen Konfiguration an. Darüber hinaus zeigt der Dialog den Status der einzelnen Ports mittels eines Symbols an.

Die folgenden Symbole stellen den Zustand der einzelnen Ports dar. In manchen Situationen überlagern sich diese Symbole. Wenn Sie den Mauszeiger über dem Portsymbol positionieren, zeigt eine Sprechblase eine detaillierte Beschreibung des Portzustandes.

Kriterium	Symbol	
Bandbreite des Ports		10 Mbit/s Port aktiviert, Verbindung in Ordnung, Vollduplexbetrieb
		100 Mbit/s Port aktiviert, Verbindung in Ordnung, Vollduplexbetrieb
		1000 Mbit/s Port aktiviert, Verbindung in Ordnung, Vollduplexbetrieb
Betriebszustände		Halbduplexbetrieb eingeschaltet Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen *Automatische Konfiguration*, Feld *Manuelle Konfiguration* und Feld *Manuelles Cable-Crossing (Auto. Konfig. aus)*.
		Autonegotiation eingeschaltet Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen *Automatische Konfiguration*.
		Port ist durch eine Redundanz-Funktion blockiert.
AdminLink		Port ist deaktiviert, Verbindung in Ordnung
		Port ist deaktiviert, keine Verbindung aufgebaut Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen *Port an* und Feld *Link/ Aktuelle Betriebsart*.

Tab. 27: Symbole zur Kennzeichnung des Zustands der Ports

13.6 Portereignis-Zähler

Die Port-Statistiktabelle versetzt den erfahrenen Netzbetreuer in die Lage, erkannte eventuelle Schwachpunkte im Netz zu identifizieren.

Diese Tabelle zeigt Ihnen die Inhalte verschiedener Ereigniszähler an. 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	– Nicht funktionierender Controller des verbundenen Gerätes – Elektromagnetische Einkoppelung im Übertragungsmedium
CRC-Fehler	– Nicht funktionierender Controller des verbundenen Gerätes – Elektromagnetische Einkoppelung im Übertragungsmedium – Nicht betriebsbereite Komponente im Netz
Kollisionen	– Nicht funktionierender Controller des verbundenen Gerätes – Netzausdehnung zu groß/Zeilen zu lang – Kollision oder Fehler beim Datenpaket ermittelt

Tab. 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***.

13.6.1 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

13.7 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.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`port-monitor condition crc-fragments count 2000`	CRC-Fragment-Zähler auf 2000 Teile pro Million festlegen.
`port-monitor condition crc-fragments interval 15`	Setzt das Messintervall für die CRC-Fragment-Erkennung auf 15 Sekunden.
`auto-disable timer 120`	Legt eine Wartezeit von `120` Sekunden fest, nach der die ***Auto-Disable***-Funktion den Port wieder einschaltet.
`exit`	Wechsel in den Konfigurationsmodus.
`auto-disable reason crc-error`	Aktivieren Sie die die Selbstabschaltfunktion für CRC.
`port-monitor condition crc-fragments mode`	Um eine Aktion auszulösen, aktivieren Sie die CRC-Fragment-Bedingung.
`port-monitor operation`	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:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`auto-disable reset`	Bietet Ihnen die Möglichkeit, den Port einzuschalten, bevor der Timer zu zählen beginnt.

13.8 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***.

13.9 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 Gerätekennung 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 verwerfen 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.

13.9.1 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.

13.9.2 LLDP-MED

Bei „LLDP for Media Endpoint Devices“ (LLDP-MED) handelt es sich um eine Erweiterung von LLDP, die zwischen Endpunktgeräten arbeitet. Endpunkte umfassen Geräte wie IP-Telefone oder andere Voice-over-IP-Geräte (VoIP-Geräte) oder Server und Netzgeräte, zum Beispiel Switches. Diese Erweiterung bietet insbesondere Unterstützung für VoIP-Anwendungen. LLDP-MED stellt diese Unterstützung mithilfe eines zusätzlichen Satzes gebräuchlicher Mitteilungen (d. h. Nachrichten des Typs „Type Length Value“, TLV) für die Ermittlung von Funktionsmerkmalen wie Netz-Richtlinien, PoE (Power over Ethernet), Bestandsverwaltung und Standortdaten bereit.

Das Gerät unterstützt folgende TLV-Meldungen:

- Funktions-TLV
  Bietet LLDP-MED-Endpunkten die Möglichkeit, zu ermitteln, welche Funktionen das angeschlossene Gerät unterstützt und welche Funktionen im Gerät aktiviert sind.
- TLV – Netzrichtlinien
  Gibt beiden Netzanschlussgeräten und Endpunkten die Möglichkeit, VLAN-Konfigurationen und verbundene Attribute für die spezifische Anwendung an dem Port anzubieten. Das Gerät übermittelt einem Telefon die VLAN-Nummer. Das Telefon stellt eine Verbindung zu einem Switch her, fragt seine VLAN-Nummer ab und startet die Kommunikation mit der Anrufsteuerung.

LLPD-MED stellt die folgenden Funktionen bereit:

- Ermittlung der Netz-Richtlinien, einschließlich VLAN ID, Priorität 802.1p und „Differentiated Service Code Point“ (DSCP).
- Gerätestandort- und Topologie-Erkennung auf der Basis von MAC-/Port-Informationen auf LAN-Ebene.
- Benachrichtigung zur Erkennung einer Endpunktverschiebung, vom Netzanschlussgerät an die zugehörige VoIP-Verwaltungsanwendung.

- Erweiterte Identifizierung von Geräten für die Bestandsverwaltung
- Identifizierung von Netzanschlussfunktionen eines Endpunktes, zum Beispiel Multiport-IP-Telefon mit integriertem Switch oder Brückenfunktion.
- Interaktionen auf Anwendungsebene mit LLDP-Protokollelementen für die zeitnahe Inbetriebnahme des LLDP zur Unterstützung der schnellen Verfügbarkeit eines Notdienstes.
- Anwendbarkeit von LLPD-MED für Wireless-LAN-Umgebungen, Unterstützung für Voice over Wireless LAN.

13.10 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.

13.11 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.
- Persistentes Protokoll
  Das Gerät speichert Protokolleinträge in einer Datei im externen Speicher (falls vorhanden). Diese Dateien sind nach dem Abschalten verfügbar. Die maximale Größe und Anzahl von speicherbaren Dateien sowie der Schweregrad der protokollierten Ereignisse sind konfigurierbar. Nach Erreichen der benutzerdefinierten maximale Größe oder Anzahl speicherbarer Dateien archiviert das Gerät die Einträge und erzeugt eine neue Datei. Das Gerät löscht die älteste Datei und benennt die anderen Dateien um, um die konfigurierte Anzahl von Dateien beizubehalten. Um diese Dateien zu prüfen, verwenden Sie CLI, oder kopieren Sie die Dateien für den späteren Zugriff auf einen externen Server.
- 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.

13.11.1 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 zwischenzuspeichern, 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 zwischenzuspeichern, 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 .

