HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

MSP HiOS-2A Rel. 09000

Referenz-Handbuch

Grafische Benutzeroberfläche

Anwender-Handbuch

Konfiguration

Referenz-Handbuch

Grafische Benutzeroberfläche
MICE Switch Power MSP30
HiOS-2A

Technische Unterstützung
https://hirschmann-support.belden.com

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.

© 2021 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken.

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

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

Die aktuelle Benutzerdokumentation für Ihr Gerät finden Sie unter: doc.hirschmann.com

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

Inhalt

Sicherheitshinweise . . . 9

Über dieses Handbuch . . . 11

Legende . . . 12

Hinweise zur grafischen Benutzeroberfläche . . . 13
Banner . . . 13
Menübereich . . . 15
Dialogbereich . . . 17

1 Grundeinstellungen . . . 21
1.1 System . . . 21
1.2 Module . . . 27
1.3 Netz . . . 29
1.3.1 Global . . . 30
1.3.2 IPv4 . . . 32
1.4 Software . . . 34
1.5 Laden/Speichern . . . 38
1.6 Externer Speicher . . . 51
1.7 Port . . . 55
1.8 Power over Ethernet . . . 61
1.8.1 PoE Global . . . 63
1.8.2 PoE Port . . . 66
1.9 Neustart . . . 69

2 Zeit . . . 73
2.1 Grundeinstellungen . . . 73
2.2 SNTP . . . 77
2.2.1 SNTP Client . . . 78
2.2.2 SNTP Server . . . 82
2.3 PTP . . . 84
2.3.1 PTP Global . . . 85
2.3.2 PTP Boundary Clock . . . 87
2.3.2.1 PTP Boundary Clock Global . . . 88
2.3.2.2 PTP Boundary Clock Port . . . 93
2.3.3 PTP Transparent Clock . . . 97
2.3.3.1 PTP Transparent Clock Global . . . 98
2.3.3.2 PTP Transparent Clock Port . . . 102

3 Gerätesicherheit . . . 105
3.1 Benutzerverwaltung . . . 105
3.2 Authentifizierungs-Liste . . . 111
3.3 LDAP . . . 114
3.3.1 LDAP Konfiguration . . . 115
3.3.2 LDAP Rollen-Zuweisung . . . 120
3.4 Management-Zugriff . . . 122

3.4.1 Server . . . 123
3.4.2 IP-Zugriffsbeschränkung . . . 136
3.4.3 Web . . . 140
3.4.4 Command Line Interface . . . 141
3.4.5 SNMPv1/v2 Community . . . 143
3.5 Pre-Login-Banner . . . 144

4 Netzsicherheit . . . 145
4.1 Netzsicherheit Übersicht . . . 145
4.2 Port-Sicherheit . . . 147
4.3 802.1X Port-Authentifizierung . . . 152
4.3.1 802.1X Global . . . 153
4.3.2 802.1X Port-Konfiguration . . . 156
4.3.3 802.1X Port-Clients . . . 162
4.3.4 802.1X EAPOL-Portstatistiken . . . 164
4.3.5 802.1X Port-Authentifizierung-Historie . . . 166
4.3.6 802.1X Integrierter Authentifikations-Server . . . 168
4.4 RADIUS . . . 169
4.4.1 RADIUS Global . . . 170
4.4.2 RADIUS Authentication-Server . . . 172
4.4.3 RADIUS Accounting-Server . . . 174
4.4.4 RADIUS Authentication Statistiken . . . 176
4.4.5 RADIUS Accounting-Statistiken . . . 178
4.5 DoS . . . 179
4.5.1 DoS Global . . . 180
4.6 DHCP-Snooping . . . 183
4.6.1 DHCP-Snooping Global . . . 185
4.6.2 DHCP-Snooping Konfiguration . . . 187
4.6.3 DHCP-Snooping Statistiken . . . 191
4.6.4 DHCP-Snooping Bindings . . . 192
4.7 IP Source Guard . . . 193
4.7.1 IP Source Guard Port . . . 195
4.7.2 IP Source Guard Bindings . . . 196
4.8 Dynamic ARP Inspection . . . 197
4.8.1 Dynamic-ARP-Inspection Global . . . 199
4.8.2 Dynamic-ARP-Inspection Konfiguration . . . 201
4.8.3 Dynamic-ARP-Inspection ARP-Regeln . . . 205
4.8.4 Dynamic-ARP-Inspection Statistiken . . . 207
4.9 ACL . . . 208
4.9.1 ACL IPv4-Regel . . . 209
4.9.2 ACL MAC-Regel . . . 218
4.9.3 ACL Zuweisung . . . 224
4.9.4 ACL Zeitprofil . . . 227

5 Switching . . . 231
5.1 Switching Global . . . 231
5.2 Lastbegrenzer . . . 234
5.3 Filter für MAC-Adressen . . . 237

5.4 IGMP-Snooping . . . 239
5.4.1 IGMP-Snooping Global . . . 240
5.4.2 IGMP-Snooping Konfiguration . . . 242
5.4.3 IGMP-Snooping Erweiterungen . . . 246
5.4.4 IGMP Snooping-Querier . . . 249
5.4.5 IGMP Snooping Multicasts . . . 252
5.5 MRP-IEEE . . . 253
5.5.1 MRP-IEEE Konfiguration . . . 254
5.5.2 MRP-IEEE Multiple MAC Registration Protocol . . . 255
5.5.3 MRP-IEEE Multiple VLAN Registration Protocol . . . 260
5.6 GARP . . . 263
5.6.1 GMRP . . . 264
5.6.2 GVRP . . . 266
5.7 QoS/Priority . . . 267
5.7.1 QoS/Priority Global . . . 268
5.7.2 QoS/Priorität Port-Konfiguration . . . 269
5.7.3 802.1D/p Zuweisung . . . 271
5.7.4 IP-DSCP-Zuweisung . . . 273
5.7.5 Queue-Management . . . 275
5.7.6 DiffServ . . . 276
5.7.6.1 DiffServ Übersicht . . . 278
5.7.6.2 DiffServ Global . . . 280
5.7.6.3 DiffServ Klasse . . . 281
5.7.6.4 DiffServ Richtlinie . . . 288
5.7.6.5 DiffServ Zuweisung . . . 298
5.8 VLAN . . . 299
5.8.1 VLAN Global . . . 301
5.8.2 VLAN Konfiguration . . . 302
5.8.3 VLAN Port . . . 304
5.8.4 VLAN Voice . . . 306
5.8.5 MAC-basiertes VLAN . . . 309
5.8.6 Subnet-basiertes VLAN . . . 310
5.8.7 Protokoll-basiertes VLAN . . . 311
5.9 L2-Redundanz . . . 312
5.9.1 MRP . . . 313
5.9.2 HIPER-Ring . . . 317
5.9.3 Spanning Tree . . . 318
5.9.3.1 Spanning Tree Global . . . 320
5.9.3.2 Spanning Tree MSTP . . . 327
5.9.3.3 Spanning Tree Port . . . 332
5.9.4 Link-Aggregation . . . 341
5.9.5 Link-Backup . . . 349
5.9.6 FuseNet . . . 352
5.9.6.1 Sub Ring . . . 354
5.9.6.2 Ring-/Netzkopplung . . . 359
5.9.6.3 Redundant Coupling Protocol . . . 365

6 Diagnose . . . 369
6.1 Statuskonfiguration . . . 369
6.1.1 Gerätestatus . . . 370
6.1.2 Sicherheitsstatus . . . 375
6.1.3 Signalkontakt . . . 383
6.1.3.1 Signalkontakt 1 / Signalkontakt 2 . . . 384
6.1.4 MAC-Benachrichtigung . . . 389
6.1.5 Alarme (Traps) . . . 392
6.2 System . . . 394
6.2.1 Systeminformationen . . . 395
6.2.2 Hardware-Zustand . . . 396
6.2.3 Konfigurations-Check . . . 397
6.2.4 IP-Adressen Konflikterkennung . . . 399
6.2.5 ARP . . . 403
6.2.6 Selbsttest . . . 404
6.3 E-Mail-Benachrichtigung . . . 406
6.3.1 E-Mail-Benachrichtigung Global . . . 407
6.3.2 E-Mail-Benachrichtigung Empfänger . . . 412
6.3.3 E-Mail-Benachrichtigung Mail-Server . . . 413
6.4 Syslog . . . 415
6.5 Ports . . . 419
6.5.1 SFP . . . 420
6.5.2 TP-Kabeldiagnose . . . 421
6.5.3 Port-Monitor . . . 423
6.5.4 Auto-Disable . . . 433
6.5.5 Port-Mirroring . . . 437
6.6 LLDP . . . 441
6.6.1 LLDP Konfiguration . . . 442
6.6.2 LLDP Topologie-Erkennung . . . 446
6.7 Loop-Schutz . . . 450
6.8 SFlow . . . 454
6.8.1 SFlow-Konfiguration . . . 455
6.8.2 SFlow Empfänger . . . 457
6.9 Bericht . . . 458
6.9.1 Bericht Global . . . 459
6.9.2 Persistentes Ereignisprotokoll . . . 464
6.9.3 System-Log . . . 467
6.9.4 Audit-Trail . . . 468

7 Erweitert . . . 469
7.1 DHCP-L2-Relay . . . 469
7.1.1 DHCP-L2-Relay Konfiguration . . . 470
7.1.2 DHCP-L2-Relay Statistiken . . . 473
7.2 DHCP Server . . . 474
7.2.1 DHCP-Server Global . . . 475
7.2.2 DHCP-Server Pool . . . 477
7.2.3 DHCP-Server Lease-Tabelle . . . 481

7.3 DNS 482
7.3.1 DNS-Client 482
7.3.1.1 DNS-Client Global 483
7.3.1.2 DNS-Client Aktuell 484
7.3.1.3 DNS-Client Statisch 485
7.3.1.4 DNS-Client Statische Hosts 487
7.4 Industrie-Protokolle 488
7.4.1 IEC61850-MMS 489
7.4.2 Modbus TCP 492
7.4.3 EtherNet/IP. 494
7.4.4 OPC UA Server 495
7.4.5 PROFINET 498
7.5 Digital-IO Modul 501
7.6 Command Line Interface 507

A **Stichwortverzeichnis** 509

B **Weitere Unterstützung** 515

C **Leserkritik** 516

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.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Über dieses Handbuch

Das Anwender-Handbuch „Konfiguration“ 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 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 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
Verweis	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	Darstellung eines CLI-Kommandos oder des Feldinhalts in der grafischen Benutzeroberfläche

Auszuführen in der grafische Benutzeroberfläche

Auszuführen im Command Line Interface

Hinweise zur grafischen Benutzeroberfläche

Voraussetzung für den Zugriff auf die grafische Benutzeroberfläche des Geräts ist ein Webbrowser mit HTML5-Unterstützung.

Die responsive grafische Benutzeroberfläche passt sich automatisch an die Größe Ihres Bildschirms an. Demzufolge können Sie auf einem großen, hochauflösenden Bildschirm mehr Details sehen als auf einem kleinen Bildschirm. Auf einem hochauflösenden Bildschirm haben die Schaltflächen zum Beispiel eine Beschriftung neben dem Symbol. Auf einem Bildschirm mit geringer Breite zeigt die grafische Benutzeroberfläche lediglich das Symbol.

Anmerkung: Auf einem konventionellen Bildschirm klicken Sie, um zu navigieren. Auf einem Gerät mit Touchscreen hingegen tippen Sie. Der Einfachheit halber verwenden wir in unseren Hilfetexten lediglich „Klicken“.

Die grafische Benutzeroberfläche ist wie folgt unterteilt:
- Banner
- Menübereich
- Dialogbereich

Banner

Das Banner zeigt die folgenden Informationen:

Blendet das Menü ein und wieder aus. Wenn das Fenster des Webbrowsers zu schmal ist, zeigt das Banner die Schaltfläche.

Hersteller-Logo

Klicken Sie auf das Logo, um die Website des Herstellers in einem neuen Fenster zu öffnen.

Name des Dialogs

Zeigt den Namen des gegenwärtig im Dialogbereich angezeigten Dialogs.

Zeigt, dass die grafische Benutzeroberfläche das Gerät nicht erreichen kann. Die Verbindung zum Gerät ist unterbrochen.

Zeigt, ob die Einstellungen im flüchtigen Speicher (*RAM*) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (*NVM*) abweichen. Das Banner zeigt das Symbol, sobald Sie die Änderungen in den flüchtigen Speicher (*RAM*) übertragen, diese jedoch noch nicht im permanenten Speicher (*NVM*) gespeichert haben.

Wenn Sie die Schaltfläche klicken, öffnet sich die Online-Hilfe in einem neuen Fenster.

Wenn Sie die Schaltfläche klicken, zeigt ein Tooltip die folgenden Informationen:

- Die Zusammenfassung des Rahmens *Geräte-Status*. Siehe Dialog *Grundeinstellungen > System*.
- Die Zusammenfassung des Rahmens *Sicherheits-Status*. Siehe Dialog *Grundeinstellungen >* System.
- Die Zusammenfassung des Rahmens *Information*. Siehe Dialog *Diagnose > System > Konfigurations-Check*.

Ein roter Punkt neben dem Symbol bedeutet, dass mindestens einer der Werte größer ist als `0`.

Wenn Sie die Schaltfläche klicken, öffnet sich ein Untermenü mit den folgenden Menüeinträgen:

- Name des Benutzerkontos
  Kontoname des Benutzers, der gegenwärtig angemeldet ist.
- Schaltfläche *Abmelden*
  Wenn Sie die Schaltfläche klicken, meldet dies den gegenwärtig angemeldeten Benutzer ab. Danach öffnet sich der Login-Dialog.

Menübereich

Die grafische Benutzeroberfläche blendet den Menübereich aus, wenn das Fenster des Webbrowsers zu schmal ist. Um den Menübereich anzuzeigen, klicken Sie im Banner auf die Schaltfläche ☰.

Der Menübereich ist wie folgt unterteilt:
- Symbolleiste
- Menübaum

Symbolleiste

Die Symbolleiste zeigt die folgenden Informationen:

Geräte-Software

Zeigt Versionsnummer der Geräte-Software, die das Gerät beim letzten Neustart geladen hat und gegenwärtig ausführt.

🔍

Zeigt ein Textfeld, um nach einem Schlüsselwort zu suchen. Wenn Sie ein Zeichen oder eine Zeichenkette einfügen, zeigt der Menübaum ausschließlich für diejenigen Dialoge einen Menüeintrag an, die mit diesem Schlüsselwort in Zusammenhang stehen.

Der Menübaum zeigt ausschließlich für diejenigen Dialoge einen Menüeintrag an, in denen mindestens ein Parameter von der Voreinstellung abweicht (*Mit Werkseinstellung vergleichen*). Um den kompletten Menübaum wieder anzuzeigen, klicken Sie die Schaltfläche .

Klappt den Menübaum zu. Der Menübaum zeigt dann ausschließlich Menüeinträge der ersten Ebene.

Klappt den Menübaum auf. Der Menübaum zeigt dann jeden Menüeintrag auf jeder Ebene.

Menübaum

Der Menübaum enthält einen Eintrag für jeden Dialog in der grafischen Benutzeroberfläche. Wenn Sie einen Menüeintrag klicken, zeigt der Dialogbereich den zugehörigen Dialog. Sie können die Ansicht des Menübaums ändern, indem Sie die Schaltflächen in der Symbolleiste am oberen Rand klicken. Des Weiteren können Sie die Ansicht des Menübaums ändern, indem Sie die folgenden Schaltflächen klicken:

+

Klappt den aktuellen Menüeintrag auf und zeigt die Menüeinträge der nächsttieferen Ebene. Der Menübaum zeigt die Schaltfläche neben jedem zugeklappten Menüeintrag an, der Menüeinträge auf der nächsttieferen Ebene enthält.

–

Klappt den Menüeintrag zu und blendet die Menüeinträge der unteren Ebenen aus. Der Menübaum zeigt die Schaltfläche neben jedem aufgeklappten Menüeintrag.

Dialogbereich

Der Dialogbereich zeigt den Dialog, den Sie im Menübaum auswählen, einschließlich seiner Bedienelemente. Hier können Sie abhängig von Ihrer Zugriffsrolle die Einstellungen des Geräts überwachen und ändern.

Nachfolgend finden Sie nützliche Informationen zur Bedienung der Dialoge.

- Bedienelemente
- Änderungsmarkierung
- Standard-Schaltflächen
- Einstellungen speichern
- Anzeige aktualisieren
- Arbeiten mit Tabellen

Bedienelemente

Die Dialoge enthalten unterschiedliche Bedienelemente. Diese Bedienelemente sind abhängig vom Parameter und von Ihrer Zugriffsrolle als Benutzer schreibgeschützt oder editierbar.

Die Bedienelemente haben folgende visuellen Eigenschaften:

- Eingabefelder
  - Ein editierbares Eingabefeld hat am unteren Rand eine Linie.
  - Ein schreibgeschütztes Eingabefeld hat keine speziellen visuellen Eigenschaften.
- Kontrollkästchen
  - Ein editierbares Kontrollkästchen hat eine kräftige Farbe.
  - Ein schreibgeschütztes Kontrollkästchen hat eine graue Farbe.
- Optionsfelder
  - Ein editierbares Optionsfeld hat eine kräftige Farbe.
  - Ein schreibgeschütztes Optionsfeld hat eine graue Farbe.

Änderungsmarkierung

Wenn Sie einen Wert ändern, zeigt das betreffende Feld oder die Tabellenzelle ein rotes Dreieck in der linken oberen Ecke. Das rote Dreieck signalisiert, dass Sie Ihre Änderung noch nicht in den flüchtigen Speicher (*RAM*) des Geräts übertragen haben.

Standard-Schaltflächen

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

✓

Überträgt die Änderungen in den flüchtigen Speicher (*RAM*) des Geräts und wendet diese an.

Informationen darüber, wie das Gerät die geänderten Einstellungen auch nach einem Neustart beibehält, finden Sie im Abschnitt „Einstellungen speichern” auf Seite 18.

Verwirft nicht gespeicherte Änderungen im gegenwärtigen Dialog. Aktualisiert die Felder mit den Werten, die im flüchtigen Speicher (*RAM*) des Geräts gespeichert sind.

Einstellungen speichern

Das Speichern überträgt die geänderten Einstellungen in den flüchtigen Speicher (*RAM*) des Geräts. Führen Sie dazu den folgenden Schritt aus:

- Klicken Sie die Schaltfläche ✓.

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 Ihres PCs erreichbar bleibt. Wenn die Verbindung abbricht, dann lädt das Gerät nach der festgelegten Zeit das im permanenten Speicher (*NVM*) gespeicherte Konfigurationsprofil. Danach ist das Gerät wieder erreichbar.

Damit die geänderten Einstellungen auch nach dem Neustart des Geräts erhalten bleiben, führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- Markieren Sie in der Tabelle das Kontrollkästchen ganz links in der Zeile des gewünschten Konfigurationsprofils.
- Wenn das Kontrollkästchen in Spalte *Ausgewählt* unmarkiert ist, klicken Sie die Schaltfläche ☰ und dann den Eintrag *Auswählen*.
- Klicken Sie die Schaltfläche 💾, um die gegenwärtigen Änderungen zu speichern.

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.

Arbeiten mit Tabellen

Die Dialoge zeigen zahlreiche Einstellungen in tabellarischer Form. Sie haben die Möglichkeit, das Erscheinungsbild der Tabellen an Ihre Bedürfnisse anzupassen.

In den folgenden Abschnitten finden Sie nützliche Informationen zur Bedienung der Tabellen:

▶ Zeilen filtern
▶ Zeilen sortieren
▶ Mehrere Tabellenzeilen auswählen

Zeilen filtern

Der Filter ermöglicht Ihnen, die Anzahl der Zeilen in der Tabelle zu verringern.

Zeigt im Tabellenkopf eine zweite Zeile, die für jede Spalte ein Textfeld enthält. Wenn Sie in ein Feld eine Zeichenfolge einfügen, zeigt die Tabelle lediglich noch die Zeilen, welche in der betreffenden Spalte diese Zeichenfolge enthalten.

Zeilen sortieren

Jede Spalte im Tabellenkopf enthält ein Symbol, mit dem Sie die Reihenfolge der Tabellenzeilen ändern können.

Zeigt, dass die Zeilen der Tabelle anhand eines anderen Kriteriums sortiert sind als anhand der Werte in dieser Spalte.

Klicken Sie das Symbol, um die Zeilen der Tabelle anhand der Einträge in der betreffenden Spalte in absteigender Reihenfolge zu sortieren. Die ursprüngliche Sortierung in der Tabelle lässt sich möglicherweise erst nach dem Abmelden und erneuten Anmelden wiederherstellen.

Zeigt, dass die Zeilen der Tabelle anhand der Einträge der betreffenden Spalte in absteigender Reihenfolge sortiert sind.

Klicken Sie das Symbol, um die Zeilen der Tabelle anhand der Einträge in der betreffenden Spalte in aufsteigender Reihenfolge zu sortieren.

Zeigt, dass die Zeilen der Tabelle anhand der Einträge der betreffenden Spalte in aufsteigender Reihenfolge sortiert sind.

Klicken Sie das Symbol, um die Zeilen der Tabelle anhand der Einträge in der betreffenden Spalte in absteigender Reihenfolge zu sortieren.

Mehrere Tabellenzeilen auswählen

Sie haben die Möglichkeit, mehrere Tabellenzeilen auf einmal auszuwählen und eine Aktion auf diese anzuwenden. Dies ist nützlich, wenn Sie in der Tabelle zum Beispiel mehrere Zeilen gleichzeitig entfernen möchten.

Um in der Tabelle einzelne Zeilen auszuwählen, markieren Sie das Kontrollkästchen ganz links in der gewünschten Zeile.

Um in der Tabelle jede Zeile auszuwählen, markieren Sie das Kontrollkästchen ganz links im Tabellenkopf.

1 Grundeinstellungen

Das Menü enthält die folgenden Dialoge:

- System
- Module
- Netz
- Software
- Laden/Speichern
- Externer Speicher
- Port
- Power over Ethernet
- Neustart

1.1 System

[Grundeinstellungen > System]

Dieser Dialog zeigt Informationen zum Betriebszustand des Geräts.

Geräte-Status

Geräte-Status

Zeigt den Geräte-Status und die gegenwärtig vorliegenden Alarme. Wenn mindestens 1 Alarm vorliegt, ist die Hintergrundfarbe rot. Andernfalls ist die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose > Statuskonfiguration > Gerätestatus*. Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht.

Ein Tooltip zeigt die Ursache der gegenwärtig vorliegenden Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat. Um den Tooltip anzuzeigen, bewegen Sie den Mauszeiger über das Feld oder tippen Sie darauf. Die Registerkarte *Status* im Dialog *Diagnose > Statuskonfiguration > Gerätestatus* zeigt eine Übersicht über die Alarme.

Anmerkung: Das Gerät meldet einen Alarm, wenn Sie an ein Gerät, das 2 redundante Netzteile unterstützt, lediglich 1 Netzteil anschließen. Um einen solchen Alarm zu vermeiden, deaktivieren Sie im Dialog *Diagnose > Statuskonfiguration > Gerätestatus* das Überwachen fehlender Netzteile.

Sicherheits-Status

Sicherheits-Status

Zeigt den Sicherheits-Status und die gegenwärtig vorliegenden Alarme. Wenn mindestens 1 Alarm vorliegt, ist die Hintergrundfarbe rot. Andernfalls ist die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose > Statuskonfiguration >* Sicherheitsstatus. Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht.

Ein Tooltip zeigt die Ursache der gegenwärtig vorliegenden Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat. Um den Tooltip anzuzeigen, bewegen Sie den Mauszeiger über das Feld oder tippen Sie darauf. Die Registerkarte *Status* im Dialog *Diagnose > Statuskonfiguration >* Sicherheitsstatus zeigt eine Übersicht über die Alarme.

Status Signalkontakt

Das Gerät enthält möglicherweise mehrere Signalkontakte.

Status Signalkontakt

Zeigt den Signalkontakt-Status und die gegenwärtig vorliegenden Alarme. Wenn mindestens 1 Alarm vorliegt, ist die Hintergrundfarbe rot. Andernfalls ist die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose > Statuskonfiguration >* Signalkontakt > *Signalkontakt 1*/*Signalkontakt 2*. Das Gerät löst einen Alarm aus, wenn ein überwachter Parameter vom gewünschten Zustand abweicht.

Ein Tooltip zeigt die Ursache der gegenwärtig vorliegenden Alarme und den Zeitpunkt, zu dem das Gerät den Alarm ausgelöst hat. Um den Tooltip anzuzeigen, bewegen Sie den Mauszeiger über das Feld oder tippen Sie darauf. Die Registerkarte *Status* im Dialog *Diagnose > Statuskonfiguration >* Signalkontakt > *Signalkontakt 1Signalkontakt 2* zeigt eine Übersicht über die Alarme.

Systemdaten

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

Systemname

Legt den Namen fest, unter dem das Gerät im Netz bekannt ist.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
  Das Gerät akzeptiert die folgenden Zeichen:
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`
  - `<Name des Gerätetyps>-<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 manche Systeme zwischen Groß- und Kleinschreibung im FQDN unterscheiden. Vergewissern Sie sich, dass dieser Name im gesamten Netz eindeutig ist.

- DHCP-Client
- *Syslog*
- *IEC61850-MMS*
- *PROFINET*

Anmerkung: Legen Sie einen Gerätenamen fest, der mit PROFINET kompatibel ist: Max. 240 Zeichen, keine Ziffer an erster Stelle. Die Teilnehmer im Netz lesen den Gerätenamen mittels SNMP und PROFINET DCP.

Standort

Legt den gegenwärtigen oder geplanten Standort 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 des Geräts vergangen ist.

Mögliche Werte:

- Zeit im Format `Tag(e), ...h ...m ...s`

Temperatur [°C]

Zeigt die gegenwärtige Temperatur im Gerät in °C.

Das Überwachen der Grenzwerte für die Temperatur aktivieren Sie im Dialog *Diagnose* > Statuskonfiguration > *Gerätestatus*.

Obere Temp.-Grenze [°C]

Legt den oberen Temperaturschwellwert in °C fest.

Weitere Informationen zum Festlegen der Temperaturschwellwerte finden Sie im Anwender-Handbuch „Installation“.

Mögliche Werte:

- `-99..99` (ganze Zahl)
  Wenn die Temperatur im Gerät den festgelegten Wert überschreitet, dann zeigt das Gerät einen Alarm.

Untere Temp.-Grenze [°C]

Legt den unteren Temperaturschwellwert in °C fest.

Weitere Informationen zum Festlegen der Temperaturschwellwerte finden Sie im Anwender-Handbuch „Installation“.

Mögliche Werte:

- `-99..99` (ganze Zahl)
  Wenn die Temperatur im Gerät den festgelegten Wert unterschreitet, dann zeigt das Gerät einen Alarm.

Obere Luftfeucht.-Grenze [%]

Legt den oberen Luftfeuchtigkeitsschwellwert in Prozent fest.

Mögliche Werte:

- `0..100` (Voreinstellung: `95`)
  Wenn die Luftfeuchtigkeit im Gerät den festgelegten Wert überschreitet, dann zeigt das Gerät einen Alarm.

Untere Luftfeucht.-Grenze [%]

Legt den unteren Luftfeuchtigkeitsschwellwert in Prozent fest.

Mögliche Werte:

- `0..100` (Voreinstellung: `5`)
  Wenn die Luftfeuchtigkeit im Gerät den festgelegten Wert unterschreitet, dann zeigt das Gerät einen Alarm.

LED-Status

Weitere Informationen zu den Gerätestatus-LEDs finden Sie im Anwender-Handbuch „Installation“.

Status

Gegenwärtig ist kein Alarm vorhanden. Der Gerätestatus ist OK.

Zum Geräte-Status liegt gegenwärtig mindestens 1 Alarm vor. Für Details siehe Rahmen *Geräte-Status*.

Power

Gerät, das 2 redundante Netzteile unterstützt: Lediglich 1 Versorgungsspannung liegt an.

Gerät, das 1 Netzteil unterstützt: Die Versorgungsspannung liegt an.

Gerät, das 2 redundante Netzteile unterstützt: Beide Versorgungsspannungen liegen an.

RM

Redundanz-Manager: *MRP*-Ring-Manager

Das Gerät arbeitet nicht als Redundanz-Manager.

Das Gerät arbeitet als Redundanz-Manager. Keine Redundanz vorhanden.

Das Gerät arbeitet als Redundanz-Manager. Redundanz vorhanden.

ACA

Kein externer Speicher angeschlossen.

Der externe Speicher ist angeschlossenen, jedoch nicht betriebsbereit.

Der externe Speicher ist angeschlossenen und betriebsbereit.

I1

IO-Eingang 1: Die Eingangsspannung ist `low`.

IO-Eingang 1: Die Eingangsspannung ist `high`.

I2

IO-Eingang 2: Die Eingangsspannung ist `low`.

IO-Eingang 2: Die Eingangsspannung ist `high`.

Status Port

Dieser Rahmen zeigt eine vereinfachte Ansicht der Ports des Geräts zum Zeitpunkt der letzten Anzeigeaktualisierung. In der Grundansicht zeigt der Rahmen lediglich Ports mit aktivem Link.

Wenn Sie die Schaltfläche klicken, zeigt der Rahmen sämtliche Ports.

Den Port-Status erkennen Sie ganz einfach an der Markierung:

- Ports mit aktivem Link:
  - Hintergrundfarbe ist Grün.
  - Neben der Port-Nummer steht die Übertragungsrate des Ports.
- Ports mit inaktivem Link:
  Hintergrundfarbe ist Grau.
- Ports, die aufgrund einer Redundanz-Funktion im Zustand *Blocking* sind:
  Gestrichelte Umrandung.

Wenn Sie den Mauszeiger über dem Port-Symbol positionieren oder darauf tippen, zeigt ein Tooltip detaillierte Informationen zum Port-Status.

1.2 Module

[Grundeinstellungen > Module]

Das Gerät ermöglicht Ihnen, die Module im laufenden Betrieb zu installieren oder zu entfernen (hot-plug).

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

- Wenn Sie das Modul durch ein baugleiches Modul ersetzen, wendet das Gerät die bisherigen Einstellungen sofort auf das neue Modul an.
- Wenn Sie das Modul durch ein Modul anderen Typs ersetzen, wendet das Gerät die Werkseinstellungen auf das neue Modul an.
- Wenn Sie ein Modul in einen leeren Steckplatz einschieben, 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.

Ethernet-Modul installieren

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.
- ☐ Um die grafische Benutzeroberfläche zu aktualisieren, klicken Sie die Schaltfläche ↻.
  Die Spalte *Ethernet-Modul-Status* zeigt für das installierte Ethernet-Modul den Wert `physical`.
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

Steckplatz aktivieren/deaktivieren

Auf einem deaktivierten Steckplatz erkennt das Gerät das installierte Modul und das Konfigurieren der Ports ist möglich. Das Modul stellt auf einem deaktivierten Steckplatz keine Verbindungen ins Netz her.

Führen Sie die folgenden Schritte aus:

- ☐ Wählen Sie in der Tabelle die Zeile des Moduls.
- ☐ Um den Steckplatz zu deaktivieren und Zugriffe auf das Netz zu unterbinden, heben Sie die Markierung des Kontrollkästchens *Aktiv* auf.
- ☐ Um den Steckplatz zu aktivieren und Zugriffe auf das Netz zu erlauben, markieren Sie das Kontrollkästchen *Aktiv*.
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

Ethernet-Modul entfernen

Führen Sie die folgenden Schritte aus:

- ☐ Entfernen Sie das Modul aus dem Steckplatz.
- ☐ Um die grafische Benutzeroberfläche zu aktualisieren, klicken Sie die Schaltfläche ↻.
  Die Spalte *Ethernet-Modul-Status* zeigt für das zuvor entfernte Modul den Wert `configurable`.
- ☐ Wählen Sie in der Tabelle die Zeile des zuvor entfernten Moduls.
- ☐ Klicken Sie die Schaltfläche ✖.
  Die Spalte *Ethernet-Modul-Status* zeigt für das zuvor entfernte Modul den Wert `remove`.
  Die Spalte *Typ* und einige andere Spalten zeigen den Wert `n/a`.
  Das markierte Kontrollkästchen *Aktiv* weist darauf hin, dass der Steckplatz noch aktiv ist.
- ☐ Um die Änderungen zwischenzuspeichern, klicken Sie die Schaltfläche ✓.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Ethernet-Modul entfernen

Entfernt das markierte Ethernet-Modul aus der Tabelle.

Ethernet-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 Zustand des 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 Versionsnummer des installierten Moduls.

Ports

Zeigt, wie viele Ports auf dem installierten Modul verfügbar sind.

Seriennummer

Zeigt die Seriennummer des installierten Moduls.

Ein Wert von `n/a` weist darauf hin, dass der Steckplatz leer ist.

Ethernet-Modul-Status

Zeigt den Status des Steckplatzes.

Mögliche Werte:

- *physical*
  Im Steckplatz ist ein Modul installiert.
- *configurable*
  Der Steckplatz ist leer und für die Konfiguration verfügbar.
- *remove*
  Der Steckplatz ist leer und deaktiviert.
- *fix*
  Das Modul kann nicht entfernt werden.

1.3 Netz

[Grundeinstellungen > Netz]

Das Menü enthält die folgenden Dialoge:

- Global
- IPv4

1.3.1 Global

[Grundeinstellungen > Netz > Global]

In diesem Dialog legen Sie die VLAN- und HiDiscovery-Einstellungen fest, die für den Zugriff über das Netz auf das Management des Geräts erforderlich sind.

Management-Schnittstelle

In diesem Rahmen legen Sie das VLAN fest, in dem das Management des Geräts erreichbar ist.

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.

MAC-Adresse Konflikterkennung

Schaltet die Funktion *MAC-Adresse Konflikterkennung* ein/aus.

Mögliche Werte:

- `markiert`
  Die Funktion *MAC-Adresse Konflikterkennung* ist eingeschaltet.
  Das Gerät prüft, ob ein weiteres Gerät im Netz die eigene MAC-Adresse verwendet.
- `unmarkiert` (Voreinstellung)
  Die Funktion *MAC-Adresse Konflikterkennung* ist ausgeschaltet.

HiDiscovery Protokoll v1/v2

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

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

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*.

Funktion

Schaltet die Funktion HiDiscovery im Gerät ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion HiDiscovery ist eingeschaltet.
  Sie haben die Möglichkeit, das Gerät mit der HiDiscovery-Software von Ihrem PC aus zu erreichen.
- `Aus`
  Die Funktion HiDiscovery ist ausgeschaltet.

Zugriff

Schaltet den Schreibzugriff auf das Gerät für die Funktion HiDiscovery ein/aus.

Mögliche Werte:

- `read-write` (Voreinstellung)
  Die Funktion HiDiscovery hat Schreibzugriff auf das Gerät. Das Gerät ermöglicht Ihnen, mit der Funktion HiDiscovery die IP-Parameter im Gerät zu ändern.
- `read-only`
  Die Funktion HiDiscovery hat lediglich Lesezugriff auf das Gerät. Das Gerät ermöglicht Ihnen, mit der Funktion HiDiscovery die IP-Parameter im Gerät anzusehen.

Empfehlung: Ändern Sie erst nach Inbetriebnahme des Geräts die Einstellung auf den Wert `read-only`.

Signal

Aktiviert/deaktiviert das Blinken der Port-LEDs wie die gleichnamige Funktion in der HiDiscovery-Software. Diese Funktion ermöglicht Ihnen, 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.

1.3.2 IPv4

[Grundeinstellungen > Netz > IPv4]

In diesem Dialog legen Sie die IPv4-Einstellungen fest, die für den Zugriff über das Netz auf das Management des Geräts erforderlich sind.

Management-Schnittstelle

Zuweisung IP-Adresse

Legt fest, aus welcher Quelle das Management des Geräts 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.
  Stellt der Server zusätzlich die Adressen von DNS-Servern bereit, zeigt das Gerät diese Adressen im Dialog *Erweitert > DNS > Cache > Aktuell*.

Anmerkung: Wenn die Antwort des BOOTP- oder DHCP-Servers ausbleibt, dann setzt das Gerät die IP-Adresse auf `0.0.0.0` und versucht erneut, eine gültige IP-Adresse zu erhalten.

IP-Parameter

Dieser Rahmen ermöglicht Ihnen, die IP-Parameter manuell zuzuweisen. Wenn Sie im Rahmen *Management-Schnittstelle*, Optionsliste *Zuweisung IP-Adresse* das Optionsfeld `Lokal` auswählen, dann sind die Felder editierbar.

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.

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

BOOTP/DHCP

Client-ID

Zeigt die DHCP-Client-ID, die das Gerät an den BOOTP- oder DHCP-Server sendet. Wenn man eine entsprechende Konfiguration des Servers voraussetzt, dann 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.

DHCP-Option 66/67/4/42

Schaltet die Funktion *DHCP-Option 66/67/4/42* im Gerät ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion *DHCP-Option 66/67/4/42* ist eingeschaltet.
  Das Gerät lädt das Konfigurationsprofil und empfängt die Zeitserverinformationen mittels der folgenden DHCP-Optionen:
  - `Option 66: TFTP server name`
    `Option 67: Boot file name`
    Das Gerät lädt mittels TFTP-Protokoll das Konfigurationsprofil automatisch vom DHCP-Server in den flüchtigen Speicher (`RAM`). Das Gerät verwendet die Einstellungen des importierten Konfigurationsprofils in der `running-config`.
  - `Option 4: Time Server`
    `Option 42: Network Time Protocol Servers`
    Das Gerät empfängt die Zeitserverinformationen vom DHCP-Server.
- `Aus`
  Die Funktion *DHCP-Option 66/67/4/42* ist ausgeschaltet.
  - Das Gerät lädt kein Konfigurationsprofil mittels DHCP-Option 66/67.
  - Das Gerät empfängt keine Zeitserverinformationen mittels DHCP-Option 4/42.

Verbleibende Lease-Time

Lease-Time [s]

Zeigt die verbleibende Zeit in Sekunden, in der die IP-Adresse noch gültig ist, die der DHCP-Server dem Managment des Geräts zugewiesen hat.

Um die Anzeige zu aktualisieren, klicken Sie die Schaltfläche ↻.

1.4 Software

[Grundeinstellungen > Software]

Dieser Dialog ermöglicht Ihnen, 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

Gespeicherte Version

Zeigt Versionsnummer und Erstellungsdatum der im Flash gespeicherten Geräte-Software. Das Gerät lädt die Geräte-Software beim nächsten Neustart.

Ausgeführte 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 *Gespeicherte Version*und die *Backup-Version* der Geräte-Software.

Das Gerät lädt die *Gespeicherte Version*beim nächsten Neustart.

Bootcode

Zeigt Versionsnummer und Erstellungsdatum des Bootcodes.

Software-Update

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

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>`

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.

Tabelle

Datei Ort

Zeigt den Speicherort der Geräte-Software.

Mögliche Werte:

- *ram*
  Flüchtiger Speicher des Geräts
- *flash*
  Permanenter Speicher (*NVM*) des Geräts
- *sd-card* (nicht verfügbar für MSP-X)
  Externer SD-Speicher (ACA31)
- *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.

1.5 Laden/Speichern

[Grundeinstellungen > Laden/Speichern]

Dieser Dialog ermöglicht Ihnen, 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. Wenn die Verbindung abbricht, dann lädt das Gerät nach der festgelegten Zeit das im permanenten Speicher (`NVM`) gespeicherte Konfigurationsprofil.

Anmerkung: Wechsel von Classic zu HiOS? Verwenden Sie unser Online-Tool, um Ihre Dateien mit der Gerätekonfiguration zu konvertieren: https://convert.hirschmann.com

Externer Speicher

Ausgewählter externer Speicher

Legt den externen Speicher fest, den das Gerät für Datei-Operationen verwendet. Das Gerät speichert in diesem externen Speicher zum Beispiel Kopien der Geräte-Konfiguration.

Mögliche Werte:

- `sd`
  Externer SD-Speicher (ACA31) (nicht verfügbar für MSP-X)
- `usb`
  Externer USB-Speicher (ACA21/ACA22)

Status

Zeigt den Betriebszustand des ausgewählten 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 im externen Speicher ist belegt.
- `genericErr`
  Das Gerät hat einen Fehler festgestellt.

Konfigurations-Verschlüsselung

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 `first` oder `second` hat und das Konfigurationsprofil unverschlüsselt ist, dann 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 Fenster *Passwort setzen*, das Ihnen beim Festlegen des Passworts hilft, das für die Verschlüsselung des Konfigurationsprofils erforderlich ist. Das Verschlüsseln des Konfigurationsprofils erschwert den unberechtigten Zugriff. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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 im externen Speicher anzuwenden.

Anmerkung: Wenden Sie diese Funktion ausschließlich dann an, wenn maximal ein 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, dann führen Sie die folgenden Schritte aus:

- ☐ 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*).

Anmerkung: Voraussetzung für das Laden eines Konfigurationsprofils vom externen Speicher ist, dass im Dialog *Grundeinstellungen > Externer Speicher* die Spalte *Konfigurations-Priorität* den Wert `first` oder `second` zeigt. Dieser Wert ist voreingestellt.

Löschen

Öffnet das Fenster *Löschen*, das Ihnen beim Aufheben der Konfigurations-Verschlüsselung im Gerät hilft. Um die Konfigurations-Verschlüsselung aufzuheben, führen Sie die folgenden Schritte aus:

- 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 im externen Speicher aufzuheben.

Anmerkung: Wenn Sie weitere Konfigurationsprofile verschlüsselt im Speicher vorhalten, sorgt das Gerät dafür, dass Sie diese Konfigurationsprofile nicht aktivieren oder als „ausgewählt“ kennzeichnen.

Konfigurationsänderungen rückgängig machen

Funktion

Schaltet die Funktion *Konfigurationsänderungen rückgängig machen* ein/aus. Mit der Funktion prüft das Gerät kontinuierlich, ob es von der IP-Adresse Ihres PCs 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`)

Information

NVM synchron mit running-config

Zeigt, ob die Einstellungen im flüchtigen Speicher (*RAM*) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (*NVM*) abweichen.

Mögliche Werte:

- `markiert`
  Die Einstellungen stimmen überein.
- `unmarkiert`
  Die Einstellungen weichen voneinander ab. Das Banner zeigt zusätzlich das Symbol !.

Externer Speicher und NVM synchron

Zeigt, ob die Einstellungen des „ausgewählten“ Konfigurationsprofils im externen Speicher (ACA) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (*NVM*) abweichen.

Mögliche Werte:

- `markiert`
  Die Einstellungen stimmen überein.
- `unmarkiert`
  Die Einstellungen weichen voneinander ab.
  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

Funktion

Schaltet die Funktion *Sichere Konfiguration auf Remote-Server beim Speichern* ein/aus.

Mögliche Werte:

- `Eingeschaltet`
  Die Funktion *Sichere Konfiguration auf Remote-Server beim Speichern* 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 Funktion *Sichere Konfiguration auf Remote-Server beim Speichern* 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

Zugangsdaten setzen

Öffnet das Fenster *Anmeldeinformationen*, das Ihnen beim Festlegen des Login-Passworts hilft, das für die Anmeldung auf dem Remote-Server erforderlich ist. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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
    Das Gerät akzeptiert die folgenden Zeichen:
    `a..z`
    `A..Z`
    `0..9`
    `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Löschen

Entfernt das in der Tabelle ausgewählte Konfigurationsprofil aus dem permanenten Speicher (*NVM*) oder vom externen Speicher.

Wenn das Konfigurationsprofil als „ausgewählt" gekennzeichnet ist, dann hilft das Gerät, das Entfernen des Konfigurationsprofils zu vermeiden.

Speichern

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, dann erzeugt das Gerät eine Kopie des Konfigurationsprofils im externen Speicher.

Zeigt ein Kontextmenü mit weiteren Funktionen für den betreffenden Dialog.

Speichern unter...

Öffnet das Fenster *Speichern unter...*, um das in der Tabelle ausgewählte Konfigurationsprofil zu kopieren und es mit benutzerdefiniertem Namen im permanenten Speicher (*NVM*) zu speichern.

- Geben Sie im Feld *Profilname* den Namen ein, unter dem Sie das Konfigurationsprofil speichern möchten.
  - Um das Konfigurationsprofil unter einem neuen Namen zu speichern, klicken Sie die Schaltfläche + .
  - Um ein bestehendes Konfigurationsprofil zu überschreiben, wählen Sie in der Dropdown-Liste den zugehörigen Eintrag aus.

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".

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.

Aktivieren

Lädt die Einstellungen des in der Tabelle ausgewählten Konfigurationsprofils in den flüchtigen Speicher (*RAM*).

- Das Gerät trennt die Verbindung zur grafischen Benutzeroberfläche. Um wieder auf das Geräte-Management zuzugreifen, führen Sie die folgenden Schritte aus:
  - 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.

Auswählen

Kennzeichnet das in der Tabelle ausgewählte 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 die Konfigurations-Verschlüsselung im Gerät eingeschaltet ist und das Passwort mit dem im Gerät gespeicherten Passwort übereinstimmt.

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“.

Importieren...

Öffnet das Fenster *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 ausgewählten externen Speicher. Siehe Rahmen *Externer Speicher*.
- Wenn oben `PC/URL` ausgewählt ist, 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, 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 Eintrag `PC/URL` auswählen.
  - `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, dann 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 Konfigurationsprofils 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.

Exportieren...

Exportiert das in der Tabelle ausgewählte 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>`

Save running-config as script

Speichert das Konfigurationsprofil `running config` als Skript-Datei auf dem lokalen PC. Dies ermöglicht Ihnen, die gegenwärtigen Einstellungen des Geräts zu sichern oder auf anderen Geräten zu verwenden.

Load running-config as script

Importiert eine Skript-Datei, die das gegenwärtige Konfigurationsprofil `running config` ändert.

Das Gerät bietet Ihnen folgende Möglichkeiten, eine Skript-Datei zu importieren:

- 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>`

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 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*).

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. Führen Sie dazu die folgenden Schritte aus:
  - Wählen Sie in der Tabelle die Zeile des Konfigurationsprofils.
  - Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Aktivieren*.
- *ENVM* (externer Speicher)
  Im 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 ermöglicht Ihnen, ein Konfigurationsprofil mit benutzerdefiniertem Namen zu speichern. Wählen Sie dazu in der Tabelle die Zeile eines vorhandenen Konfigurationsprofils, klicken die Schaltfläche ☰ und dann den Eintrag *Speichern unter...*.

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.

Das Gerät ermöglicht Ihnen, ein anderes Konfigurationsprofil als „ausgewählt“ zu kennzeichnen.

Wählen Sie dazu in der Tabelle das gewünschte Konfigurationsprofil, klicken die Schaltfläche ☰ und dann den Eintrag *Aktivieren*.

Mögliche Werte:

- `markiert`
  Das Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.
  - Das Gerät lädt die das Konfigurationsprofil beim Neustart oder beim Anwenden der Funktion *Konfigurationsänderungen rückgängig machen* 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.

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.

Anmerkung: Das Gerät wendet Skript-Dateien zusätzlich zu den gegenwärtigen Einstellungen an. Vergewissern Sie sich, dass die Skript-Datei keine Teile enthält, die mit den gegenwärtigen Einstellungen in Konflikt stehen.

Software-Version

Zeigt die Versionsnummer der Geräte-Software, die das Gerät beim Speichern des Konfigurationsprofils ausgeführt hat.

Fingerabdruck

Zeigt die im Konfigurationsprofil gespeicherte Prüfsumme.

Das Gerät berechnet die Prüfsumme beim Speichern der Einstellungen und fügt sie in das Konfigurationsprofil ein.

Fingerabdruck 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 im 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
- mit einem kleineren oder demselben Level der Geräte-Software
  wie HiOS-2A oder HiOS-3S auf einem Gerät, das HiOS-3S ausführt

Anmerkung: Diese Funktion kennzeichnet Änderungen an den Einstellungen des Konfigurationsprofils. Die Funktion bietet keinen Schutz davor, das Gerät mit geänderten Einstellungen zu betreiben.

1.6 Externer Speicher

[Grundeinstellungen > Externer Speicher]

Dieser Dialog ermöglicht Ihnen, 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

USB-Modus

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, dann legen Sie den Wert `compatibility` fest.

Information

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Typ

Zeigt den Typ des externen Speichers.

Mögliche Werte:

- *sd* (nicht verfügbar für MSP-X)
  Externer SD-Speicher (ACA31)
- *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 im 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 für 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 im 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 RSA-Schlüssels vom externen Speicher beim Neustart.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Laden des RSA-Schlüssels ist aktiviert.
  Beim Neustart lädt das Gerät den RSA-Schlüssel vom externen Speicher, wenn sich im externen Speicher folgende Dateien befinden:
  - SSH-RSA-Schlüssel-Datei
  - eine Textdatei `startup.txt` mit dem Inhalt
    `autoUpdateRSA=<Dateiname_des_SSH-RSA-Schlüssels>`

  Meldungen zeigt das Gerät auf der Systemkonsole der seriellen Schnittstelle.
- `unmarkiert`
  Das Laden des RSA-Schlüssels ist deaktiviert.

Anmerkung: Beim Laden des RSA-Schlüssels aus dem externen Speicher (*ENVM*) überschreibt das Gerät die im permanenten Speicher (*NVM*) vorhandenen Schlüssel.

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`, `second`
  Das Gerät lädt das Konfigurationsprofil von dem mit `first` gekennzeichneten externen Speicher. Findet das Gerät dort kein Konfigurationsprofil, lädt es das Konfigurationsprofil von dem mit `second` gekennzeichneten externen Speicher usw. (nicht verfügbar für MSP-X).
  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` oder `second` hat und das Konfigurationsprofil unverschlüsselt ist, dann 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 im 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 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.

1.7 Port

[Grundeinstellungen > Port]

Dieser Dialog ermöglicht Ihnen, 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Name

Bezeichnung des Ports.

Mögliche Werte:
- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen
  Das Gerät akzeptiert die folgenden Zeichen:
  - `<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 Funktion *Auto-Disable* 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.

Automatisches Ausschalten

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.

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 Funktion *Automatische Konfiguration* 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

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

Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts und vom verwendeten Modul.

Manuelles Cable-Crossing (Auto. Konfig. aus)

Legt die Belegung der Anschlüsse eines TP-Ports fest.

Voraussetzung ist, dass die Funktion *Automatische Konfiguration* ausgeschaltet ist.

Mögliche Werte:

- *`mdi`*
  Das Gerät vertauscht das Sende- und Empfangsleitungspaar auf dem Port.
- *`mdix`* (Voreinstellung auf TP-Ports)
  Das Gerät hilft, das Vertauschen der Sende- und Empfangsleitungspaare auf dem Port zu vermeiden.

- `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. Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt.

Trap senden (Link-Up/Down)

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung des Link-Status auf dem Port erkennt.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv.
  Wenn das Gerät eine Link-Status-Änderung erkennt, sendet es einen SNMP-Trap.
- `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 ein Trap-Ziel festlegen.

MTU

Legt die maximal zulässige Größe der Ethernet-Pakete auf dem Port in Byte fest.

Mögliche Werte:

- `1518..12288` (Voreinstellung: `1518`)
  Mit der Einstellung `1518` vermittelt der Port die Ethernet-Pakete bis zu einschließlich folgender Größe:
  - 1518 Byte ohne VLAN-Tag
    (1514 Byte + 4 Byte CRC)
  - 1522 Byte mit VLAN-Tag
    (1518 Byte + 4 Byte CRC)

Diese Einstellung ermöglicht Ihnen, die maximal erlaubte Größe von Ethernet-Paketen zu erhöhen, die dieser Port empfangen oder senden kann.

Mögliche Anwendungsfälle sind:

- Wenn Sie das Gerät im Transfer-Netz mit Double-VLAN-Tagging einsetzen, ist möglicherweise eine um 4 Byte größere *MTU* erforderlich.

Auf anderen Interfaces legen Sie die maximal zulässige Größe der Ethernet-Pakete wie folgt fest:

- *Link-Aggregation*-Interfaces
  Dialog *Switching > L2-Redundanz > Link-Aggregation*, Spalte *MTU*

Signal

Aktiviert/deaktiviert das Blinken der Port-LED. Diese Funktion ermöglicht Ihnen, 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.

[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 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, führen Sie die folgenden Schritte aus:

- Klicken Sie im Dialog *Grundeinstellungen > Port* die Schaltfläche 🗑 .

  oder
- Klicken Sie im Dialog *Grundeinstellungen > Neustart* die Schaltfläche *Port-Statistiken leeren*.

[Netzlast]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 ein Trap-Ziel festlegen.

1.8 Power over Ethernet

[Grundeinstellungen > Power over Ethernet]

Bei Power-over-Ethernet (PoE) versorgt das Strom liefernde Gerät (Power Source Equipment, PSE) die Stromverbraucher (Powered Devices, PD) wie IP-Telefone über das Twisted-Pair-Kabel mit Strom.

Ob Ihr Gerät *Power over Ethernet* unterstützt, können Sie anhand des Produktcodes und einer PoE-spezifischen Kennzeichnung am Gehäuse des PSE-Geräts feststellen. Die PoE-Ports des Geräts unterstützen Power over Ethernet nach IEEE 802.3at.

Das System stellt ein internes, maximales Leistungsbudget für die Ports zur Verfügung. Entsprechend der ermittelten Klasse eines angeschlossenen Stromverbrauchers reservieren die Ports Strom. Die tatsächlich abgegebene Leistung gleicht der Reserveleistung oder ist kleiner als diese.

Die Ausgangsleistung verwalten Sie mit dem Parameter *Priorität*. Wenn die Summe der für die angeschlossenen Geräte erforderlichen Leistung die verfügbare Leistung überschreitet, geht das Gerät beim Abschalten des für die Ports bereitgestellten Stroms nach der festgelegten Priorität vor. Beim Abschalten des für die Ports bereitgestellten Stroms beginnt das Gerät bei den Ports, bei denen Sie einen niedrige Priorität festgelegt haben. Wenn mehrere Ports eine niedrige Priorität aufweisen, beginnt das Gerät beim Abschalten bei den höher nummerierten Ports.

Das Menü enthält die folgenden Dialoge:

- PoE Global
- PoE Port

1.8.1 PoE Global

[Grundeinstellungen > Power over Ethernet > Global]

Anhand der in diesem Dialog festgelegten Einstellungen liefert das Gerät Strom an die Endnutzergeräte. Wenn der Stromverbrauch den benutzerdefinierten Grenzwert erreicht, sendet das Gerät einen SNMP-Trap.

Funktion

Funktion

Schaltet die Funktion *Power over Ethernet* ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion *Power over Ethernet* ist eingeschaltet.
- `Aus`
  Die Funktion *Power over Ethernet* ist ausgeschaltet.

Konfiguration

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps.

Wenn der Stromverbrauch den benutzerdefinierten Grenzwert übersteigt, sendet das Gerät einen SNMP-Trap.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Gerät sendet SNMP-Traps.
- `unmarkiert`
  Das Gerät sendet keine SNMP-Traps.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

Grenzwert [%]

Legt den Grenzwert für den allgemeinen Stromverbrauch in Prozent fest.

Das Gerät misst die Gesamtausgangsleistung und sendet einen SNMP-Trap, wenn die Ausgangsleistung diesen Grenzwert überschreitet.

Mögliche Werte:

- `0..99` (Voreinstellung: `90`)

Systemleistung

Budget [W]

Zeigt die für das globale Leistungsbudget verfügbare Gesamtstromleistung.

Reserviert [W]

Zeigt die allgemeine Reserveleistung. Entsprechend der ermittelten Klassen von angeschlossenen Stromverbrauchern reserviert das Gerät Strom. Die Reserveleistung gleicht der tatsächlich abgegebenen Leistung oder ist kleiner als diese.

Abgegeben [W]

Zeigt die tatsächlich an die Module abgegebene Leistung in Watt.

Abgegeben [mA]

Zeigt den tatsächlich an die Module abgegebenen Strom in Milliampere.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Modul

Gerätemodul, auf das sich die Tabelleneinträge beziehen.

Konfiguriertes Leistungs-Budget [W]

Legt die Modul-Leistung für die Verteilung an die Ports fest.

Mögliche Werte:

- `0..n` (Voreinstellung: n)
  Hierbei entspricht `n` dem Wert in Spalte *Max. Leistungs-Budget [W]*.

Max. Leistungs-Budget [W]

Zeigt die maximal verfügbare Leistung für dieses Modul.

Reservierte Leistung [W]

Zeigt die reservierte Leistung für das Modul entsprechend der ermittelten Klassen von angeschlossenen Stromverbrauchern.

Abgegebene Leistung [W]

Zeigt die tatsächliche Leistung in Watt, die das Gerät an die an den Port angeschlossenen Stromverbraucher abgibt.

Abgegebener Strom [mA]

Zeigt den tatsächlichen Strom in Milliampere, den das Gerät an die an den Port angeschlossenen Stromverbraucher abgibt.

Stromquelle

Zeigt den Stromversorger des Geräts.

Mögliche Werte:

- *intern*
  Interne Stromversorgung
- *extern*
  Externe Stromversorgung

Grenzwert [%]

Legt den Grenzwert für den Modul-Stromverbrauch in Prozent fest. Das Gerät misst die Gesamtausgangsleistung und sendet einen SNMP-Trap, wenn die Ausgangsleistung diesen Grenzwert überschreitet.

Mögliche Werte:

- `0..99` (Voreinstellung: `90`)

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät das Überschreiten des Stromverbrauch-Grenzwerts erkennt.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Wenn der Stromverbrauch des Moduls den benutzerdefinierten Grenzwert überschreitet, sendet das Gerät einen SNMP-Trap.
- `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 ein Trap-Ziel festlegen.

1.8.2 PoE Port

[Grundeinstellungen > Power over Ethernet > Port]

Liegt die Leistungsaufnahme über der möglichen Leistung, schaltet das Gerät den Strom für Geräte im Netz gemäß den Prioritätsstufen und Port-Nummern ab. Sollten die angeschlossenen Stromverbraucher mehr Strom anfordern als das Gerät liefert, schaltet das Gerät die Funktion *Power over Ethernet* auf den Ports aus. Das Gerät schaltet die Funktion *Power over Ethernet* zuerst auf den Ports mit niedrigster Priorität aus. Wenn mehrere Ports die gleiche Priorität haben, deaktiviert das Gerät die *Power over Ethernet*-Funktion zuerst auf den Ports mit höherer Port-Nummer. Darüber hinaus schaltet das Gerät den Strom für Geräte im Netz für einen festgelegten Zeitraum ab.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

PoE an

Aktiviert/deaktiviert den für den Port bereitgestellten PoE-Strom.

Beim Aktivieren/Deaktivieren der Funktion protokolliert das Gerät ein Ereignis in der Log-Datei (System Log).

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die PoE-Stromversorgung auf dem Port ist aktiv.
- `unmarkiert`
  Die PoE-Stromversorgung auf dem Port ist inaktiv.

Fast-Startup

Aktiviert/deaktiviert die PoE-Schnellstart-Funktion des Geräts.

Voraussetzung ist, dass das Kontrollkästchen in Spalte *PoE an* markiert ist.

Mögliche Werte:

- `markiert`
  Die Schnellstart-Funktion ist aktiv. Vor dem Laden der eigenen Konfiguration versorgt das Gerät die Stromverbraucher mit Strom.
- `unmarkiert` (Voreinstellung)
  Die Schnellstart-Funktion ist inaktiv. Nach dem Laden der eigenen Konfiguration versorgt das Gerät die Stromverbraucher mit Strom.

Priorität

Legt die Port-Priorität fest.

Um Stromüberlastungen zu vermeiden, schaltet das Gerät die Ports mit niedrigerer Priorität zuerst aus. Um zu vermeiden, dass das Gerät Ports abschaltet, die wesentliche Geräte speisen, legen Sie für diese Ports eine hohe Priorität fest.

Mögliche Werte:

- `critical`
- `high`
- `low` (Voreinstellung)

Status

Zeigt den Port-Status für die Erkennung der zu speisenden Geräte.

Mögliche Werte:

- `disabled`
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand DISABLED befindet.
- `deliveringPower`
  Zeigt, dass das Gerät die Klasse des angeschlossenen Stromverbrauchers ermittelt hat und dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand POWER ON befindet.
- `fault`
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand TEST ERROR befindet.
- `otherFault`
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand IDLE befindet.
- `searching`
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) in einem nicht gelisteten Zustand befindet.
- `test`
  Zeigt, dass sich das Zustandsdiagramm des Stromversorgers (PSE) im Zustand TEST MODE befindet.

Erkannte Klasse

Zeigt die Leistungsklasse des an den Port angeschlossenen Stromverbrauchers.

Mögliche Werte:

- `Klasse 0`
- `Klasse 1`
- `Klasse 2`
- `Klasse 3`
- `Klasse 4`

Klasse 0
Klasse 1
Klasse 2
Klasse 3
Klasse 4

Aktiviert/deaktiviert den Strom der Klassen 0 bis 4 auf dem Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
- `unmarkiert`

Verbrauch [W]

Zeigt den gegenwärtigen Stromverbrauch des Ports in Watt.

Mögliche Werte:

- `0,0..30,0`

Verbrauch [mA]

Zeigt den am Port abgegebenen Strom in Milliampere.

Mögliche Werte:

- `0..600`

Leistungs-Limit [W]

Legt die maximale Leistung in Watt fest, die der Port ausgibt.

Diese Funktion ermöglicht Ihnen, das verfügbare Leistungsbudget nach Bedarf über die PoE-Ports zu verteilen.

Für ein verbundenes Gerät ohne Angabe einer „Leistungsklasse“ reserviert der Port die feste Leistung von 15,4 W (Klasse 0), selbst wenn das Gerät eine geringere Leistung benötigt. Die überschüssige Leistung steht keinem anderen Port zur Verfügung.

Indem Sie die Leistungsgrenze festlegen, reduzieren Sie die reservierte Leistung auf den tatsächlichen Bedarf des verbundenen Geräts. Die nicht genutzte Leistung steht den anderen Ports zur Verfügung.

Wenn die exakte Leistungsaufnahme des zu speisenden Geräts unbekannt ist, zeigt das Gerät den Wert in Spalte *Max. Verbrauch [W]*. Vergewissern Sie sich, dass die Leistungsgrenze größer ist als der Wert in Spalte *Max. Verbrauch [W]*.

Wenn die festgestellte maximale Leistung über der festgelegten Leistungsgrenze liegt, betrachtet das Gerät die Leistungsgrenze als ungültig. In diesem Fall zieht das Gerät die PoE-Klasse zur Berechnung heran.

Mögliche Werte:

- `0,0..30,0` (Voreinstellung: `0`)

Max. Verbrauch [W]

Zeigt die maximale Leistung in Milliwatt, die das Gerät bis zum betreffenden Zeitpunkt aufgenommen hat.

Den Wert setzen Sie zurück, wenn Sie PoE deaktivieren oder die Verbindung zum verbundenen Gerät trennen.

Name

Legt die Bezeichnung des Ports fest.

Legen Sie einen beliebigen Namen fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..32 Zeichen

Strom automatisch ausschalten

Aktiviert/deaktiviert die Funktion *Strom automatisch ausschalten* gemäß Einstellung.

Mögliche Werte:

- `markiert`
- `unmarkiert` (Voreinstellung)

Strom ausschalten um [hh:mm]

Legt die Uhrzeit fest, zu der das Gerät bei Aktivierung der Funktion *Strom automatisch ausschalten* den Strom für den Port ausschaltet.

Mögliche Werte:

- `00:00..23:59` (Voreinstellung: `00:00`)

Strom wiedereinschalten um [hh:mm]

Legt die Uhrzeit fest, zu der das Gerät bei Aktivierung der Funktion *Strom automatisch ausschalten* den Strom für den Port einschaltet.

Mögliche Werte:

- `00:00..23:59` (Voreinstellung: `00:00`)

1.9 Neustart

[Grundeinstellungen > Neustart]

Dieser Dialog ermöglicht Ihnen, das Gerät neu zu starten, Port-Zähler und Adresstabellen zurückzusetzen sowie Log-Dateien zu löschen.

Neustart

Neustart in

Zeigt die verbleibende Zeit in Tagen, Stunden, Minuten und Sekunden 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 (`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`)
  Stunde:Minute:Sekunde

Nach Ablauf der Verzögerungszeit startet das Gerät neu und durchläuft folgende Phasen:

- Wenn Sie diese Funktion im Dialog *Diagnose > System > Selbsttest* aktivieren, dann führt das Gerät einen RAM-Test durch.
- Das Gerät startet die Geräte-Software, die das Feld *Gespeicherte 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

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*.

Statistik zum Zugriff auf das Management leeren

Setzt die Zähler der Statistik über Zugriffe auf das Management des Geräts auf `0`.

Siehe Dialog *Diagnose > System > Systeminformationen*, Tabelle `Used Management Ports`.

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*.

Persistente Log-Datei löschen

Entfernt die Log-Dateien vom externen Speicher.

Siehe Dialog *Diagnose > Bericht > Persistentes Ereignisprotokoll*.

E-Mail-Benachrichtigung Statistik leeren

Setzt die Zähler im Rahmen *Information* auf `0`.

Siehe Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.

2 Zeit

Das Menü enthält die folgenden Dialoge:
- Grundeinstellungen
- SNTP
- PTP

2.1 Grundeinstellungen

[Zeit > 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 einen Netzteil-Ausfall 3 Stunden lang. Voraussetzung dafür ist, dass das Netzteil 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

Systemzeit (UTC)

Zeigt das gegenwärtige Datum und die gegenwärtige Uhrzeit bezogen auf die koordinierte Weltzeit UTC.

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: *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.
- `ptp`
  PTP ist aktiviert und die Uhr des Geräts ist auf eine *PTP*-Master-Uhr synchronisiert.

Lokaler Offset [min]

Legt die Differenz zwischen lokaler Zeit und *Systemzeit (UTC)* in Minuten fest: *Lokaler Offset [min]* = *Systemzeit* − *Systemzeit (UTC)*

Mögliche Werte:

- `-780..840` (Voreinstellung: `60`)

[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

Sommerzeit

Schaltet den *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.

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

Woche

Legt die Woche im gegenwärtigen Monat fest.

Mögliche Werte:

- `-` (Voreinstellung)
- `erste`
- `zweite`
- `dritte`
- `vierte`
- `letzte`

Tag

Legt den Wochentag fest.

Mögliche Werte:

- `-` (Voreinstellung)
- `Sonntag`
- `Montag`
- `Dienstag`
- `Mittwoch`
- `Donnerstag`
- `Freitag`
- `Samstag`

Monat

Legt den Monat fest.

Mögliche Werte:

- `-` (Voreinstellung)
- `Januar`
- `Februar`
- `März`
- `April`
- `Mai`
- `Juni`
- `Juli`
- `August`
- `September`
- `Oktober`

- *November*
- *Dezember*

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.

Wenn die Uhrzeit im Feld *Systemzeit* den hier festgelegten Wert erreicht, schaltet das Gerät auf Winterzeit.

Woche

Legt die Woche im gegenwärtigen Monat fest.

Mögliche Werte:

- `-` (Voreinstellung)
- *erste*
- *zweite*
- *dritte*
- *vierte*
- *letzte*

Tag

Legt den Wochentag fest.

Mögliche Werte:

- `-` (Voreinstellung)
- *Sonntag*
- *Montag*
- *Dienstag*
- *Mittwoch*
- *Donnerstag*
- *Freitag*
- *Samstag*

Monat

Legt den Monat fest.

Mögliche Werte:

- `-` (Voreinstellung)
- *Januar*
- *Februar*
- *März*
- *April*
- *Mai*
- *Juni*
- *Juli*
- *August*
- *September*
- *Oktober*
- *November*
- *Dezember*

Systemzeit

Legt die Uhrzeit fest.

Mögliche Werte:

- `<HH:MM>` (Voreinstellung: `00:00`)

2.2 SNTP

[Zeit > SNTP]

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

Das Gerät ermöglicht Ihnen, 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

[Zeit > 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

Funktion

Schaltet die Funktion *SNTP Client* des Geräts ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *SNTP Client* ist eingeschaltet.
  Das Gerät arbeitet als *SNTP*-Client.
- `Aus` (Voreinstellung)
  Die Funktion *SNTP Client* ist ausgeschaltet.

Zustand

Zustand

Zeigt den Zustand des *SNTP*-Clients.

Mögliche Werte:

- `disabled`
  Der *SNTP*-Client ist ausgeschaltet.
- `notSynchronized`
  Der *SNTP*-Client ist auf keinen *SNTP*- oder *NTP*-Server synchronisiert.
- `synchronizedToRemoteServer`
  Der *SNTP*-Client ist auf einen *SNTP*- oder *NTP*-Server synchronisiert.

Konfiguration

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.

Tabelle

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 ersten Tabelleneintrag konfiguriert ist. Bleibt die Antwort des Servers aus, sendet das Gerät seine Anfragen an den *SNTP*-Server, der im nächsten Tabelleneintrag konfiguriert ist.

Wenn vorübergehend keiner der konfigurierten *SNTP*-Server antwortet, dann unterbricht 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 den Namen 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`)
- Hostname

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.

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 größeren Abständen 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.

2.2.2 SNTP Server

[Zeit > 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

Funktion

Schaltet die Funktion *SNTP Server* des Geräts ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *SNTP Server* ist eingeschaltet.
  Das Gerät arbeitet als *SNTP*-Server.
- `Aus` (Voreinstellung)
  Die Funktion *SNTP Server* ist ausgeschaltet.

Beachten Sie die Einstellung des Kontrollkästchens *Server deaktivieren bei lokaler Zeitquelle* im Rahmen *Konfiguration*.

Zustand

Zustand

Zeigt den Zustand des *SNTP*-Servers.

Mögliche Werte:

- `disabled`
  Der *SNTP*-Server ist ausgeschaltet.
- `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.

Konfiguration

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.

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 Zugriff auf das Managements des Geräts möglich ist. Siehe Dialog *Grundeinstellungen > Netz > Global*.
- `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*-Servers, wenn sich das Gerät auf die lokale Uhr synchronisiert hat.

Mögliche Werte:

- `markiert`
  Das Ausschalten des *SNTP*-Servers ist aktiv.
  Wenn das Gerät auf die lokale Uhr synchronisiert ist, dann deaktiviert das Gerät den *SNTP*-Server. 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*-Servers ist inaktiv.
  Wenn das Gerät auf die lokale Uhr synchronisiert ist, bleibt der *SNTP*-Server aktiv.

2.3 PTP

[Zeit > PTP]

Das Menü enthält die folgenden Dialoge:

- PTP Global
- PTP Boundary Clock
- PTP Transparent Clock

2.3.1 PTP Global

[Zeit > PTP > Global]

In diesem Dialog legen Sie grundlegende Einstellungen für das Protokoll *PTP* fest.

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

PTP ist erheblich genauer als SNTP. Sind im Gerät die Funktion *SNTP* und die Funktion *PTP* gleichzeitig eingeschaltet, dann hat die Funktion *PTP* Vorrang.

Anhand des *„Best Master Clock"-Algorithmus* bestimmen die Geräte im Netzwerk, welches Gerät die genauste Zeit hat. Die Geräte verwenden das Gerät mit der genauesten Zeit als Referenzzeitquelle (*Grandmaster*). Anschließend synchronisieren sich die beteiligten Geräte auf diese Referenzzeitquelle.

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

Das Protokoll unterscheidet zwischen den folgenden Uhren:

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

Funktion IEEE1588/PTP

Funktion IEEE1588/PTP

Schaltet die Funktion *PTP* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *PTP* ist eingeschaltet.
  Das Gerät synchronisiert seine Uhr mit PTP.
  Sind im Gerät die Funktion *SNTP* und die Funktion *PTP* gleichzeitig eingeschaltet, dann hat die Funktion *PTP* Vorrang.
- `Aus` (Voreinstellung)
  Die Funktion *PTP* ist ausgeschaltet.
  Das Gerät vermittelt *PTP*-Synchronisationsnachrichten ohne Korrektur auf jedem Port.

Konfiguration IEEE1588/PTP

PTP-Modus

Legt die PTP-Version und den Modus der lokalen Uhr fest.

Mögliche Werte:

- `v2-transparent-clock` (Voreinstellung)
- `v2-boundary-clock`

Untere Synchronisations-Schwelle [ns]

Legt den unteren Schwellwert in Nanosekunden fest für den Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*). Unterschreitet der Gangunterschied diesen Wert einmalig, dann gilt die lokale Uhr als synchronisiert.

Mögliche Werte:

- `1..999999999` (Voreinstellung: `30`)

Obere Synchronisations-Schwelle [ns]

Legt den oberen Schwellwert in Nanosekunden fest für den Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*). Überschreitet der Gangunterschied diesen Wert einmalig, dann gilt die lokale Uhr als unsynchronisiert.

Mögliche Werte:

- `31..1000000000` (Voreinstellung: `5000`)

PTP-Management

Aktiviert/deaktiviert das in der PTP-Norm definierte PTP-Management.

Mögliche Werte:

- `markiert`
  PTP-Management ist aktiviert.
- `unmarkiert` (Voreinstellung)
  PTP-Management ist deaktiviert.

Status

Ist synchronisiert

Zeigt, ob die lokale Uhr mit der Referenzzeitquelle (*Grandmaster*) synchronisiert ist.

Die lokale Uhr ist synchronisiert, sobald der Gangunterschied zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*) einmalig den unteren Synchronisations-Grenzwert unterschreitet. Dieser Zustand bleibt so lange erhalten, bis der Gangunterschied den oberen Synchronisations-Grenzwert einmalig überschreitet.

Die Synchronisations-Grenzwerte legen Sie fest im Rahmen *Konfiguration IEEE1588/PTP*.

Max. Offset absolut [ns]

Zeigt den maximalen Gangunterschied in Nanosekunden, der aufgetreten ist, seitdem die lokale Uhr mit der Referenzzeitquelle (*Grandmaster*) synchronisiert ist.

PTP-Zeit

Zeigt Datum und Zeit der PTP-Zeitskala, wenn die lokale Uhr mit der Referenzzeitquelle (*Grandmaster*) synchronisiert ist. Format: `TT.MM.JJJJ hh:mm:ss`

2.3.2 PTP Boundary Clock

[Zeit > PTP > Boundary Clock]

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

Das Menü enthält die folgenden Dialoge:
- PTP Boundary Clock Global
- PTP Boundary Clock Port

2.3.2.1 PTP Boundary Clock Global

[Zeit > PTP > Boundary Clock > Global]

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

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

Funktion IEEE1588/PTPv2 BC

Priorität 1

Legt die *Priorität 1* des Geräts fest.

Mögliche Werte:

▶ `0..255` (Voreinstellung: `128`)

Der *„Best Master Clock“-Algorithmus* bewertet zuerst die *Priorität 1* zwischen den beteiligten Geräten, um die Referenzzeitquelle (*Grandmaster*) zu bestimmen.

Je niedriger Sie den Wert einstellen, desto wahrscheinlicher wird das Gerät Referenzzeitquelle (*Grandmaster*). Siehe Rahmen *Grandmaster*.

Priorität 2

Legt die *Priorität 2* des Geräts fest.

Mögliche Werte:

▶ `0..255` (Voreinstellung: `128`)

Wenn die zuvor bewerteten Kriterien bei mehreren Geräten gleich sind, bewertet der *„Best Master Clock“-Algorithmus* die *Priorität 2* der beteiligten Geräte.

Je niedriger Sie den Wert einstellen, desto wahrscheinlicher wird das Gerät Referenzzeitquelle (*Grandmaster*). Siehe Rahmen *Grandmaster*.

Domänen-Nummer

Weist das Gerät einer *PTP*-Domäne zu.

Mögliche Werte:

▶ `0..255` (Voreinstellung: `0`)

Das Gerät überträgt Zeitinformationen ausschließlich von und zu Geräten in derselben Domäne.

Status IEEE1588/PTPv2 BC

Two step

Zeigt, dass die Uhr im Two-Step-Modus arbeitet.

Steps removed

Zeigt die Anzahl der durchlaufenen Kommunikationspfade zwischen der lokalen Uhr des Geräts und der Referenzzeitquelle (*Grandmaster*).

Für einen *PTP*-Slave bedeutet der Wert `1`, dass die Uhr direkt über 1 Kommunikationspfad mit der Referenzzeitquelle (*Grandmaster*) verbunden ist.

Offset zum Master [ns]

Zeigt die gemessene Differenz (Offset) zwischen lokaler Uhr und Referenzzeitquelle (*Grandmaster*) in Nanosekunden. Der *PTP*-Slave berechnet den die Differenz aus den empfangenen Zeitinformationen.

Im Two-Step-Modus besteht die Zeitinformation aus je 2 *PTP*-Synchronisationsnachrichten, die der *PTP*-Master zyklisch sendet:

- Die 1. Synchronisationsnachricht (Sync Message) enthält einen geschätzten Wert des exakten Sendezeitpunktes der Nachricht.
- Die 2. Synchronisationsnachricht (Follow-Up Message) enthält den exakten Sendezeitpunkt der 1. Nachricht.

Der *PTP*-Slave berechnet aus beiden *PTP*-Synchronisationsnachrichten die Differenz (Offset) zum Master und korrigiert seine Uhr um diesen Differenz. Dabei berücksichtigt der *PTP*-Slave den *Laufzeit zum Master [ns]*-Wert.

Laufzeit zum Master [ns]

Zeigt die Laufzeit (Delay) beim Übertragen der *PTP*-Synchronisationsnachrichten vom *PTP*-Master zum *PTP*-Slave in Nanosekunden.

Der *PTP*-Slave sendet ein „Delay Request“-Paket an den *PTP*-Master und ermittelt dabei die exakte Sendezeit des Pakets. Der *PTP*-Master generiert bei Empfang des Pakets einen Zeitstempel und sendet diesen in einem „Delay Response“-Paket an den *PTP*-Slave zurück. Der *PTP*-Slave berechnet aus beiden Paketen die Laufzeit (Delay) und berücksichtigt sie ab der nächsten Offset-Messung.

Voraussetzung ist, dass für den Laufzeitmess-Mechanismus des Slave-Ports der Wert `e2e` festgelegt ist.

Grandmaster

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

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

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

Priorität 1

Zeigt die *Priorität 1* des Geräts, das gegenwärtig Referenzzeitquelle (*Grandmaster*) ist.

Uhr-Klasse

Zeigt die Klasse der Referenzzeitquelle (*Grandmaster*). Kenngröße für den *Best-Master-Clock-Algoritmus*.

Präzision

Zeigt die geschätzte Ganggenauigkeit der Referenzzeitquelle (*Grandmaster*). Kenngröße für den *Best-Master-Clock-Algoritmus*.

Uhr-Varianz

Zeigt die Varianz der Referenzzeitquelle (*Grandmaster*), auch bezeichnet als *Offset scaled log variance*. Kenngröße für den *Best-Master-Clock-Algoritmus*.

Priorität 2

Zeigt die *Priorität 2* des Geräts, das gegenwärtig Referenzzeitquelle (*Grandmaster*) ist.

Lokale Zeit-Eigenschaften

Quelle der Zeit

Legt fest, von welcher Zeitquelle die lokale Uhr ihre Zeitinformation bezieht.

Mögliche Werte:

- `atomicClock`
- `gps`
- `terrestrialRadio`
- `ptp`
- `ntp`
- `handSet`
- `other`
- `internalOscillator` (Voreinstellung)

UTC-Offset [s]

Legt die Differenz der *PTP*-Zeitskala zur UTC fest.

Siehe Kontrollkästchen *PTP-Zeitskala*.

Mögliche Werte:

- `-32768..32767`

Anmerkung: Voreingestellt ist der zum Zeitpunkt der Erstellung der Geräte-Software gültige Wert. Weitere Informationen finden Sie im „Bulletin C“ des International Earth Rotation and Reference Systems Service (IERS): http://www.iers.org/IERS/EN/Publications/Bulletins/bulletins.html

UTC-Offset gültig

Legt fest, ob der im Feld *UTC-Offset [s]* festgelegte Wert korrekt ist.

Mögliche Werte:

- `markiert`
- `unmarkiert` (Voreinstellung)

Zeit nachvollziehbar

Zeigt, ob das Gerät die Zeit von einer primären UTC-Referenz bezieht, zum Beispiel von einem NTP-Server.

Mögliche Werte:

- `markiert`
- `unmarkiert`

Frequenz nachvollziehbar

Zeigt, ob das Gerät die Frequenz von einer primären UTC-Referenz bezieht, zum Beispiel von einem NTP-Server.

Mögliche Werte:

- `markiert`
- `unmarkiert`

PTP-Zeitskala

Zeigt, ob das Gerät die PTP-Zeitskala verwendet.

Mögliche Werte:

- `markiert`
- `unmarkiert`

Die PTP-Zeitskala ist laut IEEE 1588 die Atomzeit TAI mit dem Startzeitpunkt 01.01.1970.

Im Gegensatz zu UTC kennt TAI keine Schaltsekunden.

Mit Stand vom 1. Juli 2020 geht die TAI-Zeit 37 s gegenüber der UTC-Zeit vor.

Kennungen

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

Die Identifikationsnummern (UUID) setzen sich wie folgt zusammen:
- Die Geräte-Identifikationsnummer besteht aus der MAC-Adresse des Geräts, erweitert um die Werte `ff` und `fe` zwischen Byte 3 und Byte 4.
- Die Port-UUID besteht aus der Geräte-Identifikationsnummer, gefolgt von einer 16-bit-Port-ID.

Uhr-Kennung

Zeigt die eigene Identifikationsnummer (UUID) des Geräts.

Port-Kennung Parent

Zeigt die Port-Identifikationsnummer (UUID) des direkt übergeordneten Master-Geräts.

Grandmaster-Kennung

Zeigt die Identifikationsnummer (UUID) des Geräts der Referenzzeitquellen (*Grandmaster*).

2.3.2.2 PTP Boundary Clock Port

[Zeit > PTP > Boundary Clock > Port]

In diesem Dialog legen Sie für jeden einzelnen Port die Einstellungen der *Boundary Clock (BC)* fest.

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

PTP an

Aktiviert/deaktiviert die Übertragung von *PTP*-Synchronisationsnachrichten auf dem Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Übertragung ist aktiviert. Der Port vermittelt und empfängt *PTP*-Synchronisationsnachrichten.
- `unmarkiert`
  Die Übertragung ist deaktiviert. Der Port blockiert *PTP*-Synchronisationsnachrichten.

PTP-Status

Zeigt den gegenwärtigen Zustand des Ports.

Mögliche Werte:

- *initializing*
  Initialisierungsphase
- *faulty*
  Faulty Modus: Fehler im PTP-Protokoll.
- *disabled*
  PTP ist auf dem Port ausgeschaltet.
- *listening*
  Port wartet auf *PTP*-Synchronisationsnachrichten.
- *pre-master*
  PTP-Pre-Master-Modus
- *master*
  PTP-Master-Modus
- *passiv*
  PTP-Passiv-Modus
- *uncalibrated*
  PTP-Unkalibriert-Modus
- *slave*
  PTP-Slave-Modus

Sync-Intervall [s]

Legt das Intervall in Sekunden fest, in welchem der Port *PTP*-Synchronisationsnachrichten überträgt.

Mögliche Werte:

- `0.25`
- `0.5`
- `1` (Voreinstellung)
- `2`

Laufzeitmess-Mechanismus

Legt den Mechanismus fest, mit dem das Gerät die Laufzeit (Delay) beim Übertragen der *PTP*-Synchronisationsnachrichten misst.

Mögliche Werte:

- *`disabled`*
  Die Messung der Laufzeit (Delay) der *PTP*-Synchronisationsnachrichten zu den angeschlossenen PTP-Geräten ist deaktiviert.
- *`e2e`* (Voreinstellung)
  End-to-End: Als *PTP*-Slave misst der Port die Laufzeit der *PTP*-Synchronisationsnachrichten zum *PTP*-Master.
  Das Gerät zeigt den Messwert im Dialog *Zeit > PTP > Boundary Clock > Global*.
- *`p2p`*
  Peer-to-Peer: Das Gerät misst die Laufzeit (Delay) der *PTP*-Synchronisationsnachrichten zu allen angeschlossenen PTP-Geräten, vorausgesetzt, diese Geräte unterstützen P2P.
  Dieser Mechanismus erspart dem Gerät im Fall einer Rekonfiguration, die Laufzeit erneut zu ermitteln.

P2P-Laufzeit

Zeigt die gemessene Peer-to-Peer-Laufzeit der *PTP*-Synchronisationsnachrichten.

Voraussetzung ist, dass Sie in Spalte *Laufzeitmess-Mechanismus* den Wert *`p2p`* festlegen.

P2P-Laufzeitmess-Intervall [s]

Legt das Intervall in Sekunden fest, in welchem der Port die Peer-to-Peer-Laufzeit misst.

Voraussetzung ist, dass Sie den Wert *`p2p`* auf diesem Port und auf dem Port der Gegenstelle eingestellt haben.

Mögliche Werte:

- `1` (Voreinstellung)
- `2`
- `4`
- `8`
- `16`
- `32`

Netz-Protokoll

Legt fest, welches Protokoll der Port für das Übertragen der *PTP*-Synchronisationsnachrichten verwendet.

Mögliche Werte:

- `IEEE 802.3` (Voreinstellung)
- `UDP/IPv4`

Announce-Intervall [s]

Legt das Intervall in Sekunden fest, in welchem der Port Nachrichten für die PTP-Topologieerkennung überträgt.

Weisen Sie jedem Gerät einer *PTP*-Domäne denselben Wert zu.

Mögliche Werte:

- `1`
- `2` (Voreinstellung)
- `4`
- `8`
- `16`

Announce-Timeout

Legt die Anzahl der Announce-Intervalle fest.

Beispiel:

In der Voreinstellung (*Announce-Intervall [s]* = `2` und *Announce-Timeout* = `3`) beträgt das Timeout 3 × 2 s = 6 s.

Mögliche Werte:

- `2..10` (Voreinstellung: `3`)
  Weisen Sie jedem Gerät einer *PTP*-Domäne denselben Wert zu.

E2E-Laufzeitmess-Intervall [s]

Zeigt das Intervall in Sekunden, in welchem der Port die End-to-End-Laufzeit misst:

- Arbeitet der Port als *PTP*-Master, weist das Gerät dem Port den Wert `8` zu.
- Arbeitet der Port als *PTP*-Slave, legt der mit dem Port verbundene *PTP*-Master den Wert fest.

V1-Hardware-Kompatibilität

Legt fest, ob der Port die Länge der *PTP*-Synchronisationsnachrichten anpasst, wenn Sie in Spalte *Netz-Protokoll* den Wert `udpIpv4` festgelegt haben.

Unter Umständen erwarten andere Geräte im Netz die *PTP*-Synchronisationsnachrichten in der Länge von PTPv1-Nachrichten.

Mögliche Werte:

- `auto` (Voreinstellung)
  Das Gerät erkennt automatisch, ob andere Geräte im Netz *PTP*-Synchronisationsnachrichten in der Länge von PTPv1-Nachrichten erwarten. Ist das der Fall, erweitert das Gerät die Länge der *PTP*-Synchronisationsnachrichten vor dem Übertragen.

- `on`
  Das Gerät erweitert die Länge der *PTP*-Synchronisationsnachrichten vor dem Übertragen.
- `off`
  Das Gerät überträgt *PTP*-Synchronisationsnachrichten und behält die Länge bei.

Asymmetrie

Korrigiert den durch asymmetrische Übertragungswege verfälschten Laufzeitmesswert.

Mögliche Werte:

- `-2000000000..2000000000` (Voreinstellung: `0`)

Der Wert repräsentiert die Laufzeitasymmetrie in Nanosekunden.

Ein Laufzeitmesswert von y ns ns entspricht einer Asymmetrie von y × 2 ns.

Der Wert ist positiv, wenn die Laufzeit vom *PTP*-Master zum *PTP*-Slave länger ist als in umgekehrter Richtung.

VLAN

Legt die VLAN-ID fest, mit der das Gerät die *PTP*-Synchronisationsnachrichten auf diesem Port markiert.

Mögliche Werte:

- `kein` (Voreinstellung)
  Das Gerät überträgt *PTP*-Synchronisationsnachrichten ohne VLAN-Tag.
- `0..4042`
  VLANs, die Sie im Gerät bereits eingerichtet haben, wählen Sie in der Liste aus.

Vergewissern Sie sich, dass der Port Mitglied des VLANs ist.

Siehe Dialog *Switching > VLAN > Konfiguration*.

VLAN-Priorität

Legt die Priorität fest, mit der das Gerät die mit VLAN-ID markierten *PTP*-Synchronisationsnachrichten überträgt (Schicht 2, IEEE 802.1D).

Mögliche Werte:

- `0..7` (Voreinstellung: `6`)

Wenn Sie in Spalte *VLAN* den Wert `kein` festgelegt haben, dann ignoriert das Gerät die VLAN-Priorität.

2.3.3 PTP Transparent Clock

[Zeit > PTP > Transparent Clock]

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

Das Menü enthält die folgenden Dialoge:

- PTP Transparent Clock Global
- PTP Transparent Clock Port

2.3.3.1 PTP Transparent Clock Global

[Zeit > PTP > Transparent Clock > Global]

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

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

Funktion IEEE1588/PTPv2 TC

Laufzeitmess-Mechanismus

Legt den Mechanismus fest, mit dem das Gerät die Laufzeit (Delay) beim Übertragen der *PTP*-Synchronisationsnachrichten misst.

Mögliche Werte:

- `e2e` (Voreinstellung)
  Als *PTP*-Slave misst der Port die Laufzeit der *PTP*-Synchronisationsnachrichten zum *PTP*-Master.
  Das Gerät zeigt den Messwert im Dialog *Zeit > PTP > Transparent Clock > Global*.
- `p2p`
  Das Gerät misst die Laufzeit (Delay) der *PTP*-Synchronisationsnachrichten zu allen angeschlossenen PTP-Geräten, vorausgesetzt, diese Geräte unterstützen P2P.
  Dieser Mechanismus erspart dem Gerät im Fall einer Rekonfiguration, die Laufzeit erneut zu ermitteln.
  Wenn Sie diesen Wert festlegen, dann ist in Spalte *Netz-Protokoll* ausschließlich der Wert `IEEE 802.3` verfügbar.
- `e2e-optimized`
  Wie `e2e`, mit folgenden Besonderheiten:
  - Delay-Anfragen der *PTP*-Slaves vermittelt das Gerät ausschließlich an den *PTP*-Master, obwohl diese Anfragen Multicast-Nachrichten sind. Das Gerät entlastet damit die anderen Geräte von unnötigen Multicast-Anfragen.
  - Wenn sich die Master-Slave-Topologie ändert, lernt das Gerät den Port zum *PTP*-Master um, sobald es eine Synchronisationsnachricht von einem anderen *PTP*-Master empfängt.
  - Wenn das Gerät keinen *PTP*-Master kennt, dann überträgt es Delay-Anfragen an die Ports.
- `disabled`
  Auf dem Port ist die Laufzeitmessung ausgeschaltet. Das Gerät verwirft Nachrichten für die Laufzeitmessung.

Primäre Domäne

Weist das Gerät einer *PTP*-Domäne zu.

Mögliche Werte:

- `0..255` (Voreinstellung: `0`)

Das Gerät überträgt Zeitinformationen ausschließlich von und zu Geräten in derselben Domäne.

Netz-Protokoll

Legt fest, welches Protokoll der Port für das Übertragen der *PTP*-Synchronisationsnachrichten verwendet.

Mögliche Werte:

- `ieee8023` (Voreinstellung)
- `udpIpv4`

Multi-Domain-Modus

Aktiviert/deaktiviert in jeder *PTP*-Domäne die Korrektur von *PTP*-Synchronisationsnachrichten.

Mögliche Werte:

- `markiert`
  Das Gerät korrigiert *PTP*-Synchronisationsnachrichten in jeder *PTP*-Domäne.
- `unmarkiert` (Voreinstellung)
  Das Gerät korrigiert *PTP*-Synchronisationsnachrichten ausschließlich in der primären *PTP*-Domäne. Siehe Feld *Primäre Domäne*.

VLAN-ID

Legt die VLAN-ID fest, mit der das Gerät die *PTP*-Synchronisationsnachrichten auf diesem Port markiert.

Mögliche Werte:

- `kein` (Voreinstellung)
  Das Gerät überträgt *PTP*-Synchronisationsnachrichten ohne VLAN-Tag.
- `0..4042`
  VLANs, die Sie im Gerät bereits eingerichtet haben, wählen Sie in der Liste aus.

VLAN-Priorität

Legt die Priorität fest, mit der das Gerät die mit VLAN-ID markierten *PTP*-Synchronisationsnachrichten überträgt (Schicht 2, IEEE 802.1D).

Mögliche Werte:

- `0..7` (Voreinstellung: `6`)

Wenn Sie im Feld *VLAN-ID* den Wert `kein` festgelegt haben, dann ignoriert das Gerät den hier eingestellten Wert.

Lokale Synchronisation

Syntonize

Aktiviert/deaktiviert die Frequenz-Synchronisation der *Transparent Clock* mit dem *PTP*-Master.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Frequenz-Synchronisation ist aktiv.
  Das Gerät synchronisiert die Frequenz.
- `unmarkiert`
  Die Frequenz-Synchronisation ist inaktiv.
  Die Frequenz bleibt konstant.

Lokale Uhr synchronisieren

Aktiviert/deaktiviert die Synchronisation der lokalen Systemzeit.

Mögliche Werte:

- `markiert`
  Die Synchronisation ist aktiv.
  Das Gerät synchronisiert die lokale Systemzeit mit der per PTP empfangenen Uhrzeit. Voraussetzung ist, dass das Kontrollkästchen *Syntonize* markiert ist.
- `unmarkiert` (Voreinstellung)
  Die Synchronisation ist inaktiv.
  Die lokale Systemzeit bleibt konstant.

Aktueller Master

Zeigt die Port-Identifikationsnummer (UUID) des direkt übergeordneten Master-Geräts, auf welches das Gerät seine Frequenz synchronisiert.

Enthält der Wert ausschließlich Nullen, hat das die folgende Ursache:

- Die Funktion *Syntonize* ist ausgeschaltet.
  oder
- Das Gerät findet keinen *PTP*-Master.

Offset zum Master [ns]

Zeigt die gemessene Differenz (Offset) zwischen lokaler Uhr und dem *PTP*-Master in Nanosekunden. Das Gerät berechnet den die Differenz aus den empfangenen Zeitinformationen.

Voraussetzung ist, dass die Funktion *Lokale Uhr synchronisieren* eingeschaltet ist.

Laufzeit zum Master [ns]

Zeigt die Laufzeit (Delay) beim Übertragen der *PTP*-Synchronisationsnachrichten vom *PTP*-Master zum *PTP*-Slave in Nanosekunden.

Voraussetzung:

- Die Funktion *Lokale Uhr synchronisieren* ist eingeschaltet.
- Im Feld *Laufzeitmess-Mechanismus* ist der Wert `e2e` ausgewählt.

Status IEEE1588/PTPv2 TC

Uhr-Kennung

Zeigt die eigene Identifikationsnummer (UUID) des Geräts.

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

Die Geräte-Identifikationsnummer besteht aus der MAC-Adresse des Geräts, erweitert um die Werte `ff` und `fe` zwischen Byte 3 und Byte 4.

2.3.3.2 PTP Transparent Clock Port

[Zeit > PTP > Transparent Clock > Port]

In diesem Dialog legen Sie für jeden einzelnen Port die Einstellungen der *Transparent Clock (TC)* fest.

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

PTP an

Aktiviert/deaktiviert die Übertragung von *PTP*-Synchronisationsnachrichten auf dem Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Übertragung ist aktiv.
  Der Port vermittelt und empfängt *PTP*-Synchronisationsnachrichten.
- `unmarkiert`
  Die Übertragung ist inaktiv.
  Der Port blockiert *PTP*-Synchronisationsnachrichten.

P2P-Laufzeitmess-Intervall [s]

Legt das Intervall in Sekunden fest, in welchem der Port die Peer-to-Peer-Laufzeit misst.

Voraussetzung ist, dass Sie den Wert `p2p` auf diesem Port und auf dem Port der Gegenstelle festlegen. Siehe Optionsliste *Laufzeitmess-Mechanismus* im Dialog *Zeit > PTP > Transparent Clock > Global*.

Mögliche Werte:

- `1` (Voreinstellung)
- `2`
- `4`
- `8`
- `16`
- `32`

P2P-Laufzeit

Zeigt die gemessene Peer-to-Peer-Laufzeit der *PTP*-Synchronisationsnachrichten.

Voraussetzung ist, dass Sie in der Optionsliste *Laufzeitmess-Mechanismus* das Optionsfeld `p2p` auswählen. Siehe Feld *Laufzeitmess-Mechanismus* im Dialog *Zeit > PTP > Transparent Clock > Global*.

Asymmetrie

Korrigiert den durch asymmetrische Übertragungswege verfälschten Laufzeitmesswert.

Mögliche Werte:

▶ `-2000000000..2000000000` (Voreinstellung: `0`)

Der Wert repräsentiert die Laufzeitasymmetrie in Nanosekunden.

Ein Laufzeitmesswert von y ns ns entspricht einer Asymmetrie von y × 2 ns.

Der Wert ist positiv, wenn die Laufzeit vom *PTP*-Master zum *PTP*-Slave länger ist als in umgekehrter Richtung.

3 Gerätesicherheit

Das Menü enthält die folgenden Dialoge:
- Benutzerverwaltung
- Authentifizierungs-Liste
- LDAP
- Management-Zugriff
- Pre-Login-Banner

3.1 Benutzerverwaltung

[Gerätesicherheit > Benutzerverwaltung]

Das Gerät ermöglicht Benutzern den Zugriff auf das Management des Geräts, 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 ermöglicht Ihnen, Einstellungen für das Login festzulegen.

Login-Versuche

Legt die Anzahl der möglichen Login-Versuche fest, wenn der Benutzer auf das Management des Geräts über die grafische Benutzeroberfläche oder das Command Line Interface zugreift.

Anmerkung: Beim Zugriff auf das Management des Geräts mittels des Command Line Interface über die serielle Schnittstelle ist die Anzahl der Login-Versuche unbegrenzt.

Mögliche Werte:
- `0..5` (Voreinstellung: `0`)

Wenn sich der Benutzer ein weiteres Mal ohne Erfolg anmeldet, sperrt das Gerät für den Benutzer den Zugriff auf das Gerät.

Das Gerät ermöglicht ausschließlich Benutzern mit der Berechtigung `administrator`, die Sperre aufzuheben.

Der Wert `0` deaktiviert die Sperre. Der Benutzer hat beliebig viele Versuche, sich anzumelden.

Zeitraum für Login-Versuche (min.)

Zeigt die Zeitspanne, nach der das Gerät den Zähler im Feld *Login-Versuche* zurücksetzt.

Mögliche Werte:

▶ `0..60` (Voreinstellung: `0`)

Min. Passwort-Länge

Das Gerät akzeptiert das Passwort, wenn es sich aus mindestens so vielen Zeichen zusammensetzt, wie hier festgelegt.

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 ermöglicht Ihnen, 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.

Großbuchstaben (min.)

Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Großbuchstaben enthält, wie hier festgelegt.

Mögliche Werte:

▶ `0..16` (Voreinstellung: `1`)

Der Wert `0` deaktiviert diese Richtlinie.

Kleinbuchstaben (min.)

Das Gerät akzeptiert das Passwort, wenn es mindestens so viele Kleinbuchstaben enthält, wie hier festgelegt.

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 festgelegt.

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 festgelegt.

Mögliche Werte:

- `0..16` (Voreinstellung: `1`)

Der Wert `0` deaktiviert diese Richtlinie.

Tabelle

Jeder Benutzer benötigt ein aktives Benutzerkonto, um Zugriff auf das Management des Geräts zu erhalten. Die Tabelle ermöglicht Ihnen, Benutzerkonten einzurichten und zu verwalten. Um Einstellungen zu ändern, klicken Sie in der Tabelle den gewünschten Parameter und modifizieren den Wert.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

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

Löschen

Entfernt den ausgewählten Tabelleneintrag.

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 diesem Benutzernamen.
- `unmarkiert` (Voreinstellung)
  Das Benutzerkonto ist inaktiv. Das Gerät verweigert die Anmeldung eines Benutzers mit diesem Benutzernamen.

Wenn ausschließlich 1 Benutzerkonto mit der Berechtigung `administrator` existiert, ist dieses Benutzerkonto stets aktiv.

Passwort

Legt das Passwort fest, das der Benutzer für Zugriffe auf das Management des Geräts über die grafische Benutzeroberfläche oder das Command Line Interface verwendet.

Zeigt ***** (Sternchen) anstelle des Passworts, mit dem sich der Benutzer anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

Wenn Sie das Passwort erstmalig festlegen, verwendet das Gerät in den Spalten *SNMP-Authentifizierungspasswort* und *SNMP-Verschlüsselungspasswort* dasselbe Passwort.

- Das Gerät ermöglicht Ihnen, in den Spalten *SNMP-Authentifizierungspasswort* und *SNMP-Verschlüsselungspasswort* unterschiedliche Passwörter festzulegen.
- Wenn Sie das Passwort in der gegenwärtigen Spalte ändern, dann ändert das Gerät auch die Passwörter für die Spalten *SNMP-Authentifizierungspasswort* und *SNMP-Verschlüsselungspasswort*, allerdings ausschließlich dann, wenn diese zuvor nicht individuell angepasst wurden.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen
  Das Gerät akzeptiert die folgenden Zeichen:
  - `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, dann prüft das Gerät das Passwort gemäß der im Rahmen *Passwort-Richtlinien* festgelegten Richtlinien.

Das Gerät prüft stets die Mindestlänge des Passworts, auch wenn das Kontrollkästchen in Spalte *Richtlinien überprüfen*`unmarkiert` ist.

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, dann 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 Zugriff auf das Management des Geräts.
  Das Gerät sperrt einen Benutzer automatisch, wenn dieser zu oft erfolglos versucht, sich anzumelden.
- `unmarkiert` (ausgegraut) (Voreinstellung)
  Das Benutzerkonto ist entsperrt. Der Benutzer hat Zugriff auf das Management des Geräts.

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-Authentifizierungspasswort

Legt das Passwort fest, welches das Gerät beim Zugriff des Benutzers per SNMPv3 anwendet.

Zeigt ***** (Sternchen) anstelle des Passworts, mit dem sich der Benutzer anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

In der Voreinstellung verwendet das Gerät dasselbe Passwort, das Sie in Spalte *Passwort* festlegen.

- In der gegenwärtigen Spalte erlaubt Ihnen das Gerät, ein anderes Passwort als in Spalte *Passwort* festzulegen.
- Wenn Sie das Passwort in Spalte *Passwort* ändern, dann ändert das Gerät auch das Passwort für die gegenwärtige Spalte, allerdings ausschließlich dann, wenn dieses zuvor nicht individuell angepasst wurde.

Mögliche Werte:

▶ Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen
Das Gerät akzeptiert die folgenden Zeichen:
- `a..z`
- `A..Z`
- `0..9`
- `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

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

SNMP-Verschlüsselungspasswort

Legt das Passwort fest, welches das Gerät zur Verschlüsselung beim Zugriff des Benutzers per SNMPv3 anwendet.

Zeigt ***** (Sternchen) anstelle des Passworts, mit dem sich der Benutzer anmeldet. Um das Passwort zu ändern, klicken Sie in das betreffende Feld.

In der Voreinstellung verwendet das Gerät dasselbe Passwort, das Sie in Spalte *Passwort* festlegen.

- In der gegenwärtigen Spalte erlaubt Ihnen das Gerät, ein anderes Passwort als in Spalte *Passwort* festzulegen.
- Wenn Sie das Passwort in Spalte *Passwort* ändern, dann ändert das Gerät auch das Passwort für die gegenwärtige Spalte, allerdings ausschließlich dann, wenn dieses zuvor nicht individuell angepasst wurde.

Mögliche Werte:

▶ Alphanumerische ASCII-Zeichenfolge mit 6..64 Zeichen
Das Gerät akzeptiert die folgenden Zeichen:
- `a..z`
- `A..Z`
- `0..9`
- `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

3.2 Authentifizierungs-Liste

[Gerätesicherheit > 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 ermöglicht Benutzern den Zugriff auf das Management des Geräts, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Benutzer mit folgenden Methoden:
- Benutzerverwaltung des Geräts
- LDAP
- RADIUS

Mit der Port-basierten Zugriffskontrolle gemäß IEEE 802.1X ermöglicht das Gerät angeschlossenen Endgeräten den 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.
- Im Feld *Name* legen Sie den Namen der Liste fest.
  Mögliche Werte:
  – Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Löschen

Entfernt den ausgewählten Tabelleneintrag.

Anwendungen zuordnen

Öffnet das Fenster *Anwendungen zuordnen*. Das Fenster zeigt die Anwendungen, die Sie der ausgewählten Liste zuordnen können.

- Klicken und wählen Sie einen Eintrag, um diesen der gegenwärtig ausgewählten Liste zuzuordnen.
  Eine Anwendung, die bereits einer anderen Liste zugeordnet ist, ordnet das Gerät der gegenwärtig ausgewählten Liste zu, sobald Sie die Schaltfläche *Ok* klicken.
- Klicken und wählen Sie einen Eintrag ab, um dessen Zuordnung zur gegenwärtig ausgewählten Liste rückgängig zu machen.
  Wenn Sie die Anwendung `WebInterface` abwählen, dann bricht die Verbindung zum Gerät ab, sobald Sie auf Schaltfläche *Ok* klicken.

Name

Zeigt die Bezeichnung der Liste.

Um eine neue Liste anzulegen, klicken Sie die Schaltfläche .

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 Anmeldedaten 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 Anmeldedaten 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* oder *ldap* 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- oder LDAP-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.
- *ldap*
  Das Gerät authentifiziert die Benutzer über Authentifizierungsdaten und die Zugriffsrolle, die an einem zentralen Ort gespeichert sind. Den vom Gerät verwendeten Active-Directory-Server legen Sie im Dialog *Netzsicherheit > LDAP > Konfiguration* fest.

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 . Das Gerät ermöglicht Ihnen, jede Anwendung genau einer Liste zuzuordnen.

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.

3.3 LDAP

[Gerätesicherheit > LDAP]

Das Lightweight Directory Access Protocol (LDAP) ermöglicht Ihnen, die Benutzer an einer zentralen Stelle im Netz zu authentifizieren und zu autorisieren. Ein weit verbreiteter, mit LDAP abfragbarer Verzeichnisdienst ist Active Directory®.

Das Gerät leitet die Zugangsdaten der Benutzer mit dem LDAP-Protokoll weiter an den Authentication-Server. Der Authentication-Server entscheidet, ob die Zugangsdaten gültig sind und übermittelt dem Gerät die Berechtigungen des Benutzers.

Nach erfolgreicher Anmeldung speichert das Gerät die Anmeldeinformationen temporär zwischen. Dies beschleunigt den Anmeldevorgang, wenn sich Benutzer erneut anmelden. In diesem Fall ist keine aufwendige LDAP-Suchoperation notwendig.

Das Menü enthält die folgenden Dialoge:
- LDAP Konfiguration
- LDAP Rollen-Zuweisung

3.3.1 LDAP Konfiguration

[Gerätesicherheit > LDAP > Konfiguration]

Dieser Dialog ermöglicht Ihnen, bis zu 4 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 ersten Authentication-Server. Bleibt dessen Antwort aus, kontaktiert das Gerät den jeweils nächsten Server in der Tabelle.

Funktion

Funktion

Schaltet den *LDAP*-Client ein/aus.