13.11.2 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 ***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 .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging host add 1 addr 10.0.1.159 severity 3`	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`.
`logging syslog operation`	Einschalten der ***Syslog***-Funktion.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show logging host`	Anzeigen der Syslog-Host-Einstellungen.

```
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
```

`configure`	Wechsel in den Konfigurationsmodus.
`logging snmp-requests get operation`	Protokolliert SNMP-Get-Anfragen.
`logging snmp-requests get severity 5`	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
```

13.11.3 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.

13.11.4 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

13.12 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“.

13.13 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

13.13.1 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 empfangen Datenpakete. Die Funktion hat keine Auswirkungen auf den über die Quellports laufenden Datenstrom.

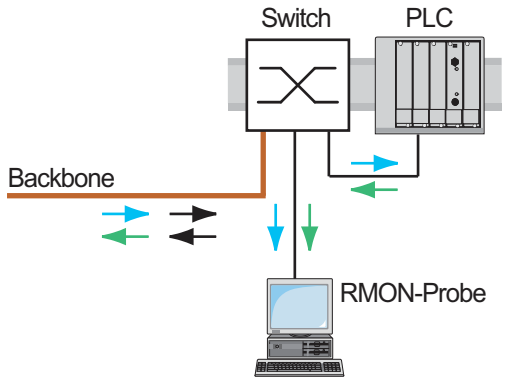


Abb. 42: Beispiel

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.

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.
- ☐ Falls erforderlicu, legen Sie einen zweiten Ziel-Port fest.
  Wählen Sie im Rahmen ***Ziel-Port***, Dropdown-Liste ***Sekundärer Port*** den gewünschten Port.
  Voraussetzung ist, dass bereits der primäre Ziel-Port festgelegt ist.
- ☐ Um über den Zielport auf die Management-Funktionen zuzugreifen:
  Markieren Sie im Rahmen ***Ziel-Port*** das Kontrollkästchen ***Management erlauben***.
- ☐ Um die Änderungen zwischenzuspeichern, 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***.

13.14 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 ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`selftest action task log-only`	Senden einer Nachricht an das Ereignisprotokoll, wenn eine Aufgabe missglückt ist.
`selftest action resource send-trap`	Senden eines SNMP-Traps bei Ressourcen-Mangel.
`selftest action software send-trap`	Senden eines SNMP-Traps bei Verlust der Software-Integrität.
`selftest action hardware reboot`	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-Funkion 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.

`selftest ramtest`	Aktivieren des RAM-Selbsttests bei einem Kaltstart
`no selftest ramtest`	Abschalten der Funktion „ramtest“
`selftest system-monitor`	Aktivieren der Funktion „SysMon1“
`no selftest system-monitor`	Abschalten der Funktion „SysMon1“
`show selftest action`	Statusanzeige der durchzuführenden Maßnahmen bei einer Beeinträchtigung des Gerätes
`show selftest settings`	Anzeige der Einstellungen für „ramtest“ und SysMon“ bei einem Kaltstart

13.15 Kupferkabeltest

Verwenden Sie diese Funktion, um ein an eine Schnittstelle angeschlossenes Kupferkabel auf einen Kurzschluss oder eine Schaltkreisunterbrechung zu testen. Der Test unterbricht den Verkehrsfluss (falls vorhanden) auf diesem Port.

Die Tabelle zeigt den Zustand und die Länge jedes einzelnen Paares an. Das Gerät gibt ein Ergebnis mit der folgenden Bedeutung zurück:

- normal – gibt an, dass das Kabel ordnungsgemäß funktioniert
- offen – gibt an, dass im Kabel eine Unterbrechung vorliegt
- Kurzschluss – gibt an, dass das Kabel einen Kurzschluss aufweist
- ungetestet – gibt an, dass ein ungetestetes Kabel vorhanden ist
- unbekannt – Kabel abgezogen

14 Erweiterte Funktionen des Gerätes

14.1 Gerät als DHCP-Server verwenden

Ein DHCP-Server („Dynamic Host Configuration Protocol“) nimmt die Zuweisung von IP-Adressen, Gateways und sonstigen Netzdefinitionen (zum Beispiel DNS- und NTP-Parameter) zu Clients vor.

Die DHCP-Operationen laufen in 4 Schritten ab: IP Discovery (Client versendet Anfrage an Server), IP Lease Offer (Server bieten IP-Adresse an), IP Request (Client fordert IP-Adresse an) und IP Lease Acknowledgement (Server bestätigt Adresse). Die Phasen sind anhand des Akronyms „DORA“ (für „Discovery“, „Offer“, „Recovery“ und „Acknowledgement“) einfach zu merken. Der Server empfängt Client-Daten über UDP-Port 67 und sendet Daten an den Client über UDP-Port 68.

Der DHCP-Server stellt IP-Adress-Pools, auch als „Pools“ bezeichnet, bereit, aus denen er den Clients IP-Adressen zuweist. Der Pool besteht aus einer Liste mit Einträgen. Ein Eintrag definiert entweder eine bestimmte IP-Adresse oder einen IP-Adressbereich.

Das Gerät bietet Ihnen die Möglichkeit, den DHCP-Server global oder je Schnittstelle zu aktivieren.

14.1.1 Pro Port oder pro VLAN zugewiesene IP-Adressen

Der DHCP-Server weist einem Client, der mit einem Port oder einem VLAN verbunden ist, eine statische IP-Adresse oder einen dynamischen Bereich von IP-Adressen zu. Das Gerät bietet Ihnen die Möglichkeit, Einträge entweder für einen Port oder ein VLAN anzulegen. Beim Erzeugen eines Eintrags für das Zuweisen von IP-Adressen zu einem VLAN wird der Port-Eintrag grau dargestellt. Beim Erzeugen eines Eintrags für das Zuweisen von IP-Adressen zu einem Port wird der VLAN-Eintrag grau dargestellt.

Bei statischer Zuordnung weist der DHCP-Server einem bestimmten Client dieselbe IP-Adresse zu. Der DHCP-Server identifiziert den Client über eine eindeutige Hardware-ID. Ein statischer Adresseintrag enthält 1 IP-Adresse, die er auf einen Port oder ein VLAN anwendet, auf dem der Server eine Anfrage von einem bestimmten Client erhält. Für eine statische Zuteilung legen Sie einen Pool-Eintrag für die Ports oder einen bestimmten Port an, geben die IP-Adresse ein und lassen die Spalte ***Letzte IP-Adresse*** frei. Legen Sie eine Hardware-Kennung fest, über die der DHCP-Server den Client eindeutig identifiziert. Diese Kennung ist entweder eine MAC-Adresse, eine Client-ID, eine Remote-ID oder eine Circuit-ID. Wenn ein Client den Server mit der konfigurierten Hardware-Kennung kontaktiert, weist der DHCP-Server die statische IP-Adresse zu.

Das Gerät gibt Ihnen die Möglichkeit, Ports oder VLANs, von denen der DHCP-Server eine freie IP-Adresse aus einem Pool zuweist, einen dynamischen IP-Adressbereich zuzuweisen. Um einen dynamischen Pool-Eintrag für die Ports oder VLANs hinzuzufügen, legen Sie die erste und letzte IP-Adresse für den IP-Adressbereich fest und lassen die Spalten ***MAC-Adresse***, ***Client-ID***, ***Remote-ID*** und ***Circuit-ID*** leer. Das Erzeugen mehrerer Pool-Einträge lässt Lücken in den IP-Adressbereichen zu.

14.1.2 Beispiel: DHCP-Server – Statische IP-Adresse

In diesem Beispiel konfigurieren Sie das Gerät so, dass es einem Port eine statische IP-Adresse zuweist. Das Gerät erkennt Clients mit eindeutiger Hardware-Kennung. Die Hardware-Kennung ist in diesem Fall die Client-MAC-Adresse `00:24:E8:D6:50:51`.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Erweitert > DHCP-Server > Pool***.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Legen Sie in Spalte ***IP-Adresse*** den Wert `192.168.23.42` fest.
- ☐ Legen Sie in Spalte ***Port*** den Wert `1/1` fest.
- ☐ Legen Sie in Spalte ***MAC-Adresse*** den Wert `00:24:E8:D6:50:51` fest.
- ☐ Um dem Client eine IP-Adresse ohne Zeitbegrenzung zuzuweisen, legen Sie in Spalte ***Lease-Time [s]*** den Wert `4294967295` fest.
- ☐ Markieren Sie das Kontrollkästchen in Spalte ***Aktiv***.
- ☐ Öffnen Sie den Dialog ***Erweitert > DHCP-Server > Global***.
- ☐ Markieren Sie für Port `1/1` das Kontrollkästchen in Spalte ***DHCP-Server aktiv***.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen ***Funktion*** das Optionsfeld .
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dhcp-server pool add 1 static 192.168.23.42`	Erzeugen eines Eintrags mit Index `1` und Hinzufügen der IP-Adresse `192.168.23.42` zum statischen Pool.
`dhcp-server pool modify 1 mode interface 1/1`	Zuweisen der statischen Adresse des Eintrags mit Index `1` zu Interface `1/1`.
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	Zuweisen der IP-Adresse in Index `1` zu dem Gerät mit der MAC-Adresse `00:24:E8:D6:50:51`.
`dhcp-server pool mode 1`	Aktivieren des Pool-Eintrages mit Index `1`.
`dhcp-server pool modify 1 leasetime infinite`	Ändern des Eintrags mit Index `1` für die unbegrenzte Zuweisung der IP-Adresse zum Client.
`dhcp-server operation`	Globales Aktivieren des DHCP-Servers.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`dhcp-server operation`	Aktivieren der ***DHCP-Server***-Funktion für diesen Port.

14.1.3 Beispiel: DHCP-Server – Dynamischer IP-Adressbereich

Das Gerät bietet Ihnen die Möglichkeit, dynamische IP-Adressbereiche anzulegen. Lassen Sie die Felder ***MAC-Adresse***, ***Client-ID***, ***Remote-ID*** und ***Circuit-ID*** frei. Um dynamische IP-Adressbereiche mit Lücken zwischen den Bereichen anzulegen, fügen Sie der Tabelle mehrere Einträge hinzu.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Erweitert > DHCP-Server > Pool***.

☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .

☐ Legen Sie in Spalte ***IP-Adresse*** den Wert `192.168.23.92` fest. Dies ist die erste IP-Adresse des Bereichs.

☐ Legen Sie in Spalte ***Letzte IP-Adresse*** den Wert `192.168.23.142` fest. Dies ist die letzte IP-Adresse des Bereichs.

Die Voreinstellung in Spalte ***Lease-Time [s]*** ist 60 Tage.

☐ Legen Sie in Spalte ***Port*** den Wert `1/2` fest.

☐ Markieren Sie das Kontrollkästchen in Spalte ***Aktiv***.

☐ Öffnen Sie den Dialog ***Erweitert > DHCP-Server > Global***.

☐ Markieren Sie für Port `1/2` das Kontrollkästchen in Spalte ***DHCP-Server aktiv***.

☐ Um die Funktion einzuschalten, wählen Sie im Rahmen ***Funktion*** das Optionsfeld .

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	Einfügen eines dynamischen Pools mit einem IP-Bereich von `192.168.23.92` bis `192.168.23.142`.
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	Einfügen der Lease Time in Sekunden bzw. als unbegrenzt.
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	Einfügen eines dynamischen Pools mit einem IP-Bereich von `192.168.23.172` bis `192.168.23.180`.
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	Einfügen der Lease Time in Sekunden bzw. als unbegrenzt.
`dhcp-server pool mode 2`	Aktivieren des Pool-Eintrages mit Index `2`.
`dhcp-server pool mode 3`	Aktivieren des Pool-Eintrages mit Index `3`.
`dhcp-server operation`	Globales Aktivieren des DHCP-Servers.
`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `2/1`.
`dhcp-server operation`	Aktivieren der ***DHCP-Server***-Funktion für diesen Port.

14.2 DHCP-L2-Relay

Ein Netzadministrator verwendet den DHCP-Schicht-2-Relay-Agenten, um DHCP-Client-Informationen hinzuzufügen. Diese Informationen werden von einem DHCP-Schicht-3-Relay-Agenten und DHCP-Servern benötigt, um einem Client eine Adresse sowie eine Konfiguration zuzuweisen.

Befinden sich ein DHCP-Client und -Server in demselben IP-Subnetz, erfolgt der Austausch von IP-Adressanfragen und IP-Adressantworten zwischen ihnen direkt. Der Einsatz eines DHCP-Servers für jedes Subnetz ist jedoch teuer und häufig unpraktisch. Eine Alternative, um den Einsatz eines DHCP-Servers für jedes Subnetz zu vermeiden, ist die Verwendung von Netzgeräten zur Weiterleitung von Paketen zwischen einem DHCP-Client und einem DHCP-Server, der sich in einem anderen Subnetz befindet.

Bei einem Schicht-3-Relay-Agenten handelt es sich im Allgemeinen um einen Router, der IP-Schnittstellen sowohl in den Client- als auch in den Server-Subnetzen besitzt und den Datenverkehr zwischen ihnen weiterleitet. In Schicht-2-vermittelten Netzen jedoch befinden sich ein oder mehrere Netzgeräte zwischen dem Client und dem Schicht-3-Relay-Agenten oder DHCP-Server, zum Beispiel Switches. In diesem Fall stellt das Gerät einen Laser-2-Relay-Agenten bereit, um Informationen hinzuzufügen, die der Schicht-3-Relay-Agent und der DHCP-Server benötigen, um ihre Funktionen bei der Adress- und Konfigurationszuweisung zu erfüllen.

Die folgende Liste enthält die Voreinstellungen für diese Funktion:

- Allgemeine Einstellungen:
  - Aktive Einstellung: deaktivieren
- Schnittstelleneinstellungen:
  - Aktive Einstellung: deaktivieren
  - Gesicherter Port: deaktivieren
- VLAN-Einstellungen:
  - Aktive Einstellung: deaktivieren