Das Gerät verwendet den *LDAP*-Client, wenn Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* den Wert `ldap` in einer der Spalten *Richtlinie 1* bis *Richtlinie 5* festlegen. Legen Sie zuvor im Dialog *Gerätesicherheit > LDAP > Rollen-Zuweisung* mindestens ein Mapping für die Rolle `administrator` fest. Damit haben Sie nach Anmeldung über LDAP weiterhin als Administrator Zugriff auf das Gerät.

Mögliche Werte:

- `An`
  Der *LDAP*-Client ist eingeschaltet.
- `Aus` (Voreinstellung)
  Der *LDAP*-Client ist ausgeschaltet.

Konfiguration

Client-Cache-Timeout [min]

Legt fest, wie viele Minuten die Anmeldeinformation nach erfolgreicher Anmeldung eines Benutzers gültig bleibt. Wenn ein Benutzer sich innerhalb dieser Zeit erneut anmeldet, ist keine aufwendige LDAP-Suchoperation notwendig. Der Anmeldevorgang ist deutlich schneller.

Mögliche Werte:

- `1..1440` (Voreinstellung: `10`)

Bind-Benutzer

Legt die Benutzerkennung in Form des „Distinguished Name“ (DN) fest, mit der das Gerät sich am LDAP-Server anmeldet.

Diese Angabe ist erforderlich, wenn der LDAP-Server bei der Anmeldung eine Benutzerkennung in Form des „Distinguished Name“ (DN) erfordert. In Active-Directory-Umgebungen ist diese Angabe nicht erforderlich.

Das Gerät meldet sich mit dieser Benutzerkennung am LDAP-Server an, um den „Distinguished Name“ (DN) für sich anmeldende Benutzer zu finden. Das Gerät sucht gemäß den Einstellungen in den Feldern *Base DN* und *Benutzername-Attribut*.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Bind-Benutzer Passwort

Legt das Passwort fest, das das Gerät bei der Anmeldung am LDAP-Server zusammen mit der in Feld *Bind-Benutzer* festgelegten Benutzerkennung verwendet.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

Base DN

Legt den Startpunkt in Form des „Distinguished Name“ (DN) fest für die Suche im Verzeichnisbaum.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Benutzername-Attribut

Legt das LDAP-Attribut fest, das einen eineindeutigen Benutzernamen enthält. Später verwendet der Benutzer den in diesem Attribut enthaltenen Benutzernamen, um sich anzumelden.

Häufig enthalten die LDAP-Attribute `userPrincipalName`, `mail`, `sAMAccountName` und `uid` einen eineindeutigen Benutzernamen.

Unter der folgenden Voraussetzung fügt das Gerät die im Feld *Default-Domain* festgelegte Zeichenfolge an den Benutzernamen an:

- Der im Attribut enthaltene Benutzername enthält kein @-Zeichen.
- Im Feld *Default-Domain* ist ein Domänenname festgelegt.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen
  (Voreinstellung: `userPrincipalName`)

Default-Domain

Legt die Zeichenfolge fest, mit der das Gerät den Benutzernamen sich anmeldender Benutzer ergänzt, sofern der Benutzername kein @-Zeichen enthält.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

CA certificate

URL

Legt Pfad und Dateiname des Zertifikats fest.

Zulässig sind Zertifikate mit folgenden Eigenschaften:

- X.509-Format
- `.PEM` Dateinamenserweiterung
- Base64-kodiert, umschlossen von
  `-----BEGIN CERTIFICATE-----`
  und
  `-----END CERTIFICATE-----`

Aus Sicherheitsgründen empfehlen wir, stets ein Zertifikat zu verwenden, das von einer Zertifizierungsstelle signiert ist.

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 der folgenden 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 der folgenden 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 der folgenden 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.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Cache leeren

Entfernt die zwischengespeicherten Anmeldeinformationen der erfolgreich angemeldeten Benutzer.

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Beschreibung

Legt die Beschreibung fest.

Wenn gewünscht, beschreiben Sie hier den Authentication-Server oder notieren zusätzliche Informationen.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Adresse

Legt IP-Adresse oder DNS-Name des Servers fest.

Mögliche Werte:

- IPv4-Adresse (Voreinstellung: `0.0.0.0`)
- DNS-Name im Format `<domain>.<tld>` oder `<host>.<domain>.<tld>`
- `_ldap._tcp.<domain>.<tld>`
  Mit diesem DNS-Namen erfragt das Gerät die LDAP-Server-Liste (SRV Resource Record) beim DNS-Server.

Verwenden Sie einen DNS-Namen, wenn in Spalte *Verbindungssicherheit* ein anderer Wert als `kein` festgelegt ist und das Zertifikat ausschließlich DNS-Namen des Servers enthält. Schalten Sie die Funktion *Client* im Dialog *Erweitert > DNS > Client > Global* ein.

Ziel-TCP-Port

Legt den TCP-Port fest, auf dem der Server die Anfragen erwartet.

Wenn in Spalte *Adresse* der Wert `_ldap._tcp.domain.tld` festgelegt ist, dann ignoriert das Gerät den hier festgelegten Wert.

Mögliche Werte:

- `0..65535` (Voreinstellung: `389`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Häufig verwendete TCP-Ports:

- `LDAP`: `389`
- `LDAP over SSL`: `636`

- `Active Directory Global Catalogue: 3268`
- `Active Directory Global Catalogue SSL: 3269`

Verbindungssicherheit

Legt das Protokoll fest, das die Kommunikation zwischen Gerät und Authentication-Server verschlüsselt.

Mögliche Werte:

- *kein*
  Keine Verschlüsselung.
  Das Gerät baut eine LDAP-Verbindung zum Server auf und überträgt die Kommunikation inklusive Passwörter im Klartext.
- *ssl*
  Verschlüsselung mit SSL.
  Das Gerät baut eine TLS-Verbindung zum Server auf und tunnelt darüber die LDAP-Kommunikation.
- *startTLS* (Voreinstellung)
  Verschlüsselung mit startTLS-Erweiterung.
  Das Gerät baut eine LDAP-Verbindung zum Server auf und verschlüsselt die Kommunikation.

Voraussetzung für die verschlüsselte Kommunikation ist, dass das Gerät die korrekte Uhrzeit verwendet. Wenn das Zertifikat ausschließlich DNS-Namen enthält, dann legen Sie in Spalte *Adresse* den DNS-Namen des Servers fest. Schalten Sie die Funktion *Client* im Dialog *Erweitert* > DNS > *Client* > *Global* ein.

Wenn das Zertifikat im Feld “Subject Alternative Name” die IP-Adresse des Servers enthält, kann das Gerät ohne DNS-Konfiguration die Identität des Servers verifizieren.

Server-Status

Zeigt den Verbindungsstatus und die Authentifizierung mit dem Authentication-Server.

Mögliche Werte:

- *ok*
  Der Server ist erreichbar.
  Wenn in Spalte *Verbindungssicherheit* ein anderer Wert als *kein* festgelegt ist, dann hat das Gerät das Zertifikat des Servers verifiziert.
- *unreachable*
  Server ist unerreichbar.
- *other*
  Das Gerät hat noch keine Verbindung zum Server aufgebaut.

Aktiv

Aktiviert/deaktiviert die Verwendung des Servers.

Mögliche Werte:

- `markiert`
  Das Gerät verwendet den Server.
- `unmarkiert` (Voreinstellung)
  Das Gerät verwendet den Server nicht.

3.3.2 LDAP Rollen-Zuweisung

[Gerätesicherheit > LDAP > Rollen-Zuweisung]

Dieser Dialog ermöglicht Ihnen, bis zu 64 Mappings zu erstellen, um Benutzern eine Rolle zuzuweisen.

In der Tabelle legen Sie fest, ob das Gerät anhand eines Attributs mit einem bestimmten Wert oder anhand der Gruppenitgliedschaft dem Benutzer eine Rolle zuweist.
- Attribut und Attributwert sucht das Gerät innerhalb des Benutzerobjekts.
- Die Gruppenmitgliedschaft prüft das Gerät durch Auswertung des in den Member-Attributen enthaltenen „Distinguished Name“ (DN).

Wenn ein Benutzer sich anmeldet, sucht das Gerät auf dem LDAP-Server folgende Informationen:
- Im zugehörigen Benutzerobjekt sucht das Gerät die in den Mappings festgelegten Attribute.
- In den Gruppenobjekten der in den Mappings festgelegten Gruppen sucht das Gerät die Member-Attribute.

Darauf basierend prüft das Gerät jedes Mapping:
- Enthält das Benutzerobjekt das erforderliche Attribut?
  oder
- Ist der Benutzer Mitglied der Gruppe?

Wenn das Gerät keine Übereinstimmung findet, dann erhält der Benutzer keinen Zugriff auf das Gerät.

Wenn das Gerät mehr als ein zutreffendes Mapping für einen Benutzer findet, dann entscheidet die Einstellung im Feld *Übereinstimmende Regel*. Entweder erhält der Benutzer die Rolle mit den weitreichenderen Berechtigungen oder die 1. in der Tabelle zutreffende Rolle.

Konfiguration

Übereinstimmende Regel

Legt fest, welche Rolle das Gerät verwendet, wenn mehr als ein Mapping für einen Benutzer zutrifft.

Mögliche Werte:
- `highest` (Voreinstellung)
  Das Gerät verwendet die Rolle mit den weitreichenderen Berechtigungen.
- `erste`
  Das Gerät wendet die Rolle mit dem kleineren Wert in Spalte *Index* auf den Benutzer an.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Index* legen Sie die Index-Nummer fest.
  Mögliche Werte:
  - `1..64`

Löschen

Entfernt den ausgewählten Tabelleneintrag.

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

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, dann 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.

Typ

Legt fest, ob in Spalte *Parameter* eine Gruppe oder ein Attribut mit einem Attributwert festgelegt ist.

Mögliche Werte:

- `attribute` (Voreinstellung)
  Die Spalte *Parameter* enthält ein Attribut mit einem Attributwert.
- `group`
  Die Spalte *Parameter* enthält den „Distinguished Name" (DN) einer Gruppe.

Parameter

Legt abhängig von der Einstellung in Spalte *Typ* eine Gruppe oder ein Attribut mit einem Attributwert fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
  Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
  - Wenn in Spalte *Typ* der Wert `attribute` festgelegt ist, dann legen Sie das Attribut in der Form `Attributname=Attributwert` fest.
    Beispiel: `l=Germany`
  - Wenn in Spalte *Typ* der Wert `group` festgelegt ist, dann legen Sie den „Distinguished Name“ (DN) einer Gruppe fest.
    Beispiel: `CN=admin-users,OU=Groups,DC=example,DC=com`

Aktiv

Aktiviert/deaktiviert das Mapping der Rolle.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Mapping der Rolle ist aktiv.
- `unmarkiert`
  Das Mapping der Rolle ist inaktiv.

3.4 Management-Zugriff

[Gerätesicherheit > Management-Zugriff]

Das Menü enthält die folgenden Dialoge:

- Server
- IP-Zugriffsbeschränkung
- Web
- Command Line Interface
- SNMPv1/v2 Community

3.4.1 Server

[Gerätesicherheit > Management-Zugriff > Server]

Dieser Dialog ermöglicht Ihnen, 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 *HTTPS*.

Mögliche Werte:

- `markiert`
  Server-Dienst ist aktiv.
- `unmarkiert`
  Server-Dienst ist inaktiv.

[SNMP]

Diese Registerkarte ermöglicht Ihnen, 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 Zugriff auf das Management des Geräts mit SNMP-basierten Anwendungen.

Konfiguration

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 💾, um die gegenwärtigen Änderungen zu 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.

[Telnet]

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

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

Funktion

Telnet server

Schaltet den Telnet-Server ein/aus.

Mögliche Werte:

- *`An`* (Voreinstellung)
  Der Telnet-Server ist eingeschaltet.
  Der Zugriff auf das Management des Geräts ist möglich mit dem Command Line Interface über eine unverschlüsselte Telnet-Verbindung.
- *`Aus`*
  Der Telnet-Server ist ausgeschaltet.

Anmerkung: Wenn der *SSH*-Server ausgeschaltet ist und Sie auch den *Telnet*-Server ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die serielle Schnittstelle des Geräts möglich.

Konfiguration

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`)

[SSH]

Diese Registerkarte ermöglicht Ihnen, 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 Zugriff auf das Management des Geräts per Fernzugriff mit dem Command Line Interface. SSH-Verbindungen sind verschlüsselt.

Der SSH-Server identifiziert sich gegenüber den Clients mit seinem öffentlichen RSA-Schlüssel. Beim 1. Verbindungsaufbau zeigt das Client-Programm dem Benutzer den Fingerprint dieses Schlüssels. Der Fingerprint enthält eine einfach zu prüfende, Base64-kodierte Zeichenfolge. Wenn Sie den Benutzern diese Zeichenfolge über einen vertrauenswürdigen Kanal zur Verfügung stellen, haben diese die Möglichkeit, beide Fingerprints zu vergleichen. Wenn die Zeichenfolgen übereinstimmen, dann ist der Client mit dem korrekten Server verbunden.

Das Gerät ermöglicht Ihnen, die für RSA 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 ermöglicht Ihnen das Gerät, den 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

SSH-Server

Schaltet den SSH-Server ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Der SSH-Server ist eingeschaltet.
  Der Zugriff auf das Management des Geräts ist möglich mit dem Command Line Interface über eine verschlüsselte SSH-Verbindung.
  Der Server lässt sich ausschließlich dann starten, wenn eine RSA-Signatur im Gerät vorhanden ist.
- `Aus`
  Der SSH-Server ist ausgeschaltet.
  Wenn Sie den SSH-Server ausschalten, bleiben bestehende Verbindungen aufgebaut. Das Gerät sorgt dafür, den Aufbau neuer Verbindungen zu verhindern.

Anmerkung: Wenn der *Telnet*-Server ausgeschaltet ist und Sie auch den *SSH*-Server ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die serielle Schnittstelle des Geräts möglich.

Konfiguration

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.

Sitzungen (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`)

Fingerabdruck

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

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

Fingerabdruck-Typ

Legt fest, welchen Fingerprint das Feld *RSA-Fingerabdruck* anzeigt.

Mögliche Werte:

- *`md5`*
  Das Feld *RSA-Fingerabdruck* zeigt den Fingerprint als hexadezimalen MD5-Hash.
- *`sha256`*
  Das Feld *RSA-Fingerabdruck* zeigt den Fingerprint als Base64-codierten SHA256-Hash.

RSA-Fingerabdruck

Zeigt den Fingerprint des öffentlichen Host-Keys des SSH-Servers.

Wenn Sie die Einstellung im Feld *Fingerabdruck-Typ* ändern, klicken Sie anschließend die Schaltflächen ✓ und ↻, um die Anzeige zu aktualisieren.

Signatur

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)

Damit der SSH-Server den generierten Host-Key verwendet, starten Sie den SSH-Server neu.

Alternativ haben Sie die Möglichkeit, einen eigenen Host-Key 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.

Betriebszustand

Zeigt, ob das Gerät gegenwärtig einen Host-Key erzeugt.

Möglicherweise hat ein anderer Benutzer diese Aktion ausgelöst.

Mögliche Werte:

- *`rsa`*
  Das Gerät erzeugt gegenwärtig einen RSA-Host-Key.
- *`kein`*
  Das Gerät generiert keinen Host-Key.

Key-Import

URL

Legt Pfad und Dateiname Ihres RSA-Host-Keys fest.

Das Gerät akzeptiert den RSA-Schlüssel, wenn dieser die folgende Schlüssellänge aufweist:

- 2048 bit (RSA)

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 der folgenden 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 der folgenden 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 der folgenden 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 *Password* 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.

[HTTP]

Diese Registerkarte ermöglicht Ihnen, 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, dann beendet das Gerät die Sitzung und trennt jede geöffnete Verbindung. Um wieder mit der grafischen Benutzeroberfläche zu arbeiten, melden Sie sich erneut an.

Funktion

HTTP server

Schaltet für den Webserver das Protokoll *HTTP* ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Das Protokoll *HTTP* ist eingeschaltet.
  Der Zugriff auf das Management des Geräts 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 Zugriff auf das Management des Geräts möglich über eine verschlüsselte *HTTPS*-Verbindung.

Anmerkung: Wenn die Protokolle *HTTP* und *HTTPS* ausgeschaltet sind, können Sie das Protokoll *HTTP* mit dem Kommando `http server` im Command Line Interface einschalten, um die grafische Benutzeroberfläche zu erreichen.

Konfiguration

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.

[HTTPS]

Diese Registerkarte ermöglicht Ihnen, 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 ermöglicht Ihnen, 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, dann beendet das Gerät die Sitzung und trennt jede geöffnete Verbindung. Um wieder mit der grafischen Benutzeroberfläche zu arbeiten, melden Sie sich erneut an.

Funktion

HTTPS server

Schaltet für den Webserver das Protokoll *HTTPS* ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Das Protokoll *HTTPS* ist eingeschaltet.
  Der Zugriff auf das Management des Geräts 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 Zugriff auf das Management des Geräts möglich über eine unverschlüsselte *HTTP*-Verbindung.

Anmerkung: Wenn die Protokolle *HTTP* und *HTTPS* ausgeschaltet sind, können Sie das Protokoll *HTTPS* mit dem Kommando `https server` im Command Line Interface einschalten, um die grafische Benutzeroberfläche zu erreichen.

Konfiguration

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.

Fingerabdruck

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, bis Sie den Server neu starten.

Fingerabdruck-Typ

Legt fest, welchen Fingerprint das Feld *Fingerabdruck* anzeigt.

Mögliche Werte:

- `sha1`
  Das Feld *Fingerabdruck* zeigt den SHA1-Fingerprint des Zertifikats.
- `sha256`
  Das Feld *Fingerabdruck* zeigt den SHA256-Fingerprint des Zertifikats.

Fingerabdruck

Zeichenfolge des digitalen Zertifikats, das der Server verwendet.

Wenn Sie die Einstellung im Feld *Fingerabdruck-Typ* ändern, klicken Sie anschließend die Schaltflächen ✓ und ↻, um die Anzeige zu aktualisieren.

Zertifikat

Anmerkung: Beim Laden der grafischen Benutzeroberfläche zeigt der Web-Browser eine Meldung, 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.

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 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.

Zertifikat-Import

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 der folgenden 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 der folgenden 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 der folgenden 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.

3.4.2 IP-Zugriffsbeschränkung

[Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung]

Dieser Dialog ermöglicht Ihnen, den Zugriff auf das Management des Geräts auf gewisse IP-Adressbereiche und ausgewählte IP-basierte Anwendungen zu beschränken.

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

Funktion

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 das Management des Geräts ist ausschließlich mit dem Command Line Interface über die serielle Schnittstelle möglich.

Funktion

Schaltet die Funktion *IP-Zugriffsbeschränkung* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *IP-Zugriffsbeschränkung* ist eingeschaltet.
  Der Zugriff auf das Management des Geräts ist beschränkt.
- `Aus` (Voreinstellung)
  Die Funktion *IP-Zugriffsbeschränkung* ist ausgeschaltet.

Tabelle

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 Zugriff auf das Management des Geräts 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`)

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.

EtherNet/IP

Aktiviert/deaktiviert den Zugriff auf den *EtherNet/IP*-Server.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Zugriff ist aktiviert für nebenstehenden IP-Adressbereich.
- `unmarkiert`
  Zugriff ist deaktiviert.

PROFINET

Aktiviert/deaktiviert den Zugriff auf den *PROFINET*-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 Zugriff auf das Management des Geräts auf den nebenstehenden IP-Adressbereich und die ausgewählten IP-basierten Anwendungen.
- `unmarkiert`
  Tabelleneintrag ist deaktiviert.

3.4.3 Web

[Gerätesicherheit > Management-Zugriff > Web]

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

Konfiguration

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.

3.4.4 Command Line Interface

[Gerätesicherheit > Management-Zugriff > CLI]

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

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Login-Banner]

[Global]

Diese Registerkarte ermöglicht Ihnen, den Prompt im Command Line Interface zu ändern und das automatische Beenden bei Inaktivität der Sitzung über die serielle Schnittstelle festzulegen.

Das Gerät bietet Ihnen folgende seriellen Schnittstellen:
- V.24-Interface

Konfiguration

Login-Prompt

Legt die Zeichenfolge fest, die das Gerät im Command Line Interface 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: `(MSP)`

Änderungen an dieser Einstellung sind in aktiven Sitzungen im Command Line Interface sofort wirksam.

Timeout serielle Schnittstelle [min]

Legt die Zeit in Minuten fest, nach der das Gerät die Sitzung eines inaktiven Benutzers automatisch beendet, der mit dem Command Line Interface über die serielle Schnittstelle angemeldet ist.

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 den *Telnet*-Server und den *SSH*-Server legen Sie das Timeout fest im Dialog *Gerätesicherheit* > Management-Zugriff > *Server*.

[Login-Banner]

In dieser Registerkarte ersetzen Sie den Startbildschirm im Command Line Interface durch einen individuellen Text.

In der Voreinstellung zeigt der 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 Command Line Interface und in der grafischen Benutzeroberfläche anzuzeigen, verwenden Sie den Dialog *Gerätesicherheit > Pre-Login-Banner*.

Funktion

Funktion

Schaltet die Funktion *Login-Banner* ein/aus.

Mögliche Werte:

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

Banner-Text

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`

3.4.5 SNMPv1/v2 Community

[Gerätesicherheit > Management-Zugriff > 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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)

3.5 Pre-Login-Banner

[Gerätesicherheit > Pre-Login-Banner]

Dieser Dialog ermöglicht Ihnen, Benutzern einen Begrüßungs- oder Hinweistext anzuzeigen, bevor diese sich anmelden.

Die Benutzer sehen den Text im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface. 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 anzuzeigen, verwenden Sie die Einstellungen im Dialog *Gerätesicherheit > Management-Zugriff > CLI*.

Funktion

Funktion

Schaltet die Funktion *Pre-Login-Banner* ein/aus.

Mit der Funktion *Pre-Login-Banner* zeigt das Gerät im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface eine Begrüßung oder einen Hinweis.

Mögliche Werte:

- `An`
  Die Funktion *Pre-Login-Banner* ist eingeschaltet.
  Das Gerät zeigt im Login-Dialog den im Feld *Banner-Text* festgelegten Text.
- `Aus` (Voreinstellung)
  Die Funktion *Pre-Login-Banner* ist ausgeschaltet.
  Das Gerät zeigt im Login-Dialog keinen Text. Haben Sie im Feld *Banner-Text* einen Text eingegeben, bleibt dieser erhalten.

Banner-Text

Banner-Text

Legt den Hinweistext fest, den das Gerät im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface 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`

4 Netzsicherheit

Das Menü enthält die folgenden Dialoge:

- Netzsicherheit Übersicht
- Port-Sicherheit
- 802.1X Port-Authentifizierung
- RADIUS
- DoS
- DHCP-Snooping
- IP Source Guard
- Dynamic ARP Inspection
- ACL

4.1 Netzsicherheit Übersicht

[Netzsicherheit > Übersicht]

Dieser Dialog zeigt eine Übersicht über die im Gerät verwendeten Netzsicherheits-Regeln.

Übersicht

Die oberste Ebene zeigt:

- Die Ports, denen eine Netzsicherheits-Regel zugewiesen ist.
- Die VLANs, denen eine Netzsicherheits-Regel zugewiesen ist.

Die untergeordneten Ebenen zeigen:

- Die festgelegten *ACL*-Regeln. Siehe Dialog *Netzsicherheit > ACL*.

Schaltflächen

Zeigt ein Textfeld, um nach einem Schlüsselwort zu suchen. Wenn Sie ein Zeichen oder eine Zeichenkette einfügen, zeigt die Übersicht ausschließlich Einträge, die mit diesem Schlüsselwort in Zusammenhang stehen.

Klappt die Ebenen zu. Die Übersicht zeigt dann ausschließlich die erste Ebene der Einträge.

Klappt die Ebenen auf. Die Übersicht zeigt dann jede Ebene der Einträge.

+

Klappt den aktuellen Eintrag auf und zeigt die Einträge der nächsttieferen Ebene.

−

Klappt den Eintrag zu und blendet die Einträge der darunter liegenden Ebenen aus.

4.2 Port-Sicherheit

[Netzsicherheit > Port-Sicherheit]

Das Gerät ermöglicht Ihnen, ausschließlich Datenpakete von erwünschten Absendern auf einem Port zu vermitteln. Wenn die Funktion *Port-Sicherheit* eingeschaltet ist, prüft das Gerät die VLAN-ID und die MAC-Adresse des Absenders, bevor es ein Datenpaket vermittelt. Die Datenpakete unerwünschter Absender verwirft das Gerät und protokolliert dieses Ereignis.

In diesem Dialog unterstützt Sie ein Fenster *Wizard*, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Im Gerät heißen diese Adressen *statische Einträge*. Zum Ansehen der festgelegten statischen Adressen wählen Sie den betreffenden Port und klicken die Schaltfläche .

Um die Einrichtung zu vereinfachen, ermöglicht Ihnen das Gerät, die Adresse der erwünschten Absender automatisch zu erfassen. Das Gerät „lernt“ die Adressen durch das Bewerten der empfangenen Datenpakete. Im Gerät heißen diese Adressen *dynamische Einträge*. Wenn die benutzerdefinierte Obergrenze erreicht ist (*Dynamisches Limit*), beendet das Gerät das "Lernen" auf dem betreffenden Port. Das Gerät leitet lediglich Datenpakete weiter, deren Absender bereits auf dem Port erfasst sind. Wenn Sie die Obergrenze an die Anzahl der zu erwartenden Absender anpassen, erschweren Sie damit *MAC-Flooding*-Attacken.

Anmerkung: Beim automatischen Erfassen der *dynamischeb Einträge* verwirft das Gerät stets das erste Datenpaket von unbekannten Absendern. Anhand dieses ersten Datenpakets prüft das Gerät, ob die Obergrenze erreicht ist. Bis zum Erreichen der Obergrenze erfasst das Gerät die Adressen. Anschließend vermittelt das Gerät Datenpakete, die es auf dem betreffenden Port von diesem Absender empfängt.

Funktion

Funktion

Schaltet die Funktion *Port-Sicherheit* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *Port-Sicherheit* ist eingeschaltet.
  Das Gerät prüft die VLAN-ID und die Absender-MAC-Adresse, bevor es ein Datenpaket vermittelt.
  Das Gerät vermittelt ein empfangenes Datenpaket ausschließlich dann, wenn die VLAN-ID und die Absender-MAC-Adresse des Datenpakets auf dem betreffenden Port erwünscht sind. Damit diese Einstellung wirksam wird, aktivieren Sie zusätzlich die Funktion *Port-Sicherheit* auf den betreffenden Ports.
- `Aus` (Voreinstellung)
  Die Funktion *Port-Sicherheit* ist ausgeschaltet.
  Das Gerät vermittelt jedes empfangene Datenpaket, ohne die Absenderadresse zu prüfen.

Konfiguration

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Port-Sicherheit* im Gerät.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für *Port-Sicherheit* ist aktiv.
  Markieren Sie zusätzlich das Kontrollkästchen in Spalte *Auto-Disable* für die gewünschten Ports.
  Das Gerät schaltet den Port aus und sendet optional einen SNMP-Trap, wenn eines der folgenden Ereignisse eintritt:
  - Das Gerät erfasst mindestens eine Adresse eines Absenders, der auf dem Port nicht erwünscht ist.
  - Das Gerät erfasst mehr Adressen als in Spalte *Dynamisches Limit* festgelegt.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für *Port-Sicherheit* ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 18.

Schaltflächen

Wizard

Öffnet das Fenster *Wizard*, das Sie dabei unterstützt, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen. Siehe „[Wizard: Port-Sicherheit]” auf Seite 150.

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *Port-Sicherheit* auf dem Port.

Mögliche Werte:

- `markiert`
  Das Gerät prüft jedes auf dem Port empfangene Datenpaket und vermittelt es ausschließlich dann, wenn die Absenderadresse des Datenpakets erwünscht ist. Schalten Sie zusätzlich im Rahmen *Funktion* die Funktion *Port-Sicherheit* ein.
- `unmarkiert` (Voreinstellung)
  Das Gerät vermittelt jedes auf dem Port empfangene Datenpaket, ohne die Absenderadresse zu prüfen.

Anmerkung: Wenn Sie das Gerät als aktiven Teilnehmer innerhalb eines *MRP*-Rings oder *HIPER-Ring*s betreiben, empfehlen wir, die Markierung des Kontrollkästchens für die Ring-Ports aufzuheben.

Anmerkung: Wenn Sie das Gerät als aktiven Teilnehmer einer *Ring-/Netzkopplung* oder *RCP* betreiben, empfehlen wir, die Markierung des Kontrollkästchens für die jeweiligen Kopplungs-Ports aufzuheben.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Port-Sicherheit* auf dem Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *Auto-Disable* ist auf dem Port aktiv.
  Das Gerät schaltet den Port aus und sendet optional einen SNMP-Trap, wenn eines der folgenden Ereignisse eintritt:
  - Das Gerät erfasst mindestens eine Adresse eines Absenders, der auf dem Port nicht erwünscht ist.
  - Das Gerät erfasst mehr Adressen als in Spalte *Dynamisches Limit* festgelegt.

  Die *Link status*-LED des Ports blinkt 3× pro Periode. Diese Begrenzung erschwert *MAC-Spoofing*-Attacken.
  Voraussetzung ist, dass im Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* markiert ist.
  - Der Dialog *Diagnose > Ports > Auto-Disable* zeigt, welche Ports aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet sind.
  - Nach einer Wartezeit schaltet die Funktion *Auto-Disable* 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 Funktion *Auto-Disable* ist auf dem Port inaktiv.

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät ein Datenpaket von einem unerwünschten Absender auf dem Port verwirft.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  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 inaktiv.

Voraussetzung für das Senden von SNMP-Traps ist, dass Sie die Funktion im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* einschalten und mindestens ein Trap-Ziel festlegen.

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 Adressen (*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 Adressen erfasst als hier festgelegt ist, dann 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`
  Keine automatische Erfassung von Adressen auf diesem Port.
- `1..600` (Voreinstellung: `600`)

Statisches Limit

Legt die Obergrenze fest für die Anzahl der Adressen, die mittels des Fensters *Wizard* mit dem Port verknüpft sind (*statische Einträge*).

Mögliche Werte:

- `0`
  Keine Verknüpfung zwischen dem Port und einem erwünschten Absender möglich. Legen Sie diesen Wert ausschließlich dann fest, wenn Sie in Spalte *Dynamisches Limit* einen Wert > 0 festlegen.
- `1..64` (Voreinstellung: `64`)

Dynamische Einträge

Zeigt, wie viele Adressen das Gerät automatisch erfasst hat.

Statische MAC Einträge

Zeigt die Anzahl der MAC-Adressen, die mit dem Port verknüpft sind.

Last violating VLAN ID/MAC

Zeigt VLAN-ID und MAC-Adresse eines unerwünschten Absenders, dessen Datenpakete das Gerät auf 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.

[Wizard: Port-Sicherheit]

Das Fenster *Wizard* unterstützt Sie dabei, die Ports mit der Adresse eines oder mehrerer erwünschter Absender zu verknüpfen.

Das Fenster *Wizard* führt Sie durch die folgenden Schritte:

- Port auswählen
- MAC-Adressen

Anmerkung: Das Gerät speichert die mit dem Port verknüpften Adressen so lange, bis Sie die Funktion *Port-Sicherheit* auf dem betreffenden Port deaktivieren oder die Funktion *Port-Sicherheit* im Gerät ausschalten.

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

Port auswählen

Port

Legt den Port fest, den Sie im nächsten Schritt mit der Adresse erwünschter Absender verknüpfen.

MAC-Adressen

Statische Einträge (x/y)

Zeigt, wie viele Adressen mit dem Port mittels des Fensters *Wizard* verknüpft sind sowie die Obergrenze für *statische Einträge*. Der untere Teil des Fensters *Wizard* zeigt die Einträge im Detail, sofern vorhanden.

🗑

Entfernt die Einträge im unteren Teil des Fensters *Wizard*. Das Gerät hebt die jeweilige Zuordnung zwischen einem Port und den erwünschten Absendern auf.

VLAN-ID

Legt die VLAN-ID des erwünschten Absenders fest.

Mögliche Werte:

- `1..4042`

MAC-Adresse

Legt die MAC-Adresse des erwünschten Absenders fest.

Mögliche Werte:

- Gültige Unicast-MAC-Adresse
  Legen Sie den Wert mit Doppelpunkt-Trennzeichen fest, zum Beispiel `00:11:22:33:44:55`.

Anmerkung: Eine MAC-Adresse können Sie lediglich einem Port zuweisen.

Hinzufügen

Erzeugt einen *statischen Eintrag* basierend auf den in den Feldern *VLAN-ID* und *MAC-Adresse* festgelegten Werten. Folglich finden Sie im unteren Teil des Fensters *Wizard* einen neuen Eintrag.

Einträge im unteren Teil des Fensters

Der untere Teil des Fensters *Wizard* zeigt VLAN-ID und MAC-Adresse der an diesem Port gewünschten Absender. Im Folgenden finden Sie eine Beschreibung der Symbole, die spezifisch für diese Einträge sind.

Statischer Eintrag: Wenn Sie das Symbol klicken, entfernt das Gerät den *statischen Eintrag* und die jeweilige Zuordnung zwischen dem Port und den gewünschten Absendern.

Dynamischer Eintrag: Wenn Sie das Symbol klicken, ändert sich das Symbol zu . Das Gerät wandelt den *dynamischen Eintrag* in einen *statischen Eintrag* um, wenn Sie das *Wizard* Fenster schließen. Um diese Änderung rückgängig zu machen, klicken Sie das Symbol noch einmal, bevor Sie das Fenster *Wizard* schließen.

4.3 802.1X Port-Authentifizierung

[Netzsicherheit > 802.1X Port-Authentifizierung]

Mit der Port-basierten Zugriffskontrolle gemäß IEEE 802.1X kontrolliert das Gerät den Zugriff angeschlossener Endgeräte auf das Netz. Das Gerät (Authenticator) ermöglicht einem Endgerät (Supplicant) den 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

[Netzsicherheit > 802.1X Port-Authentifizierung > Global]

Dieser Dialog ermöglicht Ihnen, grundlegende Einstellungen für die Port-basierte Zugriffskontrolle festzulegen.

Funktion

Funktion

Schaltet die Funktion *802.1X Port-Authentifizierung* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *802.1X Port-Authentifizierung* ist eingeschaltet.
  Das Gerät prüft den Zugriff angeschlossener Endgeräte auf das Netz.
  Die Port-basierte Zugriffskontrolle ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *802.1X Port-Authentifizierung* ist ausgeschaltet.
  Die Port-basierte Zugriffskontrolle ist ausgeschaltet.

Konfiguration

VLAN zuweisen

Aktiviert/deaktiviert die Zuweisung des betreffenden Ports zu einem VLAN. Diese Funktion ermöglicht Ihnen, 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.

Formatoptionen MAC Authentication Bypass

Gruppen-Größe

Legt die Größe der MAC-Adress-Gruppen fest. Für die Authentifizierung unterteilt das Gerät die MAC-Adresse in Gruppen. Die Größe der Gruppen ist festgelegt in Halb-Bytes, die jeweils als ein Zeichen dargestellt werden.

Mögliche Werte:

- *1*
  Das Gerät unterteilt die MAC-Adresse in 12 Gruppen mit je einem Zeichen.
  Beispiel: `A:A:B:B:C:C:D:D:E:E:F:F`
- *2*
  Das Gerät unterteilt die MAC-Adresse in 6 Gruppen mit je 2 Zeichen.
  Beispiel: `AA:BB:CC:DD:EE:FF`
- *4*
  Das Gerät unterteilt die MAC-Adresse in 3 Gruppen mit je 4 Zeichen.
  Beispiel: `AABB:CCDD:EEFF`
- *12* (Voreinstellung)
  Das Gerät formatiert die MAC-Adresse als eine Gruppe mit 12 Zeichen.
  Beispiel: `AABBCCDDEEFF`

Gruppen-Trennzeichen

Legt das Trennzeichen zwischen den Gruppen fest.

Mögliche Werte:

- *-*
  Bindestrich
- *:*
  Doppelpunkt
- *.*
  Punkt

Groß-/Kleinschreibung

Legt fest, ob das Gerät die Authentifizierungsdaten in Klein- oder Großbuchstaben formatiert.

Mögliche Werte:

- *lower-case*
- *upper-case*

Passwort

Legt für Clients, die den Authentifizierungs-Bypass verwenden, das optionale Passwort fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen
  Nach Eingabe zeigt das Feld ***** (Sternchen) anstelle des Passworts.
- `<leer>`
  Das Gerät verwendet den Benutzernamen des Clients zugleich als Passwort.

Information

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.

4.3.2 802.1X Port-Konfiguration

[Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Zugriffseinstellungen für jeden Port festzulegen.

Sind mehrere Endgeräte an einem Port angeschlossen, ermöglicht Ihnen das Gerät, diese individuell zu authentifizieren (Multi-Client-Authentifizierung). In diesem Fall ermöglicht das Gerät angemeldeten Endgeräten den Zugriff auf das Netz. Dagegen sperrt das Gerät den Zugriff für unauthentifizierte Endgeräte oder für Endgeräte, deren Authentifizierung abgelaufen ist.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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` oder `multiClient` 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` oder `multiClient` festgelegt ist.

Das Gerät ermöglicht Ihnen außerdem, 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*

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.

Benutzer (max.)

Legt die Obergrenze fest für die Anzahl von Endgeräten, die das Gerät auf diesem Port gleichzeitig authentifiziert. Diese Obergrenze gilt ausschließlich dann, wenn für den Port in Spalte *Port-Kontrolle* der Wert `multiClient` festgelegt ist.

Mögliche Werte:

- `1..16` (Voreinstellung: `16`)

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 an den 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 an den Port ein Endgerät angeschlossen ist, das sich beim Authenticator anmeldet.

Anmerkung: Wenn über denselben Port weitere Endgeräte angeschlossen sind, erhalten diese ohne zusätzliche Authentifizierung Zugriff auf das Netz.

- *`forceAuthorized`* (Voreinstellung)
  Wenn Endgeräte kein IEEE 802.1X unterstützen, gewährt das Gerät Zugriff auf das Netz. Verwenden Sie diese Einstellung, wenn an den Port ein Endgerät angeschlossen ist, das ohne Anmeldung Zugriff auf das Netz erhält.
- *`multiClient`*
  Das Gerät gewährt den Zugriff auf das Netz, wenn sich das Endgerät erfolgreich anmeldet. Wenn das Endgerät keine EAPOL-Datenpakete sendet, gewährt oder sperrt das Gerät den Zugriff auf das Netz individuell anhand der MAC-Adresse des Endgeräts. Siehe Spalte *MAC-Authorized-Bypass*.
  Verwenden Sie diese Einstellung, wenn mehrere Endgeräte an den Port angeschlossen sind oder wenn die Funktion *MAC-Authorized-Bypass* erforderlich ist.

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, weist das Gerät das VLAN-Tag anhand der MAC-Adresse des Endgeräts zu, wenn es Datenpakete ohne VLAN-Tag empfängt.

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 für einen Supplikanten 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` oder `multiClient` festgelegt ist.

Diese Funktion ermöglicht Ihnen, Endgeräten ohne Unterstützung für IEEE 802.1X den Zugriff auf ausgewählte Dienste im Netz zu gewähren.

Mögliche Werte:

- `0` (Voreinstellung)
  Der Authenticator weist dem Port kein Gast-VLAN zu.
  Wenn Sie in Spalte *MAC-Authorized-Bypass* die MAC-basierte Authentifizierung einschalten, legt das Gerät automatisch den Wert `0` fest.
- `1..4042`

Anmerkung: Die Funktion *MAC-Authorized-Bypass* und die Funktion *Gast VLAN-ID* können nicht gleichzeitig verwendet werden.

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 ermöglicht Ihnen, Endgeräten ohne gültige Zugangsdaten den 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.

MAC-Authorized-Bypass

Aktiviert/deaktiviert die MAC-basierte Authentifizierung.

Diese Funktion ermöglicht Ihnen, Endgeräte ohne Unterstützung für IEEE 802.1X anhand ihrer MAC-Adresse zu authentifizieren.

Mögliche Werte:

- `markiert`
  Die MAC-basierte Authentifizierung ist aktiv.
  Das Gerät sendet die MAC-Adresse des Endgeräts an den RADIUS-Authentication-Server. Das Gerät weist den Port dem jeweiligen VLAN zu, als hätte die Authentifizierung direkt über IEEE 802.1X stattgefunden.
- `unmarkiert` (Voreinstellung)
  Die MAC-basierte Authentifizierung ist inaktiv.

4.3.3 802.1X Port-Clients

[Netzsicherheit > 802.1X Port-Authentifizierung > Port-Clients]

Dieser Dialog zeigt Informationen über die angeschlossenen Endgeräte.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

Filter-ID

Zeigt den Namen der Filterliste, die der RADIUS-Authentication-Server dem Endgerät nach erfolgreicher Authentifizierung zugewiesen hat.

Der Authentication-Server übermittelt die Filter-ID-Attribute im Access-Accept-Datenpaket.

Zugewiesene VLAN-ID

Zeigt die VLAN-ID, die der Authenticator dem Port nach erfolgreicher Authentifizierung des Endgeräts zugewiesen hat.

Wenn für den Port im Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration*, Spalte *Port-Kontrolle* der Wert `multiClient` festgelegt ist, dann weist das Gerät das VLAN-Tag anhand der MAC-Adresse des Endgeräts zu, wenn es Datenpakete ohne VLAN-Tag empfängt.

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` oder `multiClient` 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.

Aktion beim Beenden

Zeigt die Aktion, die das Gerät bei Ablauf der Anmeldung ausführt.

Mögliche Werte:

- `default`
- `reauthenticate`

4.3.4 802.1X EAPOL-Portstatistiken

[Netzsicherheit > 802.1X Port-Authentifizierung > Statistiken]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

4.3.5 802.1X Port-Authentifizierung-Historie

[Netzsicherheit > 802.1X Port-Authentifizierung > 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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

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.

4.3.6 802.1X Integrierter Authentifikations-Server

[Netzsicherheit > 802.1X Port-Authentifizierung > Integrierter Authentifikations-Server]

Der Integrierte Authentifikationsserver (IAS) ermöglicht Ihnen, 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 ermöglicht Ihnen, bis zu 100 Zugangsdaten einzurichten.

Um die Endgeräte über den Integrierten Authentifikationsserver zu authentifizieren, weisen Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* der Liste 8021x die Richtlinie `ias` zu.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 IEEE 802.1X anzumelden.
- `unmarkiert` (Voreinstellung)
  Die Zugangsdaten sind inaktiv.

4.4 RADIUS

[Netzsicherheit > 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) ermöglicht Ihnen, die Benutzer an zentraler 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 ermöglicht Ihnen außerdem, 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

[Netzsicherheit > RADIUS > Global]

Dieser Dialog ermöglicht Ihnen, grundlegende Einstellungen für RADIUS festzulegen.

RADIUS-Konfiguration

Schaltflächen

Zurücksetzen

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

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.

Anmerkung: Das Gerät sendet das Attribut 4 ausschließlich dann mit, wenn das Paket durch die *802.1X*-Authentifizierungsanfrage eines Endgeräts (Supplicant) ausgelöst wurde.

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.

4.4.2 RADIUS Authentication-Server

[Netzsicherheit > RADIUS > Authentication-Server]

Dieser Dialog ermöglicht Ihnen, 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

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.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

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`)
  Sie können für mehrere Server den gleichen Namen festlegen. Wenn mehrere Server den gleichen Namen haben, gilt die Einstellung in Spalte *Primärer 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.

Primärer 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.
  Diese Einstellung gilt ausschließlich dann, wenn mehr als ein Server in der Tabelle den gleichen Wert in Spalte *Name* hat.
- `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.

4.4.3 RADIUS Accounting-Server

[Netzsicherheit > RADIUS > Accounting-Server]

Dieser Dialog ermöglicht Ihnen, 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. Wenn der Accounting-Server nicht antwortet, kontaktiert das Gerät den jeweils nächsten Server aus der Tabelle.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

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.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

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.

4.4.4 RADIUS Authentication Statistiken

[Netzsicherheit > 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 🗑 .

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

4.4.5 RADIUS Accounting-Statistiken

[Netzsicherheit > 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 🗑 .

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

4.5 DoS

[Netzsicherheit > 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 selbst und andere Geräte im Netz vor DoS-Angriffen zu schützen.

Das Menü enthält die folgenden Dialoge:

▶ DoS Global

4.5.1 DoS Global

[Netzsicherheit > 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 ermöglicht Ihnen, 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

Null-Scan-Filter

Aktiviert/deaktiviert den Null-Scan-Filter.

Das Gerät erkennt und verwirft eingehende TCP-Datenpakete mit den folgenden Eigenschaften:
- Keine TCP-Flags sind gesetzt.
- Die TCP-Sequenznummer ist 0.

Mögliche Werte:
- `markiert`
  Der Filter ist aktiv.
- `unmarkiert` (Voreinstellung)
  Der Filter ist inaktiv.

Xmas-Filter

Aktiviert/deaktiviert den Xmas-Filter.

Das Gerät erkennt und verwirft eingehende TCP-Datenpakete mit den folgenden Eigenschaften:
- Die TCP-Flags *FIN*, *URG* und *PSH* sind gleichzeitig gesetzt.
- Die TCP-Sequenznummer ist 0.

Mögliche Werte:
- `markiert`
  Der Filter ist aktiv.
- `unmarkiert` (Voreinstellung)
  Der Filter ist inaktiv.

SYN/FIN-Filter

Aktiviert/deaktiviert den SYN/FIN-Filter.

Das Gerät 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.

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 erkennt eingehende Datenpakete, bei denen die IP-Payload-Länge im IP-Header abzüglich der äußeren IP-Header-Größe kleiner ist als die minimale TCP-Header-Größe. Fallls es sich dabei um das erste erkannte Fragment handelt, verwirft das Gerät das Datenpaket.

Mögliche Werte:

- `markiert`
  Der Filter ist aktiv.
- `unmarkiert` (Voreinstellung)
  Der Filter ist inaktiv.

Min. Größe TCP-Header

Zeigt die minimale Größe eines gültigen TCP-Headers.

IP

Land-Attack-Filter

Aktiviert/deaktiviert den *Land Attack*-Filter. Bei der *Land Attack*-Methode sendet die angreifende Station Datenpakete, deren Quell- und Zieladressen identisch mit der IP-Adresse des Empfängers sind.

Mögliche Werte:

- `markiert`
  Der Filter ist aktiv. Das Gerät verwirft Datenpakete, deren Quell- und Zieladressen identisch sind.
- `unmarkiert` (Voreinstellung)
  Der Filter ist inaktiv.

ICMP

Dieser Dialog bietet Ihnen Filtermöglichkeiten für folgende ICMP-Parameter:

- Fragmentierte Datenpakete
- ICMP-Pakete ab einer bestimmten Größe
- Broadcast-Pings

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 Paket-Größe verwerfen

Aktiviert/deaktiviert den Filter für eingehende ICMP-Pakete.

Der Filter erkennt ICMP-Pakete, deren Payload-Größe die im Feld *Erlaubte Payload-Größe [Byte]* festgelegte Größe überschreitet und verwirft diese.

Mögliche Werte:

- `markiert`
  Der Filter ist aktiv.
- `unmarkiert` (Voreinstellung)
  Der Filter ist inaktiv.

Erlaubte Payload-Größe [Byte]

Legt die maximal erlaubte Payload-Größe von ICMP-Paketen in Byte fest.

Markieren Sie das Kontrollkästchen *Anhand Paket-Größe verwerfen*, wenn Sie eingehende Datenpakete verwerfen möchten, deren Payload-Größe die maximal erlaubte Größe von ICMP-Paketen überschreitet.

Mögliche Werte:

- `0..1472` (Voreinstellung: `512`)

Broadcast-Ping verwerfen

Aktiviert/deaktiviert den Filter für Broadcast-Pings. Broadcast Pings sind ein bekanntes Indiz für Smurf-Angriffe.

Mögliche Werte:

- `markiert`
  Der Filter ist aktiv.
  Das Gerät erkennt Broadcast-Pings und verwirft diese.
- `unmarkiert` (Voreinstellung)
  Der Filter ist inaktiv.

4.6 DHCP-Snooping

[Netzsicherheit > DHCP-Snooping]

DHCP Snooping ist eine Funktion zur Unterstützung der Netzsicherheit. DHCP Snooping überwacht DHCP-Pakete zwischen DHCP-Client und DHCP-Server und verhält sich zwischen den ungesicherten Hosts und den gesicherten DHCP-Servern wie eine Firewall.

In diesem Dialog konfigurieren und überwachen Sie die folgenden Geräteeigenschaften:

- DHCP-Pakete aus nicht vertrauenswürdigen Quellen validieren und ungültige Pakete herausfiltern.
- DHCP-Datenverkehr aus vertrauenswürdigen und nicht vertrauenswürdigen Quellen limitieren.
- Die DHCP-Snooping Binding-Datenbasis aufbauen und aktualisieren. Diese Datenbasis enthält MAC-Adresse, IP-Adresse, VLAN und Port von DHCP-Clients an nicht vertrauenswürdigen Ports.
- Folgeanfragen von nicht vertrauenswürdigen Hosts auf Basis der DHCP-Snooping Binding-Datenbasis validieren.

Sie können DHCP-Snooping global und für ein bestimmtes VLAN einschalten. Den Sicherheitsstatus (vertrauenswürdig oder nicht vertrauenswürdig) können Sie an einzelnen Ports festlegen. Vergewissern Sie sich, dass der DHCP-Server über vertrauenswürdige Ports erreichbar ist. Für DHCP-Snooping konfigurieren Sie typischerweise die Benutzer-/Client-Ports als nicht vertrauenswürdig und die Uplink-Ports als vertrauenswürdig.

Das Menü enthält die folgenden Dialoge:

- DHCP-Snooping Global
- DHCP-Snooping Konfiguration
- DHCP-Snooping Statistiken
- DHCP-Snooping Bindings

4.6.1 DHCP-Snooping Global

[Netzsicherheit > DHCP-Snooping > Global]

Dieser Dialog ermöglicht Ihnen, die globalen DHCP-Snooping-Parameter Ihres Geräts zu konfigurieren:

- *DHCP-Snooping* global ein-/ausschalten.
- *Auto-Disable* global ein-/ausschalten.
- Das Prüfen der MAC-Quelladresse ein-/ausschalten.
- Name, Ablageort und Speicherintervall für die Binding-Datenbasis konfigurieren.

Funktion

Funktion

Bei eingeschalteter Funktion ist DHCP-Snooping global eingeschaltet.

Mögliche Werte:

- `An`
- `Aus` (Voreinstellung)

Konfiguration

MAC verifizieren

Aktiviert/deaktiviert die Verifizierung der Quell-MAC-Adresse im Ethernet-Paket.

Mögliche Werte:

- `markiert`
  Die Verifizierung der Quell-MAC-Adresse ist aktiv.
  Das Gerät vergleicht die Quell-MAC-Adresse mit der MAC-Adresse des Clients im empfangenen DHCP-Paket.
- `unmarkiert` (Voreinstellung)
  Die Verifizierung der Quell-MAC-Adresse ist inaktiv.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *DHCP-Snooping*.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für *DHCP-Snooping* ist aktiv.
  Markieren Sie zusätzlich im Dialog *Netzsicherheit > DHCP-Snooping > Konfiguration*, Registerkarte *Auto-Disable* das Kontrollkästchen in Spalte *Port* für die gewünschten Ports.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für *DHCP-Snooping* ist inaktiv.

Binding-Datenbank

Remote Datei-Name

Legt den Namen der Datei fest, in der das Gerät die DHCP-Snooping Binding-Datenbasis speichert.

Anmerkung: Das Gerät speichert ausschließlich dynamische Bindungen in der persistenten Binding-Datenbasis. Statische Bindungen speichert das Gerät im Konfigurationsprofil.

Remote IP-Adresse

Legt die Remote-IP-Adresse fest, unter der das Gerät die persistente DHCP-Snooping-Binding-Datenbasis speichert. Mit dem Wert `0.0.0.0` speichert das Gerät die Binding-Datenbasis lokal.

Mögliche Werte:

- Gültige IPv4-Adresse
- `0.0.0.0` (Voreinstellung)
  Das Gerät speichert die DHCP-Snooping Binding-Datenbasis lokal.

Speicher-Intervall [s]

Legt die Zeitverzögerung in Sekunden fest, nach der das Gerät die DHCP-Snooping-Binding-Datenbasis speichert, wenn es eine Veränderung in der Datenbasis ermittelt hat.

Mögliche Werte:

- `15..86400` (Voreinstellung: `300`)

4.6.2 DHCP-Snooping Konfiguration

[Netzsicherheit > DHCP-Snooping > Konfiguration]

Dieser Dialog ermöglicht Ihnen, DHCP-Snooping für einzelne Ports und für einzelne VLANs zu konfigurieren.

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

[Port]

In dieser Registerkarte konfigurieren Sie die Funktion *DHCP-Snooping* für einzelne Ports.
- Einen Port als vertrauenswürdig / nicht vertrauenswürdig konfigurieren.
- Die Protokollierung ungültiger Pakete für einzelne Ports ein-/ausschalten.
- Die Anzahl von DHCP-Paketen begrenzen.
- Einen Port automatisch abschalten, falls der DHCP-Datenverkehr das festgelegte Limit überschreitet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Vertraue

Legt den Sicherheitsstatus (trusted, untrusted) des Ports fest.

Bei eingeschalteter Funktion ist der Port als vertrauenswürdig konfiguriert. Typischerweise haben Sie den vertrauenswürdigen Port an einen DHCP-Server angeschlossen.

Bei ausgeschalteter Funktion ist der Port als nicht vertrauenswürdig konfiguriert.

Mögliche Werte:
- `markiert`
  Der Port ist als vertrauenswürdig (trusted) konfiguriert. Über vertrauenswürdige Ports leitet DHCP-Snooping zulässige Client-Pakete weiter.
- `unmarkiert` (Voreinstellung)
  Der Port ist als nicht vertrauenswürdig (untrusted) konfiguriert. An nicht vertrauenswürdigen Ports vergleicht das Gerät in der Binding-Databasis den Empfänger-Port mit dem Client-Port.

Protokolliere

Aktiviert/deaktiviert die Protokollierung von ungültigen Paketen, die das Gerät auf diesem Port ermittelt.

Mögliche Werte:

- `markiert`
  Die Protokollierung ungültiger Pakete ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ungültiger Pakete ist inaktiv.

Lastbegrenzung

Legt die maximale Anzahl von DHCP-Paketen pro Burst-Intervall für diesen Port fest. Wenn die Anzahl der eingehenden DHCP-Pakete das festgelegte Limit in einem Burst-Intervall gegenwärtig überschreitet, dann verwirft das Gerät weitere eingehende DHCP-Pakete.

Mögliche Werte:

- `-1` (Voreinstellung)
  Hebt die Limitierung der Anzahl von DHCP-Paketen pro Burst-Intervall auf diesem Port auf.
- `0..150` Pakete pro Intervall
  Begrenzt die maximale Anzahl von DHCP-Paketen pro Burst-Intervall auf diesem Port.

Das Burst-Intervall legen Sie in Spalte *Burst-Intervall* fest.

Wenn Sie die Auto-Disable-Funktion aktiviert haben, schaltet das Gerät zusätzlich den Port aus. Die Auto-Disable-Funktion finden Sie in Spalte *Auto-Disable*.

Burst-Intervall

Legt die Länge des Burst-Intervalls in Sekunden auf diesem Port fest. Das Burst-Intervall ist für die Rate-Limiting-Funktion relevant.

Die maximale Anzahl von DHCP-Paketen pro Burst-Intervall legen Sie in Spalte *Lastbegrenzung* fest.

Mögliche Werte:

- `1..15` (Voreinstellung: `1`)

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für die Parameter, deren Einhaltung die Funktion *DHCP-Snooping* auf dem Port überwacht.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *Auto-Disable* ist auf dem Port aktiv.
  Voraussetzung ist, dass im Dialog *Netzsicherheit > DHCP-Snooping > Global*, Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* markiert ist.
  - Das Gerät schaltet den Port aus, wenn der Port während der in Spalte *Burst-Intervall* festgelegten Zeit mehr DHCP-Pakete empfängt als im Feld *Lastbegrenzung* 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.
  - Nach einer Wartezeit schaltet die Funktion *Auto-Disable* 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 Funktion *Auto-Disable* auf dem Port ist inaktiv.

[VLAN-ID]

In dieser Registerkarte konfigurieren Sie die Funktion *DHCP-Snooping* für einzelne VLANs.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

VLAN-ID

Zeigt die VLAN-ID, auf die sich der Tabelleneintrag bezieht.

Aktiv

Aktiviert/deaktiviert die Funktion *DHCP-Snooping* in diesem VLAN.

Die Funktion *DHCP-Snooping* leitet gültige DHCP-Client-Nachrichten weiter an den vertrauenswürdigen Ports in VLANs ohne Funktion *Routing*.

Mögliche Werte:

- `markiert`
  Die Funktion *DHCP-Snooping* ist in diesem VLAN aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *DHCP-Snooping* ist in diesem VLAN inaktiv.
  Das Gerät leitet DHCP-Pakete entsprechend der Switching-Einstellungen weiter, ohne die Pakete zu überwachen. Die Binding-Datenbasis bleibt unverändert.

Anmerkung: Um DHCP-Snooping für einen Port einzuschalten, schalten Sie im Dialog *Netzsicherheit > DHCP-Snooping > Global* die Funktion *DHCP-Snooping* global ein. Vergewissern Sie sich, dass der Port einem VLAN zugewiesen ist, in dem DHCP-Snooping eingeschaltet ist.

4.6.3 DHCP-Snooping Statistiken

[Netzsicherheit > DHCP-Snooping > Statistiken]

Das Gerät protokolliert beim DHCP-Snooping erkannte Fehler und erstellt Statistiken. In diesem Dialog überwachen Sie die DHCP-Snooping-Statistiken für jeden Port.

Das Gerät protokolliert folgendes:
- Erkannte Fehler bei der Prüfung der MAC-Adresse des DHCP-Clients
- DHCP-Client-Nachrichten mit erkanntem fehlerhaftem Port
- DHCP-Server-Nachrichten an nicht vertrauenswürdigen Ports

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Zurücksetzen

Setzt die Werte in der Tabelle zurück.

Port

Zeigt die Nummer des Ports.

Fehler bei MAC-Prüfung

Zeigt die Anzahl der Diskrepanzen zwischen der MAC-Adresse des DHCP-Clients im Feld 'chaddr' des DHCP-Datenpaketes und der Quelladresse im Ethernet-Paket.

Ungültige Client-Nachrichten

Zeigt die Anzahl der auf dem Port eingegangenen DHCP-Client-Meldungen, bei denen das Gerät gemäß DHCP-Snooping Binding-Datenbasis den Client auf einem anderen Port erwartet.

Ungültige Server-Nachrichten

Zeigt die Anzahl der DHCP-Server-Meldungen, die das Gerät auf dem nicht-vertrauenswürdigen Port empfangen hat.

4.6.4 DHCP-Snooping Bindings

[Netzsicherheit > DHCP-Snooping > Bindings]

DHCP-Snooping verwendet DHCP-Nachrichten, um die Binding-Datenbasis aufzubauen und zu aktualisieren.

- Statische Bindungen
  Das Gerät ermöglicht Ihnen, bis zu 1024 statische DHCP-Snooping-Bindungen in die Datenbasis einzutragen.
- Dynamische Bindungen
  Die dynamische Binding-Datenbasis enthält ausschließlich Daten für Clients an nicht vertrauenswürdigen Ports.

Dieses Menü ermöglicht Ihnen, die Einstellungen für statische und für dynamische Bindungen festzulegen.

- Neue statische Bindungen einrichten und aktiv/inaktiv setzen.
- Eingerichtete statische Bindungen anzeigen, aktivieren/deaktivieren oder löschen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

Im Feld *MAC-Adresse* legen Sie die MAC-Adresse fest, die Sie an eine IP-Adresse und VLAN-ID binden.

Mögliche Werte:

- Gültige Unicast-MAC-Adresse
  Legen Sie den Wert mit Doppelpunkt-Trennzeichen fest, zum Beispiel `00:11:22:33:44:55`.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

Voraussetzung ist, dass das Kontrollkästchen in Spalte *Aktiv* unmarkiert ist.

Außerdem entfernt das Gerät die mit der Funktion *IP Source Guard* erzeugten dynamischen Bindungen dieses Ports.

MAC-Adresse

Zeigt die MAC-Adresse, die Sie an eine IP-Adresse und VLAN-ID binden.

IP-Adresse

Legt die IP-Adresse für die statische Bindung von DHCP-Snooping fest.

Mögliche Werte:

- Gültige Unicast-IPv4-Adresse kleiner als `224.x.x.x` und außerhalb des Bereiches `127.0.0.0/8` (Voreinstellung: `0.0.0.0`)

VLAN-ID

Legt die ID des VLANs fest, für das der Tabelleneintrag gilt.

Mögliche Werte:

- `<ID der VLANs, die eingerichtet sind>`

Port

Legt den Port für die statische DHCP-Snooping-Bindung fest.

Mögliche Werte:

- Verfügbare Ports

Verbleibende Binding-Zeit

Zeigt die Restlaufzeit der dynamischen DHCP-Snooping-Bindung.

Aktiv

Aktiviert/deaktiviert die konfigurierte statische DHCP-Snooping-Bindung.

Mögliche Werte:

- `markiert`
  Die statische DHCP-Snooping-Bindung ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die statische DHCP-Snooping-Bindung ist inaktiv.

4.7 IP Source Guard

[Netzsicherheit > IP Source Guard]

IP Source Guard (IPSG) ist eine Funktion zur Unterstützung der Netzsicherheit. Die Funktion filtert IP-Datenpakete basierend auf der Source-ID (Quell-IP-Adresse oder die Quell-MAC-Adresse) des Teilnehmers. IPSG unterstützt Sie beim Schutz des Netzes vor Angriffen über IP-/MAC-Adress-Spoofing.

IPSG und DHCP-Snooping
IP Source Guard arbeitet mit der Funktion *DHCP-Snooping*zusammen.

DHCP-Snooping verwirft IP-Datenpakete an nicht vertrauenswürdigen Ports mit Ausnahme von DHCP-Nachrichten. Wenn das Gerät DHCP-Antworten empfängt und die DHCP-Snooping Binding-Datenbasis eingerichtet ist, erstellt das Gerät pro Port eine VLAN Access Control List (VACL), welche die Source-IDs der Teilnehmer enthält.

Die Parameter der Funktion *DHCP-Snooping* für einzelne Ports und für einzelne VLANs konfigurieren Sie im Dialog *Netzsicherheit > DHCP-Snooping > Konfiguration*.

IPSG und Portsicherheit
IP Source Guard arbeitet mit der Funktion *Port-Sicherheit* zusammen. Siehe Dialog *Netzsicherheit >* Port-Sicherheit. IPSG teilt der Funktion *Port-Sicherheit* auf Anfrage mit, ob eine neu gelernte MAC-Adresse zu einer gültigen Bindung gehört.

- Wenn Sie IPSG am Ingress-Port deaktiviert haben, bezeichnet IPSG das Datenpaket als gültig.
- Wenn Sie IPSG am Ingress-Port aktiviert haben, prüft IPSG die MAC-Adresse anhand der Bindings-Datenbasis. Wenn die MAC-Adresse in der Bindings-Datenbasis eingetragen ist, bezeichnet IPSG das Datenpaket als gültig, andernfalls als ungültig.

Die Funktion *Port-Sicherheit*übernimmt die weitere Behandlung von ungültigen Datenpaketen. Die Einstellungen der Funktion *Port-Sicherheit* legen Sie im Dialog *Netzsicherheit > Port-Sicherheit* fest.

Anmerkung: Damit das Gerät die IP-Adresse und die MAC-Adresse der auf dem Port empfangenen Datenpakete prüft, schalten Sie die Funktion *MAC verifizieren* ein.

Damit das Gerät vor Weiterleiten des Datenpakets die VLAN-ID und MAC-Adresse des Absenders prüft, schalten Sie zusätzlich die Funktion *Port-Sicherheit* ein. Siehe Dialog *Netzsicherheit > Port-Sicherheit*.

Das Menü enthält die folgenden Dialoge:

- IP Source Guard Port
- IP Source Guard Bindings

4.7.1 IP Source Guard Port

[Netzsicherheit > IP Source Guard > Port]

Dieser Dialog ermöglicht Ihnen, die folgenden Geräteeigenschaften pro Port anzuzeigen und zu konfigurieren:

- Quell-MAC-Adressen für die Filterung ein-/ausschließen
- Die Funktion *IP Source Guard* aktivieren/deaktivieren.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

MAC verifizieren

Aktiviert/deaktiviert bei aktiver Funktion *IP Source Guard* die Filterung nach der Quell-MAC-Adresse. Das Gerät führt diese Filterung zusätzlich zur Filterung nach der Quell-IP-Adresse durch.

Mögliche Werte:

- `markiert`
  Die Filterung nach der Quell-MAC-Adresse ist aktiv.
  Um die Funktion zu aktivieren, markieren Sie das Kontrollkästchen *Aktiv*.
- `unmarkiert` (Voreinstellung)
  Die Filterung nach der Quell-MAC-Adresse ist inaktiv.
  Um die Funktion zu deaktivieren, heben Sie die Markierung des Kontrollkästchens *Aktiv* auf.

Aktiv

Aktiviert/deaktiviert die Funktion *IP Source Guard* auf dem Port.

Mögliche Werte:

- `markiert`
  Die Funktion *IP Source Guard* ist aktiv.
  Schalten Sie zusätzlich im Dialog *Netzsicherheit > DHCP-Snooping > Global* die Funktion *DHCP-Snooping* ein.
- `unmarkiert` (Voreinstellung)
  Die Funktion *IP Source Guard* ist inaktiv.

4.7.2 IP Source Guard Bindings

[Netzsicherheit > IP Source Guard > Bindings]

Dieser Dialog zeigt statische und dynamische IP Source Guard-Bindungen.

- Dynamische Bindungen lernt das Gerät mit DHCP-Snooping. Siehe Dialog *Netzsicherheit* > DHCP-Snooping > *Konfiguration*.
- Statische Bindungen sind manuell durch Benutzer eingerichtete IP-Source-Guard-Bindungen. Der Dialog ermöglicht Ihnen, statische Bindungen zu bearbeiten.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *MAC-Adresse* legen Sie die MAC-Adresse für die statische Bindung fest.
- Im Feld *IP-Adresse* legen Sie die IP-Adresse für die statische Bindung fest.
- Im Feld *VLAN-ID*legen Sie die VLAN-ID fest.
- Im Feld *Port* legen Sie die ID des VLANs fest.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

Voraussetzung ist, dass das Kontrollkästchen in Spalte *Aktiv* unmarkiert ist.

MAC-Adresse

Zeigt die MAC-Adresse der Bindung.

IP-Adresse

Zeigt die IP-Adresse der Bindung.

VLAN-ID

Zeigt die VLAN-ID der Bindung.

Port

Zeigt die Nummer des Ports der Bindung.

Hardware-Status

Zeigt den Hardware-Status der Bindung.

Das Gerät wendet die Bindung ausschließlich dann auf die Hardware an, wenn die Einstellungen korrekt sind. Bevor das Gerät die statische IPSG-Bindung auf die Hardware anwendet, prüft es die Voraussetzungen:

- Das Kontrollkästchen *Aktiv* ist markiert.
- Die Funktion *IP Source Guard* auf dem Port ist eingeschaltet, im Dialog *Netzsicherheit > IP Source Guard > Port* ist das Kontrollkästchen *Aktiv* markiert.

Mögliche Werte:

▶ `markiert`
Die Bindung ist aktiv, das Gerät wendet die Bindung auf die Hardware an.

▶ `unmarkiert`
Die Bindung ist inaktiv.

Aktiv

Aktiviert/deaktiviert die konfigurierte statische IPSG-Bindung zwischen der festgelegten MAC-Adresse und der festgelegten IP-Adresse, für das festgelegte VLAN auf dem festgelegten Port.

Mögliche Werte:

▶ `markiert`
Die statische IPSG-Bindung ist aktiv.

▶ `unmarkiert` (Voreinstellung)
Die statische IPSG-Bindung ist inaktiv.

Anmerkung: Damit die statische Bindung wirksam wird, schalten Sie die Funktion *IP Source Guard* auf dem zugehörigen Port ein. Markieren Sie im Dialog *Netzsicherheit > IP Source Guard > Port* das Kontrollkästchen *Aktiv*.

4.8 Dynamic ARP Inspection

[Netzsicherheit > Dynamic ARP Inspection]

Dynamic ARP Inspection ist eine Funktion zur Unterstützung der Netzsicherheit. Diese Funktion analysiert ARP-Pakete, protokolliert sie und weist ungültige und feindliche ARP-Pakete zurück.

Die Funktion *Dynamic ARP Inspection* hilft, eine Reihe von Man-in-the-Middle-Angriffen zu verhindern. Bei dieser Art von Angriffen hört eine bösartige Station den Datenverkehr von anderen Teilnehmern ab, wobei sie in den ARP-Cache ihrer arglosen Nachbarn eingreift. Die bösartige Station sendet ARP-Anfragen und ARP-Antworten und trägt in der IP-zu-MAC Adress-Beziehung (Binding) bei ihrer eigenen MAC-Adresse die IP-Adresse eines anderen Teilnehmers ein.

Die Funktion *Dynamic ARP Inspection* hilft, durch folgende Maßnahmen sicherzustellen, dass das Gerät ausschließlich gültige ARP-Anfragen und ARP-Antworten weiterleitet.

▶ Abhören von ARP-Anfragen und ARP-Antworten an nicht vertrauenswürdigen Ports.
▶ Vergewissern, dass die ermittelten Pakete eine gültige IP-zu-MAC-Adress-Beziehung (Binding) haben, bevor das Gerät den lokalen ARP-Cache aktualisiert und bevor das Gerät die Pakete an die zugehörige Zieladresse weiterleitet.
▶ Verwerfen von ungültigen ARP-Paketen.

Das Gerät ermöglicht Ihnen, bis zu 100 aktive ARP-ACLs (Zugriffslisten) zu definieren. Pro ARP-ACL können Sie bis zu 20 Regeln aktivieren.

Das Menü enthält die folgenden Dialoge:

- Dynamic-ARP-Inspection Global
- Dynamic-ARP-Inspection Konfiguration
- Dynamic-ARP-Inspection ARP-Regeln
- Dynamic-ARP-Inspection Statistiken

4.8.1 Dynamic-ARP-Inspection Global

[Netzsicherheit > Dynamic ARP Inspection > Global]

Konfiguration

Quell-MAC verifizieren

Aktiviert/deaktiviert die Verifizierung der Quell-MAC-Adresse. Das Gerät führt die Prüfung sowohl in ARP-Anfragen als auch in ARP-Antworten durch.

Mögliche Werte:

- `markiert`
  Die Verifizierung der Quell-MAC-Adresse ist aktiv.
  Das Gerät prüft die Quell-MAC-Adresse empfangener ARP-Pakete.
  - ARP-Pakete mit gültiger Quell-MAC-Adresse vermittelt das Gerät an die zugehörige Zieladresse und aktualisiert den lokalen ARP-Cache.
  - ARP-Pakete mit ungültiger Quell-MAC-Adresse verwirft das Gerät.
- `unmarkiert` (Voreinstellung)
  Die Verifizierung der Quell-MAC-Adresse ist inaktiv.

Destination-MAC verifizieren

Aktiviert/deaktiviert die Verifizierung der Ziel-MAC-Adresse. Das Gerät führt die Prüfung in ARP-Antworten durch.

Mögliche Werte:

- `markiert`
  Die Verifizierung der Ziel-MAC-Adresse ist aktiv.
  Das Gerät prüft die Ziel-MAC-Adresse der eingehenden ARP-Pakete.
  - ARP-Pakete mit gültiger Ziel-MAC-Adresse leitet das Gerät an die zugehörige Zieladresse weiter und aktualisiert den lokalen ARP-Cache.
  - ARP-Pakete mit ungültiger Ziel-MAC-Adresse verwirft das Gerät.
- `unmarkiert` (Voreinstellung)
  Das Prüfen der Ziel-MAC-Adresse der eingehenden ARP-Pakete ist deaktiviert.

IP-Adresse verifizieren

Aktiviert/deaktiviert die Verifizierung der IP-Adresse.

In ARP-Anfragen prüft das Gerät die Quell-IP-Adresse. In ARP-Antworten prüft das Gerät die Ziel- und die Quell-IP-Adresse.

Das Gerät betrachtet die folgenden IP-Adressen als ungültig:

- `0.0.0.0`
- Broadcast-Adressen `255.255.255.255`
- Multicast-Adressen `224.0.0.0/4` (Class D)
- Class-E-Adressen `240.0.0.0/4` (reserviert für spätere Zwecke)
- Loopback-Adressen im Bereich `127.0.0.0/8`.

Mögliche Werte:

- `markiert`
  Die Verifizierung der IP-Adresse ist aktiv.
  Das Gerät prüft die IP-Adresse der eingehenden ARP-Pakete. ARP-Pakete mit gültiger IP-Adresse leitet das Gerät an die zugehörige Zieladresse weiter und aktualisiert den lokalen ARP-Cache. ARP-Pakete mit ungültiger IP-Adresse verwirft das Gerät.
- `unmarkiert` (Voreinstellung)
  Die Verifizierung der IP-Adresse ist inaktiv.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Dynamic ARP Inspection*.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für *Dynamic ARP Inspection* ist aktiv.
  Markieren Sie zusätzlich im Dialog *Netzsicherheit > Dynamic ARP Inspection > Konfiguration*, Registerkarte *Port* das Kontrollkästchen in Spalte *Auto-Disable* für die gewünschten Ports.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für *Dynamic ARP Inspection* ist inaktiv.

4.8.2 Dynamic-ARP-Inspection Konfiguration

[Netzsicherheit > Dynamic ARP Inspection > Konfiguration]

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

[Port]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Vertraue

Aktiviert/deaktiviert die Überwachung von ARP-Paketen auf nicht-vertrauenswürdigen Ports.

Mögliche Werte:
- `markiert`
  Die Überwachung ist aktiv.
  Das Gerät überwacht ARP-Pakete auf nicht-vertrauenswürdigen Ports.
  ARP-Pakete auf vertrauenswürdigen Ports leitet das Gerät direkt weiter.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Lastbegrenzung

Legt die maximale Anzahl von ARP-Paketen pro Intervall auf diesem Port fest. Wenn die Rate der eingehenden ARP-Pakete das festgelegte Limit in einem Burst-Intervall gegenwärtig überschreitet, verwirft das Gerät weitere eingehende ARP-Pakete. Das Burst-Intervall legen Sie in Spalte *Burst-Intervall* fest.

Optional schaltet das Gerät zusätzlich den Port aus, wenn Sie die Auto-Disable Funktion aktiviert haben. Die Funktion *Auto-Disable* schalten Sie in Spalte *Auto-Disable* ein/aus.

Mögliche Werte:
- `-1` (Voreinstellung)
  Hebt die Limitierung der Anzahl von ARP-Paketen pro Burst-Intervall auf diesem Port auf.
- `0..300` Pakete pro Intervall
  Begrenzt die maximale Anzahl von ARP-Paketen pro Burst-Intervall auf diesem Port.

Burst-Intervall

Legt die Länge des Burst-Intervalls in Sekunden auf diesem Port fest. Das Burst-Intervall ist für die Rate-Limiting-Funktion relevant.

Die maximale Anzahl von ARP-Paketen pro Burst-Intervall legen Sie in Spalte *Lastbegrenzung* fest.

Mögliche Werte:

- `1..15` (Voreinstellung: `1`)

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für die Parameter, deren Einhaltung die Funktion *Dynamic ARP Inspection* auf dem Port überwacht.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *Auto-Disable* ist auf dem Port aktiv.
  Voraussetzung ist, dass im Dialog *Netzsicherheit > Dynamic ARP Inspection > Global*, Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable* markiert ist.
  - Das Gerät schaltet den Port aus, wenn der Port während der in Spalte *Burst-Intervall* festgelegten Zeit mehr ARP-Pakete empfängt als im Feld *Lastbegrenzung* 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.
  - Nach einer Wartezeit schaltet die Funktion *Auto-Disable* 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 Funktion *Auto-Disable* auf dem Port ist inaktiv.

[VLAN-ID]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

VLAN-ID

Zeigt die VLAN-ID, auf die sich der Tabelleneintrag bezieht.

Protokolliere

Aktiviert/deaktiviert die Protokollierung von ungültigen ARP-Paketen, die das Gerät in diesem VLAN ermittelt. Das Gerät behandelt ein ARP-Paket als ungültig, wenn es bei der Prüfung von IP-Adresse, Quell-MAC-Adresse, Ziel-MAC-Adresse oder bei der Prüfung der IP-zu-MAC-Adress-Beziehung (Binding) einen Fehler erkennt.

Mögliche Werte:

- `markiert`
  Die Protokollierung ungültiger Pakete ist aktiv.
  Das Gerät protokolliert ungültige ARP-Pakete.
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ungültiger Pakete ist inaktiv.

Binding check

Aktiviert/deaktiviert das Prüfen eingehender ARP-Pakete, die das Gerät an nicht-vertrauenswürdigen Ports und an VLANs mit aktiver Funktion *Dynamic ARP Inspection* empfängt. Das Gerät prüft bei diesen ARP-Paketen die ARP- ACL und die DHCP-Snooping-Beziehung (Binding).

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Beziehungs(Binding)-Prüfung von ARP-Paketen ist aktiviert.
- `unmarkiert`
  Die Beziehungs(Binding)-Prüfung von ARP-Paketen ist deaktiviert.

ACL strict

Aktiviert/deaktiviert die strikte Prüfung von eingehenden ARP-Paketen anhand der festgelegten ARP-ACL-Regeln.

Mögliche Werte:

- `markiert`
  Die strikte Prüfung ist aktiv.
  Das Gerät prüft eingehende ARP-Pakete anhand der in Spalte *ARP ACL* festgelegten ARP-ACL-Regeln.
- `unmarkiert` (Voreinstellung)
  Die strikte Prüfung ist inaktiv.
  Das Gerät prüft eingehende ARP-Pakete anhand der in Spalte *ARP ACL* festgelegten ARP-ACL-Regeln und anschließend anhand der Einträge in der DHCP-Snooping-Datenbank.

ARP ACL

Legt die ARP-ACL fest, die das Gerät verwendet.

Mögliche Werte:

- `<Name der Regel>`
  Die Regeln erzeugen und bearbeiten Sie im Dialog *Netzsicherheit > Dynamic ARP Inspection > ARP Regeln*.

Aktiv

Aktiviert/deaktiviert die Funktion *Dynamic ARP Inspection* in diesem VLAN.

Mögliche Werte:

- `markiert`
  Die Funktion *Dynamic ARP Inspection* ist in diesem VLAN aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Dynamic ARP Inspection* ist in diesem VLAN inaktiv.

4.8.3 Dynamic-ARP-Inspection ARP-Regeln

[Netzsicherheit > Dynamic ARP Inspection > ARP Regeln]

Dieser Dialog ermöglicht Ihnen, Regeln zur Prüfung und Filterung von ARP-Paketen zu definieren.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *Name* legen Sie den Namen der ARP-Regel fest.
- Im Feld *Quell-IP-Adresse* legen Sie die Quell-IP-Adresse der ARP-Regel fest.
- Im Feld *Quell-MAC-Adresse* legen Sie die Quell-MAC-Adresse der ARP-Regel fest.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

Name

Zeigt den Namen der ARP-Regel.

Quell-IP-Adresse

Legt die Quelladresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- Gültige IPv4-Adresse
  Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Quelladresse an.

Quell-MAC-Adresse

Legt die Quelladresse der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- Gültige MAC-Adresse
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an.

Aktiv

Aktiviert/deaktiviert die *ARP*-Regel.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Regel ist aktiv.
- `unmarkiert`
  Die Regel ist inaktiv.

4.8.4 Dynamic-ARP-Inspection Statistiken

[Netzsicherheit > Dynamic ARP Inspection > Statistiken]

Dieses Fenster zeigt die Anzahl verworfener und weitergeleiteter ARP-Pakete in einer Übersicht.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Zurücksetzen

Setzt die Werte in der Tabelle zurück.

VLAN-ID

Zeigt die VLAN-ID, auf die sich der Tabelleneintrag bezieht.

Weitergeleitete Pakete

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* weitergeleitet hat.

Verworfene Pakete

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* verworfen hat.

DHCP drops

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung der DHCP-Snooping-Beziehung (Binding) verworfen hat.

DHCP permits

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung der DHCP-Snooping-Beziehung (Binding) weitergeleitet hat.

ACL drops

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung anhand der ARP-ACL-Regeln verworfen hat.

ACL permits

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung anhand der ARP-ACL-Regeln weitergeleitet hat.

Ungültige Quell-MAC

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* aufgrund eines erkannten Fehlers in der Quell-MAC-Adresse verworfen hat.

Ungültige Ziel-MAC

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* aufgrund eines erkannten Fehlers in der Ziel-MAC-Adresse verworfen hat.

Ungültige IP-Adresse

Zeigt die Anzahl der ARP-Pakete, die das Gerät nach Prüfung durch die Funktion *Dynamic ARP Inspection* aufgrund eines erkannten Fehlers in der IP-Adresse verworfen hat.

4.9 ACL

[Netzsicherheit > 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.

Wenn ein Datenpaket die Kriterien einer oder mehrerer Regeln erfüllt, dann wendet das Gerät die in der ersten zutreffenden Regel festgelegte Aktion auf den Datenstrom an. Das Gerät ignoriert die Regeln, die der ersten zutreffenden Regel folgen. Mögliche Aktionen sind:

- `permit`: Das Gerät vermittelt das Datenpaket an einen Port oder an ein VLAN.
  Wenn nötig, vermittelt das Gerät eine Kopie der Datenpakete an einen weiteren Port.
- `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 dieses Verhalten. An das Ende einer Access-Control-Liste fügt das Gerät eine implizite Deny-All-Regel ein. Demzufolge verwirft das Gerät Datenpakete, die mit keiner der Regel-Kriterien übereinstimmen. Wenn Sie ein anderes Verhalten wünschen, fügen Sie am Ende Ihrer Access-Control-Listen eine Permit-All-Regel ein.

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

- ☐ Erzeugen Sie ein Zeitprofil, wenn nötig. Siehe Dialog *Netzsicherheit > ACL > Zeitprofil*. Das Gerät wendet Access-Control-Listen mit Zeitprofil zu festgelegten Zeiten anstatt permanent an.
- ☐ 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
- ACL Zeitprofil

4.9.1 ACL IPv4-Regel

[Netzsicherheit > 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 ermöglicht Ihnen, nach folgenden Kriterien zu filtern:
- Quell- oder Ziel-IP-Adresse eines Datenpakets
- Typ des übertragenden Protokolls
- Quell- oder Ziel-Port eines Datenpakets
- Klassifizierung nach DSCP
- Klassifizierung nach ToS

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

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.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

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 in Abhängigkeit vom Wert in den folgenden Feldern an:
  - *Quell-IP-Adresse*, *Ziel-IP-Adresse*, *Protokoll*
  - *DSCP*, *TOS-Priorität*, *TOS-Maske*
  - *ICMP-Typ*, *ICMP-Code*
  - *IGMP type*
  - *Established*
  - *Paket fragmentiert*
  - *TCP-Flag*

Quell-IP-Adresse

Legt die Quelladresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `?.?.?.?` (Voreinstellung)
  Das Gerät wendet die Regel auf IP-Datenpakete mit beliebiger Quelladresse an.
- Gültige IPv4-Adresse
  Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Quelladresse an. Verwenden Sie das Zeichen `?` als Platzhalter.
  Beispiel `192.?.?.32`: Das Gerät wendet die Regel auf IP-Datenpakete an, deren Quelladresse mit `192.` beginnt und mit `.32` endet.
- Gültige IPv4-Adresse/Bitmaske
  Das Gerät wendet die Regel auf IP-Datenpakete mit der festgelegten Quelladresse an. Die inverse Bitmaske ermöglicht Ihnen, den Adressbereich bitgenau festzulegen.
  Beispiel `192.168.1.0/0.0.0.127`: Das Gerät wendet die Regel auf IP-Datenpakete mit einer Quelladresse im Bereich von `192.168.1.0` bis `….127` an.

Ziel-IP-Adresse

Legt die Zieladresse der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `?.?.?.?` (Voreinstellung)
  Das Gerät wendet die Regel auf IP-Datenpakete mit beliebiger Zieladresse an.
- Gültige IPv4-Adresse
  Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse an. Verwenden Sie das Zeichen `?` als Platzhalter.
  Beispiel `192.?.?.32`: Das Gerät wendet die Regel auf IP-Datenpakete an, deren Quelladresse mit `192.` beginnt und mit `.32` endet.
- Gültige IPv4-Adresse/Bitmaske
  Das Gerät wendet die Regel auf Datenpakete mit der festgelegten Zieladresse an. Die inverse Bitmaske ermöglicht Ihnen, den Adressbereich bitgenau festzulegen.
  Beispiel `192.168.1.0/0.0.0.127`: Das Gerät wendet die Regel auf IP-Datenpakete mit einer Zieladresse im Bereich von `192.168.1.0` bis `….127` an.

Protokoll

Legt den IP-Protokoll- oder Layer 4-Protokoll-Typ der Datenpakete fest, auf die das Gerät die Regel anwendet. Das Gerät wendet die Regel ausschließlich auf Datenpakete an, die im *Protocol*-Feld den festgelegten Wert enthalten.

Mögliche Werte:

- `any` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Protokolltyp auszuwerten.
- `icmp`
  Internet Control Message Protocol (RFC 792)
- `igmp`
  Internet Group Management Protocol
- `ip-in-ip`
  IP in IP tunneling (RFC 2003)
- `tcp`
  Transmission Control Protocol (RFC 793)
- `udp`
  User Datagram Protocol (RFC 768)
- `ip`
  Internet Protocol

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 auszuwerten.
- `1..65535`
  Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten Quell-Port enthalten.
  Um einen Port-Bereich festzulegen, können Sie einen der folgenden Operatoren voranstellen:
  - `<`
    Bereich unterhalb der festgelegten Port-Nummer
  - `>`
    Bereich oberhalb der festgelegten Port-Nummer
  - `!=`
    gesamter Port-Bereich mit Ausnahme des festgelegten Ports

  Diese Operatoren sind ausschließlich in Regeln zulässig, die das Gerät auf empfangene Datenpakete anwendet. Siehe Dialog *Netzsicherheit > ACL > Zuweisung*: Spalte *Richtung* = `inbound`.

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 auszuwerten.
- `1..65535`
  Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten Ziel-Port enthalten.
  Um einen Port-Bereich festzulegen, können Sie einen der folgenden Operatoren voranstellen:
  - `<`
    Bereich unterhalb der festgelegten Port-Nummer
  - `>`
    Bereich oberhalb der festgelegten Port-Nummer
  - `!=`
    gesamter Port-Bereich mit Ausnahme des festgelegten Ports

  Diese Operatoren sind ausschließlich in Regeln zulässig, die das Gerät auf empfangene Datenpakete anwendet. Siehe Dialog *Netzsicherheit > ACL > Zuweisung*: Spalte *Richtung* = `inbound`.

DSCP

Legt den Differentiated-Service-Code-Point (DSCP-Wert) im Header der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `-` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den DSCP-Wert auszuwerten.
- `0..63`
  Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten DSCP-Wert enthalten.

TOS-Priorität

Legt die *IP-Precedence* (*ToS*-Wert) im Header 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 *ToS*-Wert zu bewerten.
- `0..7`
  Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten *ToS*-Wert enthalten.

TOS-Maske

Legt die Bitmaske für den *ToS*-Wert im Header der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass Sie in Spalte *TOS-Priorität* einen *ToS*-Wert festlegen.

Mögliche Werte:

- `any` (Voreinstellung)
  Das Gerät wendet die Regel auf die IP-Datenpakete an und wertet den *ToS*-Wert vollständig aus.
- `1..1f`
  Das Gerät wendet die Regel auf die IP-Datenpakete an und wertet die in der Bitmaske gesetzten Bits des *ToS*-Werts aus.

ICMP-Typ

Legt den ICMP-Typ im TCP-Header der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `-1` (Voreinstellung)
  ICMP-Typ-Abgleich ist inaktiv.
- `0..255`
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an und wertet den festgelegten ICMP-Typ aus.

ICMP-Code

Legt den ICMP-Code im TCP-Header der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass Sie im *ICMP-Typ*-Feld einen ICMP-Wert festlegen.

Mögliche Werte:

- `-1` (Voreinstellung)
  ICMP-Code-Abgleich ist inaktiv.
- `0..255`
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an und wertet den festgelegten ICMP-Code aus.

IGMP type

Legt den IGMP-Typ im TCP-Header der IP-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `0` (Voreinstellung)
  IGMP-Typ-Abgleich ist inaktiv.
- `1..255`
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an und wertet den festgelegten ICMP-Typ aus.

Established

Aktiviert/deaktiviert die Anwendung der ACL-Regel auf TCP-Datenpakete, deren RST-Bit oder ACK-Bit im TCP-Header gesetzt ist.

Mögliche Werte:

- `markiert`
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an, in dem das RST-Bit oder ACK-Bit im TCP-Header gesetzt ist.
- `unmarkiert` (Voreinstellung)
  Der Abgleich ist inaktiv.

Paket fragmentiert

Aktiviert/deaktiviert die Anwendung der ACL-Regel auf die Paketfragmente.

Um das komplette Datenpaket einschließlich seiner Fragmente zu filtern, erstellen Sie 2 ACL-Regeln.

- Erstellen Sie eine ACL-Regel für das erste Datenpaket, womit Sie sowohl auf Protokollebene als auch nach TCP/UDP-Ports zu filtern.
- Erstellen Sie eine zweite ACL-Regel für die Fragmente, womit Sie lediglich auf Protokollebene filtern.

Mögliche Werte:

- `markiert`
  Das Gerät wendet die ACL-Regel auf die Fragmente an. Verwenden Sie diese Einstellung in der zweiten ACL-Regel für die Fragmente.
- `unmarkiert` (Voreinstellung)
  Das Gerät wendet die ACL-Regel nicht auf Fragmente an.

TCP-Flag

Legt TCP-Flag und Maske fest.

Das Gerät ermöglicht Ihnen, mehrere Werte einzugeben, indem Sie die Werte mit Komma trennen.

Legen Sie die Flags entweder als `+` oder als `-` fest.

Mögliche Werte:

- `-` (Voreinstellung)
  Der TCP-Flag-Abgleich ist inaktiv.
- `-`
  Wenn Sie diesen Wert in Kombination mit den folgenden Flags verwenden, wertet das Gerät Datenpakete aus, in denen das Flag nicht gesetzt ist.
- `+`
  Wenn Sie diesen Wert in Kombination mit den folgenden Flags verwenden, wertet das Gerät Datenpakete aus, in denen das Flag nicht gesetzt ist.
- `fin`
  Zeigt, dass das sendende Gerät die Übertragung beendet hat.
- `syn`
  Zeigt, dass die Nummern der `Synchronize sequence` signifikant sind. Dieses Flag ist ausschließlich für das jeweils erste gesendete Paket jedes Endgeräts gesetzt.
- `rst`
  Zeigt ein Zurücksetzen der TCP-Verbindung an.
- `psh`
  Zeigt die Push-Funktion, bei der ein Gerät die Übermittlung von gepufferten Daten zur empfangenden Anwendung anfordert.
- `ack`
  Zeigt, dass das Feld `Acknowledgment` signifikant ist. Nach dem initialen Senden des Syn-Paketes durch den Client ist dieses Flag für alle Pakete gesetzt.
- `urg`
  Zeigt, dass das Feld `Urgent pointer` signifikant ist.

Aktion

Legt fest, wie das Gerät die Datenpakete verarbeitet, wenn es die Regel anwendet.

Mögliche Werte:

- `permit` (Voreinstellung)
  Das Gerät vermittelt die IP-Datenpakete.
- *`deny`*
  Das Gerät verwirft die IP-Datenpakete.

Redirection-Port

Legt den Port fest, an den das Gerät die IP-Datenpakete vermittelt. Voraussetzung ist, dass Sie in Spalte *Aktion* den Wert *`permit`* festlegen. Das Gerät bietet Ihnen keine Möglichkeit, IP-Datenpakete über VLAN-Grenzen hinweg zu vermitteln.

Mögliche Werte:

- `-` (Voreinstellung)
  Die Funktion *Redirection-Port* ist inaktiv.
- `<Port-Nummer>`
  Das Gerät vermittelt die IP-Datenpakete an den festgelegten Port.

Mirror-Port

Legt den Port fest, an den das Gerät eine Kopie der IP-Datenpakete vermittelt. Voraussetzung ist, dass Sie in Spalte *Aktion* den Wert *`permit`* festlegen. Das Gerät bietet Ihnen keine Möglichkeit, IP-Datenpakete über VLAN-Grenzen hinweg zu vermitteln.

Mögliche Werte:

- `-` (Voreinstellung)
  Die Funktion *Mirror-Port* ist inaktiv.
- `<Port-Nummer>`
  Das Gerät vermittelt eine Kopie der IP-Datenpakete an den festgelegten Port.

Zugewiesene Queue-ID

Legt die Warteschlange fest, der das Gerät die IP-Datenpakete zuweist.

Mögliche Werte:

- `0..7` (Voreinstellung: `0`)

Protokolliere

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog *Diagnose > Bericht > System-Log*.

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiv.
  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 inaktiv.

Das Gerät ermöglicht Ihnen, für bis zu 128 Deny-Regeln diese Funktion zu aktivieren.

Zeitprofil

Legt fest, ob das Gerät die Regel permanent oder zeitgesteuert anwendet.

Mögliche Werte:

- `<leer>` (Voreinstellung)
  Das Gerät wendet die Regel permanent an.
- `[Zeitprofil]`
  Das Gerät wendet die Regel ausschließlich zu den im Zeitprofil festgelegten Zeiten an. Die Zeitprofile bearbeiten Sie im Dialog *Netzsicherheit > ACL > Zeitprofil*.

Lastbegrenzung

Legt das Limit fest für die Datentransferrate auf dem in Spalte *Redirection-Port* festgelegten Port. Das Limit gilt für die Summe aus zu sendenden und empfangenen Daten.

Diese Funktion begrenzt den Datenstrom auf dem Port oder im VLAN:

Mögliche Werte:

- `0` (Voreinstellung)
  Keine Begrenzung der Datentransferrate.
- `1..4294967295`
  Wenn die Datentransferrate auf dem Port den festgelegten Wert überschreitet, verwirft das Gerät überschüssige IP-Datenpakete. Voraussetzung ist, dass Sie in Spalte *Burst-Size* einen Wert > `0` festlegen. Die Maßeinheit des Limits legen Sie fest in Spalte *Einheit*.

Einheit

Legt die Maßeinheit fest für die in Spalte *Lastbegrenzung* festgelegte Datentransferrate.

Mögliche Werte:

- *kbps*
  kByte pro Sekunde

Burst-Size

Legt das Limit in KByte fest für das Datenvolumen während temporärer Bursts.

Mögliche Werte:

- 0 (Voreinstellung)
  Keine Begrenzung des Datenvolumens.
- 1..128
  Wenn das Datenvolumen während temporärer Bursts auf dem Port den festgelegten Wert überschreitet, verwirft das Gerät überschüssige MAC-Datenpakete. Voraussetzung ist, dass Sie in Spalte *Lastbegrenzung* einen Wert >0 festlegen.

Empfehlung:

- Wenn die Bandbreite bekannt ist:
  Burst-Size = Bandbreite × Zugelassene Dauer eines Bursts / 8.
- Wenn die Bandbreite unbekannt ist:
  Burst-Size = 10 × MTU (*Maximum Transmission Unit*) des Ports.

4.9.2 ACL MAC-Regel

[Netzsicherheit > 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 ermöglicht Ihnen, nach folgenden Kriterien zu filtern:
- Quell- oder Ziel-MAC-Adresse eines Datenpakets
- Typ des übertragenden Protokolls
- Zugehörigkeit zu einem bestimmten VLAN
- Serviceklasse eines Datenpakets

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

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.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

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.
  Das Gerät ignoriert den Wert in den Feldern *Quell-MAC-Adresse*,*Ziel-MAC-Adresse*, *Ethertype*, *Benutzerspezifischer Ethertype-Wert*, *VLAN-ID* und *COS*.
- `unmarkiert`
  Das Gerät wendet die Regel auf MAC-Datenpakete an, abhängig vom Wert in den Feldern *Quell-MAC-Adresse*,*Ziel-MAC-Adresse*, *Ethertype*, *Benutzerspezifischer Ethertype-Wert*, *VLAN-ID* und *COS*.

Quell-MAC-Adresse

Legt die Quelladresse der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `??:??:??:??:??:??` (Voreinstellung)
  Das Gerät wendet die Regel auf MAC-Datenpakete mit beliebiger Quelladresse an.
- Gültige MAC-Adresse
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an.
  Verwenden Sie das Zeichen `?` als Platzhalter.
  Beispiel `00:11:??:??:??:??`: Das Gerät wendet die Regel auf MAC-Datenpakete an, deren Quelladresse mit `00:11` beginnt.
- Gültige MAC-Adresse/Bitmaske
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an. Die Bitmaske ermöglicht Ihnen, 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 Quelladresse im Bereich von `00:11:22:33:44:54` bis `…:57` an.

Ziel-MAC-Adresse

Legt die Zieladresse der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `??:??:??:??:??:??` (Voreinstellung)
  Das Gerät wendet die Regel auf MAC-Datenpakete mit beliebiger Zieladresse an.
- Gültige MAC-Adresse
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Zieladresse an.
  Verwenden Sie das Zeichen `?` als Platzhalter.
  Beispiel `00:11:??:??:??:??`: Das Gerät wendet die Regel auf MAC-Datenpakete an, deren Zieladresse mit `00:11` beginnt.
- Gültige MAC-Adresse/Bitmaske
  Das Gerät wendet die Regel auf MAC-Datenpakete mit der festgelegten Quelladresse an. Die Bitmaske ermöglicht Ihnen, 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 Zieladresse im Bereich von `00:11:22:33:44:54` bis `…:57` an.

Ethertype

Legt das *Ethertype*-Schlüsselwort der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `custom` (Voreinstellung)
  Das Gerät wendet den in Spalte *Benutzerspezifischer Ethertype-Wert* festgelegten Wert an.
- `appletalk`
- `arp`
- `ibmsna`
- `ipv4`
- `ipv6`
- `ipxold`
- `mplsmcast`
- `mplsucast`
- `netbios`
- `novell`
- `rarp`
- `pppoe`

Benutzerspezifischer Ethertype-Wert

Legt den *Ethertype*-Wert der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass Sie in Spalte *Ethertype* den Wert `custom` festlegen.

Mögliche Werte:

- `any` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes MAC-Datenpaket an, ohne den *Ethertype*-Wert zu bewerten.
- `600..ffff`
  Das Gerät wendet die Regel ausschließlich auf MAC-Datenpakete an, welche den hier festgelegten *Ethertype*-Wert enthalten.

VLAN-ID

Legt die VLAN-ID der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `0` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes MAC-Datenpaket an, ohne die VLAN-ID auszuwerten.
- `1..4042`

COS

Legt den Class-of-Service-Wert (COS) der MAC-Datenpakete fest, auf die das Gerät die Regel anwendet.

Mögliche Werte:

- `0..7`
- `any` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes MAC-Datenpaket an, ohne den Class-of-Service-Wert auszuwerten.

Anmerkung: Bei Datenpaketen ohne VLAN-Tag verwendet das Gerät die Port-Priorität anstatt des *COS*-Wertes.

Aktion

Legt fest, wie das Gerät die MAC-Datenpakete verarbeitet, wenn es die Regel anwendet.

Mögliche Werte:

- `permit` (Voreinstellung)
  Das Gerät vermittelt die MAC-Datenpakete.
- `deny`
  Das Gerät verwirft die MAC-Datenpakete.

Redirection-Port

Legt den Port fest, an den das Gerät die MAC-Datenpakete vermittelt. Voraussetzung ist, dass Sie in Spalte *Aktion* den Wert `permit` festlegen. Das Gerät bietet Ihnen keine Möglichkeit, IP-Datenpakete über VLAN-Grenzen hinweg zu vermitteln.

Mögliche Werte:

- `-` (Voreinstellung)
  Die Funktion *Redirection-Port* ist inaktiv.
- `<Port-Nummer>`
  Das Gerät vermittelt die MAC-Datenpakete an den festgelegten Port.

Mirror-Port

Legt den Port fest, an den das Gerät eine Kopie der MAC-Datenpakete vermittelt. Voraussetzung ist, dass Sie in Spalte *Aktion* den Wert `permit` festlegen. Das Gerät bietet Ihnen keine Möglichkeit, IP-Datenpakete über VLAN-Grenzen hinweg zu vermitteln.

Mögliche Werte:

- `-` (Voreinstellung)
  Die Funktion *Mirror-Port* ist ausgeschaltet.
- `<Port-Nummer>`
  Das Gerät vermittelt eine Kopie der MAC-Datenpakete an den festgelegten Port.

Zugewiesene Queue-ID

Legt die Warteschlangen-ID fest, der das Gerät die MAC-Datenpakete zuweist.

Mögliche Werte:

- `0..7` (Voreinstellung: `0`)

Protokolliere

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog *Diagnose > Bericht > System-Log*.

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiv.
  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 inaktiv.

Das Gerät ermöglicht Ihnen, für bis zu 128 Deny-Regeln diese Funktion zu aktivieren.

Zeitprofil

Legt fest, ob das Gerät die Regel permanent oder zeitgesteuert anwendet.

Mögliche Werte:

- `<leer>` (Voreinstellung)
  Das Gerät wendet die Regel permanent an.
- `[Zeitprofil]`
  Das Gerät wendet die Regel ausschließlich zu den im Zeitprofil festgelegten Zeiten an. Die Zeitprofile bearbeiten Sie im Dialog *Netzsicherheit > ACL > Zeitprofil*.

Lastbegrenzung

Legt das Limit fest für die Datentransferrate auf dem in Spalte *Redirection-Port* festgelegten Port. Das Limit gilt für die Summe aus zu sendenden und empfangenen Daten.

Diese Funktion begrenzt den Datenstrom auf dem Port oder im VLAN:

Mögliche Werte:

- `0` (Voreinstellung)
  Keine Begrenzung der Datentransferrate.
- `1..4294967295`
  Wenn die Datentransferrate auf dem Port den festgelegten Wert überschreitet, verwirft das Gerät überschüssige MAC-Datenpakete. Voraussetzung ist, dass Sie in Spalte *Burst-Size* einen Wert > `0` festlegen. Die Maßeinheit des Limits legen Sie fest in Spalte *Einheit*.

Einheit

Legt die Maßeinheit fest für die in Spalte *Lastbegrenzung* festgelegte Datentransferrate.

Mögliche Werte:

- `kbps`
  kByte pro Sekunde

Burst-Size

Legt das Limit in KByte fest für das Datenvolumen während temporärer Bursts.

Mögliche Werte:

- `0` (Voreinstellung)
  Keine Begrenzung des Datenvolumens.
- `1..128`
  Wenn das Datenvolumen während temporärer Bursts auf dem Port den festgelegten Wert überschreitet, verwirft das Gerät überschüssige MAC-Datenpakete. Voraussetzung ist, dass Sie in Spalte *Lastbegrenzung* einen Wert > `0` festlegen.

Empfehlung:

- Wenn die Bandbreite bekannt ist:
  Burst-Size = Bandbreite × Zugelassene Dauer eines Bursts / 8.
- Wenn die Bandbreite unbekannt ist:
  Burst-Size = 10 × MTU (*Maximum Transmission Unit*) des Ports.

4.9.3 ACL Zuweisung

[Netzsicherheit > ACL > Zuweisung]

Dieser Dialog ermöglicht Ihnen, 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

Das Gerät ermöglicht Ihnen, die Access-Control-Listen auf empfangene (`inbound`) oder zu sendende (`outbound`) Datenpakete anzuwenden.

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 das Management des Geräts ist dann ausschließlich per CLI über die serielle Schnittstelle des Geräts möglich.

Anmerkung: Sie können IP-ACL-Regeln und DiffServ-Regeln für die gleiche Richtung nicht gleichzeitig auf einen Port anwenden.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 18.

Schaltflächen

Hinzufügen

Öffnet den Dialog *Erzeugen*, um einem Port oder einem VLAN eine Regel zuzuweisen.
- Im Feld *Port/VLAN* legen Sie die Nummer des Ports oder die VLAN-ID fest, auf welche das Gerät die Regel anwendet.
- Im Feld *Priorität* legen Sie die Reihenfolge fest, in der das Gerät die Regeln auf den Datenstrom anwendet.
- Im Feld *Richtung* legen Sie fest, ob das Gerät die Regel auf empfangene oder zu sendende Datenpakete anwendet.
- Im Feld *Gruppenname* legen Sie fest, welche Regel das Gerät dem Port oder dem VLAN zuweist.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

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 > MAC-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, ob das Gerät die Access-Control-Liste auf empfangene oder zu sendende Datenpakete anwendet.

Mögliche Werte:

- `inbound`
  Das Gerät wendet die Access-Control-Liste auf Datenpakete an, die es auf dem Port oder im VLAN empfängt.
- `outbound`
  Das Gerät wendet die Access-Control-Liste auf Datenpakete an, die es auf dem Port oder im VLAN sendet.

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. 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.

Mögliche Werte:

- `1..4294967295`

Aktiv

Zeigt, ob die Access-Control-Liste auf dem Port oder im VLAN aktiv ist.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Access-Control-Liste ist aktiv.
- `unmarkiert`
  Die Access-Control-Liste ist inaktiv.

4.9.4 ACL Zeitprofil

[Netzsicherheit > ACL > Zeitprofil]

Dieser Dialog ermöglicht Ihnen das Anlegen und Bearbeiten von Zeitprofilen. Wenn Sie einer ACL-Regel ein Zeitprofil zuweisen, wendet das Gerät die Regel zu den im Zeitprofil festgelegten Zeiten an. Ohne zugewiesenes Zeitprofil wendet das Gerät die Regel permanent an.

Das Gerät ermöglicht Ihnen, bis zu 100 Zeitprofile zu erstellen. Das Gerät wendet die ACL-Regeln während der im Zeitbereich festgelegten Zeit an:

Jedes Zeitprofil kann enthalten:
- Einen *Absolut*-Zeitbereich und bis zu 9 *Periodisch*-Zeitbereiche
  oder
- Bis zu 10 *Periodisch* Zeitbereiche

Die implizite Deny-All-Regel der ACLs gilt stets unabhängig von der Zeitsteuerung.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Anmerkung: Wenn Sie einen bereits eingerichteten Zeitbereich ändern, legen Sie zuerst den Endzeitpunkt und erst danach den Startzeitpunkt neu fest. Andernfalls zeigt der Dialog eine Fehlermeldung.

Schaltflächen

Hinzufügen

Öffnet den Dialog *Erzeugen*, um einen neuen Zeitbereich zu erzeugen.
- Im Feld *Profilname* legen Sie den Namen des Zeitprofils fest, dem der Zeitbereich angehört.
- Im Feld *Typ* legen Sie die Art des Zeitbereichs fest:
  - Mit dem Optionsfeld *Periodisch* legen Sie einen Zeitbereich fest, mit dem das Gerät die Regel wiederkehrend aktiviert.
  - Mit dem Optionsfeld *Absolut* legen Sie einen Zeitbereich fest, mit dem das Gerät die Regel einmalig aktiviert. In jedem Zeitprofil ist genau 1 solcher Zeitbereich erlaubt.
- Im Rahmen *Start* legen Sie den Startzeitpunkt fest, ab dem das Gerät die Regel anwendet.
- Im Rahmen *Ende* legen Sie den Endzeitpunkt fest, bis zu dem das Gerät die Regel anwendet.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

Profilname

Zeigt den Namen des Zeitprofils. Das Zeitprofil enthält die Zeitbereiche.

Betriebszustand

Zeigt, ob der Status des Zeitprofils gegenwärtig *aktiv*/*inaktiv* ist.

Index

Zeigt die Nummer des Zeitbereichs innerhalb des Zeitprofils. Das Gerät legt diese Nummer automatisch fest.

Typ

Zeigt den Typ des Zeitprofils.

Mögliche Werte:

- *Absolut*
  Das Gerät wendet die Regel einmalig an. Weitere Informationen entnehmen Sie den Spalten *Startzeitpunkt* bis *Endzeit*.
- *Periodisch*
  Das Gerät wendet die Regel wiederkehrend an. Weitere Informationen entnehmen Sie den Spalten *Start-Wochentage* bis *Endzeit*.

Startzeitpunkt

Legt das Datum fest, ab dem das Gerät die Regel einmalig anwendet.

Mögliche Werte:

- `JJJJ-MM-TT` oder `TT.MM.JJ`
  (abhängig von den Spracheinstellungen Ihres Web-Browsers)

Startzeit

Legt die Uhrzeit fest, ab der das Gerät die Regel einmalig anwendet.

Mögliche Werte:

- `hh:mm`
  Stunde:Minute

Endzeitpunkt

Legt das Datum fest, bis zu dem das Gerät die Regel einmalig anwendet.

Mögliche Werte:

- `JJJJ-MM-TT` oder `TT.MM.JJ`
  (abhängig von den Spracheinstellungen Ihres Web-Browsers)

Das Gerät ermöglicht Ihnen außerdem Zeitbereiche festzulegen, die sich über mehrere Tage erstrecken. Beispiel:

- *Startzeitpunkt*: *Sa*
- *Startzeit*: `12:00 PM`
- *Endzeitpunkt*: *So*
- *Endzeit*: `11:00 AM`

Endzeit

Legt die Uhrzeit fest, bis zu der das Gerät die Regel einmalig anwendet.

Mögliche Werte:

- `hh:mm`
  Stunde:Minute

Start-Wochentage

Legt die Wochentage fest, an denen das Gerät regelmäßig beginnt, die Regel anzuwenden.

Das Gerät ermöglicht Ihnen, in Spalte *Start-Wochentage* mehrere Werte festzulegen, zum Beispiel eine Liste der Wochentage *Mo*,*Di*,*Mi*,*Do*,*Fr*. Verifizieren Sie in diesem Fall, dass die Felder *Start-Wochentage* und *End-Wochentage* identische Werte enthalten. Das Gerät wendet die Regel dann jeden Wochentag zu den in den Feldern *Startzeit* und *Endzeit* festgelegten Zeiten an.

Mögliche Werte:

- `So`
- `Mo`
- `Di`
- `Mi`
- `Do`
- `Fr`
- `Sa`

Startzeit

Legt die Uhrzeit fest, ab der das Gerät regelmäßig beginnt, die Regel anzuwenden.

Mögliche Werte:

- `hh:mm`
  Stunde:Minute

End-Wochentage

Legt die Wochentage fest, bis zu denen das Gerät die Regel regelmäßig anwendet.

Das Gerät ermöglicht Ihnen, in Spalte *End-Wochentage* mehrere Werte festzulegen, zum Beispiel eine Liste der Wochentage *Mo*,*Di*,*Mi*,*Do*,*Fr*. Verifizieren Sie in diesem Fall, dass die Felder *Start-Wochentage* und *End-Wochentage* identische Werte enthalten. Das Gerät wendet die Regel dann jeden Wochentag zu den in den Feldern *Startzeit* und *Endzeit* festgelegten Zeiten an.

Das Gerät ermöglicht Ihnen außerdem Zeitbereiche festzulegen, die sich über mehrere Tage erstrecken. Verifizieren Sie in diesem Fall, dass die Felder *Start-Wochentage* und *End-Wochentage* jeweils einen einzigen Wert enthalten. Beispiel: *Start-Wochentage*: *Sa*, *Startzeit*: `12:00 PM`, *End-Wochentage*: *So*, *Endzeit*: `11:00 AM`.

Mögliche Werte:

- `So`
- `Mo`
- `Di`
- `Mi`
- `Do`
- `Fr`
- `Sa`

Endzeit

Legt die Uhrzeit fest, bis zu der das Gerät die Regel regelmäßig anwendet.

Mögliche Werte:

- `hh:mm`
  Stunde:Minute

5 Switching

Das Menü enthält die folgenden Dialoge:
- Switching Global
- Lastbegrenzer
- Filter für MAC-Adressen
- IGMP-Snooping
- MRP-IEEE
- GARP
- QoS/Priority
- VLAN
- L2-Redundanz

5.1 Switching Global

[Switching > Global]

Dieser Dialog ermöglicht Ihnen, folgende Einstellungen festzulegen:
- Aging-Time der Adresstabelle ändern
- Flusskontrolle im Gerät einschalten
- VLAN-Unaware-Modus einschalten

Wenn in der Warteschlange eines Ports sehr viele Datenpakete gleichzeitig eintreffen, dann 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 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, dann deaktivieren Sie damit die VLAN-Einstellungen im Gerät. Das Gerät leitet dann die Datenpakete transparent weiter und wertet ausschließlich die im Datenpaket enthaltene Prioritätsinformation aus.

Konfiguration

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*.

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 die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als 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 (IEEE 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 (IEEE 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.

5.2 Lastbegrenzer

[Switching > Lastbegrenzer]

Das Gerät ermöglicht Ihnen, den Datenverkehr an den Ports zu begrenzen, um auch bei hohem Datenverkehr einen stabilen Betrieb zu ermöglichen. Wenn der Verkehr an einem Port den eingegebenen Grenzwert überschreitet, dann verwirft das Gerät die Überlast auf 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.

Der Dialog enthält die folgenden Registerkarten:
- [Eingang]
- [Ausgang]

[Eingang]

In dieser Registerkarte schalten Sie die Funktion *Lastbegrenzer* ein. Der Grenzwert legt fest, welchen maximalen Verkehr der Port eingangsseitig vermittelt. Wenn der Verkehr auf dem Port den Grenzwert überschreitet, dann verwirft das Gerät die Überlast auf diesem Port.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

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 auf diesem Port die Überlast an Broadcast-Datenpaketen.

Broadcast-Grenzwert

Legt den Grenzwert für empfangene Broadcasts auf diesem Port fest.

Mögliche Werte:

- `0..14880000` (Voreinstellung: `0`)
  Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert *`Prozent`* auswählen, dann geben Sie einen Prozentwert zwischen `1` und `100` ein.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert *`pps`* auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

Multicast-Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Multicast-Datenpakete.

Mögliche Werte:

- `markiert`
- `unmarkiert` (Voreinstellung)

Bei Überschreiten des Grenzwerts verwirft das Gerät auf diesem Port die Überlast an Multicast-Datenpaketen.

Multicast-Grenzwert

Legt den Grenzwert für empfangene Multicasts auf diesem Port fest.

Mögliche Werte:

- `0..14880000` (Voreinstellung: `0`)
  Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert *`Prozent`* auswählen, dann geben Sie einen Prozentwert zwischen `0` und `100` ein.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert *`pps`* auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

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 auf diesem Port die Überlast an Unicast-Datenpaketen.

Unicast-Grenzwert

Legt den Grenzwert für empfangene Unicasts mit unbekannter Zieladresse auf diesem Port fest.

Mögliche Werte:

- `0..14880000` (Voreinstellung: `0`)
  Der Wert `0` deaktiviert die Lastbegrenzerfunktion auf diesem Port.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert `Prozent` auswählen, dann geben Sie einen Prozentwert zwischen `0` und `100` ein.
  - Wenn Sie in Spalte *Grenzwert Einheit* den Wert `pps` auswählen, dann geben Sie einen Absolutwert für die Datenrate ein.

[Ausgang]

In dieser Registerkarte legen Sie die Übertragungsrate für den Ausgang des Ports fest.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Bandbreite [%]

Legt die Ausgangs-Übertragungsrate fest.

Mögliche Werte:

- `0` (Voreinstellung)
  Die Bandbreitenbegrenzung ist ausgeschaltet.
- `1..100`
  Die Bandbreitenbegrenzung ist eingeschaltet.
  Der Wert legt die Prozentzahl der Gesamt-Verbindungsgeschwindigkeit für den Port in 1-%-Schritten fest.

5.3 Filter für MAC-Adressen

[Switching > Filter für MAC-Adressen]

Dieser Dialog ermöglicht Ihnen, 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 ermöglicht Ihnen, von Hand weitere Filter einzurichten.

Das Gerät vermittelt die Datenpakete wie folgt:
- Wenn die Tabelle einen Eintrag für die Zieladresse eines Datenpakets enthält, dann vermittelt das Gerät das Datenpaket vom Empfangsport an den im Tabelleneintrag festgelegten Port.
- Existiert kein Tabelleneintrag für die Zieladresse, vermittelt das Gerät das Datenpaket vom Empfangsport an jeden anderen Port.

Tabelle

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

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 festgelegten Ziel-MAC-Adresse.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

MAC-Adresstabelle zurücksetzen

Entfernt aus der Forwarding-Tabelle (FDB) die MAC-Adressen, die in Spalte *Status* den Wert `learned` haben.

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.
- *MRP-MMRP*
  Multicast-Adressfilter automatisch eingerichtet durch MMRP.
- *GMRP*
  Multicast-Adressfilter automatisch eingerichtet durch GMRP.

<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.

5.4 IGMP-Snooping

[Switching > 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 ermöglicht Ihnen, 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, erzeugt das Gerät für diesen Port einen Tabelleneintrag im Dialog *Switching > Filter für MAC-Adressen*. Verlässt der Multicast-Empfänger die Multicast-Gruppe, 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

[Switching > IGMP-Snooping > Global]

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

Funktion

Funktion

Schaltet die Funktion *IGMP-Snooping* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *IGMP-Snooping* ist im Gerät eingeschaltet gemäß RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) und Multicast Listener Discovery (MLD) Snooping Switches).
- `Aus` (Voreinstellung)
  Die Funktion *IGMP-Snooping* 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

Schaltflächen

IGMP-Snooping-Zähler zurücksetzen

Entfernt die IGMP-Snooping-Einträge und setzt den Zähler im Rahmen *Information* auf `0`.

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 Kommando `clear igmp-snooping` im Command Line Interface setzen Sie die IGMP-Snooping-Einträge zurück, inklusive des Zählers für die verarbeiteten Multicast-Kontroll-Datenpakete.

5.4.2 IGMP-Snooping Konfiguration

[Switching > IGMP-Snooping > Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Funktion *IGMP-Snooping* 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 Funktion *IGMP-Snooping* für jedes VLAN.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

VLAN-ID

Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

Aktiv

Aktiviert/deaktiviert die Funktion *IGMP-Snooping* für dieses VLAN.

Voraussetzung ist, dass die Funktion *IGMP-Snooping* 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`
  Wenn die Fast-Leave-Funktion eingeschaltet ist und das Gerät eine IGMP-Leave-Nachricht aus einer Multicast-Gruppe erhält, entfernt es 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 auf 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`)

[Port]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *IGMP-Snooping* auf dem Port.

Voraussetzung ist, dass die Funktion *IGMP-Snooping* global aktiviert ist.

Mögliche Werte:

- `markiert`
  IGMP-Snooping ist auf diesem Port eingeschaltet. Der Port ist für den 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 auf 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 auf dem Port.

Mögliche Werte:

- `markiert`
  Wenn die Fast-Leave-Funktion eingeschaltet ist und das Gerät eine IGMP-Leave-Nachricht aus einer Multicast-Gruppe erhält, entfernt es 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 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.
  Wenn Sie die Funktion *Redundant Coupling Protocol* verwenden und das Gerät als Slave arbeitet, dann verwenden Sie nicht den *Static-Query-Port*-Modus für die Ports am sekundären Ring/Netz.
- `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.

VLAN-IDs

Zeigt die ID der VLANs, für die der Tabelleneintrag gilt.

5.4.3 IGMP-Snooping Erweiterungen

[Switching > IGMP-Snooping > Snooping Erweiterungen]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Wizard

Öffnet das Fenster *Wizard*, das Sie beim Auswählen und Einrichten der Ports unterstützt. Siehe „[Wizard: IGMP-Snooping-Erweiterungen]" auf Seite 247.

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, führen Sie die folgenden Schritte aus:
  - ☐ Öffnen Sie das Fenster *Wizard*.
  - ☐ Markieren Sie im Dialog *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, führen Sie die folgenden Schritte aus:
  - Öffnen Sie das Fenster *Wizard*.
  - Markieren Sie im Dialog *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, führen Sie die folgenden Schritte aus:
  - Öffnen Sie das Fenster *Wizard*.
  - Markieren Sie im Dialog *Konfiguration* das Kontrollkästchen `Forward all`.

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 “`-`“.
- `Learned by LLDP (P)`
  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 “`-`“.

[Wizard: IGMP-Snooping-Erweiterungen]

Das Fenster *Wizard* unterstützt Sie beim Auswählen und Konfigurieren der Ports.

Das Fenster *Wizard* führt Sie durch die folgenden Schritte:
- Selection VLAN/Port
- Konfiguration

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

Selection VLAN/Port

VLAN-ID

Auswahl der ID des VLANs.

Port

Auswahl der Ports.

Konfiguration

VLAN-ID

Zeigt die ID des ausgewählten VLANs.

Port

Zeigt die Nummer der 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. Dies ermöglicht Ihnen, 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 dem Gerät, direkt verbundene Hirschmann-Geräte mit LLDP zu erkennen und die betreffenden Ports als Query-Port 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

[Switching > IGMP-Snooping > Querier]

Das Gerät ermöglicht Ihnen, 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 ermöglicht Ihnen, die Snooping-Querier-Einstellungen global und für die eingerichteten VLANs zu konfigurieren.

Funktion

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.

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.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

VLAN-ID

Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

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 vermeiden, 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.

5.4.5 IGMP Snooping Multicasts

[Switching > IGMP-Snooping > Multicasts]

Das Gerät ermöglicht Ihnen, 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.

Das Gerät ermöglicht Ihnen außerdem, die Datenpakete bekannter Multicast-Adressen an die Query-Ports zu vermitteln.

Konfiguration

Unbekannte Multicasts

Legt fest, wie das Gerät die Datenpakete unbekannter Multicast-Adressen vermittelt.

Mögliche Werte:

- `discard`
  Das Gerät verwirft Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse.
- `flood` (Voreinstellung)
  Das Gerät vermittelt Datenpakete mit unbekannter MAC-/IP-Multicast-Adresse an jeden Port.
- `query ports`
  Das Gerät vermittelt 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.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 vermittelt Datenpakete mit einer bekannten MAC-/IP-Multicast-Adresse an die Query-Ports und an registrierte Ports.
- `an registrierte Ports senden` (Voreinstellung)
  Das Gerät vermittelt Datenpakete mit einer bekannten MAC-/IP-Multicast-Adresse an registrierte Ports.

5.5 MRP-IEEE

[Switching > 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 ermöglicht Ihnen, 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

[Switching > MRP-IEEE > Konfiguration]

Dieser Dialog ermöglicht Ihnen, 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 aufrecht, 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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`)

5.5.2 MRP-IEEE Multiple MAC Registration Protocol

[Switching > MRP-IEEE > MMRP]

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 ermöglicht Ihnen, 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 ermöglicht Ihnen außerdem, 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

Funktion

Aktiviert/deaktiviert die globale Funktion *MMRP* des Geräts. 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

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an MMRP.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Bei global und auf diesem Port eingeschaltetem MMRP sendet und empfängt das Gerät MMRP-Nachrichten auf 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`
  Wenn die Funktion eingeschaltet ist und im VLAN ein statischer Filtereintrag für die MAC-Adresse vorhanden ist, ermöglicht das Gerät, die MAC-Adressattribute dynamisch zu registrieren.
- `unmarkiert` (Voreinstellung)
  Aktiviert/deaktiviert die Begrenzung der dynamischen Registrierung von MAC-Adressen mittels MMRP an dem Port.

[Service-Requirement]

Diese Registerkarte enthält für jedes aktive VLAN Weiterleitungsparameter die festlegen, für welche Ports die Multicast-Weiterleitung zutrifft. Das Gerät ermöglicht Ihnen, 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 Command Line Interface fest.

Ein Port ist ausschließlich als ForwardAll oder Forbidden eingerichtet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 auf dem 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 auf dem Port fest. Das Gerät blockiert die dynamischen MMRP-Service-Requirements für ForwardAll. Bei auf diesem Port in diesem VLAN blockierten ForwardAll-Anfragen blockiert das Gerät auf diesem Port auch Daten, die an MMRP-registrierte Multicast-MAC-Adressen gerichtet sind. Außerdem blockiert das Gerät MMRP-Service-Anfragen, diesen Wert auf diesem Port zu ändern.
- - (Voreinstellung)
  Schaltet auf diesem Port die Weiterleitungsfunktionen aus.
- Learned
  Zeigt die durch MMRP-Service-Anfragen eingesetzten Werte.

[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 ermöglicht Ihnen, die Statistiken des MMRP-Verkehrs für jeden Port zu überwachen.

Information

Schaltflächen

Statistiken zurücksetzen

Setzt die Zähler der Port-Statistiken und die Werte in Spalte *Letzte empfangene MAC-Adresse* zurück.

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

5.5.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

Das Multiple VLAN Registration Protocol (MVRP) besitzt einen Mechanismus, der Ihnen 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

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

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an MVRP.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Bei global und auf 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.

Restricted VLAN registration

Aktiviert/deaktiviert die Funktion *Restricted VLAN registration* auf diesem Port.

Mögliche Werte:

- `markiert`
  Bei eingeschalteter Funktion und vorhandenem statischem VLAN-Registrierungseintrag ermöglicht Ihnen das Gerät, ein dynamisches VLAN für diesen Eintrag zu erzeugen.
- `unmarkiert` (Voreinstellung)
  Schaltet die Funktion *Restricted VLAN registration* auf diesem Port aus.

[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 ermöglicht Ihnen, die Statistiken des MVRP-Verkehrs zu überwachen.

Information

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 18.

Schaltflächen

Statistiken zurücksetzen

Setzt die Zähler der Port-Statistiken und die Werte in Spalte *Letzte empfangene MAC-Adresse* zurück.

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 auf dem Port empfangenen MVRPDUs mit fehlerhaftem Header.

Empfangene Bad-Format-PDU

Zeigt die Anzahl der vom Gerät auf dem Port blockierten MVRPDUs mit fehlerhaftem Datenfeld.

Senden fehlgeschlagen

Zeigt die Anzahl der vom Gerät auf dem Port blockierten MVRPDUs.

Registrierungen fehlgeschlagen

Zeigt die Anzahl der auf dem Port fehlgeschlagenen Registrierungsversuche.

Letzte empfangene MAC-Adresse

Zeigt die letzte MAC-Adresse, von welcher der Port MVRPDUs empfangen hat.

5.6 GARP

[Switching > 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 Geräte im Netz. 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 dem Einschalten der Funktion *GMRP*, dass die Funktion *MMRP* ausgeschaltet ist.

Das Menü enthält die folgenden Dialoge:
- GMRP
- GVRP

5.6.1 GMRP

[Switching > GARP > GMRP]

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

GMRP und GARP sind durch IEEE 802.1P definierte Industriestandardprotokolle.

Funktion

Funktion

Aktiviert/deaktiviert die globale Funktion *GMRP* 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

Unbekannte Multicasts

Aktiviert/deaktiviert die unbekannten Multicast-Daten, die entweder geflutet oder verworfen werden sollen.

Mögliche Werte:

- `discard`
  Das Gerät verwirft unbekannte Multicast-Daten.
- `flood` (Voreinstellung)
  Das Gerät vermittelt unbekannte Multicast-Daten an jeden Port.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

GMRP aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an *GMRP*.

Voraussetzung ist, dass die Funktion *GMRP* global aktiviert ist.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Teilnahme des Ports an *GMRP* ist aktiv.
- `unmarkiert`
  Die Teilnahme des Ports an *GMRP* ist inaktiv.

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.

5.6.2 GVRP

[Switching > GARP > 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 ermöglicht Ihnen außerdem, die über 802.1Q-Trunk-Ports verbundenen VLANs dynamisch zu erzeugen und zu verwalten.

Funktion

Funktion

Aktiviert/deaktiviert die Funktion *GVRP* global im Gerät. Das Gerät nimmt am Austausch von *GVRP*-Nachrichten teil. Wenn die Funktion deaktiviert ist, dann ignoriert das Gerät *GVRP*-Nachrichten.

Mögliche Werte:

- `An`
  Die Funktion *GVRP* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *GVRP* ist ausgeschaltet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

GVRP aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an *GVRP*.

Voraussetzung ist, dass die Funktion *GVRP* global aktiviert ist.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Teilnahme des Ports an *GVRP* ist aktiv.
- `unmarkiert`
  Die Teilnahme des Ports an *GVRP* ist inaktiv.

5.7 QoS/Priority

[Switching > QoS/Priority]

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, wesentlichen Anwendungen eine Mindestbandbreite 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: Wenn Sie die Funktionen in diesem Menü nutzen, dann schalten Sie die Flusskontrolle aus. Die Flusskontrolle ist ausgeschaltet, wenn im Dialog *Switching > Global*, Rahmen *Konfiguration*, das Kontrollkästchen *Flusskontrolle* unmarkiert ist.

Das Menü enthält die folgenden Dialoge:
- QoS/Priority Global
- QoS/Priorität Port-Konfiguration
- 802.1D/p Zuweisung
- IP-DSCP-Zuweisung
- Queue-Management
- DiffServ

5.7.1 QoS/Priority Global

[Switching > QoS/Priority > Global]

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

Konfiguration

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/Priority > 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/Priority > 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 8 Warteschlangen pro Port. Jede Warteschlange ist einer bestimmten *Verkehrsklasse* zugewiesen (*Verkehrsklasse* nach IEEE 802.1D).

5.7.2 QoS/Priorität Port-Konfiguration

[Switching > QoS/Priority > Port-Konfiguration]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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/Priority > 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/Priority > 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/Priority > 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/Priority > 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/Priority > 802.1D/p Zuweisung* weisen Sie jeder VLAN-Priorität eine *Verkehrsklasse* zu.

Mögliche Werte:

- `0..7`

5.7.3 802.1D/p Zuweisung

[Switching > QoS/Priority > 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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*.

Werksseitige Zuweisung der VLAN-Priorität zu Verkehrsklassen

VLAN-Priorität	*Verkehrsklasse*	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` Zeitkritische Daten mit hoher Priorität

VLAN-Priorität	*Verkehrsklasse*	Inhaltskennzeichnung gemäß IEEE 802.1D
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

[Switching > QoS/Priority > 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

DSCP Wert

Zeigt den DSCP-Wert.

Traffic-Klasse

Legt die *Verkehrsklasse* fest, die dem DSCP-Wert zugewiesen ist.

Mögliche Werte:

- 0..7
  0ist der Warteschlange mit der niedrigsten Priorität zugewiesen.
  7ist der Warteschlange mit der höchsten Priorität zugewiesen.

Werksseitige Zuweisung der DSCP-Werte zu Verkehrsklassen

DSCP-Wert	DSCP-Name	*Verkehrsklasse*
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

DSCP-Wert	DSCP-Name	*Verkehrsklasse*
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.7.5 Queue-Management

[Switching > QoS/Priority > Queue-Management]

Dieser Dialog ermöglicht Ihnen, 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.

Außerdem haben Sie die Möglichkeit, jeder *Verkehrsklasse* eine Mindestbandbreite zuzuweisen, mit der das Gerät die Warteschlangen mit *Weighted Fair Queuing* abarbeitet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 vermittelt 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 nächstniedrigeren Priorität befinden.
  - Datenpakete mit niedriger *Verkehrsklasse* vermittelt der Port erst, wenn die Warteschlangen mit höherer Priorität leer sind. In ungünstigen Fällen sendet der Port diese Datenpakete nicht.
  - Wenn Sie diese Einstellung für eine *Verkehrsklasse* festlegen, schaltet das Gerät die Funktion auch bei *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 *Verkehrsklassen* mit niedrigerer 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 %.

Max. Bandbreite [%]

Legt die Shaping-Rate fest, mit der eine *Verkehrsklasse* Pakete vermittelt (Queue-Shaping).

Mögliche Werte:

▶ `0` (Voreinstellung)
Das Gerät reserviert für diese *Verkehrsklasse* keine Bandbreite.

▶ `1..100`
Das Gerät reserviert für diese *Verkehrsklasse* die festgelegte Bandbreite. Der festgelegte Wert in Prozent bezieht sich auf die maximal verfügbare Bandbreite auf dem Port.

Queue-Shaping ermöglicht Ihnen zum Beispiel, die Rate einer hochprioren Warteschlange zu beschränken. Die Beschränkung einer hochprioren Warteschlange ermöglicht dem Gerät außerdem, niederpriore Warteschlangen abzuarbeiten. Um Queue-Shaping zu verwenden, legen Sie die maximale Bandbreite für eine bestimmte Warteschlange fest.

5.7.6 DiffServ

[Switching > QoS/Priority > DiffServ]

Differentiated Services (DiffServ) filtern Datenpakete, um den Datenstrom zu priorisieren oder zu begrenzen.

- In einer Klasse legen Sie die Filterkriterien fest.
- In einer Richtlinie verknüpfen Sie die Klasse mit Aktionen.

Das Gerät wendet die Aktionen der Richtlinie auf diejenigen Datenpakete an, die die Filterkriterien der zugewiesenen Klasse erfüllen.

Um DiffServ einzurichten, führen Sie die folgenden Schritte aus:

☐ Erzeugen Sie eine Klasse mit den Filterkriterien.
☐ Erzeugen Sie eine Richtlinie (Policy).
☐ Weisen Sie der Richtlinie eine Klasse mit den Filterkriterien zu.
☐ Legen Sie die Aktionen der Richtlinie fest.
☐ Weisen Sie die Richtlinie einem Port zu.
☐ Schalten Sie die DiffServ-Funktion ein.

Das Gerät ermöglicht Ihnen, die folgenden Konfigurationen pro Klasse und Instanz zu verwenden:

▶ 13 Regeln pro Klasse
▶ 28 Instanzen pro Richtlinie
▶ 3 Attribute pro Instanz

Das Menü enthält die folgenden Dialoge:

- DiffServ Übersicht
- DiffServ Global
- DiffServ Klasse
- DiffServ Richtlinie
- DiffServ Zuweisung

5.7.6.1 DiffServ Übersicht

[Switching > QoS/Priority > DiffServ > Übersicht]

Dieser Dialog zeigt die im Gerät verwendeten DiffServ-Einstellungen.

Übersicht

Die oberste Ebene zeigt:

- Die Ports, für die jemand eine DiffServ-Richtlinie eingerichtet hat.
- Die Richtung der Datenpakete, auf welche die DiffServ-Richtlinie wirkt.

Die untergeordneten Ebenen zeigen:

- Die Zeichenfolge für *Policy-Name* und die Nummer für *Policy index*.
- Die Nummer für *Policy instance*.
- Die Zeichenfolge für *Name der Klasse* und den Namen für *Protokoll*.
- Die in der DiffServ-Klasse festgelegten Einstellungen.

Schaltflächen

Zeigt ein Textfeld, um nach einem Schlüsselwort zu suchen. Wenn Sie ein Zeichen oder eine Zeichenkette einfügen, zeigt die Übersicht ausschließlich Einträge, die mit diesem Schlüsselwort in Zusammenhang stehen.

Klappt die Ebenen zu. Die Übersicht zeigt dann ausschließlich die erste Ebene der Einträge.

Klappt die Ebenen auf. Die Übersicht zeigt dann jede Ebene der Einträge.

Klappt den aktuellen Eintrag auf und zeigt die Einträge der nächsttieferen Ebene.

Klappt den Eintrag zu und blendet die Einträge der darunter liegenden Ebenen aus.

Port

Port

Vereinfacht die Tabelle und zeigt die Einträge zu einem bestimmten Port. Diese Darstellung erleichtert Ihnen, die Tabelle nach Ihren Wünschen zu sortieren.

Mögliche Werte:

- *Alle* (Voreinstellung)
  Die Tabelle zeigt die Einträge für jeden Port.
- <Port-Nummer>
  Die Tabelle zeigt die Einträge für den ausgewählten Port.

5.7.6.2 DiffServ Global

[Switching > QoS/Priority > DiffServ > Global]

In diesem Dialog schalten Sie die DiffServ-Funktion ein.

Funktion

Funktion

Schaltet die Funktion *DiffServ* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *DiffServ* ist eingeschaltet.
  Das Gerät verarbeitet die Datenpakete gemäß den DiffServ-Regeln.
- `Aus` (Voreinstellung)
  Die Funktion *DiffServ* ist ausgeschaltet.

5.7.6.3 DiffServ Klasse

[Switching > QoS/Priority > DiffServ > Klasse]

In diesem Dialog legen Sie fest, auf welche Datenpakete das Gerät die im Dialog *Richtlinie* festgelegten Aktionen ausführt. Diese Zuweisung heißt Klasse.

Einer Richtlinie (Policy) kann immer nur eine Klasse zugewiesen sein. Deshalb kann jede Klasse mehrere Filterkriterien enthalten.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Erzeugen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen. Siehe „[Fenster Erzeugen]" auf Seite 281.

Name der Klasse

Legt den Namen der DiffServ-Klasse fest. Das Gerät ermöglicht Ihnen, den Namen der Klasse direkt in der Tabelle zu ändern.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..31 Zeichen

Kriterium

Zeigt die festgelegten Kriterien für diese Regel.

[Fenster Erzeugen]

Name der Klasse

Legt den Namen der DiffServ-Klasse fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..31 Zeichen

Typ

Legt den Typ der Klassenregel für die Filterung fest und bestimmt die individuellen Filterbedingungen für diese Klassenregel.

Abhängig davon, welchen Wert Sie wählen, ändern sich die folgenden, sichtbaren Parameter.

Um jedes Paket unabhängig vom Inhalt zu filtern, wählen Sie den Wert `every`.

Mögliche Werte:

- `cos` (Voreinstellung)
- `dstip`
- `dstl4port`
- `dstmac`
- `every`
- `ipdscp`
- `ipprecedence`
- `iptos`
- `protocol`
- `refclass`
- `srcip`
- `srcl4port`
- `srcmac`
- `cos2`
- `etype`
- `vlanid`
- `vlanid2`

Typ = `cos`

COS

Legt die Serviceklasse (CoS) als Filterwert für die Klasse fest.

Mögliche Werte:

- `0..7` (Voreinstellung: `0`)

Typ = `dstip`

Ziel-IP-Adresse

Legt die Ziel-IP-Adresse als Filterwert für die Klasse fest.

Mögliche Werte:

- Gültige IP-Adresse

Ziel-IP-Adressmaske

Legt die Maske für die Ziel-IP-Adresse fest.

Mögliche Werte:

- Gültige Netzmaske

Typ = `dstl4port`

Ziel-Port

Legt den Ziel-Port auf Schicht 4 als Filterwert für die Klasse fest.

Mögliche Werte:

- Gültige TCP- oder UDP-Port-Nummer

Typ = `dstmac`

Ziel-MAC-Adresse

Legt die Ziel-MAC-Adresse als Filterwert für die Klasse fest.

Mögliche Werte:

- Gültige MAC-Adresse

Ziel-MAC-Adressmaske

Legt die Maske für die Ziel-MAC-Adresse fest.

Mögliche Werte:

- Gültige Netzmaske

Typ = `ipdscp`

DSCP

Legt den DiffServ-Code-Point (DSCP) als Filterwert für die Klasse fest.

Mögliche Werte:

- `0..63` (Voreinstellung: `0(be/cs0)`)

Typ = `ipprecedence`

TOS-Priorität

Legt die IP-Precedence als Filterwert für die Klasse fest. Die Precedence-Bits sind die höherwertigen 3 Bits des Service-Typ-Oktetts im IPv4-Header.

Mögliche Werte:

- `0..7` (Voreinstellung: `0`)

Typ = `iptos`

TOS-Maske

Legt die IP-TOS-Bits und Maske als Filterwert für die Klasse fest. Die TOS-Bits sind die 8 Bits des Service-Typ-Oktetts im IPv4-Header.

Mögliche Werte:

- `0x00..0xFF`

Typ = `protocol`

Protocol number

Legt den Wert des Protocol-Felds im IPv4-Header als Filterwert für die Klasse fest.

Mögliche Werte:

- `0..255`
  Einige übliche Werte sind:
  - `1`
    ICMP
  - `2`
    IGMP
  - `4`
    IPv4 (Verkapselung von IPv4 in IPv4)
  - `6`
    TCP
  - `17`
    UDP
  - `41`
    IPv6 (Verkapselung von IPv6 in IPv4)
  - `255`
    Eine Regel mit diesem Wert filtert jedes Protokoll in der Liste.

Die IANA definierte die hier einzugebenden Internet-Protokoll-Nummern als „Assigned Internet Protocol Numbers“.

Eine Liste mit den zugewiesenen Nummern finden Sie unter folgendem Link: www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml.

Typ = `refclass`

Ref class

Legt die übergeordnete Klasse als zugehörige Referenzklasse fest. Diese Referenzklasse verwendet das Filterregel-Set, das Sie in einer übergeordneten Klasse als Filterwert festgelegt haben.

Mögliche Werte:

- `<Name der DiffServ-Klasse>`

Bedingungen:

- Wenn sich die Referenzklasse ausschließlich auf die übergeordnete Klasse bezieht, dann liefern die übergeordnete Klasse, an die Sie diese Regel binden, und die Referenzklasse die gleichen Ergebnisse.
- Das Löschen der übergeordneten Klasse ist ausgeschlossen, so lange eine andere Klasse auf sie verweist.
- Eine nachträgliche Änderung der Regeln für die übergeordnete Klasse verändert die Regeln für die Referenzklasse ausschließlich dann, wenn die Referenzklasse als Filterwert die übergeordnete Klasse verwendet.
- Sie fügen weitere Regeln, die mit den in der Referenzklasse vorhandenen Regeln kompatibel sind, zur übergeordneten Klasse hinzu.

Typ = `srcip`

Quell-IP-Adresse

Legt die Quell-IP-Adresse als Filterwert für die Klasse fest.

Mögliche Werte:

- Gültige IP-Adresse

Quell-IP-Adressmaske

Legt die Maske für die Quell-IP-Adresse fest.

Mögliche Werte:

- Gültige Netzmaske

Typ = `srcl4port`

Quell-Port

Legt den Quell-Port auf Schicht 4 als Filterwert für die Klasse fest.

Mögliche Werte:

- Gültige TCP- oder UDP-Port-Nummer

Typ = `srcmac`

Quell-MAC-Adresse

Legt die Quell-MAC-Adresse als Filterwert für die Klasse fest.

Mögliche Werte:

- Gültige MAC-Adresse und Maske

Quell-MAC-Adressmaske

Legt die Maske für die Quell-MAC-Adresse fest.

Mögliche Werte:

- Gültige Netzmaske

Typ = `cos2`

COS 2

Legt eine sekundäre Serviceklasse (Cos) als Filterwert für die Klasse fest.

Mögliche Werte:

- `0..7` (Voreinstellung: `0`)

Typ = `etype`

Etype

Legt den Ethertype als Filterwert für die Klasse fest.

Mögliche Werte:

- `custom` (Voreinstellung)
  Den Ethertype legen Sie fest im Feld *Etype value*.
- `appletalk`
- `arp`
- `ibmsna`
- `ipv4`
- `ipv6`
- `ipx`
- `mplsmcast`
- `mplsucast`
- `netbios`
- `novell`
- `pppoe`
- `rarp`

Etype value

Legt den benutzerdefinierten Ethertype-Wert fest.

Voraussetzung ist, dass Sie im Feld *Etype* den Wert `custom` festlegen.

Mögliche Werte:

- `0x0600..0xFFFF`

Typ = `vlanid`

VLAN-ID

Legt die VLAN-ID als Filterwert für die Klasse fest.

Mögliche Werte:

- `1..4042`

Typ = `vlanid2`

VLAN2-ID

Legt die sekundäre VLAN-ID als Filterwert für die Klasse fest.

Mögliche Werte:

- `1..4042`

5.7.6.4 DiffServ Richtlinie

[Switching > QoS/Priority > DiffServ > Richtlinie]

In diesem Dialog legen Sie fest, welche Aktionen das Gerät auf Datenpakete ausführt, welche die im Dialog *Klasse* festgelegten Filterkriterien erfüllen. Diese Zuweisung heißt Richtlinie (Policy).

Einem Port kann immer nur eine Richtlinie (Policy) zugewiesen sein. Jede Richtlinie (Policy) kann mehrere Aktionen enthalten.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Erzeugen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen. Siehe „[Fenster Erzeugen]" auf Seite 289.

Attribut modifizieren

Öffnet das Fenster *Attribut modifizieren*, um die Aktion festzulegen, die das Gerät auf die Datenpakete ausführt. Voraussetzung ist, dass Sie einen Tabelleneintrag auswählen, der in Spalte *Attribut* einen Wert enthält.

Policy-Name

Zeigt den Namen der Richtlinie.

Um den Wert zu ändern, klicken Sie in das betreffende Feld.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..31 Zeichen

Richtung

Zeigt, auf welche Datenpakete (empfangene oder zu sendende) das Gerät die Richtlinie anwendet.

Mögliche Werte:

- `in`
  Das Gerät wendet die Richtlinie auf Datenpakete an, die es empfängt.
- `out`
  Das Gerät wendet die Richtlinie auf Datenpakete an, die es sendet.

Name der Klasse

Zeigt den Namen der Klasse, die der Richtlinie zugewiesen ist.

In der Klasse sind die Filterkriterien festgelegt.

Attribut

Zeigt die Aktion, die das Gerät auf die Datenpakete ausführt.

- Um eine vorhandene Aktion zu ändern, markieren Sie die betreffende Zeile und klicken die Schaltfläche .
- Um einer Richtlinie weitere Aktionen hinzuzufügen, klicken Sie die Schaltfläche .

[Fenster Erzeugen]

In diesem Dialog erzeugen Sie eine neue Richtlinie oder fügen einer bestehenden Richtlinie weitere Aktionen hinzu.

Policy-Name

Legt den Namen der Richtlinie fest.

- Um eine neue Richtlinie zu erzeugen, fügen Sie einen neuen Namen ein.
- Um einer vorhandenen Richtlinie weitere Aktionen hinzuzufügen, wählen Sie in der Liste einen Namen aus.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..31 Zeichen

Richtung

Legt fest, auf welche Datenpakete (empfangene oder zu sendende) das Gerät die Richtlinie anwendet.

Mögliche Werte:

- `in` (Voreinstellung)
  Das Gerät wendet die Richtlinie auf Datenpakete an, die es empfängt.
- `out`
  Das Gerät wendet die Richtlinie auf Datenpakete an, die es sendet.

Name der Klasse

Weist der Richtlinie die Klasse zu.

In der Klasse sind die Filterkriterien festgelegt.

Typ

Legt den Policy-Typ fest.

Abhängig davon, welchen Wert Sie wählen, ändern sich die folgenden, sichtbaren Parameter.

Mögliche Werte:

- `markCosVal` (Voreinstellung)
- `markIpDscpVal`
- `markIpPrecedenceVal`
- `policeSimple`
- `policeTworate`

- *assignQueue*
- *drop*
- *redirect*
- *mirror*
- *markCosAsSecCos*

Typ = `markCosVal`

Überschreibt das Prioritätsfeld im VLAN-Tag der Ethernet-Pakete:

- Das Gerät schreibt den im Parameter *COS* festgelegten Prioritätswert in den VLAN-Tag.
- Bei QinQ-markierten (IEEE 802.1ad) Ethernet-Paketen schreibt das Gerät den Wert in das äußere Tag (*Service-Tag* oder *S-Tag*).
- Bei Datenpaketen ohne VLAN-Tag fügt das Gerät ein Priority-Tag ein.

Kombinierbar mit *Typ* = `redirect` und `mirror`.

COS

Legt den Prioritätswert fest, den das Gerät in das Prioritätsfeld des VLAN-Tags der Ethernet-Pakete schreibt.

Mögliche Werte:

▶ `0..7`

Typ = `markIpDscpVal`

Überschreibt das DS-Feld der IP-Pakete.

Das Gerät schreibt den im Parameter *DSCP* festgelegten Wert in das DS-Feld. Nachfolgende Geräte im Netz, an die das Gerät die IP-Pakete weiterleitet, priorisieren die IP-Pakete gemäß dieser Einstellung. Damit bereits dieses Gerät die IP-Pakete priorisiert, reihen Sie die IP-Pakete zusätzlich mit *Typ* = `assignQueue` in die gewünschte Sende-Warteschlange ein.

Kombinierbar mit *Typ* = `assignQueue`, `redirect` und `mirror`.

DSCP

Legt den Wert fest, den das Gerät in das DS-Feld der IP-Pakete schreibt.

Mögliche Werte:

▶ `0..63`

Typ = `markIpPrecedenceVal`

Überschreibt das TOS-Feld der IP-Pakete.

Das Gerät schreibt den im Parameter *TOS-Priorität* festgelegten Wert in das TOS-Feld.

Kombinierbar mit *Typ* = `assignQueue`, `redirect` und `mirror`.

TOS-Priorität

Legt den Wert fest, den das Gerät in das TOS-Feld der IP-Pakete schreibt.

Mögliche Werte:

▶ `0..7`

Typ = `policeSimple`

Begrenzt den klassifizierten Datenstrom auf die in den Feldern *Simple C Rate* und *Simple C Burst* festgelegten Werte:

- Wenn Transferrate und Burst-Größe des Datenstroms unterhalb der festgelegten Werte liegen, dann wendet das Gerät die im Feld *Conform Action* festgelegte Aktion an.
- Wenn Transferrate und Burst-Größe des Datenstroms oberhalb der festgelegten Werte liegen, dann wendet das Gerät die im Feld *Non Conform Action* festgelegte Aktion an.

Kombinierbar mit *Typ* = `assignQueue`, `redirect` und `mirror`.

Simple C Rate

Legt die Committed Rate in kbit/s fest.

Obergrenze des

Mögliche Werte:

▶ `1..4294967295`

Simple C Burst

Legt die Committed Burst Size in kByte fest.

Mögliche Werte:

▶ `0..128`

Conform Action, Non Conform Action

Im Feld *Conform Action* legen Sie die Aktion fest, die das Gerät auf den konformen Datenstrom anwendet. Konform bedeutet, dass sich der Datenstrom unterhalb der in den Parametern *Simple C Rate* und *Simple C Burst*festgelegten Grenzen bewegt.

Im Feld *Non Conform Action*legen Sie die Aktion fest, die das Gerät auf den nicht-konformen Datenstrom anwendet. Nicht-konform bedeutet, dass sich der Datenstrom oberhalb der in den Parametern *Simple C Rate* und *Simple C Burst*festgelegten Grenzen bewegt.

Mögliche Werte:

▶ `drop`
Verwirft die Datenpakete.

▶ `markDscp`
Überschreibt das DS-Feld der IP-Pakete.
Das Gerät schreibt den im nebenstehenden Feld festgelegten Wert [`0..63`] in das das DS-Feld.

▶ `markPrec`
Überschreibt das TOS-Feld der IP-Pakete.
Das Gerät schreibt den im nebenstehenden Feld festgelegten Wert [`0..7`] in das TOS-Feld.

▶ `send`
Vermittelt die Datenpakete.

▶ `markCos`
Überschreibt das Prioritätsfeld im VLAN-Tag der Ethernet-Pakete:
- Das Gerät schreibt den im Parameter *COS* festgelegten Prioritätswert in den VLAN-Tag.
- Bei QinQ-markierten (IEEE 802.1ad) Ethernet-Paketen schreibt das Gerät den Wert in das äußere Tag (*Service-Tag* oder *S-Tag*).
- Bei Ethernet-Paketen ohne VLAN-Tag fügt das Gerät ein Priority-Tag ein.

- `markCos2`
  Überschreibt bei QinQ-markierten Ethernet-Paketen das Prioritätsfeld im inneren Tag (*Customer-Tag* oder *C-Tag*) mit dem im nebenstehenden Feld festgelegten Wert [`0..7`].
- `markCosAsSecCos`
  Überschreibt das Prioritätsfeld im äußeren Tag (*Service-Tag* or *S-Tag*) mit dem Prioritätswert des inneren Tags (*C-Tag*).

Color Conform Class

Legt die Klasse des empfangenen Datenstroms fest, die das Gerät als konform (grün) betrachtet.

Mögliche Werte:

- `blind`
  Das Gerät arbeitet im Color-Blind-Modus. Das Gerät betrachtet den gesamten empfangenen Datenstrom als konform (grün).
- `<Name der DiffServ-Klasse>`
  Das Gerät betrachtet ausschließlich diese Klasse des empfangenen Datenstroms als konform (grün).
  Auswählbar sind Klassen, für die im Dialog *Switching > QoS/Priority > DiffServ > Klasse*, Spalte *Kriterium* eine Regel des Typs `cos`, `ipdscp`, `ipprec`, `cos2` festgelegt ist.

Vergewissern Sie sich, dass die Filterkriterien der oben in der Dropdown-Liste *Name der Klasse* ausgewählten Klasse und der in dieser Dropdown-Liste ausgewählten Klasse weder identisch sind noch sich einander ausschließen. Ausschlusskriterien sind:

- Die Filterkriterien haben denselben Regel-Typ, zum Beispiel `cos` und `cos`. Verwenden Sie Klassen mit unterschiedlichem Regel-Typ, zum Beispiel `cos` und `ipdscp`.
- Eine der Klassen referenziert mit dem Regel-Typ `refclass` eine weitere Klasse, die den verwendeten Klassen widerspricht.

Typ = `policeTworate`

Begrenzt den klassifizierten Datenstrom auf die in den Feldern *Two Rate C Rate*, *Two Rate C Burst*, *Two Rate P Rate* und *Two Rate P Burst* festgelegten Werte:

- Wenn Transferrate und Burst-Größe des Datenstroms unterhalb von *Two Rate C Rate* und *Two Rate C Burst* liegen, dann wendet das Gerät die Aktion *Conform Action* an.
- Wenn Transferrate und Burst-Größe zwischen *Two Rate C Rate* und *Two Rate P Rate* sowie *Two Rate C Burst* und *Two Rate P Burst* liegen, dann wendet das Gerät die Aktion *Exceed Action* auf den Datenstrom an.
- Wenn Transferrate und Burst-Größe des Datenstroms oberhalb von *Two Rate P Rate* und *Two Rate P Burst* liegen, dann wendet das Gerät die Aktion *Non Conform Action* an.

Kombinierbar mit *Typ* = `assignQueue`, `redirect` und `mirror`.

Two Rate C Rate

Legt die Committed Rate in kbit/s fest.

Mögliche Werte:

▶ `1..4294967295`

Two Rate C Burst

Legt die Committed Burst Size in kByte fest.

Mögliche Werte:

▶ `0..128`

Two Rate P Rate

Legt die Peak Rate (max. zulässige Transferrate des Datenstroms) in kbit/s fest.

Mögliche Werte:

▶ `1..4294967295`

Two Rate P Burst

Legt die Peak Burst Size (max. zulässige Burst-Größe) in kByte fest.

Mögliche Werte:

▶ `1..128`

Conform Action
Conform Value
Exceed Action
Exceed Value
Non Conform Action
Non Conform Value

Im Feld *Conform Action* legen Sie die Aktion fest, die das Gerät auf den konformen Datenstrom anwendet. Konform bedeutet, dass Transferrate und Burst-Größe unterhalb von *Two Rate C Rate* und *Two Rate C Burst*liegen.

Im Feld *Exceed Action* legen Sie die Aktion fest, die das Gerät auf den Datenstrom anwendet. Voraussetzung ist, dass Transferrate und Burst-Größe zwischen *Two Rate C Rate* und *Two Rate P*

Rate sowie *Two Rate C Burst* und *Two Rate P Burst*liegen.

Im Feld *Non Conform Action*legen Sie die Aktion fest, die das Gerät auf den nicht-konformen Datenstrom anwendet. Nicht-konform bedeutet, dass Transferrate und Burst-Größe oberhalb von *Two Rate P Rate* und *Two Rate P Burst*liegen.

Mögliche Werte:

- `drop`
  Verwirft die Datenpakete.
- `markDscp`
  Überschreibt das DS-Feld der IP-Pakete.
  Das Gerät schreibt den im nebenstehenden Feld festgelegten Wert [`0..63`] in das das DS-Feld.
- `markPrec`
  Überschreibt das TOS-Feld der IP-Pakete.
  Das Gerät schreibt den im nebenstehenden Feld festgelegten Wert [`0..7`] in das TOS-Feld.
- `send`
  Vermittelt die Datenpakete.
- `markCos`
  Überschreibt das Prioritätsfeld im VLAN-Tag der Ethernet-Pakete:
  – Das Gerät schreibt den im Parameter *COS* festgelegten Prioritätswert in den VLAN-Tag.
  – Bei QinQ-markierten (IEEE 802.1ad) Ethernet-Paketen schreibt das Gerät den Wert in das äußere Tag (*Service-Tag* oder *S-Tag*).
  – Bei Ethernet-Paketen ohne VLAN-Tag fügt das Gerät ein Priority-Tag ein.
- `markCos2`
  Überschreibt bei QinQ-markierten Ethernet-Paketen das Prioritätsfeld im inneren Tag (*Customer-Tag* oder *C-Tag*) mit dem im nebenstehenden Feld festgelegten Wert [`0..7`].
- `markCosAsSecCos`
  Überschreibt das Prioritätsfeld im äußeren Tag (*S-Tag*) mit dem Prioritätswert des inneren Tags (*C-Tag*).

Color Conform Class

Legt die Klasse des empfangenen Datenstroms fest, die das Gerät als konform (grün) betrachtet.

Mögliche Werte:

- `0 - blind`
  Das Gerät arbeitet im Color-Blind-Modus. Das Gerät betrachtet den gesamten empfangenen Datenstrom als konform (grün).
- `<Name der DiffServ-Klasse>`
  Das Gerät betrachtet ausschließlich diese Klasse des empfangenen Datenstroms als konform (grün).
  Auswählbar sind Klassen, für die im Dialog *Switching > QoS/Priority > DiffServ > Klasse*, Spalte *Kriterium* eine Regel des Typs `cos`, `ipdscp`, `ipprec`, `cos2` festgelegt ist.

Vergewissern Sie sich, dass die Filterkriterien der oben in der Dropdown-Liste *Name der Klasse* ausgewählten Klasse und der in dieser Dropdown-Liste ausgewählten Klasse weder identisch sind noch sich einander ausschließen. Ausschlusskriterien sind:

- Die Filterkriterien haben denselben Regel-Typ, zum Beispiel `cos` und `cos`. Verwenden Sie Klassen mit unterschiedlichem Regel-Typ, zum Beispiel `cos` und `ipdscp`.
- Eine der Klassen referenziert mit dem Regel-Typ `refclass` eine weitere Klasse, die den verwendeten Klassen widerspricht.

Typ = assignQueue

Ändert die Warteschlange, in die das Gerät die Datenpakete einreiht.

Das Gerät reiht die Datenpakete in die Warteschlange mit der im Parameter *Queue-ID* festgelegten ID ein.

Wenden Sie diese Aktion ausschließlich auf Datenpakete an, die das Gerät empfängt.

Kombinierbar mit *Typ* = `drop`, `markCosVal` und `markCosAsSecCos`.

Queue-ID

Legt die ID der Warteschlange fest, in welche das Gerät die Datenpakete einreiht. Siehe Feld *Traffic-Klasse* im Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung*.

Mögliche Werte:

- `0..7`

Typ = drop

Verwirft die Datenpakete.

Kombinierbar mit *Typ* = `mirror`, wenn `mirror` zuerst eingerichtet wird.

Typ = redirect

Das Gerät leitet den empfangenen Datenstrom auf den im Feld *Redirection-Interface* festgelegten Port um.

Wenden Sie diese Aktion ausschließlich auf Datenpakete an, die das Gerät empfängt.

Kombinierbar mit *Typ* = `markCosVal`, `markIpDscpVal`, `markIpPrecedenceVal`, `policeSimple`, `policeTworate`, `assignQueue` und `markCosAsSecCos`.

Redirection-Interface

Legt den Ziel-Port fest.

Mögliche Werte:

- `<Port-Nummer>`
  Nummer des Ziel-Ports. Das Gerät leitet die Datenpakete auf diesen Port um.

Anmerkung: Der Ziel-Port benötigt ausreichend Bandbreite, um den Datenstrom aufzunehmen. Wenn der kopierte Datenstrom die Bandbreite des Ziel-Ports überschreitet, dann verwirft das Gerät überschüssige Datenpakete auf dem Ziel-Port.

Typ = `mirror`

Das Gerät kopiert den empfangenen Datenstrom und vermittelt ihn zusätzlich auf dem im Feld *Mirror Interface*festgelegten Port.

Wenden Sie diese Aktion ausschließlich auf Datenpakete an, die das Gerät empfängt.

Kombinierbar mit *Typ* = `markCosVal`, `markIpDscpVal`, `markIpPrecedenceVal`, `policeSimple`, `policeTworate`, `assignQueue` und `markCosAsSecCos`.

Mirror Interface

Legt den Ziel-Port fest.

Mögliche Werte:

- `<Port-Nummer>`
  Nummer des Ziel-Ports. Das Gerät kopiert die Datenpakete auf diesen Port.

Anmerkung: Der Ziel-Port benötigt ausreichend Bandbreite, um den Datenstrom aufzunehmen. Wenn der kopierte Datenstrom die Bandbreite des Ziel-Ports überschreitet, dann verwirft das Gerät überschüssige Datenpakete auf dem Ziel-Port.

Typ = `markCosAsSecCos`

Überschreibt das Prioritätsfeld im äußeren VLAN-Tag der Ethernet-Pakete mit dem Prioritätswert des inneren VLAN-Tags.

Wenden Sie diese Aktion ausschließlich auf Datenpakete an, die das Gerät empfängt.

Kombinierbar mit *Typ* = `assignQueue`, `redirect` und `mirror`.

5.7.6.5 DiffServ Zuweisung

[Switching > QoS/Priority > DiffServ > Zuweisung]

In diesem Dialog weisen Sie die Richtlinie einem Port zu.

Anmerkung: Sie können IP-ACL-Regeln und DiffServ-Regeln für die gleiche Richtung nicht gleichzeitig auf einen Port anwenden.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Erzeugen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen. Siehe „[Fenster Erzeugen]" auf Seite 299.

Port

Zeigt die Nummer des Ports.

Richtung

Zeigt die Interface-Richtung, zu der Sie die Richtlinie zugewiesen haben.

Policy-Name

Zeigt den Namen der dem Interface zugewiesenen Richtlinie.

Status

Zeigt den Port-Status.

Aktiv

Aktiviert/deaktiviert die mit dieser Zeile verbundenen DiffServ-Parameter.

Mögliche Werte:

- `markiert`
  Das Gerät leitet die Daten entsprechend den festgelegten DiffServ-Einstellungen weiter.
- `unmarkiert`
  Das Gerät leitet die Daten ohne Anwendung der festgelegten DiffServ-Einstellungen weiter.

[Fenster Erzeugen]

Port

Legt den Port fest, auf den sich der Tabelleneintrag bezieht.

Mögliche Werte:
- Verfügbare Ports

Richtung

Legt die Richtung fest, in welcher das Gerät die Richtlinie anwendet.

Mögliche Werte:
- *In* (Voreinstellung)
- *Out*

Richtlinie

Legt die dem Port zugewiesene Richtlinie fest.

Mögliche Werte:
- Verfügbare Richtlinien

5.8 VLAN

[Switching > 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 die Daten 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 auf 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
- MAC-basiertes VLAN
- IP-Subnetz-basiertes VLAN
- Protokoll-basiertes VLAN
- Port-basiertes VLAN

Das Menü enthält die folgenden Dialoge:

- VLAN Global
- VLAN Konfiguration
- VLAN Port
- VLAN Voice
- MAC-basiertes VLAN
- Subnet-basiertes VLAN
- Protokoll-basiertes VLAN

5.8.1 VLAN Global

[Switching > VLAN > Global]

Dieser Dialog ermöglicht Ihnen, sich allgemeine VLAN-Parameter des Geräts anzusehen.

Konfiguration

Schaltflächen

VLAN-Einstellungen zurücksetzen

Versetzt die VLAN-Einstellungen des Geräts in den Voreinstellung.

Beachten Sie, dass Sie Ihre Verbindung zum Gerät trennen, wenn Sie im Dialog *Grundeinstellungen > Netz > Global* die VLAN-ID für das Management des Geräts geändert haben.

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 stets im Gerät eingerichtet.

5.8.2 VLAN Konfiguration

[Switching > 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, dann 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Erzeugen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

Im Feld *VLAN-ID* legen Sie die ID des VLANs fest.

VLAN-ID

ID des VLANs.

Das Gerät unterstützt bis zu 512 gleichzeitig 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*.
  Wenn Sie die Änderungen im permanenten Speicher speichern, dann bleiben die VLANs mit dieser Einstellung nach einem Neustart eingerichtet.
- `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

<Port-Nummer>

Legt fest, ob der betreffende Port Datenpakete des VLANs vermittelt und ob die Datenpakete ein VLAN-Tag 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 sorgt zudem dafür, zu vermeiden, dass 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 Zugriff auf das Management des Geräts ist ausschließlich mit dem Command Line Interface über die serielle Schnittstelle möglich.

5.8.3 VLAN Port

[Switching > 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 ermöglicht Ihnen, 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Port-VLAN-ID

Legt die ID des VLANs fest, die das Gerät Datenpaketen ohne eigenes VLAN-Tag zuweist.

Voraussetzungen:
- In Spalte *Akzeptierte Datenpakete* legen Sie den Wert `admitAll` fest.

Mögliche Werte:
- ID eines bereits eingerichteten VLANs (Voreinstellung: `1`)

Wenn Sie die Funktion *MRP* verwenden und den Ring-Ports kein VLAN zugewiesen ist, dann 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.

5.8.4 VLAN Voice

[Switching > 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 ist abhängig vom Voice-VLAN-Interface-Modus (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

Funktion

Schaltet die Funktion *VLAN Voice* des Geräts global ein/aus.

Mögliche Werte:

- `An`
- `Aus` (Voreinstellung)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 18.

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 Funktion *VLAN Voice* für diesen Tabelleneintrag.
- `kein`
  Ermöglicht es dem IP-Telefon, seine eigene Konfiguration beim 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, dann legen Sie zusätzlich in Spalte *Priorität* einen geeigneten Wert fest.

Data-Priority-Modus

Legt den Trust-Modus für Datenverkehr auf dem 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 auf dem 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 auf dem betreffenden Port.

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.

Voraussetzungen:

- In Spalte *Voice-VLAN-Modus* legen Sie den Wert `dot1p-priority` fest.

Mögliche Werte:

- `0..7`
- `kein`
  Deaktiviert die Voice-VLAN-Priorität des Ports.

DSCP

Legt den IP-DSCP-Wert fest.

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/Priority > IP-DSCP-Zuweisung* weisen Sie jedem IP-DSCP-Wert eine *Verkehrsklasse* zu.

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, dann 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`

5.8.5 MAC-basiertes VLAN

[Switching > VLAN > MAC-basiertes VLAN]

In einem MAC-basierten VLAN leitet das Gerät Datenverkehr anhand der mit einem VLAN verknüpften Quell-MAC-Adresse weiter. Benutzerdefinierte Filter legen hierbei fest, ob ein Paket zu einem bestimmten VLAN gehört.

MAC-basierte VLANs definieren Filterkriterien ausschließlich für unmarkierte Datenpakete oder für Pakete mit Prioritätsmarkierung. Weisen Sie einen Port einem MAC-basierten VLAN zu, um eine bestimmte Quell-MAC-Adresse zu routen. Das Gerät leitet dann unmarkierte Pakete, welche mit der konfigurierten MAC-Adresse angekommen sind, an die MAC-basierte VLAN-ID weiter. Andere unmarkierte Pakete unterliegen den normalen VLAN-Klassifizierungsregeln.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Erzeugen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *MAC-Adresse* legen Sie die MAC-Adresse fest.
- Im Feld *VLAN-ID* legen Sie die ID des VLANs fest.

MAC-Adresse

Zeigt die MAC-Adresse, auf die sich der Tabelleneintrag bezieht.

Das Gerät unterstützt bis zu 256 gleichzeitige Zuweisungen zu MAC-basierten VLANs.

Mögliche Werte:

- Gültige MAC-Adresse

VLAN-ID

Zeigt die ID des VLANs, für das der Tabelleneintrag gilt.

Mögliche Werte:

- `1..4042`(eingerichtete VLAN-IDs)

5.8.6 Subnet-basiertes VLAN

[Switching > VLAN > Subnet-basiertes VLAN]

In IP-Subnetz-basierten VLANs leitet das Gerät Datenverkehr anhand der mit einem VLAN verknüpften Quell-IP-Adresse und Subnetzmaske weiter. Benutzerdefinierte Filter legen hierbei fest, ob ein Paket zu einem bestimmten VLAN gehört.

IP-Subnetz-basierte VLANs definieren Filterkriterien ausschließlich für unmarkierte Datenpakete oder für Pakete mit Prioritätsmarkierung. Weisen Sie einen Port einem IP-Subnetz-basierten VLAN zu, um eine bestimmte Quelladresse zu routen. Das Gerät leitet dann unmarkierte Pakete, welche mit der konfigurierten Adresse angekommen sind, an die IP-Subnetz-basierte VLAN-ID weiter.

Zum Konfigurieren eines IP-Subnetz-basierten VLANs definieren Sie eine IP-Adresse, eine Subnetzmaske und die dazugehörige VLAN-Kennung. Bei mehreren zutreffenden Einträgen verwendet das Gerät den Eintrag mit dem längsten Präfix zuerst.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Erzeugen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen.

- Im Feld *IP-Adresse* legen Sie die IP-Adresse fest.
- Im Feld *Netzmaske*legen Sie die Netzmaske fest.
- Im Feld *VLAN-ID* legen Sie die ID des VLANs fest.

IP-Adresse

Zeigt die IP-Adresse, die dem Subnetz-basierten VLAN zugewiesen ist.

Das Gerät unterstützt bis zu 128 gleichzeitige Zuordnungen zu Subnetz-basierten VLANs.

Mögliche Werte:

- Gültige IP-Adresse

Netzmaske

Zeigt die Netzmaske, die dem Subnetz-basierten VLAN zugewiesen ist.

Mögliche Werte:

- Gültige IP-Netzmaske

VLAN-ID

Zeigt die VLAN-ID.

Mögliche Werte:

- `1..4042`

5.8.7 Protokoll-basiertes VLAN

[Switching > VLAN > Protokoll-basiertes VLAN]

In einem Protokoll-basierten VLAN vermitteln festgelegte Ports den auf dem L3-Protokoll (Ethertype) basierten Datenverkehr, der mit dem VLAN verknüpft ist. Benutzerdefinierte Paketfilter legen hierbei fest, ob ein Paket zu einem bestimmten VLAN gehört.

Protokoll-basierte VLANs definieren Filterkriterien ausschließlich für unmarkierte Datenpakete. Weisen Sie einen Port einem Protokoll-basierten VLAN zu, um ein bestimmtes Protokoll zu routen. Das Gerät leitet dann unmarkierte Pakete, welche mit dem konfigurierten Protokoll angekommen sind, an die Protokoll-basierte VLAN-ID weiter. Das Gerät weist anderen unmarkierten Paketen die VLAN-Kennung des Ports zu.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Gruppen-ID

Zeigt die Gruppenkennung des Protokoll-basierten VLAN-Eintrags.

Das Gerät unterstützt bis zu 128 gleichzeitige Zuordnungen zu Protokoll-basierten VLANs.

Mögliche Werte:

- `1..128`

Name

Zeigt den Gruppennamen des Protokoll-basierten VLAN-Eintrags.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..16 Zeichen

VLAN-ID

Legt die ID des VLANs fest.

Mögliche Werte:

- `1..4042`

Port

Legt die Ports fest, die der Gruppe zugewiesen sind.

Mögliche Werte:

- `<Port-Nummer>`
  Wählen Sie die Ports in der Dropdown-Liste.

Ethertype

Legt den Ethertype-Wert fest, der dem VLAN zugewiesen ist.

Der Ethertype ist ein aus 2 Oktetts bestehendes Feld im Ethernet-Paket, aus dem hervorgeht, welches Protokoll die Nutzdaten enthalten.

Mögliche Werte:

- `0x0600..0xFFFF`
  Ethertype in hexadezimaler Ziffernfolge
  Wenn Sie einen Dezimalwert einfügen, konvertiert das Gerät den Wert beim Klicken der Schaltfläche ✓ in eine hexadezimale Ziffernfolge.
- `ip`
  Ethertype-Schlüsselwort für IPv4 (entspricht `0x0800`)
- `arp`
  Ethertype-Schlüsselwort für ARP (entspricht `0x0806`)
- `ipx`
  Ethertype-Schlüsselwort für IPX (entspricht `0x8137`)

5.9 L2-Redundanz

[Switching > L2-Redundanz]

Das Menü enthält die folgenden Dialoge:

- MRP
- HIPER-Ring
- Spanning Tree
- Link-Aggregation
- Link-Backup
- FuseNet

5.9.1 MRP

[Switching > L2-Redundanz > MRP]

Das Media Redundancy Protocol (MRP) ist ein Protokoll, das Ihnen 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*.

Wenn Sie mit übergroßen Ethernet-Paketen arbeiten (für diesen Port ist der Wert in Spalte *MTU* > `1518`, siehe Dialog *Grundeinstellungen > Port*), ist die Umschaltzeit bei der Rekonfiguration des MRP-Rings abhängig von folgenden Parametern:

- Bandbreite der Ring-Leitung
- Größe der Ethernet-Pakete
- Anzahl der Geräte im Ring

Legen Sie die Umschaltzeit ausreichend groß fest, um Verzögerungen der MRP-Pakete aufgrund von Latenzen in den Geräten zu vermeiden. Die Formel zum Berechnen der Umschaltzeit finden Sie in IEC 62439-2, Kapitel 9.5.

Funktion

Schaltflächen

Lösche Ring-Konfiguration

Schaltet die Redundanzfunktion aus und setzt alle Einstellungen im Dialog die voreingestellten Werte zurück.

Funktion

Schaltet die Funktion *MRP* ein/aus.

Wenn alle Parameter für den MRP-Ring konfiguriert sind, schalten Sie hier die Funktion ein.

Mögliche Werte:

- `An`
  Die Funktion *MRP* ist eingeschaltet.
  Sind alle Geräte im MRP-Ring konfiguriert, ist die Redundanz aktiv.
- `Aus` (Voreinstellung)
  Die Funktion *MRP* ist ausgeschaltet.

Ring-Port 1/Ring-Port 2

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.

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

Ring-Manager

Schaltet die Funktion *Ring-Manager* ein/aus.

Aktivieren Sie diese Funktion bei genau einem Gerät an den Enden der Linie.

Mögliche Werte:

- `An`
  Die Funktion *Ring-Manager* ist eingeschaltet.
  Das Gerät arbeitet als Ring-Manager.
- `Aus` (Voreinstellung)
  Die Funktion *Ring-Manager* 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.

Wenn Sie mit übergroßen Ethernet-Paketen arbeiten, ist die Anzahl der Geräte im Ring begrenzt. Beachten Sie, dass die Umschaltzeit von mehreren Parametern abhängig ist. Siehe Beschreibung oben.

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, dann erzeugt das Gerät dieses 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

Information

Zeigt Meldungen zur Redundanzkonfiguration und mögliche Fehlerursachen.

Wenn das Gerät als Ring-Client oder als Ring-Manager arbeitet, sind folgende Meldungen möglich:

- `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.

Wenn das Gerät als Ring-Manager arbeitet, sind folgende Meldungen möglich:

- `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 einem Ring-Port.

5.9.2 HIPER-Ring

[Switching > L2-Redundanz > HIPER-Ring]

Das Konzept der Ring-Redundanz ermöglicht den Aufbau hochverfügbarer, ringförmiger Netze. Dieses Gerät stellt einen HIPER-Ring-Client bereit. Diese Funktion ermöglicht Ihnen, einen vorhandenen HIPER-Ring zu erweitern oder ein Gerät zu ersetzen, das bereits als Client in einem HIPER-Ring aktiv ist.

Ein HIPER-Ring enthält einen Ring-Manager (RM), der den Ring kontrolliert. Der Ring-Manager sendet sowohl auf dem primären als auch auf dem sekundären Port Watchdog-Pakete in den Ring. Wenn der Ring-Manager die Watchdog-Pakete auf beiden Ports empfängt, verbleibt der primäre Port im Forwarding-Status und der sekundäre Port im Discarding-Status.

Das Gerät arbeitet ausschließlich im Ring-Client-Modus. Das bedeutet, dass das Gerät in der Lage ist, an den Ring-Ports Watchdog-Pakete zu erkennen und weiterzuleiten sowie die Änderung des Link-Status an den Ring-Manager zu senden, zum Beispiel LinkDown- und LinkUp-Pakete.

Als Ring-Ports unterstützt das Gerät ausschließlich Fast-Ethernet-Ports und Gigabit-Ethernet-Ports. Des Weiteren unterstützt das Gerät ausschließlich HIPER-Ring in VLAN `1`.

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

Anmerkung: Konfigurieren Sie die Geräte des HIPER-Rings individuell. Bevor Sie die Redundanzverbindung herstellen, konfigurieren Sie jedes Gerät im HIPER-Ring vollständig. So vermeiden Sie Loops während der Konfigurationsphase.

Funktion

Funktion

Schaltet den *HIPER-Ring*-Client ein/aus.

Mögliche Werte:

- `An`
  Der *HIPER-Ring*-Client ist eingeschaltet.
- `Aus` (Voreinstellung)
  Der *HIPER-Ring*-Client ist ausgeschaltet.

Ring-Port 1/Ring-Port 2

Port

Legt die Port-Nummer für den primären/sekundären Ring-Port fest.

Mögliche Werte:

- `-` (Voreinstellung)
  Kein primärer/sekundärer Ring-Port ausgewählt.
- `<Port-Nummer>`
  Nummer des Ring-Ports

Zustand

Zeigt den Status des primären/sekundären Ring-Ports.

Mögliche Werte:

- *`not-available`*
  Der *HIPER-Ring*-Client ist ausgeschaltet.
  oder
  Kein primärer oder sekundärer Ring-Port ausgewählt.
- *`aktiv`*
  Der Ring-Port ist eingeschaltet, der Link ist vorhanden.
- *`inaktiv`*
  Kein Link auf dem Ring-Port vorhanden.
  Sobald der Link an einem Ring-Port abbricht, sendet das Gerät auf dem anderen Ring-Port ein LinkDown-Paket an den Ring-Manager.

Information

Modus

Zeigt, dass das Gerät ausschließlich im Ring-Client-Modus arbeitet.

5.9.3 Spanning Tree

[Switching > L2-Redundanz > Spanning Tree]

Das Spanning Tree Protocol (STP) ist ein Protokoll, das redundante Pfade eines Netzes deaktiviert, um 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 (RSTP) 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.

Das Gerät unterstützt das in Multiple Spanning Tree Protocol (MSTP) standardisierte IEEE 802.1, eine Weiterentwicklung des Spanning Tree Protocol (STP).

Das Menü enthält die folgenden Dialoge:

- Spanning Tree Global
- Spanning Tree MSTP
- Spanning Tree Port

5.9.3.1 Spanning Tree Global

[Switching > L2-Redundanz > Spanning Tree > Global]

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

Funktion

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

Variante

Legt das für die Funktion *Spanning Tree* verwendete Protokoll fest:

Mögliche Werte:

- `rstp` (Voreinstellung)
  Das Protokoll `RSTP` ist aktiv.
  Mit RSTP (IEEE 802.1Q-2005) arbeitet die Funktion *Spanning Tree* auf der darunterliegenden physikalischen Schicht.
- `mstp`
  Das Protokoll `MSTP` ist aktiv.
  Um längere Recovery-Zeiten zu vermeiden, legen Sie im Feld *Tx holds* den Maximalwert von `40` fest.

Traps

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps für die folgenden Ereignisse:

- Eine andere Bridge übernimmt die Rolle der Root-Bridge.
- Die Topologie ändert sich. Ein Port ändert *Port-Zustand* 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.

Ring only mode

Aktiv

Aktiviert/deaktiviert die Funktion *Ring only mode*, die dafür sorgt, dass das Gerät das Alter der BPDUs nicht verifiziert.

Mögliche Werte:

- `markiert`
  Die Funktion *Ring only mode* ist aktiv. Diese Einstellung verwenden Sie für Anwendungen mit RSTP-Ring-Diameter größer als 40.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Ring only mode* ist inaktiv.

Erster Port

Legt die Port-Nummer des 1. Interfaces fest.

Mögliche Werte:

- `<Port-Nummer>` (Voreinstellung: `-`)

Zweiter Port

Legt die Port-Nummer des 2. Interfaces fest.

Mögliche Werte:

- `<Port-Nummer>` (Voreinstellung: `-`)

Bridge-Konfiguration

Bridge-ID

Zeigt die Bridge-ID des Geräts.

Das Gerät mit dem kleinsten nummerischen Bridge-ID-Wert übernimmt die Rolle der Root-Bridge im Netz.

Mögliche Werte:

- `<Bridge-Priorität> / <MAC-Adresse>`
  Wert im Feld *Priorität* / MAC-Adresse des Geräts

Priorität

Legt die Bridge-Priorität des Geräts fest.

Mögliche Werte:

- `0..61440` in 4096er-Schritten (Voreinstellung: `32768`)

Um das Gerät zur Root-Bridge zu machen, weisen Sie dem Gerät den kleinsten nummerischen Wert für die Priorität im Netz zu.

Hello-Time [s]

Legt die Zeit in Sekunden fest zwischen dem Senden zweier Konfigurationsmeldungen (Hello-Datenpakete).

Mögliche Werte:

- `1..2` (Voreinstellung: `2`)

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann 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`)

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann 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, dann 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`)

Wenn das Gerät die Rolle der Root-Bridge übernimmt, dann 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`)
  Um längere Recovery-Zeiten bei Verwendung des Protokolls `MSTP` zu vermeiden, legen Sie den Maximalwert `40` fest.

Sendet das Gerät eine BPDU, inkrementiert das Gerät auf 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 kann es zur Unterbrechung der Kommunikation kommen, wenn das Gerät keine BPDUs empfängt.

Das Gerät dekrementiert den Zähler jede Sekunde um `1`. In der folgenden Sekunde sendet das Gerät maximal `1` neue BPDU.

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.
  - Wenn ein Edge-Port eine STP-BPDU empfängt, dann 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 Funktion *Auto-Disable*. 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 den STP-BPDU-Filter 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 verwendet diese Ports nicht im *Spanning Tree*-Betrieb.
  - 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 Funktion *Auto-Disable* für die Parameter, deren Einhaltung der *BPDU-Guard* auf dem Port überwacht.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für den *BPDU-Guard* ist aktiv.
  - Wenn der Port eine STP-BPDU empfängt, schaltet das Gerät einen Edge-Port aus. 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.
  - Nach einer Wartezeit schaltet die Funktion *Auto-Disable* 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 Funktion *Auto-Disable* für den *BPDU-Guard* ist inaktiv.

Root-Information

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

Legt die von der Root-Bridge bereitstellte maximal zulässige Astlänge fest, 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

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, dann zeigt das Feld den Wert `no Port`.

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, dann übernimmt das Gerät die Rolle der Root-Bridge.

Topologie-Änderungen

Zeigt, wie viele Male seit dem Start der *Spanning Tree*-Instanz das Gerät einen Port durch die Funktion *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>`

5.9.3.2 Spanning Tree MSTP

[Switching > L2-Redundanz > Spanning Tree > MSTP]

In dieser Registerkarte verwalten Sie die Einstellungen der globalen und lokalen MST-Instanzen.

Im Gegensatz zu den lokalen MST-Instanzen ist die globale MST-Instanz permanent im Gerät eingerichtet. Die globale MST-Instanz enthält die VLANs, die keiner lokalen MST-Instanz explizit zugeordnet sind.

Das Gerät unterstützt bis zu 16 lokale MST-Instanzen. Um eine lokale MST-Instanz zu erzeugen, klicken Sie die Schaltfläche .

Während sich bei STP ein einziger Spanning Tree über das Netz erstreckt, ermöglicht Ihnen MSTP, einen Spanning Tree pro VLAN oder einer Gruppe von VLANs einzurichten. Dadurch ist es möglich, mehrere kleinere Spanning Trees über ein Netz festzulegen.

Längere Konvergenzzeiten vermeiden Sie wie folgt:
- Verwenden Sie im Netz ausschließlich Geräte, die RSTP oder MSTP unterstützen.
- Passen Sie folgende Parameter an Topologie und Anzahl der Bridges an:
  - Maximal zulässige Anzahl der Geräte bis zur Root-Bridge
    Dialog *Switching > L2-Redundanz > Spanning Tree > Global*, Feld *Max age*
  - Maximal zulässige Anzahl der Bridges innerhalb der MST-Region in einem Ast zur Root-Bridge
    Dialog *Switching > L2-Redundanz > Spanning Tree > MSTP*, Rahmen *Globale CIST-Parameter*, Feld *Hops (max.)*

Für Bridges einer MST-Region legen Sie identische Werte für folgende Parameter fest:
- *Name* der MST-Region
- *Revision-Level* der MST-Region
- Zuordnung der VLANs zu den MST-Instanzen
  - Ports, die Bridges einer MST-Region verbinden, nehmen Sie als Mitglied in die auf den Bridges eingerichteten VLANs auf. Die Ports sollen die Datenpakete mit VLAN-Tag vermitteln. So vermeiden Sie innerhalb der MST-Region mögliche Unterbrechungen bei Topologieänderungen.
  - Ports, die eine MST-Region mit anderen MST-Regionen oder mit der CST-Region verbinden (Boundary-Ports), nehmen Sie als Mitglied in die in beiden Regionen eingerichteten VLANs auf. Die Ports sollen die Datenpakete mit VLAN-Tag vermitteln. So vermeiden Sie mögliche Verbindungsunterbrechungen bei Topologieänderungen, die die Boundary-Ports betreffen.

MST region identifier

Name

Legt den Namen der MST-Region fest, zu der das Gerät gehört.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Revision-Level

Legt die Versionsnummer der MST-Region fest, zu der das Gerät gehört.

Mögliche Werte:

- `0..65535` (Voreinstellung: `1`)

Checksumme

Zeigt die MD5-Prüfsumme der MST-Konfiguration.

Globale CIST-Parameter

Hops (max.)

Legt die maximale Anzahl der Bridges fest, die sich innerhalb der MST-Region in einem Ast zur Root-Bridge befinden.

Mögliche Werte:

- `6..40` (Voreinstellung: `20`)

Zugeordnete VLANs

Zeigt die IDs der VLANs, die ausschließlich der globalen MST-Instanz und keiner anderen lokalen MST-Instanz zugewiesen sind.

Mögliche Werte:

- `ID statisch eingerichteter VLANs`
  (Voreinstellung: `1`)

Bridge-ID

Zeigt die Bridge-ID des Geräts.

Mögliche Werte:

- `<Bridge-Priorität> / <MAC-Adresse>`
  Der Wert setzt sich wie folgt zusammen:
  - Wert im Feld *Priorität*. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*, Rahmen *Bridge-Konfiguration*.
  - MAC-Adresse des Geräts.

Root-ID

Zeigt die Bridge-ID der gegenwärtigen CIST-Root-Bridge des gesamten Schicht-2-Netzes.

Mögliche Werte:

- `<Bridge-Priorität> / <MAC-Adresse>`

Das Gerät mit der nummerisch niedrigsten Bridge-ID übernimmt die Rolle der CIST-Root-Bridge im Netz. Folgende Geräte können die Rolle der CIST-Root-Bridge übernehmen:

- Bridges, die keiner MST-Region angehören
- Bridges, die der globalen Instanz einer MST-Region angehören

Im gesamten Schicht-2-Netz verwenden die Bridges die Zeit-Einstellungen der CIST-Root-Bridge, zum Beispiel *Hello-Time [s]*.

Regionale Root-ID

Zeigt die Bridge-ID der gegenwärtigen Root-Bridge der globalen Instanz der MST-Region, zu der das Gerät gehört.

Mögliche Werte:

- `<Bridge-Priorität> / <MAC-Adresse>`

Die Werte in den Feldern *Regionale Root-ID* und *Root-ID* sind identisch, wenn die regionale Root-Bridge die niedrigste Bridge-ID im gesamten Schicht-2-Netz besitzt.

Root-Port

Zeigt den Port des Geräts, von dem aus der Pfad zur gegenwärtigen CIST-Root-Bridge des gesamten Schicht-2-Netzes führt.

Mögliche Werte:

- `no Port`
  Das Gerät übernimmt gegenwärtig die Rolle der Root-Bridge.
- `<Port-Nummer>`
  Der Pfad zur gegenwärtigen CIST-Root-Bridge des gesamten Schicht-2-Netzes führt über diesen Port.

Root-Pfadkosten

Zeigt die Pfadkosten für den Pfad, der von der regionalen Root-Bridge der MST-Region des Geräts zur gegenwärtigen CIST-Root-Bridge des gesamten Schicht-2-Netzes führt.

Mögliche Werte:

- `0..200000000`
  Wenn der Wert `0` festgelegt ist, dann ist die regionale Root-Bridge gleichzeitig in der Rolle der CIST-Root-Bridge.
  Für die Geräte innerhalb einer MST-Region sind die *Root-Pfadkosten*-Werte identisch.

Falls Sie kein MSTP einsetzen, sind die *Root-Pfadkosten*-Werte identisch mit den Root-Pfadkosten von Spanning Tree oder von Rapid Spanning Tree. In diesem Fall betrachtet sich jedes Gerät als eine eigene Region.

Interne Root-Pfadkosten

Zeigt die internen Pfadkosten für den Pfad, der vom Root-Port des Geräts zur gegenwärtigen regionalen Root-Bridge der MST-Region des Geräts führt.

Mögliche Werte:

- `0..200000000`
  Wenn der Wert `0` festgelegt ist, dann ist die lokale Bridge gleichzeitig in der Rolle der gegenwärtigen regionalen Root-Bridge.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Erzeugen

Fügt einen neuen Tabelleneintrag hinzu.

Das Gerät unterstützt bis zu 16 lokale Instanzen.

VLANs konfigurieren

Öffnet den Dialog *VLANs konfigurieren*, um der in der Tabelle ausgewählten lokalen MST-Instanz VLANs zuzuweisen.

MSTI

Zeigt die Instanz-Nummer der lokalen MST-Instanz.

Zugeordnete VLANs

Zeigt die IDs der VLANs, die dieser lokalen MST-Instanz zugeordnet sind.

Priorität

Legt die Bridge-Priorität der lokalen MST-Instanz fest.

Mögliche Werte:

- `0..61440` in 4096er-Schritten (Voreinstellung: `32768`)

Weisen Sie dem Gerät die nummerisch niedrigste Priorität in dieser lokalen MST-Instanz zu, um das Gerät zur Root-Bridge zu bestimmen.

Bridge-ID

Zeigt die Bridge-ID.

Das Gerät mit der nummerisch niedrigsten Bridge-ID übernimmt die Rolle der MSTI-(regional)-Root-Bridge in der Instanz.

Mögliche Werte:

- `<Bridge-Priorität + Nummer der Instanz> / <MAC-Adresse>`
  Summe der Werte in den Feldern *Priorität* und *MSTI* / MAC-Adresse des Geräts

Zeit seit letzter Änderung

Zeigt die Zeit, die seit der letzten Topologieänderung in dieser Instanz vergangen ist.

Topologie-Änderungen

Zeigt, wie viele Male seit dem Start der *Spanning Tree*-Instanz das Gerät einen Port durch die Funktion *Spanning Tree* in den Zustand `forwarding` gesetzt hat.

Topologie-Änderung

Zeigt, ob das Gerät eine Topologieänderung in dieser Instanz erkannt hat.

Mögliche Werte:

- `markiert`
  Das Gerät hat eine Topologieänderung erkannt.
- `unmarkiert`
  Das Gerät hat keine Topologieänderung erkannt.

Root-ID

Zeigt die Bridge-ID der gegenwärtigen Root-Bridge dieser Instanz.

Mögliche Werte:

- `<Bridge-ID> / <MAC-Adresse>`

Root-Pfadkosten

Zeigt die Pfadkosten für den Pfad, der vom Root-Port des Geräts zur gegenwärtigen Root-Bridge der Instanz führt.

Mögliche Werte:

- `0..200000000`
  Wenn der Wert `0` festgelegt ist, dann ist die Bridge gleichzeitig die Root-Bridge der Instanz.

Root-Port

Zeigt den Port des Geräts, von dem aus der Pfad zur gegenwärtigen Root-Bridge der Instanz führt.

Mögliche Werte:

- `no Port`
  Das Gerät übernimmt gegenwärtig die Rolle der Root-Bridge.
- `<Port-Nummer>`
  Der Pfad zur gegenwärtigen Root-Bridge der Instanz führt über diesen Port.

5.9.3.3 Spanning Tree Port

[Switching > L2-Redundanz > 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]
- [MSTI<MSTI>]

[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 Funktion *Spanning Tree* 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 18.

Port

Zeigt die Nummer des Ports.

STP aktiv

Schaltet die Spanning-Tree-Funktion auf dem Port ein/aus.

Mögliche Werte:
- `markiert` (Voreinstellung)
  Die Funktion *Spanning Tree* ist auf dem Port aktiv.
- `unmarkiert`
  Die Funktion *Spanning Tree* ist auf dem Port inaktiv.
  Wenn die Funktion *Spanning Tree* im Gerät eingeschaltet und auf dem Port inaktiv ist, dann sendet der Port keine STP-BPDUs und verwirft empfangene STP-BPDUs.

Port-Zustand

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 Funktion *Spanning Tree* ist auf dem Port ausgeschaltet. Der Port leitet STP-BPDUs weiter.
- *notParticipate*
  Der Port nimmt nicht an 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 blockierend).
- *designated*
  Port zur von der Root-Bridge abgewandten Seite des Baums (gegenwärtig blockierend).
- *backup*
  Port empfängt STP-BPDUs des eigenen Geräts.
- *master*
  Port mit dem günstigsten Pfad zum CIST. Der Port ist CIST-Root-Port der CIST-Regional-Root. Der Port ist in einer MST-Region einzigartig.
- *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 automatisch die Pfadkosten in Abhängigkeit von der Datenrate des Ports.

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, 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, 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, die der Port mit der Rolle `designated` senden würde.

Empfangene Port-ID

Zeigt die Port-ID des Geräts, 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, 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, die der Port mit der Rolle `designated` senden würde.

Empfangene Port-Pfadkosten

Zeigt die Pfadkosten, welche die übergeordnete Bridge von ihrem Root-Port in der lokalen MST-Instanz zur Root-Bridge hat.

Mögliche Werte:

- Für Ports mit der Rolle `designated` zeigt das Gerät die Information der STP-BPDU, 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, die der Port mit der Rolle `designated` senden würde.

Admin-Edge-Port

Aktiviert/deaktiviert den *Admin-Edge-Port*-Modus. Wenn ein Endgerät an den Port angeschlossen ist, dann verwenden Sie den *Admin-Edge-Port*-Modus. Diese Einstellung ermöglicht dem Edge-Port, nach dem LinkUp schneller in den Zustand 'forwarding' zu schalten und damit das Endgerät schneller erreichbar zu machen.

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.

Auto-Edge-Port

Aktiviert/deaktiviert die automatische Erkennung, ob an den 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 an den Port ein Endgerät oder eine STP-Bridge angeschlossen ist.

Mögliche Werte:

- `markiert`
  An den Port ist ein Endgerät angeschlossen. Der Port empfängt keine STP-BPDUs.
- `unmarkiert`
  An den 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:

- `markiert`
  Der Port ist über eine Vollduplex-Verbindung direkt mit einem STP-Gerät verbunden. Die direkte, dezentrale Kommunikation zwischen 2 Bridges ermöglicht kurze Rekonfigurationszeiten.
- `unmarkiert`
  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.

BPDU flood

Aktiviert/deaktiviert den *BPDU flood*-Modus auf dem Port, auch wenn die Funktion *Spanning Tree* auf dem Port inaktiv ist. Das Gerät flutet auf dem Port empfangene STP-BPDUs auf denjenigen Ports, für welche die Funktion *Spanning Tree* inaktiv und der *BPDU flood*-Modus zugleich aktiv ist.

Mögliche Werte:

- `markiert`
  Der *BPDU flood*-Modus ist aktiv.
- `unmarkiert` (Voreinstellung)
  Der *BPDU flood*-Modus ist inaktiv.

[Guards]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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]* zurück.
- `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 sorgt das Gerät dafür, Loops zu vermeiden, 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 sorgt dafür, Loops zu vermeiden, zum Beispiel wenn Sie die Spanning-Tree-Funktion auf dem entfernten Gerät ausschalten 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 markiert das Kontrollkästchen in Spalte *Loop-Zustand*.
  - Empfängt der Port anschließend wieder STP-BPDUs, setzt das Gerät den Zustand des Ports auf einen Wert gemäß *Port-Rolle* und hebt die Markierung des Kontrollkästchens in Spalte *Loop-Zustand* auf.
- `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`.

Loop-Zustand

Zeigt, ob der Loop-Zustand des Ports inkonsistent ist.

Mögliche Werte:

- `markiert`
  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 sorgt das Gerät dafür, mögliche Loops zu vermeiden.
- `unmarkiert`
  Der Loop-Status des Ports ist konsistent. Der Port empfängt STP-BPDUs.

Übergänge in Loop-Zustand

Zeigt, wie viele Male der Loop-Zustand inkonsistent geworden ist (markiertes Kontrollkästchen in Spalte *Loop-Zustand*).

Übergänge aus Loop-Zustand

Zeigt, wie viele Male der Loop-Zustand konsistent geworden ist (unmarkiertes Kontrollkästchen in Spalte *Loop-Zustand*).

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*.

[MSTI<MSTI>]

Diese Registerkarte ermöglicht Ihnen, an den Ports die Einstellungen für Pfadkosten und Priorität in der lokalen MST-Instanz festzulegen sowie gegenwärtige Werte anzusehen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Port-Zustand

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 Funktion *Spanning Tree* ist auf dem Port ausgeschaltet.
  Der Port leitet STP-BPDUs weiter.
- `notParticipate`
  Der Port nimmt nicht an STP teil.

Port-Rolle

Zeigt die gegenwärtige Rolle des Ports in der lokalen Instanz.

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, der STP-BPDUs des eigenen Geräts empfängt.
- `master`
  Port mit dem günstigsten Pfad zum CIST. Der Port ist CIST-Root-Port der CIST-Regional-Root. Der Port ist in einer MST-Region einzigartig.
- `disabled`
  Der Port ist inaktiv. Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.

Port-Pfadkosten

Legt die Pfadkosten des Ports in der lokalen Instanz fest.

Mögliche Werte:

- `0..200000000` (Voreinstellung: `0`)
  Mit dem Wert `0` ermittelt das Gerät automatisch die Pfadkosten in Abhängigkeit von der Datenrate des Ports.

Port-Priorität

Legt die Priorität des Ports in der lokalen Instanz fest.

Mögliche Werte:

- `16..240` in 16er-Schritten (Voreinstellung: `128`)

Empfangene Bridge-ID

Zeigt die Bridge-ID des Geräts, von dem dieser Port zuletzt eine STP-BPDU in der lokalen Instanz empfangen hat.

Empfangene Port-ID

Zeigt die Port-ID des Geräts, 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, 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, die der Port mit der Rolle *designated* senden würde.

Empfangene Port-Pfadkosten

Zeigt die Pfadkosten, 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, 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, die der Port mit der Rolle *designated* senden würde.

5.9.4 Link-Aggregation

[Switching > L2-Redundanz > Link-Aggregation]

Die Funktion *Link-Aggregation* ermöglicht Ihnen, mehrere parallele Links zu bündeln. Voraussetzung ist, dass die Links mit gleicher Geschwindigkeit und im Vollduplex-Modus arbeiten. Die Vorteile gegenüber herkömmlichen Verbindungen über eine Leitung sind die höhere Verfügbarkeit und eine höhere Übertragungsbandbreite.

Die Kriterien für die Verteilung der Last auf die parallelen Links basieren auf der Funktion *Hashing-Option*.

Das Link Aggregation Control Protocol (LACP) ermöglicht, den paketbasierten kontinuierlichen Link-Status auf den physischen Ports zu überwachen. LACP sorgt außerdem dafür, dass die Link-Partner die Voraussetzungen zum Bündeln erfüllen.

Wenn die Gegenstelle kein Link Aggregation Control Protocol (LACP) unterstützt, können Sie die Funktion *Statische Link-Aggregation* verwenden. In diesem Fall bündelt das Gerät die Links basierend auf Betriebsbereitschaft des Links, Verbindungsgeschwindigkeit und Duplexeinstellung.

Konfiguration

Hashing-Option

Legt fest, welche Informationen das Gerät berücksichtigt, um die Pakete auf die physischen Ports des LAG-Interfaces zu verteilen. Das Gerät sendet Pakete, die die gleichen verteilungsrelevanten Informationen enthalten, über denselben physischen Port, um die Paketreihenfolge beizubehalten.

Diese Einstellung überschreibt den in Spalte *Hashing-Option* für den Port festgelegten Wert.

Mögliche Werte:

- `sourceMacVlan`
  Das Gerät berücksichtigt die Paket-Felder `Quell-MAC-Adresse`, `VLAN-ID`, `EtherType` sowie den physischen Empfangs-Port.
- `destMacVlan`
  Das Gerät berücksichtigt die Paket-Felder `Ziel-MAC-Adresse`, `VLAN-ID`, `EtherType` sowie den physischen Empfangs-Port.
- `sourceDestMacVlan` (Voreinstellung)
  Das Gerät berücksichtigt die Paket-Felder `Quell-MAC-Adresse`, `Ziel-MAC-Adresse`, `VLAN-ID`, `EtherType` sowie den physischen Empfangs-Port.
- `sourceIPsourcePort`
  Das Gerät berücksichtigt die Paket-Felder `Quell-IP-Adresse` und `Quell-TCP/UDP-Port`.
- `destIPdestPort`
  Das Gerät berücksichtigt die Paket-Felder `Ziel-IP-Adresse` und `Ziel-TCP/UDP-Port`.
- `sourceDestIPPort`
  Das Gerät berücksichtigt die Paket-Felder `Quell-IP-Adresse`,`Ziel-IP-Adresse`, `Quell-TCP/UDP-Port` und `Ziel-TCP/UDP-Port`.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Erzeugen

Öffnet das Fenster *Erzeugen*, um ein LAG-Interface hinzuzufügen oder einem LAG-Interface einen physischen Port zuzuweisen.

- In der Dropdown-Liste *Trunk-Port* wählen Sie die Nummer des LAG-Interfaces.
- In der Dropdown-Liste *Port* wählen Sie die Nummer des physischen Ports, den Sie dem LAG-Interface zuweisen möchten.

Nach Erzeugen eines LAG-Interfaces fügt das Gerät das LAG-Interface der Tabelle im Dialog *Grundeinstellungen > Port*, Registerkarte *Statistiken* hinzu.

Trunk-Port

Zeigt die Nummer des LAG-Interfaces.

Name

Legt den Namen des LAG-Interfaces fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..15 Zeichen

Link/Status

Zeigt den gegenwärtigen Betriebszustand des LAG-Interfaces und der physischen Ports.

Mögliche Werte:

- `up` (Zeile `lag/…`)
  Das LAG-Interface ist in Betrieb.
  Die Voraussetzungen sind:
  - Die Funktion *Statische Link-Aggregation* ist auf diesem LAG-Interface aktiv.
    oder
  - LACP ist auf den physischen Ports aktiv, die dem LAG-Interface zugewiesen sind, siehe Spalte *LACP Aktiv*.
    und
    Der in Spalte *LACP admin key* festgelegte Schlüssel für das LAG-Interface ist identisch mit den in Spalte *LACP port actor admin key* festgelegten Schlüsseln für die physischen Ports.
    und
    Die Anzahl der sich in Betrieb befindenden physischen Ports, die dem LAG-Interface zugewiesen sind, ist größer oder gleich dem in Spalte *Aktive Ports (min.)* festgelegten Wert.
- `up`
  Der physische Port ist in Betrieb.
- `down` (Zeile `lag/…`)
  Das LAG-Interface ist außer Betrieb.
- `down`
  Der physische Port ist ausgeschaltet.
  oder
  Kein Kabel angesteckt oder kein aktiver Link.

Aktiv

Aktiviert/deaktiviert das LAG-Interface.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das LAG-Interface ist aktiv.
  Berücksichtigen Sie, dass auf den physischen Ports die folgenden Protokolle nicht ordnungsgemäß funktionieren, wenn Sie das LAG-Interface aktivieren.
  – *PTP*
- `unmarkiert`
  Das LAG-Interface ist inaktiv.

STP aktiv

Aktiviert/deaktiviert das *Spanning Tree*-Protokoll auf diesem LAG-Interface. Voraussetzung ist, dass Sie die Funktion *Spanning Tree* global im Dialog *Switching > L2-Redundanz > Spanning Tree > Global* einschalten.

Das *Spanning Tree*-Protokoll können Sie auch im Dialog *Switching > L2-Redundanz > Spanning Tree > Port* auf den LAG-Interfaces aktivieren/deaktivieren.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Protokoll *Spanning Tree* ist auf diesem LAG-Interface aktiv.
- `unmarkiert`
  Die Protokoll *Spanning Tree* ist auf diesem LAG-Interface inaktiv.

Statische Link-Aggregation

Aktiviert/deaktiviert die Funktion *Statische Link-Aggregation* auf dem LAG-Interface. Das Gerät bindet die zugewiesenen physischen Ports in das LAG-Interface ein, auch wenn die Gegenstelle LACP nicht unterstützt.

Mögliche Werte:

- `markiert`
  Die Funktion *Statische Link-Aggregation* ist auf diesem LAG-Interface aktiv. Das Gerät bindet einen zugewiesenen physischen Port in das LAG-Interface ein, sobald der physische Port einen Link aufbaut. Das Gerät sendet keine LACPDUs und verwirft empfangene LACPDUs.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Statische Link-Aggregation* ist auf diesem LAG-Interface inaktiv. Wenn die Verbindung zuvor erfolgreich mit LACP ausgehandelt wurde, bindet das Gerät einen zugewiesenen physischen Port in das LAG-Interface ein.

Hashing-Option

Legt fest, welche Informationen das Gerät berücksichtigt, um die Pakete auf die einzelnen physischen Ports des LAG-Interfaces zu verteilen. Diese Einstellung hat Vorrang vor dem Wert, der im Rahmen *Konfiguration*, Dropdown-Liste *Hashing-Option* ausgewählt ist.

Für weitere Informationen zu den Werten siehe Beschreibung der Dropdown-Liste *Hashing-Option* im Ramen *Konfiguration*.

MTU

Legt die auf dem LAG-Interface maximal zulässige Größe der Ethernet-Pakete in Byte fest. Ein vorhandenes VLAN-Tag wird nicht berücksichtigt.

Diese Einstellung ermöglicht Ihnen, für bestimmte Anwendungen die Ethernet-Pakete zu erhöhen.

Mögliche Werte:

- `1518..12288` (Voreinstellung: `1518`)
  Mit dem Wert `1518` überträgt das LAG-Interface Ethernet-Pakete bis einschließlich folgender Größe:
  - 1518 Byte ohne VLAN-Tag
    (1514 Byte + 4 Byte CRC)
  - 1522 Byte mit VLAN-Tag
    (1518 Byte + 4 Byte CRC)

Aktive Ports (min.)

Legt fest, wie viele physische Ports mindestens aktiv sein müssen, damit das LAG-Interface aktiv ist. Wenn die Anzahl der aktiven physischen Ports kleiner ist als der festgelegte Wert, dann deaktiviert das Gerät das LAG-Interface.

Mit dieser Funktion erzwingen Sie, dass das Gerät automatisch auf die redundante Leitung umschaltet, wenn im Gerät eine Redundanzfunktion wie *Spanning Tree* oder *MRP* over LAG aktiv ist.

Mögliche Werte:

- `1` (Voreinstellung)
- `2`
- Abhängig von der Hardware:
  `4`
  `8`
  `32`

Typ

Zeigt, ob das LAG-Interface mit der Funktion *Statische Link-Aggregation* oder mit LACP arbeitet.

Mögliche Werte:

- *`statisch`*
  Das LAG-Interface arbeitet mit der Funktion *Statische Link-Aggregation*.
- *`dynamisch`*
  Das LAG-Interface arbeitet mit der Funktion LACP.

Trap senden (Link-Up/Down)

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung des Link-Status auf diesem Interface erkennt.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv.
  Wenn das Gerät eine Link-Status-Änderung erkennt, sendet es einen SNMP-Trap.
- `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 ein Trap-Ziel festlegen.

LACP admin key

Legt den Schlüssel des LAG-Interfaces fest. Das Gerät verwendet den Schlüssel, um diejenigen Ports zu identifizieren, die es in das LAG-Interface einbinden darf.

Mögliche Werte:

- `0..65535`
  Den korrespondierenden Wert für die physischen Ports legen Sie in Spalte *LACP port actor admin key* fest.

Port

Zeigt die Nummer der physischen Ports, die dem LAG-Interface zugewiesen sind.

Aggregation Port Status

Zeigt, ob das LAG-Interface den physischen Port eingebunden hat.

Mögliche Werte:

- *aktiv*
  Das LAG-Interface hat den physischen Port eingebunden.
- *inaktiv*
  Das LAG-Interface hat den physischen Port nicht eingebunden.

LACP Aktiv

Aktiviert/deaktiviert LACP auf dem physischen Port.

Mögliche Werte:

- `markiert` (Voreinstellung)
  LACP ist auf dem physischen Port aktiv.
- `unmarkiert`
  LACP ist auf dem physischen Port inaktiv.

LACP port actor admin key

Legt den Schlüssel des physischen Ports fest. Das Gerät verwendet den Schlüssel, um diejenigen Ports zu identifizieren, die es in das LAG-Interface einbinden darf.

Mögliche Werte:

- `0`
  Das Gerät ignoriert den Schlüssel auf diesem physischen Port bei der Entscheidung, den Port in das LAG-Interface einzubinden.
- `1..65535`
  Das Gerät bindet diesen physischen Port ausschließlich dann in das LAG-Interface ein, wenn der Wert mit dem in Spalte *LACP admin key* für das LAG-Interface festgelegten Wert übereinstimmt.

LACP actor admin state

Legt die Statuswerte des Aktors fest, die das LAG-Interface in den LACPDUs vermittelt. Dies ermöglicht Ihnen, die LACPDU-Parameter zu verwalten.

Das Gerät ermöglicht Ihnen, die Werte zu kombinieren. Wählen Sie in der Dropdown-Liste einen oder mehrere Werte.

Mögliche Werte:

- *ACT*
  (Status `LACP_Activity`)
  Wenn ausgewählt, vermittelt der Link die LACPDUs zyklisch, andernfalls bei Bedarf.
- *STO*
  (Status `LACP_Timeout`)
  Wenn ausgewählt, vermittelt der Link die LACPDUs zyklisch mit kurzem Timeout, andernfalls mit langem Timeout.
- *AGG*
  (Status `Aggregation`)
  Wenn ausgewählt, wertet das Gerät den Link als einbindbar, andernfalls als einzelnen Link.

Für weitere Informationen zu den Werten siehe Norm IEEE 802.1AX-2014.

LACP actor oper state

Zeigt die Statuswerte des Aktors, die das LAG-Interface in den LACPDUs vermittelt.

Mögliche Werte:

- *ACT*
  (Status `LACP_Activity`)
  Wenn sichtbar, vermittelt der Link die LACPDUs zyklisch, andernfalls bei Bedarf.
- *STO*
  (Status `LACP_Timeout`)
  Wenn sichtbar, vermittelt der Link die LACPDUs zyklisch mit kurzem Timeout, andernfalls mit langem Timeout.
- *AGG*
  (Status `Aggregation`)
  Wenn sichtbar, wertet das Gerät den Link als einbindbar, andernfalls als einzelnen Link.
- *SYN*
  (Status `Synchronization`)
  Wenn sichtbar, wertet das Gerät den Link als `IN_SYNC`, andernfalls als `OUT_OF_SYNC`.
- *COL*
  (Status `Collecting`)
  Wenn sichtbar, ist das Erfassen ankommender Frames auf diesem Link eingeschaltet, andernfalls ausgeschaltet.
- *DST*
  (Status `Distributing`)
  Wenn sichtbar, ist das Verteilen der zu sendenden Frames auf diesem Link eingeschaltet, andernfalls ausgeschaltet.
- *DFT*
  (Status `Defaulted`)
  Wenn sichtbar, verwendet der Link voreingestellte Informationen für den Betrieb, die administrativ für den Partner festgelegt sind. Andernfalls verwendet der Link die in einer LACPDU empfangenen Informationen für den Betrieb.
- *EXP*
  (Status `Expired`)
  Wenn sichtbar, befindet sich der Link-Empfänger im Zustand `EXPIRED`.

LACP partner oper SysID

Zeigt die MAC-Adresse des entfernten Geräts, das mit diesem physischen Port verbunden ist.

Das LAG-Interface hat diese Informationen in einer LACPDU vom Partner empfangen.

LACP partner oper port

Zeigt die Port-Nummer des entfernten Geräts, das mit diesem physischen Port verbunden ist.

Das LAG-Interface hat diese Informationen in einer LACPDU vom Partner empfangen.

LACP partner oper port state

Zeigt die Statuswerte des Partners, die das LAG-Interface in den LACPDUs empfängt.

Mögliche Werte:

- *ACT*
- *STO*
- *AGG*
- *SYN*
- *COL*
- *DST*
- *DFT*
- *EXP*

Für weitere Informationen zu den Werten siehe Beschreibung der Spalte *LACP actor oper state* und Norm IEEE 802.1AX-2014.

5.9.5 Link-Backup

[Switching > L2-Redundanz > 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 auf dem primären Port ermittelt, nutzt die Link-Backup-Funktion den Backup-Port zur Vermittlung der Daten.

Der Dialog ermöglicht Ihnen außerdem, 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 auf dem Backup-Port und leitet dann Daten an den primären Port weiter. Dieses Verfahren hilft zu verhindern, dass das Gerät Loops im Netz verursacht.

Funktion

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 auf dem 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*
  Auf dem 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.

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*
  Auf dem 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.

Erzeugen

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

Backup-Port

Legt den Backup-Port fest, an den das Gerät die Daten vermittelt, wenn es auf dem primären Port einen Fehler ermittelt.

Mögliche Werte:

- Physikalische Ports außer dem Port, den Sie als primären Port festlegen.

5.9.6 FuseNet

[Switching > L2-Redundanz > FuseNet]

Die *FuseNet*-Protokolle ermöglichen Ihnen, Ringe zu koppeln, die mit einem der folgenden Redundanzprotokolle arbeiten:

- MRP
- HIPER Ring
- RSTP

Anmerkung: Wenn Sie das Protokoll *Ring-/Netzkopplung* verwenden, um Netze zu koppeln, dann vergewissern Sie sich, dass die Netze ausschließlich Hirschmann-Geräte enthalten.