  - Circuit-ID: aktivieren
  - Remote-ID-Typ: mac
  - Remote-ID: leer

14.2.1 Circuit- und Remote-IDs

Die Circuit-ID und die Remote-ID fügt das Gerät in das Option-82-Feld des DHCP-Request-Pakets ein, bevor es die Anfrage eines Clients an den DHCP-Server weiterleitet.

- In der Circuit-ID ist gespeichert, auf welchem Port das Gerät die Anfrage des Clients empfangen hat.
- Die Remote-ID enthält die MAC-Adresse, die IP-Adresse, den Systemnamen oder eine benutzerdefinierte Zeichenfolge. Damit identifizieren die beteiligten Geräte den Relay-Agenten, der die Anfrage des Clients empfangen hat.

Das Gerät und andere Relay-Agenten verwenden diese Information, um die Antwort des DHCP-Servers wieder an den ursprünglichen Client zurück zu leiten. Der DHCP-Server kann diese Informationen auswerten, um dem Client zum Beispiel eine IP-Adresse aus einem bestimmten Adress-Pool zuzuweisen.

Das Antwort-Paket des DHCP-Servers enthält die Circuit-ID und Remote-ID ebenfalls. Vor Weiterleiten der Antwort an den Client entfernt das Gerät die Information wieder aus dem Option-82-Feld.

14.2.2 DHCP-L2-Relay-Konfiguration

Der Dialog ***Erweitert > DHCP-L2-Relay > Konfiguration*** bietet Ihnen die Möglichkeit, die Funktion auf den aktiven Ports und in den VLANs zu aktivieren.

Das Gerät leitet DHCP-Pakete mit Option-82-Information auf denjenigen Ports weiter, für die in Spalte ***DHCP-L2-Relay*** und in Spalte ***Gesicherter Port*** das Kontrollkästchen markiert ist. Typischerweise sind das Ports im Netz des DHCP-Servers.

Auf Ports, an denen die DHCP-Clients angeschlossen sind, aktivieren Sie die ***DHCP-L2-Relay***-Funktion, lassen das Kontrollkästchen in Spalte ***Gesicherter Port*** jedoch unmarkiert. Auf diesen Ports verwirft das Gerät DHCP-Pakete mit Option-82-Information.

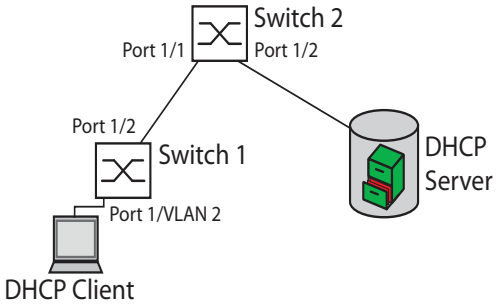


Abb. 43: Beispiel: DHCP-Schicht-2-Netz

Führen Sie an Switch 1 die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Erweitert > DHCP-L2-Relay > Konfiguration***, Registerkarte ***Interface***.
- ☐ Legen Sie die Einstellungen für Port `1/1` wie folgt fest:
  - Markieren Sie das Kontrollkästchen in Spalte ***Aktiv***.
- ☐ Legen Sie die Einstellungen für Port `1/2` wie folgt fest:
  - Markieren Sie das Kontrollkästchen in Spalte ***Aktiv***.
  - Markieren Sie das Kontrollkästchen in Spalte ***Gesicherter Port***.
- ☐ Öffnen Sie den Dialog ***Erweitert > DHCP-L2-Relay > Konfiguration***, Registerkarte ***VLAN***.
- ☐ Legen Sie die Einstellungen für VLAN 2 wie folgt fest:
  - Markieren Sie das Kontrollkästchen in Spalte ***Aktiv***.
  - Markieren Sie das Kontrollkästchen in Spalte ***Circuit-ID***.
  - Um als Remote-ID die IP-Adresse des Geräts zu verwenden, legen Sie in Spalte ***Remote-ID-Typ*** den Wert `ip` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen ***Funktion*** das Optionsfeld .
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

Führen Sie an Switch 2 die folgenden Schritte aus:

☐ Öffnen Sie den Dialog ***Erweitert > DHCP-L2-Relay > Konfiguration***, Registerkarte ***Interface***.

☐ Legen Sie die Einstellungen für Port `1/1` und Port `1/2` wie folgt fest:
- Markieren Sie das Kontrollkästchen in Spalte ***Aktiv***.
- Markieren Sie das Kontrollkästchen in Spalte ***Gesicherter Port***.

☐ Um die Funktion einzuschalten, wählen Sie im Rahmen ***Funktion*** das Optionsfeld .

☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche .

Vergewissern Sie sich, dass VLAN 2 vorhanden ist, und führen Sie anschließend die folgenden Schritte an Switch 1 aus:

☐ Richten Sie das VLAN 2 ein und legen Sie Port `1/1` als Mitglied des VLAN 2 fest.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`dhcp-l2relay circuit-id 2`	Aktivieren der Circuit-ID und der DHCP-Option-82 in VLAN `2`.
`dhcp-l2relay remote-id ip 2`	Festlegen der IP-Adresse des Geräts als Remote-ID in VLAN `2`.
`dhcp-l2relay mode 2`	Aktivieren der ***DHCP-L2-Relay***-Funktion in VLAN `2`.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`dhcp-l2relay mode`	Aktivieren der ***DHCP-L2-Relay***-Funktion auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`dhcp-l2relay trust`	Festlegen des Ports als ***Gesicherter Port***.
`dhcp-l2relay mode`	Aktivieren der ***DHCP-L2-Relay***-Funktion auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`dhcp-l2relay mode`	Einschalten der ***DHCP-L2-Relay***-Funktion auf dem Gerät.

Führen Sie an Switch 2 die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`dhcp-l2relay trust`	Festlegen des Ports als ***Gesicherter Port***.
`dhcp-l2relay mode`	Aktivieren der ***DHCP-L2-Relay***-Funktion auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`dhcp-l2relay trust`	Festlegen des Ports als ***Gesicherter Port***.
`dhcp-l2relay mode`	Aktivieren der ***DHCP-L2-Relay***-Funktion auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`dhcp-l2relay mode`	Einschalten der ***DHCP-L2-Relay***-Funktion auf dem Gerät.

14.3 GARP

Das Generic Attribute Registration Protocol (*GARP*) wurde durch die IEEE definiert, um ein generisches Framework bereitzustellen, in welchem Switches Attributwerte registrieren und de-registrieren, zum Beispiel VLAN-Kennungen und Multicast-Gruppen-Mitgliedschaften.

Wird ein Attribut für einen Teilnehmer gemäß *GARP*-Funktion registriert oder deregistriert, wird der Teilnehmer auf der Grundlage spezifischer Regeln geändert. Bei den Teilnehmern handelt es sich um eine Reihe erreichbarer Endgeräte und Netzgeräte. Der definierte Satz von Teilnehmern zu einem bestimmten Zeitpunkt zusammen mit den zugehörigen Attributen stellt den Erreichbarkeitsbaum für die Teilmenge der Netztopologie dar. Das Gerät leitet die Datenpakete ausschließlich an die registrierten Endgeräte weiter. Durch die Registrierung von Stationen wird vermieden, dass versucht wird, Daten an nicht erreichbare Endgeräte zu senden.

14.3.1 GMRP konfigurieren