Verwenden Sie die folgende Tabelle, um das *FuseNet*-Kopplungs-Protokoll auszuwählen, das in Ihrem Netz zum Einsatz kommt:

Haupt-Ring	Verbundenes Netz		
	MRP	HIPER-Ring	RSTP
MRP	*Sub Ring*[1)]	*Redundant Coupling Protocol* *Ring-/Netzkopplung*	*Redundant Coupling Protocol* *Ring-/Netzkopplung*
HIPER-Ring	*Sub Ring*	*Ring-/Netzkopplung*	*Redundant Coupling Protocol* *Ring-/Netzkopplung*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	–

– kein geeignetes Kopplungs-Protokoll

1) mit *MRP* eingerichtet an unterschiedlichen VLANs

Das Menü enthält die folgenden Dialoge:

- Sub Ring
- Ring-/Netzkopplung
- Redundant Coupling Protocol

5.9.6.1 Sub Ring

[Switching > L2-Redundanz > FuseNet > Sub Ring]

Dieser Dialog ermöglicht Ihnen, das Gerät als Subring-Manager einzurichten.

Die Funktion *Sub Ring* ermöglicht Ihnen eine einfache Ankopplung von Netzsegmenten an bestehende Redundanz-Ringe. Der Subring-Manager (SRM) koppelt einen Subring an einen vorhandenen Ring (Base-Ring).

Im Subring können Sie beliebige Geräte, die MRP unterstützen, als Ring-Teilnehmer verwenden. Diese Geräte benötigen keine Subring-Manager-Funktion.

Berücksichtigen Sie beim Einrichten von Subringen folgende Regeln:
- Das Gerät unterstützt *Link-Aggregation* im Subring
- Kein Spanning Tree auf Subring-Ports
- Gleiche *MRP-Domäne* auf Geräten innerhalb eines Subrings
- Unterschiedliche VLANs für Base-Ring und Subring

Legen Sie die VLAN-Einstellungen wie folgt fest:
- VLAN `X` für Base-Ring
  - auf den Ring-Ports der Base-Ring-Teilnehmer
  - auf den Base-Ring-Ports des Subring-Managers
- VLAN `Y` für Subring
  - auf den Ring-Ports der Subring-Teilnehmer
  - auf den Subring-Ports des Subring-Managers

Anmerkung: Um Loops zu vermeiden, schließen Sie die redundante Strecke erst dann, wenn in jedem am Ring beteiligten Gerät die Einstellungen festgelegt sind.

Funktion

Funktion

Schaltet die Funktion *Sub Ring* ein/aus.

Mögliche Werte:
- `An`
  Die Funktion *Sub Ring* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *Sub Ring* ist ausgeschaltet.

Information

Tabelleneinträge (max.)

Zeigt die maximale Anzahl an Subringen, die das Gerät unterstützt.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Sub-Ring-ID

Zeigt die eindeutige Kennung des Subrings.

Mögliche Werte:

- `1..8`

Name

Legt den Namen des Subringes fest (optional).

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Aktiv

Aktiviert/deaktiviert den Subring.

Aktivieren Sie den Subring, wenn die Konfiguration jedes Geräts des Subringes abgeschlossen ist. Schließen Sie den Subring erst, nachdem Sie die Funktion *Sub Ring* aktiviert haben.

Mögliche Werte:

- `markiert`
  Der Subring ist aktiviert.
- `unmarkiert` (Voreinstellung)
  Der Subring ist inaktiv.

Konfigurations-Status

Zeigt den Betriebszustand der Subring-Konfiguration.

Mögliche Werte:

- *`noError`*
  Das Gerät erkennt eine geeignete Subring-Konfiguration.
- *`ringPortLinkError`*
  - Der Ring-Port hat keine Datenverbindung.
  - Eine der Subring-Leitungen ist verbunden mit einem weiteren Anschluss des Geräts. Jedoch ist die Subring-Leitung nicht verbunden mit einem der Ringports des Geräts.
- *`multipleSRM`*
  Der Subring-Manager empfängt Datenpakete von mehr als einem Subring-Manager im Subring.
- *`noPartnerManager`*
  Der Subring-Manager empfängt seine eigenen Datenpakete.
- *`concurrentVLAN`*
  Das MRP-Protokoll im Basis-Ring verwendet das VLAN der Subring-Manager-Domäne.
- *`concurrentPort`*
  Ein weiteres Redundanzprotokoll verwendet den Ring-Port der Subring-Manager-Domäne.
- *`concurrentRedundancy`*
  Die Subring-Manager-Domäne ist inaktiv aufgrund eines weiteren aktiven Redundanzprotokolls.

- `trunkMember`
  Der Ring-Port der Subring-Manager-Domäne ist Mitglied einer *Link-Aggregation*-Verbindung.
- `sharedVLAN`
  Die Subring-Manager-Domäne ist inaktiv, weil Shared-VLAN aktiv ist und der Hauptring außerdem das MRP-Protokoll verwendet.

Redundanz verfügbar

Zeigt den Betriebszustand der Ring-Redundanz im Subring.

Mögliche Werte:

- `redGuaranteed`
  Die Redundanz-Reserve ist verfügbar.
- `redNotGuaranteed`
  Verlust der Redundanz-Reserve.

Port

Legt den Port fest, der das Gerät mit dem Subring verbindet.

Mögliche Werte:

- `<Port-Nummer>`

SRM-Modus

Legt den Modus des Subring-Managers fest.

Ein Subring hat 2 Manager gleichzeitig, die den Subring an den Base-Ring koppeln. So lange der Subring physikalisch geschlossen ist, blockiert ein Manager seinen Subring-Port.

Mögliche Werte:

- `manager` (Voreinstellung)
  Der Subring-Port vermittelt Datenpakete.
  Wenn dieser Wert auf beiden Geräten, die den Subring an den Base-Ring koppeln, eingestellt ist, arbeitet das Gerät mit der höheren MAC-Adresse als `redundantManager`.
- `redundantManager`
  Der Subring-Port ist blockiert, so lange der Subring physikalisch geschlossen ist. Bei einer Unterbrechung des Subrings vermittelt der Subring-Port die Datenpakete.
  Wenn dieser Wert auf beiden Geräten, die den Subring an den Base-Ring koppeln, eingestellt ist, arbeitet das Gerät mit der höheren MAC-Adresse als `redundantManager`.
- `singleManager`
  Verwenden Sie diesen Wert, wenn der Subring über ein einziges Gerät an den Base-Ring gekoppelt ist. Voraussetzung sind 2 Instanzen des Subrings in der Tabelle. Weisen Sie diesen Wert beiden Instanzen zu. Der Subring-Port der Instanz mit der höheren Port-Nummer ist blockiert, so lange der Subring physikalisch geschlossen ist.

SRM-Status

Zeigt den gegenwärtigen Modus des Subring-Managers.

Mögliche Werte:

- `manager`
  Der Subring-Port vermittelt Datenpakete.

- *redundantManager*
  Der Subring-Port ist blockiert, so lange der Subring physikalisch geschlossen ist. Bei einer Unterbrechung des Subrings vermittelt der Subring-Port die Datenpakete.
- *singleManager*
  Der Subring ist über ein einziges Gerät an den Base-Ring gekoppelt. Der Subring-Port der Instanz mit der höheren Port-Nummer ist blockiert, so lange der Subring physikalisch geschlossen ist.
- *disabled*
  Der Subring ist inaktiv.

Status Port

Zeigt den Verbindungsstatus des Subring-Ports.

Mögliche Werte:

- *forwarding*
  Der Port leitet Datenpakete gemäß IEEE 802.1D weiter.
- *disabled*
  Der Port verwirft jedes Datenpaket.
- *blocked*
  Der Port verwirft jedes Datenpaket außer in den folgenden Fällen.
  - Der Port leitet Datenpakete weiter, die vom festgelegten Ring-Protokoll verwendet werden und für die das Passieren von blockierten Ports zugelassen ist.
  - Der Port leitet Datenpakete von anderen Protokollen weiter, für die das Passieren von blockierten Ports zugelassen ist.
- *nicht verbunden*
  Die Datenverbindung auf dem Port ist unterbrochen.

VLAN

Legt das VLAN fest, dem dieser Subring zugewiesen ist. Wenn kein VLAN mit der festgelegten VLAN-ID existiert, dann erstellt das Gerät dieses automatisch.

Mögliche Werte:

- Verfügbare eingerichtete VLANs (Voreinstellung: 0)
  Wenn Sie für diesen Subring kein eigenständiges VLAN benutzen möchten, dann lassen Sie den Eintrag auf „0“.

Partner-MAC

Zeigt die MAC-Adresse des Subring-Managers am anderen Ende des Subringes.

MRP-Domäne

Legt die MRP-Domäne des Subring-Managers fest. Weisen Sie jedem Mitglied im Subring denselben MRP-Domänen-Namen zu. Wenn Sie ausschließlich Hirschmann-Geräte verwenden, übernehmen Sie den voreingestellten Wert für die MRP-Domäne; andernfalls passen Sie diesen Wert gegebenenfalls an. Bei mehreren Subringen ermöglicht Ihnen diese Funktion, für die Subringe dieselbe MRP-Domänen-Bezeichnung zu verwenden.

Mögliche Werte:

- Erlaubte MRP-Domänen-Bezeichnungen (Voreinstellung: `255.255.255.255.255.255.255.255.255.255.255.255.255.255.255.255`)

Protokoll

Legt das Protokoll fest.

Mögliche Werte:

- *`iec-62439-mrp`*

5.9.6.2 Ring-/Netzkopplung

[Switching > L2-Redundanz > FuseNet > Ring-/Netzkopplung]

Verwenden Sie die Funktion *Ring-/Netzkopplung*, um einen vorhandenen HIPER-, MRP- oder Fast HIPER-Ring an ein weiteres Netz oder an einen Ring redundant zu koppeln. Vergewissern Sie sich, dass die Kopplungspartner Hirschmann-Geräte sind.

Anmerkung: Vergewissern Sie sich bei der 2-Switch-Kopplung vor der Konfiguration der *Ring-/Netzkopplung*, dass Sie einen HIPER-Ring, einen MRP-Ring oder einen Fast-HIPER-Ring konfiguriert haben.

Im Dialog *Ring-/Netzkopplung* können Sie die folgenden Aufgaben ausführen:
- Übersicht über die bestehende *Ring-/Netzkopplung*anzeigen
- *Ring-/Netzkopplung*konfigurieren
- neue *Ring-/Netzkopplung*erzeugen.
- *Ring-/Netzkopplung*löschen
- *Ring-/Netzkopplung*aktivieren/deaktivieren

Legen Sie bei der Konfiguration der Kopplungsports die folgenden Einstellungen im Dialog *Grundeinstellungen > Port* fest.

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optical	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optical	1 Gbit/s	`markiert`	`markiert`	–

Anmerkung: Die tatsächlich zur Verfügung stehenden Betriebsmodi des Ports sind abhängig von der Ausstattung des Geräts und vom verwendeten Modul.

Haben Sie VLANs konfiguriert, beachten Sie die VLAN-Konfiguration der Kopplungs- und Partner-Kopplungsports. In der *Ring-/Netzkopplung*-Konfiguration wählen Sie für Kopplungs- und Partner-Kopplungsports die folgenden Werte:
- `VLAN ID 1` und *Ingress-Filtering* in der Port-Tabelle deaktiviert
- VLAN-Mitgliedschaft `T` in der Tabelle *VLAN Konfiguration*

Unabhängig von den VLAN-Einstellungen sendet das Gerät die Ring-Kopplungs-Frames mit `VLAN ID 1` und Priorität `7`. Vergewissern Sie sich, dass das Gerät VLAN-1-Datenpakete im lokalen Ring und im angeschlossenen Netz mit einem VLAN-Tag markiert vermittelt. Durch das Tagging der VLAN- Datenpakete bleibt die Priorität der Ring-Kopplungs-Frames erhalten.

Die Funktion *Ring-/Netzkopplung* arbeitet mit Test-Datenpaketen. Die Geräte senden ihre Test-Datenpakete mit VLAN-Tag, einschließlich VLAN-ID `1` und der höchsten VLAN-Priorität `7`. Wenn der weiterleitende Port Mitglied in VLAN `1` ist und die Datenpakete ohne VLAN-Tag vermittelt, dann sendet das Gerät ebenfalls Test-Pakete.

Funktion

Schaltflächen

Zurücksetzen

Deaktiviert die Redundanzfunktion und setzt die Parameter im Dialog auf die voreingestellten Werte zurück.

Funktion

Schaltet die Funktion *Ring-/Netzkopplung* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *Ring-/Netzkopplung* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *Ring-/Netzkopplung* ist ausgeschaltet.

Information

Redundanz verfügbar

Zeigt, ob die Redundanz verfügbar ist.

Fällt eine Komponente des Rings aus, übernimmt die redundante Strecke deren Funktion.

Mögliche Werte:

- `redGuaranteed`
  Redundanz ist verfügbar.
- `redNotGuaranteed`
  Keine Redundanz verfügbar.

Konfigurationsfehler

Sie haben die Funktion falsch konfiguriert oder die Ring-Port-Verbindung ist nicht vorhanden.

Mögliche Werte:

- `noError`
- `slaveCouplingLinkError`
  Die Kopplungs-Leitung ist nicht verbunden mit dem Kopplungs-Port des Slave-Geräts. Stattdessen ist die Kopplungs-Leitung mit einem anderen Port des Slave-Geräts verbunden.
- `slaveControlLinkError`
  Der Steuer-Port des Slave-Geräts hat keine Datenverbindung.
- `masterControlLinkError`
  Die Steuer-Leitung ist nicht verbunden mit dem Steuer-Port des Master-Geräts. Stattdessen ist die Steuer-Leitung mit einem anderen Port des Master-Geräts verbunden.
- `twoSlaves`
  Die Steuer-Leitung verbindet zwei Slave-Geräte.

- `localPartnerLinkError`
  Die Partner-Kopplungs-Leitung ist nicht verbunden mit dem Partner-Kopplungs-Port des Slave-Geräts. Stattdessen ist die Partner-Kopplungs-Leitung im `Ein-Switch-Kopplung`-Modus mit einem anderen Port des Slave-Geräts verbunden.
- `localInvalidCouplingPort`
  Im `Ein-Switch-Kopplung`-Modus ist die Kopplungs-Leitung nicht mit dem selben Gerät verbunden wie die Partner-Leitung. Stattdessen ist die Kopplungs-Leitung mit einem anderen Gerät verbunden.
- `couplingPortNotAvailable`
  Der Kopplungs-Port ist nicht verfügbar, da das Modul nicht verfügbar ist, zu welchem der Port gehört, oder der Port auf diesem Modul nicht vorhanden ist.
- `controlPortNotAvailable`
  Der Steuer-Port ist nicht verfügbar, da das Modul nicht verfügbar ist, zu welchem der Port gehört, oder der Port auf diesem Modul nicht vorhanden ist.
- `partnerPortNotAvailable`
  Der Partner-Kopplungs-Port ist nicht verfügbar, da das Modul nicht verfügbar ist, zu welchem der Port gehört, oder der Port auf diesem Modul nicht vorhanden ist.

Modus

Typ

Legt die für die Kopplung von Netzen verwendete Methode fest.

Mögliche Werte:

- `Ein-Switch-Kopplung`
  Ermöglicht Ihnen, die Port-Einstellungen in den Rahmen *Kopplungs-Port* und *Partner-Kopplungs-Port* festzulegen.
- `Zwei-Switch-Kopplung, Master`
  Ermöglicht Ihnen, die Port-Einstellungen im Rahmen *Kopplungs-Port* festzulegen.
- `Zwei-Switch-Kopplung, Slave`
  Ermöglicht Ihnen, die Port-Einstellungen im Rahmen *Kopplungs-Port* festzulegen.
- `Zwei-Switch-Kopplung mit Steuer-Leitung, Master`
  Ermöglicht Ihnen, die Port-Einstellungen in den Rahmen *Kopplungs-Port* und *Steuer-Port* festzulegen.
- `Zwei-Switch-Kopplung mit Steuer-Leitung, Slave`
  Ermöglicht Ihnen, die Port-Einstellungen in den Rahmen *Kopplungs-Port* und *Steuer-Port* festzulegen.

Kopplungs-Port

Port

Legt den Port fest, über den Sie die Redundanzverbindung herstellen.

Mögliche Werte:

- `-`
  Kein Port ausgewählt.
- `<Port-Nummer>`

Wenn Sie auch Ring-Ports konfiguriert haben, dann verwenden Sie für Kopplungs- und Ring-Ports unterschiedliche Ports.

Um Loops zu vermeiden, schaltet das Gerät den Kopplungs-Ports in den folgenden Fällen aus:

- bei Deaktivierung der Funktion
- bei Änderung der Konfiguration, während die Datenverbindungen an den Ports aktiv sind

Wenn das Gerät den Kopplungs-Port deaktiviert hat, ist im Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration* das Kontrollkästchen *Port an* unmarkiert.

Zustand

Zeigt den Status des ausgewählten Ports.

Mögliche Werte:

- `aktiv`
  Der Port ist aktiv.
- `standby`
  Der Port befindet sich im Standby-Modus.
- `nicht verbunden`
  Der Port ist nicht verbunden.
- `unzutreffend`
  Der Port ist mit dem konfigurierten Steuerungsmodus inkompatibel.

Partner-Kopplungs-Port

Port

Legt den Port fest, mit dem Sie den Partner-Port verbinden.

Mögliche Werte:

- `-`
  Kein Port ausgewählt.
- `<Port-Nummer>`

Wenn Sie auch Ring-Ports konfiguriert haben, dann verwenden Sie für Kopplungs- und Ring-Ports unterschiedliche Ports.

Zustand

Zeigt den Status des ausgewählten Ports.

Mögliche Werte:

- `aktiv`
  Der Port ist aktiv.
- `standby`
  Der Port befindet sich im Standby-Modus.
- `nicht verbunden`
  Der Port ist nicht verbunden.
- `unzutreffend`
  Der Port ist mit dem konfigurierten Steuerungsmodus inkompatibel.

IP-Adresse

Zeigt die IP-Adresse des Partnergeräts, wenn die Geräte verbunden sind.

Voraussetzung ist, dass Sie eine 2-Switch-Kopplungs-Methode auswählen und den Partner im Netz einschalten.

Steuer-Port

Port

Zeigt den Port, an dem Sie die Steuer-Leitung anschließen.

Mögliche Werte:

- `-`
  Kein Port ausgewählt.
- `<Port-Nummer>`

Zustand

Zeigt den Status des ausgewählten Ports.

Mögliche Werte:

- *`aktiv`*
  Der Port ist aktiv.
- *`standby`*
  Der Port befindet sich im Standby-Modus.
- *`nicht verbunden`*
  Der Port ist nicht verbunden.
- *`unzutreffend`*
  Der Port ist mit dem konfigurierten Steuerungsmodus inkompatibel.

Konfiguration

Redundanz-Modus

Aktiviert/deaktiviert das Gerät, damit das Gerät auf einen Ausfall des Remote-Rings oder des Netzes reagiert.

Mögliche Werte:

- *`Redundante Ring-/Netz-Kopplung`*
  Entweder die Hauptleitung oder die redundante Leitung ist aktiv. Niemals sind beide Leitungen gleichzeitig aktiv. Wenn das Gerät erkennt, dass zwischen den Geräten im angeschlossenen Netz keine Verbindung besteht, behält das Standby-Gerät den Standby-Modus des redundanten Ports bei.
- *`Erweiterte Redundanz`*
  Die Hauptleitung und die redundante Leitung sind gleichzeitig aktiv. Erkennt das Gerät ein Problem in Bezug auf die Datenverbindung zwischen den Geräten im angeschlossenen Netz, leitet das Standby-Gerät die Daten auf dem redundanten Port weiter. Mit dieser Einstellung können Sie die Kontinuität im Remote-Netz sicherstellen.

Anmerkung: Während der Rekonfigurationszeit können Datenpaket-Doppelungen auftreten. Daher können Sie diese Einstellung auswählen, wenn Ihre Anwendung in der Lage ist, Datenpaket-Dopplungen zu erkennen.

Kopplungs-Modus

Die Einstellungen in diesem Rahmen bieten Ihnen die Möglichkeit, einen spezifischen Netztyp zu koppeln.

Mögliche Werte:

- *Ring-Kopplung*
  Das Gerät koppelt redundante Ringe. Das Gerät ermöglicht Ihnen, Ringe zu koppeln, welche die folgenden Redundanzprotokolle verwenden:
  - HIPER-Ring
  - Fast HIPER-Ring
  - MRP-Ring
- *Netz-Kopplung*
  Das Gerät koppelt Netzsegmente. Die Funktion ermöglicht Ihnen, Mesh- und Bus-Netze miteinander zu koppeln.

5.9.6.3 Redundant Coupling Protocol

[Switching > L2-Redundanz > FuseNet > RCP]

Eine Ringtopologie bietet kurze Übergangszeiten bei minimalem Ressourceneinsatz. Allerdings ist es eine Herausforderung, die Ringe redundant an ein übergeordnetes Netz zu koppeln.

Wenn Sie ein Standardprotokoll, zum Beispiel MRP für die Ringredundanz und RSTP zum Koppeln der Ringe verwenden möchten, bietet Ihnen das *Redundant Coupling Protocol* die entsprechenden Optionen.

Verwenden Sie keines der folgenden Redundanzprotokolle auf den Ports des *RCP*-Primär-Rings und der *RCP*-Sekundär-Ringe:

- *Sub Ring*
- *Ring-/Netzkopplung*

Funktion

Funktion

Schaltet die Funktion *RCP* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *RCP* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *RCP* ist ausgeschaltet.

Primärer Ring/Netzwerk / Sekundärer Ring/Netzwerk

Wenn das Gerät als Slave arbeitet (Wert im *Rolle*-Feld ist `slave`), dann aktivieren Sie nicht den *Static-Query-Port*-Modus für die Ports im Sekundär-Ring/Netz.

Innerer Port

Legt die Nummer des inneren Ports im Primär-/Sekundär-Ring fest. Dieser Port ist direkt mit der Partner-Bridge verbunden.

Mögliche Werte:

- `-` (Voreinstellung)
  Kein Port ausgewählt.
- `<Port-Nummer>`

Äußerer Port

Legt die Nummer des äußeren Ports im Primär-/Sekundär-Ring fest.

Mögliche Werte:

- `-` (Voreinstellung)
  Kein Port ausgewählt.
- `<Port-Nummer>`

Protokoll Primärer Ring/Protokoll Sekundärer Ring

Zeigt das Protokoll, das auf dem redundanten Kopplungs-Port in den Geräten im primären/sekundären Ring aktiv ist.

Koppler-Konfiguration

Rolle

Legt die Rolle des lokalen Geräts fest.

Mögliche Werte:

- `master`
  Das Gerät arbeitet als Master.
- `slave`
  Das Gerät arbeitet als Slave.
- `auto` (Voreinstellung)
  Das Gerät wählt automatisch seine Rolle als *master* oder *slave*.

Momentane Rolle

Zeigt die gegenwärtige Rolle des lokalen Geräts. Der Wert kann von der konfigurierten Rolle abweichen:

- Haben Sie beide Partner-Bridges als `auto` konfiguriert, übernimmt die Partner-Bridge, die gegenwärtig die Instanzen koppelt, die `master`-Rolle. Die andere Partner-Bridge übernimmt die `slave`-Rolle.
- Sind beide Partner-Bridges als `master` oder beide als `slave` konfiguriert, übernimmt die Partner-Bridge mit der kleineren Basis-MAC-Adresse die `master`-Rolle.
  Die andere Partner-Bridge übernimmt die `slave`-Rolle.
- Ist beim Aktivieren des Protokolls auf einer Bridge in der konfigurierten Rolle `master`, `slave` oder `auto` deren Partner-Bridge unauffindbar, setzt die Bridge ihre eigene Rolle auf `listening`.
- Wenn das Gerät ein Konfigurationsproblem feststellt, zum Beispiel wenn die inneren Ring-Ports über Kreuz verbunden sind, dann setzt das Gerät seine Rolle auf `error`.

Timeout [ms]

Legt die maximale Zeit in Millisekunden fest, während der das Slave-Gerät auf den äußeren Ports auf Testpakete vom Master-Gerät wartet, bevor das Slave-Gerät die Kopplung übernimmt. Dies gilt lediglich in dem Zustand, in dem beide inneren Ports des Slave-Geräts die Datenverbindung zum Master-Gerät verloren haben.

Konfigurieren Sie den Timeout länger als die längste anzunehmende Unterbrechungszeit des Redundanzprotokolls der schnelleren Instanz. Andernfalls können Loops auftreten.

Mögliche Werte:

- `5..60000` (Voreinstellung: `250`)

Partner MAC-Adresse

Zeigt die Basis-MAC-Adresse des Partnergeräts.

Partner IP-Adresse

Zeigt die IP-Adresse des Partnergeräts.

Kopplungs-Zustand

Zeigt den Koppungsstatus des lokalen Geräts.

Mögliche Werte:

- *forwarding*
  Der Port befindet sich im Kopplungsstatus „weiterleitend“.
- *blocking*
  Der Port befindet sich im Kopplungsstatus „blocking“.

Redundanz-Zustand

Zeigt, ob die Redundanz verfügbar ist.

Bei einer Master-Slave-Konfiguration zeigen beide Bridges diese Information an.

Mögliche Werte:

- *redAvailable*
  Redundanz ist verfügbar.
- *redNotAvailable*
  Keine Redundanz verfügbar.

6 Diagnose

Das Menü enthält die folgenden Dialoge:

- Statuskonfiguration
- System
- E-Mail-Benachrichtigung
- Syslog
- Ports
- Loop-Schutz
- LLDP
- SFlow
- Bericht

6.1 Statuskonfiguration

[Diagnose > Statuskonfiguration]

Das Menü enthält die folgenden Dialoge:

- Gerätestatus
- Sicherheitsstatus
- Signalkontakt
- MAC-Benachrichtigung
- Alarme (Traps)

6.1.1 Gerätestatus

[Diagnose > Statuskonfiguration > Gerätestatus]

Der Gerätestatus gibt einen Überblick über den Gesamtzustand des Geräts. Viele Prozessvisualisierungssysteme erfassen den Gerätestatus 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 anhand der einzelnen Überwachungsergebnisse.

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

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

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einer überwachten Funktion erkennt.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine 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 ein Trap-Ziel festlegen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Verbindungsfehler

Aktiviert/deaktiviert die Überwachung des Linkstatus 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.
  In der Registerkarte *Port* haben Sie die Möglichkeit, die zu überwachenden Ports/Interfaces einzeln auszuwählen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Temperatur

Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Wenn die Temperatur die festgelegten Schwellwerte überschreitet oder unterschreitet, wechselt der Wert im Rahmen *Geräte-Status* auf `error`.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Temperaturschwellwerte legen Sie fest im Dialog *Grundeinstellungen* > *System*, Feld *Obere Temp.-Grenze [°C]* und Feld *Untere Temp.-Grenze [°C]*.

Ethernet-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.

Den aktiven externen Speicher legen Sie fest im Dialog *Grundeinstellungen > Laden/Speichern*, Rahmen *Externer Speicher*.

Externer Speicher nicht synchron

Aktiviert/deaktiviert die Überwachung der Konfigurationsprofile im Gerät und im 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 im externen Speicher.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

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.

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.

Ethernet-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 *Ethernet-Modul entfernen* markieren.

[Port]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

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 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.

[Status]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

6.1.2 Sicherheitsstatus

[Diagnose > Statuskonfiguration > 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 anhand der einzelnen Überwachungsergebnisse.

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

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

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einer überwachten Funktion 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 ein Trap-Ziel festlegen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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*.

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 mindestens eine der folgenden Richtlinien 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 Funktion *Richtlinien überprüfen*.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn die Funktion *Richtlinien überprüfen* bei mindestens ein 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*.

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 Funktion *SNMPv1* ist eingeschaltet.
  - Die Funktion *SNMPv2* 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 serieller Schnittstelle möglich

Aktiviert/deaktiviert die Überwachung des System-Monitors.

Wenn der System-Monitor aktiviert ist, haben Sie die Möglichkeit, während des Starts des Geräts über eine serielle 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 im 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 im externen Speicher aktivieren/deaktivieren Sie im Dialog *Grundeinstellungen > Externer Speicher*.

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 Funktion HiDiscovery.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion HiDiscovery einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion HiDiscovery schalten Sie im Dialog *Grundeinstellungen > Netz > Global* ein/aus.

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 im externen Speicher gespeicherte Konfigurationsprofil ist unverschlüsselt.
    und
  - Die Spalte *Konfigurations-Priorität* im Dialog *Grundeinstellungen > Externer Speicher* hat den Wert `first` oder `second`.
- `unmarkiert`
  Die Überwachung ist inaktiv.

IEC61850-MMS aktiv

Aktiviert/deaktiviert die Überwachung der Funktion *IEC61850-MMS*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *IEC61850-MMS* einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion *IEC61850-MMS* schalten Sie im Dialog *Industrie-Protokolle > IEC61850-MMS*, 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.

Modbus TCP aktiv

Aktiviert/deaktiviert die Überwachung der Funktion *Modbus TCP*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *Modbus TCP* einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion *Modbus TCP* schalten Sie im Dialog *Erweitert > Industrie-Protokolle > Modbus TCP*, Rahmen *Funktion*ein/aus.

EtherNet/IP aktiv

Aktiviert/deaktiviert die Überwachung der Funktion *EtherNet/IP*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *EtherNet/IP* einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion *EtherNet/IP* schalten Sie im Dialog *Erweitert > Industrie-Protokolle > EtherNet/IP*, Rahmen *Funktion*ein/aus.

PROFINET aktiv

Aktiviert/deaktiviert die Überwachung der Funktion *PROFINET*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *PROFINET* einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion *PROFINET* schalten Sie im Dialog *Erweitert > Industrie-Protokolle > PROFINET*, Rahmen *Funktion*ein/aus.

[Port]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

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.

[Status]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

6.1.3 Signalkontakt

[Diagnose > Statuskonfiguration > Signalkontakt]

Der Signalkontakt ist ein potentialfreier Relaiskontakt. Das Gerät ermöglicht Ihnen damit eine 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

[Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 1]

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

Der Signalkontakt bietet Ihnen folgende Möglichkeiten:
- Funktionsüberwachung des Geräts.
- Signalisierung des Gerätestatus 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

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 Eintrag `Manuelle Einstellung` auswählen.

Mögliche Werte:

- `offen`
  Der Signalkontakt ist geöffnet.
- `geschlossen`
  Der Signalkontakt ist geschlossen.

Signalkontakt-Status

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

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an einer überwachten Funktion 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 ein 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.

Verbindungsfehler

Aktiviert/deaktiviert die Überwachung des Linkstatus auf dem Port/Interface.

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.

Temperatur

Aktiviert/deaktiviert die Überwachung der Temperatur im Gerät.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn die Temperatur die festgelegten Schwellwerte überschreitet oder unterschreitet.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Temperaturschwellwerte 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.

Ethernet-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.

Externer Speicher wurde entfernt

Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers.

Den aktiven externen Speicher legen Sie fest im Dialog *Grundeinstellungen > Laden/Speichern*, Rahmen *Externer Speicher*.

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 im 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 im externen Speicher.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Ethernet-Loops

Aktiviert/deaktiviert die Überwachung von Layer-2-Ethernet-Loops. Die Einstellungen der Funktion *Loop-Schutz* legen Sie im Dialog *Diagnose > Loop-Schutz* fest.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn das Gerät einen Ethernet-Loop feststellt.
- `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.

Ethernet-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 *Ethernet-Modul entfernen* markieren.

[Port]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

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.

[Status]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

6.1.4 MAC-Benachrichtigung

[Diagnose > Statuskonfiguration > MAC-Benachrichtigung]

Das Gerät ermöglicht Ihnen, 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 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

Funktion

Schaltet die Funktion *MAC-Benachrichtigung* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *MAC-Benachrichtigung* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *MAC-Benachrichtigung* ist ausgeschaltet.

Konfiguration

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: `1`)

Das Gerät erfasst vor dem Senden eines SNMP-Trap bis zu 20 MAC-Adressen. Wenn das Gerät sehr viele Änderungen erkennt, dann sendet es den SNMP-Trap bereits vor Ablauf des Sendeintervalls.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *MAC-Benachrichtigung* auf dem Port.

Mögliche Werte:

▶ `markiert`
Die Funktion *MAC-Benachrichtigung* 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 Funktion *MAC-Benachrichtigung* 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 ein Trap-Ziel festlegen.

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.

6.1.5 Alarme (Traps)

[Diagnose > Statuskonfiguration > Alarme (Traps)]

Das Gerät ermöglicht Ihnen, 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

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

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.

Löschen

Entfernt den ausgewählten Tabelleneintrag.

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.

6.2 System

[Diagnose > System]

Das Menü enthält die folgenden Dialoge:

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

6.2.1 Systeminformationen

[Diagnose > System > 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

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

[Diagnose > System > Hardware-Zustand]

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

Information

Betriebsstunden

Zeigt die Gesamtbetriebszeit des Geräts seit Lieferung.

Mögliche Werte:

- `..d ..h ..m ..s`
  Tag(e) Stunde(n) Minute(n) Sekunde(n)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

6.2.3 Konfigurations-Check

[Diagnose > System > Konfigurations-Check]

Das Gerät ermöglicht Ihnen, 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.

Wenn im Gerät mehr als 39 VLANs eingerichtet 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.

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.

Information

Wenn Sie die Schaltfläche im Banner klicken, zeigt ein Tooltip die Zusammenfassung der Informationen in diesem Rahmen.

Fehler

Zeigt, wie viele Abweichungen des Levels `ERROR` das Gerät beim Konfigurations-Check erkannt hat.

Warnung

Zeigt, wie viele Abweichungen des Levels `WARNING` das Gerät beim Konfigurations-Check erkannt hat.

Information

Zeigt, wie viele Abweichungen des Levels `INFORMATION` das Gerät beim Konfigurations-Check erkannt hat.

Tabelle

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

6.2.4 IP-Adressen Konflikterkennung

[Diagnose > System > IP-Adressen Konflikterkennung]

Mit der Funktion *IP-Adressen Konflikterkennung* 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.

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

Funktion

Funktion

Schaltet die Funktion *IP-Adressen Konflikterkennung* ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion *IP-Adressen Konflikterkennung* ist eingeschaltet.
  Das Gerät prüft, ob ein weiteres Gerät im Netz die eigene IP-Adresse verwendet.
- `Aus`
  Die Funktion *IP-Adressen Konflikterkennung* ist ausgeschaltet.

Konfiguration

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 DHCPDEC-LINE-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 das Gerät den Adresskonflikt behebt, 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 das Gerät den Adresskonflikt behebt, 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: `1`)

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..10000` (Voreinstellung: `10000`)

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät einen Adresskonflikt 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 ein Trap-Ziel festlegen.

Information

Konflikt erkannt

Zeigt, ob gegenwärtig ein Adresskonflikt besteht.

Mögliche Werte:

- `markiert`
  Das Gerät erkennt einen Adresskonflikt.
- `unmarkiert`
  Das Gerät erkennt keinen Adresskonflikt.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

6.2.5 ARP

[Diagnose > System > ARP]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

ARP-Tabelle zurücksetzen

Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

Port

Zeigt die Nummer des Ports.

IP-Adresse

Zeigt die IPv4-Adresse eines benachbarten Geräts.

MAC-Adresse

Zeigt die MAC-Adresse eines benachbarten Geräts.

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 Eintrags.

Mögliche Werte:

- `statisch`
  Statischer Eintrag. Der statische Eintrag bleibt nach dem Löschen der ARP-Tabelle erhalten.
- `dynamisch`
  Dynamischer Eintrag. Das Gerät löscht den dynamischen Eintrag nach Überschreiten der *Aging-Time [s]*, falls das Gerät während dieser Zeit keine Daten von diesem Gerät empfängt.
- `lokal`
  IP- und MAC-Adresse des Geräte-Managements.

Aktiv

Zeigt, dass die ARP-Tabelle die IP/MAC-Adresszuweisung als aktiven Eintrag enthält.

6.2.6 Selbsttest

[Diagnose > System > Selbsttest]

Dieser Dialog ermöglicht Ihnen, Folgendes zu tun:
- 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

Die folgenden Einstellungen sperren Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.
- Kontrollkästchen *SysMon1 ist verfügbar* ist `unmarkiert`.
- Kontrollkästchen *Bei Fehler Default-Konfiguration laden* ist `unmarkiert`.

Dies ist zum Beispiel dann der Fall, wenn sich das Passwort des zu ladenden Konfigurationsprofils von dem im Gerät festgelegten Passwort unterscheidet. Um das Gerät wieder entsperren zu lassen, wenden Sie sich an Ihren Vertriebspartner.

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 ermöglicht Ihnen, 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 ermöglicht Ihnen u. a., die Gerätesoftware 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 Zugriff auf das Management des Geräts ist ausschließlich mit dem Command Line Interface über die serielle 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.

Tabelle

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 ein Trap-Ziel festlegen.

6.3 E-Mail-Benachrichtigung

[Diagnose > E-Mail-Benachrichtigung]

Das Gerät ermöglicht Ihnen, mehrere Empfänger per E-Mail über aufgetretene Ereignisse zu benachrichtigen.

Das Gerät sendet die E-Mails sofort oder in regelmäßigen Abständen, abhängig vom Schweregrad des Ereignisses. Üblicherweise legen Sie fest, dass Ereignisse mit hohem Schweregrad sofort gemeldet werden.

Sie können jeweils mehrere Empfänger festlegen, an die das Gerät die E-Mails entweder sofort oder in regelmäßigen Abständen sendet.

Das Menü enthält die folgenden Dialoge:

- E-Mail-Benachrichtigung Global
- E-Mail-Benachrichtigung Empfänger
- E-Mail-Benachrichtigung Mail-Server

6.3.1 E-Mail-Benachrichtigung Global

[Diagnose > E-Mail-Benachrichtigung > Global]

In diesem Dialog legen Sie die Absender-Einstellungen fest. Außerdem legen Sie fest, für welche Ereignis-Schweregrade das Gerät die E-Mails sofort und für welche in regelmäßigen Abständen sendet.

Funktion

Funktion

Schaltet das Senden von E-Mails ein/aus.

Mögliche Werte:

- `An`
  Das Senden von von E-Mails ist eingeschaltet.
- `Aus` (Voreinstellung)
  Das Senden von von E-Mails ist ausgeschaltet.

Information

Schaltflächen

E-Mail-Benachrichtigung Statistik leeren

Setzt die Zähler im Rahmen *Information* auf `0`.

Gesendete Nachrichten

Zeigt, wie viele Male das Gerät erfolgreich E-Mails an den Mail-Server gesendet hat.

Unzustellbare Nachrichten

Zeigt, wie viele Male das Gerät erfolglos versucht hat, E-Mails an den Mail-Server zu senden.

Zeitpunkt der letzten Nachricht

Zeigt den Zeitpunkt (Datum und Uhrzeit), zu dem das Gerät zuletzt eine E-Mail an den Mail-Server gesendet hat.

Zertifikat

Das Gerät kann Nachrichten über ungesicherte Netze an einen Server senden. Um einen „Man in the Middle“-Angriff zu unterbinden, fordern Sie die Erstellung eines Zertifikates für den Server durch die Zertifizierungsstelle an. Konfigurieren Sie den Server, so dass er das Zertifikat verwendet. Übertragen Sie das Zertifikat auf das Gerät.

Für das Festlegen der Mail-Server-Einstellungen verwenden Sie die IP-Adresse oder den DNS-Namen, welche(r) im Zertifikat als `Common Name` oder `Subject Alternative Name` angegeben ist. Andernfalls wird die Validierung des Zertifikats fehlschlagen.

URL

Legt Pfad und Dateiname des Zertifikats fest.

Zulässig sind Zertifikate mit folgenden Eigenschaften:

- X.509-Format
- `.PEM` Dateinamenserweiterung
- Base64-kodiert, umschlossen von
  `-----BEGIN CERTIFICATE-----`
  und
  `-----END CERTIFICATE-----`

Aus Sicherheitsgründen empfehlen wir, stets ein Zertifikat zu verwenden, das von einer Zertifizierungsstelle signiert ist.

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 der folgenden 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 der folgenden 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 der folgenden 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.

Absender

Adresse

Legt die E-Mail-Adresse des Geräts fest.

Das Gerät sendet die E-Mails mit dieser E-Mail-Adresse als Absender.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
  (Voreinstellung: `switch@hirschmann.com`)

Benachrichtigung sofort

Hier legen Sie die Einstellungen für E-Mails fest, die das Gerät sofort sendet.

Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest, für die das Gerät die E-Mail sofort sendet. Wenn ein Ereignis mit diesem Schweregrad oder mit einem dringenderen Schweregrad auftritt, dann sendet das Gerät eine E-Mail an die Empfänger.

Mögliche Werte:

- *emergency*
- *alert* (Voreinstellung)
- *critical*
- *error*
- *warning*
- *notice*
- *informational*
- *debug*

Betreff

Legt den Betreff der E-Mail fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Benachrichtigung periodisch

Hier legen Sie die Einstellungen für E-Mails fest, die das Gerät in regelmäßigen Abständen sendet.

Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest, für die das Gerät die E-Mail in regelmäßigen Abständen sendet. Wenn ein Ereignis mit diesem Schweregrad oder mit einem dringenderen Schweregrad auftritt, dann puffert das Gerät das Ereignis. Das Gerät sendet den Pufferinhalt in regelmäßigen Abständen oder wenn der Puffer überläuft.

Ereignisse mit weniger dringendem Schweregrad puffert das Gerät nicht.

Mögliche Werte:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (Voreinstellung)
- *notice*
- *informational*
- *debug*

Betreff

Legt den Betreff der E-Mail fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Sende-Intervall [min]

Legt das Sendeintervall in Minuten fest.

Wenn das Gerät mindestens ein Ereignis gepuffert hat, dann sendet es nach dieser Zeit eine E-Mail mit dem Pufferinhalt.

Mögliche Werte:

- `30..1440` (Voreinstellung: `30`)

Senden

Sendet sofort eine E-Mail mit dem Pufferinhalt und leert den Puffer.

Bedeutung der Ereignis-Schweregrade

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

6.3.2 E-Mail-Benachrichtigung Empfänger

[Diagnose > E-Mail-Benachrichtigung > Empfänger]

In diesem Dialog legen Sie die Empfänger fest, an die das Gerät E-Mails sendet. Das Gerät ermöglicht Ihnen, bis zu 10 Empfänger festzulegen.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Benachrichtigungs-Typ

Legt fest, ob das Gerät die E-Mails an diesen Empfänger sofort oder in regelmäßigen Abständen sendet.

Mögliche Werte:

- *sofort*
  Das Gerät sendet die E-Mails an diesen Empfänger sofort.
- *periodisch*
  Das Gerät sendet die E-Mails an diesen Empfänger in regelmäßigen Abständen.

Adresse

Legt die E-Mail-Adresse des Empfängers fest.

Mögliche Werte:

- Gültige E-Mail-Adresse mit bis zu 255 Zeichen

Aktiv

Aktiviert/deaktivert das Benachrichtigen des Empfängers.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Benachrichtigen des Empfängers ist aktiv.
- `unmarkiert`
  Das Benachrichtigen des Empfängers ist inaktiv.

6.3.3 E-Mail-Benachrichtigung Mail-Server

[Diagnose > E-Mail-Benachrichtigung > Mail-Server]

In diesem Dialog legen Sie die Einstellungen für die Mail-Server fest. Das Gerät unterstützt verschlüsselte und unverschlüsselte Verbindungen zum Mail-Server.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Verbindung testen

Öffnet den Dialog *Verbindung testen*, um eine Test-E-Mail zu senden.

Wenn die Mail-Server-Einstellungen korrekt sind, dann erhalten die ausgewählten Empfänger eine Test-E-Mail.

- Im Feld *Empfänger* legen Sie fest, an welche Empfänger das Gerät die E-Mail sendet:
  - *sofort*
    Das Gerät sendet die Test-E-Mail an diejenigen Empfänger, an die das Gerät die E-Mails sofort sendet.
  - *periodisch*
    Das Gerät sendet die Test-E-Mail an diejenigen Empfänger, an die das Gerät die E-Mails in regelmäßigen Abständen sendet.
- Im Feld *Nachrichtentext* legen Sie den Text der E-Mail fest.

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Beschreibung

Legt den Namen des Servers fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

IP-Adresse

Legt IP-Adresse oder DNS-Name des Servers fest.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)
- DNS-Name im Format `domain.tld` oder `host.domain.tld`
  Wenn Sie einen DNS-Namen fetlegen, dann schalten Sie außerdem die Funktion *Client* im Dialog *Erweitert > DNS > Client > Global* ein.
  Wenn Sie verschlüsselte Verbindungen herstellen und dafür das Zertifikat verwenden, dann vergewissern Sie sich, dass der DNS-Name und der im Zertifikat angegebene DNS-Name des Servers gleich sind.

Ziel-TCP-Port

Legt den TCP-Port des Servers fest.

Mögliche Werte:

- `1..65535` (Voreinstellung: `25`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Häufig verwendete TCP-Ports:

- SMTP `25`
- Message Submission `587`

Verschlüsselung

Legt das Protokoll fest, das die Verbindung zwischen Gerät und Mail-Server verschlüsselt.

Mögliche Werte:

- `none` (Voreinstellung)
  Das Gerät baut eine unverschlüsselte Verbindung zum Server auf.
- `tlsv1`
  Das Gerät baut eine verschlüsselte Verbindung zum Server auf und verwendet die startTLS-Erweiterung.

Benutzername

Legt den Benutzernamen für das Konto fest, das das Gerät verwendet, um sich beim Mail-Server anzumelden.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Passwort

Legt das Passwort für das Konto fest, das das Gerät verwendet, um sich beim Mail-Server anzumelden.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Timeout [s]

Legt fest, nach welcher Zeit in Sekunden das Gerät eine E-Mail noch einmal sendet. Voraussetzung ist, dass das Gerät aufgrund eines Verbindungsfehlers die E-Mail unvollständig gesendet hat.

Mögliche Werte:

- `1..15` (Voreinstellung: `3`)

Aktiv

Aktiviert/deaktiviert die Verwendung des Mail-Servers.

Mögliche Werte:

- `markiert`
  Der Mail-Server ist aktiv.
  Das Gerät sendet E-Mails an diesen Mail-Server.
- `unmarkiert` (Voreinstellung)
  Der Mail-Server ist inaktiv.
  Das Gerät sendet keine E-Mails an diesen Mail-Server.

6.4 Syslog

[Diagnose > Syslog]

Das Gerät ermöglicht Ihnen, 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

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.

Zertifikat

Das Gerät kann Nachrichten über ungesicherte Netze an einen Server senden. Um einen „Man in the Middle“-Angriff zu unterbinden, fordern Sie die Erstellung eines Zertifikates für den Server durch die Zertifizierungsstelle an. Konfigurieren Sie den Server, so dass er das Zertifikat verwendet. Übertragen Sie das Zertifikat auf das Gerät.

Vergewissern Sie sich, dass Sie beim Festlegen der Parameter auf dem Server die IP-Adresse und den DNS-Namen festlegen, die im Zertifikat als allgemeiner Name (CN) oder als alternativer Name des Betreffs (SAN) festgelegt sind. Andernfalls wird die Validierung des Zertifikats fehlschlagen.

Anmerkung: Um die Änderungen nach dem Laden eines neuen Zertifikates zu übernehmen, starten Sie die Funktion *Syslog* neu.

URL

Legt Pfad und Dateiname des Zertifikats fest.

Zulässig sind Zertifikate mit folgenden Eigenschaften:

- X.509-Format
- `.PEM` Dateinamenserweiterung
- Base64-kodiert, umschlossen von
  `-----BEGIN CERTIFICATE-----`
  und
  `-----END CERTIFICATE-----`

Aus Sicherheitsgründen empfehlen wir, stets ein Zertifikat zu verwenden, das von einer Zertifizierungsstelle signiert ist.

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 der folgenden 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 der folgenden 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 der folgenden 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 *Password* 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.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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`)
- Hostname

Ziel-UDP-Port

Legt den TCP- oder UDP-Port fest, auf dem der Syslog-Server die Log-Einträge erwartet.

Mögliche Werte:

- `1..65535` (Voreinstellung: `514`)

Transport-Typ

Legt den Transporttyp fest, den das Gerät verwendet, um Ereignisse an den Syslog-Server zu senden.

Mögliche Werte:

- `udp` (Voreinstellung)
  Das Gerät sendet die Ereignisse über den in Spalte *Ziel-UDP-Port* festgelegten UDP-Port.
- `tls`
  Das Gerät sendet die Ereignisse mit TLS über den in Spalte *Ziel-UDP-Port* festgelegten TCP-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`

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.

6.5 Ports

[Diagnose > Ports]

Das Menü enthält die folgenden Dialoge:

- SFP
- TP-Kabeldiagnose
- Port-Monitor
- Auto-Disable
- Port-Mirroring

6.5.1 SFP

[Diagnose > Ports > SFP]

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

Tabelle

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

6.5.2 TP-Kabeldiagnose

[Diagnose > Ports > 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. Das Gerät zeigt auch die einzelnen, an den Port angeschlossenen Kabelpaare. Wenn das Gerät einen Kurzschluss oder eine Unterbrechung im Kabel ermittelt, zeigt es auch die geschätzte Entfernung zu dem Problem.

Um verlässliche Ergebnisse zu erhalten, verwenden Sie die Funktion *TP-Kabeldiagnose* für Twisted-Pair-Kabel, die mindestens 3 Meter lang sind.

Anmerkung: Dieser Test unterbricht den Datenverkehr auf dem betreffenden Port.

Information

Port

Zeigt die Nummer des Ports.

Starte Kabeldiagnose...

Öffnet den Dialog *Port auswählen*.

In der Dropdown-Liste *Port* wählen Sie den zu testenden Port. Wenden Sie den Test ausschließlich für drahtgebundene Ports an.

Um den Kabeltest auf dem ausgewählten Port auszuführen, klicken Sie die Schaltfläche *Ok*.

Status

Status des virtuellen Kabeltesters.

Mögliche Werte:

- `aktiv`
  Der Kabeltest ist im Gange.
  Um den Test zu starten, klicken Sie die Schaltfläche *Starte Kabeldiagnose...*. Diese Aktion öffnet den Dialog *Port auswählen*.
- `erfolgreich`
  Das Gerät zeigt diesen Eintrag nach einem erfolgreichen Test.
- `Fehler`
  Das Gerät zeigt diesen Eintrag nach einer Unterbrechung des Tests.
- `nicht initialisiert`
  Das Gerät zeigt diesen Eintrag, während es sich im Standby befindet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

In den folgenden Fällen zeigt das Gerät andere Werte als erwartet:

- Wenn kein Kabel an den 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 *Status* im Rahmen *Information* den Wert `aktiv`, `Fehler` oder `nicht initialisiert` zeigt.

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 *Status* 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 *Status* im Rahmen *Information* den Wert `aktiv`, `Fehler` oder `nicht initialisiert` zeigt.

6.5.3 Port-Monitor

[Diagnose > Ports > Port-Monitor]

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

Um die *Port-Monitor*-Funktion anzuwenden, führen Sie die folgenden Schritte aus:

- Registerkarte *Global*
  - Schalten Sie im Rahmen *Funktion* die Funktion *Port-Monitor* ein.
  - Aktivieren Sie für jeden Port diejenigen Parameter, deren Einhaltung die Funktion *Port-Monitor* 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 Funktion *Port-Monitor* 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 Funktion *Port-Monitor* ein und legen die Parameter fest, deren Einhaltung die Funktion *Port-Monitor* überwacht. Außerdem legen Sie die Aktion fest, die das Gerät ausführt, wenn die Funktion *Port-Monitor* eine Überschreitung der Parameter erkennt.

Funktion

Funktion

Schaltet die Funktion *Port-Monitor* global ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *Port-Monitor* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *Port-Monitor* ist ausgeschaltet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Zurücksetzen

Öffnet das Fenster *Welche Statistik soll gelöscht werden?*. Das Fenster zeigt die Ports, die Sie wieder einschalten und die zugehörigen Zähler auf `0` zurücksetzen können. Klicken und wählen Sie einen Eintrag, um den zugehörigen Port wieder einzuschalten.

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*

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 Funktion *Port-Monitor* überwacht Linkänderungen auf dem Port.
  - Wenn das Gerät zu viele Linkänderungen erkennt, dann 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 Funktion *Port-Monitor* überwacht CRC-/Fragmentfehler auf dem Port.
  - Wenn das Gerät zu viele CRC-/Fragmentfehler erkennt, dann 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 Funktion *Port-Monitor* überwacht Duplex-Mismatches auf dem Port.
  - Wenn das Gerät einen Duplex-Mismatch erkennt, dann führt es die in Spalte *Aktion* festgelegte Aktion aus.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Überlast-Erkennung an

Aktiviert/deaktiviert auf dem Port die Überlast-Erkennung.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  - Die Funktion *Port-Monitor* 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 Funktion *Port-Monitor* überwacht Verbindungsgeschwindigkeit und Duplex-Modus auf dem Port.
  - Wenn das Gerät eine unzulässige Kombination von Verbindungsgeschwindigkeit und Duplex-Modus feststellt, dann 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.

Aktion

Legt die Aktion fest, die das Gerät ausführt, wenn die Funktion *Port-Monitor* 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, wählen Sie die Zeile des Ports, klicken die Schaltfläche 🗑.
  - Wenn die Überschreitung der Parameter aufgehoben ist, dann schaltet die Funktion *Auto-Disable* den betreffenden Port nach der festzulegenden Wartezeit wieder ein. 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 ein 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.
  - Nach einer Wartezeit schaltet die Funktion *Auto-Disable* 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.

[Auto-Disable]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Grund

Zeigt die von der Funktion *Port-Monitor* überwachten Parameter.

Markieren Sie das nebenstehende Kontrollkästchen, damit die Funktion *Port-Monitor* bei Erkennen einer Überschreitung der überwachten Parameter die Aktion `auto-disable` ausführt.

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für nebenstehende Parameter.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für nebenstehende Parameter ist aktiv.
  Bei Überschreiten der nebenstehenden Parameter führt das Gerät die Funktion *Auto-Disable* aus, wenn in Spalte *Aktion* der Wert `auto-disable` festgelegt ist.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für nebenstehende Parameter ist inaktiv.

[Link-Änderungen]

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

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

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

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Abtast-Intervall [s]

Legt den Zeitraum in Sekunden fest, in welchem die Funktion *Port-Monitor* einen Parameter überwacht, um Abweichungen zu erkennen.

Mögliche Werte:

- `1..180` (Voreinstellung: `10`)

Link-Änderungen

Legt die Anzahl der Linkänderungen fest.

Wenn die Funktion *Port-Monitor* diese Anzahl an Linkänderungen im überwachten Zeitraum erkennt, dann 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.

[CRC/Fragmente]

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

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

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

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Abtast-Intervall [s]

Legt den Zeitraum in Sekunden fest, in welchem die Funktion *Port-Monitor* 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 Funktion *Port-Monitor* diese Fragmentfehlerrate im überwachten Zeitraum erkennt, dann 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.

[Überlast-Erkennung]

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

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

Außerdem sehen Sie die Anzahl an Datenpaketen, die das Gerät bisher erkannt hat.

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

Die Funktion *Port-Monitor* überwacht keine Ports, die Mitglied einer Link-Aggregation-Gruppe sind.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die Nummer des Ports.

Traffic-Typ

Legt den Typ der Datenpakete fest, den das Gerät beim Überwachen der Last auf dem Port berücksichtigt.

Mögliche Werte:

- `all`
  Die Funktion *Port-Monitor* überwacht Broadcast-, Multicast- und Unicast-Pakete.
- `bc` (Voreinstellung)
  Die Funktion *Port-Monitor* überwacht ausschließlich Broadcast-Pakete.
- `bc-mc`
  Die Funktion *Port-Monitor* 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 Funktion *Auto-Disable* 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 Funktion *Port-Monitor* diese Last im überwachten Zeitraum erkennt, dann führt das Gerät die festgelegte Aktion aus.

Mögliche Werte:

- `0..10000000` (Voreinstellung: `0)`)

Intervall [s]

Legt den Zeitraum in Sekunden fest, den die Funktion *Port-Monitor* 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.

[Link-Speed-/Duplex-Mode-Erkennung]

In dieser Registerkarte aktivieren Sie für jeden Port die erlaubten Kombinationen von Geschwindigkeit und Duplex-Modus.

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

Die Funktion *Port-Monitor* überwacht ausschließlich eingeschaltete physische Ports.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 berücksichtigt die Kombinationen aus 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 berücksichtigt die Kombinationen aus 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 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 berücksichtigt die Kombinationen aus 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 berücksichtigt die Kombinationen aus 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 berücksichtigt die Kombinationen aus 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.

6.5.4 Auto-Disable

[Diagnose > Ports > Auto-Disable]

Die Funktion *Auto-Disable* ermöglicht Ihnen, überwachte Ports automatisch auszuschalten und auf Wunsch wieder einzuschalten.

Beispielsweise die Funktion *Port-Monitor* und ausgewählte Funktionen im Menü *Netzsicherheit* verwenden die Funktion *Auto-Disable*, um Ports bei Überschreiten überwachter Parameter auszuschalten.

Wenn die Überschreitung der Parameter aufgehoben ist, dann schaltet die Funktion *Auto-Disable* den betreffenden Port nach der 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 Funktion *Auto-Disable* den betreffenden Port automatisch wieder ein, sofern die Überschreitung der Parameter aufgehoben ist.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Zurücksetzen

Öffnet das Fenster *Welche Statistik soll gelöscht werden?*. Das Fenster zeigt die Ports, die Sie wieder einschalten und die zugehörigen Zähler auf 0 zurücksetzen können. Klicken und wählen Sie einen Eintrag, um den zugehörigen Port wieder einzuschalten.

Davon betroffen sind die Zähler in den folgenden Dialogen:
- Dialog *Diagnose > Ports > Auto-Disable*
- Dialog *Diagnose > Ports > Port-Monitor*
  - Registerkarte *Link-Änderungen*
  - Registerkarte *CRC/Fragmente*
  - Registerkarte *Überlast-Erkennung*

Port

Zeigt die Nummer des Ports.

Reset-Timer [s]

Legt die Wartezeit in Sekunden fest, nach der die Funktion *Auto-Disable* den Port wieder einschaltet.

Mögliche Werte:

- `0` (Voreinstellung)
  Der Timer ist inaktiv. Der Port bleibt ausgeschaltet.
- `30..4294967295`
  Wenn die Überschreitung der Parameter aufgehoben ist, dann schaltet die Funktion *Auto-Disable* den betreffenden Port nach der hier festgelegten Wartezeit wieder ein.

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 Funktion *Auto-Disable* den Port wieder einschaltet.

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*.
- `DHCP_SNP`
  DHCP-Snooping
  Siehe Dialog *Netzsicherheit > DHCP-Snooping*.
- `DOT1S`
  BPDU-Guard
  Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- `DAI`
  Dynamic ARP Inspection
  Siehe Dialog *Netzsicherheit > Dynamic ARP Inspection*.

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*.

- `dhcp-snooping`
  Zu viele DHCP-Pakete aus nicht-vertrauenswürdigen Quellen. Siehe Dialog *Netzsicherheit* > DHCP-Snooping > *Konfiguration*, Registerkarte *Port*.
- `arp-rate`
  Zu viele ARP-Pakete aus nicht-vertrauenswürdigen Quellen. Siehe Dialog *Netzsicherheit* > Dynamic ARP Inspection > *Konfiguration*, Registerkarte *Port*.
- `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*.
- `Loop protection`
  Layer-2-Loop auf dem Port erkannt. Siehe Dialog *Diagnose* > *Loop-Schutz*, Spalte *Loop erkannt*.

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.

[Status]

Diese Registerkarte zeigt, für welche überwachten Parameter die Funktion *Auto-Disable* aktiviert ist.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Grund

Zeigt die Parameter, die das Gerät überwacht.

Markieren Sie das nebenstehende Kontrollkästchen, damit die Funktion *Auto-Disable* 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 zu den Funktionen im Menü *Diagnose > Port > Port-Monitor*.
- `network-security`
  Der Parameter gehört zu den Funktionen im Menü *Netzsicherheit*.
- `l2-redundancy`
  Der Parameter gehört zu den Funktionen im Menü *Switching > L2-Redundanz* oder zur Funktion *Loop-Schutz*, siehe Dialog *Diagnose > Loop-Schutz*.

Auto-Disable

Zeigt, ob die Funktion *Auto-Disable* für den nebenstehenden Parameter aktiviert/deaktiviert ist.

Mögliche Werte:

- `markiert`
  Die Funktion *Auto-Disable* für nebenstehende Parameter ist aktiv.
  Die Funktion *Auto-Disable* schaltet bei Überschreiten der überwachten Parameter den betreffenden Port aus und ggf. wieder ein.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Auto-Disable* für nebenstehende Parameter ist inaktiv.

6.5.5 Port-Mirroring

[Diagnose > Ports > Port-Mirroring]

Die Funktion *Port-Mirroring* ermöglicht Ihnen, 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 Zugriff über den Ziel-Port auf das Management des Geräts einzuschalten, markieren Sie vor Einschalten der Funktion *Port-Mirroring* das Kontrollkästchen *Management erlauben* im Rahmen *Ziel-Port*.

Funktion

Schaltflächen

Konfiguration zurücksetzen

Setzt die Einstellungen des Dialogs auf die voreingestellten Werte zurück und überträgt die Änderungen in den flüchtigen Speicher des Geräts (`RAM`).

Funktion

Schaltet die Funktion *Port-Mirroring* ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *Port-Mirroring* ist eingeschaltet.
  Das Gerät kopiert die Datenpakete von den ausgewählten Quell-Ports auf den Ziel-Port.
- `Aus` (Voreinstellung)
  Die Funktion *Port-Mirroring* ist ausgeschaltet.

Ziel-Port

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, dann verwirft das Gerät überschüssige Datenpakete auf dem Ziel-Port.

Sekundärer Port

Legt einen zweiten Ziel-Port fest. Voraussetzung ist, dass Sie einen ersten Ziel-Port festgelegt haben.

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.
  Der Port überträgt dieselben Daten wie der oben festgelegte Port. Ausnahme:
  - keine *VLAN-Mirroring*-Daten
  - keine *RSPAN*-Daten

Management erlauben

Aktiviert/deaktiviert den Zugriff auf das Management des Geräts über den Ziel-Port.

Mögliche Werte:

- `markiert`
  Der Zugriff über den Ziel-Port auf das Management des Geräts ist aktiv.
  Das Gerät ermöglicht den Benutzern über den Ziel-Port Zugriff auf das Management, 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 Zugriff über den Ziel-Port auf das Management des Gerätes ist, dass der Ziel-Port Mitglied im Geräte-Management-VLAN ist.
- `unmarkiert` (Voreinstellung)
  Der Zugriff über den Ziel-Port auf das Management des Geräts ist inaktiv.
  Das Gerät unterbindet den Zugriff auf das Management des Geräts über den Ziel-Port.

VLAN-Mirroring

Die Funktion *VLAN-Mirroring* ermöglicht Ihnen, die in einem VLAN empfangenen Datenpakete an den festgelegten Ziel-Port zu kopieren. Das Gerät leitet den Datenstrom auf den festgelegten Ziel-Port um.

Anmerkung: Die Funktion *VLAN-Mirroring* ist ausschließlich auf dem primären Port verfügbar.

Quell-VLAN-ID

Legt das VLAN fest, dessen Daten das Gerät an den Ziel-Port spiegelt.

Mögliche Werte:

- `0` (Voreinstellung)
  Schaltet die Funktion *VLAN-Mirroring* aus.
- `2..4042`
  Das Gerät ermöglicht Ihnen, ausschließlich dann ein VLAN festzulegen, wenn kein Quell-Port festgelegt ist.

RSPAN

Die Funktion *RSPAN* (Remote Switched Port Analyzer) erweitert die Spiegelungsfunktion, indem sie dem Gerät die Möglichkeit bietet, die überwachten Daten in einem bestimmten VLAN über mehrere Geräte an 1 Ziel weiterzuleiten.

Anmerkung: Wenn Sie das Gerät auf dem Pfad zwischen Quell- und Zielgerät einsetzen, dann legen Sie im Feld *VLAN-ID* das für die Funktion *RSPAN* benötigte VLAN fest. Die Funktion *Port-Mirroring* wird hierfür nicht benötigt und bleibt ausgeschaltet.

Anmerkung: Die Funktion *RSPAN* ist ausschließlich auf dem primären Port verfügbar.

Quell-VLAN-ID

Legt das Quell-VLAN fest, von dem das Gerät Daten zum Ziel-VLAN spiegelt.

Mögliche Werte:

- `0` (Voreinstellung: `0`)
  Das Quell-VLAN ist inaktiv.
- `2..4042`
  Gespiegelte Ports dürfen kein RSPAN-VLAN-Mitglied sein.

VLAN-ID

Legt das VLAN fest, welches das Gerät zum Markieren und Weiterleiten der gespiegelten Daten verwendet.

Mögliche Werte:

- `0` (Voreinstellung: `0`)
  Das RSPAN VLAN ist inaktiv.
- `2..4042`
  Das Gerät verwendet den Wert zum Markieren und Weiterleiten von gespiegelten Daten.

Ziel-VLAN-ID

Legt das VLAN fest, welches das Gerät zum Weiterleiten des Netzverkehrs zum Zielgerät verwendet.

Mögliche Werte:

- `0` (Voreinstellung: `0`)
  Das Ziel-VLAN ist inaktiv.
- `2..4042`
  Das Gerät verwendet diesen Wert zum Markieren von Daten und zum Weiterleiten des Netzverkehrs zum Zielgerät.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 ermöglicht Ihnen, abzüglich des Ziel-Ports jeden physischen Port als Quell-Port festzulegen.

Typ

Legt fest, welche Datenpakete das Gerät auf den Ziel-Port kopiert.

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.

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.

6.6 LLDP

[Diagnose > LLDP]

Das Gerät ermöglicht Ihnen, 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 ermöglicht Ihnen, die Topologie-Erkennung zu konfigurieren und die empfangenen Informationen in Tabellenform anzuzeigen.

Das Menü enthält die folgenden Dialoge:
- LLDP Konfiguration
- LLDP Topologie-Erkennung

6.6.1 LLDP Konfiguration

[Diagnose > LLDP > Konfiguration]

Dieser Dialog ermöglicht Ihnen, die Topologie-Erkennung für jeden Port zu konfigurieren.

Funktion

Funktion

Schaltet die Funktion *LLDP* ein/aus.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion *LLDP* ist eingeschaltet.
  Die Topologie-Erkennung mit LLDP ist auf dem Gerät aktiv.
- `Aus`
  Die Funktion *LLDP* ist ausgeschaltet.

Konfiguration

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, dann 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 Werts im Feld *Sende-Intervall [s]* 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

Benachrichtigung

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`)

FDB-Modus

Legt fest, welche Funktion das Gerät verwendet, um benachbarte Geräte auf diesem Port zu erfassen.

Mögliche Werte:

- `lldpOnly`
  Das Gerät verwendet ausschließlich LLDP-Datenpakete, um benachbarte Geräte auf diesem Port zu erfassen.
- `macOnly`
  Das Gerät verwendet gelernte MAC-Adressen, um benachbarte Geräte auf 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 auf diesem Port zu erfassen.
- `autoDetect` (Voreinstellung)
  Wenn das Gerät auf diesem Port LLDP-Datenpakete empfängt, dann arbeitet das Gerät wie mit der Einstellung `lldpOnly`. Andernfalls arbeitet das Gerät wie mit der Einstellung `macOnly`.

6.6.2 LLDP Topologie-Erkennung

[Diagnose > 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 ermöglicht Ihnen, 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 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, 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 einen Port mehrere Geräte anschließen (zum Beispiel über einen Hub), zeigt die Tabelle für jedes angeschlossenes Gerät je eine Zeile.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 18.

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 Zugriff auf das Management des Nachbargeräts 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 aktiv 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.

[LLDP-MED]

Bei „LLDP for Media Endpoint Devices“ (LLDP-MED) handelt es sich um eine Erweiterung von LLDP, welche zwischen Endgeräten und Geräten im Netz 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 18.

Port

Zeigt die Nummer des Ports.

Geräteklasse

Zeigt die Geräteklasse des über Fernverbindung angeschlossen Geräts.

- Der Wert `notDefined` zeigt, dass das Gerät Funktionsmerkmale aufweist, welche durch keine der *LLDP-MED*-Klassen abgedeckt sind.
- Der Wert `endpointClass1..3` zeigt, dass das Gerät die Funktionsmerkmale „EndPoint-Klasse 1..3“ aufweist.
- Der Wert `networkConnectivity` zeigt, dass das Gerät die Funktionsmerkmale eines Netzwerkverbindungsgeräts aufweist.

VLAN-ID

Zeigt die Erweiterung für die VLAN-Kennung des entfernten Systems, welches an diesen 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, welche dem an diesen Port angeschlossenen entfernten System zugeordnet ist.

DSCP

Zeigt den Wert für den „Differentiated Service Code Point“, welcher dem an diesen Port angeschlossenen entfernten System zugeordnet ist.

Status Unknown-Bit

Zeigt den sog. „Unknown Bit Status“ des eingehenden Verkehrs.

- Der Wert `true` zeigt, dass die Netz-Richtlinie für den festgelegten 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.

Status Tagged-Bit

Zeigt den sog. „Tagged Bit Status“.

- Der Wert `true` zeigt, dass die Anwendung ein markiertes VLAN verwendet.
- Der Wert `false` zeigt, 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.

Firmware-Revision

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Firmware-Revisionskennung.

Software-Revision

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Software-Revisionskennung.

Seriennummer

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Seriennummer.

Herstellername

Zeigt den vom entfernten Endpunkt mitgeteilten spezifischen Herstellernamen.

Modellname

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Modellbezeichnung.

Asset-ID

Zeigt die vom entfernten Endpunkt mitgeteilte herstellerspezifische Kennung zur Produktverfolgung.

6.7 Loop-Schutz

[Diagnose > Loop-Schutz]

Die Funktion *Loop-Schutz* unterstützt beim Schutz vor Layer-2-Loops.

Ein Loop im Netz kann zu einem Stillstand des Netzes aufgrund von Überlastung führen. Eine mögliche Ursache ist das ständige Duplizieren von Datenpaketen aufgrund einer Fehlkonfiguration. Die Ursache kann z. B. ein falsch gestecktes Kabel oder fehlerhafte Einstellungen in der Software sein.

Ein Layer-2-Loop im Netz entsteht zum Beispiel in den folgenden Fällen, wenn keine Redundanzprotokolle aktiv sind:
- Zwei Ports desselben Geräts sind direkt miteinander verbunden.
- Zwischen zwei Geräten ist mehr als eine aktive Verbindung eingerichtet.

In redundanten Netztopologien sind typischerweise verschiedene Redundanzprotokolle aktiv. In der Regel deaktivieren Sie die *Spanning Tree*-Funktion auf Ports, die an anderen Redundanzprotokollen beteiligt sind. Die Redundanzprotokolle unterstützen bereits beim Vermeiden von Loops.

Funktion

Funktion

Schaltet die Funktion *Loop-Schutz* ein/aus.

Mögliche Werte:

▶ `An`
Die Funktion *Loop-Schutz* ist eingeschaltet.
- An aktiven und passiven Ports wertet das Gerät empfangene *Loop-Detection*-Pakete aus.
  An aktiven Ports sendet das Gerät *Loop-Detection*-Pakete in regelmäßigen Abständen, wie im Feld *Sende-Intervall* angegeben.
  Voraussetzung ist, dass die Funktion *Loop-Schutz* auf dem Port aktiv ist.
- Das Gerät ermöglicht Ihnen, Ethernet-Loops mit dem Signalkontakt zu überwachen. Siehe Dialog *Diagnose > Statuskonfiguration > Signalkontakt > Signalkontakt 1*, Kontrollkästchen für den Parameter *Ethernet-Loops*.

▶ `Aus` (Voreinstellung)
Die Funktion *Loop-Schutz* ist ausgeschaltet.
Das Gerät sendet weder *Loop-Detection*-Pakete noch wertet es empfangene *Loop-Detection*-Pakete aus.

Global

Sende-Intervall

Legt das Intervall in Sekunden fest, in dem das Gerät *Loop-Detection*-Pakete sendet, wenn die Funktion *Loop-Schutz* auf dem Port aktiv ist.

Mögliche Werte:

▶ `1..10`

Empfang-Grenzwert

Legt den Schwellenwert für die Anzahl der nacheinander empfangenen *Loop-Detection*-Pakete fest. Wenn die Anzahl diesen Schwellenwert erreicht oder überschreitet, dann führt das Gerät die in Spalte *Aktion* festgelegte Aktion aus.

Mögliche Werte:

▶ `1..50`

Konfiguration

Auto-Disable

Aktiviert/deaktiviert die Funktion *Auto-Disable* für *Loop-Schutz*.

Mögliche Werte:

▶ `markiert`
Die Funktion *Auto-Disable* für *Loop-Schutz* ist aktiv.
Voraussetzung für das Abschalten des Ports ist, dass in Spalte *Aktion* die Aktion *auto-disable* oder die Aktion *alle* festgelegt ist.
Das Gerät ermöglicht Ihnen, die Wartezeit in Sekunden festzulegen, nach der die Funktion *Auto-Disable* den Port wieder einschaltet. Legen Sie dazu im Dialog *Diagnose > Ports > Auto-Disable* in Spalte *Reset-Timer [s]* die Wartezeit fest.

▶ `unmarkiert` (Voreinstellung)
Die Funktion *Auto-Disable* für *Loop-Schutz* ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Port-Statistiken leeren

Setzt die Werte in den folgenden Spalten zurück:

- *Loop-Anzahl*
- *Gesendete Pakete*
- *Empfangene Pakete*

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *Loop-Schutz* auf dem Port.

Mögliche Werte:

- `markiert`
  Die Funktion *Loop-Schutz* ist auf dem Port aktiv.
  Aktivieren Sie die Funktion ausschließlich auf Ports, die nicht Teil eines redundanten Netzpfads sind. Dies hilft, ein versehentliches Abschalten auf redundanten Netzpfaden zu vermeiden.
  Wenn das Gerät auf diesem Port ein *Loop-Detection*-Paket empfängt, das von einem anderen Port desselben Geräts gesendet wurde, dann führt das Gerät die in Spalte *Aktion* festgelegte Aktion aus.
- `unmarkiert` (Voreinstellung)
  Die Funktion *Loop-Schutz* ist auf dem Port inaktiv. Der Port sendet weder *Loop-Detection*-Pakete noch wertet er empfangene *Loop-Detection*-Pakete aus.

Modus

Legt das Verhalten der Funktion *Loop-Schutz* auf dem Port fest.

Mögliche Werte:

- `aktiv`
  Das Gerät sendet *Loop-Detection*-Pakete und wertet empfangene *Loop-Detection*-Pakete aus.
- `passiv`
  Das Gerät wertet empfangene *Loop-Detection*-Pakete aus.

Aktion

Legt die Aktion fest, die das Gerät ausführt, wenn es einen Layer-2-Loop an diesem Port erkennt.

Mögliche Werte:

- `trap`
  Das Gerät sendet einen Trap.
- `auto-disable`
  Das Gerät schaltet den Port mit der Funktion *Auto-Disable* aus.
  Voraussetzung für das Abschalten des Ports ist, dass das Kontrollkästchen *Auto-Disable* im Rahmen *Konfiguration* markiert ist.
- `alle`
  Das Gerät sendet einen Trap. Dann schaltet das Gerät den Port mit der Funktion *Auto-Disable* aus.
  Voraussetzung für das Abschalten des Ports ist, dass das Kontrollkästchen *Auto-Disable* im Rahmen *Konfiguration* markiert ist.

VLAN-ID

Legt das VLAN fest, in welchem das Gerät die *Loop-Detection*-Pakete sendet.

Mögliche Werte:

- `0` (Voreinstellung)
  Das Gerät sendet die *Loop-Detection*-Pakete ohne VLAN-Tag.
- `1..4042`
  Das Gerät sendet die *Loop-Detection*-Pakete im festgelegten VLAN. Voraussetzung ist, dass das VLAN bereits eingerichtet ist und dass der Port ein Mitglied des VLANs ist. Siehe Dialog *Switching > VLAN > Port*.

Loop erkannt

Zeigt, ob das Gerät einen Layer-2-Loop auf dem Port erkannt hat.

Mögliche Werte:

- *ja*
  Das Gerät hat einen Layer-2-Loop auf dem Port erkannt.
  Nachdem der Loop aufgehoben und der Port wieder freigegeben ist, setzt das Gerät den Wert auf *nein* zurück.
- *nein*
  Das Gerät hat keinen Layer-2-Loop auf dem Port erkannt.

Loop-Anzahl

Zeigt die Anzahl der Loops, die das Gerät auf dem Port seit dem letzten Zurücksetzen der Portstatistik oder seit dem letzten Neustart des Geräts erkannt hat.

Letzter Loop-Zeitpunkt

Zeigt den Zeitpunkt, an dem das Gerät den letzten Loop auf dem Port erkannt hat.

Voraussetzung für die korrekte Ermittlung des Werts ist, dass Sie die Systemzeit des Gerätes mit der entsprechenden Referenzzeit synchronisieren. Siehe Dialog *Zeit > Grundeinstellungen*.

Gesendete Pakete

Zeigt die Anzahl der *Loop-Detection* an, die seit dem letzten Zurücksetzen der Portstatistik oder seit dem letzten Neustart des Geräts auf dem Port gesendet wurden.

Empfangene Pakete

Zeigt die Anzahl der gesendeten und wieder empfangenen *Loop-Detection*-Pakete auf dem Port seit dem letzten Zurücksetzen der Portstatistik oder seit dem letzten Neustart des Geräts.

Verworfene Pakete

Zeigt die Anzahl der verworfenen *Loop-Detection*-Pakete auf dem Port.

Beispiele für Gründe für verworfene Pakete:

- Das Gerät erkennt Pakete mit einem falschen Format.
- Das Gerät erkennt Pakete mit abgelaufenen Zeitstempeln (Pakete, die das Gerät mehr als 5 Sekunden nach dem Senden empfängt).
- Das Gerät hat ein Datenpaket mit einer nicht vorgesehenen VLAN-Information empfangen.
- Das Gerät erkennt empfangene Pakete an einem Port, der deaktiviert ist.

6.8 SFlow

[Diagnose > SFlow]

Bei sFlow handelt es sich um ein Standardprotokoll zur Überwachung von Netzen. Die im Gerät implementierte sFlow-Funktion macht Netz-Aktivitäten sichtbar und ermöglicht hierdurch ein effektives Management und eine effektive Steuerung von Netz-Ressourcen.

Das sFlow-Überwachungssystem besteht aus einem sFlow-Agenten und einem zentralen sFlow-Kollektor. Der Agent verwendet die folgenden Methoden zur Stichprobenentnahme:

- statistische, paketbasierte Abtastung von Paketflüssen
- zeitbasierte Abtastung von Zählern

Das Gerät setzt beide Stichprobenarten zu Datagrammen zusammen. sFlow verwendet die Datagramme, um die abgetasteten Verkehrsstatistiken zur Analyse an den sFlow-Kollektor weiterzuleiten.

Für eine Abtastung von Paketflüssen stellen Sie bei einer Instanz eine Abtastrate ein. Anschließend stellen Sie bei dieser Instanz ein Abfrage-Intervall zur Abtastung der Zähler ein.

Das Menü enthält die folgenden Dialoge:

- SFlow-Konfiguration
- SFlow Empfänger

6.8.1 SFlow-Konfiguration

[Diagnose > SFlow > Konfiguration]

Dieser Dialog zeigt die Geräteparameter und ermöglicht Ihnen, sFlow-Instanzen einzurichten.

Der Dialog enthält die folgenden Registerkarten:
- [Global]
- [Sampler]
- [Poller]

[Global]

Information

Version

Zeigt die MIB-Version, das für die Implementierung des Agenten verantwortliche Unternehmen sowie die Version der Geräte-Software.

IP-Adresse

Zeigt zugehörige IP-Adresse des Agenten, welcher die SNMP-Konnektivität bereitstellt.

[Sampler]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die physikalische Datenquelle für den Sampler.

Empfänger

Zeigt die Kennziffer des mit dem Sampler verknüpften Empfängers.

Abtastrate

Legt die statistische Abtastrate für die Abtastung der Pakete von dieser Quelle fest.

Mögliche Werte:

- `0` (Voreinstellung)
  Deaktiviert die Abtastung.
- `256..65535`
  Wenn der Port Daten empfängt, zählt das Gerät bis zum eingestellten Wert hoch und tastet dann die Daten ab.

Max. Header-Größe [Byte]

Legt die maximale, von einem abgetasteten Paket kopierte Header-Größe in Bytes fest.

Mögliche Werte:

- `20..256` (Voreinstellung: `128`)

[Poller]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

Zeigt die physikalische Datenquelle für den Abfragezähler.

Empfänger

Zeigt die Kennziffer des mit dem Abfragezähler verknüpften Empfängers.

Mögliche Werte:

- `0..8` (Voreinstellung: `0`)

Intervall [s]

Legt die maximale Anzahl von Sekunden zwischen aufeinanderfolgenden Stichproben der Zähler fest, welche mit dieser Datenquelle verknüpft sind.

Mögliche Werte:

- `0..86400` (Voreinstellung: `0`)

Ein Abtastintervall mit dem Wert `0` deaktiviert die Abtastung der Zähler.

6.8.2 SFlow Empfänger

[Diagnose > SFlow > Empfänger]

Um eine Situation zu vermeiden, wo 2 Personen oder Unternehmen versuchen, denselben Sampler zu steuern, definiert die entsprechende Person (bzw. das Unternehmen) sowohl den Parameter *Name* wie auch den Parameter *Timeout [s]* innerhalb derselben SNMP-Set-Anfrage.

Zur Freigabe eines Samplers löscht die den Sampler steuernde Person (bzw. das Unternehmen) den Wert in Spalte *Name*. Die den Sampler steuernde Person (bzw. das Unternehmen) setzt auch die anderen Parameter dieser Zeile wieder auf die voreingestellten Werte.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Name

Legt den Namen der Person oder des Unternehmens fest, welche bzw. welches den Eintrag verwendet. Ein leeres Feld zeigt, dass der Eintrag gegenwärtig unbeansprucht ist. Editieren Sie dieses Feld, bevor Sie Änderungen an den anderen Sampler-Parametern vornehmen.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..127 Zeichen

Timeout [s]

Zeigt die bis zur Freigabe des Samplers bzw. bis zum Ende der Abtastung verbleibende Zeit in Sekunden.

Datagram-Größe [Byte]

Legt die maximale Anzahl von Datenbytes fest, die in einem einzelnen Sample-Datagramm gesendet werden.

Mögliche Werte:

- `200..3996` (Voreinstellung: `1400`)

IP-Adresse

Legt die IP-Adresse des sFlow-Kollektors fest.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)

Ziel-UDP-Port

Legt die Nummer des UDP-Ports für sFlow-Datagramme fest.

Mögliche Werte:

- `1..65535` (Voreinstellung: `6343`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Datagram-Version

Zeigt die Version der angeforderten sFlow-Datagramme.

6.9 Bericht

[Diagnose > Bericht]

Das Menü enthält die folgenden Dialoge:

- Bericht Global
- Persistentes Ereignisprotokoll
- System-Log
- Audit-Trail

6.9.1 Bericht Global

[Diagnose > Bericht > Global]

Das Gerät ermöglicht Ihnen, über die folgenden Ausgaben bestimmte Ereignisse zu protokollieren:
- auf der Konsole
- auf einen oder mehreren Syslog-Servern
- auf einer per SSH aufgebauten Verbindung zum Command Line Interface
- auf einer per Telnet aufgebauten Verbindung zum Command Line Interface

In diesem Dialog legen Sie die erforderlichen Einstellungen fest. Durch Zuweisen eines Schweregrads legen Sie fest, welche Ereignisse das Gerät protokolliert.

Der Dialog ermöglicht Ihnen, ein ZIP-Archiv mit detaillierten Informationen zum Gerät für Supportzwecke auf Ihrem PC zu speichern.

Console-Logging

Schaltflächen

Support-Informationen herunterladen

Erzeugt ein ZIP-Archiv, das Sie mit dem Web-Browser vom Gerät herunterladen können.

Das ZIP-Archiv enthält Dateien mit detaillierten Informationen zum Gerät für Supportzwecke. Weitere Informationen finden Sie unter „Support-Informationen: Dateien im ZIP-Archiv" auf Seite 462.

Funktion

Schaltet die Funktion *Console-Logging* ein/aus.

Mögliche Werte:
- `An`
  Die Funktion *Console-Logging* ist eingeschaltet.
  Das Gerät protokolliert die Ereignisse auf der Konsole.
- `Aus` (Voreinstellung)
  Die Funktion *Console-Logging* ist ausgeschaltet.

Schweregrad

Legt den Mindest-Schweregrad für die Ereignisse fest. Das Gerät protokolliert Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden. Weitere Informationen finden Sie unter „Bedeutung der Ereignis-Schweregrade" auf Seite 462.

Das Gerät gibt die Meldungen auf der seriellen Schnittstelle aus.

Mögliche Werte:
- `emergency`
- `alert`
- `critical`
- `error`
- `warning` (Voreinstellung)

- `notice`
- `informational`
- `debug`

SNMP-Logging

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`. 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.

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. Weitere Informationen finden Sie unter „Bedeutung der Ereignis-Schweregrade" auf Seite 462.

Mögliche Werte:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning`
- `notice` (Voreinstellung)
- `informational`
- `debug`

Schweregrad Set-Request

Legt den Schweregrad des Ereignisses fest, welches das Gerät bei SNMP Set requests protokolliert. Weitere Informationen finden Sie unter „Bedeutung der Ereignis-Schweregrade" auf Seite 462.

Mögliche Werte:

- `emergency`
- `alert`
- `critical`
- `error`
- `warning`
- `notice` (Voreinstellung)
- `informational`
- `debug`

Buffered-Logging

Das Gerät puffert protokollierte Ereignisse in 2 getrennten Speicherbereichen, damit die Log-Einträge für dringliche Ereignisse erhalten bleiben.

Dieser Rahmen ermöglicht Ihnen, den Mindest-Schweregrad für Ereignisse festzulegen, die das Gerät im höher priorisierten Speicherbereich puffert.

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. Weitere Informationen finden Sie unter „Bedeutung der Ereignis-Schweregrade" auf Seite 462.

Mögliche Werte:

- `emergency`
- `alert`
- `critical`

- `error`
- `warning` (Voreinstellung)
- `notice`
- `informational`
- `debug`

CLI-Logging

Funktion

Schaltet die Funktion *CLI-Logging* ein/aus.

Mögliche Werte:

- *An*
  Die Funktion *CLI-Logging* ist eingeschaltet.
  Das Gerät protokolliert jeden Befehl, den es über das Command Line Interface empfängt.
- *Aus* (Voreinstellung)
  Die Funktion *CLI-Logging* ist ausgeschaltet.

Support-Informationen: Dateien im ZIP-Archiv

Dateiname	Format	Bemerkungen
`audittrail.html`	HTML	Enthält die im Audit Trail chronologisch aufgezeichneten Systemereignisse und gespeicherten Änderungen durch die Benutzer.
`config.xml`	XML	Enthält die im „ausgewählten“ Konfigurationsprofil gespeicherten Einstellungen des Geräts.
`defaultconfig.xml`	XML	Enthält die Voreinstellungen des Geräts.
`script`	TEXT	Enthält die Ausgaben des Kommandos `show running-config script`.
`runningconfig.xml`	XML	Enthält die gegenwärtigen Betriebseinstellungen des Geräts.
`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 Ereignis-Schweregrade

Schweregrad	Bedeutung
`emergency`	Gerät nicht betriebsbereit
`alert`	Sofortiger Bedienereingriff erforderlich
`critical`	Kritischer Zustand
`error`	Fehlerhafter Zustand

Schweregrad	Bedeutung
`warning`	Warnung
`notice`	Signifikanter, normaler Zustand
`informational`	Informelle Nachricht
`debug`	Debug-Nachricht

6.9.2 Persistentes Ereignisprotokoll

[Diagnose > Bericht > Persistentes Ereignisprotokoll]

Das Gerät ermöglicht Ihnen, die Log-Einträge in einer Datei im 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. Wenn die Log-Datei die festgelegte Größe erreicht, archiviert das Gerät diese Datei und speichert die folgenden Log-Einträge ein einer neu erstellten Datei.

In der Tabelle zeigt das Gerät die im 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 im externen Speicher ausreichend Speicherplatz verfügbar.

Anmerkung: Vergewissern Sie sich, dass ein externer Speicher angeschlossen ist. Um festzustellen, ob ein externer Speicher angeschlossen ist, siehe Spalte *Status* im Dialog *Grundeinstellungen > Externer Speicher*. Wir empfehlen, die Verbindung des externen Speichers mit der Funktion *Gerätestatus* zu überwachen, siehe Parameter *Externen Speicher entfernen* im Dialog *Diagnose > Statuskonfiguration > Gerätestatus*.

Funktion

Funktion

Schaltet die Funktion *Persistentes Ereignisprotokoll* ein/aus.

Aktivieren Sie die Funktion ausschließlich dann, wenn der externe Speicher im Gerät verfügbar ist.

Mögliche Werte:

- `An` (Voreinstellung)
  Die Funktion *Persistentes Ereignisprotokoll* ist eingeschaltet.
  Das Gerät speichert die Log-Einträge in einer Datei im externen Speicher.
- `Aus`
  Die Funktion *Persistentes Ereignisprotokoll* ist ausgeschaltet.

Konfiguration

Max. Datei-Größe [kByte]

Legt die maximale Größe der Log-Datei in KBytes fest. Wenn die Log-Datei die festgelegte Größe erreicht, 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 im 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.

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 im 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:

- `sd` (nicht verfügbar für MSP-X)
  Externer SD-Speicher (ACA31)
- `usb`
  Externer USB-Speicher (ACA21/ACA22)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Persistente Log-Datei löschen

Entfernt die Log-Dateien vom externen Speicher.

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 im externen Speicher.

Mögliche Werte:

- `messages`
- `messages.X`

Datei-Größe [Byte]

Zeigt die Größe der Log-Datei im externen Speicher in Bytes.

6.9.3 System-Log

[Diagnose > Bericht > System-Log]

Das Gerät protokolliert geräteinterne Ereignisse in einer Log-Datei (System Log).

Dieser Dialog zeigt die Log-Datei (System Log). Der Dialog ermöglicht Ihnen, 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

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.

6.9.4 Audit-Trail

[Diagnose > Bericht > Audit-Trail]

Dieser Dialog zeigt die Log-Datei (Audit Trail). Der Dialog ermöglicht Ihnen, 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. Dies ermöglicht Ihnen, 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 mit dem Command Line Interface (lokal oder remote)
- Manuelle Abmeldung eines Benutzers
- Automatische Abmeldung eines Benutzers im Command Line Interface nach vorgegebener Zeit der Inaktivität
- Neustart des Geräts
- Sperrung eines Benutzerkontos aufgrund erfolgloser Anmeldeversuche
- Sperrung des Zugriffs auf des Management des Geräts aufgrund erfolgloser Anmeldeversuche
- Im Command Line Interface 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

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
- DNS
- Industrie-Protokolle
- Digital-IO Modul
- Command Line Interface

7.1 DHCP-L2-Relay

[Erweitert > DHCP-L2-Relay]

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

Sofern aktiv, fügt das Relay 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 zeigen eindeutige Informationen über den Client und das Relay an. Diese eindeutige Kennung besteht aus einer *Circuit-ID* für den Client und einer *Remote-ID* für das Relay.

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, einer Client-Kennung 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

[Erweitert > DHCP-L2-Relay > Konfiguration]

Dieser Dialog ermöglicht Ihnen, 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 nicht vertrauenswürdigen Ports. Zudem ermöglicht Ihnen das Gerät, die Remote-Kennung festzulegen.

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

Funktion

Funktion

Schaltet die DHCP-L2-Relay-Funktion des Geräts global ein oder aus.

Mögliche Werte:
- `An`
  Schaltet die Funktion *DHCP-L2-Relay* im Gerät ein.
- `Aus` (Voreinstellung)
  Schaltet die Funktion *DHCP-L2-Relay* im Gerät aus.

[Interface]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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 Funktion *DHCP-L2-Relay* ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *DHCP-L2-Relay* ist inaktiv.

Gesicherter Port

Aktiviert/deaktiviert den gesicherten *DHCP-L2-Relay*-Modus für den betreffenden Port.

Mögliche Werte:

- `markiert`
  Das Gerät akzeptiert DHCPv4-Pakete mit *Option 82*-Informationen.
- `unmarkiert` (Voreinstellung)
  Das Gerät verwirft DHCPv4-Pakete, die an einem ungesicherten Port empfangen werden, der *Option 82*-Informationen enthält.

[VLAN-ID]

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

VLAN-ID

VLAN, auf das sich der Tabelleneintrag bezieht.

Aktiv

Aktiviert/deaktiviert die Funktion *DHCP-L2-Relay* in diesem VLAN.

Voraussetzung ist, dass Sie die Funktion global aktivieren.

Mögliche Werte:

- `markiert`
  Die Funktion *DHCP-L2-Relay* ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *DHCP-L2-Relay* ist inaktiv.

Circuit-ID

Aktiviert oder 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`
  Wenn Sie diesen Wert verwenden, geben Sie benutzerdefinierte Informationen in Spalte *Remote-ID* ein.

Remote-ID

Zeigt die *Remote-ID* für das VLAN.

Legen Sie die ID fest, wenn Sie in Spalte *Remote-ID-Typ* den Wert `other` festlegen.

7.1.2 DHCP-L2-Relay Statistiken

[Erweitert > DHCP-L2-Relay > Statistiken]

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

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Zurücksetzen

Setzt die Zähler der Statistik auf 0.

Port

Zeigt die Nummer des Ports.

Ungesicherte Server-Nachrichten mit Option 82

Zeigt die Anzahl der Nachrichten vom DHCP-Server, die mit *Option 82*-Informationen auf dem nicht vertrauenswürdigen Interface eingegangen sind.

Ungesicherte Client-Nachrichten mit Option 82

Zeigt die Anzahl der Nachrichten vom DHCP-Client, die mit *Option 82*-Informationen auf dem nicht vertrauenswürdigen Interface eingegangen sind.

Gesicherte Server-Nachrichten ohne Option 82

Zeigt die Anzahl der Nachrichten vom DHCP-Server, die ohne *Option 82*-Informationen auf dem vertrauenswürdigen Port eingegangen sind.

Gesicherte Client-Nachrichten ohne Option 82

Zeigt die Anzahl der Nachrichten des DHCP-Client, die ohne *Option 82*-Informationen auf dem vertrauenswürdigen Interface eingegangen sind.

7.2 DHCP Server

[Erweitert > 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 Standard-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. Ist der DHCP-Client außerstande, die Adresse zu verlängern, geht die Adresse 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

[Erweitert > DHCP Server > Global]

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

Funktion

Funktion

Schaltet die DHCP-Server-Funktion des Geräts global ein oder aus.

Mögliche Werte:

- `An`
- `Aus` (Voreinstellung)

Konfiguration

IP-Überprüfung

Aktiviert/deaktiviert das Prüfen auf eindeutige IP-Adressen. Vor dem Zuweisen einer IP-Adresse prüft der Server mit einer *ICMP Echo*-Abfrage, ob diese IP-Adresse bereits im Netz verwendet wird.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *IP-Überprüfung* ist aktiv.
- `unmarkiert`
  Die Funktion *IP-Überprüfung* ist inaktiv.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

7.2.2 DHCP-Server Pool

[Erweitert > 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 nimmt maximal 128 Pools auf. Die Pools zusammen nehmen maximal 1000 Einträge auf.

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 eine 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. Kontaktiert ein Client mit einer bekannten Hardware-Kennung das Gerät, weist der DHCP-Server die statische IP-Adresse zu.

Kontaktiert ein DHCP-Client bei dynamischer Zuweisung einen Port, 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. Dies ermöglicht Ihnen, einen IP-Adressbereich zu erzeugen, der Lücken enthält.

Dieser Dialog zeigt die unterschiedlichen Informationen, 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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

VLAN-ID

Zeigt das VLAN, auf das sich der Tabelleneintrag bezieht.

Der Wert `1` entspricht dem Standard-VLAN für das Management des Geräts.

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 mit Doppelpunkt-Trennzeichen fest, zum Beispiel `00:11:22:33:44:55`.
- `-`
  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. Empfängt der DHCP-Server die Anfrage eines Clients über ein anderes DHCP-Relay, ignoriert er diese Anfrage.

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.xml`

Wenn Sie dieses Feld leer lassen, lässt das Gerät dieses Optionsfeld in der DHCP-Nachricht leer.

Lease-Time [s]

Legt die Vergabezeit in Sekunden fest.

Mögliche Werte:

- `60..220752000` (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 dieses Feld leer lassen, lässt das Gerät dieses Optionsfeld in der DHCP-Nachricht leer.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..64 Zeichen

7.2.3 DHCP-Server Lease-Tabelle

[Erweitert > DHCP Server > Lease-Tabelle]

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

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

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.

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.

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.

7.3 DNS

[Erweitert > DNS]

Das Menü enthält die folgenden Dialoge:
- DNS-Client

7.3.1 DNS-Client

[Erweitert > DNS > Client]

DNS (Domain Name System) ist ein Dienst im Netz, der Hostnamen in IP-Adressen übersetzt. Diese Namensauflösung ermöglicht Ihnen, andere Geräte mit ihrem Hostnamen anstatt mit ihrer IP-Adresse zu erreichen.

Mittels der Funktion *Client* sendet das Gerät Anfragen zur Auflösung von Hostnamen in IP-Adressen an einen DNS-Server.

Das Menü enthält die folgenden Dialoge:
- DNS-Client Global
- DNS-Client Aktuell
- DNS-Client Statisch
- DNS-Client Statische Hosts

7.3.1.1 DNS-Client Global

[Erweitert > DNS > Client > Global]

In diesem Dialog schalten Sie die Funktion *Client* und die Funktion *Cache* ein.

Funktion

Funktion

Schaltet die Funktion *Client* ein/aus.

Mögliche Werte:

- *An*
  Die Funktion *Client* ist eingeschaltet.
  Das Gerät sendet Anfragen zur Auflösung von Hostnamen in IP-Adressen an einen DNS-Server.
- *Aus* (Voreinstellung)
  Die Funktion *Client* ist ausgeschaltet.

Cache

Schaltflächen

Cache leeren

Entfernt jeden Eintrag aus dem DNS-Cache.

Cache

Schaltet die Funktion *Cache* ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Die Funktion *Cache* ist eingeschaltet.
  Das Gerät speichert flüchtig im Cache bis zu 128 DNS-Server-Antworten (Hostname und zugehörige IP-Adresse). Bei einer erneuten Anfrage löst das Gerät den Hostnamen selbst auf, wenn der Cache einen passenden Eintrag enthält. Die erneute Anfrage bei einem DNS-Server ist damit unnötig.
- *Aus*
  Die Funktion *Cache* ist ausgeschaltet.

7.3.1.2 DNS-Client Aktuell

[Erweitert > DNS > Client > Aktuell]

Dieser Dialog zeigt, an welche DNS-Server das Gerät Anfragen zur Auflösung von Hostnamen in IP-Adressen weiterleitet.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Index

Zeigt die fortlaufende Nummer des DNS-Servers.

Adresse

Zeigt die IP-Adresse des DNS-Servers. Das Gerät leitet Anfragen zur Auflösung von Hostnamen in IP-Adressen an den DNS-Server mit dieser IP-Adresse weiter.

7.3.1.3 DNS-Client Statisch

[Erweitert > DNS > Client > Statisch]

In diesem Dialog legen Sie die DNS-Server fest, an die das Gerät Anfragen zur Auflösung von Hostnamen in IP-Adressen weiterleitet.

Das Gerät ermöglicht Ihnen, selbst bis zu 4 IP-Adressen festzulegen oder die IP-Adressen von einem DHCP-Server zu beziehen.

Konfiguration

Konfigurationsquelle

Legt die Quelle fest, aus der das Gerät die IP-Adresse anzufragender DNS-Server bezieht.

Mögliche Werte:

- `user`
  Das Gerät verwendet die in der Tabelle festgelegten IP-Adressen.
- `mgmt-dhcp` (Voreinstellung)
  Das Gerät verwendet die IP-Adressen, die der DHCP-Server dem Gerät übergibt.

Domänen-Name

Legt den Domain-Namen gemäß RFC 1034 fest, den das Gerät an Hostnamen ohne Domain-Suffix anfügt.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

Request-Timeout [s]

Legt den Zeitabstand in Sekunden für das erneute Senden einer Anfrage an den Server fest.

Mögliche Werte:

- `0`
  Deaktiviert die Funktion. Das Gerät sendet keine erneute Anfrage an den Server.
- `1..3600` (Voreinstellung: `3`)

Request-Wiederholungen

Legt fest, wie viele Male das Gerät das Senden einer Anfrage wiederholt.

Voraussetzung ist, dass Sie im Feld *Request-Timeout [s]* einen Wert >`0`festlegen.

Mögliche Werte:

- `0..100` (Voreinstellung: `2`)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Index

Zeigt die fortlaufende Nummer des DNS-Servers.

Das Gerät ermöglicht Ihnen, bis zu 4 DNS-Server festzulegen.

Adresse

Legt die IP-Adresse des DNS-Servers fest.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)

Aktiv

Aktiviert/deaktiviert den Tabelleneintrag.

Das Gerät sendet Anfragen an den im ersten aktiven Tabelleneintrag konfigurierten DNS-Server. Erhält das Gerät von diesem Server keine Antwort, sendet es Anfragen an den im nächsten aktiven Tabelleneintrag konfigurierten DNS-Server.

Mögliche Werte:

- `markiert`
  Der DNS-Client sendet Anfragen an diesen DNS-Server.
  Voraussetzungen:
  - ☐ Schalten Sie im Dialog *Erweitert > DNS > Global* die DNS-Client-Funktion ein.
  - ☐ Legen Sie im Rahmen *Konfiguration*, Dropdown-Liste *Konfigurationsquelle* den Wert `user` fest.
- `unmarkiert` (Voreinstellung)
  Das Gerät sendet keine Anfragen an diesen DNS-Server.

7.3.1.4 DNS-Client Statische Hosts

[Erweitert > DNS > Client > Statische Hosts]

Dieser Dialog ermöglicht Ihnen, bis zu 64 Hostnamen festzulegen, die mit jeweils einer IP-Adresse verknüpft sind. Bei Anfragen zur Auflösung von Hostnamen in IP-Adressen sucht das Gerät in dieser Tabelle nach einem passenden Eintrag. Findet das Gerät keinen passenden Eintrag, leitet es die Anfrage weiter.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Index

Zeigt die Index-Nummer, auf die sich der Tabelleneintrag bezieht.

Mögliche Werte:

- `1..64`

Name

Legt den Host-Namen fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen

IP-Adresse

Legt die IP-Adresse fest, mit der der Host erreichbar ist.

Mögliche Werte:

- Gültige IPv4-Adresse

Aktiv

Aktiviert/deaktiviert den Tabelleneintrag.

Mögliche Werte:

- `markiert`
  Das Gerät löst eine Anfrage nach dem Host-Namen für diesen Eintrag auf.
- `unmarkiert`
  Nachdem das Gerät eine Anforderung für diesen Host-Namen empfangen hat, sendet es eine Anforderung zur Auflösung an einen der konfigurierten Namens-Server.

7.4 Industrie-Protokolle

[Erweitert > Industrie-Protokolle]

Das Menü enthält die folgenden Dialoge:

- IEC61850-MMS
- Modbus TCP
- EtherNet/IP
- OPC UA Server
- PROFINET

7.4.1 IEC61850-MMS

[Erweitert > Industrie-Protokolle > 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. Wenn der Schreibzugriff für IEC61850/MMS eingeschaltet ist, 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 die Möglichkeit eines unbefugten Zugriffs zu verringern.

Dieser Dialog ermöglicht Ihnen, 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

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.

Information

Status

Zeigt den gegenwärtigen Status des *IEC61850-MMS*-Servers.

Mögliche Werte:
- `unavailable`
- `starting`
- `running`

- *stopping*
- *halted*
- *error*

Aktive Verbindungen

Zeigt die Anzahl der aktiven MMS-Server-Verbindungen.

Konfiguration

Schaltflächen

ICD-Datei herunterladen

Kopiert die ICD-Datei auf Ihren PC.

Schreibzugriff

Aktiviert/deaktiviert den Schreibzugriff auf den MMS-Server

Mögliche Werte:

- `markiert`
  Der Schreibzugriff auf den MMS-Server ist aktiviert. Diese Einstellung ermöglicht Ihnen, 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.

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
  Das Gerät akzeptiert die folgenden Zeichen:
  - `_`
  - `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.

Sitzungen (max.)

Legt die maximale Anzahl an MMS-Server-Verbindungen fest.

Mögliche Werte:

- `1..15` (Voreinstellung: `5`)

7.4.2 Modbus TCP

[Erweitert > Industrie-Protokolle > 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 ermöglicht Ihnen, 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 „Konfiguration“.

Der Dialog ermöglicht Ihnen, 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 *Modbus TCP*-Schreibzugriffs stellt möglicherweise ein unvermeidbares Sicherheitsrisiko dar, da das Protokoll keine Benutzerzugriffe authentifiziert.

Um das unvermeidbare 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 Ihren Geräten zugewiesen sind. Darüber hinaus ist die Voreinstellung für das Aktivieren der Überwachungsfunktion im Dialog *Diagnose* > Statuskonfiguration > *Sicherheitsstatus*, Registerkarte *Global* aktiv.

Funktion

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

Schreibzugriff

Aktiviert/deaktiviert den Schreibzugriff auf die *Modbus TCP* parameter.

Anmerkung: Das Aktivieren des *Modbus TCP*-Schreibzugriffs stellt möglicherweise ein unvermeidbares Sicherheitsrisiko dar, da das Protokoll keine Benutzerzugriffe authentifiziert.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Der Lese-/Schreibzugriff für den *Modbus TCP*-Server ist aktiv. Dies ermöglicht Ihnen, die Geräte-Konfiguration über das *Modbus TCP*-Protokoll zu ändern.
- `unmarkiert`
  Der Lesezugriff für den *Modbus TCP*-Server ist aktiv.

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.

Sitzungen (max.)

Legt die maximale Anzahl von gleichzeitigen Sitzungen fest, die der *Modbus TCP*-Server aufrechterhält.

Mögliche Werte:

- `1..5` (Voreinstellung: `5`)

7.4.3 EtherNet/IP

[Erweitert > Industrie-Protokolle > EtherNet/IP]

Dieser Dialog ermöglicht Ihnen, die *EtherNet/IP*-Einstellungen festzulegen. Sie haben die folgenden Möglichkeiten:

- Die Funktion *EtherNet/IP* im Gerät ein-/ausschalten.
- Die Lese-/Schreibfähigkeit des Protokolls *EtherNet/IP* aktivieren/deaktivieren.
- Das Elektronische Datenblatt (EDS) vom Gerät herunterladen.

Funktion

Funktion

Schaltet die Funktion *EtherNet/IP* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *EtherNet/IP* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *EtherNet/IP* ist ausgeschaltet.

Konfiguration

Schaltflächen

EDS-Datei herunterladen

Kopiert die folgenden Informationen in eine Zip-Datei auf Ihren PC:

- Elektronisches Datenblatt (EDS) mit gerätebezogenen Informationen
- Gerätsymbol

Schreibzugriff

Aktiviert/deaktiviert den Lese-/Schreibzugriff des Protokolls *EtherNet/IP*.

Mögliche Werte:

- `markiert`
  Das Protokoll *EtherNet/IP* akzeptiert GET- und SET-Requests.
- `unmarkiert` (Voreinstellung)
  Das Protokoll *EtherNet/IP* akzeptiert ausschließlich GET-Requests.

7.4.4 OPC UA Server

[Erweitert > Industrie-Protokolle > OPC UA Server]

Das Protokoll *OPC UA* ist ein standardisiertes Protokoll für die industrielle Kommunikation, das in der Norm IEC 62541 definiert ist. Die Funktion *OPC UA Server* überwacht die *OPC UA*-Informationsmodell-Daten von Geräten für die industrielle Automatisierung wie speicherprogrammierbare Steuerungen (SPS), Sensoren und Messgeräte.

Um die *OPC UA*-Informationsmodell-Daten der angeschlossenen Endgeräte zu überwachen, verwenden Sie eine *OPC UA*-Client-Anwendung.

In diesem Dialog schalten Sie die Funktion *OPC UA Server* ein und legen die erforderlichen Einstellungen fest. Darüber hinaus können Sie in diesem Dialog die Anzahl der Sitzungen festlegen, die zeitgleich geöffnet sein dürfen. Der Dialog ermöglicht Ihnen die Verwaltung der *OPC UA*-Benutzerkonten, die erforderlich sind, um mit einer*OPC UA*-Client-Anwendung auf das Gerät zuzugreifen. Jeder *OPC UA*-Benutzer benötigt ein aktives *OPC UA*-Benutzerkonto, um Zugriff auf den *OPC UA*-Server des Geräts zu erhalten.

Funktion

Funktion

Schaltet die Funktion *OPC UA Server* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *OPC UA Server* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *OPC UA Server* ist ausgeschaltet.

Konfiguration

Listening-Port

Legt die TCP-Port-Nummer fest, die der *OPC UA Server*-Server für die Kommunikation verwendet.

Mögliche Werte:

- `1..65535` (Voreinstellung: `4840`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Sitzungen (max.)

Legt fest, wie viele gleichzeitige *OPC UA*-Verbindungen zum Gerät maximal möglich sind. Jede zugreifende *OPC UA*-Client-Anwendung stellt eine separate *OPC UA*-Verbindung zum Gerät her.

Mögliche Werte:

- `1..5` (Voreinstellung: `5`)

Security-Policy

Legt das Authentifizierungsprotokoll fest, welches das Gerät für den *OPC UA*-Benutzer anwendet.

Mögliche Werte:

- *`kein`* (Voreinstellung)
  Der *OPC UA*-Benutzer benötigt keine Authentifizierung.
- *`basic128Rsa15`*
  Der *OPC UA*-Benutzer authentifiziert sich mit dem Protokoll *Basic128Rsa15*.
- *`basic256`*
  Der *OPC UA*-Benutzer authentifiziert sich mit dem Protokoll *Basic256*.
- *`basic256Sha256`*
  Der *OPC UA*-Benutzer authentifiziert sich mit dem Protokoll *Basic256Sha256*.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erzeugen*, um der Tabelle einen neuen Eintrag hinzuzufügen. Das Gerät ermöglicht Ihnen, bis zu 4 *OPC UA*-Benutzerkonten festzulegen.

- Im Feld *Benutzername* legen Sie die Bezeichnung des *OPC UA*-Benutzerkontos fest.
  Mögliche Werte:
  Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
  Das Gerät akzeptiert die folgenden Zeichen:
  - `a..z`
  - `A..Z`
  - `0..9`
  - `<Leerzeichen>`
  - `-_`

Löschen

Entfernt den ausgewählten Tabelleneintrag.

Benutzername

Zeigt den Namen des *OPC UA*-Benutzers, der Zugriff auf das Gerät mit einer *OPC UA*-Client-Anwendung hat.

Passwort

Legt das Passwort fest, das der Benutzer für den Zugriff auf das Gerät mit einer *OPC UA* Client-Anwendung verwendet.

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
  Das Gerät akzeptiert die folgenden Zeichen:
  - `a..z`
  - `A..Z`
  - `0..9`
  - `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

Rolle

Legt die Rolle fest, die den Zugriff des *OPC UA*-Benutzers mit einer *OPC UA*-Client-Anwendung regelt.

Mögliche Werte:

- *`read-only`* (Voreinstellung)
  Das Benutzerkonto *OPC UA* hat Lesezugriff auf das Gerät. Der *OPC UA*-Benutzer kann die *OPC UA*-Informationsmodell-Daten der angeschlossenen Endgeräte ansehen.

Aktiv

Aktiviert/deaktiviert das *OPC UA*-Benutzerkonto im Gerät.

Mögliche Werte:

- `markiert`
  Das *OPC UA*-Benutzerkonto ist aktiv. Das Gerät akzeptiert die Anmeldung eines *OPC UA*-Benutzers mit diesem Benutzernamen.
- `unmarkiert` (Voreinstellung)
  Das *OPC UA*-Benutzerkonto ist inaktiv. Das Gerät verweigert die Anmeldung eines *OPC UA*-Benutzers mit diesem Benutzernamen.

7.4.5 PROFINET

[Erweitert > Industrie-Protokolle > PROFINET]

Dieser Dialog ermöglicht Ihnen, das PROFINET-Protokoll im Gerät zu konfigurieren, das zusammen mit PROFINET-Controllern und PROFINET-Geräten verwendet wird. Die Funktion *PROFINET* des Geräts basiert auf dem PROFINET-Stack V2.2 von Siemens für gängige Ethernet-Controller. Das PROFINET-Protokoll im Gerät entspricht Class B für Antworten in Echtzeit gemäß IEC 61158.

Funktionen mit direktem Einfluss auf die Funktion *PROFINET* erfordern das Ändern folgender voreingestellter Werte. Wenn Sie das Gerät in einer speziell erhältlichen *PROFINET*-Variante erworben haben, dann sind diese Werte bereits voreingestellt:

PROFINET

Dialog *Erweitert > Industrie-Protokolle > PROFINET*

- Rahmen *Funktion*
  Funktion = `An`
- Rahmen *Konfiguration*
  Feld *Stationsname* = `<leer>`

Netz

Dialog *Grundeinstellungen > Netz > IPv4*

- Rahmen *Management-Schnittstelle*
  Optionsfeld *Zuweisung IP-Adresse* = `Lokal`
- Rahmen *HiDiscovery Protokoll v1/v2*
  Dropdown-Liste *Zugriff* = `readOnly`
- Rahmen *IP-Parameter*
  Feld *IP-Adresse* = `0.0.0.0`
  Feld *Netzmaske* = `0.0.0.0`
  Feld *Gateway-Adresse* = `0.0.0.0`

VLAN

Dialog *Switching > Global*

- Rahmen *Konfiguration*
  Kontrollkästchen *VLAN-Unaware-Modus* = `markiert`

LLDP

Dialog *Diagnose > LLDP > Konfiguration*

- Rahmen *Konfiguration*
  Feld *Sende-Intervall [s]* = `5`
  Feld *Sende-Verzögerung [s]* = `1`

Funktion

Funktion

Schaltet die Funktion *PROFINET* im Gerät ein/aus.

Mögliche Werte:

- `An`
  Die Funktion *PROFINET* ist eingeschaltet.
- `Aus` (Voreinstellung)
  Die Funktion *PROFINET* ist ausgeschaltet.

Konfiguration

Schaltflächen

GSDML-Datei herunterladen

Kopiert die GSDML-Datei auf Ihren PC.

Stationsname

Legt den Namen des Geräts fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..240 Zeichen
  Das Gerät erlaubt keine Verwendung einer Ziffer als erstes Zeichen.

Information

Aktive Application-Relations

Zeigt, wie viele Application-Relations aktiv sind.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Port

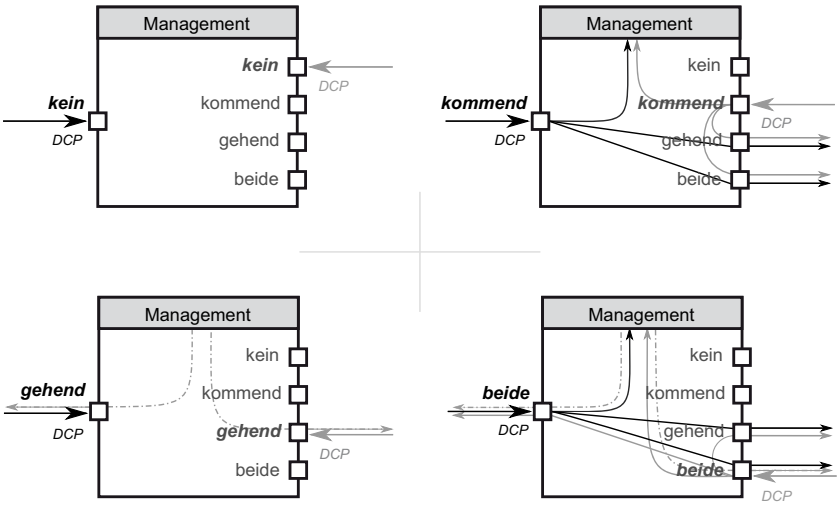
Zeigt die Nummer des Ports.

DCP mode

Legt die Richtung des Datenstroms für DCP-Pakete auf dem zu überwachenden Port fest.

Die speicherprogrammierbare Steuerung (SPS) erkennt PROFInet-Geräte über das Discovery-and-Configuration-Protokoll (DCP).

Die DCP-Identifzierunganfrage-Pakete sind multicast, die Antworten der Agenten sind unicast. Unabhängig von den Einstellungen leitet das Gerät die empfangenen DCP-Pakete an andere Ports mit der Einstellung `gehend` oder `beide` weiter.



Mögliche Werte:

- `kein`
  Der Agent antwortet auf keine Pakete, die auf diesem Port empfangen wurden. Der Port leitet keine Pakete weiter, die auf anderen Ports empfangen wurden.
- `kommend`
  Der Agent antwortet auf Pakete, die auf diesem Port empfangen wurden. Der Port leitet keine Pakete weiter, die auf anderen Ports empfangen wurden.
- `gehend`
  Der Agent antwortet auf keine Pakete, die auf diesem Port empfangen wurden. Der Port leitet Pakete weiter, die auf anderen Ports empfangen wurden.
- `beide` (Voreinstellung)
  Der Agent antwortet auf Pakete, die auf diesem Port empfangen wurden. Der Port leitet Pakete weiter, die auf anderen Ports empfangen wurden.

7.5 Digital-IO Modul

[Erweitert > Digital-IO Modul]

Mit den digitalen Eingängen können Sie Signale von digitalen Sensoren erfassen und weiterleiten.

Mit den digitalen Ausgängen können Sie das von den Eingängen übermittelte Signal auf die Aktoren anwenden. Die Spannung am digitalen Ausgang beträgt +24 VDC. Als Aktor können Sie zum Beispiel anschließen:

- Kontrollleuchten
- Einen akustischen Alarmgeber
- Ein Relais, das zum Beispiel eine Heizung, eine Pumpe, einen Motor oder ein Ventil ein-/ausschaltet.

Das Gerät überträgt Sensor-Signale in das gesamte Netz und aktiviert auf diese Weise die entsprechenden Aktoren. Über die Eingangsanschlüsse erfasst das Modul die Signale und leitet sie an die Ausgänge weiter. Abhängig von der Position der Aktoren leitet das Gerät die Signale an Ausgänge weiter, die entweder auf demselben Modul, auf einem anderen Moduls desselben Geräts oder auf einem anderen Gerät installiert sind.

Bildet das Gerät die digitalen Eingänge auf die digitalen Ausgänge ab, besteht eine 1:N-Beziehung. Das Gerät spiegelt den Datenstrom eines digitalen Eingangs an eine beliebige Anzahl von digitalen Ausgängen.

Bildet das Gerät die digitalen Ausgänge auf die digitalen Eingänge ab, besteht eine 1:1-Beziehung. Ein digitaler Ausgang spiegelt den Datenstrom eines digitalen Eingangs.

Der Dialog enthält die folgenden Registerkarten:

- [IO-Eingang]
- [IO-Ausgang]

[IO-Eingang]

Diese Registerkarte bietet Ihnen folgende Möglichkeiten:

- die Abfrage der digitalen Eingänge global aktivieren oder deaktivieren
- den Zeitabstand konfigurieren, in dem das Gerät die Werte der digitalen Eingänge abfragt
- die Protokollierung von Ereignissen aktivieren oder deaktivieren
- das Senden von SNMP-Traps aktivieren oder deaktivieren

Funktion

Funktion

Schaltet die zyklische Abfrage der digitalen Eingänge ein oder aus.

Mögliche Werte:

- `An`
  Ermöglicht das Abfragen der Eingangswerte.
- `Aus` (Voreinstellung)

Konfiguration

Aktualisierungs-Intervall [ms]

Legt den Zeitabstand in Millisekunden fest, in dem das Gerät die Werte der digitalen Eingänge abfragt.

Mögliche Werte:

- `1000..10000` (Voreinstellung: `1000`)

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Input-ID

Zeigt die Steckplatznummer des Moduls (x) und die Nummer des digitalen Eingangs (o), für den dieser Eintrag gilt.

Schreibweise: `x.i`

Mögliche Werte:

- x =`0..7`
  Der Wert `0` entspricht der Haupteinheit (MU).
- i =`1..4`

Wert

Legt den digitalen Eingangspegel fest.

Mögliche Werte:

- `low`
  Die Eingangsspannung am digitalen Eingang beträgt 0 V.
- `high`
  Die Eingangsspannung am digitalen Eingang beträgt +24 VDC.
- `not-available`
  Die Eingangsspannung am digitalen Eingang hat einen anderen Wert als 0 V oder +24 VDC. Vergewissern Sie sich, dass das Modul vorhanden und ordnungsgemäß befestigt ist.

Ereignis protokollieren

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog *Diagnose > Bericht > System-Log*.

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiviert.
  Das Gerät prüft den Status der digitalen Eingänge im Intervall, das im Rahmen *Konfiguration*, Feld *Aktualisierungs-Intervall [ms]* festgelegt ist.
  Treten Änderungen an den digitalen Eingängen auf, protokolliert das Gerät ein Ereignis in der Log-Datei (System Log).
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ist deaktiviert.

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an den digitalen Eingängen erkennt.

Das Gerät prüft den Status der digitalen Eingänge im Intervall, das im Rahmen *Konfiguration*, Feld *Aktualisierungs-Intervall [ms]* festgelegt ist.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es Änderungen an den digitalen Eingängen 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 ein Trap-Ziel festlegen.

[IO-Ausgang]

Diese Registerkarte bietet Ihnen folgende Möglichkeiten:

- das Spiegeln der digitalen Eingänge auf die digitalen Ausgänge global aktivieren oder deaktivieren
- den Zeitabstand konfigurieren, in dem das Gerät die Werte der digitalen Eingänge abfragt
- die Ereignisprotokollierung bei Änderungen des Ausgangsstatus aktivieren oder deaktivieren
- das Senden von SNMP-Traps aktivieren oder deaktivieren
- die Quelle für die Spiegelung sowie die lokalen und entfernten Modul-Eingänge für die Ausgänge bestimmen, indem Sie die IP-Adresse und den SNMP-Port der Quelle festlegen

Funktion

Funktion

Schaltet das zyklische Einstellen der digitalen Ausgänge (IO Output) ein oder aus.

Mögliche Werte:

- *An*
  Aktiviert das Spiegeln der Eingangswerte auf die Ausgangs-Ports.
- *Aus* (Voreinstellung)
  Deaktiviert das Spiegeln der Eingangswerte auf die Ausgangs-Ports.

Konfiguration

Aktualisierungs-Intervall [ms]

Legt den Wert für das Aktualisierungsintervall des Ausgangs in Millisekunden fest.

Mögliche Werte:

- `1000..10000` (Voreinstellung: `1000`)
  Die Genauigkeit des Intervall-Wertes beträgt 100 ms.

Wiederholungen

Legt die Anzahl von Wiederholungen für Ausgangswerte fest.

Mögliche Werte:

- `1..10` (Voreinstellung: `3`)
  Wenn SNMP-Get-Anfragen unbeantwortet zurückkommen, dann setzt das Gerät den Ausgangswert auf `invalid`, nachdem es die benutzerdefinierte Anzahl von Wiederholungen erreicht hat.

Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 18.

Output-ID

Zeigt die Steckplatznummer des Moduls (x) sowie die Nummer des digitalen Ausgangs (o), für den dieser Eintrag gilt.

Schreibweise: `x.o`

Mögliche Werte:

- x =`0..7`
  Der Wert `0` entspricht der Haupteinheit (MU).
- o =`1..4`

Wert

Legt den digitalen Ausgangspegel am Relais fest.

Mögliche Werte:

- `low`
  Der Ausgangspegel hat den Zustand „0“.
- `high`
  Der Ausgangspegel hat den Zustand „1“.
- `not-available`
  Der Ausgangspegel hat einen anderen Zustand als `low` oder `high`.
  Prüfen Sie, ob im Rahmen *Funktion* das Optionsfeld *`An`* ausgewählt ist.
- `invalid`
  Der Ausgangspegel ist `low`, das Gerät hat keine Möglichkeit, die Informationen vom IO-Eingang zu lesen.
- `not-configured`
  Der Ausgangspegel ist `low`.
  Prüfen Sie die Einstellungen des IO-Ausgangs.

Quell-Adresse

Legt die IP-Adresse des mit einem Modul bestückten Geräts fest, von dem aus Sie einen digitalen Eingang analysieren wollen.

Das Gerät spiegelt einen Eingang pro Ausgang.

Mögliche Werte:

- Gültige IPv4-Adresse
- `0.0.0.0`
  Deaktiviert die Funktion.
- `127.0.0.1`
  Lokaler Eingang.

SNMP-Quell-Port

Legt die SNMP-Port-Nummer des mit einem Modul bestückten Geräts fest, von dem aus Sie einen digitalen Eingang analysieren wollen.

Das Gerät spiegelt einen Eingang pro Ausgang.

Mögliche Werte:

- `1..65535` (Voreinstellung: `161`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

Input-ID

Steckplatznummer des Moduls (x) und Nummer des digitalen Eingangs (o), für den dieser Eintrag gilt.

Schreibweise: x.i

Mögliche Werte:

- x = `0..7`
  Der Wert `0` entspricht der Haupteinheit (MU).
- i = `1..4`

Ereignis protokollieren

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog *Diagnose > Bericht > System-Log*.

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiviert.
  Das Gerät prüft den Status der digitalen Ausgänge im Intervall, das im Rahmen *Konfiguration*, Feld *Aktualisierungs-Intervall [ms]* festgelegt ist.
  Treten Änderungen an den digitalen Ausgängen auf, protokolliert das Gerät ein Ereignis in der Log-Datei (System Log).
- `unmarkiert` (Voreinstellung)
  Die Protokollierung ist deaktiviert.

Trap senden

Aktiviert/deaktiviert das Senden von SNMP-Traps, wenn das Gerät eine Änderung an den digitalen Ausgängen erkennt.

Das Gerät prüft den Status der digitalen Ausgänge im Intervall, das im Rahmen *Konfiguration*, Feld *Aktualisierungs-Intervall [ms]* festgelegt ist.

Mögliche Werte:

- `markiert`
  Das Senden von SNMP-Traps ist aktiv.
  Das Gerät sendet einen SNMP-Trap, wenn es Änderungen an den digitalen Ausgängen 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 ein Trap-Ziel festlegen.

7.6 Command Line Interface

[Erweitert > CLI]

Dieser Dialog ermöglicht Ihnen, mit dem Command Line Interface auf das Gerät zuzugreifen.

Die Voraussetzungen sind:
- Schalten Sie im Gerät den SSH-Server ein, siehe Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- Installieren Sie auf Ihrer Workstation eine SSH-fähige Client-Anwendung, die in Ihrem Betriebssystem einen Handler für URLs registriert, die mit `ssh://` beginnen.

Schaltflächen

SSH-Verbindung starten

Öffnet die SSH-fähige Client-Anwendung.

Wenn Sie die Schaltfläche klicken, übergibt die Web-Anwendung den URL des Geräts beginnend mit `ssh://` und den Benutzernamen des gegenwärtig angemeldeten Benutzers.

Wenn der Web-Browser eine SSH-fähige Client-Anwendung findet, dann stellt der SSH-fähige Client eine Verbindung mit dem SSH-Protokoll zum Gerät her.

A Stichwortverzeichnis

0-9
802.1D/p-Mapping 271
802.1X 111, 152

A
Access-Control-Listen 208
ACL 208
Adresskonflikt-Erkennung 30, 399
Aging-Time 231, 403
Alarme 392
Anforderungsintervall 79
ARP 399
ARP-Inspection 197
ARP-Tabelle 403
Audit-Trail 468
Ausgangs-Lastbegrenzer 234
Authentifizierungs-Historie 166
Authentifizierungs-Liste 111
Auto-Disable 148, 149, 185, 200, 202, 324, 426, 427, 433, 451

B
Benutzerverwaltung 105
Boundary Clock 87
Bridge 320

C
CLI 141
Command Line Interface 141
Community-Namen 143

D
DHCP-L2-Relay 469
DHCP-Server 474
DHCP-Snooping 183
Digitalausgang 504
Digitaleingang 26, 501
DNS 482
DNS-Cache 483
DNS-Client 483
Domain Name System 482
DoS 179
DSCP 273
Dynamic ARP Inspection 197

E
EAPOL 164
EDS für EtherNet/IP herunterladen 494
Eingangs-Lastbegrenzer 234
Einstellungen 38
E-Mail Benachrichtigung 406
ENVM 36, 48, 51, 372, 379, 387, 465
Ereignis-Schweregrad 411, 462
EtherNet/IP 381, 494
EtherNet/IP, EDS herunterladen 494
EtherNet/IP, Lese-/Schreibfähigkeit 494
Externer Speicher 25, 36, 48, 51, 465

F
FDB 237
Fingerprint 129, 133
Flash-Speicher 36, 396
Flusskontrolle 231
Forwarding-Tabelle 237

G
GARP 263
Geräte-Software 34
Geräte-Software Backup 34
Gerätestatus 21, 370
GMRP 264
Grenzwerte Netzlast 234
Guards 337
GVRP 266

H
Hardware-Uhr 73
Hardware-Zustand 396
Häufig gestellte Fragen 515
HiDiscovery 30, 379, 468
HIPER-Ring 317
Host-Key 131
HTML 395, 467
HTTP 131
HTTPS 132
HTTP-Server 378

I
IAS 111, 168
IEC61850 MMS 380, 489
IEEE 802.1X 111
IGMP-Snooping 239
Industrial HiVision 11, 125
Ingress Filtering 305
Integrierter Authentifikations-Server 111, 168
IO-Eingang 26, 501
IP Source Guard 193
IP-Adressen Konflikterkennung 399
IP-DSCP-Mapping 273
IPv4-Regel 209
IP-Zugriffsbeschränkung 136

K
Kabeldiagnose 421
Konfigurations-Check 397
Konfigurationsprofil 18, 38

L

L2-Relay . . . 469
Laden/Speichern . . . 38
Lastbegrenzer . . . 234
LDAP . . . 111
Lese-/Schreibfähigkeit für EtherNet/IP . . . 494
Link-Aggregation . . . 341
Link-Backup . . . 349
LLDP . . . 441
Logdatei . . . 69, 467
Login-Banner . . . 142, 144
Loops . . . 318
Loop-Schutz . . . 387

M

MAC Address Conflict Detection . . . 30
MAC-Adress-Filter . . . 237
MAC-Adress-Tabelle . . . 237
MAC-Flooding . . . 147
MAC-Regel . . . 218
MAC-Spoofing . . . 149
Mail-Benachrichtigung . . . 406
Management-VLAN . . . 30
Management-Zugriff . . . 30, 136
Manufacturing Message Specification . . . 489
Media Redundancy Protocol . . . 313
MMRP . . . 255
MMS . . . 489
Modbus TCP . . . 381, 492
Module . . . 372, 387
MRP . . . 313
MRP-IEEE . . . 253
MSTP . . . 320
MVRP . . . 260

N

Netzlast . . . 60
Netzteil . . . 23, 373, 388
Neustart . . . 69
NVM . . . 18, 36, 48

P

Passwort . . . 106, 376, 377
Passwort-Länge . . . 106, 376
Persistentes Ereignisprotokoll . . . 464
PoE . . . 61
Port-basierte Zugriffskontrolle . . . 152
Port-Clients . . . 162
Port-Konfiguration . . . 156, 269
Port-Mirroring . . . 437
Port-Monitor . . . 433
Port-Priorität . . . 269
Portsicherheit . . . 147
Port-Statistiken . . . 164
Port-VLAN . . . 304
Power over Ethernet . . . 61
Pre-Login-Banner . . . 144
PROFINET . . . 381, 498

Q
Queue-Management 275
Queues 268

R
RADIUS 111, 169
RAM 47
RAM-Test 404
RCP 365
Redundant Coupling Protocol 365
Relay 469
Ring-/Netzkopplung 359
Ringstruktur 313
RNC 359
Root-Bridge 320
RSTP 318, 320

S
Schulungsangebote 515
Schweregrad 411, 462
Secure Shell 127
Selbsttest 404
Serielle Schnittstelle 378
sFlow 454
SFP-Modul 420
Sicherheitsstatus 22, 375
Signalkontakt 22, 383
SNMP-Server 125, 378
SNMP-Traps 58, 63, 65, 149, 320, 345, 371, 376, 385, 392, 401, 426, 503, 506
SNMPv1/v2 143
SNTP 77
SNTP-Client 78
SNTP-Server 82
Software-Backup 34
Software-Update 34
Sommerzeit 74
Source Guard 193
Spanning Tree Protocol 318
SSH-Server 127
Subring 354
Support-Informationen (ZIP-Archiv) 462
Syslog 415
System Log 467
Systeminformationen 395
System-Monitor 404
Systemzeit 73

T
Technische Fragen 515
Telnet-Server 126, 377
Temperatur 24, 371, 386
Topologie-Erkennung 446
Transparent Clock 97
Traps 58, 63, 65, 149, 320, 345, 371, 376, 385, 392, 401, 426, 503, 506
Trap-Ziel 392
Trust Modus 269
Twisted-Pair 421

U
Unaware-Modus 231

V
Verschlüsselung 38
Virtual Local Area Network 299
VLAN 30, 299, 453
VLAN Konfiguration 302
VLAN-Ports 304
VLAN-Unaware-Modus 231

W
Warteschlange (Queue) 268
Watchdog 38, 40
Webserver 131, 132

Z
Zähler-Reset 69
Zeitprofil 227
Zertifikat 23, 47, 117, 134, 135, 380, 408, 416
ZIP-Archiv mit Support-Informationen 462
Zugriffsbeschränkung 136
Zugriffskontrolle 152

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 www.hirschmann.com.

Eine Liste von Telefonnummern und E-Mail-Adressen für direkten technischen Support durch Hirschmann finden Sie unter hirschmann-support.belden.com.

Sie finden auf dieser Website außerdem eine kostenfreie Wissensdatenbank sowie einen Download-Bereich für Software.

Technische Unterlagen

Die aktuellen Handbücher und Bedienungsanleitungen für Hirschmann-Produkte finden Sie unter doc.hirschmann.com.

Customer Innovation Center

Das Customer Innovation 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 www.belden.com/solutions/customer-innovation-center.
- Der Support reicht von der Inbetriebnahme über den Bereitschaftsservice bis zu Wartungskonzepten.

Mit dem Customer Innovation Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.

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 unterstützen uns, die Qualität und den Informationsgrad dieser Dokumentation noch zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	gut	befriedigend	mäßig	schlecht
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

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

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
  Deutschland

HIRSCHMANN

A BELDEN BRAND

Anwender-Handbuch

Konfiguration
MICE Switch Power MSP30
HiOS-2A

Technische Unterstützung
https://hirschmann-support.belden.com

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.

© 2021 Hirschmann Automation and Control GmbH

Handbücher sowie Software sind urheberrechtlich geschützt. Alle Rechte bleiben vorbehalten. Das Kopieren, Vervielfältigen, Übersetzen, Umsetzen in irgendein elektronisches Medium oder maschinell lesbare Form im Ganzen oder in Teilen ist nicht gestattet. Eine Ausnahme gilt für die Anfertigungen einer Sicherungskopie der Software für den eigenen Gebrauch zu Sicherungszwecken.

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

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

Die aktuelle Benutzerdokumentation für Ihr Gerät finden Sie unter: doc.hirschmann.com

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

Inhalt

Sicherheitshinweise . . . 11

Über dieses Handbuch . . . 13

Legende . . . 14

Ersetzen eines defekten Geräts . . . 15

1 Benutzeroberflächen . . . 17
1.1 Grafische Benutzeroberfläche . . . 17
1.2 Command Line Interface . . . 18
1.2.1 Datenverbindung vorbereiten . . . 18
1.2.2 Zugriff auf das Command Line Interface mit Telnet . . . 18
1.2.3 Zugriff auf das Command Line Interface mit SSH (Secure Shell) . . . 21
1.2.4 Zugriff auf das Command Line Interface über die serielle Schnittstelle . . . 23
1.2.5 Modus-basierte Kommando-Hierarchie . . . 25
1.2.6 Ausführen von Kommandos . . . 29
1.2.7 Aufbau eines Kommandos . . . 30
1.2.8 Beispiele für Kommandos . . . 32
1.2.9 Eingabeprompt . . . 33
1.2.10 Tastaturkombinationen . . . 34
1.2.11 Eingabehilfen . . . 36
1.2.12 Anwendungsfälle . . . 37
1.2.13 Service Shell . . . 38
1.3 System-Monitor . . . 41
1.3.1 Funktionsumfang . . . 41
1.3.2 System-Monitor starten . . . 41

2 IP-Parameter festlegen . . . 43
2.1 Grundlagen IP Parameter . . . 43
2.1.1 IPv4 . . . 43
2.2 IP-Parameter mit dem Command Line Interface festlegen . . . 47
2.2.1 IPv4 . . . 47
2.3 IP-Parameter mit HiDiscovery festlegen . . . 49
2.4 IP-Parameter mit grafischer Benutzeroberfläche festlegen . . . 51
2.4.1 IPv4 . . . 51
2.5 IP-Parameter mit BOOTP festlegen . . . 52
2.6 IP-Parameter mit DHCP festlegen . . . 53
2.6.1 IPv4 . . . 53
2.7 Erkennung von Adresskonflikten verwalten . . . 55
2.7.1 Aktive und passive Erkennung . . . 55

3 Zugriff auf das Gerät . . . 57
3.1 Berechtigungen . . . 57
3.2 Erste Anmeldung (Passwortänderung) . . . 58
3.3 Authentifizierungs-Listen . . . 59
3.3.1 Anwendungen . . . 59
3.3.2 Richtlinien . . . 59
3.3.3 Authentifizierungs-Listen verwalten . . . 59
3.3.4 Einstellungen anpassen . . . 60

3.4 Benutzerverwaltung . . . 62
3.4.1 Berechtigungen . . . 62
3.4.2 Benutzerkonten verwalten . . . 64
3.4.3 Voreinstellung . . . 65
3.4.4 Voreingestellte Passwörter ändern . . . 65
3.4.5 Neues Benutzerkonto einrichten . . . 66
3.4.6 Benutzerkonto deaktivieren . . . 67
3.4.7 Richtlinien für Passwörter anpassen . . . 68
3.5 LDAP . . . 70
3.5.1 Abstimmung mit dem Server-Administrator . . . 70
3.5.2 Beispiel-Konfiguration . . . 71
3.6 SNMP-Zugriff . . . 74
3.6.1 SNMPv1/v2-Zugriff . . . 74
3.6.2 SNMPv3-Zugriff . . . 74

4 Die Systemzeit im Netz synchronisieren . . . 77
4.1 Grundeinstellungen . . . 77
4.1.1 Uhrzeit einstellen . . . 77
4.1.2 Automatische Sommerzeitumschaltung . . . 79
4.2 SNTP . . . 80
4.2.1 Vorbereitung . . . 81
4.2.2 Einstellungen des SNTP-Clients festlegen . . . 82
4.2.3 Einstellungen des SNTP-Servers festlegen . . . 83
4.3 PTP . . . 84
4.3.1 Typen von Uhren . . . 84
4.3.2 Best-Master-Clock-Algorithmus . . . 85
4.3.3 Laufzeitmessung . . . 85
4.3.4 PTP-Domänen . . . 86
4.3.5 PTP verwenden . . . 86

5 Konfigurationsprofile verwalten . . . 87
5.1 Geänderte Einstellungen erkennen . . . 87
5.1.1 Flüchtiger Speicher (RAM) und nichtflüchtiger Speicher (NVM) . . . 87
5.1.2 Externer Speicher (ACA) und nichtflüchtiger Speicher (NVM) . . . 88
5.2 Einstellungen speichern . . . 89
5.2.1 Konfigurationsprofil im Gerät speichern . . . 89
5.2.2 Konfigurationsprofil im externen Speicher speichern . . . 91
5.2.3 Konfigurationsprofil auf einem Remote-Server sichern . . . 91
5.2.4 Konfigurationsprofil exportieren . . . 92
5.3 Einstellungen laden . . . 94
5.3.1 Konfigurationsprofil aktivieren . . . 94
5.3.2 Konfigurationsprofil aus dem externen Speicher laden . . . 94
5.3.3 Konfigurationsprofil importieren . . . 96
5.4 Gerät auf Lieferzustand zurücksetzen . . . 99
5.4.1 Mit grafischer Benutzeroberfläche oder Command Line Interface . . . 99
5.4.2 System-Monitor starten . . . 99

6 Neueste Software laden . . . 101
6.1 Frühere Software-Version laden . . . 101
6.2 Software-Update vom PC . . . 102
6.3 Software-Update von einem Server . . . 103

6.4 Software-Update aus dem externen Speicher . . . 104
6.4.1 Manuell – durch den Administrator initiiert . . . 104
6.4.2 Automatisch – durch das Gerät initiiert . . . 104

7 Ports konfigurieren . . . 107
7.1 Port ein-/ausschalten . . . 107
7.2 Betriebsart wählen . . . 108

8 Unterstützung beim Schutz vor unberechtigtem Zugriff . . . 109
8.1 SNMPv1/v2-Community ändern . . . 109
8.2 SNMPv1/v2 ausschalten . . . 110
8.3 HTTP ausschalten . . . 111
8.4 Telnet ausschalten . . . 112
8.5 HiDiscovery-Zugriff ausschalten . . . 113
8.6 IP-Zugriffsbeschränkung aktivieren . . . 114
8.7 Session-Timeouts anpassen . . . 116
8.8 Nicht verwendete Module deaktivieren . . . 118

9 Datenverkehr kontrollieren . . . 119
9.1 Unterstützung beim Schutz vor DoS-Attacken . . . 119
9.1.1 Filter für *TCP*- und *UDP*-Pakete . . . 120
9.1.2 Filter für *IP*-Pakete . . . 124
9.1.3 Filter für *ICMP*-Pakete . . . 124
9.2 ACL . . . 127
9.2.1 Erzeugen und Bearbeiten von IPv4-Regeln . . . 128
9.2.2 Erzeugen und Konfigurieren einer IP-ACL im Command Line Interface . . . 129
9.2.3 Erzeugen und Bearbeiten von MAC-Regeln . . . 129
9.2.4 Erzeugen und Konfigurieren einer MAC-ACL im Command Line Interface . . . 130
9.2.5 Zuweisen von ACLs zu Ports oder VLANs . . . 131
9.3 MAC-Authentication-Bypass . . . 132

10 Netzlaststeuerung . . . 133
10.1 Gezielte Paketvermittlung . . . 133
10.1.1 Lernen der MAC-Adressen . . . 133
10.1.2 Aging gelernter MAC-Adressen . . . 133
10.1.3 Statische Adresseinträge . . . 134
10.2 Multicasts . . . 137
10.2.1 Beispiel für eine Multicast-Anwendung . . . 137
10.2.2 IGMP-Snooping . . . 137
10.3 Lastbegrenzung . . . 142
10.4 QoS/Priorität . . . 143
10.4.1 Beschreibung Priorisierung . . . 143
10.4.2 Behandlung empfangener Prioritätsinformationen . . . 144
10.4.3 VLAN-Tagging . . . 144
10.4.4 IP ToS (Type of Service) . . . 145
10.4.5 Handhabung der *Verkehrsklassen* . . . 146
10.4.6 Queue-Management . . . 147
10.4.7 Management-Priorisierung . . . 149
10.4.8 Priorisierung einstellen . . . 150
10.5 Differentiated Services . . . 154
10.5.1 DiffServ-Beispiel . . . 155

10.6 Flusskontrolle . . . 157
10.6.1 Halbduplex- oder Vollduplex-Verbindung. . . . 158
10.6.2 Flusskontrolle einrichten . . . 158

11 VLANs . . . 159
11.1 Beispiele für ein VLAN . . . 159
11.1.1 Beispiel 1 . . . 160
11.1.2 Beispiel 2 . . . 163
11.2 Gast-VLAN / Unauthentifiziertes VLAN . . . 168
11.3 RADIUS-VLAN-Zuordnung . . . 170
11.4 Voice-VLAN erzeugen . . . 171
11.5 MAC-basierte VLANs . . . 172
11.6 IP-Subnetz-basierte VLANs . . . 173
11.7 Protokoll-basiertes VLAN . . . 174
11.8 VLAN-Unaware-Modus . . . 175

12 Redundanz . . . 177
12.1 Netz-Topologie vs. Redundanzprotokolle . . . 177
12.1.1 Netz-Topologien . . . 177
12.1.2 Redundanzprotokolle . . . 178
12.1.3 Kombinationen von Redundanzprotokollen . . . 179
12.2 Media Redundancy Protocol (MRP) . . . 180
12.2.1 Netzstruktur . . . 180
12.2.2 Rekonfigurationszeit. . . . 181
12.2.3 Advanced Mode . . . 181
12.2.4 Voraussetzungen für MRP . . . 181
12.2.5 Erweiterte Informationen . . . 182
12.2.6 Beispiel-Konfiguration . . . 183
12.2.7 MRP-over-LAG . . . 188
12.3 HIPER-Ring-Client . . . 192
12.3.1 VLANs am HIPER-Ring . . . 192
12.3.2 Erweiterte Informationen . . . 193
12.3.3 HIPER-Ring über LAG . . . 195
12.4 Spanning Tree . . . 196
12.4.1 Grundlagen . . . 196
12.4.2 Regeln für die Erstellung der Baumstruktur . . . 200
12.4.3 Beispiele. . . . 202
12.5 Das Rapid Spanning Tree Protokoll . . . 205
12.5.1 Port-Rollen . . . 205
12.5.2 Port-Stati . . . 206
12.5.3 Spanning Tree Priority Vector . . . 207
12.5.4 Schnelle Rekonfiguration . . . 207
12.5.5 Gerät konfigurieren . . . 208
12.5.6 Guards . . . 210
12.5.7 Ring only mode . . . 213
12.6 Link-Aggregation . . . 215
12.6.1 Funktionsweise . . . 215
12.6.2 Link-Aggregation Beispiel . . . 216
12.7 Link-Backup . . . 218
12.7.1 Beschreibung Fail-Back . . . 218
12.7.2 Beispiel-Konfiguration . . . 219
12.8 FuseNet . . . 221

12.9 Subring . . . 222
12.9.1 Beschreibung für einen Subring . . . 222
12.9.2 Beispiel für einen Subring . . . 224
12.9.3 Subring-Beispielkonfiguration . . . 225
12.10 Subring mit LAG . . . 228
12.10.1 Beispiel . . . 228
12.11 Ring-/Netzkopplung . . . 232
12.11.1 Methoden der Ring-/Netzkopplung . . . 232
12.11.2 Erweiterte Informationen . . . 234
12.11.3 Ring-/Netzkopplung vorbereiten . . . 239
12.12 RCP . . . 253
12.12.1 Voraussetzungen für RCP . . . 255
12.12.2 Erweiterte Informationen . . . 255
12.12.3 Anwendungsbeispiel für RCP-Kopplung . . . 256

13 Funktionsdiagnose . . . 261
13.1 SNMP-Traps senden . . . 261
13.1.1 Auflistung der SNMP-Traps . . . 262
13.1.2 SNMP-Traps für Konfigurationsaktivitäten . . . 263
13.1.3 SNMP-Trap-Einstellung . . . 263
13.1.4 ICMP-Messaging . . . 264
13.2 Gerätestatus überwachen . . . 265
13.2.1 Ereignisse, die überwacht werden können . . . 265
13.2.2 Gerätestatus konfigurieren . . . 266
13.2.3 Gerätestatus anzeigen . . . 268
13.3 Sicherheitsstatus . . . 269
13.3.1 Ereignisse, die überwacht werden können . . . 269
13.3.2 Konfigurieren des Sicherheitsstatus . . . 270
13.3.3 Anzeigen des Sicherheitsstatus . . . 272
13.4 Out-of-Band-Signalisierung . . . 273
13.4.1 Signalkontakt steuern . . . 273
13.4.2 Gerätestatus und Sicherheitsstatus überwachen . . . 274
13.5 Portereignis-Zähler . . . 277
13.5.1 Erkennen der Nichtübereinstimmung der Duplex-Modi . . . 277
13.6 Auto-Disable . . . 279
13.7 SFP-Zustandsanzeige . . . 282
13.8 Topologie-Erkennung . . . 283
13.8.1 Anzeige der Topologie-Erkennung . . . 283
13.8.2 LLDP-MED . . . 284
13.9 Erkennen von Loops . . . 285
13.10 Unterstützung beim Schutz vor Layer-2-Loops . . . 286
13.10.1 Anwendungsbeispiel . . . 286
13.10.2 Empfehlungen für redundante Ports . . . 288
13.11 Benutzen der Funktion E-Mail-Benachrichtigung . . . 289
13.11.1 Absender-Adresse festlegen . . . 289
13.11.2 Auslösende Ereignisse festlegen . . . 289
13.11.3 Sendeintervall ändern . . . 291
13.11.4 Empfänger festlegen . . . 291
13.11.5 Mail-Server festlegen . . . 292
13.11.6 Funktion E-Mail-Benachrichtigung ein-/ausschalten . . . 292
13.11.7 Test-Nachricht senden . . . 293

13.12 Berichte . . . 294
13.12.1 Globale Einstellungen . . . 294
13.12.2 Syslog . . . 296
13.12.3 System-Log . . . 297
13.12.4 Syslog über TLS . . . 298
13.12.5 Audit Trail . . . 299
13.13 Netzanalyse mit TCPDump . . . 300
13.14 Datenverkehr beobachten . . . 301
13.14.1 Port-Mirroring . . . 301
13.14.2 VLAN-Mirroring . . . 302
13.14.3 Remote SPAN . . . 304
13.15 Selbsttest . . . 316
13.16 Kupferkabeltest . . . 318
13.17 Netzüberwachung mit sFlow . . . 319

14 Erweiterte Funktionen des Geräts . . . 321
14.1 Gerät als DHCP-Server verwenden . . . 321
14.1.1 Pro Port oder pro VLAN zugewiesene IP-Adressen . . . 321
14.1.2 Beispiel: DHCP-Server – Statische IP-Adresse . . . 322
14.1.3 Beispiel: DHCP-Server – Dynamischer IP-Adressbereich . . . 323
14.2 DHCP-L2-Relay . . . 324
14.2.1 Circuit- und Remote-IDs . . . 324
14.2.2 DHCP-L2-Relay-Konfiguration . . . 324
14.3 Gerät als DNS-Client verwenden . . . 327
14.3.1 Beispiel: DNS-Server konfigurieren . . . 327
14.4 Digitales I/O-Modul . . . 329
14.4.1 Digitale I/O-Signale verwalten . . . 329
14.5 GARP . . . 331
14.5.1 GMRP konfigurieren . . . 331
14.5.2 GVRP konfigurieren . . . 332
14.6 MRP-IEEE . . . 333
14.6.1 MRP-Funktion . . . 333
14.6.2 MRP-Timer . . . 333
14.6.3 MMRP . . . 334
14.6.4 MVRP . . . 336

15 Industrieprotokolle . . . 339
15.1 IEC 61850/MMS . . . 340
15.1.1 Switch-Modell für IEC 61850 . . . 340
15.1.2 Integration in ein Steuerungssystem . . . 341
15.2 Modbus TCP . . . 344
15.2.1 Modbus TCP/IP Client/Server-Modus . . . 344
15.2.2 Unterstützte Funktionen und Speicherzuordnung . . . 344
15.2.3 Beispiel-Konfiguration . . . 347
15.3 EtherNet/IP . . . 350
15.3.1 Integration in ein Steuerungssystem . . . 350
15.3.2 EtherNet/IP-Entity-Parameter . . . 351

15.4 PROFINET . . . 366
15.4.1 Gerätemodelle für PROFINET-GSDML-Version 2.3 . . . 366
15.4.2 Grafische Benutzeroberfläche und Command Line Interface . . . 367
15.4.3 Gerät in ein Steuerungssystem integrieren . . . 368
15.4.4 Gerät in die Konfiguration einbinden . . . 369
15.4.5 PROFINET-Parameter . . . 374
15.5 *OPC UA*-Server . . . 380
15.5.1 *OPC UA*-Server einschalten . . . 383
15.5.2 Ein *OPC UA*-Benutzerkonto einrichten . . . 384
15.5.3 Ein *OPC UA*-Benutzerkonto deaktivieren . . . 385
15.5.4 Ein *OPC UA*-Benutzerkonto löschen . . . 385

A Konfigurationsumgebung einrichten . . . 387
A.1 DHCP/BOOTP-Server einrichten . . . 387
A.2 DHCP-Server Option 82 einrichten . . . 391
A.3 SSH-Zugriff vorbereiten . . . 394
A.3.1 Schlüssel auf dem Gerät erzeugen . . . 394
A.3.2 Eigenen Schlüssel in das Gerät laden . . . 394
A.3.3 SSH-Client-Programm vorbereiten . . . 395
A.4 HTTPS-Zertifikat . . . 397
A.4.1 HTTPS-Zertifikatsverwaltung . . . 397
A.4.2 Zugang über HTTPS . . . 398

B Anhang . . . 399
B.1 Literaturhinweise . . . 399
B.2 Wartung . . . 400
B.3 Management Information BASE (MIB) . . . 401
B.4 Liste der RFCs . . . 403
B.5 Zugrundeliegende IEEE-Normen . . . 405
B.6 Zugrundeliegende IEC-Normen . . . 406
B.7 Zugrundeliegende ANSI-Normen . . . 407
B.8 Technische Daten . . . 408
15.5.5 Switching . . . 408
15.5.6 VLAN . . . 408
15.5.7 Access-Control-Listen (ACL) . . . 408
B.9 Copyright integrierter Software . . . 409
B.10 Verwendete Abkürzungen . . . 410

C Stichwortverzeichnis . . . 411

D Weitere Unterstützung . . . 419

E Leserkritik . . . 420

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.

Die Nichtbeachtung dieser Anweisungen kann Tod, schwere Verletzungen oder Sachschäden zur Folge haben.

Über dieses Handbuch

Das Anwender-Handbuch „Konfiguration“ 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 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 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
Verweis	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	Darstellung eines CLI-Kommandos oder des Feldinhalts in der grafischen Benutzeroberfläche

Auszuführen in der grafische Benutzeroberfläche

Auszuführen im Command Line Interface

Ersetzen eines defekten Geräts

Das Gerät bietet folgende Plug-and-Play-Lösungen, um ein defektes Gerät durch ein Gerät des gleichen Typs zu ersetzen:

- Das neue Gerät lädt das Konfigurationsprofil des ersetzten Geräts vom externen Speicher.
  Siehe „Konfigurationsprofil aus dem externen Speicher laden" auf Seite 94.
- Das neue Gerät erhält seine IP-Adresse mittels DHCP *Option 82*.
  Siehe „DHCP-L2-Relay" auf Seite 324.
  Siehe „DHCP-Server Option 82 einrichten" auf Seite 391.

Bei jeder Lösung erhält das neue Gerät beim Neustart die gleichen IP-Einstellungen, die das ersetzte Gerät zuvor hatte.

- Für Zugriffe auf das Management des Geräts über HTTPS verwendet das Gerät ein digitales Zertifikat. Sie haben die Möglichkeit, ein eigenes Zertifikat in das Gerät zu importieren.
  Siehe „HTTPS-Zertifikatsverwaltung" auf Seite 397.
- Für Zugriffe auf das Management des Geräts mittels SSH verwendet das Gerät einen RSA-Host-Key. Sie haben die Möglichkeit, einen eigenen Host-Key im PEM-Format in das Gerät zu importieren.
  Siehe „Eigenen Schlüssel in das Gerät laden" auf Seite 394.

1 Benutzeroberflächen

Das Gerät ermöglicht Ihnen, die Einstellungen des Geräts über folgende Benutzeroberflächen festzulegen.

Tab. 1: Benutzeroberflächen für Zugriff auf das Management des Geräts

Benutzeroberfläche	Erreichbar über …	Voraussetzung
Grafische Benutzeroberfläche	Ethernet (In-Band)	Web-Browser
Command Line Interface	Ethernet (In-Band) Serielle Schnittstelle (Out-of-Band)	Terminalemulations-Software
System-Monitor	Serielle Schnittstelle (Out-of-Band)	Terminalemulations-Software

1.1 Grafische Benutzeroberfläche

Systemanforderungen

Um die grafische Benutzeroberfläche zu öffnen, benötigen Sie die Desktop-Version eines Web-Browsers mit HTML5-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. Um Validierungskonflikte mit Software von Drittanbietern zu beheben, übertragen Sie Ihr eigenes, aktuelles Zertifikat auf das Gerät oder generieren Sie das Zertifikat mit der neuesten Firmware.

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 43.

Führen Sie die folgenden Schritte aus:
- ☐ Starten Sie Ihren Web-Browser.
- ☐ Fügen Sie die IP-Adresse des Geräts in das Adressfeld des Web-Browsers ein.
  Verwenden Sie die folgende Form: `https://xxx.xxx.xxx.xxx`
  Der Web-Browser stellt die Verbindung zum Gerät her und zeigt den Login-Dialog.
- ☐ Wenn Sie die Sprache der grafischen Benutzeroberfläche ändern möchten, klicken Sie im Login-Dialog auf den entsprechenden Link oben rechts.
- ☐ 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 Geräts 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 Interfaces erhalten Sie zum Beispiel mit Hilfe des Freeware-Programms *PuTTY*. Sie können die Software von www.putty.org herunterladen.

- ☐ Installieren Sie auf Ihrem Rechner das Programm *PuTTY*.

1.2.2 Zugriff auf das Command Line Interface mit Telnet

Telnet-Verbindung über Windows

Telnet ist ausschließlich bei Windows-Versionen vor Windows Vista standardmäßig installiert.

Führen Sie die folgenden Schritte aus:

- ☐ Starten Sie auf Ihrem Rechner das Programm *Command Prompt*.
- ☐ Fügen Sie das Kommando `telnet <IP_address>` ein.

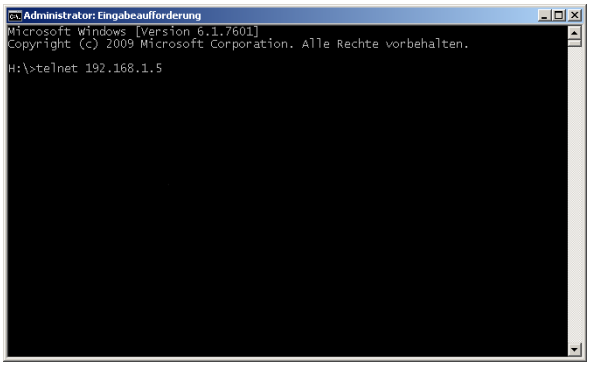


Abb. 1: Command Prompt: Telnet-Verbindung zum Gerät herstellen

Telnet-Verbindung über PuTTY

Führen Sie die folgenden Schritte aus:

- Starten Sie auf Ihrem Rechner das Programm *PuTTY*.

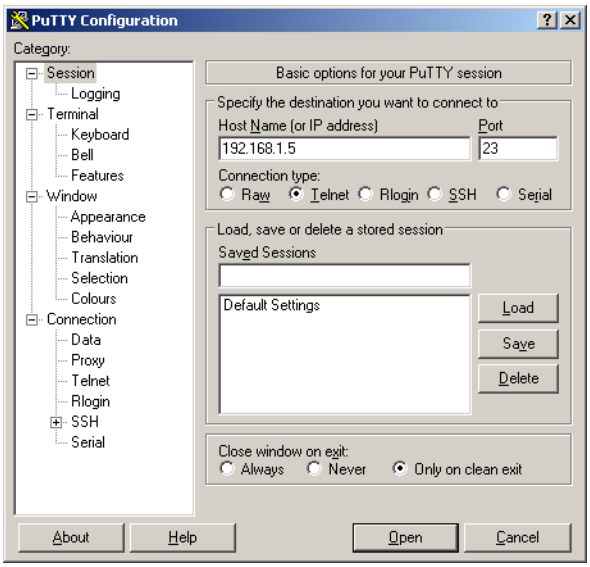


Abb. 2: PuTTY-Eingabemaske

- In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Geräts ein.
  Die IP-Adresse 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 Command Line Interface 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.

Anmerkung: Dieses Gerät ist ein sicherheitsrelevantes Produkt. Ändern Sie das Passwort gleich bei der ersten Inbetriebnahme.

Führen Sie die folgenden Schritte aus:

- 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.

```
                Copyright (c) 2011-2021 Hirschmann Automation and Control GmbH

                                    All rights reserved

                              MSP30 Release HiOS-2A-09.0.00

                              (Build date 2021-12-15 09:30)


                    System Name   :  MSP30-ECE555d5e911
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    System Time   :  2021-12-17 12:42:19


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MSP>
```

Abb. 3: Start-Bildschirm des Command Line Interfaces

1.2.3 Zugriff auf das Command Line Interface mit SSH (Secure Shell)

Im folgenden Beispiel verwenden wir das Programm *PuTTY*. Eine weitere Möglichkeit, über SSH auf Ihr Gerät zuzugreifen, ist die OpenSSH Suite.

Führen Sie die folgenden Schritte aus:

- Starten Sie auf Ihrem Rechner das Programm *PuTTY*.

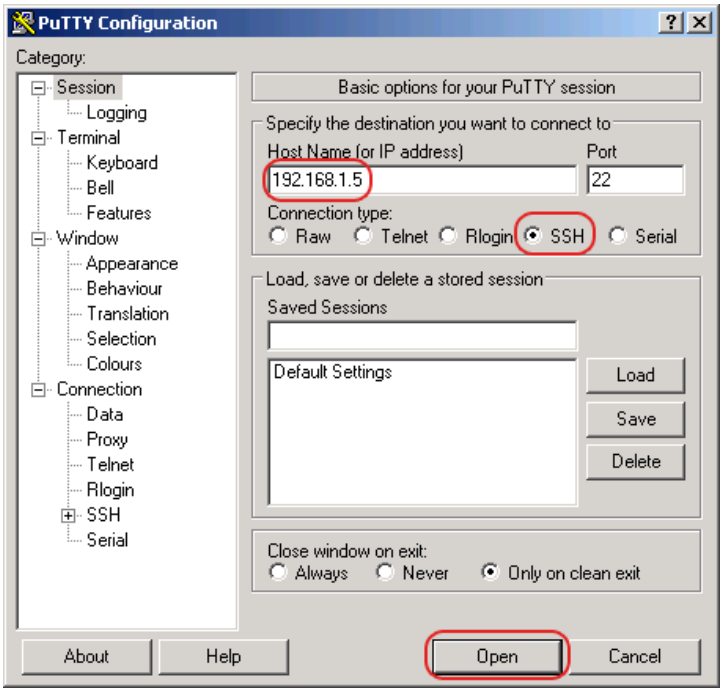


Abb. 4: PuTTY-Eingabemaske

- In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Geräts ein.
  Die IP-Adresse besteht aus 4 Dezimalzahlen im Wert von `0` bis `255`. Die 4 Dezimalzahlen sind durch einen Punkt getrennt.
- Um den Verbindungstyp auszuwählen, wählen Sie in der Optionsliste *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 zeigt das Programm *PuTTY* gegen Ende des Verbindungsaufbaus eine Sicherheitswarnmeldung und ermöglicht Ihnen, den Fingerabdruck des Schlüssels zu prüfen.

Abb. 5: Sicherheitsabfrage für den Fingerabdruck

- Prüfen Sie den Fingerabdruck.
  Das hilft Ihnen dabei, sich vor unliebsamen Gästen zu schützen.
- Stimmt der Fingerabdruck mit dem Fingerabdruck des Geräteschlüssels überein, klicken Sie die Schaltfläche *Yes*.
  Das Gerät ermöglicht Ihnen, die Fingerabdrücke der Geräteschlüssel mit dem Kommando `show ssh` oder in der grafischen Benutzeroberfläche im Dialog *Gerätesicherheit > Management-Zugriff >* Server, Registerkarte *SSH* auszulesen.
  Das Command Line Interface 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.
- 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.

Anmerkung: Dieses Gerät ist ein sicherheitsrelevantes Produkt. Ändern Sie das Passwort gleich bei der ersten Inbetriebnahme.

```
login as: admin
admin@192.168.1.5's password:


                Copyright (c) 2011-2021 Hirschmann Automation and Control GmbH

                                    All rights reserved

                              MSP30 Release HiOS-2A-09.0.00

                              (Build date 2021-12-15 09:30)


                    System Name   :  MSP30-ECE555d5e911
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    System Time   :  2021-12-17 12:42:19


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MSP>
```

Abb. 6: Start-Bildschirm des Command Line Interfaces

1.2.4 Zugriff auf das Command Line Interface über die serielle Schnittstelle

Die serielle Schnittstelle dient zum lokalen Anschließen einer externen Netz-Management-Station (VT100-Terminal oder PC mit Terminal-Emulation). Die Schnittstelle ermöglicht Ihnen, eine Datenverbindung zum Command Line Interface und zum Systemmonitor herzustellen.

Einstellungen VT 100 Terminal	
Speed	9600 bit/s
Data	8 bit
Stopbit	1 bit
Handshake	off
Parity	none

Führen Sie die folgenden Schritte aus:

- ☐ Verbinden Sie das Gerät über die serielle Schnittstelle 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 die serielle Schnittstelle mit dem Programm *PuTTY*. Drücken Sie die <Enter>-Taste.

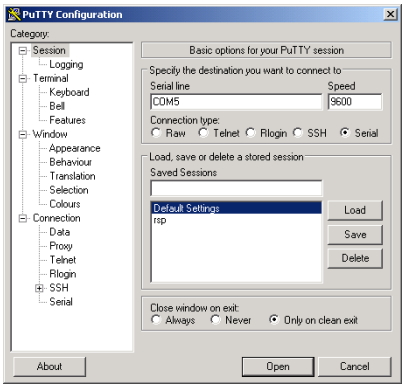


Abb. 7: Serielle Datenverbindung über die serielle Schnittstelle mit dem Programm PuTTY

- ☐ 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.

Anmerkung: Dieses Gerät ist ein sicherheitsrelevantes Produkt. Ändern Sie das Passwort gleich bei der ersten Inbetriebnahme.

```
                Copyright (c) 2011-2021 Hirschmann Automation and Control GmbH

                                    All rights reserved

                                MSP30 Release HiOS-2A-09.0.00

                                (Build date 2021-12-15 09:30)


                    System Name   :  MSP30-ECE555d5e911
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    System Time   :  2021-12-17 12:42:19


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MSP>
```

Abb. 8: Start-Bildschirm des Command Line Interfaces

1.2.5 Modus-basierte Kommando-Hierarchie

Im Command Line Interface sind die Kommandos in zugehörige Modi gruppiert, entsprechend der Art des Kommandos. Jeder Kommando-Modus unterstützt bestimmte Hirschmann Software-Kommandos.

Die Kommandos, die Ihnen als Benutzer zur Verfügung stehen, sind abhängig von Ihrer Berechtigungsstufe (`administrator`, `operator`, `guest`, `auditor`). Sie sind außerdem abhängig vom Modus, in dem Sie gerade arbeiten. Die Kommandos in einem bestimmten Modus sind für Sie verfügbar, wenn Sie zu diesem Modus umschalten.

Eine Ausnahme bilden die User Exec-Modus Kommandos. Das Command Line Interface bietet Ihnen die Möglichkeit, diese Kommandos auch im Privileged Exec Modus auszuführen.

Die folgende Abbildung zeigt die Modi des Command Line Interfaces.

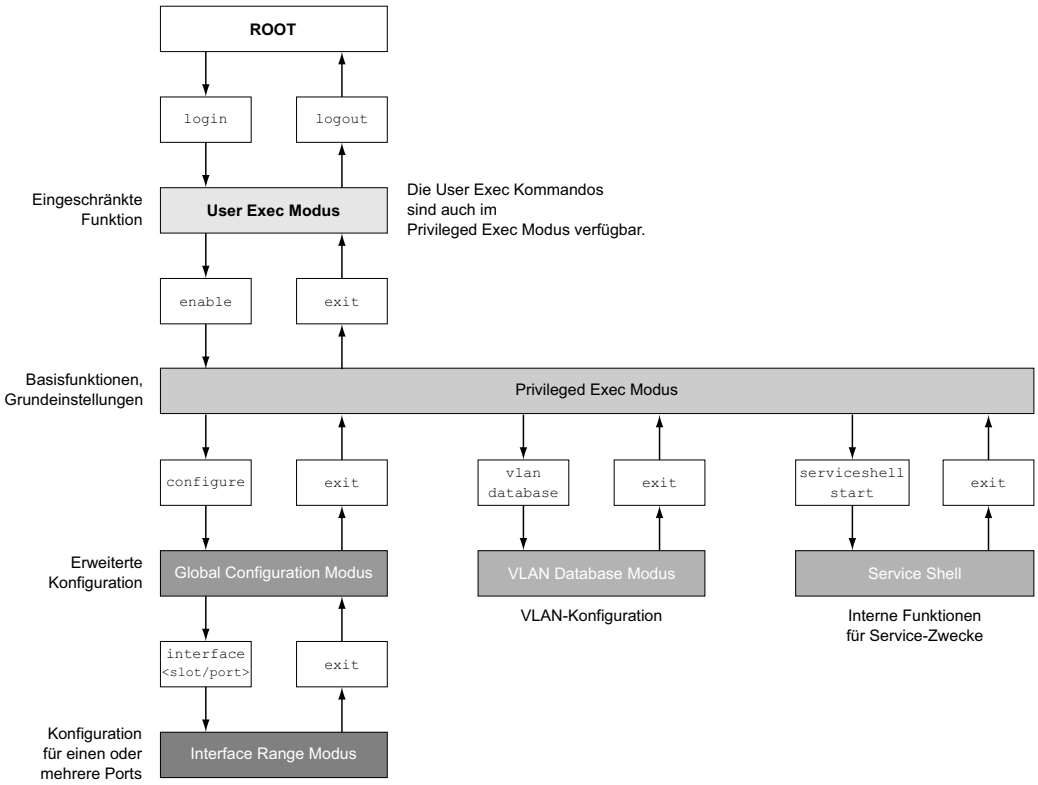


Abb. 9: Aufbau des Command Line Interfaces

Das Command Line Interface unterstützt, abhängig von der Berechtigungsstufe (User Level), die folgenden Modi:

- User Exec Modus
  Nach Anmelden mit dem Command Line Interface befinden Sie sich im User Exec Modus. Der User Exec Modus enthält einen begrenzten Umfang an Kommandos.
  Kommando-Prompt: `(MSP) >`
- Privileged Exec Modus
  Um Zugriff auf den gesamten Befehlsumfang zu haben, wechseln Sie in den Privileged Exec Modus. Voraussetzung für den Wechsel in den Privileged Exec Modus ist, dass Sie sich als privilegierter Benutzer anmelden. Vom Privileged Exec Modus aus sind auch die Kommandos des User Exec Modus ausführbar.
  Kommando-Prompt: `(MSP) #`
- VLAN-Modus
  Der VLAN-Modus enthält VLAN-bezogene Kommandos.
  Kommando-Prompt: `(MSP) (VLAN)#`
- Service Shell
  Die Service Shell dient ausschließlich zu Service-Zwecken.
  Kommando-Prompt: `/mnt/fastpath #`

- Global Config Modus
  Der Global Config Modus ermöglicht Ihnen, Modifikationen an der laufenden Konfiguration durchzuführen. In diesem Modus sind allgemeine Setup-Kommandos zusammengefasst.
  Kommando-Prompt: `(MSP) (config)#`
- Interface Range Modus
  Die Befehle Interface Range Modus wirken sich auf einen bestimmten Port, auf eine ausgewählte Gruppe von mehreren Ports oder auf alle Ports aus. Die Befehle modifizieren einen Wert oder schalten eine Funktion an einem oder an mehreren bestimmten Ports an/aus.
  - Alle physikalischen Ports des Gerätes
    Kommando-Prompt: `(MSP) ((interface) all)#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MSP) (config)#interface all
    (MSP) ((Interface)all)#
    ```
  - Einzelner Port an einem Interface
    Kommando-Prompt: `(MSP) (interface <slot/port>)#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MSP) (config)#interface 2/1
    (MSP) (interface 2/1)#
    ```
  - Eine Portreihe an einem Interface
    Kommando-Prompt: `(MSP) (interface <interface range> )#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MSP) (config)#interface 1/2-1/4
    (MSP) ((Interface)1/2-1/4)#
    ```
  - Eine Auflistung von einzelnen Ports
    Kommando-Prompt: `(MSP) (interface <interface list>)#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MSP) (config)#interface 1/2,1/4,1/5
    (MSP) ((Interface)1/2,1/4,1/5)#
    ```
  - Eine Auflistung von Portreihen und einzelnen Ports
    Kommando-Prompt: `(MSP) (interface <complex range>)#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MSP) (config)#interface 1/2-1/4,1/6-1/9
    (MSP) ((Interface)1/2-1/4,1/6-1/9)
    ```

Die folgende Tabelle zeigt die Kommando Modi, die im jeweiligen Modus sichtbaren Kommando-Prompts (Eingabeaufforderungszeichen) und die Möglichkeit, mit der Sie den Modus beenden.

Tab. 2: Kommando-Modi

Kommando-modus	Zugriffsmethode	Beenden oder nächsten Modus starten

User Exec Modus	Erste Zugriffsebene. Basisaufgaben ausführen und Systeminformationen auflisten.	Zum Beenden geben Sie `logout` ein:
		`(MSP) >logout`
		`Are you sure (Y/N) ?y`

Privileged Exec Modus	Aus dem User Exec Modus geben Sie den Befehl `enable` ein.
	`(MSP) >enable`
	`(MSP) #`
		Um den Privileged Exec Modus zu beenden und in den User Exec Modus zurückzukehren, geben Sie `exit` ein:
		`(MSP) #exit`
		`(MSP) >`

VLAN-Modus	Aus dem Privileged Exec Modus geben Sie den Befehl `vlan database` ein.
	`(MSP) #vlan database`
	`(MSP) (Vlan)#`
		Um den VLAN-Modus zu beenden und in den Privileged Exec Modus zurückzukehren, geben Sie `exit` ein oder drücken Sie Ctrl-Z.
		`(MSP) (Vlan)#exit`
		`(MSP) #`

Global Config Modus	Aus dem Privileged Exec Modus geben Sie den Befehl `configure` ein.
	`(MSP) #configure`
	`(MSP) (config)#`
	Aus dem User Exec Modus geben Sie Befehl `enable` und dann im Privileged Exec Modus den Befehl `Configure` ein.
	`(MSP) >enable`
	`(MSP) #configure`
	`(MSP) (config)#`
		Um den Global Config Modus zu beenden und in den Privileged Exec Modus zurückzukehren, geben Sie `exit` ein:
		`(MSP) (config)#exit`
		`(MSP) #`
		Um anschließend den Privileged Exec Modus zu beenden und in den User Exec Modus zurückzukehren, geben Sie erneut `exit` ein:
		`(MSP) #exit`
		`(MSP) >`

Interface Range Modus	Aus dem Global Config Modus geben Sie den Befehl `interface {all|<slot/port>|<interface range> |<interface list>|<complex range>}` ein.
	`(MSP) (config)#interface <slot/port>`
	`(MSP) (interface slot/port)#`
		Um den Interface Range Modus zu beenden und in den Global Config Modus zurückzukehren, geben Sie `exit` ein. Um zum Privileged Exec Modus zurückzukehren, drücken Sie Ctrl-Z.
		`(MSP) (interface slot/port)#exit`
		`(MSP) #`

Wenn Sie ein Fragezeichen (?) nach dem Prompt eingeben, gibt das Command Line Interface Ihnen die Liste der verfügbaren Kommandos und eine Kurzbeschreibung zu den Kommandos aus.

```
(MSP)>
  cli              Set the CLI preferences.
  enable           Turn on privileged commands.
  help             Display help for various special keys.
  history          Show a list of previously run commands.
  logout           Exit this session.
  ping             Send ICMP echo packets to a specified IP address.
  show             Display device options and settings.
  telnet           Establish a telnet connection to a remote host.

(MSP)>
```

Abb. 10: Kommandos im User Exec Modus

1.2.6 Ausführen von Kommandos

Syntaxanalyse

Nach Anmelden mit dem Command Line Interface befinden Sie sich im User Exec Modus. Das Command Line Interface gibt das `(MSP)>` Prompt auf dem Bildschirm aus.

Wenn Sie ein Kommando eingeben und die <Eingabetaste> drücken, startet das Command Line Interface die Syntax-Analyse. Das Command Line Interface durchsucht den Kommandobaum nach dem gewünschten Kommando.

Falls das Kommando außerhalb des Command Line Interface Kommandoumfangs liegt, zeigt Ihnen eine Meldung den erkannten Fehler.

Beispiel:

Sie beabsichtigen, den Befehl `show system info` auszuführen, geben jedoch `info` ohne `f` ein und drücken die <Enter>-Taste.

Das Command Line Interface gibt daraufhin eine Meldung aus:

```
(MSP)>show system ino

Error: Invalid command 'ino'
```

Kommandobaum

Die Kommandos im Command Line Interface sind in einer Baumstruktur organisiert. Die Kommandos und ggf. die zugehörigen Parameter verzweigen sich so lange weiter, bis das Kommando komplett definiert und damit ausführbar ist. Das Command Line Interface prüft die Eingaben. Wenn Sie den Befehl und die Parameter korrekt und vollständig eingegeben haben, führen Sie den Befehl durch Dücken der <Enter>-Taste aus.

Nachdem Sie den Befehl und die erforderlichen Parameter eingegeben haben, behandelt das CLI die weiteren eingegebenen Parameter wie optionale Parameter. Wenn einer der Parameter unbekannt ist, gibt das Command Line Interface eine Syntax-Meldung aus.

Der Kommandobaum verzweigt sich bei erforderlichen Parametern weiter, bis die erforderlichen Parameter die letzte Abzweigung der Struktur erreicht haben.

Bei optionalen Parametern verzweigt sich der Kommandobaum weiter, bis die erforderlichen und die optionalen Parameter die letzte Abzweigung der Struktur erreicht haben.

1.2.7 Aufbau eines Kommandos

Dieser Abschnitt beschreibt Syntax, Konventionen und Terminologie und stellt diese anhand von Beispielen dar.

Format der Kommandos

Ein Großteil der Kommandos enthält Parameter.

Fehlt der Kommando-Parameter, zeigt das Command Line Interface einen Hinweis auf eine erkannte fehlerhafte Syntax des Befehls.

Dieses Handbuch stellt die Befehle und Parameter in der Schriftart `Courier` dar.

Parameter

Die Reihenfolge der Parameter ist für die korrekte Syntax eines Kommandos relevant.

Parameter sind notwendige Werte, optionale Werte, Auswahlen oder eine Kombination davon. Die Darstellung zeigt die Art des Parameters.

Tab. 3: Parameter- und Kommando-Syntax

`<command>`	Kommandos in spitzen Klammern (`<>`) sind obligatorisch.
`[command]`	Kommandos in eckigen Klammern (`[]`) sind optional.
`<parameter>`	Parameter in spitzen Klammern (`<>`) sind obligatorisch.
`[parameter]`	Parameter in eckigen Klammern (`[]`) sind optional.
`...`	Auslassungspunkte (3 aufeinander folgende Punkte ohne Leerzeichen) nach einem Element zeigen an, dass Sie das Element wiederholen können.

Tab. 3: Parameter- und Kommando-Syntax

`[Choice1 | Choice2]`	Eine senkrechte Linie, eingeschlossen in Klammern, zeigt eine Auswahlmöglichkeit. Wählen Sie einen Wert. Durch eine senkrechte Linie getrennte Elemente, eingeschlossen in eckigen Klammern, zeigen eine optionale Auswahlmöglichkeit an (Auswahl1 oder Auswahl2 oder keine Auswahl).
`{list}`	Die geschweiften Klammern (`{}`) zeigen eine Auswahlmöglichkeit von Parametern aus einer Liste.
`{Choice1 | Choice2}`	Durch eine senkrechte Linie getrennte Elemente, eingeschlossen in geschweiften Klammern (`{}`), zeigen eine obligatorische Auswahlmöglichkeit an (Auswahl1 oder Auswahl2).
`[param1 {Choice1 | Choice2}]`	Zeigt einen optionalen Parameter, der eine obligatorische Auswahl beinhaltet.
`<a.b.c.d>`	Kleinbuchstaben sind Wildcards (Jokerzeichen). Parameter der Notation a.b.c.d geben Sie mit Punkten ein (zum Beispiel IP-Adressen).
`<cr>`	Erzeugen Sie durch Drücken der <Enter>-Taste einen Zeilenumbruch.

Die folgende Liste zeigt mögliche Parameterwerte innerhalb des Command Line Interface:

Tab. 4: Parameterwerte im Command Line Interface

Wert	Beschreibung
IP-Adresse	Dieser Parameter stellt eine gültige IPv4-Adresse dar. Die Adresse besteht aus 4 Hexadezimalzahlen vom Wert 0 bis 255. Die 4 Dezimalzahlen sind durch einen Dezimalpunkt getrennt. Die Eingabe der IP-Adresse `0.0.0.0` ist gültig.
MAC-Adresse	Dieser Parameter stellt eine gültige MAC-Adresse dar. Die Adresse besteht aus 6 Hexadezimalzahlen vom Wert 00 bis FF. Die Zahlen werden durch Doppelpunkte getrennt, zum Beispiel `00:F6:29:B2:81:40`.
string	Benutzerdefinierter Text mit einer Länge im festgelegten Bereich, zum Beispiel maximal 32 Zeichen.
character string	Verwenden Sie zwei Anführungszeichen, um eine Zeichenkette zu kennzeichnen, zum Beispiel `"System name with space character"`.
number	Ganze Zahl im festgelegten Bereich, zum Beispiel `0..999999`.
date	Datum im Format `YYYY-MM-DD`.
time	Zeit im Format `HH:MM:SS`.

Netzadressen

Netzadressen sind Voraussetzung beim Aufbau einer Datenverbindung zu einer entfernten Arbeitsstation, einem Server oder einem anderen Netz. Man unterscheidet zwischen IP-Adressen und MAC-Adressen.

Die IP-Adresse ist eine Adresse, die der Netzadministrator vergibt. Die IP-Adresse ist in einem Netz eindeutig.

Die MAC-Adressen vergibt der Hardware-Hersteller. MAC-Adressen sind weltweit eindeutig.

Die folgende Tabelle zeigt die Darstellung und den Bereich der Adresstypen:

Tab. 5: Format und Bereich von Netzadressen

Adresstyp	Format	Bereich	Beispiel
IP-Adresse	nnn.nnn.nnn.nnn	nnn: 0 bis 255 (dezimal)	192.168.11.110
MAC-Adresse	mm:mm:mm:mm:mm:mm	mm: 00 bis ff (hexadezimale Zahlenpaare)	A7:C9:89:DD:A9:B3

Zeichenfolgen (Strings)

Anführungszeichen markieren eine Zeichenfolge (String). Zum Beispiel: `"System name with space character"`. Leerzeichen sind keine gültigen benutzerdefinierten Strings. Ein Leerzeichen in einem Parameter geben Sie innerhalb von Anführungszeichen ein.

Beispiel:

```
*(MSP)#cli prompt Device name
Error: Invalid command 'name'

*(MSP)#cli prompt 'Device name'

*(Device name)#
```

1.2.8 Beispiele für Kommandos

Beispiel 1: clear arp-table-switch

Kommando zum Löschen der ARP-Tabelle des Management-Agenten (Cache).

`clear arp-table-switch` ist die Befehlsbezeichnung. Das Kommando ist ohne weitere Parameter durch Drücken der <Enter>-Taste ausführbar.

Beispiel 2: radius server timeout

Kommando, um die Zeitüberschreitung des RADIUS Servers zu konfigurieren.

```
(MSP) (config)#radius server timeout
 <1..30>              Timeout in seconds (default: 5).
```

`radius server timeout` ist die Befehlsbezeichnung.

Der Parameter ist notwendig. Der Wertebereich ist `1..30`.

Beispiel 3: radius server auth modify <1..8>

Kommando, um die Parameter für den RADIUS Authentication Server 1 einzustellen.

```
(MSP) (config)#radius server auth modify 1
 [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.
  <cr>                  Press Enter to execute the command.
```

`radius server auth modify` ist die Befehlsbezeichnung.

Der Parameter `<1..8>` (RADIUS server index) ist notwendig. Der Wertebereich ist `1..8` (Integer).

Die Parameter `[name]`, `[port]`, `[msgauth]`, `[primary]`, `[status]`, `[secret]` und `[encrypted]` sind optional.

1.2.9 Eingabeprompt

Kommandomodus

Das Command Line Interface zeigt durch das Eingabeprompt, in welchem der Modi Sie sich befinden:

- `(MSP) >`
  User Exec Modus
- `(MSP) #`
  Privileged Exec Modus
- `(MSP) (config)#`
  Global Config Modus
- `(MSP) (Vlan)#`
  VLAN Database mode
- `(MSP) ((Interface)all)#`
  Interface Range Modus / Alle Ports des Geräts
- `(MSP) ((Interface)2/1)#`
  Interface Range Modus / Einzelner Port auf einem Interface
- `(MSP) ((Interface)1/2-1/4)#`
  Interface Range Modus / Eine Reihe von Ports auf einem Interface
- `(MSP) ((Interface)1/2,1/4,1/5)#`
  Interface Range Modus / Eine Auflistung von einzelnen Ports
- `(MSP) ((Interface)1/1-1/2,1/4-1/6)#`
  Interface Range Modus / Eine Auflistung von Reihen von Ports und einzelnen Ports

Stern, Rautezeichen und Ausrufezeichen

- Stern `*`
  Ein Stern `*` an erster oder zweiter Stelle des Eingabeprompts zeigt, dass sich die Einstellungen im flüchtigen Speicher von den Einstellungen im nicht-flüchtigen Speicher unterscheiden. Das Gerät hat ungespeicherte Änderungen in Ihrer Konfiguration erkannt.
  `*(MSP)>`

- Rautezeichen `#`
  Ein Rautezeichen `#` zu Beginn des Eingabeprompts zeigt, dass sich die Boot-Parameter von den Parametern während der Bootphase unterscheiden.
  *`#(MSP)>`
- Ausrufezeichen `!`
  Ein Ausrufezeichen `!` zu Beginn des Eingabeprompts zeigt: das Passwort für die Benutzerkonten `user` oder `admin` stimmt mit dem Lieferzustand überein.
  `!(MSP)>`

Wildcards

Das Gerät ermöglicht Ihnen, den Prompt der Befehlszeile zu ändern.

Das Command Line Interface unterstützt die folgenden Platzhalter:

Tab. 6: Verwendung von Wildcards am Eingabeprompt des Command Line Interfaces

Wildcard	Beschreibung
`%d`	Systemdatum
`%t`	Systemzeit
`%i`	IP-Adresse des Geräts
`%m`	MAC-Adresse des Gerätes
`%p`	Produktbezeichnung des Geräts

```
!(MSP)>enable

!(MSP)#cli prompt %i

!192.168.1.5#cli prompt (MSP)%d

!*(MSP)2021-12-17#cli prompt (MSP)%d%t

!*(MSP)2021-12-17 12:42:19#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.10 Tastaturkombinationen

Die folgenden Tastaturkombinationen erleichtern Ihnen die Arbeit mit dem Command Line Interface:

Tab. 7: Tastenkombinationen im Command Line Interface

Tastaturkombination	Beschreibung
<STRG> + <H>, <Zurück (Backspace)>	Letztes Zeichen löschen
<STRG> + <A>	Zum Zeilenanfang gehen
<STRG> + <E>	Zum Zeilenende gehen

Tab. 7: Tastenkombinationen im Command Line Interface

Tastaturkombination	Beschreibung
<STRG> + <F>	Ein Zeichen nach vorn gehen
<STRG> + <B>	Ein Zeichen zurück gehen
<STRG> + <D>	Nächstes Zeichen löschen
<STRG> + <U>, <X>	Zeichen bis zum Anfang der Zeile löschen
<STRG> + <K>	Zeichen bis zum Ende der Zeile löschen
<STRG> + <W>	Vorheriges Wort löschen
<STRG> + <P>	Zur vorherigen Zeile im Speicher wechseln
<STRG> + <R>	Zeile erneut schreiben oder Inhalte einfügen
<STRG> + <N>	Zur nächsten Zeile im Speicher wechseln
<STRG> + <Z>	Zum Ursprung wechseln
<STRG> + <G>	Laufende tcpdump-Ausgabe abbrechen
<Tabulator>, <LEER-TASTE>	Kommandozeilen Vervollständigung
`Exit`	Exit zur nächsten, niedrigen Kommandozeile wechseln
<?>	Auswahl anzeigen / Hilfe darstellen

Das Help-Kommando listet die möglichen Tastenkombinationen des Command Line Interface auf dem Bildschirm auf:

```
(MSP) #help

HELP:
Special keys:

  Ctrl-H, BkSp delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Z  .... return to root command prompt
  Ctrl-G  .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices

(MSP) #
```

Abb. 11: Auflisten der Tastenkombinationen mit dem Help-Kommando

1.2.11 Eingabehilfen

Befehlsergänzung

Das Command Line Interface ermöglicht Ihnen, die Befehlsvervollständigung (Tab-Completion) zu verwenden, um die Eingabe von Befehlen zu vereinfachen. Damit haben Sie die Möglichkeit, Schlüsselwörter abzukürzen.

- Tippen Sie den Beginn eines Schlüsselwortes ein. Wenn die eingegebenen Buchstaben ein Schlüsselwort (keyword) kennzeichnen und Sie die Tabulator- oder Leertaste betätigen, ergänzt das Command Line Interface das Schlüsselwort. Falls mehr als eine Schlüsselwort-Ergänzung möglich ist, geben Sie den oder die zur eindeutigen Identifizierung notwendigen Buchstaben ein. Betätigen Sie erneut die Tabulator- oder Leertaste. Das System ergänzt daraufhin den Befehl oder Parameter.
- Wenn Sie bei einer mehrdeutigen Eingabe 2 Mal die Taste <Tab>oder <Leerzeichen> drücken, gibt das Command Line Interface eine Auswahlliste aus.
- Bei einer mehrdeutigen Eingabe und Drücken der Taste <Tab> oder <Leerzeichen> ergänzt das Command Line Interface den Befehl bis zum Beginn der Mehrdeutigkeit. Wenn Sie anschließend erneut die Taste <Tab> oder <Leerzeichen> drücken, zeigt das Command Line Interface eine Auswahlliste.
  Beispiel:
  ```
  (MSP) (Config)#lo
  (MSP) (Config)#log
  logging logout
  ```
  Bei der Eingabe von `lo` und <Tab> oder <Leerzeichen> ergänzt das Command Line Interface den Befehl bis zum Beginn der Mehrdeutigkeit zu `log`.
  Wenn Sie anschließend erneut die Taste <Tab> oder <Leerzeichen> drücken, zeigt das Command Line Interface eine Auswahlliste (`logging logout`).

Mögliche Befehle/Parameter

Eine Darstellung der Befehle oder der möglichen Parameter erhalten Sie durch die Eingabe von `help` oder `?`, zum Beispiel durch Eingabe von `(MSP) >show ?`

Durch Eingabe des dargestellten Befehls erhalten Sie eine Liste der verfügbaren Parameter zum Befehl `show`.

Durch die Eingabe des Befehls ohne Leerzeichen vor dem Fragezeichen zeigt das Gerät den Hilfetext zum Befehl selbst:

```
!*#(MSP)(Config)#show?

   show          Display device options and settings.
```

1.2.12 Anwendungsfälle

Konfiguration speichern

Damit Ihre Password-Einstellungen und Ihre sonstigen Konfigurationsänderungen nach einem Reset des Gerätes oder nach einer Unterbrechung der Spannungsversorgung erhalten bleiben, speichern Sie die Konfiguration. Führen Sie dazu die folgenden Schritte aus:

- ☐ Wechseln Sie mit `enable` in den Privileged Exec Modus.
- ☐ Geben Sie das folgende Kommando ein:
  `save [profile]`
- ☐ Führen Sie den Befehl aus durch Betätigen der <Enter>-Taste.

Syntax des Kommandos „radius server auth add“

Verwenden Sie dieses Kommando, um einen RADIUS-Authentication-Server hinzuzufügen.

- Kommandomodus: `Global Config` Modus
- Berechtigungsstufe: Administrator
- Format: `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `[name]`: Name des RADIUS Authentication Servers.
  - `[port]`: Port des RADIUS Authentication Servers (Voreinstellung: `1813`).

Parameter	Bedeutung	Wertebereich
`<1..8>`	Index des RADIUS Servers.	`1..8`
`<a.b.c.d>`	IP-Adresse des RADIUS Accounting Servers.	IP-Adresse
`<string>`	Geben Sie einen benutzerdefinierten Text ein, maximal 32 Zeichen lang.	
`<1..65535>`	Geben Sie eine Portnummer zwischen 1 und 65535 ein.	`1..65535`

Modus und Berechtigungsstufe:

- Voraussetzung für das Ausführen des Kommandos: Sie befinden sich im Global Config Modus. Siehe „Modus-basierte Kommando-Hierarchie” auf Seite 25.
- Voraussetzung für das Ausführen des Kommandos: Sie haben die Berechtigungsstufe Administrator.

Syntax der Kommandos und Parameter: Siehe „Aufbau eines Kommandos” auf Seite 30.

Beispiele für ausführbare Kommandos:

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

1.2.13 Service Shell

Die Service Shell dient ausschließlich zu Service-Zwecken.

Die Service Shell ermöglicht Benutzern den Zugriff auf interne Funktionen des Geräts. Wenn Sie beim Zugriff auf Ihr Gerät Unterstützung benötigen, verwendet das Service-Personal die Service Shell, um interne Zustände wie Switch-Register und CPU-Register zu überwachen.

Führen Sie keine interne Funktionen ohne die Anweisung eines Servicetechnikers aus. Das Ausführen interner Funktionen, zum Beispiel das Löschen des Inhalts des permanenten Speichers *NVM*, **kann dazu führen, dass Ihr Gerät funktionsunfähig wird**.

Service Shell starten

Voraussetzung ist, dass Sie sich im User Exec-Modus befinden: `(MSP) >`

Führen Sie die folgenden Schritte aus:

- ☐ Fügen Sie `enable` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - Fügen Sie `e` ein und drücken die <Enter>-Taste.
- ☐ Fügen Sie `serviceshell start` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - Fügen Sie `ser` ein und drücken die <Enter>-Taste.
  - Fügen Sie `s` ein und drücken die <Enter>-Taste.

```
!MSP >enable

!*MSP #serviceshell start
 WARNING! The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.

 You can return to the previous mode using the 'exit' command.

 BusyBox v1.31.0 (2021-12-17 12:42:19 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

Arbeiten mit der Service Shell

Wenn die Service Shell aktiv ist, ist das Timeout des Command Line Interfaces inaktiv. Um Inkonsistenzen in der Gerätekonfiguration zu vermeiden, beenden Sie die Service Shell, bevor ein anderer Benutzer die Übertragung einer neuen Konfiguration auf das Gerät startet.

Service Shell-Kommandos anzeigen

Voraussetzung ist, dass Sie die Service Shell bereits gestartet haben.

Führen Sie die folgenden Schritte aus:
☐ Fügen Sie `help` ein und drücken die <Enter>-Taste.

```
/mnt/fastpath # help
Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let
        local pwd read readonly return set shift source test times trap
        true type ulimit umask unalias unset wait
/mnt/fastpath #
```

Service Shell beenden

Führen Sie die folgenden Schritte aus:
☐ Fügen Sie `exit` ein und drücken die <Enter>-Taste.

Service Shell permanent im Gerät deaktivieren

Wenn Sie die Service Shell deaktivieren, haben Sie weiterhin die Möglichkeit, das Gerät zu konfigurieren Sie schränken jedoch die Möglichkeiten des Service-Personals zur Durchführung von System-Diagnosen ein. Der Service-Techniker hat dann keine Möglichkeit mehr, auf interne Funktionen Ihres Geräts zuzugreifen.

Die Deaktivierung ist unumkehrbar. Die Service Shell bleibt dauerhaft deaktiviert. **Um die Service Shell zu reaktivieren ist das Öffnen des Geräts seitens des Herstellers erforderlich.**

Die Voraussetzungen sind:
- Die Service Shell ist nicht gestartet.
- Sie befinden sich im User Exec-Modus: `(MSP) >`

Führen Sie die folgenden Schritte aus:
☐ Fügen Sie `enable` ein und drücken die <Enter>-Taste.
Um den Aufwand beim Tippen zu reduzieren:
– Fügen Sie `e` ein und drücken die <Enter>-Taste.