Das GARP Multicast Registration Protocol (*GMRP*) ist ein Generic Attribute Registration Protocol (*GARP*), das einen Mechanismus für die dynamische Registrierung von Gruppenmitgliedschaften durch Netzgeräte und Endgeräte bereitstellt. Die Geräte registrieren Informationen zur Gruppenmitgliedschaft mit den Geräten, die mit demselben LAN-Segment verbunden sind. Die *GARP*-Funktion bietet den Geräten außerdem die Möglichkeit, die Informationen über Netzgeräte hinweg zu verbreiten, die erweiterte Filterdienste unterstützen.

Anmerkung: Vergewissern Sie sich vor dem Einschalten der *GMRP*-Funktion, dass die *MMRP*-Funktion ausgeschaltet ist.

Das folgende Beispiel beschreibt die Konfiguration der *GMRP*-Funktion. Das Gerät unterstützt eingeschränktes Mulitcast-Flooding für einen ausgewählten Port.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > GARP > GMRP*.
- ☐ Um eingeschränktes Multicast Flooding an einem Port auszuführen, markieren Sie das Kontrollkästchen in Spalte *GMRP aktiv*.
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`garp gmrp operation`	Einschalten der *GMRP*-Funktion auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`garp gmrp operation`	Globales Einschalten der *GMRP*-Funktion.

14.3.2 GVRP konfigurieren

Verwenden Sie die ***GVRP***-Funktion, um dem Gerät das Austauschen von VLAN-Konfigurationsinformationen mit anderen ***GVRP***-Geräten zu ermöglichen. Auf diese Weise reduziert das Gerät unnötigen Broadcast-Verkehr und unbekannten Unicast-Verkehr. Außerdem erzeugt und verwaltet die ***GVRP***-Funktion dynamisch VLANs auf Geräten, die über 802.1Q-Trunk-Ports angeschlossen sind.

Das folgende Beispiel beschreibt die Konfiguration der ***GVRP***-Funktion. Das Gerät bietet Ihnen die Möglichkeit, VLAN-Konfigurationsinformationen mit anderen ***GVRP***-Geräten auszutauschen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog ***Switching > GARP > GVRP***.
- ☐ Um VLAN-Konfigurationsinformationen mit anderen ***GVRP***-Geräten auszutauschen, markieren Sie das Kontrollkästchen in Spalte ***GVRP aktiv*** für den Port.
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 3/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `3/1`.
`garp gvrp operation`	Einschalten der ***GVRP***-Funktion auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`garp gvrp operation`	Globales Einschalten der ***GVRP***-Funktion.

14.4 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.

14.4.1 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-Emty(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.

14.4.2 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: ≥ (2x 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.

14.4.3 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.

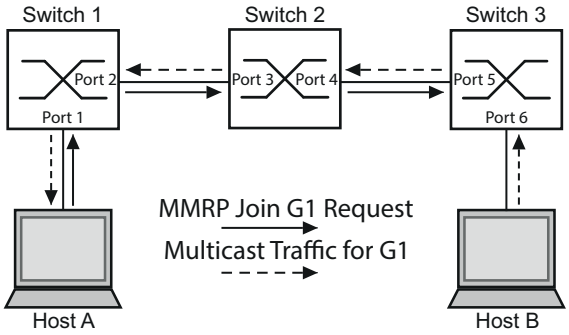


Abb. 44: MMRP-Netz für MAC-Adressen-Registrierung

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 zwischenzuspeichern, 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.

`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 mmrp operation`	Einschalten der *MMRP*-Funktion auf dem Port.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
`mrp-ieee mmrp operation`	Einschalten der *MMRP*-Funktion auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`mrp-ieee mrp periodic-state-machine`	Globales Einschalten der *Periodische State-Machine*-Funktion.
`mrp-ieee mmrp operation`	Globales Einschalten der *MMRP*-Funktion.

14.4.4 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-Registration-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.

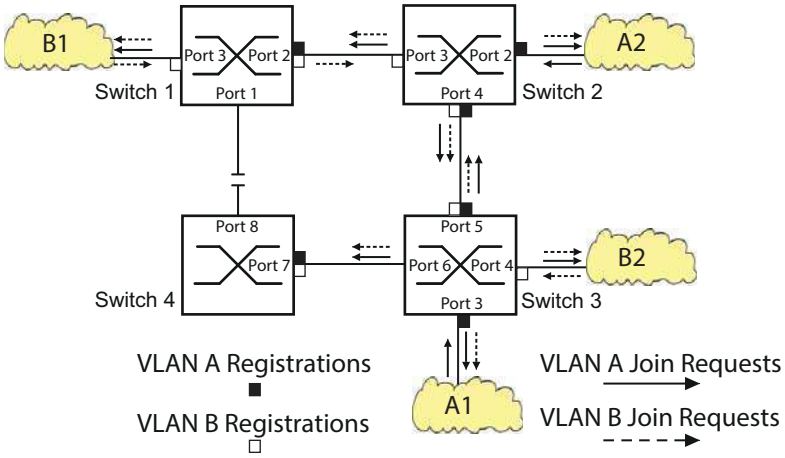


Abb. 45: MVRP-Beispiel-Netz für VLAN-Registrierung

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 ***MVRP***-Funktion auf dem Port.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
`mrp-ieee mvrp operation`	Einschalten der ***MVRP***-Funktion auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`mrp-ieee mvrp periodic-state-machine`	Globales Einschalten der ***Periodische State-Machine***-Funktion.
`mrp-ieee mvrp operation`	Globales Einschalten der ***MVRP***-Funktion.

14.5 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.

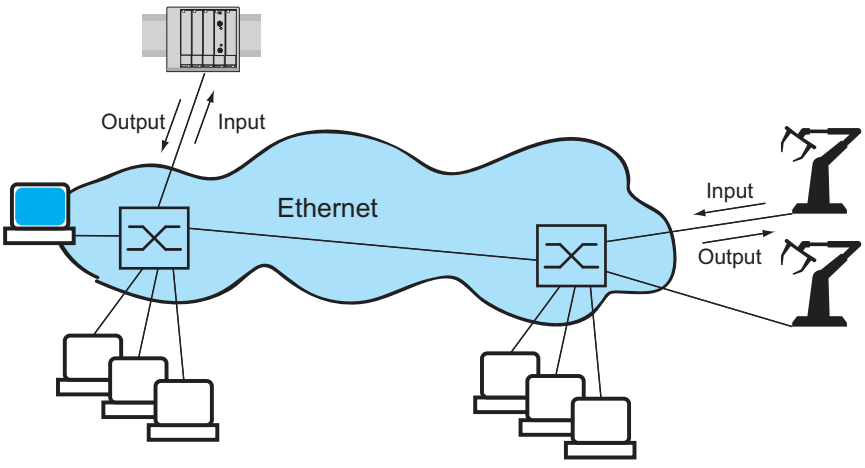


Abb. 46: Beispiel für die Kommunikation.

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.

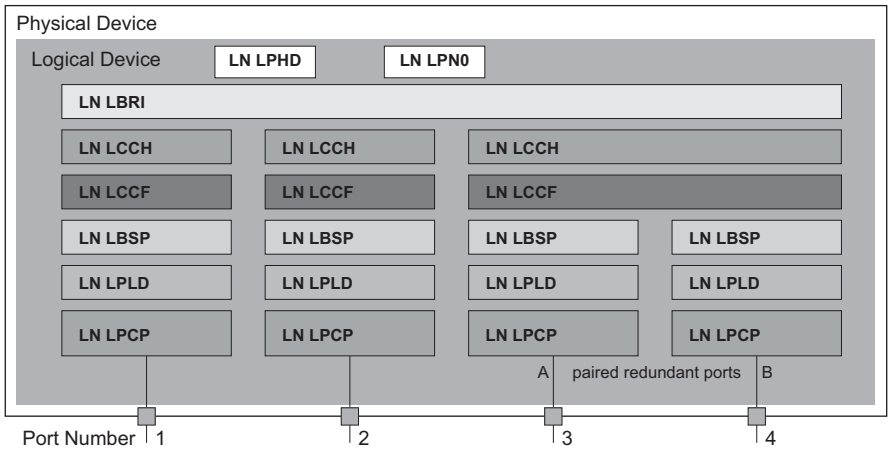


Abb. 47: Bridge-Modell nach Technical Report IEC 61850 90-4

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

Tab. 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 LPHD	TmpAlm	Ändert sich, wenn die im Gerät gemessene Temperatur die festgelegten Temperaturschwellen über- oder unterschreitet.
	PhyHealth	Ändert sich, wenn sich der Status der RCB-Objekte LPHD.TmpAlm ändert.
LN LPHD	TmpAlm	Ändert sich, wenn die im Gerät gemessene Temperatur die festgelegten Temperaturschwellen über- oder unterschreitet.
	PwrSupAlm	Ändert sich, wenn eine der redundanten Spannungsversorgungen ausfällt oder wieder in Betrieb geht.
	PhyHealth	Ändert sich, wenn sich der Status der RCB-Objekte LPHD.PwrSupAlm oder LPHD.TmpAlm ändert.
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:

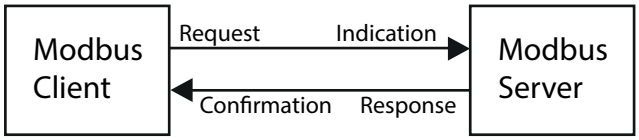


Abb. 48: Modbus TCP/IP Client/Server-Modus

- 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 `0x03Read Holding Registers` und `0x05Write 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***.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network management access add 2`	Erzeugt den Eintrag für den Adressbereich im Netz. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: `2`.
`network management access modify 2 ip 10.17.1.0`	Legt die IP-Adresse fest.
`network management access modify 2 mask 29`	Legt die Netzmaske fest.
`network management access modify 2 modbus-tcp enable`	Legt fest, dass ***Modbus TCP*** Verwaltungszugriff hat.
`network management access operation`	Schaltet die IP-Zugriffsbeschränkung ein.
`configure`	Wechsel in den Konfigurationsmodus.
`security-status monitor modbus-tcp-enabled`	Legt fest, dass das Gerät die Aktivierung des ***Modbus TCP***-Servers überwacht.
`modbus-tcp operation`	Schaltet den ***Modbus TCP***-Server ein.
`modbus-tcp port <1..65535>`	Den TCP-Port für die ***Modbus TCP***-Kommunikation festlegen (optional). Voreingestellt ist Port `502`.
`show modbus-tcp`	Die ***Modbus TCP***-Server-Einstellungen anzeigen.