- Fügen Sie `serviceshell deactivate` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - Fügen Sie `ser` ein und drücken die <Enter>-Taste.
  - Fügen Sie `dea` ein und drücken die <Enter>-Taste.
- **Dieser Schritt ist unumkehrbar!**
  Drücken Sie die <Y>-Taste.

```
!MSP >enable

!*MSP #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

1.3 System-Monitor

Der System-Monitor ermöglicht Ihnen, 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

Voraussetzungen:

- 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 die serielle Schnittstelle des Geräts 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: ...-9.0 (2021-12-15 09:30))

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. 12: 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 Geräts 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 „In-Band“-Methode, wenn Sie Ihr Gerät außerhalb seiner Betriebsumgebung vorkonfigurieren oder Sie den Netzzugang („Out-of-Band“) zu dem Gerät wiederherstellen.
- Eingabe über das Protokoll HiDiscovery.
  Wählen Sie diese „In-Band“-Methode für ein bereits installiertes Gerät im Netz, 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 im externen Speicher gespeichert haben.
- Verwendung von BOOTP.
  Wählen Sie diese „In-Band“-Methode, um die Konfiguration des installierten Geräts 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 Geräts 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 IPv4

IP-Adresse

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.

Tab. 8: IP-Adressklassen

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

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

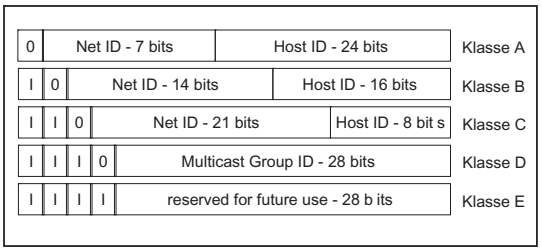


Abb. 13: Bitdarstellung der IP-Adresse

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.

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:

Dezimale Darstellung
255.255.192.0

Binäre Darstellung
11111111.11111111.11000000.00000000

Subnetzmaskenbits
Klasse B

Beispiel für IP-Adressen mit Subnetzzuordnung gemäß der Netzmaske:

Dezimale Darstellung
129.218.65.17
└──── 128 < 129 191 › Klasse B

Binäre Darstellung
10000001.11011010.01000001.00010001
└──── Subnetz 1
└──── Netzadresse

Dezimale Darstellung
129.218.129.17
└──── 128 < 129 191 › Klasse B

Binäre Darstellung
10000001.11011010.10000001.00010001
└──── Subnetz 2

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?

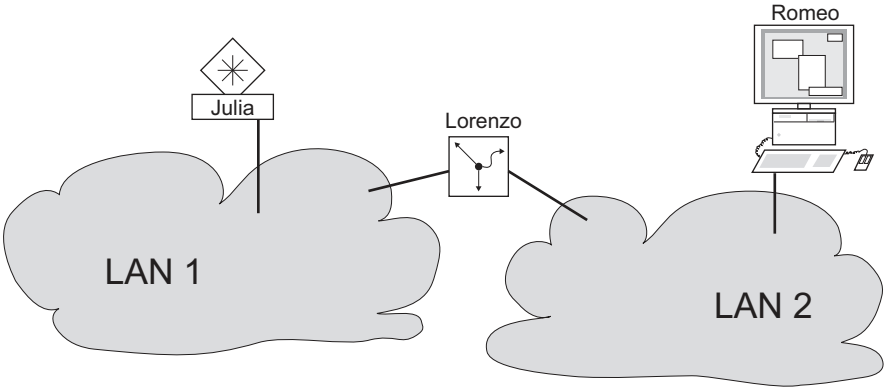


Abb. 14: Management-Agent durch Router von der Netz-Management-Station getrennt

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.

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-Adresse, dezimal	Netzmaske, dezimal	IP-Adresse, binär
192.168.112.1	255.255.255.128	11000000 10101000 01110000 00000001
192.168.112.127		11000000 10101000 01110000 01111111
		25 Maskenbits

CIDR-Schreibweise: 192.168.112.0/25

Maskenbits

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 Command Line Interface festlegen

2.2.1 IPv4

Es gibt folgende Möglichkeiten, die IP-Parameter einzugeben:
- BOOTP/DHCP
- HiDiscovery-Protokoll
- Externer Speicher
- Command Line Interface über eine serielle Verbindung

Das Gerät ermöglicht Ihnen, die IP-Parameter über das HiDiscovery-Protokoll oder über die serielle Schnittstelle mit Hilfe des Command Line Interfaces festzulegen.

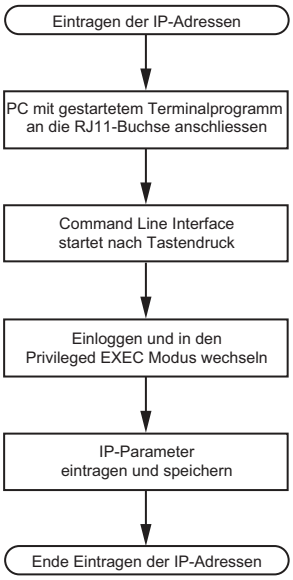


Abb. 15: Ablaufdiagramm Eintragen der IP-Adressen

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.

Führen Sie die folgenden Schritte aus:

- 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 45 „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`	In den Privileged-EXEC-Modus wechseln.
`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`	Aktuelle Einstellungen im „ausgewählten” Konfigurationsprofil im permanenten Speicher (`nvm`) speichern.

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.

Führen Sie die folgenden Schritte aus:

- Installieren Sie auf Ihrem Rechner das Programm HiDiscovery.
  Sie können die Software von https://catalog.belden.com/index.cfm?event=pd&p=PF_HiDiscovery herunterladen.
- Starten Sie das Programm HiDiscovery.

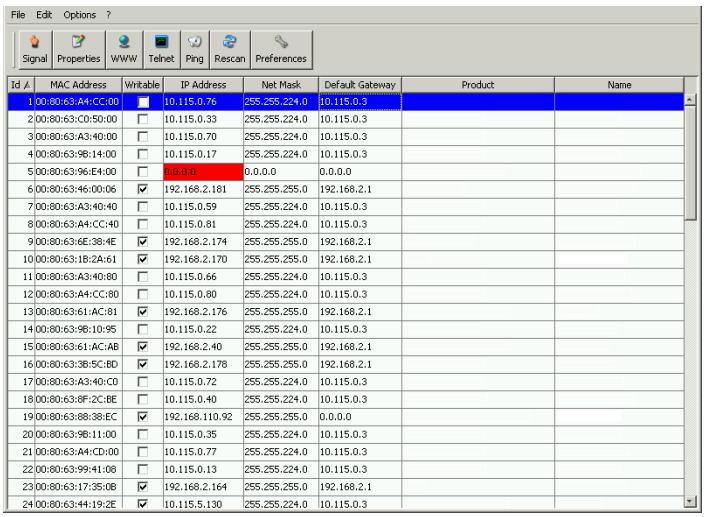


Abb. 16: HiDiscovery

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 die 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.

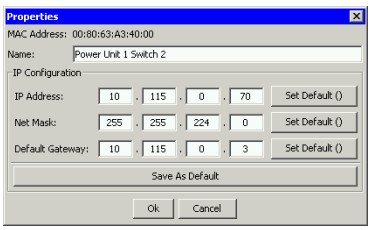


Abb. 17: HiDiscovery – IP-Parameter-Zuweisung

Anmerkung: Schalten Sie die Funktion HiDiscovery im Geräts 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

2.4.1 IPv4

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Netz > Global*.

In diesem Dialog legen Sie das VLAN fest, in dem das Management des Geräts erreichbar ist, und konfigurieren den HiDiscovery-Zugang.

- Legen Sie in Spalte *VLAN-ID* das VLAN fest, in welchem das Management des Geräts über das Netz erreichbar ist.

Beachten Sie hierbei, dass das Management des Geräts ausschließlich über Ports erreichbar ist, die Mitglied des betreffenden VLANS sind.

Das Feld *MAC-Adresse* zeigt die MAC-Adresse des Geräts, 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.
- Öffnen Sie den Dialog *Grundeinstellungen > Netz > IPv4*.

In diesem Dialog legen Sie fest, aus welcher Quelle das Gerät seine IP-Parameter nach dem Start erhält.

- Legen Sie im Rahmen *Management-Schnittstelle* zunächst fest, woher das Gerät seine IP-Parameter bezieht:

▶ Im Modus `BOOTP` erfolgt die Konfiguration durch einen BOOTP- oder DHCP-Server auf Basis der MAC-Adresse des Geräts.
▶ Im Modus `DHCP` erfolgt die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Geräts.
▶ Im Modus `Lokal` 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.

- Fügen Sie im Rahmen *IP-Parameter* die IP-Adresse, die Netzmaske und das Gateway bei Bedarf ein.

- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

2.5 IP-Parameter mit BOOTP festlegen

Bei aktivierter Funktion *BOOTP* sendet das Gerät eine Boot-Anforderungsnachricht an den BOOTP-Server. Die Boot-Anforderungsnachricht enthält die in dem Dialog *Grundeinstellungen > Netz > IPv4* 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

2.6.1 IPv4

Das DHCP (Dynamic Host Configuration Protocol) ist eine Weiterentwicklung von BOOTP und hat dieses abgelöst. DHCP ermöglicht zusätzlich die Konfiguration eines DHCP-Clients über einen Namen anstatt über die MAC-Adresse.

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.

Tab. 9: DHCP-Optionen, die das Gerät anfordert

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

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. Im Dialog *Grundeinstellungen > Netz > IPv4* können Sie DHCP aktivieren oder deaktivieren.

Anmerkung: Vergewissern Sie sich bei Anwendung des Netzmanagements Industrial HiVision, dass DHCP jedem Gerät die originale 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 finden Sie im 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*: `An`
- *Erkennungs-Modus*: `aktiv und passiv`
- *Periodische ARP-Überprüfung senden*: `markiert`
- *Erkennungs-Verzögerung [ms]*: `200`
- *Rückfallverzögerung [s]*: `15`
- *Address-Protections*: `3`
- *Protektions-Intervall [ms]*: `200`
- *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. Wenn die IP-Adresse vorhanden ist, versucht das Gerät, die vorherige Konfiguration wiederherzustellen und nach Ablauf der konfigurierten Verzögerungszeit für die Freigabe eine weitere Prüfung durchzuführen.

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 Geräts die Verbindung mit dem Netz, sofern weiterhin eine Verbindung des entfernten Geräts mit dem Netz besteht.

Wenn der DHCP-Server dem Gerät eine IP-Adresse zuweist und dabei ein Adressenkonflikt auftritt, gibt das Gerät eine DHCP-Decline-Nachricht zurück.

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.

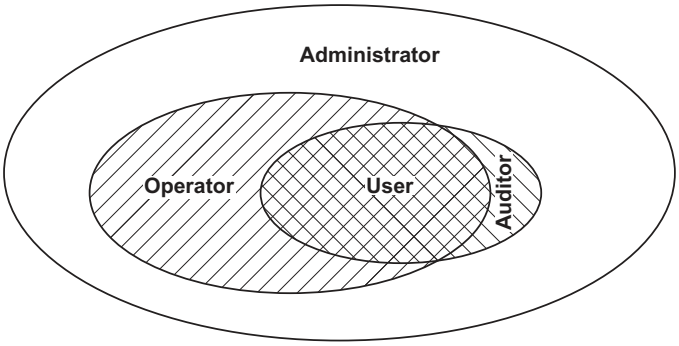
3 Zugriff auf das Gerät

3.1 Berechtigungen

Die Funktionen des Gerätes, die Ihnen als Benutzer zur Verfügung stehen, hängen von Ihrer Berechtigungsstufe ab. Der Funktionsumfang einer Berechtigungsstufe ist für Sie verfügbar, wenn Sie als Benutzer mit dieser Berechtigungsstufe angemeldet sind.

Die Kommandos, die Ihnen als Benutzer zur Verfügung stehen, sind außerdem abhängig vom Modus des Command Line Interface, in welchem Sie sich gerade befinden. Siehe „Modus-basierte Kommando-Hierarchie" auf Seite 25.

Das Gerät bietet Ihnen folgende Berechtigungsstufen:



Tab. 10: Berechtigungsstufen und Umfang der Benutzerrechte

Berechtigungs-stufe	Benutzerrechte
`guest`	Mit der Berechtigungsstufe `guest` angemeldete Benutzer sind berechtigt, das Gerät zu überwachen.
`auditor`	Mit der Berechtigungsstufe `auditor` angemeldete Benutzer sind berechtigt, das Gerät zu überwachen und das Protokoll im Dialog *Diagnose > Bericht > Audit-Trail* zu speichern.
`operator`	Mit der Berechtigungsstufe `operator` angemeldete Benutzer sind berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern – mit Ausnahme der Sicherheitseinstellungen für den Zugriff auf das Gerät.
`administrator`	Mit der Berechtigungsstufe `administrator` angemeldete Benutzer sind berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern.
`unauthorized`	Unauthorisierte Benutzer sind gesperrt, das Gerät verweigert die Anmeldung der Benutzer. Weisen Sie diesen Wert zu, um das Benutzerkonto vorübergehend zu sperren. Wenn beim Zuweisen eines anderen Berechtigungsprofils ein Fehler auftritt, weist das Gerät dem Benutzerkonto diese Berechtigung zu.

3.2 Erste Anmeldung (Passwortänderung)

Um unerwünschte Zugriffe auf das Gerät zu verhindern, ist es unerlässlich, dass Sie das voreingestellte Passwort bei der ersten Anmeldung ändern.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie die grafische Benutzeroberfläche, die Anwendung HiView oder das Command Line Interface, wenn Sie sich zum ersten Mal anmelden.
- ☐ Melden Sie sich mit dem voreingestellten Passwort an.
  Das Gerät fordert Sie auf, ein neues Passwort einzugeben.
- ☐ Geben Sie Ihr neues Passwort ein.
  Um die Sicherheit zu erhöhen, wählen Sie ein Passwort mit mindestens 8 Zeichen, das Großbuchstaben, Kleinbuchstaben, numerische Ziffern und Sonderzeichen enthält.
- ☐ Wenn Sie sich mit dem Command Line Interface anmelden, fordert Sie das Gerät auf, Ihr neues Passwort zu bestätigen.
- ☐ Melden Sie sich mit Ihrem neuen Passwort erneut an.

Anmerkung: Wenn Sie Ihr Passwort vergessen haben, dann wenden Sie sich an Ihren lokalen Support.

Weitere Informationen finden Sie unter hirschmann-support.belden.com.

3.3 Authentifizierungs-Listen

Wenn ein Benutzer über eine bestimmte Verbindung auf das Gerät zugreift, verifiziert das Gerät die Anmeldedaten des Benutzers in einer Authentifizierungs-Liste, die die Richtlinien enthält, die das Gerät für die Authentifizierung anwendet.

Voraussetzung für den Zugriff eines Benutzers auf das Management des Geräts ist, dass der Authentifizierungs-Liste derjenigen Anwendung, über die der Zugriff erfolgt, mindestens eine Richtlinie zugeordnet ist.

3.3.1 Anwendungen

Das Gerät stellt für jede Art von Verbindung, über die jemand auf das Gerät zugreift, eine Anwendung zur Verfügung:

- Zugriff auf das Command Line Interface über eine serielle Verbindung: `Console(V.24)`
- Zugriff auf das Command Line Interface mit SSH: `SSH`
- Zugriff auf das Command Line Interface mit Telnet: `Telnet`
- Zugriff auf 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`

3.3.2 Richtlinien

Das Gerät ermöglicht Benutzern den Zugriff auf das Management des Geräts, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Benutzer mit folgenden Richtlinien:

- Benutzerverwaltung des Geräts
- LDAP
- RADIUS

Mit der Port-basierten Zugriffskontrolle gemäß IEEE 802.1X ermöglicht das Gerät angeschlossenen Endgeräten den 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.

3.3.3 Authentifizierungs-Listen verwalten

Die Authentifizierungs-Listen verwalten Sie in der grafischen Benutzeroberfläche oder im Command Line Interface. Führen Sie dazu die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

Der Dialog zeigt die eingerichteten Authentifizierungs-Listen.

`show authlists`	Eingerichtete Authentifizierungs-Listen anzeigen.

☐ 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.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`authlists disable defaultDot1x8021AuthList`	Authentifizierungs-Liste deaktivieren.`default-Dot1x8021AuthList`.

3.3.4 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 dazu 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`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`authlists add loginGUI`	Authentifizierungs-Liste erzeugen`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 vermeiden.

☐ Markieren Sie in Spalte *Aktiv* das Kontrollkästchen.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`authlists set-policy loginGUI radius local reject reject reject`	Die Richtlinien `radius`, `local` und `reject` der Authentifizierungs-Liste `loginGUI` zuweisen.
`show authlists`	Eingerichtete Authentifizierungs-Listen anzeigen.
`authlists enable loginGUI`	Authentifizierungs-Liste aktivieren.`loginGUI`.

☐ Weist der Authentifizierungs-Liste `loginGUI` eine Anwendung zu.

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*.
- ☐ Wählen Sie in der Tabelle die Authentifizierungsliste `loginGUI`.
- ☐ Klicken Sie die Schaltfläche 📋.
  Der Dialog zeigt das Fenster *Anwendungen zuordnen*.
- ☐ Klicken Sie die Anwendung `WebInterface` an, um diese zu markieren.
- ☐ 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`show applists`	Anwendungen und zugewiesene Listen anzeigen.
`applists set-authlist WebInterface loginGUI`	Die Anwendung `loginGUI` der Authentifizierungs-Liste `WebInterface` zuweisen.

3.4 Benutzerverwaltung

Das Gerät ermöglicht Benutzern den Zugriff auf das Management des Geräts, 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.

3.4.1 Berechtigungen

Das Gerät ermöglicht Ihnen, durch ein rollenbasiertes Berechtigungsmodell die Zugriffe auf das Management des Geräts 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 jede Anwendung an, mit welcher Zugriffe auf das Management des Geräts möglich sind.

Jedes Benutzerkonto ist mit einer Berechtigung verknüpft, das den Zugriff auf die einzelnen Funktionen des Geräts reguliert. Abhängig von der vorgesehenen Tätigkeit des jeweiligen Benutzers weisen Sie ihm eine vordefinierte Berechtigung zu. Das Gerät unterscheidet die folgenden Berechtigungen.

Tab. 11: Berechtigungen für Benutzerkonten

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 ▶ Jedes Passwort 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 ▶ Skripte anwenden mit dem Command Line Interface ▶ CLI-Logging und SNMP-Logging ein- und ausschalten ▶ Externen Speicher aktivieren und deaktivieren ▶ System-Monitor aktivieren und deaktivieren ▶ Dienste für den Zugriff auf das Management des Geräts (zum Beispiel SNMP) ein- und ausschalten. ▶ Zugriffsbeschränkungen auf die grafische Benutzeroberfläche oder das Command Line Interface 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. 11: Berechtigungen für Benutzerkonten (Forts.)

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. ▶ Wenn beim Zuweisen einer anderen Berechtigung ein Fehler auftritt, dann weist das Gerät dem Benutzerkonto diese Berechtigung zu.	Keine erlaubten Tätigkeiten.

3.4.2 Benutzerkonten verwalten

Die Benutzerkonten verwalten Sie in der grafischen Benutzeroberfläche oder im Command Line Interface. Führen Sie dazu die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.

Der Dialog zeigt die eingerichteten Benutzerkonten.

`show users` Eingerichtete Benutzerkonten anzeigen.

3.4.3 Voreinstellung

Im Lieferzustand sind die Benutzerkonten `admin` und `user` im Gerät eingerichtet.

Tab. 12: Voreinstellungen der werkseitig eingerichteten Benutzerkonten

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`

Ändern Sie das Passwort des Benutzerkontos `admin`, bevor Sie das Gerät im Netz zugänglich machen.

3.4.4 Voreingestellte Passwörter ändern

Um ungewünschte Eingriffe zu vermeiden, ändern Sie das Passwort der voreingestellten Benutzerkonten. Führen Sie dazu 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. Das Gerät prüft stets die Mindestlänge des Passworts.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`users password-policy-check <user> enable`	Für das Benutzerkonto `<user>` das Prüfen des Passwortes anhand der festgelegten Richtlinien aktivieren. 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`	Für das Benutzerkonto `<user>` das Passwort `SECRET` festlegen. Fügen Sie mindestens 6 Zeichen ein.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

3.4.5 Neues Benutzerkonto einrichten

Weisen Sie Benutzern, die auf das Management des Geräts 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 dazu 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. Das Gerät prüft stets die Mindestlänge des Passworts.
- ☐ 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
  Der Dialog zeigt die eingerichteten Benutzerkonten.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`users add USER`	Benutzerkonto `USER` erzeugen.

`users password-policy-check USER enable`	Für das Benutzerkonto `USER` das Prüfen des Passwortes anhand der festgelegten Richtlinien aktivieren. Damit erzielen Sie eine höhere Komplexität des Passwortes.
`users password USER SECRET`	Für das Benutzerkonto `USER` das Passwort `SECRET` festlegen. Fügen Sie mindestens 6 Zeichen ein.
`users access-role USER operator`	Die Rolle *`operator`* dem Benutzerkonto `USER` zuweisen.
`users enable USER`	Benutzerkonto `USER` aktivieren.
`show users`	Eingerichtete Benutzerkonten anzeigen.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

Anmerkung: Denken Sie daran, das Passwort zuzuweisen, wenn Sie ein neues Benutzerkonto im Command Line Interface einrichten.

3.4.6 Benutzerkonto deaktivieren

Nach Deaktivieren eines Benutzerkontos verweigert das Gerät Zugriffe des zugehörigen Benutzers auf das Management des Geräts. Im Gegensatz zum vollständigen Löschen ermöglicht Ihnen das Deaktivieren, die Einstellungen des Benutzerkontos für eine künftige Wiederverwendung beizubehalten. Führen Sie dazu 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.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`users disable <user>`	Deaktivieren eines Benutzerkontos.
`show users`	Eingerichtete Benutzerkonten anzeigen.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

☐ Um die Einstellungen des Benutzerkontos dauerhaft zu deaktivieren, löschen Sie das Benutzerkonto.

☐ Wählen Sie die Tabellenzeile des betreffenden Benutzerkontos.

☐ Klicken Sie die Schaltfläche .

`users delete <user>`	Benutzerkonto `<user>` löschen.
`show users`	Eingerichtete Benutzerkonten anzeigen.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

3.4.7 Richtlinien für Passwörter anpassen

Das Gerät ermöglicht Ihnen, die Passwörter der Benutzerkonten auf Einhaltung vorgegebener Richtlinien zu prüfen. Durch Einhaltung der Richtlinien erzielen Sie Passwörter mit höherer Komplexität.

Die Benutzerverwaltung des Geräts ermöglicht Ihnen, die Prüfung in jedem Benutzerkonto individuell ein- oder auszuschalten. Bei eingeschalteter Prüfung akzeptiert das Gerät ein geändertes Passwort, 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 dazu 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.

Anmerkung: Das Gerät ermöglicht ausschließlich Benutzern mit der Berechtigung `administrator`, die Sperre aufzuheben.

Die Anzahl der Login-Versuche sowie die mögliche Sperre des Benutzers beziehen sich ausschließlich auf den Zugriff auf das Management des Geräts über:

- die grafische Benutzeroberfläche
- das SSH-Protokoll
- das Telnet-Protokoll

Anmerkung: Beim Zugriff auf das Management des Geräts mittels des Command Line Interface über die serielle Schnittstelle ist die Anzahl der Login-Versuche unbegrenzt.

☐ 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 ermöglicht Ihnen, diesen Wert im Bereich `0..5` festzulegen.
  Im obigen Beispiel deaktiviert der Wert `0` die Funktion.
- Das Feld *Min. Passwort-Länge* ermöglicht Ihnen, Werte im Bereich `1..64` einzufügen.

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.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`passwords min-length 6`	Richtlinie für die Mindestlänge des Passworts festlegen.
`passwords  min-lowercase-chars 1`	Richtlinie für die Mindestanzahl von Kleinbuchstaben im Passwort festlegen.
`passwords  min-numeric-chars 1`	Richtlinie für die Mindestanzahl von Ziffern im Passwort festlegen.
`passwords  min-special-chars 1`	Richtlinie für die Mindestanzahl von Sonderzeichen im Passwort festlegen.
`passwords  min-uppercase-chars 1`	Richtlinie für die Mindestanzahl von Großbuchstaben im Passwort festlegen.
`show passwords`	Eingerichtete Richtlinien anzeigen.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern.

3.5 LDAP

Server-Administratoren verwalten Active Directorys, die Benutzeranmelde-Informationen für in Büroumgebungen eingesetzte Anwendungen enthalten. Ein Active Directory weist eine hierarchische Struktur auf und enthält Benutzernamen, Passwörter und die autorisierten Berechtigungsstufen mit Lese-/Schreibrechten für die einzelnen Benutzer.

Um Benutzeranmeldeinformationen und Berechtigungsstufen aus einem Active Directory abzurufen, verwendet das Gerät das Lightweight Directory Access Protocol (LDAP). Dies ermöglicht das „Single Sign-On“ (einmalige Anmeldung) für Geräte im Netz. Das Abrufen der Anmeldedaten aus einem Active Directory ermöglicht dem Benutzer, sich mit denselben Anmeldedaten anzumelden, die in der Büroumgebung verwendet werden.

Eine LDAP-Sitzung beginnt damit, dass das Gerät den Directory System Agent (DSA) kontaktiert, um das Active Directory eines LDAP-Servers zu durchsuchen. Findet der Server für einen Benutzer mehrere Einträge im Active Directory, sendet der Server die höhere ermittelte Berechtigungsstufe. Der DSA lauscht nach Informationsanforderungen und sendet Antworten für LDAP über TCP-Port `389` oder für LDAP über SSL (LDAPS) über TCP-Port `636`. Clients und Server kodieren LDAPS-Anfragen und -Antworten mittels der Basic Encoding Rules (BER). Das Gerät öffnet für jede Anfrage eine neue Verbindung und schließt die Verbindung, nachdem das Gerät eine Antwort vom Server empfangen hat.

Das Gerät ermöglicht Ihnen, ein CA-Zertifikat zur Validierung des Servers für SSL- (Secure Socket Layer) und TLS-Sitzungen (Transport Layer Security) hochzuladen. Hierbei ist das Zertifikat für TLS-Sitzungen optional.

Das Gerät ist in der Lage, Anmeldedaten für bis zu 1024 Benutzer im Speicher zwischenzuspeichern. Sind die Active-Directory-Server nicht erreichbar, können sich die Benutzer weiterhin über ihre Büro-Anmeldedaten anmelden.

3.5.1 Abstimmung mit dem Server-Administrator

Die Konfiguration der Funktion *LDAP* erfordert, dass der Netzadministrator die folgenden Informationen vom Server-Administrator anfordert:

- Server-Name oder IP-Adresse
- Ort, an dem sich das Active Directory auf dem Server befindet
- Verwendeter Verbindungstyp
- TCP-Überwachungs-Port
- Falls erforderlich, Speicherort des Zertifikats
- Name des Attributs, das den Benutzeranmeldenamen enthält
- Namen der Attribute, welche die Benutzerberechtigungsstufen enthalten

Der Server-Administrator kann Berechtigungsstufen individuell mit einem Attribut wie `description` oder einer Gruppe mit dem Attribut `memberOf` zuweisen. Im Dialog *Gerätesicherheit > LDAP > Rollen-Zuweisung* legen Sie fest, welche Attribute die verschiedenen Berechtigungsstufen erhalten.

Sie haben außerdem die Möglichkeit, über einen LDAP-Browser wie JXplorer oder Softerra die Namen der Attribute abzurufen, die den Benutzeranmeldenamen und die Berechtigungsstufen enthalten.

3.5.2 Beispiel-Konfiguration

Das Gerät ist in der Lage, eine verschlüsselte Verbindung zu einem lokalen Server ausschließlich über den Server-Namen oder zu einem Server in einem anderen Netz über eine IP-Adresse herzustellen. Der Server-Administrator verwendet Attribute zur Identifizierung der Anmeldedaten eines Benutzers und für die Zuordnung von individuellen Berechtigungsstufen und Gruppenberechtigungsstufen.

Legen Sie anhand der vom Server-Administrator erhaltenen Informationen fest, welche Attribute im Active Directory die Benutzer-Anmeldedaten und die Berechtigungsstufe enthalten. Das Gerät vergleicht anschließend die Benutzer-Anmeldedaten mit den auf dem Gerät festgelegten Berechtigungsstufen und ermöglicht dem Benutzer die Anmeldung mit der zugewiesenen Berechtigungsstufe.

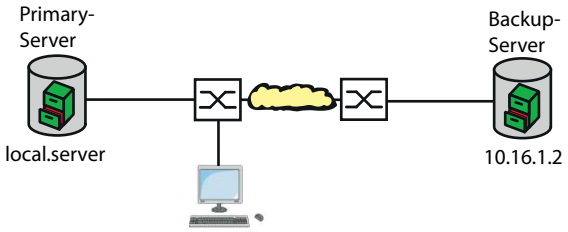


Abb. 18: Beispiel für eine LDAP-Konfiguration

In diesem Beispiel hat der Server-Administrator die folgenden Informationen gesendet:

Information	Primary Server	Backup Server
Server-Name oder IP-Adresse	`local.server`	`10.16.1.2`
Ort, an dem sich das Active Directory auf dem Server befindet	`Land/Stadt/Benutzer`	`Land/Unternehmen/Benutzer`
Verwendeter Verbindungstyp	`TLS` (mit Zertifikat)	`SSL`
Der Server-Administrator hat das CA-Zertifikat in einer E-Mail gesendet.	Lokal gespeichertes CA-Zertifikat für den primären Server	Lokal gespeichertes CA-Zertifikat für den Backup-Server
TCP-Überwachungs-Port	`389 (tls)`	`636 (ssl)`
Name des Attributs, das den Benutzernamen enthält	`userPrincipalName`	`userPrincipalName`
Namen der Attribute, welche die Benutzerberechtigungsstufen enthalten	`OPERATOR` `ADMINISTRATOR`	`OPERATOR` `ADMINISTRATOR`

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*.
- ☐ Um das Gerät so zu konfigurieren, dass es bei der Anmeldung über die grafische Benutzeroberfläche die Benutzer-Anmeldedaten zuerst aus dem Active Directory abruft, legen Sie für die Liste `defaultLoginAuthList` in Spalte *Richtlinie 1* den Wert `ldap` fest.
- ☐ Öffnen Sie den Dialog *Gerätesicherheit > LDAP > Konfiguration*.

- Das Gerät ermöglicht Ihnen festzulegen, über welchen Zeitraum das Gerät die Benutzer-Anmeldedaten im Cache speichert. Um Benutzer-Anmeldedaten für einen Tag im Cache zu speichern, legen Sie im Rahmen *Konfiguration*, Feld *Client-Cache-Timeout [min]* den Wert `1440` fest.
- Der Eintrag *Bind-Benutzer* ist optional. Wenn festgelegt, fügen Benutzer ihren Benutzernamen ein, um sich anzumelden. Der Dienstbenutzer kann jede Person mit Anmeldedaten sein, die im Active Directory unter dem in Spalte *Benutzername-Attribut* festgelegten Attribut aufgeführt sind. Legen Sie in Spalte *Bind-Benutzer* den Benutzernamen und die Domäne fest.
- Der *Base DN* ist eine Kombination der Domänenkomponente (DC) und der Organisationseinheit (OU). Der *Base DN* ermöglicht dem Gerät, einen Server in einer Domäne (DC) zu orten und das Active Directory (OU) ausfindig zu machen. Legen Sie den Speicherort des Active Directory fest. Legen Sie in Spalte *Base DN* den Wert `ou=Users,ou=City,ou=Country,dc=server,dc=local` fest.
- Um das Attribut festzulegen, unter dem der Server-Administrator die Benutzer aufführt, legen Sie in Spalte *Benutzername-Attribut* den Wert `userPrincipalName` fest.

Das Gerät verwendet zur Verifizierung des Servers ein CA-Zertifikat.

- 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.
- Um das CA-Zertifikat auf das Gerät zu übertragen, klicken Sie die Schaltfläche *Start*.
- Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- Um eine Beschreibung festzulegen, fügen Sie in Spalte *Beschreibung* den Wert `Primary AD Server` ein.
- Um den Server-Namen und die Domäne des primären Servers festzulegen, fügen Sie in Spalte *Adresse* den Wert `local.server` ein.
- Der primäre Server verwendet für die Kommunikation den TCP-Port `389`, welches der voreingestellte Wert für *Ziel-TCP-Port* ist.
- Der primäre Server verwendet TLS für die Verschlüsselung der Kommunikation und ein CA-Zertifikat für die Server-Validierung. Legen Sie in Spalte *Verbindungssicherheit* den Wert `startTLS` fest.
- Um den Eintrag zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- Fügen Sie eine weitere Zeile hinzu, die Sie mit den vom Server-Administrator für den Backup-Server empfangenen Dateien konfigurieren und aktivieren.

- Öffnen Sie den Dialog *Gerätesicherheit > LDAP > Rollen-Zuweisung*.
- Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .

Wenn ein Benutzer sich mit konfiguriertem und aktiviertem LDAP anmeldet, sucht das Gerät im Active Directory nach den Anmeldedaten des Benutzers. Wenn das Gerät feststellt, dass Benutzername und Passwort korrekt sind, sucht das Gerät nach dem Wert, den Sie in die Spalte *Typ* festgelegt haben. Wenn das Gerät das Attribut findet und der Text in Spalte *Parameter* mit dem Text im Active Directory übereinstimmt, ermöglicht das Gerät dem Benutzer die Anmeldung mit der zugewiesenen Berechtigungsstufe. Wenn der Wert `attribute` in Spalte *Typ* festgelegt ist, legen Sie den Wert in Spalte *Parameter* in der folgenden Form fest: `attributeName=attributeValue`.

- Um die Benutzer-Rolle festzulegen, legen Sie in Spalte *Rolle* den Wert `operator` fest.
- Um den Eintrag zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.

- Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Fügen Sie die vom Server-Administrator erhaltenen Werte für die Rolle `administrator` ein.
  Um den Eintrag zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- Öffnen Sie den Dialog *Gerätesicherheit > LDAP > Konfiguration*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.

Die folgende Tabelle beschreibt die Vorgehensweise zum Konfigurieren der Funktion *LDAP* auf dem Gerät mit dem Command Line Interface. Die Tabelle zeigt die Kommandos für `Index 1`. Um `Index 2` zu konfigurieren, verwenden Sie dieselben Kommandos und ersetzen die entsprechenden Informationen.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`ldap cache-timeout 1440`	Festlegen, dass das Gerät den permanenten Speicher nach einem Tag leert.
`ldap client server add 1 local.server port 389`	Eine Verbindung zum Remote-Authentifizierungs-Client-Server mit dem Host-Namen `local.server` und UDP-Port `389` hinzufügen.
`ldap client server modify 1 security startTLS`	Sicherheitstyp für die Verbindung festlegen.
`ldap client server modify 1 description Primary_AD_Server`	Konfigurationsnamen für den Eintrag festlegen.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server,dc=local`	Basisdomänennamen festlegen, der zur Ermittlung des Active Directory auf dem Server verwendet wird.
`ldap search-attr userPrincipalName`	Attribut festlegen, nach dem in dem Active Directory, das die Anmeldedaten der Benutzer enthält, gesucht wird.
`ldap bind-user user@company.com`	Namen und Domäne des Bind-Account-Benutzers festlegen.
`ldap bind-passwd Ur-123456`	Passwort des Bind-Account-Benutzers festlegen.
`ldap client server enable 1`	Remote-Authentifizierungs-Client-Server-Verbindung aktivieren.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	Für die Rolle `operator` einen Eintrag zur Zuordnung der Remote-Authentifizierungsrolle hinzufügen. Ordnen Sie die Rolle `operator` dem Attribut zu, welches das Wort `OPERATOR` enthält.
`ldap mapping enable 1`	Eintrag für die Remote-Zuordnung von Authentifizierungsrollen aktivieren.
`ldap operation`	Funktion für die Remote-Authentifizierung aktivieren.

3.6 SNMP-Zugriff

Das Protokoll SNMP ermöglicht Ihnen, mit einem Netzmanagementsystem das Gerät über das Netz zu überwachen und seine Einstellungen zu ändern.

3.6.1 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, den Zugriff auf das Gerät.

Erschweren Sie unerwünschten Zugriff auf das Gerät. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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 Geräts 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.

3.6.2 SNMPv3-Zugriff

Mit SNMPv3 kommunizieren das Netzmanagementsystem und das Gerät verschlüsselt. Das Netzmanagementsystem authentifiziert sich gegenüber dem Gerät mit den Anmeldedaten eines Benutzers. Voraussetzung für den SNMPv3-Zugriff ist, dass im Netzmanagementsystem dieselben Einstellungen wie im Gerät festgelegt sind.

Das Gerät ermöglicht Ihnen, 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`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`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern.

4 Die Systemzeit im Netz synchronisieren

Viele Anwendungen sind auf eine möglichst korrekte Zeit angewiesen. Die notwendige Genauigkeit, also die zulässige Abweichung zur Echtzeit, ist abhängig vom Anwendungsgebiet.

Anwendungsgebiete sind beispielsweise:
- Logbucheinträge
- Produktionsdaten mit Zeitstempel versehen
- Prozesssteuerung

Das Gerät ermöglicht Ihnen, die Zeit im Netz mit den folgenden Optionen zu synchronisieren:
- Das Simple Network Time Protocol (SNTP) ist eine einfache Lösung für geringere Genauigkeitsanforderungen. Unter idealen Bedingungen erzielt SNTP eine Genauigkeit im Millisekunden-Bereich. Die Genauigkeit ist abhängig von der Signallaufzeit.
- IEEE 1588 mit dem Precision Time Protocol (PTP) erreicht eine Genauigkeit im Submikrosekunden-Bereich. Diese Methode eignet sich auch für anspruchsvolle Anwendungen bis hin zur Prozesssteuerung.

PTP ist 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 Geräts beeinflussen, sind Situationen denkbar, in denen beide Protokolle konkurrieren.

4.1 Grundeinstellungen

Im Dialog *Zeit > Grundeinstellungen* legen Sie allgemeine Einstellungen für die Zeit fest.

4.1.1 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 Ausschalten des Netzteils puffert das Gerät die Einstellungen der Echtzeituhr bis zu 24 Stunden lang.

Alternativ legen Sie die Einstellungen im Gerät so fest, dass es die aktuelle Uhrzeit automatisch von einer PTP-Uhr oder von einem SNTP-Server bezieht.

Alternativ legen Sie die Einstellungen im Gerät so fest, dass es die aktuelle Uhrzeit automatisch von einem SNTP-Server bezieht.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Zeit > Grundeinstellungen*.
- Das Feld *Systemzeit (UTC)* zeigt die aktuelle UTC (Universal Time Coordinated) des Geräts. 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.

Anmerkung: PTP sendet die Internationale Atomzeit (TAI). Mit Stand vom 1. Juli 2020 geht die TAI-Zeit 37 s gegenüber der UTC-Zeit vor. Wenn auf der PTP-Referenzzeitquelle der UTC-Offset korrekt festgelegt ist, korrigiert das Gerät diesen Unterschied bei der Anzeige im Feld *Systemzeit (UTC)* automatisch.

- 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. Das Gerät wählt automatisch die Quelle mit der höchsten Genauigkeit.
  Die Quelle ist zunächst `local`.
  Ist SNTP aktiviert und empfängt das Gerät ein gültiges SNTP-Paket, setzt es seine Zeitquelle auf `sntp`.
  Ist PTP aktiviert und empfängt das Gerät eine gültige PTP-Nachricht, setzt es seine Zeitquelle auf `ptp`. Das Gerät gibt der Zeitquelle PTP den Vorrang vor SNTP.
- Der Wert *Lokaler Offset [min]* legt die Zeitdifferenz fest zwischen der lokalen Zeit und der *Systemzeit (UTC)*.
- Damit das Gerät die Zeitzone Ihres PCs ermittelt, klicken Sie die Schaltfläche *Setze Zeit vom PC*. Das Gerät berechnet daraus die lokale Zeitdifferenz zur UTC-Zeit und trägt die Differenz in das Feld *Lokaler Offset [min]* ein.

Anmerkung: Das Gerät bietet die Möglichkeit, den lokalen Offset von einem DHCP-Server beziehen.

- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	Systemzeit des Geräts einstellen.
`clock timezone offset <-780..840>`	Zeitdifferenz zwischen der lokalen Zeit und der empfangenen UTC-Zeit in Minuten angeben.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern.

4.1.2 Automatische Sommerzeitumschaltung

Wenn Sie das Gerät in einer Zeitzone betreiben, in der es die Sommerzeitumstellung gibt, richten Sie auf der Registerkarte *Sommerzeit* die automatische Zeitumstellung 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 dazu 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 `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`clock summer-time mode <disable|recurring|eu|usa>`	Automatische Sommerzeitumstellung konfigurieren: einschalten, ausschalten oder mit Profil aktivieren.
`clock summer-time recurring start`	Startzeitpunkt für die Umschaltung eingeben.
`clock summer-time recurring end`	Endzeitpunkt für die Umschaltung eingeben.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern.

4.2 SNTP

Das Simple Network Time Protocol (SNTP) ermöglicht Ihnen, 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.

Tab. 13: IPv4-Zieladressklassen für Broadcast-Betriebsmodus

IPv4-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

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.

4.2.1 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.

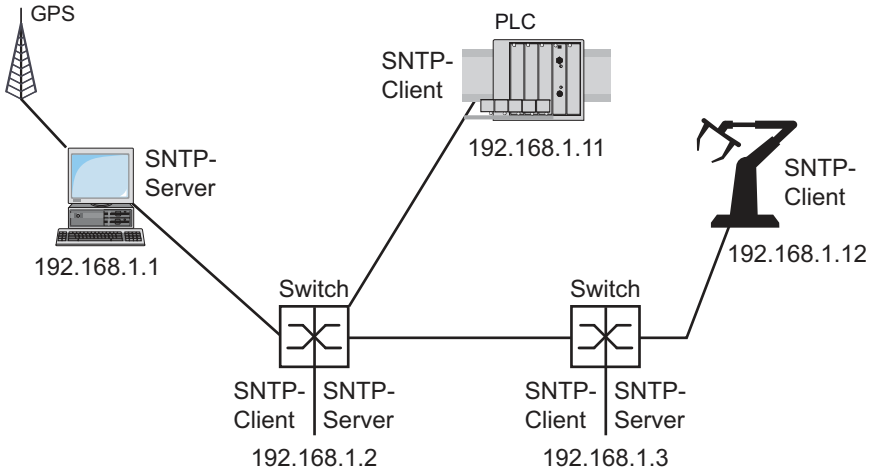


Abb. 19: Beispiel SNTP-Kaskade

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, sendet er die Anfrage an den 3. und schließlich an den 4. SNTP-Server. Antwortet keiner dieser SNTP-Server, 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.

4.2.2 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 dazu 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*- oder *Multicast*-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 Funktion *SNTP Client* 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 `An`.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- Das Feld *Zustand* zeigt den aktuellen Status der Funktion *SNTP Client*.

Tab. 14: Einstellungen der SNTP-Clients für das Beispiel

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Funktion *SNTP Client*	`Aus`	`An`	`An`	`An`	`An`

Tab. 14: Einstellungen der SNTP-Clients für das Beispiel (Forts.)

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
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

4.2.3 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 dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Zeit > SNTP > Server*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ 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 IPv4-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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ▶ Das Feld *Zustand* zeigt den aktuellen Status der Funktion *SNTP Server*.

Tab. 15: Einstellungen für das Beispiel

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Funktion *SNTP Server*	*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

4.3 PTP

Damit über ein LAN gesteuerte Anwendungen ohne Latenz arbeiten, ist ein präzises Zeitmanagement erforderlich. IEEE 1588 beschreibt mit PTP (Precision Time Protocol) ein Verfahren, das die präzise Synchronisation der Uhren im Netz ermöglicht.

Das PTP erlaubt die Synchronisation mit einer Genauigkeit bis zu wenigen 100 ns. PTP verwendet Multicasts für die Synchronisationsnachrichten, dadurch ist die Netzlast gering.

4.3.1 Typen von Uhren

Das PTP definiert für die Uhren im Netz die Rollen „Master“ und „Slave“:
- Eine Master-Uhr (Referenzzeitquelle) verteilt ihre Zeit.
- Eine Slave-Uhr synchronisiert sich auf das von der Master-Uhr empfangene Zeitsignal.

Boundary Clock

Die Durchlaufzeit (Latenz) in Routern und Switches wirkt sich messbar auf die Präzision der Zeitübertragung aus. Um solche Ungenauigkeiten zu korrigieren, definiert PTP sogenannte Boundary-Clocks.

Eine Boundary-Clock ist die Referenzzeitquelle (Master-Uhr) in einem Netzsegment, auf die sich die untergeordneten Slave-Uhren synchronisieren. Typischerweise übernehmen Router und Switches die Rolle der Boundary-Clock.

Die Boundary-Clock bezieht ihrerseits die Uhrzeit von einer übergeordneten Referenzzeitquelle (Grandmaster).

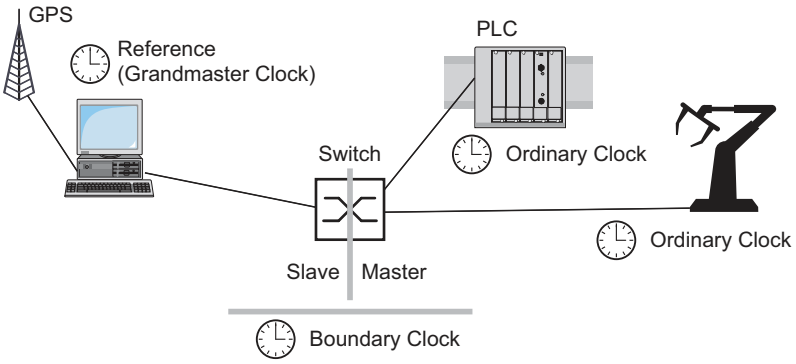


Abb. 20: Position der Boundary-Clock in einem Netz

Transparent Clock

Typischerweise übernehmen Switches die Rolle der Transparent Clock, um über Kaskaden hinweg eine hohe Genauigkeit zu ermöglichen. Die Transparent Clock ist eine Slave-Uhr, die beim Weiterleiten empfangener Synchronisationsnachrichten die eigene Durchlaufzeit korrigiert.

Ordinary Clock

Die Uhr in einem Endgerät bezeichnet PTP als „Ordinary Clock“. Eine Ordinary Clock funktioniert entweder als Master-Uhr oder als Slave-Uhr.

4.3.2 Best-Master-Clock-Algorithmus

Die an PTP beteiligten Geräte bestimmen ein Gerät im Netz zur Referenzzeitquelle (Grandmaster). Dabei kommt der „Best Master Clock“-Algorithmus zum Einsatz, der die Genauigkeit der verfügbaren Uhren im Netz ermittelt.

Der „Best Master Clock“-Algorithmus bewertet dabei folgende Kriterien:
- *Priorität 1*
- *Uhr-Klasse*
- *Präzision*
- *Uhr-Varianz*
- *Priorität 2*

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

Das Gerät ermöglicht Ihnen, in den Einstellungen der Boundary-Clock den Wert für *Priorität 1* und *Priorität 2* individuell festzulegen. Dies ermöglicht Ihnen, Einfluss darauf zu nehmen, welches Gerät die Referenzzeitquelle (Grandmaster) im Netz wird.

4.3.3 Laufzeitmessung

Die Laufzeit der Synchronisationsnachrichten zwischen den beteiligten Geräten hat Einfluss auf die Genauigkeit. Durch die Laufzeitmessung berücksichtigen die Geräte die mittlere Laufzeit.

PTP Version 2 bietet folgende Verfahren für die Laufzeitmessung:
- `e2e` (End to End)
  Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
- `e2e-optimized`
  Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
  Dieses Verfahren ist ausschließlich für Transparent-Clocks verfügbar. Das Gerät vermittelt die per Multicast gesendeten Synchronisationsnachrichten ausschließlich an die Master-Uhr und hält dadurch die Netzlast gering. Wenn das Gerät eine Synchronisationsnachricht von einer anderen Master-Uhr empfängt, vermittelt es die Synchronisationsnachrichten ausschließlich an diesen neuen Port.
  Kennt das Gerät keine Master-Uhr, vermittelt es Synchronisationsnachrichten an jeden Port.
- `p2p` (Peer to Peer)
  Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
  Zusätzlich misst die Master-Uhr die Laufzeit zu jeder Slave-Uhr, auch über blockierte Ports hinweg. Voraussetzung ist, dass Master- und Slave-Uhr Peer-to-Peer (`p2p`) unterstützen.
  Bei Unterbrechung eines redundanten Rings beispielsweise wird eine Slave-Uhr zur Master-Uhr und die Master-Uhr zur Slave-Uhr. Dieser Wechsel findet ohne Präzisionsverlust statt, weil die Uhren die Laufzeit in die andere Richtung bereits kennen.

4.3.4 PTP-Domänen

Synchronisationsnachrichten überträgt das Gerät ausschließlich von und zu Geräten in derselben PTP-Domäne. Das Gerät ermöglicht Ihnen, die Domäne für die Boundary-Clock und für die Transparent-Clock individuell festzulegen.

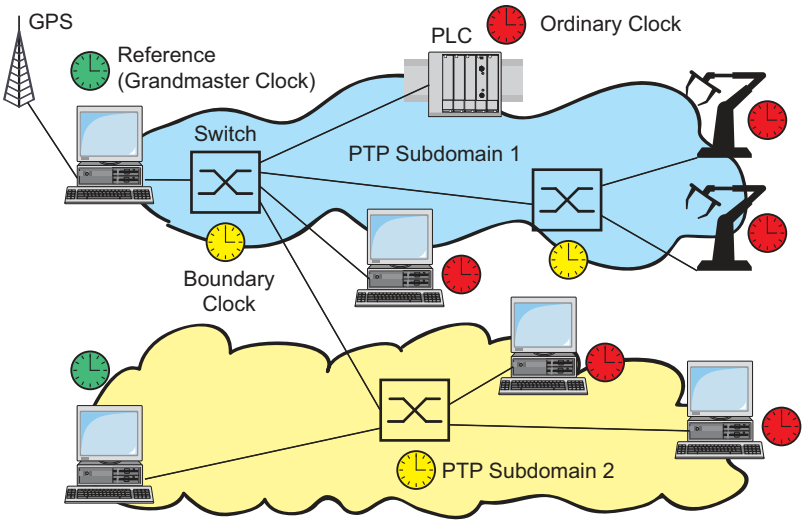


Abb. 21: Beispiel für PTP-Domänen

4.3.5 PTP verwenden

Um die Uhren präzise mit PTP zu synchronisieren, verwenden Sie als Netzknoten ausschließlich Switches mit Boundary-Clock oder Transparent-Clock.

Führen Sie die folgenden Schritte aus:

- ☐ Um sich einen Überblick über die Uhrenverteilung zu verschaffen, zeichnen Sie einen Netzplan mit den am PTP beteiligten Geräten.
- ☐ Legen Sie für jeden beteiligten Switch die Rolle fest (Boundary-Clock oder Transparent-Clock). Im Gerät heißt diese Einstellung *PTP-Modus*.

Tab. 16: Mögliche Einstellwerte für den PTP-Modus

PTP-Modus	Anwendung
`v2-boundary-clock`	Als Boundary-Clock verteilt das Gerät die Synchronisationsnachrichten an die Slave-Uhren im untergeordneten Netzsegment. Die Boundary-Clock bezieht ihrerseits die Uhrzeit von einer übergeordneten Referenzzeitquelle (Grandmaster).
`v2-transparent-clock`	Als Transparent-Clock leitet das Gerät empfangene Synchronisationsnachrichten korrigiert um die eigene Durchlaufzeit weiter.

- ☐ Schalten Sie PTP auf jedem beteiligten Switch ein.
  PTP konfiguriert sich anschließend weitestgehend automatisch.
- ☐ Schalten Sie PTP auf den Endgeräten ein.
- ☐ Das Gerät ermöglicht Ihnen, Einfluss darauf zu nehmen, welches Gerät im Netz Referenzzeitquelle (Grandmaster) wird. Ändern Sie dazu für die *Boundary Clock* den voreingestellten Wert in den Feldern *Priorität 1* und *Priorität 2*.

5 Konfigurationsprofile verwalten

Wenn Sie die Einstellungen des Geräts im laufenden Betrieb ändern, dann speichert das Gerät diese Änderungen im flüchtigen Speicher (*RAM*). Nach einem Neustart sind diese Einstellungen verloren.

Damit die Änderungen einen Neustart überdauern, ermöglicht Ihnen das Gerät, die Einstellungen 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, dann speichert das Gerät automatisch eine Kopie des Konfigurationsprofils im externen Speicher (*ENVM*). Sie können diese Funktion ausschalten.

5.1 Geänderte Einstellungen erkennen

Das Gerät speichert die während des Betriebs geänderten Einstellungen im flüchtigen Speicher (*RAM*). Das Konfigurationsprofil im permanenten Speicher (*NVM*) bleibt dabei so lange unverändert, bis Sie die geänderten Einstellungen explizit speichern. Bis dahin unterscheiden sich die Konfigurationsprofile im flüchtigen und im permanenten Speicher. Das Gerät unterstützt Sie dabei, geänderte Einstellungen zu erkennen.

5.1.1 Flüchtiger Speicher (RAM) und nichtflüchtiger Speicher (NVM)

Sie können erkennen, ob die Einstellungen im flüchtigen Speicher (*RAM*) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (*NVM*) abweichen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Prüfen Sie das Banner der grafischen Benutzeroberfläche:
  - Wenn das Symbol **!** sichtbar ist, weichen die Einstellungen voneinander ab.
  - Wenn kein Symbol **!** sichtbar ist, stimmen die Einstellungen überein.

oder:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Prüfen Sie den Zustand des Kontrollkästchens im Rahmen *Information*:
  - Wenn das Kontrollkästchen markiert ist, stimmen die Einstellungen überein.
  - Wenn das Kontrollkästchen nicht markiert ist, weichen die Einstellungen voneinander ab.

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.......................out of sync
...
```

5.1.2 Externer Speicher (ACA) und nichtflüchtiger Speicher (NVM)

Sie können erkennen, ob die Einstellungen des „ausgewählten“ Konfigurationsprofils (ACA) im externen Speicher von den Einstellungen des „ausgewählten“ Konfigurationsprofils im permanenten Speicher (*NVM*) abweichen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Prüfen Sie den Zustand des Kontrollkästchens im Rahmen *Information*:
  - Wenn das Kontrollkästchen markiert ist, stimmen die Einstellungen überein.
  - Wenn das Kontrollkästchen nicht markiert ist, weichen die Einstellungen voneinander ab.

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to ACA.................................out of sync
...
```

5.2 Einstellungen speichern

5.2.1 Konfigurationsprofil im Gerät speichern

Wenn Sie die Einstellungen des Geräts im laufenden Betrieb ändern, dann 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 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`	Die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile anzeigen.
`enable`	In den Privileged-EXEC-Modus wechseln.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern.

Einstellungen in Konfigurationsprofil kopieren

Das Gerät ermöglicht Ihnen, 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`	Die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile anzeigen.
`enable`	In den Privileged-EXEC-Modus wechseln.
`copy config running-config nvm profile <string>`	Aktuelle Einstellungen im Konfigurationsprofil mit der Bezeichnung `<string>` im permanenten Speicher (`nvm`) speichern. Wenn vorhanden, überschreibt das Gerät ein namensgleiches Konfigurationsprofil. Das neue Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

Konfigurationsprofil auswählen

Wenn der permanente Speicher (*NVM*) mehrere Konfigurationsprofile enthält, haben Sie die Möglichkeit, dort ein beliebiges Konfigurationsprofil auszuwählen. Das Gerät speichert die Einstellungen 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`	In den Privileged-EXEC-Modus wechseln.
`show config profiles nvm`	Die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile anzeigen.
`configure`	In den Konfigurationsmodus wechseln.
`config profile select nvm 1`	Konfigurationsprofil auswählen. Orientieren Sie sich am nebenstehenden Namen des Konfigurationsprofils.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern.

5.2.2 Konfigurationsprofil im externen Speicher speichern

Wenn ein externer Speicher angeschlossen ist und Sie ein Konfigurationsprofil speichern, speichert das Gerät automatisch eine Kopie im *Ausgewählter externer Speicher*. In der Voreinstellung ist die Funktion eingeschaltet. Sie können diese Funktion ausschalten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Externer Speicher*.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Sichere Konfiguration beim Speichern*, damit das Gerät beim Speichern automatisch eine Kopie im externen Speicher speichert.
- ☐ Um die Funktion zu deaktivieren, heben Sie die Markierung des Kontrollkästchens in Spalte *Sichere Konfiguration beim Speichern* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`config envm config-save sd` `config envm config-save usb`	Funktion einschalten. Beim Speichern eines Konfigurationsprofils speichert das Gerät eine Kopie im externen Speicher. `sd` = Externer SD-Speicher `usb` = Externer USB-Speicher
`no config envm config-save sd` `no config envm config-save usb`	Funktion ausschalten. Das Gerät speichert keine Kopie im externen Speicher. `sd` = Externer SD-Speicher `usb` = Externer USB-Speicher
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

5.2.3 Konfigurationsprofil auf einem Remote-Server sichern

Das Gerät ermöglicht Ihnen, 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*.
  Führen Sie im Rahmen *Sichere Konfiguration auf Remote-Server beim Speichern* die folgenden Schritte 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`show config remote-backup`	Status der Funktion prüfen.
`configure`	In den Konfigurationsmodus wechseln.
`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`	Funktion einschalten.

Wenn die Übertragung zum entfernten Server scheitert, dann protokolliert das Gerät dieses Ereignis in der Protokolldatei System Log.

5.2.4 Konfigurationsprofil exportieren

Das Gerät ermöglicht Ihnen, ein Konfigurationsprofil als XML-Datei auf einem Server zu speichern. Wenn Sie die grafische Benutzeroberfläche verwenden, dann haben Sie die Möglichkeit, die XML-Datei direkt auf Ihrem PC zu speichern.

Voraussetzungen:
- ▶ 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.

Exportieren Sie das Konfigurationsprofil auf Ihren PC. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie den Link in Spalte *Profilname*.
  Das Konfigurationsprofil wird heruntergeladen und als XML-Datei auf ihrem PC gespeichert.

Exportieren Sie das Konfigurationsprofil auf einen Remote-Server. Führen Sie dazu 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 *Password* ein, um sich am Server anzumelden.
- Klicken Sie die Schaltfläche *Ok*.
  Das Konfigurationsprofil ist jetzt als XML-Datei am festgelegten Ort gespeichert.

`show config profiles nvm`	Die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile anzeigen.
`enable`	In den Privileged-EXEC-Modus wechseln.
`copy config running-config remote tftp://<IP_address>/ <path>/<file_name>`	Aktuelle Einstellungen auf einem TFTP-Server speichern.
`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	Das „ausgewählte” Konfigurationsprofil im permanenten Speicher `nvm` auf einem SFTP-Server speichern.
`copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>`	Das Konfigurationsprofil `config3` im permanenten Speicher (`nvm`) auf einem TFTP-Server speichern.
`copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>`	Das Konfigurationsprofil `config3` im permanenten Speicher (`nvm`) auf einem FTP-Server speichern.

5.3 Einstellungen laden

Wenn Sie mehrere Konfigurationsprofile im Speicher hinterlegen, haben Sie die Möglichkeit, ein anderes Konfigurationsprofil zu laden.

5.3.1 Konfigurationsprofil aktivieren

Der permanente Speicher des Geräts kann mehrere Konfigurationsprofile enthalten. Wenn Sie ein im permanenten Speicher (*NVM*) hinterlegtes Konfigurationsprofil aktivieren, dann verändern Sie die Einstellungen des Geräts unmittelbar. Das Gerät benötigt keinen 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 ab sofort die Einstellungen des Konfigurationsprofils.

- ☐ Laden Sie die grafische Benutzeroberfläche neu.
- ☐ Melden Sie sich erneut an.

In Spalte *Ausgewählt* ist das Kontrollkästchen des zuvor aktivierten Konfigurationsprofils `markiert`.

`show config profiles nvm`	Die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile anzeigen.
`enable`	In den Privileged-EXEC-Modus wechseln.
`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 Verbindung zum Command Line Interface. Das Gerät verwendet ab sofort die Einstellungen des Konfigurationsprofils `config3`.

5.3.2 Konfigurationsprofil aus dem externen Speicher laden

Wenn der externe Speicher angeschlossen ist, dann lädt das Gerät beim Neustart automatisch ein Konfigurationsprofil aus dem externen Speicher. Das Gerät ermöglicht Ihnen, diese Einstellungen wieder in einem Konfigurationsprofil im permanenten Speicher zu speichern.

Wenn der externe Speicher das Konfigurationsprofil eines baugleichen Geräts enthält, 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`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`config envm load-priority sd first`	Funktion einschalten. Beim Neustart lädt das Gerät ein Konfigurationsprofil aus dem externen Speicher. `sd` = Externer SD-Speicher
`config envm load-priority usb first`	Funktion einschalten. Beim Neustart lädt das Gerät ein Konfigurationsprofil aus dem externen Speicher. `usb` = Externer USB-Speicher
`show config envm settings`	Einstellungen des externen Speichers (`envm`) anzeigen.

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
sd     ok          [x]         [x]         second
usb    ok          [x]         [x]         first
```

`save`	Die Einstellungen in einem Konfigurationsprofil im permanenten Speicher (*NVM*) des Geräts speichern.

Das Gerät ermöglicht Ihnen, mit dem Command Line Interface die Einstellungen aus dem externen Speicher in den permanenten Speicher (*NVM*) zu kopieren.

`show config profiles nvm`	Die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile anzeigen.
`enable`	In den Privileged-EXEC-Modus wechseln.
`copy config envm profile config3 nvm`	Das Konfigurationsprofil `config3` aus dem externen Speicher (`envm`) in den permanenten Speicher (`nvm`) kopieren.

Während des Bootvorgangs kann das Gerät außerdem automatisch ein Konfigurationsprofil aus einer Skriptdatei laden.

Voraussetzungen:
- Vergewissern Sie sich, dass der externe Speicher angeschlossen ist, bevor Sie das Gerät starten.
- Das Root-Verzeichnis des externen Speichers enthält eine Textdatei `startup.txt` mit dem Inhalt `script=<Dateiname>`. Der Platzhalter `<Dateiname>` repräsentiert die Skriptdatei, die das Gerät während des Bootvorgangs ausführt.
- Das Root-Verzeichnis des externen Speichers enthält die Skript-Datei. Sie haben die Möglichkeit, das Skript unter einem benutzerdefinierten Namen zu speichern. Speichern Sie die Datei mit der Dateiendung `.cli`.

Anmerkung: Vergewissern Sie sich, dass das im externen Speicher gespeicherte Skript nicht leer ist. Wenn das Skript leer ist, dann lädt das Gerät gemäß den Einstellungen der Konfigurations-Priorität das nächste Konfigurationsprofil.

Nach Anwenden des Skripts speichert das Gerät das Konfigurationsprofil aus der Skriptdatei automatisch als XML-Datei im externen Speicher. Sie haben die Möglichkeit, diese Funktion auszuschalten, wenn Sie den betreffenden Befehl in die Skriptdatei einfügen:

- `no config envm config-save sd`
  Das Gerät erzeugt keine Kopie im externen SD-Speicher.
- `no config envm config-save usb`
  Das Gerät erzeugt keine Kopie im externen USB-Speicher.

Enthält die Skriptdatei einen falschen Befehl, wendet das Gerät diesen Befehl während des Bootvorgangs nicht an. Das Gerät protokolliert das Ereignis in der Log-Datei (System Log).

5.3.3 Konfigurationsprofil importieren

Das Gerät ermöglicht Ihnen, ein als XML-Datei gespeichertes Konfigurationsprofil von einem Server zu importieren. Wenn Sie die grafische Benutzeroberfläche verwenden, dann können Sie die XML-Datei direkt von Ihrem PC importieren.

Voraussetzungen:
- 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* den Speicherort aus, von dem 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 aus dem ausgewählten externen Speicher.

Importieren Sie das Konfigurationsprofil vom lokalen PC oder von einem Remote-Server. Führen Sie dazu 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, dann trennt das Gerät die Verbindung zur grafischen Benutzeroberfläche und verwendet sofort die Einstellungen.

Importieren Sie das Konfigurationsprofil aus dem externen Speicher. Führen Sie dazu 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, dann trennt das Gerät die Verbindung zur grafischen Benutzeroberfläche und verwendet sofort die Einstellungen.

`enable`	In den Privileged-EXEC-Modus wechseln.
`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 Verbindung zum Command Line Interface. Das Gerät verwendet ab sofort die Einstellungen des importierten Konfigurationsprofils.
`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 Verbindung zum Command Line Interface. Das Gerät verwendet ab sofort die Einstellungen des importierten Konfigurationsprofils.
`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 Verbindung zum Command Line Interface. Das Gerät verwendet ab sofort die Einstellungen des importierten Konfigurationsprofils.
`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.

Anmerkung: Wechsel von Classic zu HiOS? Verwenden Sie unser Online-Tool, um Ihre Dateien mit der Gerätekonfiguration zu konvertieren: https://convert.hirschmann.com

5.4 Gerät auf Lieferzustand zurücksetzen

Wenn Sie die Einstellungen im Gerät auf den Lieferzustand zurücksetzen, dann löscht das Gerät die Konfigurationsprofile im flüchtigen Speicher und im permanenten Speicher.

Wenn ein externer Speicher angeschlossen ist, dann löscht das Gerät auch die im externen Speicher gespeicherten Konfigurationsprofile.

Anschließend startet das Gerät neu und lädt die Werkseinstellungen.

5.4.1 Mit grafischer Benutzeroberfläche oder Command Line Interface

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 Meldung.
- ☐ Klicken Sie die Schaltfläche *Ok*.

Das Gerät löscht die Konfigurationsprofile im flüchtigen Speicher (`RAM`) und im permanenten Speicher (*`NVM`*).

Wenn ein externer Speicher angeschlossen ist, dann löscht das Gerät auch die im externen Speicher gespeicherten Konfigurationsprofile.

Nach kurzer Zeit startet das Gerät neu und lädt die Werkseinstellungen.

`enable`	In den Privileged-EXEC-Modus wechseln.
`clear factory`	Konfigurationsprofile im flüchtigen Speicher und im permanenten Speicher löschen. Wenn ein externer Speicher angeschlossen ist, dann löscht das Gerät auch die im externen Speicher gespeicherten Konfigurationsprofile. Nach kurzer Zeit startet das Gerät neu und lädt die Werkseinstellungen.

5.4.2 System-Monitor starten

Voraussetzung:
- Ihr PC ist per Terminal-Kabel mit der seriellen Schnittstelle des Geräts 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).
  Wenn ein externer Speicher angeschlossen ist, dann löscht das Gerät auch die im 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>.

6 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:

- Frühere Software-Version laden
- Software-Update vom PC
- Software-Update von einem Server
- Software-Update aus dem externen Speicher

Anmerkung: Die Einstellungen im Gerät bleiben nach dem Aktualisieren der Geräte-Software erhalten.

Die Version der installierten Geräte-Software sehen Sie im Login-Dialog der grafischen Benutzeroberfläche.

Um die Version der installierten Geräte-Software anzuzeigen, wenn Sie bereits eingeloggt sind, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
  Das Feld *Ausgeführte Version* zeigt Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Neustart geladen hat und gegenwärtig ausführt.

`enable`	In den Privileged-EXEC-Modus wechseln.
`show system info`	Systeminformationen anzeigen, unter anderem Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Neustart geladen hat und gegenwärtig ausführt.

6.1 Frühere Software-Version laden

Das Gerät ermöglicht Ihnen, die Geräte-Software durch eine frühere 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.

6.2 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.

6.3 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 gegenwärtig 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`	In den Privileged-EXEC-Modus wechseln.
`copy firmware remote tftp://10.0.1.159/product.bin system`	Datei `product.bin` vom TFTP-Server mit der IP-Adresse `10.0.1.159` auf das Gerät übertragen.

6.4 Software-Update aus dem externen Speicher

6.4.1 Manuell – durch den Administrator initiiert

Das Gerät ermöglicht Ihnen, die Geräte-Software mit wenigen Mausklicks zu aktualisieren. Voraussetzung ist, dass sich die Image-Datei der Geräte-Software im 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 im externen Speicher zeigt.
- ☐ Rechtsklicken Sie, um das Kontextmenü anzuzeigen.
- ☐ Um den Update-Vorgang zu starten, klicken Sie im Kontextmenü den Eintrag *Update*.
  Die gegenwärtig 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.

6.4.2 Automatisch – durch das Gerät initiiert

Wenn sich folgende Dateien im externen Speicher befinden, aktualisiert das Gerät beim Neustart die Geräte-Software automatisch:

- ▶ 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` festgelegt ist?
  - Ist die Software-Version der Image-Datei aktueller als die gegenwärtig im Gerät ausgeführte Software?

  Wenn die Kriterien erfüllt sind, startet das Gerät den Update-Vorgang.
  Die gegenwärtig ausgeführte Geräte-Software kopiert das Gerät in den Backup-Bereich.
  Sobald der Update-Vorgang erfolgreich beendet ist, startet das Gerät selbstständig 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 Gerät die Image-Datei nicht gespeichert hat.

7 Ports konfigurieren

Folgende Funktionen für die Port-Konfiguration stehen zur Verfügung:
- Port ein-/ausschalten
- Betriebsart wählen

7.1 Port ein-/ausschalten

In der Voreinstellung ist jeder Port eingeschaltet. Um die Zugriffssicherheit zu erhöhen, deaktivieren Sie Ports, die nicht angeschlossen sind. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`no shutdown`	Die Schnittstelle aktivieren.

7.2 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 *Konfiguration*.
- ☐ Wenn das an diesem Port angeschlossene Gerät eine feste Einstellung voraussetzt, dann führen Sie anschließend die folgenden Schritte aus:
  - ☐ 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`no auto-negotiate`	Modus für die automatische Konfiguration ausschalten.
`speed 100 full`	Port-Geschwindigkeit 100 MBit/s, Vollduplex festlegen.

8 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 Geräts die folgenden Schritte aus, um die Möglichkeit eines unbefugten Zugriffs auf das Gerät zu verringern.

- 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
- Nicht verwendete Module deaktivieren

8.1 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, ermöglicht das Gerät jedem, der den Community-Namen kennt, den Zugriff auf das Gerät.

Voreingestellt sind die Community-Namen `public` für Lese-Zugriffe und `private` für Schreib-Zugriffe. Wenn Sie SNMPv1 oder SNMPv2 verwenden, dann ändern Sie die voreingestellten Community-Namen. Behandeln Sie die Community-Namen vertraulich. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community*.

  Der Dialog zeigt die eingerichteten Communitys.
- ☐ Legen Sie für die `Write`-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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`snmp community rw <community name>`	Community für Lese-/Schreibzugriffe festlegen.
`show snmp community`	Eingerichtete Communities anzeigen.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

8.2 SNMPv1/v2 ausschalten

Wenn Sie SNMPv1 oder SNMPv2 benötigen, dann 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 dazu 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`no snmp access version v1`	Protokoll SNMPv1 deaktivieren.
`no snmp access version v2`	Protokoll SNMPv2 deaktivieren.
`show snmp access`	Einstellungen des SNMP-Servers anzeigen.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern.

8.3 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 dazu 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 *Aus*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`no http server`	Protokoll HTTP ausschalten.

Wenn das Protokoll HTTP ausgeschaltet ist, erreichen Sie die grafische Benutzeroberfläche des Geräts ausschließlich über HTTPS. In der Adresszeile des Web-Browsers fügen Sie vor der IP-Adresse des Geräts 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 den HTTPS-Server mit dem Command Line Interface ein. Führen Sie dazu die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`https server`	Protokoll HTTPS einschalten.

8.4 Telnet ausschalten

Das Gerät ermöglicht Ihnen, über Telnet oder SSH per Fernzugriff auf das Management des Geräts 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 dazu 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 `Aus`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`no telnet server`	Telnet-Server ausschalten.

Wenn der SSH-Server ausgeschaltet ist und Sie auch Telnet ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die serielle Schnittstelle des Geräts möglich. Um per Fernzugriff mit dem Command Line Interface zu arbeiten, schalten Sie SSH ein. Führen Sie dazu 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 `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`ssh server`	SSH-Server einschalten.

8.5 HiDiscovery-Zugriff ausschalten

HiDiscovery ermöglicht Ihnen, 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 Geräts HiDiscovery ausschließlich Leserechte zu gewähren oder den HiDiscovery-Zugriff vollständig auszuschalten. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netz > 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 *`Aus`*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`network hidiscovery mode read-only`	Der HiDiscovery-Software die Schreibrechte entziehen.
`no network hidiscovery operation`	HiDiscovery-Zugriff ausschalten.

8.6 IP-Zugriffsbeschränkung aktivieren

Per Voreinstellung erreichen Sie das Management des Geräts von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle.

Die IP-Zugriffsbeschränkung ermöglicht Ihnen, den Zugriff auf das Management des Geräts 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-Schlüssels.

Tab. 17: Parameter für die IP-Zugriffsbeschränkung

Parameter	Firmennetz	Mobilfunknetz
Netzadresse	`192.168.1.0`	`109.237.176.0`
Netzmaske	`24`	`24`
Gewünschte Protokolle	https, snmp	ssh

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 Benutzern 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 das Management des Geräts ist ausschließlich mit dem Command Line Interface über die serielle Schnittstelle des Geräts möglich.

- Um die IP-Zugriffsbeschränkung einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`show network management access global`	Zeigen, 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 jedes ungewünschte Protokoll 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 jedes ungewünschte Protokoll wiederholen.
`no network management access status 1`	Voreingestellten Eintrag deaktivieren. Dieser Eintrag ermöglicht Benutzern 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.

8.7 Session-Timeouts anpassen

Das Gerät ermöglicht Ihnen, 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:
- Command Line Interface: Sessions über eine SSH-Verbindung
- Command Line Interface: Sessions über eine Telnet-Verbindung
- Command Line Interface: Sessions über eine serielle Verbindung
- Grafische Benutzeroberfläche

Timeout im Command Line Interface für Sessions über eine 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`ssh timeout <0..160>`	Timeout-Zeit in Minuten festlegen für Sessions im Command Line Interface über eine SSH-Verbindung.

Timeout im Command Line Interface für Sessions über eine 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`telnet timeout <0..160>`	Timeout-Zeit in Minuten festlegen für Sessions im Command Line Interface über eine Telnet-Verbindung.

Timeout im Command Line Interface für Sessions über eine serielle Verbindung

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > CLI*, Registerkarte *Global*.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Timeout serielle Schnittstelle [min]* die Timeout-Zeit in Minuten fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`cli serial-timeout <0..160>`	Timeout-Zeit in Minuten festlegen für Sessions im Command Line Interface über eine serielle 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`network management access web timeout <0..160>`	Timeout-Zeit in Minuten festlegen für Sitzungen mit der grafischen Benutzeroberfläche.

8.8 Nicht verwendete Module deaktivieren

Die Voreinstellungen eines Medienmodul-Steckplatzes ermöglichen den Zugriff auf das Netz. Wenn ein Medienmodul in einen leeren Steckplatz eingesetzt wird, bauen die Ports des Medienmoduls in der Voreinstellung Netzverbindungen auf.

Um unbefugten Netzzugriff zu vermeiden, deaktivieren Sie nicht verwendete Steckplätze. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Module*.
- ☐ Um den Steckplatz zu deaktivieren und Zugriffe auf das Netz zu unterbinden, heben Sie die Markierung des Kontrollkästchens *Aktiv* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

9 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 Geräts.

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 Geräts in folgender Reihenfolge:
- DoS … wenn `permit` oder `accept`, dann weiter zur nächsten Regel
- ACL … wenn `permit` oder `accept`, dann weiter zur nächsten Regel

9.1 Unterstützung beim Schutz vor DoS-Attacken

DoS ist ein Cyber-Angriff, der darauf abzielt, den Betrieb bestimmter Dienste oder Geräte zu stören. Sowohl Angreifer als auch Netzwerkadministratoren können mit der Port-Scan-Methode offene Ports in einem Netzwerk aufspüren, um verwundbare Geräte zu finden. Die Funktion unterstützt Sie beim Schutz Ihres Netzes gegen ungültige oder gefälschte Datenpakete, die auf den Ausfall bestimmter Dienste oder Geräte abzielen. Sie haben die Möglichkeit, Filter festzulegen, die den Datenstrom zum Schutz vor DoS-Angriffen begrenzen. Die Filter prüfen die empfangenen Datenpakete. Das Gerät verwirft ein Datenpaket, wenn es den Filterkriterien entspricht.

Zur Unterstützung beim Schutz des Geräts selbst und anderer Geräte im Netz gegen DoS-Attacken ermöglicht Ihnen das Gerät, folgende Filter festzulegen:
- Filter für *TCP- und UDP-Pakete*
- Filter für *IP-Pakete*
- Filter für *ICMP-Pakete*

Die Filter unterstützen dabei, eine angreifende Station daran zu hindern:
- Dienste und Anwendungen zu entdecken, welche die offenen Ports verwenden
- Aktive Geräte in einem Netz zu entdecken
- Auf sensible Daten in einem Netz zuzugreifen
- aktive Security-Geräte zu entdecken, wie eine Firewall, die in einem Netz verwendet wird

Anmerkung: Sie können die Filter in beliebiger Weise kombinieren. Wenn Sie mehrere Filter aktivieren, wendet das Gerät die Filter in der Reihenfolge an, in welcher sie in der IP-Tabelle festgelegt sind. Wenn ein eingehendes Datenpaket einem Filter entspricht, verwirft das Gerät das betreffende Datenpaket und beendet die weitere Verarbeitung.

9.1.1 Filter für TCP- und UDP-Pakete

Um gezielt *TCP*- und *UDP*-Pakete zu bearbeiten, bietet Ihnen das Gerät folgende Filter:
- Funktion Null-Scan-Filter aktivieren
- Funktion Xmas-Filter aktivieren
- Funktion SYN/FIN-Filter aktivieren
- Funktion TCP-Offset-Protection aktivieren
- Funktion TCP-SYN-Protection aktivieren
- Funktion L4-Port-Protection aktivieren
- Funktion Min.-Header-Size-Filter aktivieren

Funktion Null-Scan-Filter aktivieren

Bei der *Null Scan*-Methode sendet die angreifende Station Datenpakete mit den folgenden Eigenschaften:
- Keine *TCP*-Flags sind gesetzt.
- Die *TCP*-Sequenznummer ist 0.

Das Gerät verwendet die Funktion *Null-Scan-Filter*, um *TCP*-Datenpakete zu verwerfen, die bösartige Eigenschaften enthalten.

In der Voreinstellung ist die Funktion *Null-Scan-Filter* ausgeschaltet. Um die Funktion *Null-Scan-Filter* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *Null-Scan-Filter*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *Null-Scan-Filter*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos tcp-null`	Funktion *Null-Scan-Filter* aktivieren.
`no dos tcp-null`	Funktion *Null-Scan-Filter* deaktivieren.

Funktion Xmas-Filter aktivieren

Bei der *Xmas*-Methode sendet die angreifende Station Datenpakete mit den folgenden Eigenschaften:
- Die *TCP*-Flags *FIN*, *URG* und *PSH* sind gleichzeitig gesetzt.
- Die *TCP*-Sequenznummer ist 0.

Das Gerät verwendet die Funktion *Xmas-Filter*, um *TCP*-Datenpakete zu verwerfen, die bösartige Eigenschaften enthalten.

In der Voreinstellung ist die Funktion *Xmas-Filter* ausgeschaltet. Um die Funktion *Xmas-Filter* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *Xmas-Filter*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *Xmas-Filter*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos tcp-xmas`	Funktion *Xmas-Filter* aktivieren.
`no dos tcp-xmas`	Funktion *Xmas-Filter* deaktivieren.

Funktion SYN/FIN-Filter aktivieren

Bei der *SYN/FIN*-Methode sendet die angreifende Station Datenpakete, bei denen die *TCP*-Flags *SYN* und *FIN* gleichzeitig gesetzt sind. Das Gerät verwendet die Funktion *SYN/FIN-Filter*, um empfangene Datenpakete zu verwerfen, in denen die *TCP*-Flags *SYN* und *FIN* gleichzeitig gesetzt sind.

In der Voreinstellung ist die Funktion *SYN/FIN-Filter* ausgeschaltet. Um die Funktion *SYN/FIN-Filter* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *SYN/FIN-Filter*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *SYN/FIN-Filter*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos tcp-syn-fin`	Funktion *SYN/FIN-Filter* aktivieren.
`no dos tcp-syn-fin`	Funktion *SYN/FIN-Filter* deaktivieren.

Funktion TCP-Offset-Protection aktivieren

Bei der *TCP Offset*-Methode sendet die angreifende Station Datenpakete, deren Fragment-Offset gleich `1` ist. Der Fragment-Offset ist ein Feld im *IP*-Header, das dabei hilft, die Reihenfolge von Fragmenten in empfangenen Datenpaketen zu identifizieren. Das Gerät verwendet die Funktion *TCP-Offset-Protection*, um eingehende *TCP*-Datenpakete zu verwerfen, deren Fragment-Offset-Feld im *IP*-Header gleich `1` ist.

Anmerkung: Das Gerät akzeptiert *UDP*- und *ICMP*-Pakete, bei denen das Fragment-Offset-Feld im *IP*-Header gleich `1` ist.

In der Voreinstellung ist die Funktion *TCP-Offset-Protection* ausgeschaltet. Um die Funktion *TCP-Offset-Protection* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *TCP-Offset-Protection*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *TCP-Offset-Protection*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos tcp-offset`	Funktion *TCP-Offset-Protection* aktivieren.
`no dos tcp-offset`	Funktion *TCP-Offset-Protection* deaktivieren.

Funktion TCP-SYN-Protection aktivieren

Bei der *TCP SYN*-Methode sendet die angreifende Station Datenpakete, in denen das *TCP*-Flag *SYN* gesetzt ist und bei denen der L4- (Layer 4-) Quell-Port <1024 ist. Das Gerät verwendet die Funktion *TCP-SYN-Protection*, um eingehende Datenpakete zu verwerfen, in denen das *TCP*-Flag *SYN* gesetzt ist und bei denen der L4- (Layer 4-) Quell-Port <1024 ist.

In der Voreinstellung ist die Funktion *TCP-SYN-Protection* ausgeschaltet. Um die Funktion *TCP-SYN-Protection* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *TCP-SYN-Protection*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *TCP-SYN-Protection*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos tcp-syn`	Funktion *TCP-SYN-Protection* aktivieren.
`no dos tcp-syn`	Funktion *TCP-SYN-Protection* deaktivieren.

Funktion L4-Port-Protection aktivieren

Eine angreifende Station kann *TCP*- oder *UDP*-Datenpakete senden, bei denen Quell- und Ziel-Port-Nummer identisch sind. Das Gerät verwendet die Funktion *L4-Port-Protection*, um eingehende *TCP*- und *UDP*-Pakete zu verwerfen, bei denen L4-Quell- und Ziel-Port-Nummer identisch sind.

In der Voreinstellung ist die Funktion *L4-Port-Protection* ausgeschaltet. Um die Funktion *L4-Port-Protection* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *L4-Port-Protection*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *L4-Port-Protection*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos l4-port`	Funktion *L4-Port-Protection* aktivieren.
`no dos l4-port`	Funktion *L4-Port-Protection* deaktivieren.

Funktion Min.-Header-Size-Filter aktivieren

Die Funktion *Min.-Header-Size-Filter* erkennt empfangene Datenpakete mit den folgenden Eigenschaften:

(*IP*-Nutzlastlänge im *IP*-Header - äußere *IP*-Header-Größe) < minimale *TCP*-Header-Größe.

Falls es sich bei dem empfangenen Paket um das erste Fragment handelt, welches das Gerät erkennt, dann verwirft das Gerät das Datenpaket.

In der Voreinstellung ist die Funktion *Min.-Header-Size-Filter* ausgeschaltet. Um die Funktion *Min.-Header-Size-Filter* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *Min.-Header-Size-Filter*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *Min.-Header-Size-Filter*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos tcp-min-header`	Funktion *Min.-Header-Size-Filter* aktivieren.
`no dos tcp-min-header`	Funktion *Min.-Header-Size-Filter* deaktivieren.

9.1.2 Filter für IP-Pakete

Um gezielt *IP*-Pakete zu bearbeiten, bietet Ihnen das Gerät folgende Filter:
- Funktion Land-Attack-Filter aktivieren

Funktion Land-Attack-Filter aktivieren

Bei der *Land Attack*-Methode sendet die angreifende Station Datenpakete, deren Quell- und Ziel-adressen identisch mit der *IP*-Adresse des Empfängers sind. Das Gerät verwendet die Funktion *Land-Attack-Filter*, um empfangene Pakete zu verwerfen, deren Quell- und Ziel-Adresse identisch sind.

In der Voreinstellung ist die Funktion *Land-Attack-Filter* ausgeschaltet. Um die Funktion *Land-Attack-Filter* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *Land-Attack-Filter*. Markieren Sie dazu im Rahmen *IP* das Kontrollkästchen *Land-Attack-Filter*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos ip-land enable`	Funktion *Land-Attack-Filter* aktivieren.
`no dos ip-land disable`	Funktion *Land-Attack-Filter* deaktivieren.

9.1.3 Filter für ICMP-Pakete

Um gezielt *ICMP*-Pakete zu bearbeiten, bietet Ihnen das Gerät folgende Filter:
- Funktion Fragmentierte Pakete filtern aktivieren
- Funktion Anhand Paket-Größe verwerfen aktivieren
- Funktion Broadcast-Ping verwerfen aktivieren

Funktion Fragmentierte Pakete filtern aktivieren

Das Gerät verwendet die Funktion *Fragmentierte Pakete filtern*, um das Netzwerk vor angreifenden Stationen zu schützen, die fragmentierte *ICMP*-Pakete senden. Fragmentierte *ICMP*-Pakete können eine Fehlfunktion des Zielgeräts verursachen, wenn das Zielgerät die fragmentierten *ICMP*-Pakete falsch verarbeitet. Das Gerät verwendet die Funktion *Fragmentierte Pakete filtern*, um fragmentierte *ICMP*-Pakete zu verwerfen.

In der Voreinstellung ist die Funktion *Fragmentierte Pakete filtern* ausgeschaltet. Um die Funktion *Fragmentierte Pakete filtern* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *Fragmentierte Pakete filtern*. Markieren Sie dazu im Rahmen *ICMP* das Kontrollkästchen *Fragmentierte Pakete filtern*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos icmp-fragmented`	Funktion *Fragmentierte Pakete filtern* aktivieren.
`no dos icmp-fragmented`	Funktion *Fragmentierte Pakete filtern* deaktivieren.

Funktion Anhand Paket-Größe verwerfen aktivieren

Das Gerät verwendet die Funktion *Anhand Paket-Größe verwerfen*, um Datenpakete zu verwerfen, deren Nutzlastgröße die im Feld *Erlaubte Payload-Größe [Byte]* festgelegte Größe überschreitet.

Die Funktion *Anhand Paket-Größe verwerfen* hilft dabei, das Netz vor angreifenden Stationen zu schützen, die *ICMP*-Pakete senden, deren Nutzlastgröße die im Feld *Erlaubte Payload-Größe [Byte]* festgelegte Größe überschreitet.

In der Voreinstellung ist die Funktion *Anhand Paket-Größe verwerfen* ausgeschaltet. Um die Funktion *Anhand Paket-Größe verwerfen* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *Anhand Paket-Größe verwerfen*. Markieren Sie dazu im Rahmen *ICMP* das Kontrollkästchen *Anhand Paket-Größe verwerfen*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos icmp payload-check`	Funktion *Anhand Paket-Größe verwerfen* aktivieren.
`no dos icmp payload-check`	Funktion *Anhand Paket-Größe verwerfen* deaktivieren.

Funktion Broadcast-Ping verwerfen aktivieren

Die Funktion *Broadcast-Ping verwerfen* hilft beim Schutz des Netzes vor Broadcast-Ping-Attacken, auch bekannt als ICMP Smurf-Attacken. Bei der Broadcast-Ping-Methode flutet der Angreifer ein Zielgerät (das Opfer), indem er eine große Anzahl von ICMP Echo request- (Ping-) Paketen an die IPv4-Broadcast-Adresse sendet. Diese Pakete enthalten eine gefälschte IP-Quelladresse, welche die IP-Adresse des Opfers ist. Stationen, die auf den Broadcast-Ping reagieren, senden ihre Antworten an das Opfer, fluten das Opfer dadurch und verursachen möglicherweise Instabilität.

Das Gerät verwendet die Funktion *Broadcast-Ping verwerfen*, um Broadcast-Pings zu verwerfen.

In der Voreinstellung ist die Funktion *Broadcast-Ping verwerfen* ausgeschaltet. Um die Funktion *Broadcast-Ping verwerfen* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *Broadcast-Ping verwerfen*. Markieren Sie dazu im Rahmen *ICMP* das Kontrollkästchen *Broadcast-Ping verwerfen*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dos icmp-smurf-attack`	Funktion *Broadcast-Ping verwerfen* aktivieren.
`no dos icmp-smurf-attack`	Funktion *Broadcast-Ping verwerfen* deaktivieren.

9.2 ACL

In diesem Menü haben Sie die Möglichkeit, die Parameter für die Access-Control-Listen (ACL) einzufügen.

Das Gerät verwendet ACLs, um Datenpakete zu filtern, die es in VLANs oder auf einzelnen oder mehreren Ports empfängt. In einer ACL legen Sie Regeln fest, anhand derer das Gerät Datenpakete filtert. Wenn eine solche Regel auf ein Paket zutrifft, wendet das Gerät die in der Regel festgelegten Aktionen auf das Paket an. Die folgenden Aktionen sind verfügbar:

- zulassen (`permit`)
- verwerfen (`deny`)
- umleiten an einen bestimmten Port (siehe Feld *Redirection-Port*)
- spiegeln (siehe Feld *Mirror-Port*)

Die folgende Liste enthält Kriterien, anhand derer Sie die Datenpakete filtern können:

- Quell- oder Zieladresse eines Pakets (MAC)
- Quell- oder Zieladresse eines Datenpakets (IPv4)
- Typ des übertragenden Protokolls (MAC/IPv4)
- Quell- oder Ziel-Port eines Datenpakets (IPv4)
- Serviceklasse eines Pakets (MAC)
- Zugehörigkeit zu einem bestimmten VLAN (MAC)
- DSCP-Klassifizierung (IPv4)
- ToS-Klassifizierung (IPv4)
- Paket-Fragmentierung (IPv4)

Folgende ACL-Typen können Sie festlegen:

- IP-ACLs für VLANs
- IP-ACLs für Ports
- MAC-ACLs für VLANs
- MAC-ACLs für Ports

Wenn Sie einem Interface eine IP-ACL und eine MAC-ACL zuweisen, wendet das Gerät zuerst die IP-ACL an, um den Datenstrom zu filtern. Nachdem die Pakete durch die IP-ACL gefiltert sind, wendet das Gerät die MAC-ACL-Regeln an. Die Priorität einer ACL und der Index einer Regel sind voneinander unabhängig.

Innerhalb einer ACL verarbeitet das Gerät die Regeln der Reihe nach. Der Index der jeweiligen Regel bestimmt die Reihenfolge, in welcher das Gerät den Datenstrom filtert. Wenn Sie einem Port oder VLAN eine ACL zuweisen, können Sie deren Priorität mit der Index-Nummer festlegen. Je kleiner die Zahl, desto höher die Priorität. Das Gerät verarbeitet zuerst die Regel mit höherer Priorität.

Wenn keine der in einer ACL festgelegten Regeln auf ein Datenpaket zutrifft, gilt die implizite `deny`-Regel. Infolgedessen verwirft das Gerät empfangene Datenpakete.

Beachten Sie, dass das Gerät die implizite `deny`-Regel direkt implementiert.

Anmerkung: Die Anzahl der verfügbaren ACLs ist geräteabhängig. Weitere Informationen zu den Werten der ACLs finden Sie im Kapitel „Technische Daten” auf Seite 408.

Anmerkung: Eine einzelne ACL können Sie beliebig vielen Port oder VLANs zuweisen.

Anmerkung: Wenn Sie für eine Regel die Funktion *Paket fragmentiert* aktivieren, dann verarbeitet die Regel IPv4-Fragmente, deren Offset ungleich Null ist. Die Regel verarbeitet jedes IPv4-Fragment, mit Ausnahme des initialen IPv4-Fragments.

Das Menü *ACL* enthält die folgenden Dialoge:
- *ACL IPv4-Regel*
- *ACL MAC-Regel*
- *ACL Zuweisung*

Diese Dialoge bieten folgende Möglichkeiten:
- Die Regeln für die einzelnen ACL-Typen festlegen.
- Die Regeln mit den erforderlichen Prioritäten versehen.
- Die ACLs den Ports oder VLANs zuweisen.

9.2.1 Erzeugen und Bearbeiten von IPv4-Regeln

Beim Filtern von IPv4-Datenpaketen ermöglicht Ihnen das Gerät:
- 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

Anmerkung: Sie können IP-ACL-Regeln und DiffServ-Regeln für die gleiche Richtung nicht gleichzeitig auf einen Port anwenden.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > ACL > IPv4-Regel*.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Legen Sie den Namen der ACL (Gruppe) fest.
  - ☐ Um die Regel in einer bestehenden ACL zu erzeugen, klicken Sie das Feld *Gruppenname* und wählen in der Dropdown-Liste den Namen aus.
  - ☐ Um die Regel in einer neuen ACL zu erzeugen, legen Sie im Feld *Gruppenname* einen aussagekräftigen Namen fest und klicken das Symbol + .
- ☐ Im Feld *Index* legen Sie die Nummer der Regel innerhalb der ACL fest.
  Diese Nummer bestimmt die Priorität der Regel.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Gerät fügt die Regel der ACL (Gruppe) in der Tabelle hinzu.
  Die Regel ist sofort aktiv.
  - ☐ Um eine Regel zu entfernen, markieren Sie in der Tabelle die gewünschte Zeile und klicken die Schaltfläche .
- ☐ Bearbeiten Sie die Parameter der Regel in der Tabelle. Um einen Wert zu ändern, doppelklicken Sie in das betreffende Feld.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓ .

Anmerkung: Das Gerät ermöglicht Ihnen, in den Parametern *Quell-IP-Adresse* und *Ziel-IP-Adresse* Platzhalter zu verwenden. Wenn Sie zum Beispiel `192.168.?.?` einfügen, lässt das Gerät Adressen zu, die mit `192.168` beginnen.

Anmerkung: Voraussetzung für das 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 für das Ändern des Werts in Spalte *Redirection-Port* und *Mirror-Port* ist, dass Sie in Spalte *Aktion* den Wert `permit` festlegen.

9.2.2 Erzeugen und Konfigurieren einer IP-ACL im Command Line Interface

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.

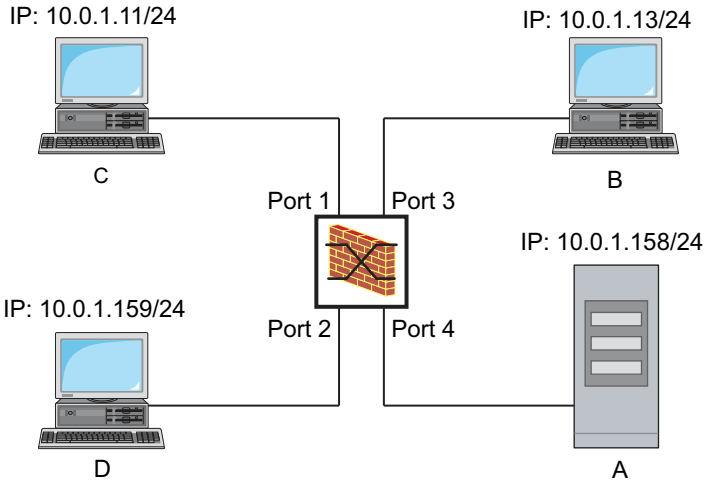


Abb. 22: Beispiel einer IP-ACL

Führen Sie die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	IP-ACL mit dem Namen `filter1` einfügen. Regel hinzufügen, die IP-Datenpakete von `10.0.1.11` bis `10.0.1.158` ablehnt. Priorität `1` (höchste Priorität).
`ip access-list extended name filter1 permit src any dst any`	Der IP-ACL eine Regel hinzufügen, die IP-Datenpakete erlaubt.
`show access-list ip filter1`	Regeln der IP-ACL `filter1` anzeigen.
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	IP-ACL mit dem Namen `filter2` einfügen. Regel hinzufügen, die IP-Datenpakete von `10.0.1.13` bis `10.0.1.158` ablehnt. Priorität `1` (höchste Priorität).
`show access-list ip filter2`	Regeln der IP-ACL `filter2` anzeigen.

9.2.3 Erzeugen und Bearbeiten von MAC-Regeln

Beim Filtern von MAC-Datenpaketen ermöglicht Ihnen das Gerät:
- 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*.
- ☐ Legen Sie den Namen der ACL (Gruppe) fest.
  - ☐ Um die Regel in einer bestehenden ACL zu erzeugen, klicken Sie das Feld *Gruppenname* und wählen in der Dropdown-Liste den Namen aus.
  - ☐ Um die Regel in einer neuen ACL zu erzeugen, legen Sie im Feld *Gruppenname* einen aussagekräftigen Namen fest und klicken das Symbol + .
- ☐ Im Feld *Index* legen Sie die Nummer der Regel innerhalb der ACL fest.
  Diese Nummer bestimmt die Priorität der Regel.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Gerät fügt die Regel der ACL (Gruppe) in der Tabelle hinzu.
  Die Regel ist sofort aktiv.
  - ☐ Um eine Regel zu entfernen, markieren Sie in der Tabelle die gewünschte Zeile und klicken die Schaltfläche .
- ☐ Bearbeiten Sie die Parameter der Regel in der Tabelle. Um einen Wert zu ändern, doppelklicken Sie in das betreffende Feld.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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.

9.2.4 Erzeugen und Konfigurieren einer MAC-ACL im Command Line Interface

Das Beispiel sieht vor, dass AppleTalk und IPX aus dem gesamten Netz gefiltert werden. Führen Sie dazu die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`mac acl add 1 macfilter`	MAC-ACL mit ID `1` und dem Namen `macfilter` einfügen.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	Regel an Position `1` in der MAC-ACL mit ID `1` einfügen, die Pakete mit Ethertype `0x809B (AppleTalk)` abweist.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	Regel an Position `2` in der MAC-ACL mit ID `1` einfügen, die Pakete mit Ethertype `0x8137 (IPX alt)` abweist.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	Regel an Position `3` in der MAC-ACL mit ID `1` einfügen, die Pakete mit Ethertype `0x8138 (IPX)` abweist.
`mac acl rule add 1 4 permit src any any dst any any`	Regel an Position `4` in der MAC-ACL mit ID `1` einfügen, die Pakete weiterleitet.

`show acl mac rules 1`	Regeln der MAC-ACL mit ID `1` anzeigen.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	In den Interface-Konfigurationsmodus der Interfaces `1/1` bis `1/6` wechseln.
`acl mac assign 1 in 1`	MAC-ACL mit ID `1` den auf den Interfaces `1/1` bis `1/6` empfangenen Datenpaketen (`in`) zuweisen.
`exit`	Interface-Modus verlassen.
`show acl mac assignment 1`	Zuweisung von Interfaces oder VLANS der MAC-ACL mit ID `1` anzeigen.

9.2.5 Zuweisen von ACLs zu Ports oder VLANs

Wenn Sie ACLs einem Port oder VLAN zuweisen, bietet das Gerät die folgenden Möglichkeiten:

- Den Port oder das VLAN festlegen.
- Die ACL-Priorität festlegen.
- Die Richtung festlegen.
- Die ACL anhand des Gruppennamens auswählen.

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 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

9.3 MAC-Authentication-Bypass

Die Funktion *MAC-Authorized-Bypass* ermöglicht Clients, die 802.1X nicht unterstützen, zum Beispiel Drucker und Faxgeräte, sich mit ihrer MAC-Adresse im Netz zu authentifizieren. Das Gerät ermöglicht Ihnen, das Format der MAC-Adressen festzulegen, mit der sich die Clients beim RADIUS-Server authentifizieren.

Beispiel:

Unterteilen Sie die MAC-Adresse in 6 Gruppen mit je 2 Zeichen. Verwenden Sie Großbuchstaben und einen Doppelpunkt als Trennzeichen: `AA:BB:CC:DD:EE:FF`

Verwenden Sie das Passwort `xY-45uM_e`. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Global*.
  Führen Sie im Rahmen *Formatoptionen MAC Authentication Bypass* die folgenden Schritte aus:
- ☐ Wählen Sie in der Dropdown-Liste *Gruppen-Größe* den Wert `2`.
  Das Gerät unterteilt die MAC-Adresse in 6 Gruppen mit je 2 Zeichen.
- ☐ Wählen Sie in der Dropdown-Liste *Gruppen-Trennzeichen* das Zeichen `:`.
- ☐ Wählen Sie in der Dropdown-Liste *Groß-/Kleinschreibung* den Eintrag `upper-case`.
- ☐ Geben Sie im Feld *Passwort* das Passwort `xY-45uM_e` ein.
  Das Gerät verwendet dieses Passwort für jeden Client, der sich beim RADIUS-Server authentifiziert. Wenn Sie das Feld leer lassen, dann verwendet das Gerät die formatierte MAC-Adresse auch als Passwort.
- ☐ Um die Einstellungen flüchtig zu speichern, klicken Sie die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dot1x mac-authentication-bypass format group-size 2`	Festlegen, dass die Gruppen jeweils `2` Zeichen enthalten.
`dot1x mac-authentication-bypass format group-separator :`	Das Trennzeichen `:` festlegen.
`dot1x mac-authentication-bypass format letter-case upper-case`	Festlegen, dass das Gerät die Authentifizierungsdaten in Großbuchstaben formatiert.
`dot1x mac-authentication-bypass password xY-45uM_e`	Das Passwort `xY-45uM_e` festlegen. Das Gerät verwendet dieses Passwort, um jeden Client auf dem RADIUS-Server zu authentifizieren.

10 Netzlaststeuerung

Das Gerät bietet Ihnen eine Reihe von Funktionen, die Ihnen helfen können, die Netzlast zu reduzieren:

- Gezielte Paketvermittlung
- Multicasts
- Lastbegrenzung
- Priorisierung - QoS
- Differentiated Services
- 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 jeden Port 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 Geräts.

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 oder im Command Line Interface.

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 festgelegten Ziel-MAC-Adresse im festgelegten 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`mac-filter <MAC address> <VLAN ID>`	MAC-Adressfilter erzeugen, bestehend aus MAC-Adresse und VLAN-ID.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`mac-filter <MAC address> <VLAN ID>`	Dem Port einen bereits erzeugten MAC-Adressfilter zuweisen.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

☐ 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`.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

☐ Statischen Adresseintrag deaktivieren.

☐ Öffnen Sie den Dialog *Switching > Filter für MAC-Adressen*.

☐ Um einen statischen Adresseintrag zu deaktivieren, entfernen Sie ihn aus der Tabelle. Markieren Sie dazu die Zeile mit dem Wert `permanent` in Spalte *Status* und klicken die Schaltfläche ✕.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`no mac-filter <MAC address> <VLAN ID>`	Auf dem Port die Zuweisung des MAC-Adressfilters aufheben.
`exit`	In den Konfigurationsmodus wechseln.
`no mac-filter <MAC address> <VLAN ID>`	MAC-Adressfilter löschen, bestehend aus MAC-Adresse und VLAN-ID.
`exit`	In den Privileged-EXEC-Modus wechseln.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

☐ Gelernte MAC-Adressen löschen.

☐ Um die gelernten Adressen aus der MAC-Adresstabelle (FDB) zu löschen, klicken Sie die Schaltfläche 🗑 .
Alternativ öffnen Sie den Dialog *Grundeinstellungen > Neustart* und klicken die Schaltfläche *MAC-Adresstabelle zurücksetzen*.

`clear mac-addr-table`	Die gelernten MAC-Adressen aus der MAC-Adresstabelle (FDB) löschen.

10.2 Multicasts

In der Grundeinstellung flutet das Gerät Datenpakete mit einer Multicast-Adresse, d.h. das Gerät leitet diese Datenpakete an jeden Port 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 Funktion *IGMP-Snooping* im Gerät funktioniert gemäß RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Multicast-Router mit aktiver Funktion *IGMP* 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 Funktion *IGMP* 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.

Wenn mehrere IGMP-Multicast-Router im selben Netz sind, übernimmt das Gerät mit der kleineren IP-Adresse die Query-Funktion. Wenn sich kein Multicast-Router im Netz befindet, haben Sie die Möglichkeit, die Query-Funktion in einem 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 Funktion *IGMP* 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 jeden Port. 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 `An`.

Wenn die Funktion *IGMP-Snooping* ausgeschaltet ist, dann verhält sich das Gerät wie folgt:
- ▶ Das Gerät ignoriert die empfangenen Query- und Report-Nachrichten.
- ▶ Das Gerät vermittelt (flutet) empfangene Datenpakete mit einer Multicast-Adresse als Zieladresse an jeden Port.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

☐ Einstellungen für einen Port festlegen:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Konfiguration*, Registerkarte *Port*.
- ☐ Um die Funktion *IGMP-Snooping* auf einem Port zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv* für den betreffenden Port.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

☐ Einstellungen für ein VLAN festlegen.

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Konfiguration*, Registerkarte *VLAN-ID*.
- ☐ Um die Funktion *IGMP-Snooping* für ein bestimmtes VLAN zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv* für das betreffende VLAN.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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 (Funktion *IGMP Snooping-Querier*).

Voraussetzung:

Die Funktion *IGMP-Snooping* ist global eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Querier*.
- ☐ Im Rahmen *Funktion* schalten Sie die Funktion *IGMP Snooping-Querier* des Geräts global ein oder aus.
- ☐ Um die Funktion *IGMP Snooping-Querier* 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-Quelladresse des anderen Multicast-Queriers niedriger ist als die eigene, 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

IGMP-Snooping-Erweiterungen (Tabelle)

Der Dialog *Switching > IGMP-Snooping > Snooping Erweiterungen* gibt Ihnen Zugriff auf erweiterte Einstellungen für die Funktion *IGMP-Snooping*. 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 einen 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“).
- ▶ `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 Funktion *IGMP Snooping-Querier* entsprechend. Der Eintrag `ALA` zeigt, dass die Funktion `Learn by LLDP` 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 vermittelt das Gerät an diesen 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 dem Umschalten des Rings ermöglicht die Funktion `Forward All`, das Netz für Datenpakete mit registrierten Multicast-Zieladressen zügig neu zu konfigurieren. Aktivieren Sie die Funktion `Forward All` auf jedem Ring-Port.

Voraussetzung:

Die Funktion *IGMP-Snooping* 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`igmp-snooping vlan-id 1 forward-all 1/1`	Funktion `Forward All` für Port `1/1` in VLAN `1` aktivieren.

Multicasts konfigurieren

Das Gerät ermöglicht Ihnen, 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 leitet unbekannte Multicasts an jeden Port weiter.
- Das Gerät vermittelt unbekannte Multicasts an die Ports, 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 vermittelt bekannte Multicasts an die Ports, 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 hilft sicherzustellen, dass die Übermittlung bei grundlegenden Anwendungen ohne weitere Konfiguration funktioniert.
- Das Gerät vermittelt bekannte Multicasts ausschließlich an die registrierten Ports. Diese Einstellung hat den Vorteil, die verfügbare Bandbreite durch gezielte Vermittlung optimal zu nutzen.

Voraussetzung:

Die Funktion *IGMP-Snooping* 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.
- ☐ In der Tabelle legen Sie fest, wie das Gerät Datenpakete an bekannte Multicast-Adressen vermittelt.
  - ▶ `an Query- und registrierte Ports senden`
    Das Gerät vermittelt Datenpakete mit einer bekannten MAC-/IP-Multicast-Adresse an die Query-Ports und an registrierte Ports.
  - ▶ `an registrierte Ports senden`
    Das Gerät vermittelt Datenpakete mit einer bekannten MAC-/IP-Multicast-Adresse an registrierte Ports.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

10.3 Lastbegrenzung

Die Lastbegrenzer-Funktion sorgt auch bei hohem Verkehrsaufkommen für einen stabilen Betrieb, indem sie den Verkehr auf den Ports begrenzt. Die Lastbegrenzung erfolgt individuell für jeden Port sowie separat für Eingangs- und Ausgangsdatenverkehr.

Wenn die Datenrate an einem Port den definierten Grenzwert überschreitet, 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 geräteinterne 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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 ermöglicht Ihnen, Daten der wichtigsten Anwendungen zu priorisieren.

Die Priorisierung vermeidet 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* ist abhängig vom Gerätetyp.

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.

Verkehrsklassen priorisieren

Zur Priorisierung von *Verkehrsklassen* verwendet das Gerät folgende Methoden:

- *Strict Priority*
  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 Priority* priorisiert ist, blockiert das Gerät bei hoher Netzlast die Daten niedrigerer *Verkehrsklassen* möglicherweise permanent.
- *Weighted Fair Queuing*
  Die *Verkehrsklasse* erhält eine spezifische Bandbreite zugewiesen. Dies hilft sicherzustellen, dass das Gerät die Daten dieser *Verkehrsklasse* sendet, 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“).

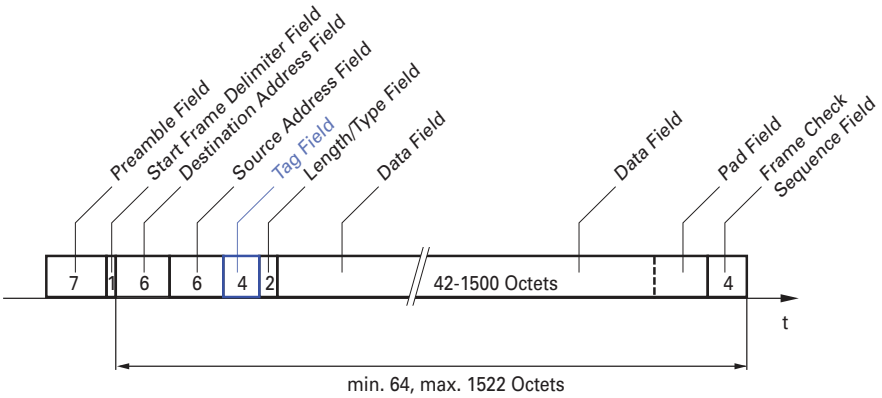


Abb. 23: Ethernet-Datenpaket mit Tag

Das Gerät wertet bei Datenpaketen mit VLAN-Tags folgende Informationen aus:
- Prioritätsinformation
- VLAN-Tag, sofern VLANs eingerichtet sind

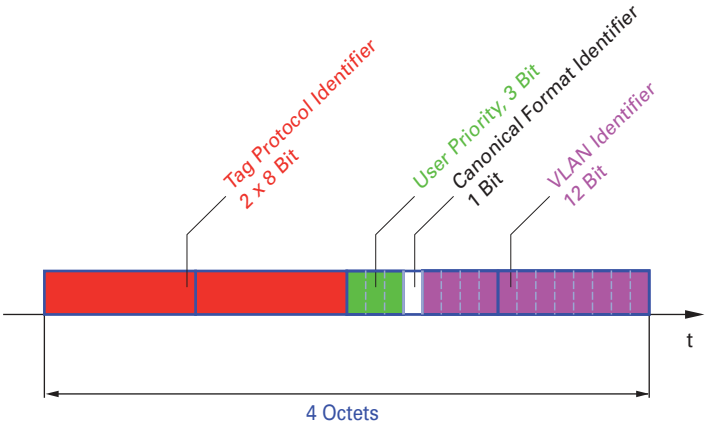


Abb. 24: Aufbau des VLAN-Tag

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.

Tab. 18: ToS-Feld im IP-Header

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - 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		

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 keine Pakete mit niedriger Priorität, 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, weisen Sie jeder *Verkehrsklasse* eine minimale oder reservierte Bandbreite zu. Dies hilft sicherzustellen, 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

Vergewissern Sie sich beim Kombinieren von *Weighted Fair Queuing* mit *Strict Priority*, 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

Queue Shaping

Queue Shaping drosselt die Geschwindigkeit, mit der Warteschlangen Pakete vermitteln. Mit Queue Shaping beschränken Sie zum Beispiel die Geschwindigkeit für eine Warteschlange mit höherer Priorität und ermöglichen so einer Warteschlange mit niedrigerer Priorität Pakete zu senden, obwohl noch höherpriore Pakete auf die Vermittlung warten. Das Gerät ermöglicht Ihnen, Queue Shaping für jede Warteschlange einzurichten. Sie legen Queue Shaping fest als die maximale Geschwindigkeit, mit der Daten die Warteschlange passieren, indem Sie einen prozentualen Anteil der verfügbaren Bandbreite zuweisen.

Einstellungen für das Queue-Management festlegen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > 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 *Weighted Fair Queuing* für *Traffic-Klasse* = `3` 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 *Weighted Fair Queuing* und Queue Shaping für *Traffic-Klasse* = `4` zu kombinieren, 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.
  - ▶ Legen Sie in Spalte *Max. Bandbreite [%]* den Wert `10` fest.

  Wenn Sie *Weighted Fair Queuing* und Queue Shaping kombiniert für eine bestimmte *Verkehrsklasse* verwenden, legen Sie in Spalte *Max. Bandbreite [%]* einen Wert fest, der größer ist als der Wert in Spalte *Min. Bandbreite [%]*.

- Um das *Weighted Fair Queuing* für *Traffic-Klasse* = 5 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* = 6 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 *Strict Priority* und Queue Shaping für *Traffic-Klasse* = 7 zu kombinieren, gehen Sie wie folgt vor:
  - Markieren Sie das Kontrollkästchen in Spalte *Strict priority*.
  - Legen Sie in Spalte *Max. Bandbreite [%]* den Wert 10 fest.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`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.
`cos-queue weighted 3`	*Weighted Fair Queuing* für die *Verkehrsklasse* 3 einschalten.
`cos-queue min-bandwidth: 3 20`	Gewichtung 20 % der *Verkehrsklasse* 3 zuweisen.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

Weighted Fair Queuing und Queue Shaping kombinieren

Führen Sie die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`cos-queue weighted 4`	*Weighted Fair Queuing* für die *Verkehrsklasse* 4 einschalten.
`cos-queue min-bandwidth: 4 10`	Gewichtung 10 % der *Verkehrsklasse* 4 zuweisen.
`cos-queue max-bandwidth: 4 10`	Gewichtung 10 % der *Verkehrsklasse* 4 zuweisen.

`cos-queue weighted 5`	*Weighted Fair Queuing* für die *Verkehrsklasse* 5 einschalten.
`cos-queue min-bandwidth: 5 5`	Gewichtung 5 % der *Verkehrsklasse* 5 zuweisen.
`cos-queue weighted 6`	*Weighted Fair Queuing* für die *Verkehrsklasse* 6 einschalten.
`cos-queue min-bandwidth: 6 10`	Gewichtung 10 % der *Verkehrsklasse* 6 zuweisen.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Queue Shaping einrichten

Führen Sie die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`cos-queue max-bandwidth: 7 10`	Gewichtung 10 % der *Verkehrsklasse* 7 zuweisen.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

10.4.7 Management-Priorisierung

Das Gerät ermöglicht Ihnen, die Management-Pakete zu priorisieren, damit Sie in Situationen mit hoher Netzlast jederzeit Zugriff auf das Management des Geräts haben.

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.
  Voraussetzung für diese Funktion ist, dass die entsprechenden Ports so eingestellt sind, dass sie das Senden von Paketen mit VLAN-Tag erlauben.
- 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/Priority > 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`vlan priority 3`	Interface `1/1` die Port-Priorität `3` zuweisen.
`exit`	In den Konfigurationsmodus wechseln.

VLAN-Priorität einer Verkehrsklasse zuweisen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung*.
- ☐ Um einer VLAN-Priorität eine *Verkehrsklasse* zuzuweisen, fügen Sie in Spalte *Traffic-Klasse* den betreffenden Wert ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`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`	In den Privileged-EXEC-Modus wechseln.
`show classofservice dot1p-mapping`	Zuordnung anzeigen.

Empfangenen Datenpaketen die Port-Priorität zuweisen

Führen Sie die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`classofservice trust untrusted`	Dem Interface den Modus `untrusted` zuweisen.
`classofservice dot1p-mapping 0 2` `classofservice dot1p-mapping 1 2`	Der VLAN-Priorität `0` die *Verkehrsklasse* `2` zuweisen. Der VLAN-Priorität `1` die *Verkehrsklasse* `2` zuweisen.
`vlan priority 1`	Für die Port-Priorität den Wert `1` festlegen.
`exit`	In den Konfigurationsmodus wechseln.
`exit`	In den Privileged-EXEC-Modus wechseln.
`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/Priority > IP-DSCP-Zuweisung*.
- ☐ Legen Sie in Spalte *Traffic-Klasse* den gewünschten Wert fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`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`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`classofservice trust ip-dscp`	Den Modus `trust ip-dscp` global zuweisen.
`exit`	In den Konfigurationsmodus wechseln.
`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
 .             .
```

Traffic Shaping auf einem Port konfigurieren

Führen Sie die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/2`	In den Interface-Konfigurationsmodus von Interface `1/2` wechseln.
`traffic-shape bw 50`	Maximale Bandbreite des Ports `1/2` auf 50% begrenzen.
`exit`	In den Konfigurationsmodus wechseln.
`exit`	In den Privileged-EXEC-Modus wechseln.
`show traffic-shape`	Traffic-Shaping-Konfiguration anzeigen.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

Management-Priorität Schicht 2 konfigurieren

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > Global*.
- ☐ Legen Sie im Feld *VLAN-Priorität für Management-Pakete* die VLAN-Priorität fest, mit der das Gerät Management-Datenpakete sendet.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`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/Priority > Global*.
- ☐ Legen Sie im Feld *IP-DSCP-Wert für Management-Pakete* den DSCP-Wert fest, mit dem das Gerät Management-Datenpakete sendet.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`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 Differentiated Services

RFC 2474 definiert das Feld „Differentiated Services“ im IP-Header. Dieses Feld bezeichnet man auch als „DiffServ Codepoint“ oder DSCP. Das DSCP-Feld dient der Einteilung der Pakete in unterschiedliche Qualitätsklassen.

Das DSCP-Feld löst das ToS-Feld ab. Die ersten 3 Bits des DSCP-Felds dienen der Einteilung in Klassen. Die nachfolgenden 3 Bits dienen der weiteren Unterteilung der Klassen nach unterschiedlichen Kriterien. Daraus ergeben sich bis zu 64 unterschiedliche Dienstgüteklassen.

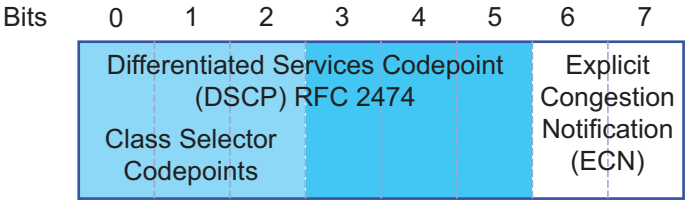


Abb. 25: Differentiated-Services-Feld im IP-Header

Die unterschiedlichen DSCP-Werte bewirken bei dem Gerät ein unterschiedliches Weiterleitungsverhalten, das sog. „Per Hop Behavior“ (PHB). Folgende PHB-Klassen sind definiert:

- Class Selector (CS0–CS7)
  Aus Gründen der Abwärtskompatibilität weist das Class Selector PHB die 7 möglichen IP-Präzedenzwerte aus dem bisherigen ToS-Feld bestimmten DSCP-Werten zu.
- Expedited Forwarding (EF)
  Für Anwendungen mit hoher Priorität. Das Expedited Forwarding PHB reduziert Verzögerungen (Delay, Latenz), Jitter und Paketverluste (RFC 2598).
- Assured Forwarding (AF)
  Das Assured Forwarding PHB bietet ein differenziertes Schema zur Behandlung unterschiedlichen Datenverkehrs (RFC 2597).
- Default Forwarding/Best Effort
  Dieses PHB steht für den Verzicht auf eine bestimmte Priorisierung.

Tab. 19: Zuordnung der IP-Präzedenzwerte zum DSCP-Wert

ToS-Bedeutung	Präzedenzwert	Zugewiesener DSCP
Network Control	111	CS7 (111000)
Internetwork Control	110	CS6 (110000)
Critical	101	CS5 (101000)
Flash Override	100	CS4 (100000)
Flash	011	CS3 (011000)
Immediate	010	CS2 (010000)
Priority	001	CS1 (001000)
Routine	000	CS0 (000000)

10.5.1 DiffServ-Beispiel

Konfigurieren Sie mit den folgenden Schritten das Gerät so, dass es auf Port `1/1` empfangene Pakete mit der Quell-IP-Adresse `10.20.10.11`, dem TCP-Protokoll und dem Quell-Port `80` verwirft.

Führen Sie die folgenden Schritte aus:

☐ Schritt 1: Erzeugen Sie eine Klasse.

☐ Öffnen Sie den Dialog *Switching > QoS/Priority > DiffServ > Klasse*.

☐ Erzeugen Sie eine Klasse:

- Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
- Fügen Sie in das Feld *Name der Klasse* den Namen `class1` ein.
- Wählen Sie in der Dropdown-Liste *Typ* den Eintrag *`protocol`*.
- Geben Sie in das Feld *Protocol number* den Wert `6` ein.
  Legen Sie einen Wert entsprechend den von der IANA definierten „Assigned Internet Protocol Numbers“ fest. Über diesen Link finden Sie eine Liste mit möglichen Werten:
  http://www.iana.org/assignments/protocol-numbers/protocol-numbers.xhtml
- Klicken Sie die Schaltfläche *Ok*.

☐ Fügen Sie die Quell-IP-Adresse und -Maske der Klasse hinzu.

- Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
- Fügen Sie in das Feld *Name der Klasse* den Namen `class1` ein oder wählen Sie ihn aus der Liste aus.
- Wählen Sie in der Dropdown-Liste *Typ* den Eintrag *`srcip`*.
- Geben Sie in das Feld *Quell-IP-Adresse* den Wert `10.20.10.11` ein.
- Klicken Sie die Schaltfläche *Ok*.

☐ Fügen Sie den Quell-Port der Klasse hinzu.

- Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
- Fügen Sie in das Feld *Name der Klasse* den Namen `class1` ein oder wählen Sie ihn aus der Liste aus.
- Wählen Sie in der Dropdown-Liste *Typ* den Eintrag *`srcl4port`*.
- Geben Sie in das Feld *Quell-IP-Adresse* den Wert `80` ein.
- Klicken Sie die Schaltfläche *Ok*.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

☐ Schritt 2: Erzeugen Sie eine Richtlinie.

☐ Öffnen Sie den Dialog *Switching > QoS/Priority > DiffServ > Richtlinie*.

☐ Erzeugen Sie eine Richtlinie (Policy):

- Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
- Geben Sie im Feld *Policy-Name* den Eintrag `policy1` ein.
- Wählen Sie in der Dropdown-Liste *Richtung* den Eintrag *`in`*.
- Wählen Sie im Feld *Name der Klasse* den Eintrag `class1`.
- Wählen Sie im Feld *Typ* den Eintrag *`drop`*.
- Klicken Sie die Schaltfläche *Ok*.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

☐ Schritt 3: Weisen Sie die Richtlinie einem Port zu.

☐ Öffnen Sie den Dialog *Switching > QoS/Priority > DiffServ > Zuweisung*.

☐ Weisen Sie die Richtlinie einem Port zu:

- Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
- Wählen Sie in der Dropdown-Liste *Port* den Port `1/1`.
- Wählen Sie in der Dropdown-Liste *Richtung* den Eintrag `In`.
- Wählen Sie in der Dropdown-Liste *Richtlinie* den Eintrag `policy1`.
- Klicken Sie die Schaltfläche *Ok*.

Anmerkung: Sie können IP-ACL-Regeln und DiffServ-Regeln für die gleiche Richtung nicht gleichzeitig auf einen Port anwenden.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

☐ Schritt 4: Schalten Sie die Funktion global ein.

☐ Öffnen Sie den Dialog *Switching > QoS/Priority > DiffServ > Global*.

☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

In Spalte *Status* ist der Wert `up`, wenn der Link auf dem Port aktiv ist.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`class-map match-all class1`	Eine Klasse mit dem Namen `class1` erzeugen.
`class-map name class1 match protocol tcp`	Der Klasse das Protokoll `tcp` als Filterbedingung hinzufügen.
`class-map name class1 match srcip 10.20.10.11 255.255.255.0`	Der Klasse die Quell-IP-Adresse `10.20.10.11` als Filterbedingung hinzufügen.
`class-map name class1 match srcl4port http`	Der Klasse den Wert `http` (TCP Port 80) als Filterbedingung hinzufügen.
`policy-map create policy1 in`	Eine Richtlinie mit dem Namen `policy1` für empfangene Datenpakete (`in`) erzeugen.
`policy-map name policy1 class add class1`	Die Klasse mit dem Namen `class1` der Richtlinie mit dem Namen `policy1` zuweisen.
`policy-map name policy1 class name class1 drop`	Datenpakete verwerfen.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`service-policy in policy1`	Die Richtlinie mit dem Namen `policy1` dem Interface `1/1` zuweisen.
`exit`	In den Konfigurationsmodus wechseln.
`diffserv enable`	Funktion *DiffServ* global einschalten.

10.6 Flusskontrolle

Wenn in der Warteschlange eines Ports sehr viele Datenpakete gleichzeitig eintreffen, dann führt dies möglicherweise zum Überlaufen des Port-Speichers. Dies geschieht zum Beispiel, 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 Geräts 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.

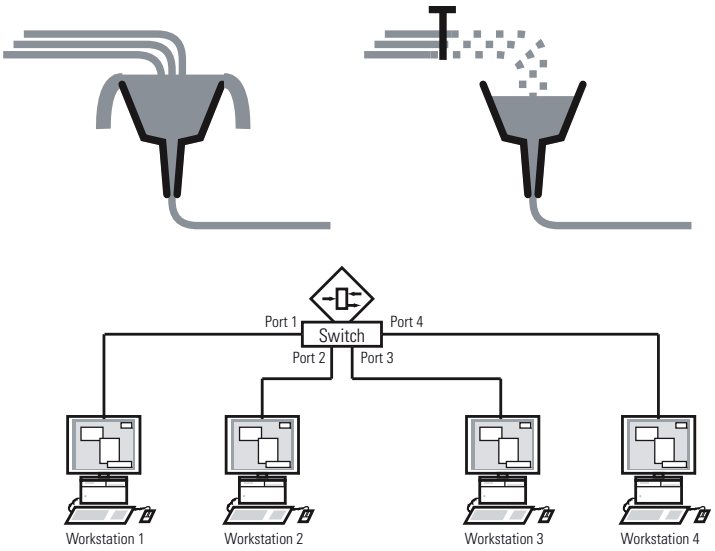


Abb. 26: Beispiel für Flusskontrolle

10.6.1 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.

10.6.2 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓ .

Anmerkung: Wenn Sie eine Redundanzfunktion verwenden, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Ports. Wenn die Flusskontrolle und die 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 Funktion *VLAN* 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 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.

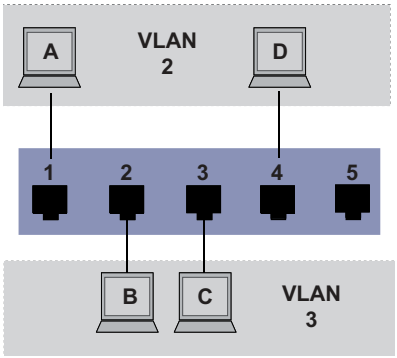


Abb. 27: Beispiel für ein einfaches Port-basiertes VLAN

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`.

Tab. 20: Ingress-Tabelle

Endgerät	Port	Port VLAN Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Tab. 21: Egress-Tabelle

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

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* 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`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 2`	Ein neues VLAN mit VLAN-ID `2` erzeugen.
`name 2 VLAN2`	Dem VLAN `2` den Namen `VLAN2` zuweisen.
`vlan add 3`	Ein neues VLAN mit VLAN-ID `3` erzeugen.
`name 3 VLAN3`	Dem VLAN `3` den Namen `VLAN3` zuweisen.
`name 1 VLAN1`	Dem VLAN `1` den Namen `VLAN1` zuweisen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`show vlan brief`	Aktuelle VLAN-Konfiguration anzeigen.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................ 512
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 > Konfiguration*.

☐ 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 Funktion *GVRP* sind gesperrt.
- `-` = Der Port ist kein Mitglied in diesem VLAN.
  Änderungen durch die Funktion *GVRP* sind erlaubt.

Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie den Wert `U` fest.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Der Wert in Spalte *Ingress-Filtering* hat in diesem Beispiel keinen Einfluss auf die Funktion.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`vlan participation include 2`	Port `1/1` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port `2` die Port-VLAN-ID `1/1` zuweisen.
`exit`	In den Konfigurationsmodus wechseln.
`interface 1/2`	In den Interface-Konfigurationsmodus von Interface `1/2` wechseln.
`vlan participation include 3`	Port `1/2` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port `3` die Port-VLAN-ID `1/2` zuweisen.
`exit`	In den Konfigurationsmodus wechseln.
`interface 1/3`	In den Interface-Konfigurationsmodus von Interface `1/3` wechseln.
`vlan participation include 3`	Port `1/3` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port `3` die Port-VLAN-ID `1/3` zuweisen.
`exit`	In den Konfigurationsmodus wechseln.
`interface 1/4`	In den Interface-Konfigurationsmodus von Interface `1/4` wechseln.
`vlan participation include 2`	Port `1/4` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port `2` die Port-VLAN-ID `1/4` zuweisen.
`exit`	In den Konfigurationsmodus wechseln.
`exit`	In den Privileged-EXEC-Modus wechseln.
`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).

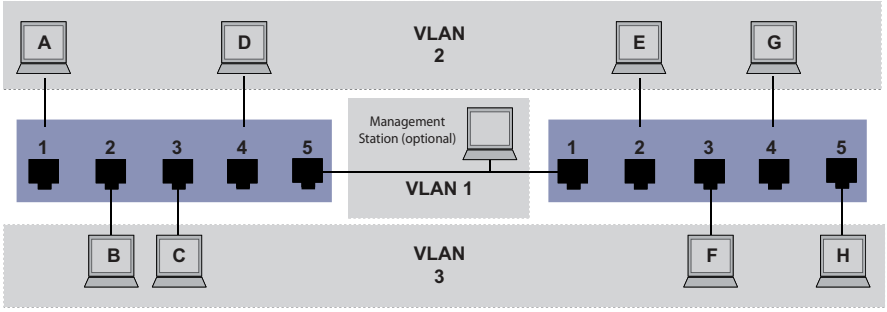


Abb. 28: Beispiel für eine komplexere VLAN-Konfiguration

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.

Tab. 22: Ingress-Tabelle Gerät links

Endgerät	Port	Port VLAN Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

Tab. 23: Ingress-Tabelle Gerät rechts

Endgerät	Port	Port VLAN Identifer (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

Tab. 24: Egress-Tabelle Gerät links

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tab. 25: Egress-Tabelle Gerät rechts

VLAN-ID	Port				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Die Kommunikationsbeziehungen sind hierbei wie folgt: Endgeräte an Port 1 und 4 des linken Geräts sowie Endgeräte an Port 2 und 4 des rechten Geräts sind Mitglied im VLAN 2 und können somit untereinander kommunizieren. Ebenso verhält es sich mit den Endgeräten an Port 2 und 3 des linken Geräts sowie den Endgeräten an Port 3 und 5 des rechten Geräts. 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`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 2`	Ein neues VLAN mit VLAN-ID `2` erzeugen.
`name 2 VLAN2`	Dem VLAN `2` den Namen `VLAN2` zuweisen.
`vlan add 3`	Ein neues VLAN mit VLAN-ID `3` erzeugen.
`name 3 VLAN3`	Dem VLAN `3` den Namen `VLAN3` zuweisen.
`name 1 VLAN1`	Dem VLAN `1` den Namen `VLAN1` zuweisen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`show vlan brief`	Aktuelle VLAN-Konfiguration anzeigen.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 512
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 > Konfiguration*.
- ☐ 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 Funktion *GVRP* sind gesperrt.
  - `-` = Der Port ist kein Mitglied in diesem VLAN.
    Änderungen durch die Funktion *GVRP* 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`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 `1/1` die Port-VLAN-ID `1` zuweisen.
`vlan ingressfilter`	Ingress Filtering auf Port `1/1` aktivieren.
`vlan acceptframe vlanonly`	Port `1/1` überträgt ausschließlich Pakete mit VLAN Tag.
`exit`	In den Konfigurationsmodus wechseln.
`interface 1/2`	In den Interface-Konfigurationsmodus von Interface `1/2` wechseln.
`vlan participation include 2`	Port `1/2` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port `1/2` die Port-VLAN-ID `2` zuweisen.
`exit`	In den Konfigurationsmodus wechseln.
`interface 1/3`	In den Interface-Konfigurationsmodus von Interface `1/3` wechseln.
`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`	In den Konfigurationsmodus wechseln.
`interface 1/4`	In den Interface-Konfigurationsmodus von Interface `1/4` wechseln.
`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`	In den Konfigurationsmodus wechseln.
`interface 1/5`	In den Interface-Konfigurationsmodus von Interface `1/5` wechseln.
`vlan participation include 3`	Port `1/5` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port `1/5` die Port-VLAN-ID `3` zuweisen.

```
exit
```
In den Konfigurationsmodus wechseln.

```
exit
```
In den Privileged-EXEC-Modus wechseln.

```
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

Ein Gast-VLAN 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.

Ein UnauthentifiziertesVLAN ermöglicht dem Gerät, Dienste für 802.1x-fähige Supplikanten bereitzustellen, welche sich nicht korrekt anmelden. Diese Funktion ermöglicht den nicht autorisierten Supplikanten den Zugriff auf eine begrenzte Zahl von Diensten. Wenn Sie an einem Port ein Unauthentifiziertes VLAN konfigurieren und die 802.1x-Port-Authentifizierung ebenso wie die globale Funktion aktiviert haben, ordnet das Gerät den Port dem Unauthentifizierten VLAN zu. Wenn sich ein Supplikant mit 802.1x-Fähigkeit nicht korrekt an dem Port authentisiert, fügt das Gerät den Supplikanten dem Unauthentifizierten VLAN hinzu. Wenn Sie zudem ein Gast-VLAN an dem Port konfigurieren, verwenden Supplikanten ohne 802.1x-Fähigkeit das Gast-VLAN.

Bei Zuweisung eines Unauthentifizierten VLANs zählt der Zähler für die Reauthentifizierung herunter. Das Unauthentifizierte VLAN authentifiziert sich erneut, wenn die in Spalte *Reauthentifizierungs-Periode [s]* festgelegte Zeit abläuft und Supplikanten auf dem 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 `An`.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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*
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 10`	VLAN `10` erzeugen.
`vlan add 20`	VLAN `20` erzeugen.
`name 10 Guest`	VLAN `10` in `Guest` umbenennen.
`name 20 Unauth`	VLAN `20` in `Unauth` umbenennen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dot1x system-auth-control enable`	Funktion *802.1X Port-Authentifizierung* global einschalten.
`dot1x port-control auto`	Port-Kontrolle auf Port `1/4` einschalten.
`interface 1/4`	In den Interface-Konfigurationsmodus von Interface `1/4` wechseln.
`dot1x guest-vlan 10`	Port `1/4` das Gast-VLAN zuweisen.
`dot1x unauthenticated-vlan 20`	Port `1/4` das nicht autorisierte VLAN zuweisen.
`exit`	In den Konfigurationsmodus wechseln.

11.3 RADIUS-VLAN-Zuordnung

Die Funktion der RADIUS-VLAN-Zuordnung ermöglicht, 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 Mitglied hinzu und setzt die Port-VLAN-ID (PVID) auf den vorgegebenen Wert. Der Port vermittelt die Datenpakete ohne VLAN-Tag.

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 ist abhängig von der Konfiguration des Voice-VLAN-Interfaces.

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, ermöglicht dem Gerät, 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, ermöglicht dem Gerät, 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 MAC-basierte VLANs

Verwenden Sie das MAC-basierte VLAN, um Datenverkehr anhand der mit dem VLAN verknüpften Quell-MAC-Adresse weiterzuleiten. Ein MAC-basiertes VLAN definiert Filterkriterien für unmarkierte Datenpakete oder für Pakete mit Prioritätsmarkierung.

Sie legen einen MAC-basierten VLAN-Filter fest, indem Sie einem MAC-basierten VLAN eine bestimmte Quelladresse zuweisen. Das Gerät leitet dann unmarkierte Pakete weiter, welche mit dieser Quell-MAC-Adresse an der MAC-basierten VLAN-ID angekommen sind. Die anderen unmarkierten Pakete unterliegen den normalen VLAN-Klassifizierungsregeln.

11.6 IP-Subnetz-basierte VLANs

In einem IP-Subnetz-basierten VLAN leitet das Gerät Datenverkehr anhand der mit einem VLAN verknüpften Quell-IP-Adresse und Subnetzmaske weiter. Benutzerdefinierte Filter legen hierbei fest, ob ein Paket zu einem bestimmten VLAN gehört.

Verwenden Sie das IP-Subnetz-basierte VLAN, um die Filterkriterien für unmarkierte Datenpakete oder für Pakete mit Prioritätsmarkierung festzulegen. Weisen Sie zum Beispiel einem IP-Subnetz-basierten VLAN eine bestimmte Subnetz-Adresse zu. Wenn das Gerät unmarkierte Pakete von der Subnetz-Adresse empfängt, leitet es die Pakete an das IP-Subnetz-basierte VLAN weiter. Andere unmarkierte Pakete unterliegen den normalen VLAN-Klassifizierungsregeln.

Zum Konfigurieren eines IP-Subnetz-basierten VLANs legen Sie eine IP-Adresse, eine Subnetzmaske und die dazugehörige VLAN-Kennung fest. Bei mehreren zutreffenden Einträgen verknüpft das Gerät die VLAN-ID zuerst mit dem Eintrag, welcher das längste Präfix aufweist.

11.7 Protokoll-basiertes VLAN

In einem Protokoll-basierten VLAN überbrückt das Gerät den Datenverkehr über festgelegte Ports auf Grundlage des Protokolls, das mit dem VLAN verknüpft ist. Benutzerdefinierte Paketfilter legen hierbei fest, ob ein Paket zu einem bestimmten VLAN gehört.

Konfigurieren Sie Protokoll-basierte VLANs, indem Sie den Wert in Spalte *Ethertype* als Filterkriterium für unmarkierte Pakete verwenden. Weisen Sie zum Beispiel einem Protokoll-basierten VLAN ein bestimmtes Protokoll zu. Wenn das Gerät unmarkierte Pakete mit diesem Protokoll empfängt, leitet es die Pakete an das Protokoll-basierte VLAN weiter. Das Gerät weist die anderen unmarkierten Pakete der VLAN-ID des Ports zu.

11.8 VLAN-Unaware-Modus

Die Funktion *VLAN-Unaware-Modus* legt die Funktion des Geräts 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. Das Gerät versendet 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 wesentliche 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

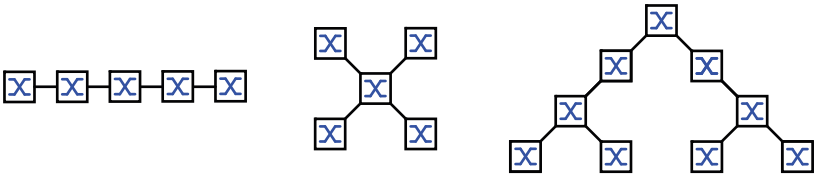


Abb. 29: Netz mit Linien-, Stern- und Baum-Topologie

Um bei Ausfall einer Verbindung die Kommunikation dennoch aufrecht zu erhalten, installieren Sie zwischen den Netzknoten zusätzliche physische Verbindungen. Redundanzprotokolle sorgen dafür, dass die zusätzlichen Verbindungen abgeschaltet bleiben, so lange die ursprüngliche Verbindung besteht. Wenn die Verbindung ausfällt, 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.

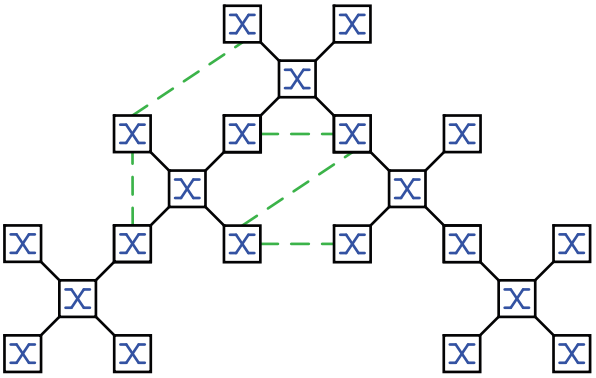


Abb. 30: Maschen-Topologie: Baum-Topologie mit physikalischen Schleifen

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.

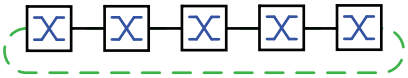


Abb. 31: Ring-Topologie: Linien-Topologie mit verbundenen Enden

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:

Tab. 26: Redundanzprotokolle im Überblick

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.
Subring	Ring	Die Funktion *Sub Ring* ermöglicht Ihnen eine einfache Ankopplung von Netzsegmenten an bestehende Redundanz-Ringe.
Ring-/Netzkopplung	Ring	
RCP	Ring	
RSTP	beliebige Struktur	Die Umschaltzeit ist abhängig von der Netz-Topologie und von Anzahl der Geräte. ▶ typ. < 1 s bei RSTP ▶ typ. < 30 s bei STP
Link-Aggregation	beliebige Struktur	Eine Link-Aggregation-Gruppe (LAG) ist eine Kombination von 2 oder mehr Verbindungen zwischen 2 Switches, um die Bandbreite zu erhöhen. Jede der beteiligten Verbindungen arbeitet im Vollduplex-Modus und mit der selben Datenrate.

Tab. 26: Redundanzprotokolle im Überblick (Forts.)

Redundanzpro-tokoll	Netz-Topologie	Bemerkungen
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.
HIPER-Ring-Client	Ring	Vorhandenen HIPER-Ring erweitern oder ein Gerät ersetzen, das bereits als Client in einem HIPER-Ring aktiv ist.
HIPER-Ring über LAG	Ring	Geräte über eine Link-Aggregationsgruppe (LAG) miteinander verbinden. Die Ring-Clients und der Ring-Manager verhalten sich wie ein Ring ohne eine LAG-Instanz.

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

12.1.3 Kombinationen von Redundanzprotokollen

Tab. 27: Überblick der Kombinationen von Redundanzprotokollen

	MRP	RSTP/MSTP	Link-Aggreg.	Link-Backup	Subring	HIPER-Ring
MRP	▲	—	—	—	—	—
RSTP/ MSTP [3]	▲ [1]	▲	—	—	—	—
Link-Aggreg.	▲ [2]	▲ [2]	▲	—	—	—
Link-Backup	▲	▲	▲	▲	—	—
Subring	▲	▲	▲ [2]	▲	▲	—
HIPER-Ring	▲	▲ [1]	▲ [2]	▲	▲	▲

▲ Kombinierbar

○ Nicht kombinierbar

1) Eine redundante Kopplung zwischen diesen Netztopologien führt möglicherweise zu Loops.
Wie Sie diese Topologien redundant koppeln, entnehmen Sie Kapitel „FuseNet” auf Seite 221.

2) Kombinierbar auf demselben Port

3) In Kombination mit MSTP können sich die Umschaltzeiten anderer Redundanzprotokolle geringfügig erhöhen.

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.

Wenn Sie den festgelegten MRP-Redundanzport (Fixed Backup) verwenden und der primäre Ring-Link ausfällt, vermittelt der Ring-Manager die Daten an den sekundären Ring-Link. Bei Wiederherstellung des primären Links wird der sekundäre Link weiterhin benutzt.

12.2.1 Netzstruktur

Das Konzept der Ring-Redundanz ermöglicht Ihnen, hochverfügbare, ringförmige Netzstrukturen aufzubauen.

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.

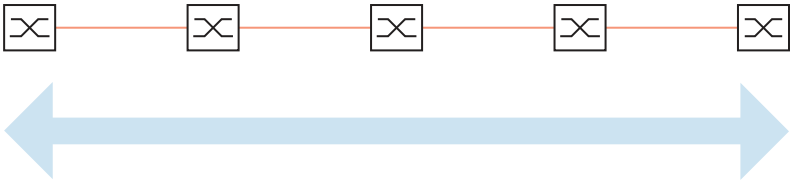


Abb. 32: Linienstruktur

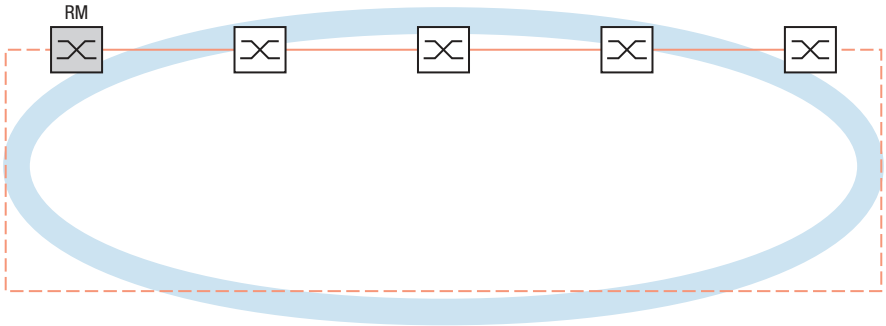


Abb. 33: Redundante Ringstruktur
RM = Ring-Manager
—— Hauptleitung
- - - redundante Leitung

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:
- `500ms`
- `30ms`

Anmerkung: Wenn jedes Gerät im Ring die kürzere Verzögerungszeit unterstützt, können Sie die Rekonfigurationszeit mit einem kleineren Wert als `500ms` konfigurieren.

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 festgelegten 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 ein 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` (unmarkiert) 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 Erweiterte Informationen

MRP-Pakete

MRP verwendet Testpakete, Link-Change-Pakete und Topologieänderungs-Pakete (FDB-Lösch-Pakete)

Der Ring-Manager (RM) ist mit 2 Ring-Ports mit dem Ring verbunden. Solange alle Verbindungen im Ring funktionieren, setzt der RM einen seiner Ports, den redundanten Port, in einen blockierten Zustand. In diesem Zustand sendet und empfängt der redundante Port keine normalen (Nutzlast-) Datenpakete. Auf diese Weise verhindert der RM einen Loop.

Der RM sendet periodisch Testpakete von beiden Ringports in den Ring. Die Testpakete sind spezielle Pakete. Der RM sendet und empfängt Testpakete auch am redundanten Port, obwohl der redundante Port normale Pakete blockiert. Der RM erwartet, die Testpakete am jeweils anderen Ring-Port zu empfangen. Wenn der RM für eine festgelegte Zeit keine erwarteten Testpakete empfängt, erkennt der RM einen Ring-Ausfall.

Wenn die *Advanced mode*-Funktion aktiviert ist, reagiert der RM auch auf Link-Down-Pakete von Ring-Geräten. Die Voraussetzung ist, dass jedes Ring-Gerät das Senden von Link-Change-Paketen an den RM unterstützt, wenn eine Verbindung zwischen 2 Ring-Geräten ausfällt oder hergestellt wird. Diese Pakete helfen dem RM dabei, schneller auf den Ausfall oder die Wiederherstellung einer Verbindung zu reagieren. Der RM empfängt die Link-Change-Pakete auch an seinem redundanten Port.

Bei der Rekonfiguration des Rings löscht der RM seine Forwarding Database (FDB) und sendet Topologieänderungs-Pakete an die Ring-Geräte. Die Topologieänderungs-Pakete veranlassen die Ring-Geräte dazu, ebenfalls ihre FDB zu löschen. Dieses Verfahren hilft dabei, die Nutzlast-Pakete rascher über den neuen Pfad zu vermitteln. Dieses Verfahren wird ausgeführt, gleichgültig, ob die Ring-Rekonfiguration durch einen Verbindungs-Ausfall oder eine Verbindungs-Herstellung verursacht wurde.

Tab. 28: MRP-Pakete

Paket-Typ	Sende-Modus	Zeit-Parameter	Wert
Testpaket[1]	Periodisch	Sende-Intervall	50 ms (für Ring-Wiederherstellungs-Zeit 500 ms) 20 ms (für Ring-Wiederherstellungs-Zeit 200 ms)
		Empfangs-Zeitüberschreitung	400 ms (für Ring-Wiederherstellungs-Zeit 500 ms) 160 ms (für Ring-Wiederherstellungs-Zeit 200 ms)
Link-Down-Paket[2]	Ereignis-getrieben	Beim Verbindungs-Ausfall eines Ring-Ports.	-
Topologieänderungs-Paket[3]	Ereignis-getrieben	Bei Rekonfiguration	-

1. Ausschließlich vom Ring-Manager versendet.
2. Gesendet von unterstützenden Ring-Geräten.
3. Der Empfang eines Topologieänderungs-Pakets veranlasst die unterstützenden Ring-Geräte dazu, ihre FDB zu löschen.

MRP-Paket-Priorisierung

Das Ring-Gerät sendet die Testpakete, die Link-Change- und die Topologieänderungs-Pakete mit einer konfigurierbaren MRP-VLAN-ID. Die voreingestellte MRP-VLAN-ID ist 0, was bedeutet, dass die Geräte die Testpakete ohne VLAN-Tag und damit ohne Prioritäts- (Class of Service-) Information senden.

Um die Rekonfigurations-Zeit bei hoher Netzlast zu minimieren, können Sie diese Pakete mit VLAN-Tag und damit mit Prioritätsinformation versehen. Die Geräte senden und vermitteln diese Pakete dann mit der IEEE 802.1Q Class of Service-Priorität 7 (Netz-Steuerung).

Um diese Pakete zu priorisieren, führen Sie die folgenden Schritte auf dem Rimg-Manager und auf allen Ring-Geräten aus:

- Legen Sie die MRP-VLAN-ID auf einen Wert ≥ `1` fest.
- Legen Sie die Ring-Ports als `T` (Mitglied mit VLAN-Tag) dieser MRP-VLAN-ID fest.

Anmerkung: Wenn Sie die MRP-VLAN-ID im *Switching > L2-Redundanz > MRP*-Dialog auf einen Wert ≥ `1` festlegen, dann fügt das Gerät seine Ring-Ports als `T` (Mitglied mit VLAN-Tag) für diese MRP-VLAN-ID hinzu. Wenn das neue VLAN nicht existiert, erzeugt das Gerät automatisch dieses VLAN. Nach dem Festlegen einer neuen MRP-VLAN-ID überprüfen Sie im *Switching > VLAN > Konfiguration*-Dialog die VLAN- und Port-Einstellungen.

12.2.6 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.

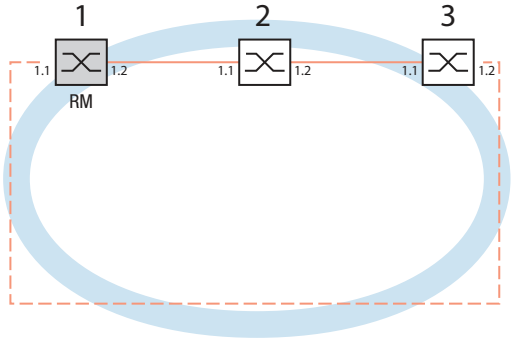


Abb. 34: Beispiel eines MRP-Rings
RM = Ring-Manager
—— Hauptleitung
- - - redundante Leitung

Die folgende Beispielkonfiguration beschreibt die Konfiguration des Ring-Manager-Geräts (1). Konfigurieren Sie die 2 anderen Geräte (2 bis 3) in gleicher Weise, jedoch ohne die *Ring-Manager*-Funktion einzuschalten. Dieses Beispiel nutzt kein VLAN. Als Ring-Wiederherstellungszeit legen Sie den Wert `30ms` fest. Jedes Gerät unterstützt den Advanced Mode des Ring-Managers.

- ☐ Bauen Sie das Netz nach Ihren Erfordernissen auf.
- ☐ Konfigurieren Sie jeden Port so, dass die Datenrate und die Duplexeinstellungen der Strecken der folgenden Tabelle entsprechen:

Tab. 29: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–

Anmerkung: Optische Ports ohne Unterstützung für Autonegotiation (automatische Konfiguration) konfigurieren Sie mit 100 Mbit/s Vollduplex (FDX) oder 1000 Mbit/s Vollduplex (FDX). Das Abschalten der automatischen Verbindungsaushandlung (Autonegotiation) kann die Erkennung einer Änderung des Verbindungs-Status beschleunigen.

Anmerkung: Optische Ports ohne Unterstützung für Autonegotiation (automatische Konfiguration) konfigurieren Sie mit 100 Mbit/s Vollduplex (FDX). Das Abschalten der automatischen Verbindungsaushandlung (Autonegotiation) kann die Erkennung einer Änderung des Verbindungs-Status beschleunigen.

Anmerkung: Konfigurieren Sie jedes Gerät des MRP-Rings individuell. Bevor Sie die redundante Leitung anschließen, vergewissern Sie sich, dass Sie die Konfiguration jedes Geräts des MRP-Rings abgeschlossen haben. So vermeiden Sie Loops 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 jedem Port eingeschaltet.)

Schalten Sie die *Spanning Tree*-Funktion in jedem Gerät im Netz aus. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Ausschalten der Funktion.
  Im Lieferzustand ist Spanning Tree für das Gerät aktiviert.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`no spanning-tree operation`	Spanning Tree ausschalten.
`show spanning-tree global`	Zur Kontrolle die Parameter anzeigen.

Schalten Sie MRP auf allen Geräten im Netz ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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 jeden Ringteilnehmer mit der gleichen MRP-Domänen-ID. 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`	Eine neue MRP-Domäne mit der ID `default-domain` erzeugen.
`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. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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`	Funktion *Fixed backup* auf dem sekundären Port aktivieren. 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`	Festlegen, dass das Gerät als *Ring-Manager* arbeitet. Bei den anderen Geräten im Ring belassen Sie die Voreinstellung.

- ☐ Markieren Sie das Kontrollkästchen im Feld *Advanced mode*.

`mrp domain modify  advanced-mode enabled`	Advanced Mode einschalten.

- ☐ Wählen Sie im Feld *Ring-Rekonfiguration* den Wert `30ms` aus.

`mrp domain modify recovery-delay 200ms`	Den Wert `30ms` festlegen als max. Verzögerungszeit bei der Rekonfiguration des Rings.

Anmerkung: Wenn bei der Wahl des Werts `30ms` für die Ringrekonfiguration die Stabilität des Rings nicht den Anforderungen an Ihr Netz entspricht, dann wählen Sie den Wert `500ms`.

- ☐ Aktivieren Sie die Funktion des MRP-Rings.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`mrp domain modify operation enable`	MRP-Ring einschalten.

Wenn jeder Ring-Teilnehmer konfiguriert ist, 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 Geräts. Führen Sie dazu die folgenden Schritte aus:

`show mrp`	Zur Kontrolle die Parameter anzeigen.

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.

Wenn das Gerät als Ring-Client oder als Ring-Manager arbeitet, sind folgende Meldungen möglich:

- *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.

Wenn das Gerät als Ring-Manager arbeitet, sind folgende Meldungen möglich:

- *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 1 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 einem Ring-Port.

Gliedern Sie den MRP-Ring gegebenenfalls in ein VLAN ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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-VLAN-ID 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 VLAN-ID auf `0`.
    Legen Sie im Dialog *Switching > VLAN > Konfiguration* für die Ring-Ports im VLAN `U` die VLAN-Zugehörigkeit `1` (unmarkiert) fest.
  - Soll der MRP-Ring einem VLAN zugewiesen sein, geben Sie eine VLAN-ID > `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>` VLAN-ID zuweisen.

12.2.7 MRP-over-LAG

Hirschmann-Geräte ermöglichen Ihnen, zum Erhöhen der Bandbreite Link-Aggregation-Gruppen (LAG) mit dem für die Redundanz eingesetzten Media-Redundancy-Protokoll (MRP) zu kombinieren. Die Funktion ermöglicht Ihnen, die Bandbreite in einzelnen Segmenten oder im gesamten Netz zu erhöhen.

Die Funktion *Link-Aggregation* unterstützt Sie dabei, die Bandbreitenbegrenzung für einzelne Ports aufzuheben. LAG ermöglicht Ihnen, 2 oder mehr Verbindungen zu einer logischen Verbindung zwischen 2 Geräten zusammenzufassen. Die parallelen Links erhöhen die Übertragungsbandbreite zwischen den 2 Geräten.

Ein MRP-Ring besteht aus bis zu 50 Geräten, die das MRP-Protokoll nach IEC 62439 unterstützen. Wenn Sie ausschließlich Hirschmann-Geräte verwenden, dann ermöglicht Ihnen das Protokoll, MRP-Ringe mit bis zu 100 Geräten zu konfigurieren.

MRP-over-LAG verwenden Sie in folgenden Fällen:
- zum Erhöhen der Bandbreite in einzelnen Segmenten eines MRP-Rings
- zum Erhöhen der Bandbreite im gesamten MRP-Ring

Netzstruktur

Beim Konfigurieren eines MRP-Rings mit LAGs überwacht der Ring-Manager (RM) beide Enden des Backbones auf Durchgang. Der RM blockiert Daten auf dem sekundären (redundanten) Port, solange der Backbone intakt ist. Wenn der RM eine Unterbrechung des Datenstroms im Ring erkennt, dann vermittelt er die Daten an den sekundären Port und sorgt so für eine erneute Backbone-Anbindung.

LAG-Instanzen verwenden Sie in MRP-Ringen ausschließlich, um die Bandbreite zu erhöhen, während MRP für die Redundanz sorgt.

Damit ein RM eine Unterbrechung im Ring erkennt, benötigt MRP ein Gerät, das jeden Port in der LAG-Instanz blockiert, wenn ein Port in der Instanz ausfällt.

LAG in einem einzelnen Segment eines MRP-Rings

Das Gerät ermöglicht Ihnen, eine LAG-Instanz in einzelnen Segmenten eines MRP-Rings zu konfigurieren.

Für Geräte im MRP-Ring nutzen Sie das LAG-Single-Switch-Verfahren. Das Single-Switch-Verfahren bietet Ihnen eine preiswerte Möglichkeit, Ihr Netz zu erweitern, indem Sie lediglich ein Gerät auf jeder Seite eines Segments verwenden, um die physischen Ports zur Verfügung zu stellen. Um die Bandbreite für bestimmte Segmente im Bedarfsfall zu erhöhen, fassen Sie die Ports des Geräts zu einer LAG-Instanz zusammen.

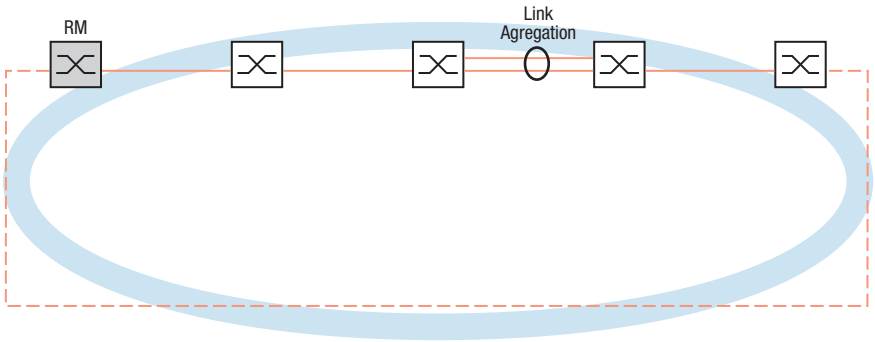


Abb. 35: Link-Aggregation über eine einzelne Verbindung eines MRP-Rings

LAG im gesamten MRP-Ring

Neben dem Konfigurieren einer LAG-Instanz in bestimmten Segmenten eines MRP-Rings ermöglichen Ihnen Hirschmann-Geräte auch, LAG-Instanzen in jedem Segment zu konfigurieren, um die Bandbreite im gesamten MRP-Ring zu erhöhen.

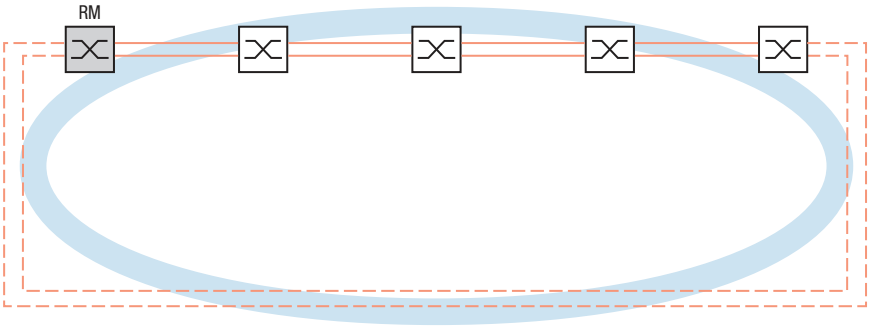


Abb. 36: Link-Aggregation für den gesamten MRP-Ring

Ermittlung von Unterbrechungen im Ring

Beim Konfigurieren der LAG-Instanz legen Sie den Wert *Aktive Ports (min.)* fest, um die Gesamtzahl der in der LAG-Instanz verwendeten Ports anzugleichen. Wenn ein Gerät eine Unterbrechung an einem Port in der LAG-Instanz erkennt, dann blockiert es die Daten an den anderen Ports der Instanz. Wenn jeder Port einer Instanz blockiert ist, dann erkennt der RM, dass der Ring geöffnet ist und vermittelt die Daten an den sekundären Port. Auf diese Weise sorgt der RM für eine Verbindung zur anderen Seite des unterbrochenen Segments.

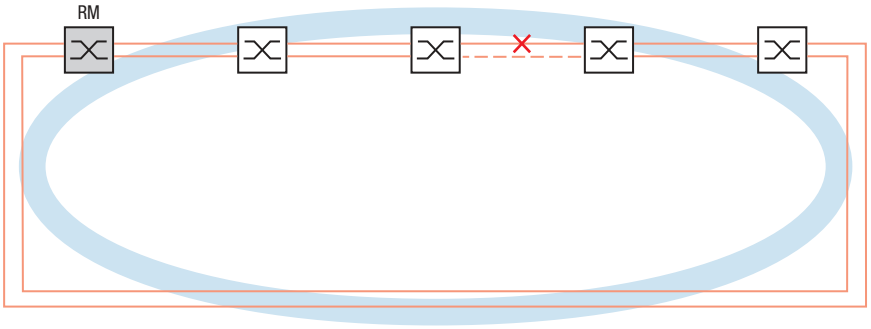


Abb. 37: Unterbrechung einer Verbindung in einem MRP-Ring

Beispiel-Konfiguration

Im folgenden Beispiel verbinden Switch A und Switch B zwei Abteilungen. Das Verkehrsaufkommen der Abteilungen übersteigt die individuelle Bandbreitenkapazität der Ports. Um die Bandbreite des Segments zu erhöhen, konfigurieren Sie eine LAG-Instanz für das einzelne Segment des MRP-Rings.

Voraussetzung für die Beispielkonfiguration ist, dass Sie mit einem funktionsfähigen MRP-Ring beginnen.

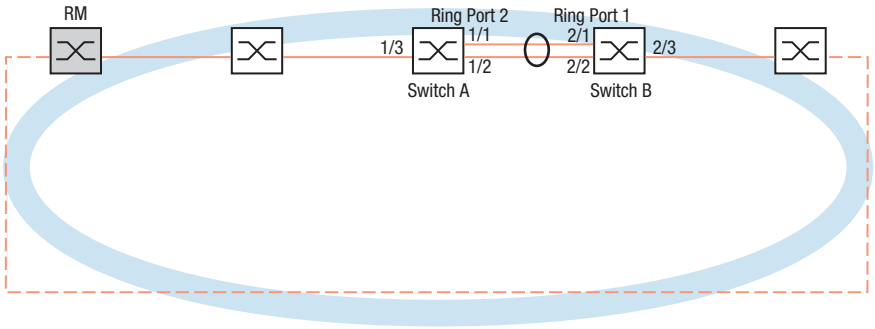


Abb. 38: Beispielkonfiguration für MRP-over-LAG

Konfigurieren Sie den Switch A zuerst. Führen Sie dazu die folgenden Schritte aus. Konfigurieren Sie Switch B mit den gleichen Schritten und ersetzen Sie dabei die entsprechenden Port- und Ring-Port-Nummern.

- ☐ 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 *Ok*.
- ☐ Wiederholen Sie die vorherigen Schritte und wählen Sie den Port *1/2*.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ In Spalte *Aktive Ports (min.)* geben Sie `2` ein, was in diesem Fall die Gesamtzahl der Ports in der LAG-Instanz ist. Wenn Sie MRP und LAG kombinieren, legen Sie die Gesamtzahl der Ports als *Aktive Ports (min.)* fest. Wenn das Gerät eine Unterbrechung an einem Port erkennt, dann blockiert es die anderen Ports der Instanz und bewirkt so das Öffnen des Rings. Der Ring-Manager erkennt, dass der Ring geöffnet ist und vermittelt die Daten an den sekundären Ring-Port, womit er die Verbindung zu den anderen Geräten im Netz wiederherstellt.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > MRP*.
- ☐ Wählen Sie im Rahmen *Ring-Port 2*, Dropdown-Liste *Port* den Port `lag/1`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`link-aggregation add lag/1`	Eine Link-Aggregation-Gruppe `lag/1` erzeugen.
`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.
`mrp domain modify port secondary lag/1`	Port `lag/1` als Ring-Port `2` festlegen.
`copy config running-config nvm`	Aktuelle Einstellungen im „ausgewählten” Konfigurationsprofil im permanenten Speicher (`nvm`) speichern.

12.3 HIPER-Ring-Client

Das Konzept der HIPER-Ring-Redundanz ermöglicht den Aufbau hochverfügbarer, ringförmiger Netzstrukturen. Die *HIPER-Ring*-Client-Funktion ermöglicht dem Netzadministrator, einen vorhandenen HIPER-Ring zu erweitern oder ein Client-Gerät zu ersetzen, das bereits Teilnehmer eines HIPER-Ringes ist.

Wenn das Gerät feststellt, dass der Daten-Link am Ring-Port abbricht, sendet das Gerät ein Link-Down-Datenpaket an den Ring-Manager (RM) und leert die FDB-Tabelle. Sobald der Ring-Manager das LinkDown-Datenpaket empfängt, vermittelt der Ring-Manager den Datenstrom über den Primär- und über den Sekundär-Ring-Port. So ist der Ring-Manager in der Lage, die Integrität des HIPER-Ringes aufrecht zu erhalten.

Das Gerät unterstützt ausschließlich Fast-Ethernet-Ports und Gigabit-Ethernet-Ports als Ring-Ports. Außerdem können Sie die Ring-Ports in eine LAG-Instanz einschließen.

In der Voreinstellung ist der HIPER-Ring-Client inaktiv, und die primären Ports und sekundären Ports sind auf `no Port` gesetzt.

Anmerkung: Deaktivieren Sie das Spanning Tree Protocol (STP) für die Ring-Ports im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, da das STP und der HIPER-Ring verschiedene Reaktionszeiten besitzen.

Tab. 30: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–

12.3.1 VLANs am HIPER-Ring

Das Gerät ermöglicht Ihnen, VLAN-Daten über den HIPER-Ring weiterzuleiten. Somit bietet das Gerät Redundanz für Ihre VLAN-Daten. Das Ring-Gerät leitet Management-Daten um den Ring herum, zum Beispiel in VLAN 1. Damit die Daten die Management-Station erreichen, leiten die Ring-Geräte die unmarkierten Management-Daten an den Ring-Ports weiter. Legen Sie außerdem die Ring-Ports als Mitglieder in VLAN 1. fest.

Wenn andere VLANs Ihre Ring-Geräte durchqueren, leiten die Ring-Geräte die anderen VLAN-Daten als markiert weiter.

Legen Sie die VLAN-Einstellungen fest. Führen Sie dazu die folgenden Schritte auf allen Ring-Teilnehmern und auf dem Ring-Manager aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Unmarkierte VLAN-Management-Daten an den Ring-Ports weiterleiten.
  Wählen Sie für VLAN 1 in der Dropdown-Liste derjenigen Spalten, die sich auf den Ring-Port beziehen, den Eintrag `U`.
- ☐ Verhindern der Weiterleitung von Redundanzprotokoll-Paketen an die Nicht-Ring-Ports:
  Wählen Sie für VLAN 1 in der Dropdown-Liste den Eintrag `-` in den Spalten aus, die sich **nicht** auf die Ring-Ports beziehen.
- ☐ Zulassen, dass ein Gerät im Ring die VLAN-Daten an und von Ports mit VLAN-Mitgliedschaft vermittelt.
  Wählen Sie für die anderen VLANs in der Dropdown-Liste den Eintrag `T` in den Spalten aus, die sich auf die Ring-Ports beziehen.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Den Ring-Ports die Mitgliedschaft in VLAN 1 zuweisen.
  Fügen Sie für die Ring-Ports in Spalte *Port-VLAN-ID* den Wert `1` ein.
- ☐ Den Nicht-Ring-Ports die Mitgliedschaft im VLAN zuweisen.
  Fügen Sie für die Nicht-Ring-Ports in Spalte *Port-VLAN-ID* die entsprechende VLAN-ID ein.

12.3.2 Erweiterte Informationen

Der HIPER Ring ist der proprietäre Vorgänger von MRP. Der HIPER Ring arbeitet ähnlich wie MRP, verwendet jedoch andere Pakete. Um einen redundanten Ring neu aufzusetzen, empfiehlt Hirschmann, MRP zu verwenden.

HIPER Ring-Pakete

Der HIPER Ring verwendet Testpakete, Link-Down-Pakete und Topologieänderungs-Pakete.

Anmerkung: HiOS bietet HIPER Ring-Client-Funktionen. HIPER Ring-Manager-Funktionen werden von Geräten mit Classic-Software angeboten. Die HIPER Ring-Manager-Funktionen werden hier nur der Vollständigkeit halber erwähnt. Details finden Sie in der Dokumentation zu Ihrem HIPER Ring-Manager-Gerät.

Der Ring-Manager (RM) ist mit 2 Ring-Ports mit dem Ring verbunden. Solange alle Verbindungen im Ring funktionieren, setzt der RM einen seiner Ports, den redundanten Port, in einen blockierten Zustand. In diesem Zustand sendet und empfängt der redundante Port keine normalen (Nutzlast-) Datenpakete. Auf diese Weise verhindert der RM einen Loop.

Der RM sendet periodisch Testpakete von beiden Ringports in den Ring. Die Testpakete sind spezielle Pakete. Der RM sendet und empfängt Testpakete auch am redundanten Port, obwohl der redundante Port normale Pakete blockiert. Der RM erwartet, die Testpakete am jeweils anderen Ring-Port zu empfangen. Wenn der RM für eine festgelegte Zeit keine erwarteten Testpakete empfängt, erkennt der RM einen Ring-Ausfall.

Wenn eine Verbindung zwischen 2 Ring-Geräten ausfällt, senden die betroffenen Ring-Geräte ein Link-Down-Paket an den RM. Dies hilft dem RM dabei, rascher auf einen Verbindungsausfall zu reagieren. Der RM empfängt die Link-Down-Pakete auch auf seinem redundanten Port.

Bei der Rekonfiguration des Rings löscht der RM seine Forwarding Database (FDB) und sendet Topologieänderungs-Pakete an die Ring-Geräte. Die Topologieänderungs-Pakete veranlassen die Ring-Geräte dazu, ebenfalls ihre FDB zu löschen. Dieses Verfahren hilft dabei, die Nutzlast-Pakete rascher über den neuen Pfad zu vermitteln. Dieses Verfahren wird ausgeführt, gleichgültig, ob die Ring-Rekonfiguration durch einen Verbindungs-Ausfall oder eine Verbindungs-Herstellung verursacht wurde.

Tab. 31: HIPER Ring-Pakete

Paket-Typ	Sende-Modus	Zeit-Parameter	Wert
Testpaket[1]	Periodisch	Sende-Intervall[2]	20 ms (beschleunigte Ring-Wiederherstellungs-Zeit) 60 ms (Standard-Ring-Wiederherstellungs-Zeit)
		Empfangs-Zeitüberschreitung	280 ms (beschleunigte Ring-Wiederherstellungs-Zeit) 480 ms (Standard-Ring-Wiederherstellungs-Zeit)
Link-Down-Paket[3]	Ereignis-getrieben	Beim Verbindungs-Ausfall eines Ring-Ports.	-
Topologieänderungs-Paket[4]	Ereignis-getrieben	Bei Rekonfiguration	-

1. Ausschließlich vom HIPER Ring-Manager (Classic Software) versendet.
2. Ausschließlich im HIPER Ring-Manager (Classic Software) festgelegt.
3. Gesendet von unterstützenden Ring-Teilnehmern.
4. Der Empfang eines Topologieänderungs-Pakets veranlasst die unterstützenden Ring-Teilnehmer dazu, ihre FDB zu löschen.

HIPER Ring-Paket-Priorisierung

Die Ring-Geräte senden die Testpakete, die Link-Change- und die Topologieänderungs-Pakete mit der festen VLAN-ID 1. In der Voreinstellung haben die Pakete kein VLAN-Tag und damit keine Prioritäts- (Class of Service-) Information. Um die Rekonfigurations-Zeit bei hoher Netzlast zu minimieren, können Sie diese Pakete mit VLAN-Tag und damit mit Prioritätsinformation versehen. Der Ring-Manager und die Ring-Teilnehmer senden und vermitteln diese Pakete dann mit der IEEE 802.1Q Class of Service-Priorität 7 (Netz-Steuerung).

Konfigurieren Sie dazu die Ring-Ports als `T` (Mitglied mit VLAN-Tag) von VLAN 1 auf jedem Ring-Teilnehmer und auf dem Ring-Manager (Classic Software).

Anmerkung: Diese Einstellungen für VLAN 1 weichen von den im Kapitel „VLANs am HIPER-Ring" auf Seite 192 beschriebenen VLAN-Einstellungen ab.

12.3.3 HIPER-Ring über LAG

Die Funktion *HIPER-Ring* ermöglicht Ihnen, die Geräte über eine Link-Aggregation-Gruppe (LAG) miteinander zu verbinden. Die Ring-Clients und der Ring-Manager verhalten sich wie ein Ring ohne eine LAG-Instanz.

Beim Ausfall einer LAG-Verbindung fällt auch die andere Datenverbindung in der Instanz aus und verursacht eine Unterbrechung des Ringes. Nach der Erkennung einer Unterbrechung im Ring senden die betroffenen Ports ein LinkDown-Datenpaket an den Ring-Manager. Der Ring-Manager hebt die Blockierung seines redundanten Ports auf, sendet Daten in beide Richtungen in den Ring und antwortet mit einem Topologieänderungs-Paket. Nach Empfang eines Topologieänderungs-Pakets löschen die Ring-Teilnehmer ihre FDB.

12.4 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 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 vermeidet Loops 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` erhöht werden.

Wenn das als Root arbeitende Gerät ausfällt und ein anderes Gerät dessen Funktion übernimmt, bestimmt die neue Root-Bridge die größtmögliche erlaubte Anzahl der Geräte in einem Branch durch ihre *Max age*-Einstellung.

Anmerkung: Der RSTP-Standard schreibt vor, dass jedes Gerät innerhalb eines Netzes mit dem (Rapid-) Spanning-Tree-Algorithmus arbeitet. 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.

12.4.1 Grundlagen

Da RSTP eine Weiterentwicklung des STP ist, gilt jede der folgenden Beschreibungen des STP auch für 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 ermöglicht 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 Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation besitzt die höchste Priorität.

Nach dem ursprünglichen Standard IEEE 802.1D-1998 sind die 2 höchstwertigen Bytes die Bridge-Priorität. Bei der Konfiguration einer Bridge kann der Bridge-Administrator die Voreinstellung für die Bridge-Priorität ändern, die `32768` (8000H) ist.

Im neueren Standard IEEE 802.1Q-2014 wird die Bridge-Priorität anders interpretiert. Die höchsten 4 Bits repräsentieren die Bridge-Priorität. Die niedrigeren 12 Bits sind für die VLAN-ID reserviert und sind alle Null. Als Folge kann der Bridge-Administrator die Bridge-Priorität in 4096er-Schritten einstellen. Der voreingestellte Wert ist `32768` (8000H) und der Maximalwert ist `61440` (F000H).

Die 6 niederwertigen Bytes der Bridge-Identifikation sind die MAC-Adresse der Bridge. Die MAC-Adresse ermöglicht, dass jede Bridge eine eindeutige Bridge-Identifikation besitzt.

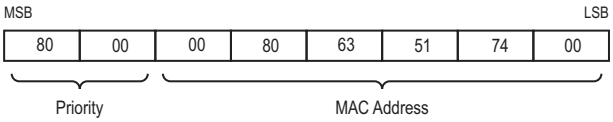


Abb. 39: Bridge-Identifikation, Beispiel (Interpretation nach IEEE 802.1D-1998, Werte in Hexadezimalschreibweise)

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 32 auf Seite 198). Dabei weist das Gerät Pfaden mit niedrigerer Datenrate höhere Pfadkosten zu.

Alternativ dazu kann auch der Administrator die Pfadkosten festlegen. Dabei weist der Administrator - wie das Gerät - Pfaden mit niedrigerer Datenrate höhere 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 der einzelnen Pfadkosten derjenigen Pfade, die ein Datenpaket zwischen dem angeschlossenen Port einer Bridge und der Root-Bridge passiert.

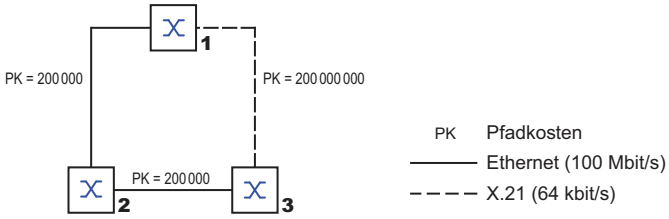


Abb. 40: Pfadkosten

Tab. 32: Empfohlene Pfadkosten beim RSTP in Abhängigkeit von der Datenrate.

Datenrate	Empfohlener Wert	Empfohlener Bereich	Möglicher Bereich
≤100 kbit/s	200 000000[1]	20000000-200000000	1-200000000
1 Mbit/s	20000000[a]	2000000-200000000	1-200000000
10 Mbit/s	2000000[a]	200000-20000000	1-200000000
100 Mbit/s	200000[a]	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200 000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

1. 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

Nach dem ursprünglichen Standard IEEE 802.1D-1998 besteht die Port-Identifikation aus 2 Bytes. Das niederwertigere Byte enthält die physikalische Portnummer. Dies gewährleistet eine eindeutige Bezeichnung des Port dieser Bridge. Das höherwertige Byte ist die Port-Priorität, die der Administrator festlegt (Voreinstellung: `128` oder 80H).

Im neueren Standard IEEE 802.1Q-2014 wird die Port-Priorität anders interpretiert. Die höchsten 4 Bits repräsentieren die Port-Priorität. Die niedrigeren 12 Bits sind die Port-Nummer. Dies berücksichtigt Bridges mit bis zu 4095 Ports. Als Folge kann der Bridge-Administrator die Port-Priorität in 4096er-Schritten einstellen, wenn sie als 16 Bit-Zahl betrachtet wird. Der voreingestellte Wert ist `32768` (8000H) und der Maximalwert ist `61440` (F000H). Als 4-Bit-Zahl betrachtet, ist die Voreinstellung `8` (8H), der Minimalwert ist `0` (0H) und der Maximalwert ist `15` (FH).

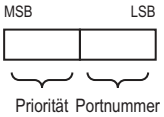


Abb. 41: Port-Identifikation (Interpretation nach IEEE 802.1D-1998)

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).

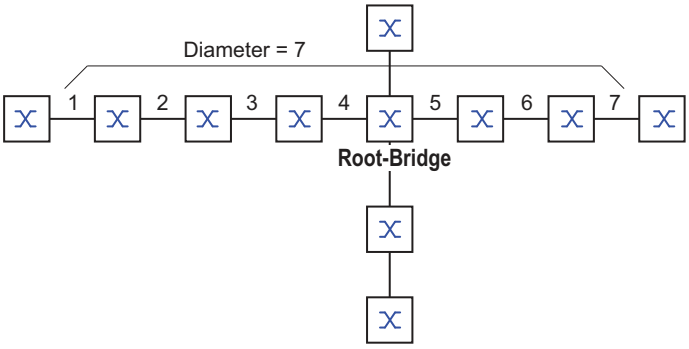


Abb. 42: Definition „Diameter“

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.

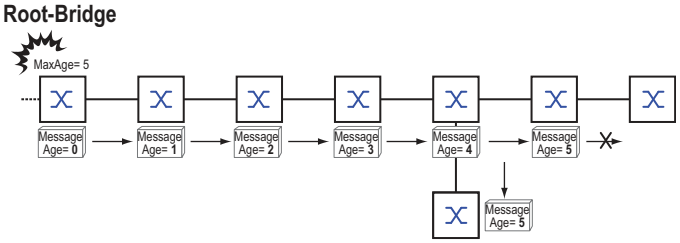


Abb. 43: Übertragung einer STP-BPDU in Abhängigkeit von MaxAge

12.4.2 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 ist abhängig von den Root-Pfadkosten. 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 41 auf Seite 199). Die Bridge blockiert dabei den Port, der zu dem Port mit der schlechteren ID führt. Haben 2 Ports die gleiche Priorität, hat der Port mit der höheren Port-Nr. die numerisch höhere ID; dies ist die logisch schlechtere.

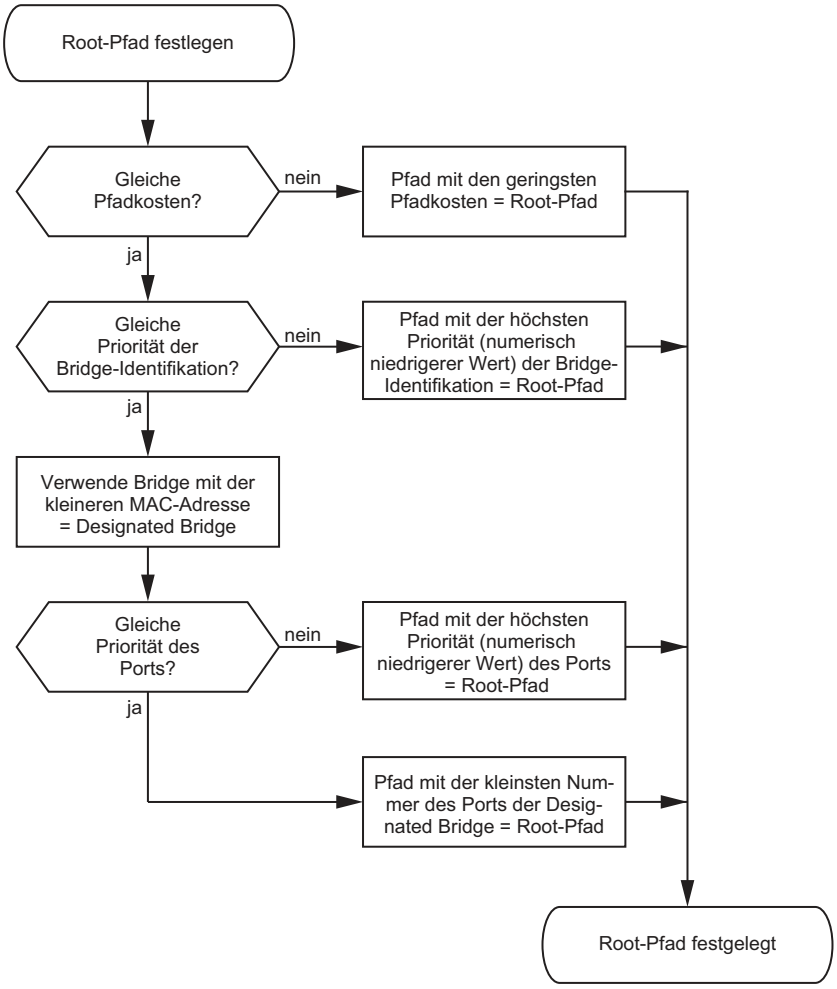


Abb. 44: Flussdiagramm Root-Pfad festlegen

12.4.3 Beispiele

Beispiel für die Bestimmung des Root-Pfads

Anhand des Netzplanes kann man das Flussdiagramm (siehe Abbildung 44 auf Seite 201) 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 belastet jeder Teilpfad die gleichen Pfadkosten. Das Protokoll blockiert den Pfad zwischen Bridge 2 und Bridge 3, da eine Verbindung von Bridge 3 über Bridge 2 zur Root-Bridge höhere Pfadkosten verursachen würde.

Interessant ist der Pfad von der Bridge 6 zur Root-Bridge:

- Der Pfad über Bridge 5 und Bridge 3 verursacht die gleichen Root-Pfadkosten wie der Pfad über Bridge 4 und Bridge 2.
- 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).

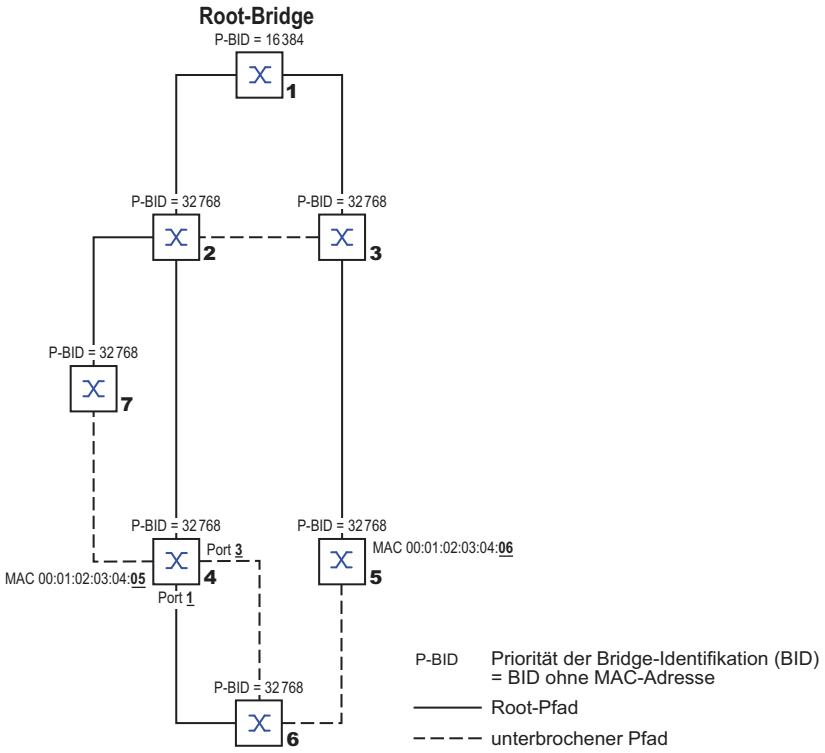


Abb. 45: Beispiel eines Netzplans für die Bestimmung des Root-Pfads

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 kann man das Flussdiagramm (siehe Abbildung 44 auf Seite 201) 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.

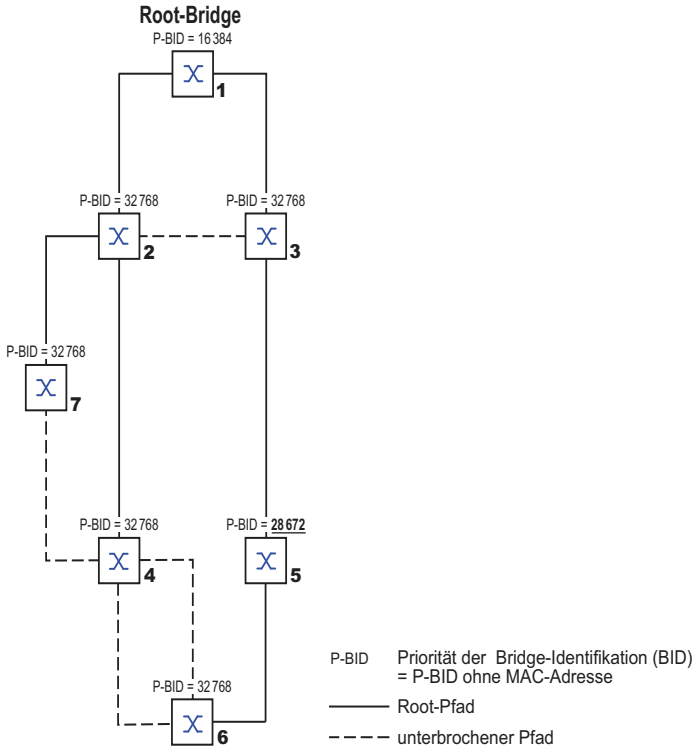
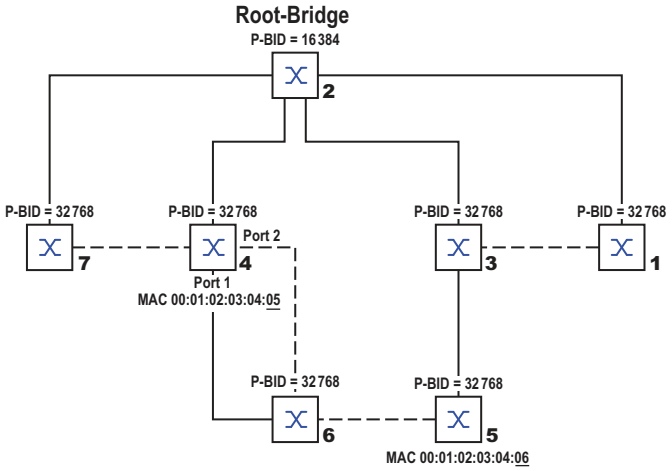


Abb. 46: Beispiel eines Netzplans für die Manipulation des Root-Pfads

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 jeder anderen Bridge sendet.

Konfiguriert der Management-Administrator die Bridge 2 als Root-Bridge, dann verteilt sich die Belastung der Teilnetze durch Kontrollpakete wesentlich besser. Daraus ergibt sich die in der folgenden Abbildung dargestellte Konfiguration. Die Pfadkosten der meisten Bridges zur Root-Bridge sind kleiner geworden.



P-BID Priorität der Bridge-Identifikation (BID) = P-BID ohne MAC-Adresse

——— Root-Pfad

– – – – unterbrochener Pfad

Abb. 47: Beispiel für die Manipulation der Baumstruktur

12.5 Das Rapid Spanning Tree Protokoll

Das RSTP behält die Berechnung der Baumstruktur vom STP unverändert bei. Wenn eine Verbindung oder eine Bridge ausfällt, ändert RSTP lediglich Parameter und fügt neue Parameter und Mechanismen hinzu, die die Rekonfiguration beschleunigen.

Eine zentrale Bedeutung erfahren in diesem Zusammenhang die Ports.

12.5.1 Port-Rollen

RSTP weist jedem Bridge-Port eine der folgenden Rollen zu:

- Root-Port:
  Dies ist der Port, an dem eine Bridge Datenpakete mit den niedrigsten Pfadkosten von der Root-Bridge empfängt.
  Existieren mehrere Ports mit gleich niedrigen Pfadkosten, dann entscheidet die Bridge-Identifikation der zur Root führenden Bridge (Designated Bridge), welchem ihrer Ports die weiter von der Root entfernte Bridge die Rolle des Root-Ports gibt.
  Hat eine Bridge mehrere Ports mit gleich niedrigen Pfadkosten zur selben Bridge, entscheidet die Bridge anhand der Portidentifikation der zur Root führenden Bridge (Designated Bridge), welchen Port sie lokal als Root-Port wählt. Siehe Abbildung 44 auf Seite 201.
  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 dem 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
  Beim Ausfall der Verbindung zur Root-Bridge übernimmt dieser blockierte Port die Aufgabe des Root-Ports. Der Alternate-Port dient als Reserve für die Verbindung zur Root Bridge.

- 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.

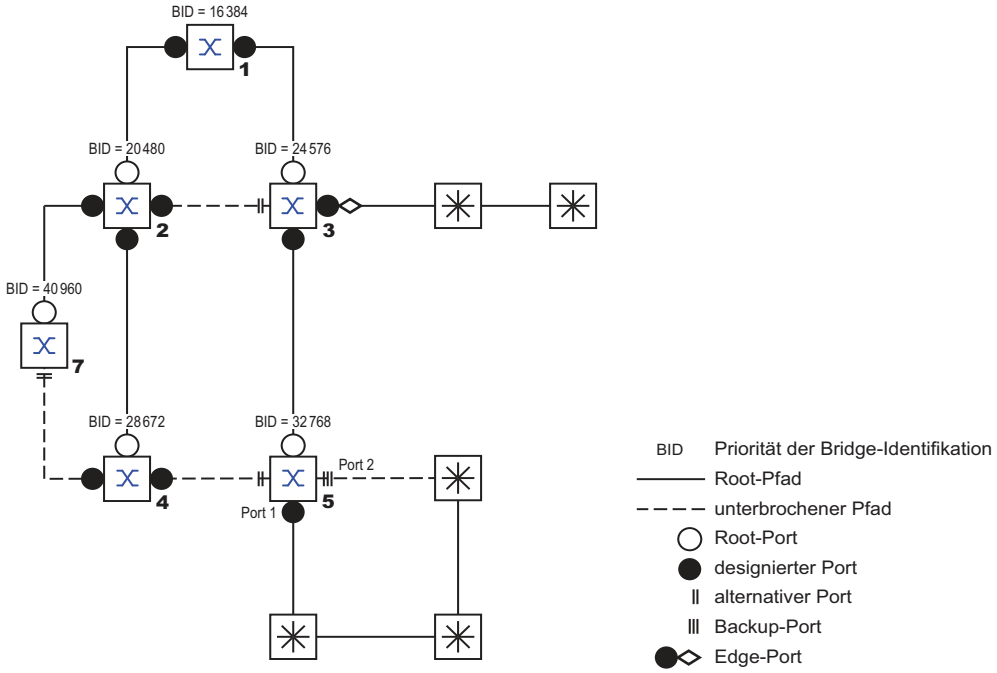


Abb. 48: Port-Rollen-Zuweisung

12.5.2 Port-Stati

In Abhängigkeit von der Baumstruktur und dem Status der ausgewählten Verbindungswege weist RSTP den Ports ihren Status zu.

Tab. 33: Beziehung zwischen Port-Status-Werten bei STP und RSTP

STP Port Status	Administrative Bridge Port-Status	MAC Operational	RSTP Port-Status	Aktive Topology (Port Rolle)
DISABLED	Ausgeschaltet	FALSE	Discarding[1]	Excluded (Disabled)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (Disabled)
BLOCKING	Enabled	TRUE	Discarding[2]	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)

1. Die dot1d-MIB zeigt „Disabled“.
2. Die dot1d-MIB zeigt „Blocked“.

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 jedes Paket-Typs (nicht ausschließlich STP-BPDUs)

12.5.3 Spanning Tree Priority Vector

Um den Ports Rollen zuzuteilen, tauschen die RSTP-Bridges Konfigurationsinformationen untereinander aus. Diese Informationen heißen "Spanning Tree Priority Vector". Sie sind Teil der RST BPDUs und enthalten folgende Informationen:

- Bridge-Identifikation der Root-Bridge
- Root-Pfadkosten der sendenden Bridge
- Bridge-Identifikation der sendenden Bridge
- Portidentifikation des Ports, durch den die Nachricht gesendet wurde
- Portidentifikation des Ports, durch den die Nachricht empfangen wurde

Auf Basis dieser Informationen sind die an RSTP beteiligten Bridges in der Lage, selbstständig Port-Rollen zu bestimmen und den Port-Status ihrer lokalen Ports zu definieren.

12.5.4 Schnelle Rekonfiguration

Warum kann RSTP schneller als STP auf eine Unterbrechung des Root-Pfades reagieren?

- Einführung von Edge-Ports:
  Bei einer Rekonfiguration setzt RSTP einen Edge-Port nach Ablauf von 3 Sekunden (Voreinstellung) in den Vermittlungsmodus. Um sich zu vergewissern, dass keine BPDU-sendende Bridge angeschlossen ist, wartet RSTP "Hello Time" ab.
  Wenn Sie sich vergewissern, 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: Datenpakete können während der Rekonfigurationsphase der RSTP-Topologie dupliziert werden und/oder mit vertauschter Reihenfolge beim Empfänger ankommen. Sie können auch das Spanning Tree Protocol verwenden oder Sie wählen eines der anderen in diesem Handbuch beschriebenen Redundanzverfahren.

12.5.5 Gerät konfigurieren

RSTP konfiguriert die Netztopologie komplett selbstständig. 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.

Führen Sie die folgenden Schritte aus:

- ☐ 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 jedem Port eingeschaltet.)
- ☐ Schalten Sie MRP auf jedem Gerät aus.
- ☐ Schalten Sie Spanning Tree auf jedem Gerät im Netz ein.
  Im Lieferzustand ist Spanning Tree auf dem Gerät eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Einschalten der Funktion.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`spanning-tree operation`	Spanning Tree einschalten.
`show spanning-tree global`	Zur Kontrolle die Parameter anzeigen.

Schließen Sie nun die redundanten Strecken an.

Legen Sie die Einstellungen für das Gerät fest, das die Rolle der Root-Bridge übernimmt.

Führen Sie die folgenden Schritte aus:

- ☐ 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`spanning-tree mst priority 0 <0..61440>`	Bridge-Priorität des Geräts festlegen. **Anmerkung:** Legen Sie die Bridge-Priorität im Bereich `0..61440` in 4096er-Schritten 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`	Zur Kontrolle die Parameter anzeigen.

- ☐ 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`spanning-tree forward-time <4..30>`	Verzögerungszeit für Zustandswechsel in Sekunden festlegen.
`spanning-tree max-age <6..40>`	Maximal zulässige Astlänge festlegen, d. h. die Anzahl der Geräte bis zur Root-Bridge.
`show spanning-tree global`	Zur Kontrolle die Parameter anzeigen.

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, dann 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 Geräts sowie der Root-Bridge.
- Nummer des Geräte-Ports, der zur Root-Bridge führt.
- Pfadkosten vom Root-Port des Geräts bis zur Root-Bridge.

Führen Sie die folgenden Schritte aus:

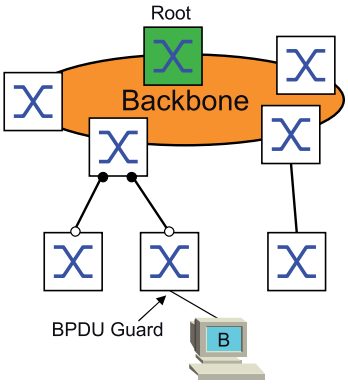
`show spanning-tree global`	Zur Kontrolle die Parameter anzeigen.

12.5.6 Guards

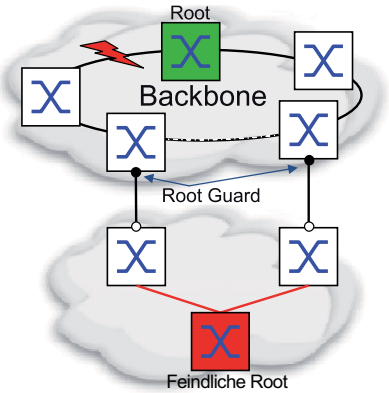
Das Gerät ermöglicht Ihnen, an den Geräte-Ports verschiedene Schutzfunktionen (Guards) zu aktivieren.

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.

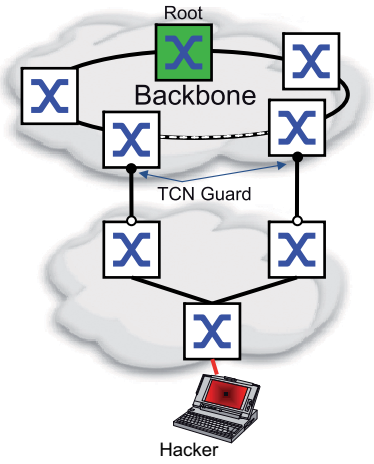


  Endgeräte-Ports empfangen im Normalfall keine STP-BPDUs. Versucht ein Angreifer, auf diesem Port trotzdem STP-BPDUs einzuspeisen, deaktiviert das Gerät den Geräte-Port.
- Root Guard – für Designated-Ports
  Diese Schutzfunktion aktivieren Sie für jeden Geräte-Port separat.



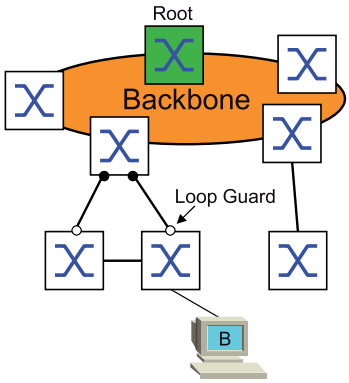
  Empfängt ein Designated-Port eine STP-BPDU mit besserer Pfadinformation zur Root-Bridge, verwirft das Gerät die STP-BPDU und setzt den Vermittlungsstatus des Ports auf `discarding` anstatt auf `root`.
  Bleiben die STP-BPDUs mit besserer Pfadinformation zur Root-Bridge aus, setzt das Gerät den Status 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 empfangenen 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.



Wenn der Port keine STP-BPDUs mehr empfängt, hilft diese Schutzfunktion, den irrtümlichen Wechsel des Vermittlungsstatus eines Ports auf `forwarding` zu vermeiden. Tritt dieser Fall ein, kennzeichnet das Gerät den Loop-Status des Ports als inkonsistent, leitet aber keine Datenpakete weiter.

BPDU Guard einschalten

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Markieren Sie das Kontrollkästchen *BPDU-Guard*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`spanning-tree bpdu-guard`	BPDU Guard einschalten.
`show spanning-tree global`	Zur Kontrolle die Parameter anzeigen.

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Wechseln Sie in die Registerkarte *CIST*.
- ☐ Markieren Sie für Endgeräte-Ports das Kontrollkästchen in Spalte *Admin-Edge-Port*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`interface <x/y>`	In den Interface-Konfigurationsmodus von Interface `<x/y>` wechseln.
`spanning-tree edge-port`	Den Port als Endgeräte-Port (Edge Port) kennzeichnen.
`show spanning-tree port x/y`	Zur Kontrolle die Parameter anzeigen.
`exit`	Interface-Modus verlassen.

Empfängt ein Edge-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 Spalte *Port an* unmarkiert.
- ▶ Das Gerät kennzeichnet den Port.

Sie können feststellen, ob ein Port sich selbst abgeschaltet hat, weil er eine BPDU empfangen hat. Führen Sie dazu die folgenden Schritte aus:

Im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *Guards* ist das Kontrollkästchen in Spalte *BPDU guard effect* markiert.

`show spanning-tree port x/y`	Zur Kontrolle die Parameter des Ports anzeigen. Der Wert des Parameters *BPDU guard effect* ist `enabled`.

Setzen Sie den Zustand des Geräteports auf den Wert `forwarding` zurück. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Wechseln Sie in die Registerkarte *Guards*.
- ☐ Für Designated-Ports markieren Sie das Kontrollkästchen in Spalte *Root-Guard*.
- ☐ Für Ports, die STP-BPDUs mit Topology-Change-Flag empfangen, markieren Sie das Kontrollkästchen in Spalte *TCN-Guard*.
- ☐ Für Root-, Alternate- oder Backup-Ports markieren Sie das Kontrollkästchen in 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* aktiv ist, deaktiviert das Gerät die Funktion *Loop-Guard*.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface <x/y>`	In den Interface-Konfigurationsmodus von Interface `<x/y>` wechseln.
`spanning-tree guard-root`	Root Guard auf dem Designated-Port einschalten.
`spanning-tree guard-tcn`	TCN Guard auf dem Port einschalten, der STP-BPDUs mit Topology-Change-Flag empfängt.
`spanning-tree guard-loop`	Loop Guard auf einem Root-, Alternate- oder Backup-Port einschalten.
`exit`	Interface-Modus verlassen.
`show spanning-tree port x/y`	Zur Kontrolle die Parameter des Ports anzeigen.

12.5.7 Ring only mode

Verwenden Sie die Funktion *Ring only mode*, um Vollduplex-Konnektivität zu erkennen, und um Ports zu konfigurieren, die mit Endgeräten verbunden sind. Die Funktion *Ring only mode* ermöglicht dem Gerät, in den Zustand „forwarding“ zu wechseln und Topology Change Notification PDUs zu unterdrücken.

Ring only mode konfigurieren

Wenn Sie die Funktion *Ring only mode* 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 Funktion *Ring only mode*.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > 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 *1/2*.
- ☐ Um die Funktion zu aktivieren, markieren Sie im Rahmen *Ring only mode* das Kontrollkästchen *Aktiv*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`spanning-tree ring-only-mode operation`	Funktion *Ring only mode* einschalten.
`spanning-tree ring-only-mode first-port 1/1`	Port *1/1* als erstes Interface festlegen.
`spanning-tree ring-only-mode second-port 1/2`	Port *1/2* als zweites Interface festlegen.

12.6 Link-Aggregation

Die Funktion *Link-Aggregation* mit dem Single-Switch-Verfahren hilft Ihnen, 2 Einschränkungen bei Ethernet-Links zu überwinden, und zwar Bandbreite und Redundanz.

Die Funktion *Link-Aggregation* unterstützt Sie dabei, die Bandbreitenbegrenzung für einzelne Ports aufzuheben. Die Funktion *Link-Aggregation* ermöglicht Ihnen, 2 oder mehr Verbindungen zu 1 logischen Verbindung zwischen 2 Geräten zusammenzufassen. Die parallelen Links erhöhen die Übertragungsbandbreite zwischen den 2 Geräten.

Sie verwenden die Funktion *Link-Aggregation* üblicherweise im Backbone-Netz. Die Funktion bietet Ihnen die Möglichkeit, die Bandbreite schrittweise, kostengünstig zu erhöhen.

Die Funktion *Link-Aggregation* bietet des Weiteren Redundanz mit einer unterbrechungsfreien Umschaltung. Wenn bei 2 oder mehr parallel konfigurierten Links ein Link ausfällt, leiten die anderen Links in der Gruppe den Datenverkehr weiter.

Das Gerät verwendet eine Hash-Option, um die Lastverteilung über die Port-Gruppe zu bestimmen. Das Markieren des Egress-Datenverkehrs ermöglicht dem Gerät, zusammengehörige Datenpakete über denselben Link zu übertragen.

Die Voreinstellungen für eine neue *Link-Aggregation*-Instanz sind:
- Der Wert im Rahmen *Konfiguration*, Feld *Hashing-Option* ist `sourceDestMacVlan`.
- 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 *Hashing-Option* ist der Wert `sourceDestMacVlan`.
- In Spalte *Aktive Ports (min.)* ist der Wert `1`.

12.6.1 Funktionsweise

Das Gerät arbeitet mit dem Single-Switch-Verfahren. Das Single-Switch-Verfahren bietet Ihnen eine kostengünstige Möglichkeit, Ihr Netz zu erweitern. Das Single-Switch-Verfahren legt fest, dass Sie ein 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 erste Port, den Sie zur Gruppe hinzufügen, ist der Master-Port und bestimmt die Bandbreite für die weiteren Mitglieder der Link-Aggregation-Group.

Das Gerät ermöglicht Ihnen, bis zu 8 Link-Aggregation-Gruppen einzurichten. Die Anzahl der verwendbaren Ports je Link-Aggregation-Gruppe ist geräteabhängig.

Hash-Algorithmus

Der Datenpaket-Verteiler ist dafür zuständig, Datenpakete von den Endgeräten zu empfangen und sie über die Link-Aggregation-Group zu übertragen. Der Frame-Distributor implementiert einen Verteilungsalgorithmus, der den für die Übertragung eines Datenpaketes verwendeten Link auswählt. Die Hash-Option hilft Ihnen, eine Lastverteilung über die Gruppe zu erreichen.

Die folgende Liste enthält Optionen, die Sie für die Auswahl des Links festlegen.
- Quell-MAC-Adresse, VLAN-ID, Ethertype und empfangender Port
- Ziel-MAC-Adresse, VLAN-ID, Ethertype und empfangender Port
- Quell-/Ziel-MAC-Adresse, VLAN-ID, Ethertype und empfangender Port
- Quell-IP-Adresse und Quell-TCP-/UDP-Port
- Ziel-IP-Adresse und Ziel-TCP-/UDP-Port
- Quell-/Ziel-IP-Adresse und Quell-/Ziel-TCP-/UDP-Port

Statische und dynamische Links

Das Gerät ermöglicht Ihnen, statische und dynamische Links einzurichten.
- Statische Links: Der Administrator richtet die Links manuell ein und verwaltet die Links manuell. Wenn beispielsweise ein Link ausfällt und ein Medienkonverter zwischengeschaltet ist, überträgt der Medienkonverter weiterhin den Datenstrom auf den Link, der den Ausfalls des Links verursacht hat. Eine andere Möglichkeit ist, dass die Verkabelung oder ein unerkannter Konfigurationsfehler unerwünschtes Netzverhalten hervorruft. In diesem Fall ändert der Netzadministrator manuell die Link-Einstellung, um den Datenverkehr wiederherzustellen.
- Dynamische Links: Das Gerät bestätigt, dass die Einstellung auf dem entfernten Gerät die Link-Aggregation bewerkstelligen kann und eine Umschaltung tritt automatisch auf.

12.6.2 Link-Aggregation Beispiel

Verbinden Sie mehrere Workstations, indem Sie eine aggregierte Link-Gruppe zwischen Switch 1 und 2 verwenden. Durch das Aggregieren mehrerer Links können höhere Geschwindigkeiten ohne Hardware-Upgrade erreicht werden.

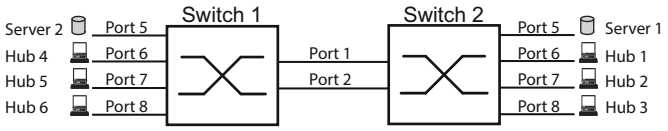


Abb. 49: Link Aggregation Switch-zu-Switch-Netz

Konfigurieren Sie Switch 1 and 2 über die grafische Benutzeroberfläche. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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 *Ok*.

- ☐ Wiederholen Sie die vorherigen Schritte und wählen Sie den Port *1/2*.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`link-aggregation add lag/1`	Eine Link-Aggregation-Gruppe `lag/1` erzeugen.
`link-aggregation modify lag/1 addport 1/1`	Port *1/1* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 addport 1/2`	Port *1/2* zur Link-Aggregation-Gruppe hinzufügen.

12.7 Link-Backup

Link-Backup bietet einen redundanten Link für Datenverkehr auf Schicht-2-Geräten. Wenn das Gerät einen Fehler auf dem primären Link erkannt hat, leitet das Gerät den Datenverkehr zum Backup-Link um. Sie verwenden Link-Backup üblicherweise in Netzen von 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, ermöglicht Ihnen das Gerät, mehr als ein 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 ein Port 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 ist, weisen Sie dem zweiten Port des Paares dasselbe VLAN zu.

Die Voreinstellung für diese Funktion ist „deaktiviert“ ohne Link-Backup-Paare.

Anmerkung: Vergewissern Sie sich, dass das Spanning-Tree-Protokoll auf den Link-Backup-Ports ausgeschaltet ist.

12.7.1 Beschreibung Fail-Back

Link-Backup ermöglicht Ihnen, 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 Topologieänderungs-Paket zum entfernten Gerät. Das Topologieänderungs-Paket hilft dem entfernten Gerät dabei, die MAC-Adressen schnell wieder zu lernen.

12.7.2 Beispiel-Konfiguration

Im Beispiel-Netzwerk unten verbinden Sie die Ports *2/3* und *2/4* auf Switch A mit dem Uplink der Switches B und C. Wenn Sie die Ports als Link-Backup-Paar einrichten, leitet ein 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.

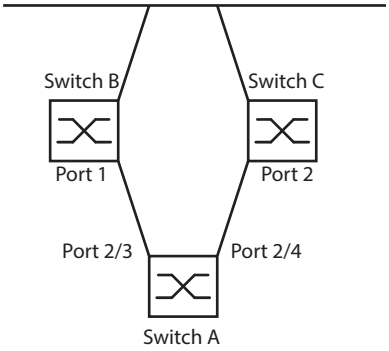


Abb. 50: Link-Backup Beispiel-Netzwerk

Die folgenden Tabellen enthalten Beispiele für Parameter, um Switch A zu konfigurieren.

Führen Sie die folgenden Schritte aus:

- ☐ 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 Funktion *Fail back* 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 *An* das Optionsfeld *Funktion*.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 2/3`	In den Interface-Konfigurationsmodus von Interface *2/3* wechseln.

`link-backup add 2/4`	Eine Link-Backup-Instanz erzeugen, 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`	Zeichenfolge `Link_Backup_1` als Name des Backup-Paares festlegen.
`link-backup modify 2/4 failback-status enable`	Fail-Back-Timer einschalten.
`link-backup modify 2/4 failback-time 30`	Fail-Back-Verzögerungszeit auf `30` s festlegen.
`link-backup modify 2/4 status enable`	Link-Backup-Instanz einschalten.
`exit`	In den Konfigurationsmodus wechseln.
`link-backup operation`	Die Funktion *Link-Backup* global auf dem Gerät einschalten.

12.8 FuseNet

Die *FuseNet*-Protokolle ermöglichen Ihnen, Ringe zu koppeln, die mit einem der folgenden Redundanzprotokolle arbeiten:

- MRP
- HIPER-Ring
- RSTP

Anmerkung: Voraussetzung für das Koppeln eines Netzes an den Haupt-Ring mittels des Protokolls *Ring-/Netzkopplung* ist, dass das angeschlossene Netz ausschließlich Netzkomponenten enthält, die das Protokoll *Ring-/Netzkopplung* unterstützen.

Verwenden Sie die folgende Tabelle, um das *FuseNet*-Kopplungs-Protokoll auszuwählen, das in Ihrem Netz zum Einsatz kommt:

Haupt-Ring	Verbundenes Netz		
	MRP	**HIPER-Ring**	**RSTP**
MRP	*Sub Ring*[1)]	– *Redundant Coupling Protocol* – *Ring-/Netzkopplung*	– *Redundant Coupling Protocol* – *Ring-/Netzkopplung*
HIPER-Ring	*Sub Ring*	*Ring-/Netzkopplung*	– *Redundant Coupling Protocol* – *Ring-/Netzkopplung*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	–

– kein geeignetes Kopplungs-Protokoll

1) mit *MRP* eingerichtet an unterschiedlichen VLANs

12.9 Subring

Die Funktion *Sub Ring* ist eine Erweiterung des Media Redundancy Protocol (MRP). Diese Funktion ermöglicht Ihnen, einen Subring an einen Hauptring mit unterschiedlichen Netzstrukturen zu koppeln.

Das Subring-Protokoll ermöglicht, Redundanz für Geräte durch das Koppeln der beiden Enden eines Netzes in Linienstruktur zu einem Hauptring herzustellen.

Die Einrichtung von Subringen bietet folgende Vorteile:
- Mit der Kopplung nehmen Sie das neue Netzsegment in das Redundanz-Konzept auf.
- Subringe ermöglichen das einfache Einbinden neuer Bereiche in ein bestehendes Netz.
- Subringe bieten Ihnen die Möglichkeit, die Organisationsstruktur eines Bereichs in einer Netztopologie abzubilden.
- In einem MRP-Ring liegen die Umschaltzeiten des Subrings im Redundanzfall üblicherweise bei < 100 ms.

12.9.1 Beschreibung für einen Subring

Das Subring-Konzept ermöglicht Ihnen die Kopplung neuer Netzsegmente an geeignete Geräte in einem bestehenden Ring (Hauptring). Die Geräte, die einen Subring an den Hauptring ankoppeln, heißen „Subring-Manager“ (SRM).

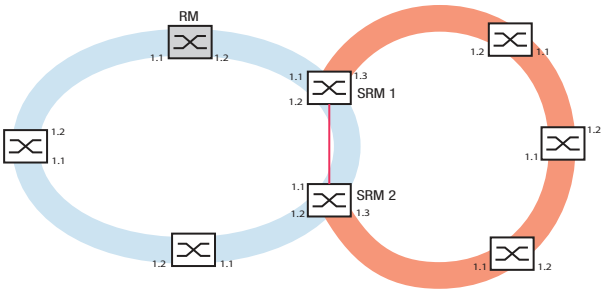


Abb. 51: Beispiel für eine Subring-Struktur
blauer Ring = Hauptring
oranger Ring = Subring
rote Linie = redundante Verbindung des Subrings
SRM = Subring-Manager
RM = Ring-Manager

Die Subring-Manager-fähigen Geräte unterstützen bis zu 8 Instanzen und verwalten daher bis zu 8 Subringe gleichzeitig.

Die Funktion *Sub Ring* ermöglicht Ihnen, MRP-fähige Geräte als Ring-Teilnehmer zu integrieren. Die Geräte, die den Subring an den Hauptring ankoppeln, benötigen die *Sub Ring*-Manager-Funktion.

Jeder Subring kann aus bis zu 200 Teilnehmern bestehen, zuzüglich den Subring-Managern und den Geräten zwischen den Subring-Managern im Hauptring.

Die folgenden Abbildungen zeigen Beispiele möglicher Subring-Topologien:

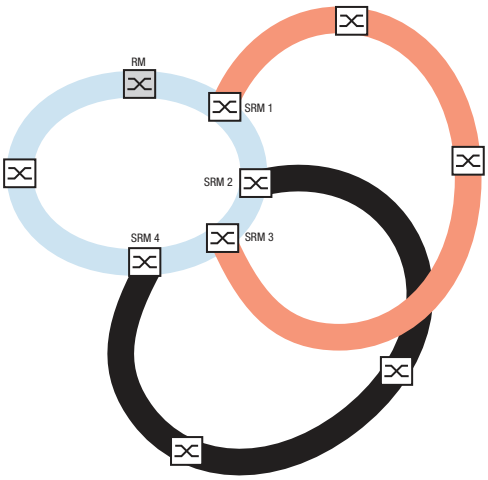


Abb. 52: Beispiel für eine überlappende Subring-Struktur

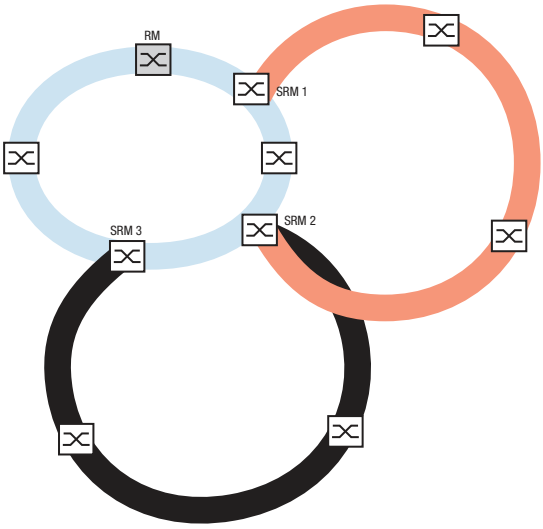


Abb. 53: Sonderfall: Ein Subring-Manager verwaltet 2 Subringe (2 Instanzen). Der Subring-Manager ist in der Lage, bis zu 8 Instanzen zu verwalten.

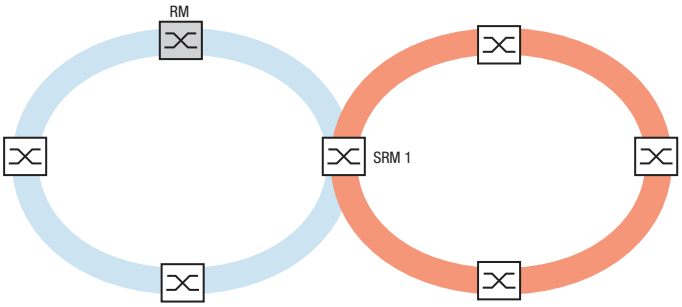


Abb. 54: Sonderfall: Ein Subring-Manager verwaltet beide Enden eines Subrings an unterschiedlichen Ports (Single-Subring-Manager).

Anmerkung: In den vorherigen Beispielen koppeln die Subring-Manager lediglich die Subringe an vorhandene Hauptringe an. Die Funktion *Sub Ring* verbietet kaskadierte Subringe, also das Ankoppeln eines Subrings an einen bereits vorhandenen Subring.

Wenn Sie MRP für den Hauptring und den Subring verwenden, legen Sie die VLAN-Einstellungen wie folgt fest:

- VLAN `X` für den Hauptring
  - auf den Ring-Ports der Hauptring-Teilnehmer
  - auf den Hauptring-Ports des Subring-Managers
- VLAN `Y` für den Subring
  - auf den Ring-Ports der Subring-Teilnehmer
  - auf den Subring-Ports des Subring-Managers

  Sie können dasselbe VLAN für verschiedene Subringe nutzen.

12.9.2 Beispiel für einen Subring

Im folgenden Beispiel koppeln Sie ein neues Netzsegment mit 3 Geräten an einen bestehenden Hauptring, der das MRP-Protokoll nutzt. Wenn Sie das Netz anstatt an einem Ende an beiden Enden koppeln, bietet der Subring eine höhere Verfügbarkeit.

Das neue Netzsegment koppeln Sie als Subring an. Den Subring koppeln Sie an vorhandene Geräte im Hauptring, indem Sie folgenden Konfigurationstypen verwenden:

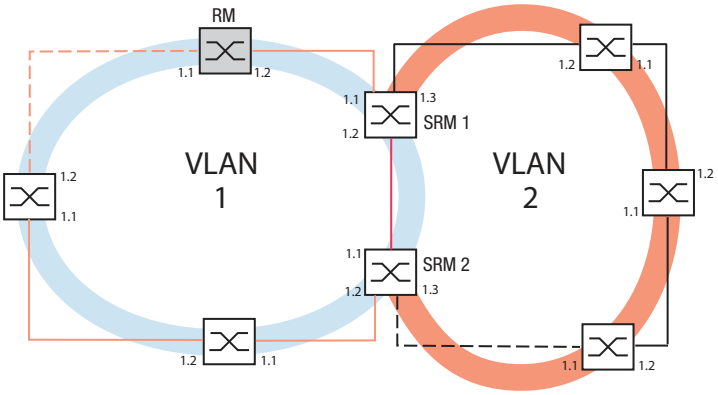


Abb. 55: Beispiel für eine Subring-Struktur
orangefarbene Linie = Mitglieder des Hauptrings in VLAN 1
schwarze Linie = Mitglieder des Subrings in VLAN 2
orange gestrichelte Linie = unterbrochenes Segment im Hauptring
schwarz gestrichelte Linie = unterbrochenes Segment im Subring
rote Linie = redundante Verbindung, Mitglied in VLAN 1
SRM = Subring-Manager
RM = Ring-Manager

Um den Subring zu konfigurieren, führen Sie die folgenden Schritte aus:

- ☐ Konfigurieren Sie die 3 Geräte des neuen Netzsegments als Teilnehmer in einem MRP-Ring:
  - Konfigurieren Sie die Übertragungsrate und den Duplex-Modus für die Ring-Ports gemäß der folgenden Tabelle:

Tab. 34: Port-Einstellungen für Subring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–

Die folgenden Schritte beinhalten zusätzliche Einstellungen für die Konfiguration von Subringen:

- Um die Möglichkeit von Loops während der Konfiguration zu verringern, deaktivieren Sie die Subring-Manager-Funktion für die Geräte im Hauptring und im Subring. Nachdem Sie jedes im Hauptring und in den Subringen teilnehmende Gerät vollständig konfiguriert haben, aktivieren Sie die globale Funktion *Sub Ring* und die Subring-Manager.
- Deaktivieren Sie die Funktion RSTP an den im Subring verwendeten MRP-Ring-Ports.
- Vergewissern Sie sich, dass die Funktion *Link-Aggregation* auf den Ports inaktiv ist, die im Hauptring und in den Subringen teilnehmen.
- Legen Sie für Hauptring-Ports und Subring-Ports unterschiedliche VLANs fest, wenn der Hauptring das MRP-Protokoll nutzt. Verwenden Sie zum Beispiel VLAN-ID `1` für den Hauptring und die Redundanzverbindung und anschließend VLAN-ID `2` für den Subring.
  - Für im Hauptring teilnehmende Geräte öffnen Sie den Dialog *Switching > VLAN > Konfiguration*. Erzeugen Sie VLAN `1` in der statischen VLAN-Tabelle. Markieren Sie die Hauptring-Ports zur Mitgliedschaft in VLAN `1`, indem Sie in der Dropdown-Liste der betreffenden Port-Spalten den Eintrag `T` auswählen.
  - Für die im Subring teilnehmenden Geräte wenden Sie die oben beschriebenen Schritte an und fügen die Ports in der statischen VLAN-Tabelle zu VLAN `2` hinzu.
- Aktivieren Sie die Funktion *MRP* für die Geräte im Hauptring und im Subring.
  - Im Dialog *Switching > L2-Redundanz > MRP* konfigurieren Sie die 2 im Hauptring teilnehmenden Ring-Ports an den Geräten des Hauptrings.
  - Für die im Subring teilnehmenden Geräte wenden Sie die oben beschriebenen Schritte an und konfigurieren die im Subring teilnehmenden 2 Ring-Ports an den Geräten des Subrings.
  - Weisen Sie den Geräten im Hauptring und im Subring dieselbe MRP-Domänen-ID zu. Wenn Sie ausschließlich Hirschmann-Geräte verwenden, dann genügen die voreingestellten Werte für die MRP-Domain-ID.

Anmerkung: Die *MRP-Domäne* ist eine Folge aus 16 Ziffernblöcken im Bereich zwischen `0` und `255`. Voreingestellt ist der Wert `255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255`. Eine ausschließlich aus Nullen bestehende *MRP-Domäne* ist ungültig.

Der *Sub Ring*-Dialog ermöglicht Ihnen, die MRP-Domain-ID bei Bedarf zu ändern. Alternativ benutzen Sie das Command Line Interface. Führen Sie dazu die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`mrp domain delete`	Aktuelle MRP-Domäne löschen.
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99`	Eine neue MRP-Domäne mit der festgelegten MRP-Domänen-ID erzeugen. Alle folgenden Änderungen der MRP-Domäne gelten für diese Domänen-ID.

12.9.3 Subring-Beispielkonfiguration

Anmerkung: Vermeiden Sie Loops während der Konfiguration. Konfigurieren Sie jedes Gerät des Subrings individuell. Konfigurieren Sie jedes Subring-Gerät vollständig, bevor Sie die Redundanzverbindung aktivieren.

Konfigurieren Sie die 2 Subring-Manager in dem Beispiel. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Sub Ring*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche ⊞.
- ☐ Wählen Sie in Spalte *Port* den Port, der das Gerät an den Subring koppelt.
  Verwenden Sie für dieses Beispiel Port *1/3*.
  Verwenden Sie für die Kopplung einen der verfügbaren Ports, mit Ausnahme der bereits mit dem Hauptring verbundenen Ports.
- ☐ Weisen Sie in Spalte *Name* dem Subring einen Namen zu.
  Geben Sie für dieses Beispiel `Test` ein.
- ☐ Wählen Sie in Spalte *SRM-Modus* den Subring-Manager-Modus.
  So legen Sie fest, welcher Port zur Kopplung des Sub-Rings an den Hauptring der redundante Port des Subring-Managers wird.
  Die Möglichkeiten der Kopplung sind:
  - ▶ `manager`
    Wenn Sie beiden Subring-Managern denselben Wert zuweisen, verwaltet das Gerät mit der höheren MAC-Adresse die Redundanzverbindung.
  - ▶ `redundant manager`
    Das Gerät verwaltet die Redundanzverbindung, solange Sie den anderen Subring-Manager als `manager` konfiguriert haben. Andernfalls ist das Gerät mit der höheren MAC-Adresse der Redundanz-Manager.

  Legen Sie entsprechend der Abbildung für dieses Beispiel den Subring-Manager 1 als `manager` fest.
- ☐ Lassen Sie die Werte in Spalte *VLAN* und in Spalte *MRP-Domäne* unverändert.
  Die voreingestellten Werte sind korrekt für die Beispielkonfiguration.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`sub-ring add 1`	Einen neuen Subring mit der Subring-ID `1` erzeugen.
`sub-ring modify 1 port 1/3`	Port *1/3* als Subring-Port festlegen.
`sub-ring modify 1 name Test`	Subring `Test` den Namen `1` zuweisen.
`sub-ring modify 1 mode manager`	Subring `manager` den Modus `1` zuweisen.
`show sub-ring ring`	Status der Subringe auf diesem Gerät anzeigen.
`show sub-ring global`	Globalen Status der Subringe auf diesem Gerät anzeigen.

- ☐ Konfigurieren Sie den 2. Subring-Manager entsprechend.
  Legen Sie entsprechend der Abbildung für dieses Beispiel den Subring-Manager 2 als `redundant manager` fest.

- ☐ Um die Subring-Manager-Funktion zu aktivieren, markieren Sie in den betreffenden Zeilen das Kontrollkästchen *Aktiv*.
- ☐ Nachdem Sie beide Subring-Manager und die im Subring teilnehmenden Geräte konfiguriert haben, schalten Sie die Funktion ein und schließen die Redundanzverbindung.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`sub-ring enable 1`	Subring `1` aktivieren.
`sub-ring enable 2`	Subring `2` aktivieren.
`exit`	In den Privileged-EXEC-Modus wechseln.
`show sub-ring ring <Domain ID>`	Einstellungen der ausgewählten Subringe anzeigen.
`show sub-ring global`	Globale Subring-Einstellungen anzeigen.
`copy config running-config nvm profile Test`	Aktuelle Einstellungen im Konfigurationsprofil mit der Bezeichnung `Test` im permanenten Speicher (`nvm`) speichern.

12.10 Subring mit LAG

Eine Link-Aggregation-Verbindung („LAG-Verbindung“) liegt vor, wenn zwischen 2 Geräten mindestens 2 parallele redundante Verbindungsleitungen („Trunks“) existieren und diese zu einer logischen Verbindung zusammengefasst werden.

Das Gerät ermöglicht Ihnen, die LAG-Ports als Ring-Ports mit dem *Sub Ring*-Protokoll zu verwenden.

12.10.1 Beispiel

Das folgende Beispiel beinhaltet eine einfache Einrichtung zwischen einem MRP-Ring und einem Subring.

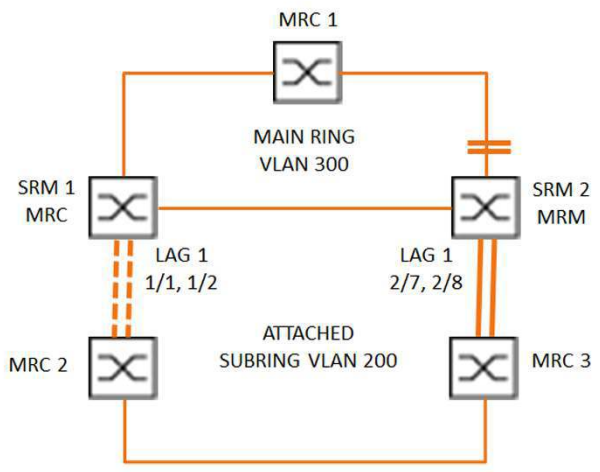


Abb. 56: Subring mit Link-Aggregation

Die folgende Tabelle beschreibt die in der obigen Abbildung dargestellten Geräterollen. Die Tabelle stellt Informationen zur Verwendung der Ring-Ports und Subring-Ports als LAG-Ports bereit.

Tab. 35: Geräte, Ports und Rollen

Gerätename	Ring-Port	Rolle des Haupt-rings	Rolle des Subrings	Subring-Port
MRC1	1/3, 1/4	MRP-Client	-	-
SRM1	1/3, 1/4	MRP-Client	Redundanz-Manager	lag/1
SRM2	2/4, 2/5	MRP-Manager	Manager	lag/1
MRC2	lag/1, 1/3	-	MRP-Client	-
MRC3	lag/1, 1/3	-	MRP-Client	-

MRP-Ring-Konfiguration

Die im Hauptring teilnehmenden Geräte sind Mitglieder von VLAN 300.

Führen Sie die folgenden Schritte aus:

SRM2

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`mrp domain add default-domain`	Eine neue MRP-Domäne mit der ID `default-domain` erzeugen.
`mrp domain modify port primary 2/4`	Port *2/4* als Ring-Port `1` festlegen.
`mrp domain modify port secondary 2/5`	Port *2/5* als Ring-Port `2` festlegen.
`mrp domain modify mode manager`	Festlegen, dass das Gerät als *Ring-Manager* arbeitet. Schalten Sie die Funktion *Ring-Manager* auf keinem weiteren Gerät ein.
`mrp domain modify operation enable`	MRP-Ring einschalten.
`mrp domain modify vlan 300`	Für die VLAN-ID `300` festlegen.
`mrp operation`	Funktion *MRP* auf dem Gerät einschalten.