```
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`	Zeigen Sie alle Sicherheitsstatus-Einstellungen.

```
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`	Die aufgetretenen Sicherheitsstatus-Ereignisse anzeigen.

```
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]
```

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***.

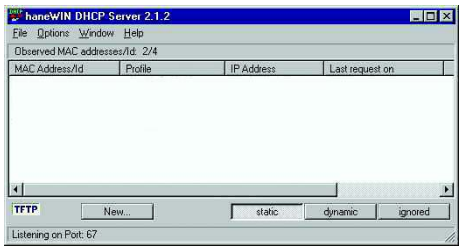


Abb. 49: Startfenster des Programms ***haneWIN DHCP-Server***

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*.

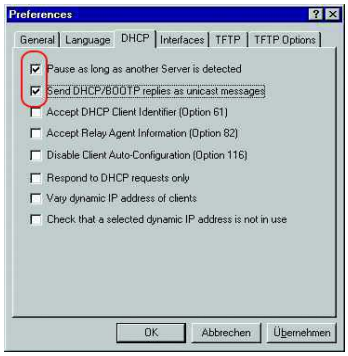


Abb. 50: DHCP-Einstellung

☐ 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*.

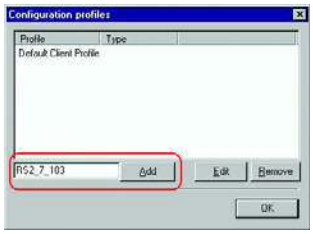


Abb. 51: Konfigurationsprofile hinzufügen

☐ Legen Sie die Netzmaske fest.

☐ Klicken Sie die Schaltfläche *Übernehmen*.

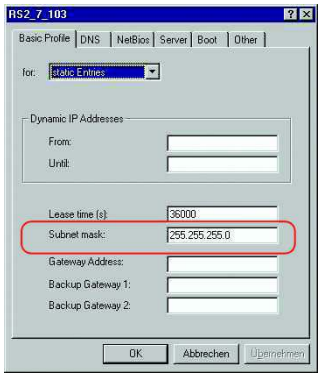


Abb. 52: Netzmaske im Konfigurationsprofil

☐ Wählen Sie die Registerkarte *Boot*.

☐ Geben Sie die IP-Adresse Ihres tftp-Servers.

☐ Geben Sie den Pfad und den Dateinamen für die Konfigurationsdatei ein.

☐ Klicken Sie die Schaltfläche *Übernehmen* und dann den Eintrag *OK*.

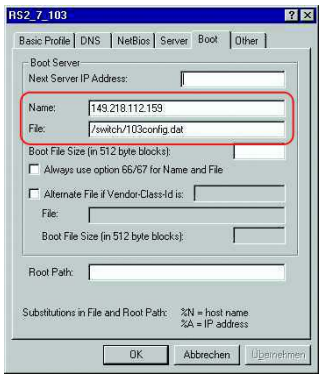


Abb. 53: Konfigurationsdatei auf dem tftp-Server

☐ 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. 54: Konfigurationsprofile verwalten

☐ Zur Eingabe der statischen Adressen klicken Sie im Hauptfenster die Schaltfläche *Statisch*.

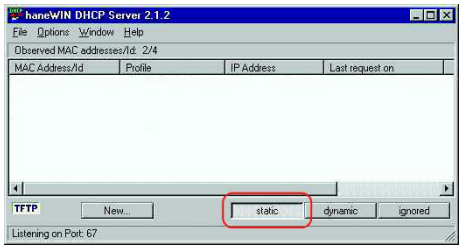


Abb. 55: Statische Adresseingabe

☐ Klicken Sie die Schaltfläche *Hinzufügen*.

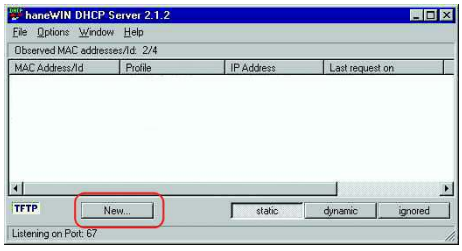


Abb. 56: Statische Adressen hinzufügen

☐ 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*.

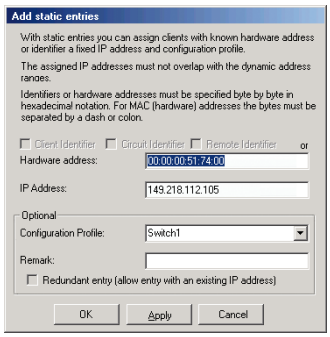


Abb. 57: Einträge für statische Adressen

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

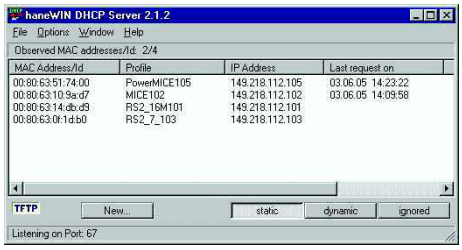


Abb. 58: DHCP-Server mit Einträgen

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***.

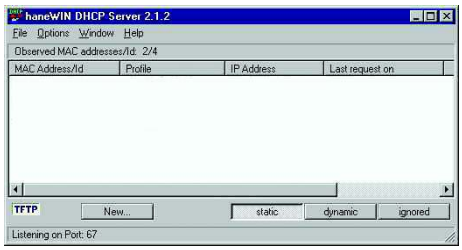


Abb. 59: Startfenster des Programms ***haneWIN DHCP-Server***

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.

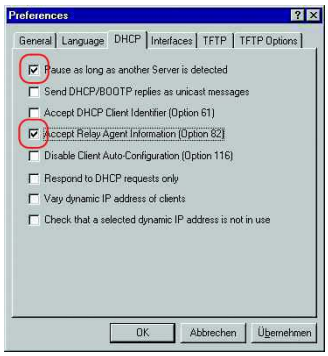


Abb. 60: DHCP-Einstellung

☐ Zur Eingabe der statischen Adressen klicken Sie die Schaltfläche ***Hinzufügen***.

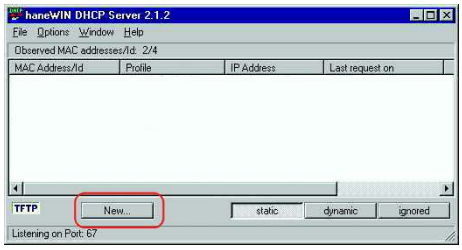


Abb. 61: Statische Adressen hinzufügen

☐ Markieren Sie das Kontrollkästchen ***Circuit Identifier***.

☐ Markieren Sie das Kontrollkästchen ***Remote Identifier***.

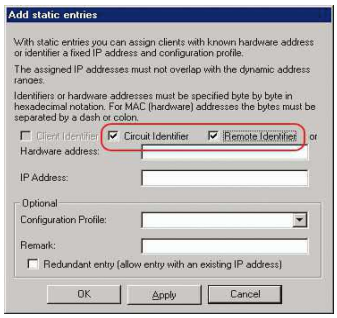


Abb. 62: Voreinstellung für die feste Adresszuweisung

☐ 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:
`ciclhhvvvvssmmpprirlxxxxxxxxxxxx`

- `ci`
  Subidentifier für den Typ der Circuit-ID.
- `cl`
  Länge der Circuit-ID.
- `hh`
  Hirschmann-Identifier:
  `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`
  Subidentifier 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.

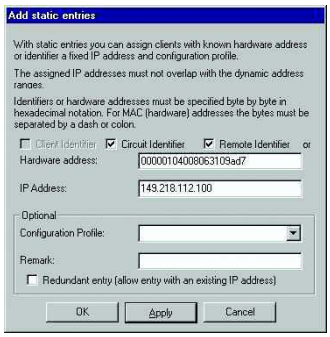


Abb. 63: Festlegen der Adressen

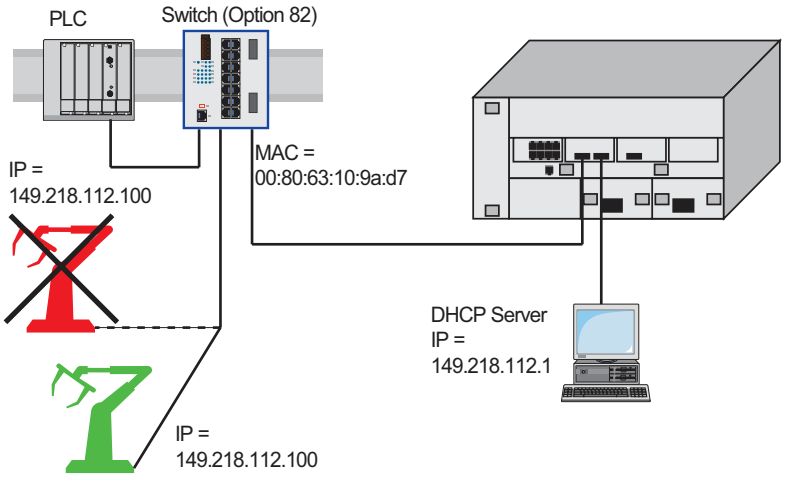


Abb. 64: Anwendungsbeispiel für den Einsatz von Option 82

A.3 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.3.1 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 zwischenzuspeichern, 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 zwischenzuspeichern, klicken Sie die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ssh key dsa generate`	Erzeugen eines neuen DSA-Schlüssels.

A.3.2 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`	Wechsel in den Privileged-EXEC-Modus.
`copy sshkey envm <file name>`	Eigenen Schlüssel vom externen Speicher in das Gerät laden.

A.3.3 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.

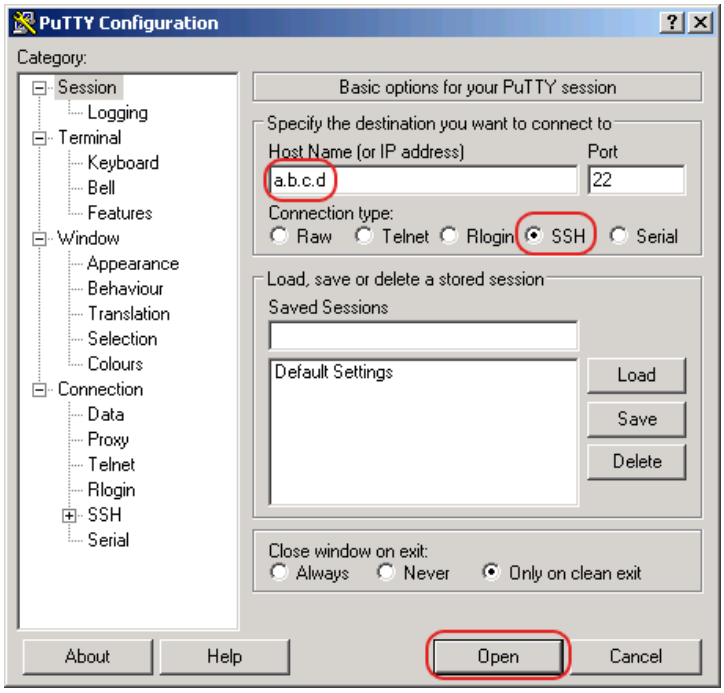


Abb. 65: PuTTY-Eingabemaske

☐ 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. 66: 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.4 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.4.1 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 zwischenzuspeichern, 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 ***HTTPS***-Funktion.
`https server`	Einschalten der ***HTTPS***-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 zwischenzuspeichern, 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`	Ausschalten der ***HTTPS***-Funktion.
`https server`	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.4.2 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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`https port 443`	Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTPS-Anfragen von den Clients entgegennimmt.
`https server`	Einschalten der ***HTTPS***-Funktion.
`show https`	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 Subidentifier (SID) werden sie instanziert.

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 Subidentifiers `2` wird diese abstrakte Information auf die Wirklichkeit abgebildet, instanziert, und bezeichnet so den Betriebszustand des Netzteils `2`. Diese Instanz bekommt einen Wert zugewiesen, der gelesen werden kann. Damit liefert die Instanz `get 1.3.6.1.4.1.248.11.11.1.1.1.1.2.1` 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.

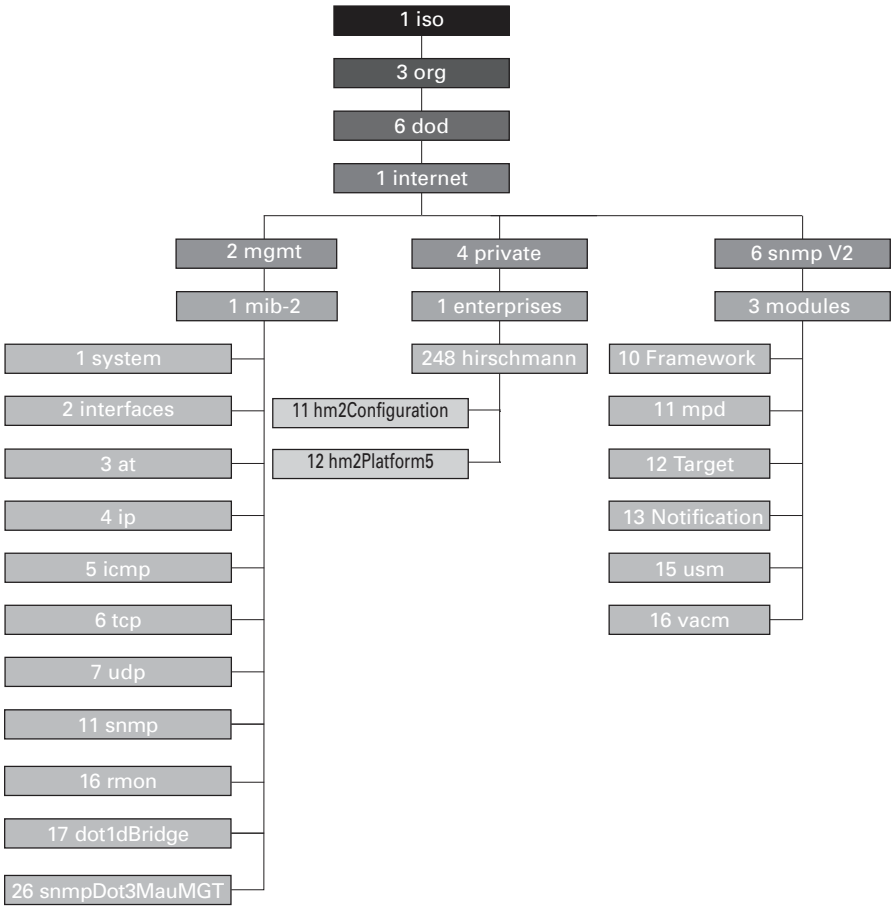


Abb. 67: Baumstruktur der Hirschmann-MIB

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 MRP – Media Redundancy Protocol based on a ring topology

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)	16384
Max. Anzahl statisch konfigurierter MAC-Adressfilter	100
Max. Anzahl der mit IGMP-Snooping lernbaren MAC-Adressfilter	512
Max. Anzahl der MAC-Adresseinträge (MMRP)	64
Anzahl Warteschlangen	8 Queues
Einstellbare Port-Prioritäten	0..7

VLAN	
VLAN-ID-Bereich	1..4042
Anzahl der VLANs	max. 128 gleichzeitig pro Gerät max. 128 gleichzeitig pro Port

Access-Control-Listen (ACL)	
Max. Anzahl der ACLs	50
Max. Anzahl der Regeln pro Port	18
Max. Anzahl der Regeln pro ACL	18
Anzahl der insgesamt konfigurierbaren Regeln	900 (50x18)
Max. Anzahl der VLAN-Zuweisungen (in)	12
Max. Anzahl der Regeln, die ein Ereignis protokollieren	900 (50x18)
Max. Anzahl der Ingress-Regeln	18

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 60, 269
Advanced Mode 150, 152
Aging-Time 114
Alarm 183
Alarmnachrichten 180
Alternate-Port 164, 170
APNIC 30
ARIN 30
ARP 32
Authentifizierungs-Liste 46
Automatische Konfiguration 81

B
Backup-Port 164, 170
Bandbreite 128
Baumstruktur (Spanning Tree) 159, 163
Benutzernamen 21, 23, 25
Berechtigungen 49
Bericht 205
BOOTP 29
BPDU 159
BPDU Guard 169, 170
Bridge Identifier 156
Bridge Protocol Data Unit 159

C
CDROM 244, 248
CIDR 33
Classless Inter Domain Routing 33
Command Line Interface 19

D
Datenverkehr 93
Denial of Service 94
Denial-of-Service 93
Designated Bridge 164
Designated Port 164, 169
DHCP 29
DHCP-L2-Relay 221
DHCP-Server 102, 105, 244, 248
Diameter (Spanning Tree) 158
DiffServ 119
Disabled-Port 164
DoS 93, 94
DSCP 119, 126

E
Echtzeit 119
Edge-Port 164, 169
Ereignisprotokoll 208
Erstinstallation 29

F
Fast\ MRP 148
FAQ 273
Ferndiagnose 191
Flusskontrolle 128
Flüchtiger Speicher (RAM) 59
Funktionsüberwachung 191

G
Gateway 31, 35
GARP 224
Generische Objektklassen 260
Gerätestatus 184
GMRP 224
Grafische Benutzeroberfläche starten 18

H
HaneWin 244, 248
Hardware-Reset 180
HiDiscovery 29, 34, 36, 38, 83, 88, 188, 209, 241
Hostadresse 30

I
IANA 30
IAS 46
IEC 61850 234
IEEE 802.1X 46
IEEE-MAC-Adresse 201
IGMP-Snooping 113, 113
Industrial HiVision 11, 40, 56
Instanzierung 260
Integrated authentication server 46
IP-Adresse 30, 35, 40
IP-Header 119, 122
ISO/OSI-Schichtenmodell 32

K
Kompatibilität (STP) 167
Konfigurationsänderungen 180
Konfigurationsdatei 40

L
LACNIC 30
Leave-Nachricht 114
Link Aggration 148
Link-Überwachung 184, 191
Login-Seite 18
Loop Guard 170, 171

M
MaxAge 158
MAC-Adressen-Filter 110
MAC-Zieladresse 32
MMS 234
Modus 81
MRP 147, 148, 149, 150
Multicast 113

N
Nachricht 180
Netzlast 155, 156
Netzmanagement 40
Netzmaske 31, 35
NVM (permanenter Speicher) 59

O

Object Description 260
Object-ID 260
Objektklassen 260
OpenSSH-Suite 23
Option 82 248

P

Passwort 21, 23, 25
Permanenter Speicher (NVM) 59
Pfadkosten 157, 159
Polling 180
Portnummer 157
Port-Identifikation 156, 157
Port-Mirroring 211
Port-Priorität 125
Port-Priorität (Spanning Tree) 157
Port-Rollen (RSTP) 164
Port-Status 165
Priorität 121
Priority Tagged Frames 121
PuTTY 19

Q

QoS 120
Query 113

R

Rapid Spanning Tree 147, 147, 148, 164
RADIUS 46
RAM (flüchtiger Speicher) 59
Redundanz 155
Referenzzeitquelle 102, 105
Rekonfiguration 156
Rekonfigurationszeit (MRP) 150
Relaiskontakt 191
Report-Nachricht 113
RFC 262
Ring 149
Ring-Manager 149
RIPE NCC 30
RMON-Probe 211
RM-Funktion 149
Root Bridge 159
Root Guard 169, 171
Root-Pfad 161, 162
Root-Pfadkosten 156
Root-Port 164, 170
Router 31
RSTP 167
RST BPDU 164, 166
Ruhestromschaltung 191

S

Schulungsangebote 273
Schutzfunktionen (Guards) 169
Secure Shell 19, 22
Secure Shell 19
Segmentierung 180
Service 205
Service-Shell-Funktion reaktivieren 58
SFP-Modul 200
Signalkontakt 191
SNMP 180
SNMP-Trap 180, 183
SNTP 101
Software-Version 73
Sommerzeitumschaltung 103
SSH 19, 19, 22
STP-BPDU 159
STP-Kompatibilität 167
Store and Forward 110
Strict-Priority 122
Subidentifier 260
Subnetz 35
Systemanforderungen (GUI) 18

T

TCN Guard 169, 171
Technische Fragen 273
Topology-Change-Flag 169
ToS 119, 122
Trap 180, 183
Trap-Ziel-Tabelle 180
Type of Service 122

U

Uhrzeit einstellen 102
Update 26
Übertragungssicherheit 180

V

Verkehrsklasse 122, 126
Verzögerungszeit (MRP) 150
Video 122
VLAN 131
VLAN-Priorität 125
VLAN-Tag 121, 131
VoIP 122
VT100 24
V.24 19, 24

W

Warteschlange 122
Weighted Fair Queuing 123
Weighted Round Robin 123

Z

Ziel-Tabelle 180
Zugangsschutz 80

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**	**befriedi-gend**	**mäßig**	**schlecht**
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

Haben Sie in diesem Handbuch Fehler entdeckt?
Wenn ja, welche auf welcher Seite?

Anregungen, Verbesserungsvorschläge, Ergänzungsvorschläge:

Allgemeine Kommentare:

Absender:

Firma / Abteilung:

Name / Telefonnummer:

Straße:

PLZ / Ort:

E-Mail:

Datum / Unterschrift:

Sehr geehrter Anwender,

Bitte schicken Sie dieses Blatt ausgefüllt zurück

- als Fax an die Nummer +49 (0)7127 14-1600 oder
- per Post an

  Hirschmann Automation and Control GmbH
  Abteilung 01RD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen

HIRSCHMANN

A BELDEN BRAND