MRC1, SRM1

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`mrp domain add default-domain`	Eine neue MRP-Domäne mit der ID `default-domain` erzeugen.
`mrp domain modify port primary 1/3`	Port *1/3* als Ring-Port `1` festlegen.
`mrp domain modify port secondary 1/4`	Port *1/4* als Ring-Port `2` festlegen.
`mrp domain modify mode client`	Für die Geräterolle Ring-Client festlegen.
`mrp domain modify operation enable`	MRP-Ring einschalten.
`mrp domain modify vlan 300`	Für die VLAN-ID `300` festlegen.
`mrp operation`	Funktion *MRP* auf dem Gerät einschalten.

Subring-Konfiguration

Die im verbundenen Subring teilnehmenden Geräte sind Mitglieder von VLAN 200.

Führen Sie die folgenden Schritte aus:

SRM1

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`link-aggregation add lag/1`	Eine Link-Aggregation-Gruppe `lag/1` erzeugen.

`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.
`link-aggregation modify lag/1 adminmode`	Link-Aggregation-Gruppe aktivieren.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`sub-ring add 1`	Einen neuen Subring mit der Subring-ID `1` erzeugen.
`sub-ring modify 1 name SRM1`	Subring `SRM1` den Namen `1` zuweisen.
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/1`	Dem Gerät die Rolle `Sub-ring redundant manager` in Subring `1` zuweisen. Wenn der Subring geschlossen ist, blockiert das Gerät den Ring-Port. Für die VLAN-ID der Domäne ist VLAN `200` festgelegt. Port `lag/1` ist als Mitglied in VLAN `200` festgelegt.
`sub-ring enable 1`	Subring `1` aktivieren.
`sub-ring operation`	Globale Subring-Manager-Funktion auf diesem Gerät aktivieren.

`SRM2`

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`link-aggregation add lag/1`	Eine Link-Aggregation-Gruppe `lag/1` erzeugen.
`link-aggregation modify lag/1 addport 2/7`	Port *2/7* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 addport 2/8`	Port *2/8* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 adminmode`	Link-Aggregation-Gruppe aktivieren.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`sub-ring add 1`	Einen neuen Subring mit der Subring-ID `1` erzeugen.
`sub-ring modify 1 mode manager vlan 200 port lag/1`	Dem Gerät die Rolle `Subring manager` in Subring `1` zuweisen. Für die VLAN-ID der Domäne ist VLAN `200` festgelegt. Port `lag/1` ist als Mitglied in VLAN `200` festgelegt.
`sub-ring modify 1 name SRM2`	Subring `SRM2` den Namen `1` zuweisen.
`sub-ring enable 1`	Subring `1` aktivieren.
`sub-ring operation`	Globale Subring-Manager-Funktion auf diesem Gerät aktivieren.

MRC 2, 3

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`mrp domain add default-domain`	Eine neue MRP-Domäne mit der ID `default-domain` erzeugen.
`mrp domain modify port primary lag/1`	Port `lag/1` als Ring-Port `1` festlegen.
`mrp domain modify port secondary 1/3`	Port *1/3* als Ring-Port `2` festlegen.
`mrp domain modify mode client`	Für die Geräterolle Ring-Client festlegen.
`mrp domain modify operation enable`	MRP-Ring einschalten.
`mrp domain modify vlan 200`	Für die VLAN-ID `200` festlegen.
`mrp operation`	Funktion *MRP* auf dem Gerät einschalten.

STP deaktivieren

Schalten Sie die Funktion *Spanning Tree* auf jedem Port aus, den Sie als MRP- oder Subring-Port festgelegt haben. Das folgende Beispiel verwendet Port *1/3*.

Führen Sie die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/3`	In den Interface-Konfigurationsmodus von Interface *1/3* wechseln.
`no spanning-tree operation`	Funktion *Spanning Tree* auf dem Port ausschalten.

12.11 Ring-/Netzkopplung

Die Funktion *Ring-/Netzkopplung* koppelt Ringe oder Netzsegmente redundant auf Basis eines Rings. *Ring-/Netzkopplung* verbindet 2 Ringe/Netzsegmente über 2 separate Pfade.

Wenn die Geräte im gekoppelten Netz Hirschmann-Geräte sind, unterstützt die Funktion *Ring-/Netzkopplung* die Kopplung gemäß den folgenden Ring-Protokollen im Primär-Ring und in den Sekundär-Ringen:

- HIPER-Ring
- Fast HIPER-Ring
- MRP

Die Funktion *Ring-/Netzkopplung* bietet auch die Möglichkeit zum Koppeln der Netzsegmente eines Bus und von Mesh-Strukturen.

12.11.1 Methoden der Ring-/Netzkopplung

1-Switch-Kopplung

2 Ports **eines** Geräts im 1. Ring/Netz stellen eine Verbindung zu jeweils einem Port der 2 Geräte im 2. Ring/Netz her. Siehe Abbildung 64 auf Seite 240.

Bei der Methode der 1-Switch-Kopplung leitet die Hauptleitung Daten weiter und das Gerät blockiert die redundante Leitung.

Falls die Hauptleitung ausfällt, hebt das Gerät die Blockierung der redundanten Leitung unverzüglich auf. Wenn die Hauptleitung wiederhergestellt ist, blockiert das Gerät die Daten auf der redundanten Leitung. Die Hauptleitung leitet die Daten wieder weiter.

Die Ring-Kopplung erkennt und bearbeitet Fehler innerhalb von 500 ms (in der Regel 150 ms).

2-Switch-Kopplung

Jeweils ein Port der **2** Geräte im 1. Ring/Netz stellt eine Verbindung zu jeweils einem Port der 2 Geräte im 2. Ring/Netzsegment her. Siehe Abbildung 66 auf Seite 243.

Um einander über den jeweiligen Betriebszustand zu informieren, verwenden das Gerät mit der redundanten Leitung und das Gerät mit der Hauptleitung Steuerpakete (über das Netzwerk oder über eine Steuerleitung).

Wenn die Hauptleitung ausfällt, hebt das redundante (Stand-By-) Gerät die Blockierung der redundanten Leitung auf. Wenn die Hauptleitung wiederhergestellt ist, informiert das mit der Hauptleitung verbundene Gerät das redundante Gerät darüber. Das Stand-by-Gerät blockiert dann wieder Daten auf der redundanten Leitung. Das an die Hauptleitung angeschlossene Gerät vermittelt dann wieder Daten auf der Hauptleitung.

Die Ring-Kopplung erkennt und behandelt einen Ausfall innerhalb von 500 ms (in der Regel 150 ms).

Auswahl einer Kopplungs-Methode

Die Art der Kopplungskonfiguration wird primär durch die Netzwerktopologie und den gewünschten Verfügbarkeitsgrad bestimmt.

Tab. 36: Auswahlkriterien für die Konfigurationsarten für die redundante Kopplung

	1-Switch-Kopplung	2-Switch-Kopplung	2-Switch-Kopplung mit Steuerleitung
Anwendung	Die 2 Geräte sind topologisch ungünstig verteilt. Ein Link zwischen den Geräten wäre bei einer 2-Switch-Kopplung daher aufwendig.	Die 2 Geräte sind topologisch günstig verteilt. Die Verlegung einer Steuerleitung wäre äußerst aufwendig.	Die 2 Geräte sind topologisch günstig verteilt. Die Verlegung einer Steuerleitung wäre nicht aufwendig.
Nachteil	Bei Ausfall des für die redundante Kopplung konfigurierten Switches ist keine Verbindung zwischen den Netzen mehr vorhanden.	Höherer Aufwand für die Verbindung der 2 Geräte mit dem Netz (im Vergleich zur 1-Switch-Kopplung).	Höherer Aufwand für die Verbindung der 2 Geräte mit dem Netz (im Vergleich zur 1-Switch-Kopplung und 2-Switch-Kopplung).
Vorteil	Weniger Aufwand für die Verbindung der 2 Geräte mit dem Netz (im Vergleich zur 2-Switch-Kopplung).	Falls eines der für die redundante Kopplung konfigurierten Geräte ausfällt, sind die gekoppelten Netze weiterhin verbunden.	Falls eines der für die redundante Kopplung konfigurierten Geräte ausfällt, sind die gekoppelten Netze weiterhin verbunden. Die Partnerermittlung zwischen den koppelnden Geräten erfolgt zuverlässiger und schneller als ohne Steuerleitung.

12.11.2 Erweiterte Informationen

Verbindungs-Topologie der 1-Switch-Kopplung

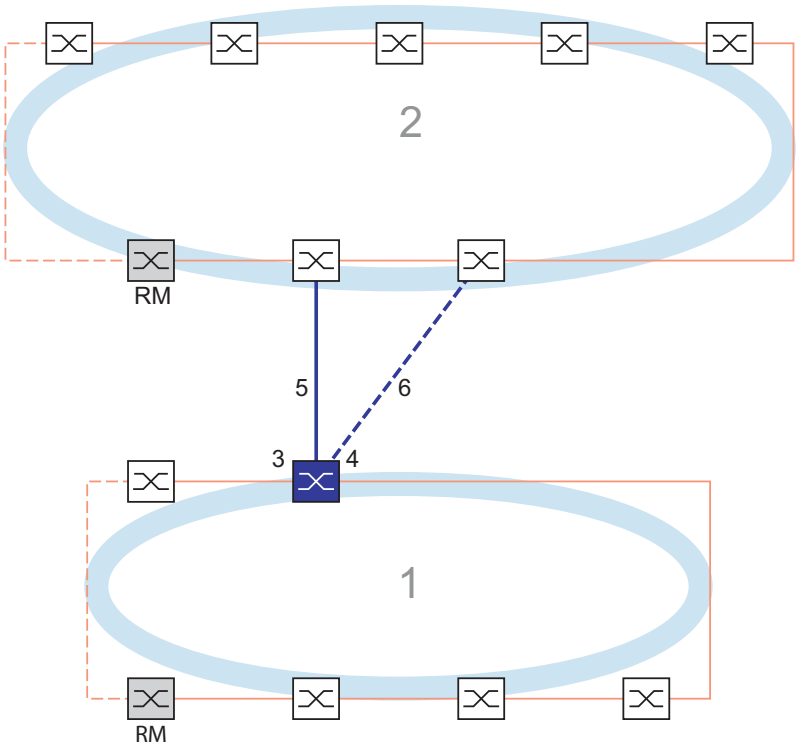


Abb. 57: Beispiel für die 1-Switch-Kopplung
1: Ring
2: Backbone
3: Partner-Kopplungs-Port
4: Kopplungs-Port
5: Hauptleitung
6: Redundante Leitung

Bei einer 1-Switch-Kopplung (siehe Abbildung 57) verwaltet ein Gerät beide Koppel-Leitungen:
- Der Partner-Kopplungsport (3) verbindet die Hauptleitung (5).
- Der Kopplungsport (4) verbindet die redundante Leitung (6).

Das einzelne Kopplungs-Gerät sendet die folgenden Testpakete:
- Der Partner-Kopplungsport (3) sendet *Ring-/Netzkopplung*-Unicast-Testpakete A.
- Der Kopplungsport (4) sendet *Ring-/Netzkopplung*-Unicast-Testpakete B.

Anmerkung: Die 2 Ring-Ports (nicht nummeriert) binden den lokalen redundanten Ring (rote Linien in Grafik) an und senden keine *Ring-/Netzkopplung*-Testpakete.

Verbindungs-Topologie der 2-Switch-Kopplung

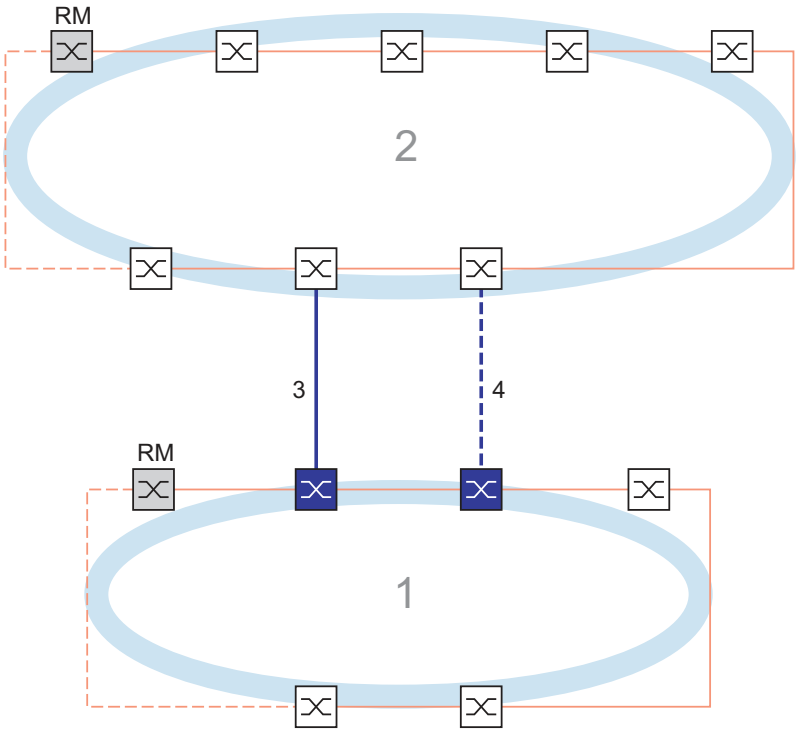


Abb. 58: Beispiel für die 2-Switch-Kopplung
1: Ring
2: Backbone
3: Hauptleitung
4: Redundante Leitung

In einer 2-Switch-Kopplung (siehe Abbildung 58) haben die 2 Geräte spezifische Rollen:
- Der Kopplungsport (1) des primären Geräts verbindet die Hauptleitung (siehe Abbildung 59).
- Der Partner-Kopplungsport (1) des sekundären Geräts verbindet die redundante (Stand-By-) Leitung (4) (siehe Abbildung 60).

Das primäre Gerät (siehe Abbildung 59) sendet keine Testpakete.

Das sekundäre Gerät (siehe Abbildung 60) sendet die folgenden Testpakete:
- Die 2 Ring-Ports (nicht nummeriert) senden *Ring-/Netzkopplung*-Unicast-Testpakete A.
- Der Kopplungsport (4) sendet *Ring-/Netzkopplung*-Unicast-Testpakete B.

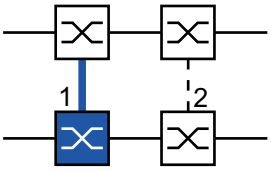


Abb. 59: 2-Switch-Kopplung, primäres Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port

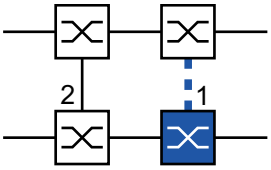


Abb. 60: 2-Switch-Kopplung, Standby-Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port

Verbindungs-Topologie der 2-Switch-Kopplung mit Steuerleitung

Diese Topologie unterscheidet sich von der vorhergehenden durch die zusätzliche Steuerleitung. Die Steuerleitung hilft, die Rekonfiguration zu beschleuningen.

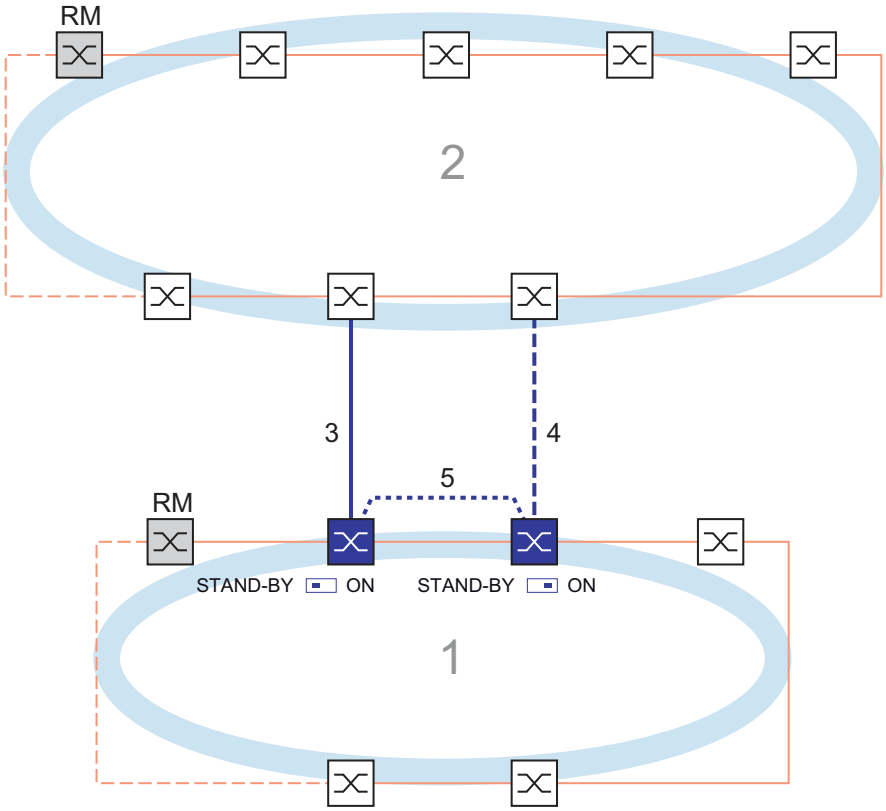


Abb. 61: Beispiel für die 2-Switch-Kopplung mit Steuerleitung
1: Ring
2: Backbone
3: Hauptleitung
4: Redundante Leitung
5: Steuerleitung

In einer 2-Switch-Kopplung mit Steuerleitung (siehe Abbildung 61) sind die 2 Geräte wie folgt verbunden:

- Das primäre und das sekundäre Gerät sind über ihre Steuer-Ports (nicht nummeriert) mit der Steuerleitung (5) verbunden.
- Der Kopplungsport (1) des primären Geräts verbindet die Hauptleitung (siehe Abbildung 62).
- Der Partner-Kopplungsport (1) des sekundären Geräts verbindet die redundante (Stand-By-) Leitung (4) (siehe Abbildung 63).

Das primäre Gerät (siehe Abbildung 62) sendet Steuerpakete an seinem Steuer-Port.

Das sekundäre Gerät (siehe Abbildung 63) sendet die folgenden Pakete:
- Der Steuer-Port (nicht nummeriert) sendet Steuerpakete.
- Die 2 Ring-Ports (nicht nummeriert) senden *Ring-/Netzkopplung*-Unicast-Testpakete A.
- Der Kopplungsport (4) sendet *Ring-/Netzkopplung*-Unicast-Testpakete B.

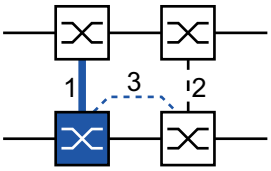


Abb. 62: 2-Switch-Kopplung mit Steuerleitung, primäres Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port
3: Steuerleitung

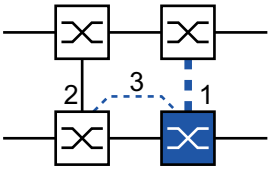


Abb. 63: 2-Switch-Kopplung mit Steuerleitung, Standby-Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port
3: Steuerleitung

Pakete

Das Protokoll *Ring-/Netzkopplung* verwendet Testpakete, Steuerpakete, Link-Change-Pakete und *Ring-/Netzkopplung*-Topologieänderungs-Pakete:

Tab. 37: Ring-/Netzkopplungs-Pakete

Paket-Typ	Sende-Modus	Zeit-Parameter	Wert
Unicast-Testpakete A[1]	Periodisch	Sende-Intervall	80 ms (50 ms während Konfigurationsphase)
		Empfangs-Zeitüberschreitung	1500 ms
Unicast-Testpaket B[2]	Periodisch	Sende-Intervall	80 ms (50 ms während Konfigurationsphase)
		Empfangs-Zeitüberschreitung	1500 ms
Steuerpaket[3]	Ereignis-getrieben	Bei Rekonfiguration	-
Link-Change-Paket[4]	Ereignis-getrieben	Bei Verbindungsausfall oder Verbindungs-Wiederherstellung an einem Ring-Port oder einem Kopplungs-Port	-
Ring-/Netzkopplung-Topologieänderungs-Paket	Ereignis-getrieben	Bei Rekonfiguration	-

1. 2-Switch-Kopplung: Ausschließlich vom sekundären (Stand-By-) Gerät gesendet. Zieladresse: Geräte-MAC-Adresse+1, Quelladresse: Geräte-MAC-Adresse+2.

2. 2-Switch-Kopplung: Ausschließlich vom sekundären (Stand-By-) Gerät gesendet. Zieladresse: Geräte-MAC-Adresse+2, Quelladresse: Geräte-MAC-Adresse+1 (Adressen vertauscht im Vergleich zum Unicast-Testpaket A).
3. Zieladresse (Multicast): 01:80:63:07:00:02, Quelladresse: 00:80:63:07:10:01.
4. Gesendet von unterstützenden Ring-Geräten.

1-Switch-Kopplung: Das lokale Gerät sendet periodisch Testpakete A von beiden Ring-Ports aus in den Ring. Das lokale Gerät erwartet den Rückempfang der Testpakete A an seinem jeweils anderen Ring-Port. Wenn das lokale Gerät für eine festgelegte Zeitspanne keine Testpakete A empfängt, erkennt das lokale Gerät einen Netz-Ausfall.

Das lokale Gerät sendet außerdem Testpakete B von seinem Partner-Kopplungs-Port. Die Testpakete B sind spezielle Pakete, die das lokale Gerät am Kopplungs-Port empfängt, obwohl der Kopplungs-Port den Empfang normaler Pakete blockiert. Das lokale Gerät erwartet den Rückempfang der Testpakete B an seinem Kopplungs-Port. Wenn das lokale Gerät für eine festgelegte Zeitspanne keine Testpakete B empfängt, erkennt das lokale Gerät einen Koppelnetz-Ausfall.

2-Switch-Kopplung: Das sekundäre (Stand-By-) Gerät sendet periodisch Testpakete A von beiden Ring-Ports aus in den Ring. Das sekundäre Gerät erwartet den Rückempfang der Testpakete A an seinem jeweils anderen Ring-Port. Wenn das sekundäre Gerät für eine festgelegte Zeitspanne keine Testpakete A empfängt, erkennt das sekundäre Gerät einen Netz-Ausfall.

Das sekundäre (Stand-By-) Gerät sendet außerdem Testpakete B von seinem Kopplungs-Port. Die Testpakete B sind spezielle Pakete, die das sekundäre Gerät vom Kopplungs-Port sendet, obwohl der Kopplungs-Port das Senden normaler Pakete blockiert. Das primäre Gerät leitet die empfangenen Testpakete B an das sekundäre Gerät weiter. Das sekundäre Gerät erwartet den Rückempfang der Testpakete B an seinem Ring-Port, der mit dem primären Gerät verbunden ist. Wenn das sekundäre Gerät für eine festgelegte Zeitspanne keine Testpakete B empfängt, erkennt das sekundäre Gerät einen Koppelnetz-Ausfall.

Im erweiterten Redundanz-Modus werden die gleichen Pakete verwendet, lediglich die Reaktion auf einen erkannten Netz-Ausfall unterscheidet sich.

Bei der Rekonfiguration der Ring-/Netzkopplung löscht das sekundäre (Stand-By-) Gerät seine Forwarding Database (FDB) und sendet Ring-/Netzkopplungs-Topologieänderungs-Pakete an sein Partner-Gerät. Es sendet außerdem Ring-/Netzkopplungs-Topologieänderungs-Pakete an die angeschlossenen Ringe.

Wenn ein Ring-Gerät in einem angeschlossenen Ring ein Ring-/Netzkopplungs-Topologieänderungs-Paket empfängt, löscht es seine FDB. Es konvertiert außerdem das Ring-/Netzkopplungs-Topologieänderungs-Paket in ein Ring-Topologieänderungs-Paket und sendet das Ring-Topologieänderungs-Paket weiter. Die Ring-Topologieänderungs-Pakete veranlassen die anderen Ring-Geräte dazu, ebenfalls ihre FDB zu löschen. Dies trifft auf alle Ringe zu, welche die Ring-/Netz-Kopplung verbindet. Dieses Verfahren hilft dabei, die Nutzlast-Pakete rascher über den neuen Pfad zu vermitteln.

Die Ring-/Netz-Kopplungs-Geräte reagieren außerdem auf Ring-Topology-Change-Pakete von einem Ring-Manager, weil die Ring-/Netz-Kopplungs-Geräte Mitglieder dieses Rings sind.

Paket-Priorisierung

Die Ring-/Netzkopplungs-Geräte senden ihre Testpakete, Steuerpakete, Link-Down- und Ring-/Netzkopplungs-Topologieänderungs-Pakete mit der festen VLAN-ID 1. In der Voreinstellung haben die Pakete kein VLAN-Tag und damit keine Prioritäts- (Class of Service-) Information. Um die Rekonfigurations-Zeit bei hoher Netzlast zu minimieren, können Sie diese Pakete mit VLAN-Tag und damit mit Prioritätsinformation versehen. Die Geräte senden und vermitteln die Pakete dann mit der IEEE 802.1Q Class of Service-Priorität 7 (Netz-Steuerung).

Um diese Pakete zu priorisieren, konfigurieren Sie jeden der folgenden Ports als `T` (Mitglied mit VLAN-Tag) von VLAN 1:

- Im lokalen Ring, in dem sich das Kopplungs-Gerät (oder die -Geräte) befinden:
  - Der Kopplungsport des jeweiligen Kopplungs-Geräts (lokal oder sekundär)
  - Der Partner-Kopplungsport des jeweiligen Kopplungs-Geräts (lokal oder primär)
  - Die Ring-Ports aller Geräten im lokalen Ring, inklusive des Ring-Managers
- Im entfernten Ring:
  - Der Port des Geräts im entfernten Ring, das mit dem Kopplungsport verbunden ist
  - Der Port des Geräts im entfernten Ring, das mit dem Partner-Kopplungsport verbunden ist
  - Die 2 Ring-Ports, welche die 2 eben erwähnten Geräte miteinander verbinden

Anmerkung: Bei einer 2-Switch-Kopplung mit Steuerleitung müssen die VLAN-Mitglieds-Einstellungen beider Steuerports übereinstimmen. Sie können die vorgegebenen Einstellungen der Steuerports beibehalten (Mitglied in VLAN 1, ohne VLAN-Tag).

Anforderungen an die Verbindungs-Topologie

Ohne Paket-Priorisierung müssen die folgenden Verbindungen direkt sein, ohne irgendwelche dazwischengeschaltete Geräte:

- Die 2 Kopplungs-Verbindungen, die das Kopplungs-Gerät (oder die -Geräte) im lokalen Ring mit den 2 gekoppelten Geräten im entfernten Ring verbinden
- Die Verbindung im entfernten Ring zwischen den 2 gekoppelten Geräten
- Bei einer 2-Switch-Kopplung: Die Verbindung im lokalen Ring zwischen den 2 Kopplungs-Geräten
- Bei einer 2-Switch-Kopplung mit Steuerleitung empfiehlt Hirschmann eine direkte Verbindung, wobei diese nicht zwingend erforderlich ist.

Dies hilft sicherzustellen, dass die Pakete mit minimaler Verzögerung und hoher Zuverlässigkeit übertragen werden. Dies hilft wiederum dabei, die Rekonfigurationszeit unter hoher Netzlast zu minimieren.

Anmerkung: Hirschmann empfiehlt die obige Verbindungs-Topologie auch bei Paket-Priorisierung.

12.11.3 Ring-/Netzkopplung vorbereiten

Legen Sie die Rolle der Geräte innerhalb der *Ring-/Netzkopplung* anhand der Abbildungen im Dialog fest.

Die folgenden Screenshots und Diagramme verwenden folgende Konventionen:

- Blaue Felder und Linien bezeichnen Geräte oder Verbindungen im gegenwärtigen Betrachtungsumfang.
- Durchgängige Linien stellen eine Hauptverbindung dar.
- Gestrichelte Linien stellen Standby-Verbindungen dar.
- Gepunktete Linien stellen die Steuerleitung dar.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das erforderliche Optionsfeld.
  - `Ein-Switch-Kopplung`
  - `Zwei-Switch-Kopplung, Master`
  - `Zwei-Switch-Kopplung, Slave`
  - `Zwei-Switch-Kopplung mit Steuer-Leitung, Master`
  - `Zwei-Switch-Kopplung mit Steuer-Leitung, Slave`

Anmerkung: Vermeiden Sie die Kombination des Rapid-Spanning-Tree-Protokolls und der *Ring-/Netzkopplung* auf den selben Ports.

1-Switch-Kopplung

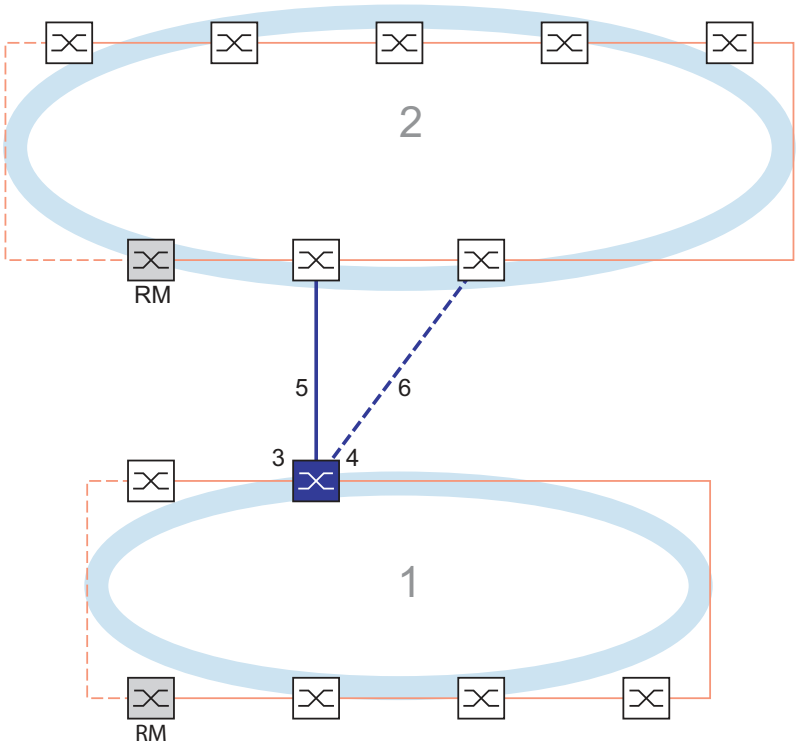


Abb. 64: Beispiel für die 1-Switch-Kopplung
1: Ring
2: Backbone
3: Partner-Kopplungs-Port
4: Kopplungs-Port
5: Hauptleitung
6: Redundante Leitung

Die durch die durchgängige blaue Linie gekennzeichnete Hauptleitung, die mit dem Partner-Kopplungs-Port verbunden ist, stellt die Kopplung zwischen den 2 Netzen im normalen Betriebsmodus her. Bei Ausfall der Hauptleitung übernimmt die durch die gestrichelte blaue Linie gekennzeichnete redundante Leitung, die mit dem Kopplungs-Port verbunden ist, die Ring-/Netzkopplung. **Ein** Switch nimmt die Kopplungsumschaltung vor.

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

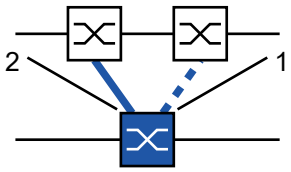


Abb. 65: 1-Switch-Kopplung
1: Kopplungs-Port
2: Partner-Kopplungs-Port

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld `Ein-Switch-Kopplung`.

Anmerkung: Konfigurieren Sie den *Partner-Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.

- ☐ Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die redundante Leitung anschließen möchten.
- ☐ Wählen Sie im Rahmen *Partner-Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Hauptleitung anschließen.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *An* das Optionsfeld *Funktion*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Verbinden Sie die redundante Leitung mit dem Partner-Kopplungs-Port.
  Das Feld *Partner-Kopplungs-Port* im Rahmen *Zustand* zeigt den Status des Partner-Kopplungs-Ports.
- ☐ Verbinden Sie die Hauptleitung mit dem Kopplungs-Port.
  Das Feld *Kopplungs-Port* im Rahmen *Zustand* zeigt den Status des Kopplungs-Ports.

Das Feld *Information* im Rahmen *Redundanz verfügbar* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

Anmerkung: Für die Kopplungs-Ports sind die folgenden Einstellungen erforderlich.

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Legen Sie für die Ports, die als Kopplungs-Ports ausgewählt sind, die Einstellungen gemäß der Parameter in der folgenden Tabelle fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Tab. 38: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–

Falls Sie VLANs an den Kopplungs-Ports konfiguriert haben, legen Sie die VLAN-Einstellungen für die Kopplungs- und Partner-Kopplungs-Ports fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Zum Taggen der redundanten Verbindungen für `VLAN 1` und für die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Das koppelnde Gerät sendet nun die Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Redundanz-Modus* den Redundanztyp:
  - ▶ Mit der Einstellung *Redundante Ring-/Netz-Kopplung* ist entweder die Hauptleitung oder die redundante Leitung aktiv. Die Einstellung ermöglicht den Geräten, zwischen beiden Leitungen umzuschalten.
  - ▶ Wenn Sie die Einstellung *Erweiterte Redundanz* aktivieren, können die Hauptleitung und die redundante Leitung gleichzeitig aktiv werden, falls erforderlich. Die Einstellung ermöglicht Ihnen, Redundanz zum entfernten (gekoppelten) Netz hinzuzufügen. Wenn die Verbindung zwischen den gekoppelten Geräten im 2. Netz unterbrochen wird, fahren die gekoppelten Geräte mit der Übertragung und dem Empfang von Daten fort.

Anmerkung: Während der Rekonfigurationszeit können Paketdoppelungen auftreten. Wählen Sie diese Einstellung daher nur, wenn Ihre Geräte Paketdoppelungen erkennen.

Der *Kopplungs-Modus* beschreibt den Typ des Backbone-Netzes, mit dem Sie das Ring-Netz verbinden. Siehe Abbildung 64 auf Seite 240.

- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Kopplungs-Modus* den Typ des zweiten Netzes:
  - ☐ Wenn Sie eine Verbindung zu einem Ring-Netz herstellen, wählen Sie das Optionsfeld *Ring-Kopplung*.
  - ☐ Wenn Sie eine Verbindung zu einer Bus- oder einer Maschen-Struktur herstellen, wählen Sie das Optionsfeld *Netz-Kopplung*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Sie können die Kopplungseinstellungen auf den Grundzustand zurücksetzen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche 🗑.

2-Switch-Kopplung

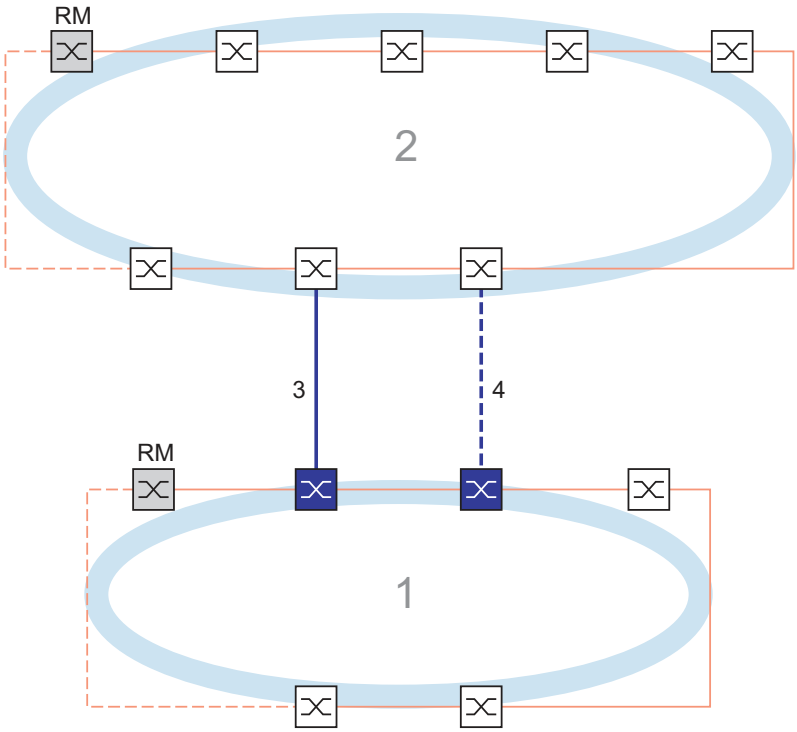


Abb. 66: Beispiel für die 2-Switch-Kopplung
1: Ring
2: Backbone
3: Hauptleitung
4: Redundante Leitung

Die Kopplung zwischen 2 Netzen erfolgt über die Hauptleitung, die durch die durchgängige blaue Linie gekennzeichnet ist. Wenn die Hauptleitung oder eines der daran angeschlossenen Geräte ausfällt, übernimmt die redundante Leitung, die durch die gestrichelte schwarze Linie gekennzeichnet ist, die Netzkopplung. Die Kopplung wird von 2 Geräten durchgeführt.

Die Geräte senden einander Kontrollpakete über das Netz.

Das an die Hauptleitung angeschlossene primäre Gerät und das an die redundante Leitung angeschlossene Standby-Gerät sind Partner in Bezug auf die Kopplung.
☐ Verbinden Sie die 2 Partner über die Ring-Ports.

2-Switch-Kopplung, primäres Gerät

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

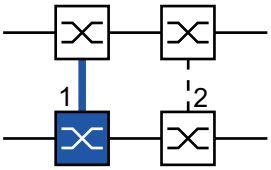


Abb. 67: 2-Switch-Kopplung, primäres Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld `Zwei-Switch-Kopplung, Master`.
- Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Netzsegmente anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *An* das Optionsfeld *Funktion*.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- Verbinden Sie die Hauptleitung mit dem *Kopplungs-Port*.
  Das Feld *Kopplungs-Port* im Rahmen *Zustand* zeigt den Status des Kopplungs-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

Das Feld *Information* im Rahmen *Redundanz verfügbar* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Um dauerhafte Loops zu vermeiden, während die Verbindungen an den Ring-Kopplungs-Ports aktiv sind, führen Sie eine der folgenden Aktionen aus. Das Gerät setzt den Port-Status des Kopplungs-Ports auf „aus“:
- Betrieb deaktivieren
- Konfiguration ändern

Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- Legen Sie für die Ports, die als Kopplungs-Ports ausgewählt sind, die Einstellungen gemäß der Parameter in der folgenden Tabelle fest.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Tab. 39: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–

Falls Sie VLANs an den Kopplungs-Ports konfiguriert haben, legen Sie die VLAN-Einstellungen für die Kopplungs- und Partner-Kopplungs-Ports fest. Führen Sie dazu die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > VLAN > Port*.
- Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.

- Zum Taggen der redundanten Verbindungen für `VLAN 1` und der Erzeugung der VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Das koppelnde Gerät sendet nun die Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

2-Switch-Kopplung, Standby-Gerät

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

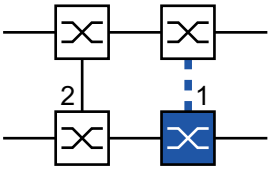


Abb. 68: 2-Switch-Kopplung, Standby-Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld `Zwei-Switch-Kopplung, Slave`.
- Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Netzsegmente anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *An* das Optionsfeld *Funktion*.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- Verbinden Sie die redundante Leitung mit dem *Kopplungs-Port*.
  Das Feld *Kopplungs-Port* im Rahmen *Zustand* zeigt den Status des Kopplungs-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

Das Feld *Information* im Rahmen *Redundanz verfügbar* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Um dauerhafte Loops zu vermeiden, während die Verbindungen an den Ring-Kopplungs-Ports aktiv sind, führen Sie eine der folgenden Aktionen aus. Das Gerät setzt den Port-Status des Kopplungs-Ports auf „aus“:
- Betrieb deaktivieren
- Konfiguration ändern

Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Legen Sie für die Ports, die als Kopplungs-Ports ausgewählt sind, die Einstellungen gemäß der Parameter in der folgenden Tabelle fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Tab. 40: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–

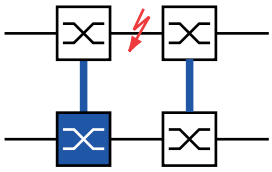
Falls Sie VLANs an den Kopplungs-Ports konfiguriert haben, legen Sie die VLAN-Einstellungen für die Kopplungs- und Partner-Kopplungs-Ports fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Zum Taggen der redundanten Verbindungen für `VLAN 1` und für die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Die koppelnden Geräte senden nun die Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

Legen Sie die *Redundanz-Modus*- und *Kopplungs-Modus*-Einstellungen fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Redundanz-Modus* eines der folgenden Optionsfelder.
  - ▶ `Redundante Ring-/Netz-Kopplung`
    Mit dieser Einstellung ist entweder die Hauptleitung oder die redundante Leitung aktiv. Die Einstellung ermöglicht den Geräten, zwischen beiden Leitungen umzuschalten.
  - ▶ `Erweiterte Redundanz`
    Mit dieser Einstellung sind die Hauptleitung und die redundante Leitung gleichzeitig aktiv. Die Einstellung ermöglicht Ihnen, Redundanz zum 2. Netz hinzuzufügen. Wenn die Verbindung zwischen den gekoppelten Geräten im 2. Netz unterbrochen wird, fahren die gekoppelten Geräte mit der Übertragung und dem Empfang von Daten fort.

    Während der Rekonfigurationszeit können Paketdoppelungen auftreten. Wählen Sie diese Einstellung daher nur, wenn Ihre Geräte Paketdoppelungen erkennen.
- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Kopplungs-Modus* eines der folgenden Optionsfelder.
  - ☐ Wenn Sie eine Verbindung zu einem Ring-Netz herstellen, wählen Sie das Optionsfeld *Ring-Kopplung*.
  - ☐ Wenn Sie eine Verbindung zu einer Bus- oder einer Maschen-Struktur herstellen, wählen Sie das Optionsfeld *Netz-Kopplung*.

  Der *Kopplungs-Modus* beschreibt den Typ des Backbone-Netzes, mit dem Sie das Ring-Netz verbinden. Siehe Abbildung 66 auf Seite 243.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Setzen Sie die Kopplungseinstellungen auf den Grundzustand zurück. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche 🗑.

2-Switch-Kopplung mit Steuerleitung

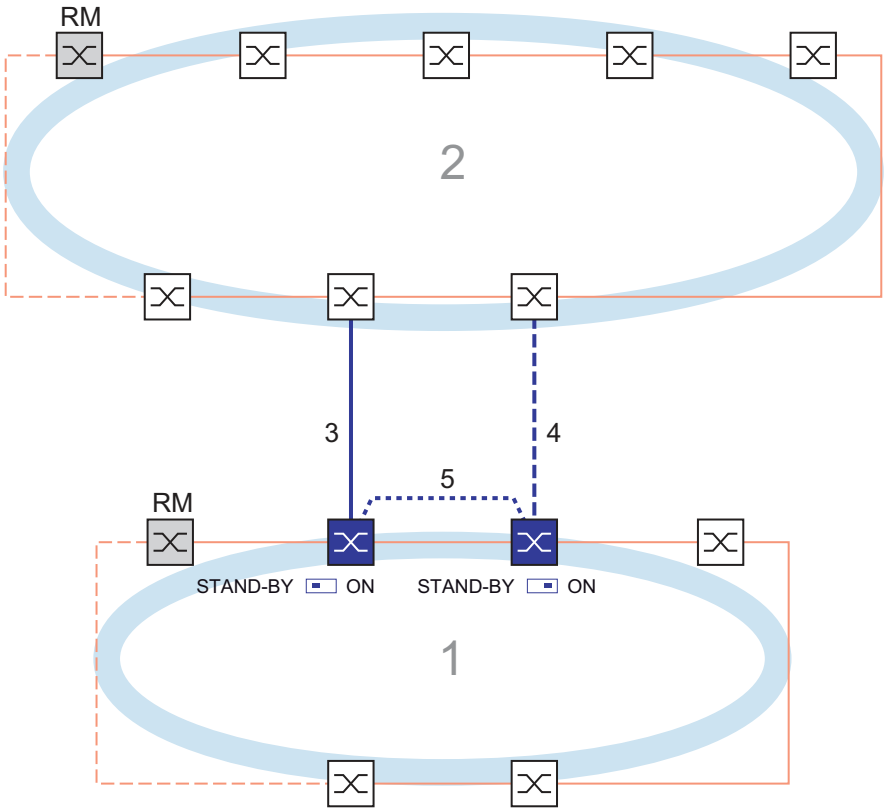


Abb. 69: Beispiel für die 2-Switch-Kopplung mit Steuerleitung
1: Ring
2: Backbone
3: Hauptleitung
4: Redundante Leitung
5: Steuerleitung

Die Kopplung zwischen 2 Netzen erfolgt über die Hauptleitung, die durch die durchgängige blaue Linie gekennzeichnet ist. Wenn die Hauptleitung oder eines der benachbarten Geräte ausfällt, übernimmt die redundante Leitung, die durch die gestrichelte blaue Linie gekennzeichnet ist, die Kopplung der 2 Netze. Die Ring-Kopplung wird von 2 Geräten durchgeführt.

Die Geräte senden Kontrollpakete über eine Steuerleitung, die in der folgenden Abbildung durch eine gepunktete blaue Linie gekennzeichnet ist. Siehe Abbildung 70 auf Seite 249.

Das an die Hauptleitung angeschlossene primäre Gerät und das an die redundante Leitung angeschlossene Standby-Gerät sind Partner in Bezug auf die Kopplung.
☐ Verbinden Sie die 2 Partner über die Ring-Ports.

2-Switch-Kopplung mit Steuerleitung, primäres Gerät

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

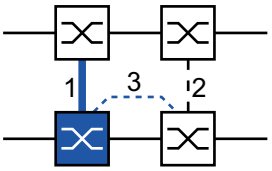


Abb. 70: 2-Switch-Kopplung mit Steuerleitung, primäres Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port
3: Steuerleitung

Führen Sie die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.

☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld `Zwei-Switch-Kopplung mit Steuer-Leitung, Master`.

☐ Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Netzsegmente anschließen.
Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.

☐ Wählen Sie im Rahmen *Steuer-Port*, Dropdown-Liste *Port* den Port, an den Sie die Steuerleitung anschließen.
Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.

☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *An* das Optionsfeld *Funktion*.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

☐ Verbinden Sie die redundante Leitung mit dem Kopplungs-Port.
Das Feld *Kopplungs-Port* im Rahmen *Zustand* zeigt den Status des Kopplungs-Ports.
Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

☐ Verbinden Sie die Steuerleitung mit dem Steuer-Port.
Das Feld *Steuer-Port* im Rahmen *Zustand* zeigt den Status des Steuer-Ports.
Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

Das Feld *Information* im Rahmen *Redundanz verfügbar* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Um dauerhafte Loops zu vermeiden, während die Verbindungen an den Ring-Kopplungs-Ports aktiv sind, führen Sie eine der folgenden Aktionen aus. Das Gerät setzt den Port-Status des Kopplungs-Ports auf „aus“:
- Betrieb deaktivieren
- Konfiguration ändern

Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- Legen Sie für die Ports, die als Kopplungs-Ports ausgewählt sind, die Einstellungen gemäß der Parameter in der folgenden Tabelle fest.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Tab. 41: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–

Falls Sie VLANs an den Kopplungs-Ports konfiguriert haben, legen Sie die VLAN-Einstellungen für die Kopplungs- und Partner-Kopplungs-Ports fest. Führen Sie dazu die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > VLAN > Port*.
- Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- Zum Taggen der redundanten Verbindungen für `VLAN 1` und für die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Das koppelnde Gerät sendet nun die Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

2-Switch-Kopplung mit Steuerleitung, Standby-Gerät

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

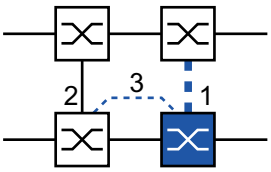


Abb. 71: 2-Switch-Kopplung mit Steuerleitung, Standby-Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port
3: Steuerleitung

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld `Zwei-Switch-Kopplung mit Steuer-Leitung, Slave`.
- ☐ Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Netzsegmente anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- ☐ Wählen Sie im Rahmen *Steuer-Port*, Dropdown-Liste *Port* den Port, an den Sie die Steuerleitung anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *An* das Optionsfeld *Funktion*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Verbinden Sie die redundante Leitung mit dem Kopplungs-Port.
  Das Feld *Kopplungs-Port* im Rahmen *Zustand* zeigt den Status des Kopplungs-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.
- ☐ Verbinden Sie die Steuerleitung mit dem Steuer-Port.
  Das Feld *Steuer-Port* im Rahmen *Zustand* zeigt den Status des Steuer-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

Das Feld *Information* im Rahmen *Redundanz verfügbar* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Um dauerhafte Loops zu vermeiden, während die Verbindungen an den Ring-Kopplungs-Ports aktiv sind, führen Sie eine der folgenden Aktionen aus. Das Gerät setzt den Port-Status des Kopplungs-Ports auf „aus“:

- Betrieb deaktivieren
- Konfiguration ändern

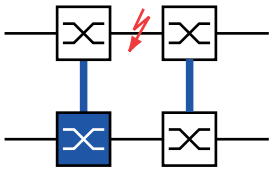
Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Zum Taggen der redundanten Verbindungen für `VLAN 1` und für die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Die koppelnden Geräte senden nun die Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

Legen Sie die *Redundanz-Modus*- und *Kopplungs-Modus*-Einstellungen fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Redundanz-Modus* eines der folgenden Optionsfelder.
  - ▶ `Redundante Ring-/Netz-Kopplung`
    Mit dieser Einstellung ist entweder die Hauptleitung oder die redundante Leitung aktiv. Die Einstellung ermöglicht den Geräten, zwischen beiden Leitungen umzuschalten.
  - ▶ `Erweiterte Redundanz`
    Mit dieser Einstellung sind die Hauptleitung und die redundante Leitung gleichzeitig aktiv. Die Einstellung ermöglicht Ihnen, Redundanz zum 2. Netz hinzuzufügen. Wenn die Verbindung zwischen den gekoppelten Geräten im 2. Netz unterbrochen wird, fahren die gekoppelten Geräte mit der Übertragung und dem Empfang von Daten fort.

    Während der Rekonfigurationszeit können Paketdoppelungen auftreten. Wählen Sie diese Einstellung daher nur, wenn Ihre Geräte Paketdoppelungen erkennen.
- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Kopplungs-Modus* eines der folgenden Optionsfelder.
  - ☐ Wenn Sie eine Verbindung zu einem Ring-Netz herstellen, wählen Sie das Optionsfeld *Ring-Kopplung*.
  - ☐ Wenn Sie eine Verbindung zu einer Bus- oder einer Maschen-Struktur herstellen, wählen Sie das Optionsfeld *Netz-Kopplung*.

  Der *Kopplungs-Modus* beschreibt den Typ des Backbone-Netzes, mit dem Sie das Ring-Netz verbinden. Siehe Abbildung 69 auf Seite 248.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Setzen Sie die Kopplungseinstellungen auf den Grundzustand zurück. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche 🗑.

12.12 RCP

Industrielle Anwendungen fordern von ihren Netzen eine hohe Verfügbarkeit. Dies beinhaltet deterministische, kurze Unterbrechungszeiten, wenn ein Netz-Gerät oder eine Netz-Verbindung ausfällt.

Eine Ringtopologie bietet kurze Übergangszeiten bei minimalem Ressourceneinsatz. Allerdings stellen Ringtopologien eine Herausforderung hinsichtlich der redundanten Kopplung dieser Ringe dar.

Das Redundant Coupling Protocol *RCP* ermöglicht Ihnen, Ringe zu koppeln, die mit einem der folgenden Redundanzprotokolle arbeiten:

- MRP
- HIPER-Ring
- RSTP

Die Funktion *RCP* ermöglicht Ihnen außerdem, mehrere Sekundär-Ringe mit einem Primär-Ring zu koppeln. Siehe folgende Abbildung. Ausschließlich die Geräte, welche die Ringe koppeln, benötigen die *RCP*-Funktion.

Innerhalb dieser gekoppelten Netzwerke können Sie auch Geräte verwenden, bei denen es sich nicht um Hirschmann-Geräte handelt.

Die Funktion *RCP* verwendet ein Master- und ein Slave-Gerät für die Übertragung von Daten zwischen den Netzen. Nur das Master-Gerät vermittelt Frames zwischen den Ringen.

Mittels proprietärer Hirschmann-Multicast-Nachrichten informieren die *RCP*-Master- und die Slave-Geräte einander über ihren jeweiligen Betriebsmodus. Konfigurieren Sie die Geräte im sekundären Ring, die keine Kopplungsgeräte sind, darauf, die folgenden Multicast-Adressen weiterzuleiten:

- `01:80:63:07:00:09`
- `01:80:63:07:00:0A`

Verbinden Sie die Master- und Slave-Geräte als direkte Nachbarn.

Um die redundante Kopplung herzustellen, verwenden Sie 4 Ports je Gerät. Konfigurieren Sie die gekoppelten Geräte mit 2 inneren Ports und 2 äußeren Ports in jedem Netz.

- Die inneren Ports stellen eine Verbindung zwischen den Master- und den Slave-Geräten her.
- Die äußeren Ports verbinden die Geräte mit den anderen, benachbarten Geräten im Netz.

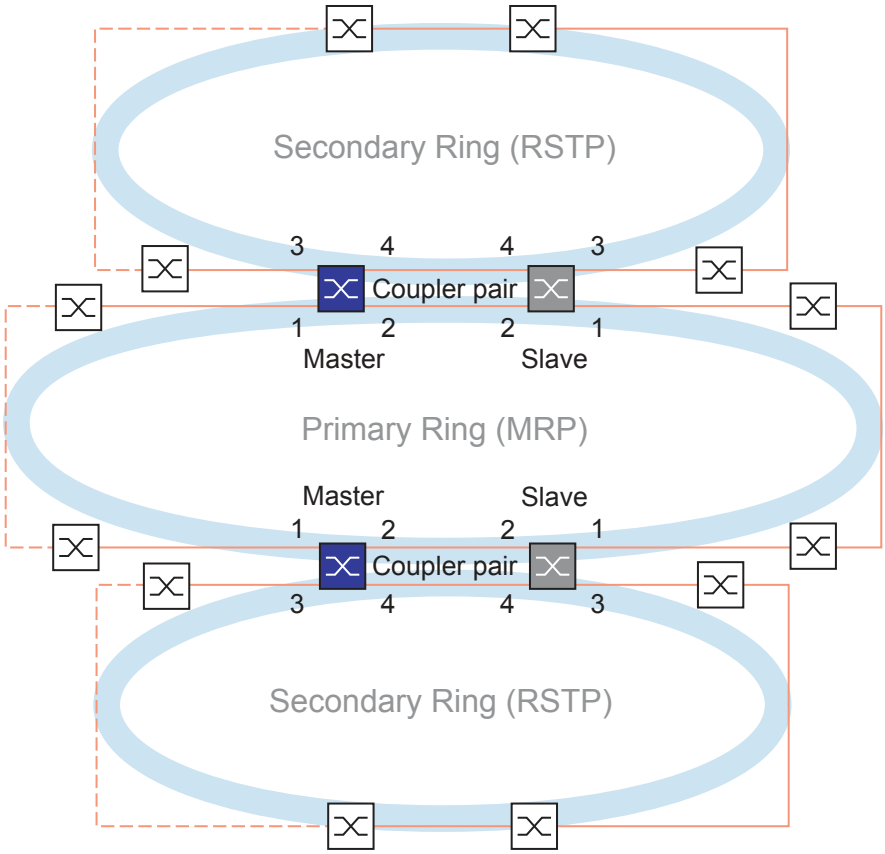


Abb. 72: Beispiel einer redundanten 2-Switch-Kopplung (2 Kopplerpaare)
1: Äußerer Kopplungs-Port im Primär-Ring
2: Innerer Kopplungs-Port im Primär-Ring
3: Äußerer Kopplungs-Port im Sekundär-Ring
4: Innerer Kopplungs-Port im Sekundär-Ring

Wenn Sie die Rolle des koppelnden Geräts als *auto* festlegen, wählt das koppelnde Gerät seine Rolle als *master* oder *slave* automatisch. Wenn Sie ein vorgegebenes Master- oder Slave-Gerät möchten, konfigurieren Sie die Rollen explizit.

Wenn das Master-Gerät nicht mehr über die inneren Kopplungs-Ports erreichbar ist, wartet das Slave-Gerät bis zum Ablauf eines festgelegten Timeout-Zeitraums, bevor es die Master-Rolle übernimmt. Während des Timeout-Zeitraums versucht das Slave-Gerät, das Master-Gerät mit Hilfe der äußeren Kopplungs-Ports zu erreichen. Wenn das Master-Gerät immer noch unerreichbar ist, übernimmt das Slave-Gerät die Master-Rolle. Um die Stabilität des Netzes zu erhalten, das mit den äußeren Kopplungs-Ports verbunden ist, konfigurieren Sie den Timeout-Zeitraum so, dass dieser länger ist als der Recovery-Zeitraum der gekoppelten Ringe.

Anmerkung: Deaktivieren Sie RSTP an den inneren und äußeren *RCP*-Ports für die redundante Kopplung, die nicht mit dem RSTP-Ring verbunden sind. In der Beispielkonfiguration deaktivieren Sie RSTP an den Ports 1 und 2 jedes Geräts.

12.12.1 Voraussetzungen für RCP

Voraussetzung für das Einrichten eines RCP-Kopplerpaars ist, dass jedes Gerät im Netz (neben dem Kopplerpaar) die Weiterleitung von Multicast-Paketen ohne VLAN-Tag unterstützt.

12.12.2 Erweiterte Informationen

Topologieübersicht

RCP unterstützt die folgende Topologie:
- 2-Switch-Redundante Kopplung

Anmerkung: Für ein Topologie-Beispiel mit 2 Instanzen einer 2-Switch-Redundanten Kopplung (siehe Abbildung 72).

Diese Topologie hat die folgenden Eigenschaften:
- Jedes RCP-Gerät hat 2 interne Netz-Segmente;
  - Ein Primär-Segment
  - Ein Sekundär-Segment
- Im Normalbetrieb behandelt das RCP-Gerät Pakete, die zwischen diesen 2 Netz-Segmenten unterwegs sind, wie folgt:
  - Das RCP-Master-Gerät leitet Pakete zwischen den 2 Netz-Segmenten weiter.
  - Das RCP-Slave-Gerät leitet **keine** Pakete zwischen den 2 Netz-Segmenten weiter.
- Port-Zuordnungen:
  - Nur diejenigen Ports, die explizit als innere oder äußere RCP-Ports für das Sekundär-Segment konfiguriert sind, gehören zu dem RCP-Sekundär-Segment des Geräts.
  - Die inneren und äußeren RCP-Ports für das Primär-Segment gehören zum RCP-Primär-Segment.
  - Alle anderen Ports gehören implizit zum RCP-Primär-Segment.
- Das Management eines RCP-Geräts befindet sich immer im Primär-Segment.

Anmerkung: Wenn Sie auf das Management eines RCP-Slave-Geräts vom Sekundär-Segment aus zugreifen möchten, vermeiden Sie die portbasierte Routing-Funktion auf den äußeren Ports für das Sekundär-Segment. Dies hilft dabei, den Management-Zugriff auf das Gerät vom Sekundär-Segment aus aufrecht zu erhalten.

Topologie der 2-Switch-Redundanten Kopplung

Bei einer 2-Switch-Redundanten Kopplung koppelt ein Geräte-Paar die 2 Ringe. Jedes der gepaarten Geräte hat eine eindeutige Kopplungs-Rolle, Master oder Slave, die entweder automatisch oder explizit konfiguriert ist.

Die Geräte sind wie folgt verbunden (siehe Abbildung 72):
- Die Ring-Ports (1) von beiden Geräten sind mit dem primären Ring/Netz verbunden. Diese Ports sind die äußeren Ports für das Primär-Netz.
- Die Ring-Ports (2) von beiden Geräten verbinden einander für das primäre Ring/Netz. Diese Ports sind die inneren Ports für das Primär-Netz.
- Die Ring-Ports (3) von beiden Geräten sind mit dem sekundären Ring/Netz verbunden. Diese Ports sind die äußeren Ports für das Sekundär-Netz.
- Die Ring-Ports (4) von beiden Geräten verbinden einander für den sekundären Ring. Diese Ports sind die inneren Ports für das Sekundär-Netz.

Pakete

RCP verwendet Multicast-Testpakete, die nach der RCP-Rollen-Nummer (1..4) des sendenden Ports benannt sind.

Tab. 42: RCP-Pakete

Paket-Typ	Betriebszustand	Zeit-Parameter	Wert
Testpakete 2 und 4 (auf den inneren Ports)	Normalbetrieb der inneren Ports	Sende-Intervall	45 ms
		Zeitüberschreitung beim Empfang[1]	180 ms (4 Sendeintervalle, fest)
Testpakete 1 und 3 (auf den äußeren Ports)	Bei Verbindungs-verlust an den inneren Ports	Sende-Intervall	10 ms (während der ersten 90 ms des Empfangs-Timeouts) 5 ms (nachdem 90 ms des Empfangs-Timeouts verstrichen sind)
		Topologieände-rungs-Timeout[2]	5 ms..60000 ms (einstellbar, Vorein-stellung: 250 ms)

1. Der Slave behandelt die Zeitüberschreitung beim Empfang als Verbindungsausfall des betreffenden Ports, selbst wenn der Port noch eine Verbindung hat.
2. Nach dem Feststellen einer Verbindungsunterbrechung wartet das Slave-Gerät den Topologieänderungs-Timeout ab, bevor es Pakete zwischen den 2 Netzwerk-Segmenten weiterleitet.

Anforderungen an die Verbindungs-Topologie

Die folgenden Verbindungen müssen direkt sein, ohne irgendwelche dazwischengeschaltete Geräte:

- Die 2 Verbindungen, welche die inneren Ports (2, 4) jedes Koppler-Paars in den jeweiligen Primär- und Sekundär-Ringen verbinden.

Dies hilft sicherzustellen, dass eine Verbindungsunterbrechung von den RCP-Geräten rasch erkannt wird.

12.12.3 Anwendungsbeispiel für RCP-Kopplung

Die Hirschmann-Geräte unterstützen die 2-Switch-Redundant-Coupling-Protocol-Methode. Um beispielsweise ein Netz zur Verfügung zu stellen, das in einem Zug installiert ist, können Sie die Funktion *RCP* verwenden. Das Netz stellt Fahrgästen Informationen zum Zugstandort oder zu den verschiedenen Bahnhöfen auf der Strecke bereit. Das Netz kann auch zur Sicherheit der Fahrgäste beitragen, zum Beispiel mittels Videoüberwachung.

Die Primär-Ringe in der Abbildung repräsentieren einen *MRP*-Ring innerhalb jedes Waggons. Jeder Primär-Ring besteht aus 4 Geräten. Siehe folgende Abbildung.

Die Sekundär-Ringe in der Abbildung repräsentieren RSTP-Ringe, die sich automatisch bilden, wenn 2 Waggons gekoppelt werden. Jeder Sekundär-Ring besteht aus 2 Koppler-Paaren, die über ihre jeweiligen äußeren Ports miteinander verbunden sind. In der Abbildung werden diese Geräte-Vierfache als Koppler A und B bezeichnet.

Um die Port-Konfiguration zu vereinfachen, werden den *MRP*-Ring-Ports und den inneren und äußeren *RCP*-Ports auf jedem Switch die selben Port-Nummern zugewiesen. Zum Beispiel legen Sie auf den Switches 2A..2D die Ports *2/1* und *2/2* als MRP-Ring-Ports fest, die Ports *2/4* als innere *RCP*-Ports und die Ports *2/3* als äußere *RCP*-Ports.

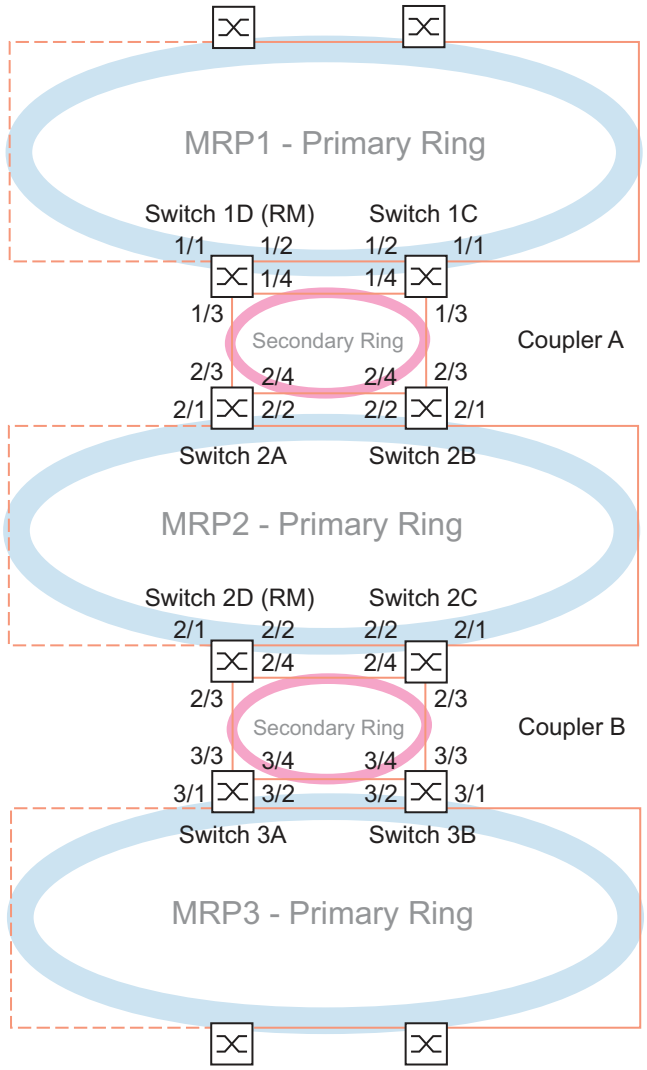


Abb. 73: Redundant Coupling Protocol-Zugtopologie:
- Ports x/1 und x/2 sind MRP-Ring-Ports
- Ports x/3 sind äußere RCP-Ports
- Ports x/4 sind äußere RCP-Ports

Die folgenden Schritte beschreiben, wie Sie die Parameter für den Waggon festlegen, der durch den MRP2-Ring repräsentiert wird.

Konfigurieren Sie die Switches 2A..2C als MRP-Ringteilnehmer. Konfigurieren Sie ausschließlich Switch 2D als MRP-Ringmanager. Konfigurieren Sie die Switches 2A und 2B als ein RCP-Koppler-Paar und die Switches 2C und 2D als das zweite Koppler-Paar.

Die RSTP-Funktion an den MRP-Ring-Ports abschalten

MRP und RSTP funktionieren nicht zusammen. Deaktivieren Sie daher die Funktion RSTP an den *RCP*-Ports, die im *MRP*-Ring verwendet werden. In der Beispielkonfiguration werden Ports `x/1` und `x/2` für den *MRP*-Ring verwendet. Aktivieren Sie die Funktion RSTP ausschließlich an den inneren und äußeren *RCP*-Ports, die im Sekundär-Ring verwendet werden. Aktivieren Sie die Funktion RSTP beispielsweise an den Ports `x/3` und `x/4`.

Anmerkung: Ersetzen sie die Beispiel-Portbezeichnung wie `x/1` mit den tatsächlichen Port-Nummern in Ihrem System. Abhängig von Ihrem Gerät kann die Portbezeichnung ausschließlich aus der Port-Nummer bestehen.

Führen Sie die folgenden Schritte auf den Switches 2A..2D aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*.
- ☐ In der Voreinstellung ist die Funktion RSTP an den Ports aktiviert. Um die Funktion RSTP an den *MRP*-Ring-Ports zu deaktivieren, heben Sie die Markierung des Kontrollkästchens *STP aktiv* für Port `x/1` und Port `x/2` auf.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Um die *Spanning Tree*-Funktion einzuschalten, wählen Sie das Optionsfeld *An* im Rahmen *Funktion*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface x/1`	In den Interface-Konfigurationsmodus von Interface `x/1` wechseln.
`no spanning-tree mode`	Funktion *Spanning Tree* auf dem Port ausschalten.
`exit`	In den Konfigurationsmodus wechseln.
`interface x/2`	In den Interface-Konfigurationsmodus von Interface `x/2` wechseln.
`no spanning-tree mode`	Funktion *Spanning Tree* auf dem Port ausschalten.
`exit`	In den Konfigurationsmodus wechseln.
`spanning-tree operation`	Funktion *Spanning Tree* einschalten.

Festlegen der Ringteilnehmer und des Ring-Managers im MRP-Ring

Legen Sie die Switches 2A..2C in den *MRP*-Ringen als Ringteilnehmer fest. Legen Sie Switch 2D als den *MRP*-Ring-Manager fest. Siehe Abbildung 73 auf Seite 257.

Legen Sie die anderen Switches in den Ringen als Ring-Clients fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > MRP*.
- ☐ Legen Sie den 1. Ring-Port im Rahmen *Ring-Port 1* fest.
  Wählen Sie in der Dropdown-Liste *Port* den Port `x/1`.
- ☐ Legen Sie den 2. Ring-Port im Rahmen *Ring-Port 2* fest.
  Wählen Sie in der Dropdown-Liste *Port* den Port `x/2`.

- ☐ Ausschließlich auf Switch 2D: Um das Gerät als *MRP*-Ring-Manager zu kennzeichnen, schalten Sie die Funktion *Ring-Manager* ein. Für die Switches 2A..2C belassen Sie die Voreinstellung.
- ☐ Um die *MRP*-Funktion einzuschalten, wählen Sie das Optionsfeld *An* im Rahmen *Funktion*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`mrp domain add default-domain`	Eine neue *MRP*-Domäne mit der ID `default-domain` erzeugen.
`mrp domain modify port primary x/1`	Port `x/1` als Ring-Port `1` festlegen.
`mrp domain modify port secondary x/2`	Port `x/2` als Ring-Port `2` festlegen.
`mrp domain modify mode manager`	Ausschließlich auf Switch 2D: Festlegen, dass das Gerät als der *Ring-Manager* arbeitet. Für die Switches 2A..2C belassen Sie die Voreinstellung.
`mrp domain modify operation enable`	Funktion *MRP* einschalten.

Die Ports für die RCP-Koppler-Paare festlegen

Anmerkung: Das Beispiel belässt die Rollen der Koppler-Paar-Geräte bei dem voreingestellten Wert *auto*. Die Koppler-Paar-Geräte wählen dann automatisch ihre Rollen als *master* oder *slave*. Wenn Sie vorgegebene Master- oder Slave-Rollen für ein Geräte-Paar haben möchten, konfigurieren Sie die Rollen explizit.

Führen Sie die folgenden Schritte auf den Switches 2A..2D aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > RCP*.
- ☐ Legen Sie den *Innerer Port* im Rahmen *Primärer Ring/Netzwerk* fest. Wählen Sie Port `x/2`.
- ☐ Legen Sie den *Äußerer Port* im Rahmen *Primärer Ring/Netzwerk* fest. Wählen Sie Port `x/1`.
- ☐ Legen Sie den *Innerer Port* im Rahmen *Sekundärer Ring/Netzwerk* fest. Wählen Sie Port `x/4`.
- ☐ Legen Sie den *Äußerer Port* im Rahmen *Sekundärer Ring/Netzwerk* fest. Wählen Sie Port `x/3`.

- ☐ Um die *RCP*-Funktion einzuschalten, wählen Sie das Optionsfeld *An* im Rahmen *Funktion*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`redundant-coupling port primary inner x/2`	Port `x/2` als primären inneren Port festlegen.
`redundant-coupling port primary outer x/1`	Port `x/1` als primären äußeren Port festlegen.

`redundant-coupling port secondary inner x/4`	Port `x/4` als sekundären inneren Port festlegen.
`redundant-coupling port secondary outer x/3`	Port `x/3` als sekundären äußeren Port festlegen.
`redundant-coupling operation`	Funktion *RCP* auf dem Gerät einschalten.

13 Funktionsdiagnose

Das Gerät bietet Ihnen folgende Diagnosewerkzeuge:
- SNMP-Traps senden
- Gerätestatus überwachen
- Out-of-Band-Signalisierung durch Signalkontakt
- Ereigniszähler auf Portebene
- Erkennen der Nichtübereinstimmung der Duplex-Modi
- Auto-Disable
- SFP-Zustandsanzeige
- Topologie-Erkennung
- IP-Adresskonflikte erkennen
- Erkennen von Loops
- Unterstützung beim Schutz vor Layer-2-Loops
- 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 ermöglicht Ihnen, 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:

Tab. 43: Mögliche SNMP-Traps

Bezeichnung des SNMP-Traps	Bedeutung
`authenticationFailure`	Wird gesendet, wenn eine Station versucht, unberechtigt auf einen Agenten zuzugreifen.
`coldStart`	Wird nach einem Neustart gesendet.
`hm2DevMonSenseExtNvmRe-moval`	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.
`hm2AgentPortSecurityViola-tion`	Wird gesendet, wenn eine an diesem Port erkannte MAC-Adresse nicht den aktuellen Einstellungen des Parameters `hm2AgentPortSecurityEntry` entspricht.
`hm2DiagSelftestActionTrap`	Wird gesendet, wenn ein Selbsttest gemäß der konfigurierten Einstellungen für die vier Kategorien „Aufgabe“, „Ressource“, „Software“ und „Hardware“ durchgeführt wird.
`hm2MrpReconfig`	Wird gesendet, wenn sich die Konfiguration des MRP-Rings ändert.
`hm2DiagIfaceUtilization-Trap`	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.
`hm2PtpSynchronization-Chance`	Wird gesendet, wenn der Status der PTP-Synchronisation geändert wird.
`hm2ConfigurationSavedTrap`	Wird gesendet, nachdem das Gerät seine Konfiguration erfolgreich lokal gespeichert hat.
`hm2ConfigurationChanged-Trap`	Wird gesendet, wenn Sie die Konfiguration des Geräts nach dem lokalen Speichern erstmalig ändern.
`hm2PlatformStpInstanceLoo-pInconsistentStartTrap`	Wird gesendet, wenn der Port in dieser STP-Instanz in den Status „loop inconsistent“ geht.
`hm2PlatformStpInstanceLoo-pInconsistentEndTrap`	Wird gesendet, wenn der Port in dieser STP-Instanz bei Empfang eines BPDU-Pakets den Status „loop inconsistent“ verlässt.

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 Speichers (*ENVM*), die angeben, ob die aktuelle Konfiguration mit dem nichtflüchtigen Speicher und dem externen Speicher 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 ermöglicht Ihnen, als Reaktion auf bestimmte Ereignisse einen SNMP-Trap zu senden. Legen Sie mindestens ein 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Das Auslösen eines SNMP-Traps legen Sie zum Beispiel in den folgenden Dialogen fest:

- Dialog *Grundeinstellungen > Port*
- Dialog *Grundeinstellungen > Power over Ethernet > Global*
- 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*
- Dialog *Erweitert > Digital-IO Modul*

13.1.4 ICMP-Messaging

Das Gerät ermöglicht Ihnen, 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.

13.2 Gerätestatus überwachen

Der Gerätestatus gibt einen Überblick über den Gesamtzustand des Geräts. Viele Prozessvisualisierungssysteme erfassen den Gerätestatus 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 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* ermöglicht Ihnen, 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
- Wenn das Gerät außerhalb der benutzerdefinierten Temperaturschwellwerte arbeitet
- 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 im externen Speicher stimmt nicht mit der Konfiguration 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.

13.2.1 Ereignisse, die überwacht werden können

Tab. 44: 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* markiert ist.
Temperatur	Aktivieren Sie diese Funktion, um zu überwachen, ob die Temperatur die festgelegten Schwellwerte überschreitet oder unterschreitet.
Ethernet-Modul entfernen	Aktivieren Sie diese Funktion, um das Entfernen eines Moduls zu überwachen. Aktivieren Sie außerdem das jeweilige zu überwachende Modul.

Tab. 44: Gerätestatus-Ereignisse (Forts.)

Name	Bedeutung
Externen Speicher entfernen	Aktivieren Sie diese Funktion, um das Vorhandensein eines externen Speichergeräts zu überwachen.
Externer Speicher nicht synchron	Das Gerät überwacht die Synchronisation zwischen der Gerätekonfiguration und der im externen Speicher (*ENVM*) gespeicherten Konfiguration.
Ring-Redundanz	Aktivieren Sie diese Funktion, um das Vorhandensein der Ring-Redundanz zu überwachen.
Netzteil	Aktivieren Sie diese Funktion, um das Netzteil zu überwachen.

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 ein Trap-Ziel fest, das SNMP-Traps empfängt.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.
- ☐ Um die Temperatur zu überwachen, legen Sie im Rahmen *Systemdaten* die Temperaturschwellwerte fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`device-status trap`	Einen SNMP-Trap senden, wenn sich der Gerätestatus ändert.
`device-status monitor envm-not-in-sync`	Konfigurationsprofile im Gerät und im externen Speicher überwachen. In folgenden Situationen wechselt der *Geräte-Status* auf `error`: • Das Konfigurationsprofil existiert ausschließlich im Gerät. • Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher.
`device-status monitor envm-removal`	Aktiven externen Speicher überwachen. 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`	Netzteil `1` überwachen. Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn das Gerät einen Fehler am Netzteil feststellt.

`device-status monitor ring-redundancy`	Ring-Redundanz überwachen. In folgenden Situationen wechselt der *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.
`device-status monitor temperature`	Temperatur im Gerät überwachen. Wenn die Temperatur die festgelegten Grenzwerte überschreitet oder unterschreitet, wechselt der Wert im Rahmen *Geräte-Status* auf `error`.
`device-status monitor module-removal`	Module überwachen. Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn Sie ein Modul aus dem Gerät entfernen.
`device-status module 1`	Modul `1` überwachen. 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`device-status monitor link-failure`	Den Link auf den Ports/Interfaces überwachen. Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn der Link auf einem überwachten Port/Interface abbricht.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`device-status link-alarm`	Den Link auf dem Port/Interface überwachen. Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn der Link auf einem überwachten Port/Interface abbricht.

Anmerkung: Die obigen Kommandos schalten Überwachung und Trapping für die unterstützten Komponenten ein. Wenn Sie die Überwachung für einzelne Komponenten ein- bzw. ausschalten möchten, finden Sie die entsprechende Syntax im Referenzhandbuch „Command Line Interface“ oder in der Hilfe der Konsole des Command Line Interfaces. Um die Hilfe im Command Line Interface anzuzeigen, fügen Sie ein Fragezeichen `?` ein und drücken Sie die <Enter>-Taste.

13.2.3 Gerätestatus anzeigen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.

`enable`	In den Privileged-EXEC-Modus wechseln.
`show device-status all`	Gerätestatus und Einstellung zur Ermittlung des Gerätestatus anzeigen.

13.3 Sicherheitsstatus

Der Sicherheitsstatus gibt Überblick über die Gesamtsicherheit des Geräts. Viele Prozesse dienen als Hilfsmittel für die Systemvisualisierung, indem sie den Sicherheitsstatus des Geräts 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 `error` oder `ok`. 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

Führen Sie die folgenden Schritte aus:
- ☐ Legen Sie die Ereignisse fest, die das Gerät überwacht.
- ☐ Markieren Sie für den betreffenden Parameter das Kontrollkästchen in Spalte *Überwachen*.

Tab. 45: Sicherheitsstatus-Ereignisse

Name	Bedeutung
Passwort-Voreinstellung unverändert	Um die Sicherheit zu erhöhen, ändern Sie nach der Installation die Passwörter. Bei aktivierter Funktion zeigt das Gerät einen Alarm an, wenn 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	Aktivieren Sie diese Funktion, um zu überwachen, ob die Funktion *Telnet* aktiv ist.
HTTP-Server aktiv	Aktivieren Sie diese Funktion, um zu überwachen, ob die Funktion *HTTP* aktiv ist.
SNMP unverschlüsselt	Aktivieren Sie diese Funktion, um zu überwachen, ob die Funktion *SNMPv1* oder *SNMPv2* aktiv ist.
Zugriff auf System-Monitor mit serieller Schnittstelle 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.

Tab. 45: Sicherheitsstatus-Ereignisse (Forts.)

Name	Bedeutung
Verbindungsabbruch auf eingeschalteten Ports	Das Gerät überwacht den Link-Status der aktiven Ports.
Zugriff mit HiDiscovery möglich	Aktivieren Sie diese Funktion, um zu überwachen, ob die Funktion HiDiscovery Schreibzugriff auf das Gerät hat.
Unverschlüsselte Konfiguration vom externen Speicher laden	Das Gerät überwacht die Sicherheitseinstellungen für das Laden der Konfiguration aus dem externen Speicher.
IEC61850-MMS aktiv	Das Gerät überwacht, wann Sie das Protokoll IEC 61850-MMS einschalten.
Self-signed HTTPS-Zertifikat vorhanden	Das Gerät überwacht, ob der HTTPS-Server ein selbst erzeugtes digitales Zertifikat verwendet.
Modbus TCP aktiv	Das Gerät überwacht, wann Sie das Modbus TCP/IP-Protokoll einschalten.

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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Legen Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* mindestens ein Trap-Ziel fest, das SNMP-Traps empfängt.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`security-status monitor pwd-change`	Passwort für die lokal eingerichteten Benutzerkonten `user` und `admin` überwachen. 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`	Den in Richtlinie *Min. Passwort-Länge* festgelegten Wert überwachen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `8`, wenn für die Richtlinie *Min. Passwort-Länge* ein Wert kleiner als `error` festgelegt ist.

`security-status monitor pwd-policy-config`	Passwort-Richtlinien-Einstellungen überwachen. 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`	Passwort-Richtlinien-Einstellungen überwachen. 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`	Telnet-Server überwachen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie den Telnet-Server einschalten.
`security-status monitor http-enabled`	HTTP-Server überwachen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie den HTTP-Server einschalten.
`security-status monitor snmp-unsecure`	SNMP-Server überwachen. 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 der System Monitor-Funktion in dem Gerät.
`security-status monitor extnvm-upd-enabled`	Überwachen der Aktivierung der Aktualisierung des externen nichtflüchtigen Speichers.
`security-status monitor iec61850-mms-enabled`	Funktion *IEC61850-MMS* überwachen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *IEC61850-MMS* einschalten.
`security-status trap`	Einen SNMP-Trap senden, 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`security-status monitor no-link-enabled`	Den Link auf aktiven Ports überwachen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn der Link auf einem aktiven Port abbricht.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`security-status monitor no-link`	Den Link auf Interface/Port `1` überwachen.

13.3.3 Anzeigen des Sicherheitsstatus

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.

`enable`	In den Privileged-EXEC-Modus wechseln.
`show security-status all`	Gerätestatus und Einstellung zur Ermittlung des Gerätestatus anzeigen.

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
- Wenn das Gerät außerhalb der benutzerdefinierten Temperaturschwellwerte arbeitet
- 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 im externen Speicher stimmt nicht mit der Konfiguration 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 `Manuelle Einstellung` dient der Fernsteuerung des Signalkontaktes.

Anwendungsmöglichkeiten:

- Simulation eines bei einer SPS-Fehlerüberwachung erkannten Fehlers.
- Fernbedienen eines Geräts 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 Eintrag `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`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`signal-contact 1 mode manual`	Manuellen Einstellungsmodus für Signalkontakt `1` auswählen.
`signal-contact 1 state open`	Signalkontakt `1` öffnen.
`signal-contact 1 state closed`	Signalkontakt `1` schließen.

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 `Funktionsüberwachung` 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Legen Sie im Dialog *Diagnose* > *Statuskonfiguration* > *Alarme (Traps)* mindestens ein Trap-Ziel fest, das SNMP-Traps empfängt.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Die Temperaturschwellwerte für die Temperaturüberwachung legen Sie im Dialog *Grundeinstellungen* > *System* fest.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`signal-contact 1 monitor temperature`	Temperatur im Gerät überwachen. Der Signalkontakt öffnet, wenn die Temperatur die Schwellwerte überschreitet oder unterschreitet.

`signal-contact 1 monitor ring-redundancy`	Ring-Redundanz überwachen. 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`	Den Link auf den Ports/Interfaces überwachen. Der Signalkontakt öffnet, wenn der Link auf einem überwachten Port/Interface abbricht.
`signal-contact 1 monitor envm-removal`	Aktiven externen Speicher überwachen. Der Signalkontakt öffnet, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen.
`signal-contact 1 monitor envm-not-in-sync`	Konfigurationsprofile im Gerät und im externen Speicher überwachen. In folgenden Situationen öffnet der Signalkontakt: • Das Konfigurationsprofil existiert ausschließlich im Gerät. • Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher.
`signal-contact 1 monitor power-supply 1`	Netzteil `1` überwachen. Der Signalkontakt öffnet, wenn das Gerät einen Fehler an diesem Netzteil feststellt.
`signal-contact 1 monitor module-removal 1`	Modul `1` überwachen. Der Signalkontakt öffnet, wenn Sie Modul `1` aus dem Gerät entfernen.
`signal-contact 1 trap`	Einen SNMP-Trap bei Änderung des Status der Funktionsüberwachung senden.
`no signal-contact 1 trap`	SNMP-Trap deaktivieren.

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`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`signal-contact 1 monitor link-failure`	Den Link auf den Ports/Interfaces überwachen. Der Signalkontakt öffnet, wenn der Link auf einem überwachten Port/Interface abbricht.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`signal-contact 1 link-alarm`	Den Link auf dem Port/Interface überwachen. Der Signalkontakt öffnet, wenn der Link auf einem Port/Interface abbricht.

Ereignisse, die überwacht werden können

Tab. 46: 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.
Temperatur	Aktivieren Sie diese Funktion, um zu überwachen, ob die Temperatur die festgelegten Schwellwerte überschreitet oder unterschreitet.
Ethernet-Modul entfernen	Aktivieren Sie diese Funktion, um das Entfernen eines Moduls zu überwachen. Aktivieren Sie außerdem das jeweilige zu überwachende Modul.
Externer Speicher wurde entfernt	Aktivieren Sie diese Funktion, um das Vorhandensein eines externen Speichergeräts zu überwachen.
Externer Speicher und NVM nicht synchron	Das Gerät überwacht die Synchronisation zwischen der Gerätekonfiguration und der im externen Speicher (*ENVM*) gespeicherten Konfiguration.
Ring-Redundanz	Aktivieren Sie diese Funktion, um das Vorhandensein der Ring-Redundanz zu überwachen.
Netzteil	Aktivieren Sie diese Funktion, um das Netzteil zu überwachen.

Signalkontakt-Anzeige

Das Gerät bietet Ihnen weitere Möglichkeiten, den Zustand des Signalkontaktes darzustellen:
- Anzeige in der grafischen Benutzeroberfläche
- Abfrage im Command Line Interface

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.
  Der Rahmen *Status Signalkontakt* zeigt den Status des Signalkontakts und informiert über aufgetretene Alarme.

`show signal-contact 1 all`	Einstellungen für den festgelegten Signalkontakt anzeigen.

13.5 Portereignis-Zähler

Die Port-Statistiktabelle ermöglicht erfahrenen Netzadministratoren, möglicherweise erkannte Schwachpunkte im Netz zu identifizieren.

Diese Tabelle zeigt die Inhalte verschiedener Ereigniszähler. Die Paketzähler summieren die Ereignisse aus Sende- und Empfangsrichtung. Im Dialog *Grundeinstellungen > Neustart* können Sie die Ereigniszähler zurücksetzen.

Tab. 47: Beispiele für die Angabe bekannter Schwächen

Zähler	Angabe bekannter möglicher Schwächen
Empfangene Fragmente	• Nicht funktionierender Controller des verbundenen Geräts • Elektromagnetische Einkoppelung im Übertragungsmedium
CRC-Fehler	• Nicht funktionierender Controller des verbundenen Geräts • Elektromagnetische Einkoppelung im Übertragungsmedium • Nicht betriebsbereite Komponente im Netz
Kollisionen	• Nicht funktionierender Controller des verbundenen Geräts • Netzausdehnung zu groß/Zeilen zu lang • Kollision oder Fehler beim Datenpaket ermittelt

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*.

13.5.1 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 ermöglicht Ihnen, 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.

Tab. 48: Bewertung des nicht übereinstimmenden Duplex-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

13.6 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 Funktion *Auto-Disable* wieder einschalten, erzeugt das Gerät einen Protokolleintrag.

Die Funktion *Auto-Disable* 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 Funktion *Auto-Disable* hat die folgenden Aufgaben:
- Sie unterstützt den Netzadministrator bei der Port-Analyse.
- Dies verringert die Wahrscheinlichkeit, dass der betreffende Port ein instabiles Netz verursacht.

Die Funktion *Auto-Disable* steht für folgende Funktionen zur Verfügung:
- *Link-Änderungen* (Funktion *Port-Monitor*)
- *CRC/Fragmente* (Funktion *Port-Monitor*)
- Duplex Mismatch-Erkennung (Funktion *Port-Monitor*)
- *DHCP-Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port-Sicherheit*
- *Überlast-Erkennung* (Funktion *Port-Monitor*)
- *Link-Speed-/Duplex-Mode-Erkennung* (Funktion *Port-Monitor*)

Im folgenden Beispiel konfigurieren Sie das Gerät so, dass es einen Port deaktiviert und anschließend automatisch reaktiviert, wenn es eine Überschreitung der im *Diagnose > Ports > Port-Monitor*, Registerkarte *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 festgelegten 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 `An`.
- ☐ 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, wählen Sie die Tabellenzeile des Ports und klicken die Schaltfläche 🗑 .
  - 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* ermöglicht Ihnen, den Port zu aktivieren, bevor die in Spalte *Reset-Timer [s]* festgelegte Zeit abgelaufen ist.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`port-monitor condition crc-fragments count 2000`	CRC-Fragment-Zähler auf 2000 Teile pro Million festlegen.
`port-monitor condition crc-fragments interval 15`	Messintervall für die CRC-Fragment-Erkennung auf 15 Sekunden setzen.
`auto-disable timer 120`	Wartezeit von `120` Sekunden festlegen, nach der die Funktion *Auto-Disable* den Port wieder einschaltet.
`exit`	In den Konfigurationsmodus wechseln.
`auto-disable reason crc-error`	Selbstabschaltfunktion für CRC aktivieren.
`port-monitor condition crc-fragments mode`	Zur Auslösung einer Aktion die CRC-Fragment-Bedingung aktivieren.
`port-monitor operation`	Funktion *Port-Monitor* aktivieren.

Wenn das Gerät einen Port wegen Grenzwertüberschreitungen ausschaltet, ermöglicht Ihnen das Gerät, den ausgeschalteten Port mit den folgenden Kommandos manuell zurückzusetzen.

Führen Sie die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`auto-disable reset`	Ermöglicht Ihnen, den Port einzuschalten, bevor der Timer zu zählen beginnt.

13.7 SFP-Zustandsanzeige

Die SFP-Zustandsanzeige ermöglicht Ihnen, 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 den folgenden Schritt aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Ports > SFP*.

13.8 Topologie-Erkennung

IEEE 802.1AB beschreibt das Link Layer Discovery Protocol (LLDP). Das LLDP ermöglicht Ihnen die automatische Topologie-Erkennung im lokalen Netz.

Geräte mit aktivem LLDP:
- senden ihre Verbindungs- und Verwaltungsdaten an die angrenzenden Geräte des gemeinsamen LANs. Die Bewertung der Geräte erfolgt, wenn die Funktion *LLDP* 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
- Gegenwärtig 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.

13.8.1 Anzeige der Topologie-Erkennung

Zeigen Sie die Topologie des Netzes an. Führen Sie dazu den folgenden Schritt aus:

- ☐ Öffnen Sie den Dialog *Diagnose > 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.

Das Aktivieren der Einstellung „FDB Einträge anzeigen“ am unteren Ende der Tabelle ermöglicht Ihnen, 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.

Sind an einen Port ausschließlich Geräte ohne aktive Topologie-Erkennung angeschlossen, enthält die Tabelle eine Zeile für diesen Port, um die angeschlossenen Geräte darzustellen. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.

Die FDB-Adresstabelle enthält MAC-Adressen von Geräten, die die Topologie-Tabelle aus Gründen der Übersicht ausblendet.

13.8.2 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 Geräte im Netz, zum Beispiel Switches. Sie 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
  Ermöglicht den LLDP-MED-Endpunkten, zu ermitteln, welche Funktionen das angeschlossene Gerät unterstützt und welche Funktionen im Gerät aktiviert sind.
- TLV – Netzrichtlinien
  Ermöglicht beiden Netzanschlussgeräten und Endpunkten, 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.

13.9 Erkennen von Loops

Loops im Netz können Verbindungsunterbrechungen oder Datenverlust verursachen. Dies gilt auch dann, wenn sie nur vorübergehend sind. Die automatische Detektion und Meldung dieser Situation ermöglicht Ihnen, diese rascher zu entdecken und leichter zu diagnostizieren.

Eine Fehlkonfiguration kann einen Loop verursachen, zum Beispiel wenn Sie Spanning Tree deaktivieren.

Das Gerät ermöglicht Ihnen, 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 Geräts oder an demselben Port empfangen werden, sind ein typischer Effekt eines Loops.

Um zu prüfen, ob das Gerät einen Loop detektiert hat, führen Sie die folgenden Schritte aus;

- Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*.
- Prüfen Sie den Wert in den Feldern *Port-Zustand* und *Port-Rolle*. Wenn das Feld *Port-Zustand* den Wert `discarding` und das Feld *Port-Rolle* den Wert `backup` zeigt, befindet sich der Port in einem Loop-Zustand.
  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 Loop-Zustand.

13.10 Unterstützung beim Schutz vor Layer-2-Loops

Das Gerät unterstützt beim Schutz vor Layer-2-Loops.

Ein Loop im Netz kann zu einem Stillstand des Netzes aufgrund von Überlastung führen. Eine mögliche Ursache ist das ständige Duplizieren von Datenpaketen aufgrund einer Fehlkonfiguration. Die Ursache kann z. B. ein falsch gestecktes Kabel oder fehlerhafte Einstellungen in der Software sein.

Ein Layer-2-Loop im Netz entsteht zum Beispiel in den folgenden Fällen, wenn keine Redundanzprotokolle aktiv sind:
- Zwei Ports desselben Geräts sind direkt miteinander verbunden.
- Zwischen zwei Geräten ist mehr als eine aktive Verbindung eingerichtet.

13.10.1 Anwendungsbeispiel

Die Abbildung zeigt Beispiele für mögliche Layer-2-Loops in einem Netz. In jedem Gerät ist die Funktion *Loop-Schutz* eingeschaltet.
- **A**: *Aktiver Modus*
  Ports, die zum Anschluss von Endgeräten vorgesehen sind, arbeiten im Modus *aktiv*. Das Gerät sendet auf diesen Ports *Loop-Detection*-Pakete und wertet diese aus.
- **P**: *Passiver Modus*
  Ports, die zu den redundanten Ringen gehören, arbeiten im Modus *passiv*. Das Gerät wertet *Loop-Detection*-Pakete auf diesen Ports nur aus.
- **Loop 1**..**Loop 4**
  Unbeabsichtigt eingerichtete Layer-2-Loops.

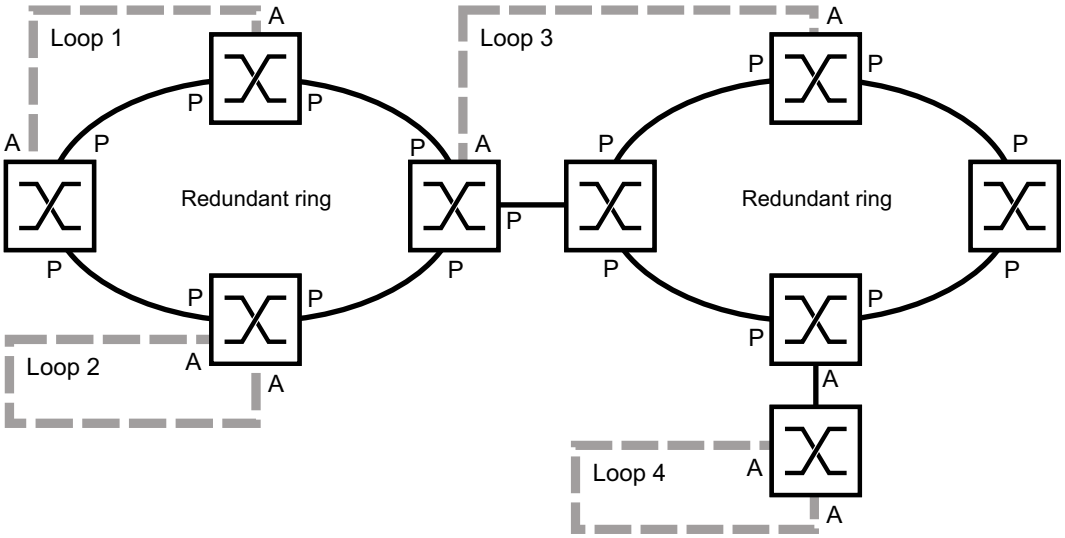


Abb. 74: Beispiele für unbeabsichtigte Layer-2-Loops

Loop-Schutz-Einstellungen den Ports zuweisen

Weisen Sie jedem *aktiven* und *passiven* Port die Einstellungen der Funktion *Loop-Schutz* zu.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Loop-Schutz*.
- ☐ Passen Sie im Rahmen *Global*, Feld *Sende-Intervall* den Wert an, falls erforderlich.
- ☐ Passen Sie im Rahmen *Global*, Feld *Empfang-Grenzwert* den Wert an, falls erforderlich.
- ☐ Legen Sie in Spalte *Modus* das Verhalten der Funktion *Loop-Schutz* auf dem Port fest:
  - `aktiv` für Ports, die für den Anschluss von Endgeräten vorgesehen sind
  - `passiv` für Ports, die zu den redundanten Ringen gehören
- ☐ Legen Sie in Spalte *Aktion* den Wert *alle* fest.
  Wenn das Gerät einen Layer-2-Loop an diesem Port erkennt, dann sendet es einen Trap und deaktiviert den Port mit Hilfe der Funktion *Auto-Disable*. Passen Sie den Wert an, falls erforderlich.
- ☐ Markieren Sie in Spalte *Aktiv* das Kontrollkästchen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`loop-protection tx-interval 5`	Sende-Intervall festlegen, falls erforderlich.
`loop-protection rx-threshold 1`	Empfang-Grenzwert festlegen, falls erforderlich.
`interface 1/1`	In den Interface-Modus wechseln. Beispiel: Port *1/1*.
`loop-protection mode active`	Für Ports, an die Endgeräte angeschlossen werden, den Modus `active` festlegen.
`loop-protection mode passive`	Für Ports, die zu den redundanten Ringen gehören, den Modus `passive` festlegen.
`loop-protection action all`	Aktion festlegen, die das Gerät ausführt, wenn es einen Layer-2-Loop an diesem Port erkennt.
`loop-protection operation`	Funktion *Loop-Schutz* auf dem Port aktivieren.
`exit`	In den Konfigurationsmodus wechseln.

Funktion Auto-Disable aktivieren

Nachdem Sie den Ports die *Loop-Schutz*-Einstellungen zugewiesen haben, aktivieren Sie die Funktion *Auto-Disable*.

Führen Sie die folgenden Schritte aus:

- ☐ Markieren Sie im Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`loop-protection auto-disable`	Funktion *Auto-Disable* aktivieren.

Funktion Loop-Schutz im Gerät einschalten

Abschließend schalten Sie die Funktion *Loop-Schutz* im Gerät ein.

Führen Sie die folgenden Schritte aus:

- ☐ Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`loop-protection operation` Funktion *Loop-Schutz* auf dem Gerät einschalten.

13.10.2 Empfehlungen für redundante Ports

Abhängig von den *Loop-Schutz*-Einstellungen schaltet das Gerät mit der Funktion *Auto-Disable* Ports aus, wenn das Gerät einen Layer-2-Loop erkennt.

Wenn auf einem Port eine Redundanzfunktion aktiv ist, dann aktivieren Sie nicht den Modus *aktiv* auf diesem Port. Andernfalls kann das Ausschalten von Ports auf redundanten Pfaden im Netz die Folge sein. Im obigen Beispiel sind dies die Ports, die zu den redundanten Ringen gehören.

Vergewissern Sie sich, dass ein redundanter Pfad im Netz als Backup-Medium verfügbar ist. Bei Ausfall des primären Pfads wechselt das Gerät auf den redundanten Pfad.

Die folgenden Einstellungen helfen, das Abschalten von Ports auf redundanten Netzwerkpfaden zu vermeiden:

- ☐ Deaktivieren Sie die Funktion *Loop-Schutz* auf redundanten Ports.
  oder
- ☐ Aktivieren Sie den *passiv*-Modus auf redundanten Ports.

Die Funktion *Loop-Schutz* und die Funktion *Spanning Tree* beeinflussen sich gegenseitig. Die folgenden Schritte helfen, ein unerwartetes Verhalten des Geräts zu vermeiden:

- ☐ Schalten Sie die *Spanning Tree*-Funktion an dem Port aus, an dem Sie die *Loop-Schutz*-Funktion einschalten möchten. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Spalte *STP aktiv*.
- ☐ Schalten Sie die Funktion*Spanning Tree* auf dem angeschlossenen Port jedes angeschlossenen Geräts aus. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree*.

13.11 Benutzen der Funktion E-Mail-Benachrichtigung

Das Gerät ermöglicht Ihnen, Benutzer per E-Mail über das Eintreten von Ereignissen zu benachrichtigen. Voraussetzung ist ein über das Netz erreichbarer Mail-Server, an den das Gerät die E-Mails übergibt.

Um im Gerät das Senden von E-Mails einzurichten, führen Sie die Schritte in den folgenden Kapiteln aus:

- ☐ Absender-Adresse festlegen
- ☐ Auslösende Ereignisse festlegen
- ☐ Empfänger festlegen
- ☐ Mail-Server festlegen
- ☐ Funktion E-Mail-Benachrichtigung ein-/ausschalten
- ☐ Test-Nachricht senden

13.11.1 Absender-Adresse festlegen

Die Absender-Adresse ist die E-Mail-Adresse, die den Empfängern zeigt, wer die E-Mail gesendet hat. Die Voreinstellung im Gerät ist `switch@hirschmann.com`.

Ändern Sie den voreingestellten Wert. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.
- ☐ Ändern Sie im Rahmen *Absender* den Wert im Feld *Adresse*.
  Fügen Sie eine gültige E-Mail-Adresse ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging email from-addr <user@doma.in>`	Absender-Adresse ändern.

13.11.2 Auslösende Ereignisse festlegen

Das Gerät unterscheidet Ereignisse mit den folgenden Schweregraden:

Tab. 49: Bedeutung der Schweregrade für Ereignisse

Schweregrad	Bedeutung
`emergency`	Gerät nicht betriebsbereit
`alert`	Sofortiger Bedienereingriff erforderlich
`critical`	Kritischer Zustand
`error`	Fehlerhafter Zustand
`warning`	Warnung

Tab. 49: Bedeutung der Schweregrade für Ereignisse (Forts.)

Schweregrad	Bedeutung
`notice`	Signifikanter, normaler Zustand
`informational`	Informelle Nachricht
`debug`	Debug-Nachricht

Sie haben die Möglichkeit, selbst festzulegen, über welche Ereignisse das Gerät Sie benachrichtigt. Hierzu weisen Sie den Benachrichtigungsstufen des Geräts den gewünschten Mindest-Schweregrad zu.

Das Gerät benachrichtigt die Empfänger wie folgt:

- *Benachrichtigung sofort*
  Wenn ein Ereignis mit diesem Schweregrad oder mit einem dringenderen Schweregrad auftritt, sendet das Gerät sofort eine E-Mail.
- *Benachrichtigung periodisch*
  - Wenn ein Ereignis mit dem zugewiesenen oder einem kritischeren Schweregrad eintritt, protokolliert das Gerät das Ereignis in einem Puffer.
  - Das Gerät sendet eine E-Mail mit dem Protokoll periodisch oder wenn der Puffer voll ist.
  - Ereignisse mit einem weniger kritischen Schweregrad protokolliert das Gerät nicht.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.

Im Rahmen *Benachrichtigung sofort* legen Sie die Einstellungen für E-Mails fest, die das Gerät sofort sendet.

- ☐ Legen Sie im Feld *Schweregrad* den Mindest-Schweregrad fest.
- ☐ Im Feld *Betreff* legen Sie den Betreff der E-Mail fest.

Im Rahmen *Benachrichtigung periodisch* legen Sie die Einstellungen für E-Mails fest, die das Gerät in regelmäßigen Abständen sendet.

- ☐ Legen Sie im Feld *Schweregrad* den Mindest-Schweregrad fest.
- ☐ Im Feld *Betreff* legen Sie den Betreff der E-Mail fest.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging email severity immediate <level>`	Mindest-Schweregrad der Ereignisse festlegen, für die das Gerät die E-Mail sofort sendet.
`logging email severity periodic <level>`	Mindest-Schweregrad der Ereignisse festlegen, für die das Gerät die E-Mail in regelmäßigen Abständen sendet.
`logging email subject add <immediate | periodic> TEXT`	Betreffzeile mit dem Inhalt `TEXT` erzeugen.

13.11.3 Sendeintervall ändern

Das Gerät ermöglicht Ihnen, festzulegen, in welchem Intervall es E-Mails mit dem Protokoll sendet. Die Voreinstellung ist `30` Minuten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.

Im Rahmen *Benachrichtigung periodisch* legen Sie die Einstellungen für E-Mails fest, die das Gerät in regelmäßigen Abständen sendet.

- ☐ Ändern Sie den Wert im Feld *Sende-Intervall [min]*, um das Intervall zu ändern.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging email duration <30..1440>`	Intervall festlegen, in dem das Gerät E-Mails mit Protokoll sendet.

13.11.4 Empfänger festlegen

Das Gerät ermöglicht Ihnen, bis zu 10 Empfänger festzulegen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Empfänger*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche ⊞.
- ☐ Im Rahmen *Benachrichtigungs-Typ* legen Sie fest, ob das Gerät die E-Mails an diesen Empfänger sofort oder in regelmäßigen Abständen sendet.
- ☐ Legen Sie im Feld *Adresse* die E-Mail-Adresse des Empfängers fest.
- ☐ Markieren Sie in Spalte *Aktiv* das Kontrollkästchen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately | periodically>`	Empfänger mit der E-Mail-Adresse `user@doma.in` festlegen. Das Gerät verwaltet die Einstellungen auf dem Speicherplatz `1..10`.

13.11.5 Mail-Server festlegen

Das Gerät unterstützt verschlüsselte und unverschlüsselte Verbindungen zum Mail-Server.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Mail-Server*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Legen Sie in Spalte *IP-Adresse* die IP-Adresse oder den DNS-Namen des Servers fest.
- ☐ Legen Sie in Spalte *Verschlüsselung* das Protokoll fest, das die Verbindung zwischen Gerät und Mail-Server verschlüsselt.
- ☐ Legen Sie in Spalte *Ziel-TCP-Port* den TCP-Port fest, wenn der Mail-Server einen anderen als den Well-known-Port verwendet.

Wenn der Mail-Server eine Authentifizierung erfordert:

- ☐ Legen Sie in den Spalten *Benutzername* und *Passwort* die Anmeldeinformationen für das Konto fest, mit dem sich das Gerät beim Mail-Server anmeldet.
- ☐ Fügen Sie in Spalte *Beschreibung* eine aussagekräftige Bezeichnung für den Mail-Server ein.
- ☐ Markieren Sie in Spalte *Aktiv* das Kontrollkästchen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	Mail-Server mit der IP-Adresse `IP ADDRESS` festlegen. Das Gerät verwaltet die Einstellungen auf dem Speicherplatz `1..5`.

13.11.6 Funktion E-Mail-Benachrichtigung ein-/ausschalten

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging email operation`	Senden von E-Mails einschalten.
`no logging email operation`	Senden von E-Mails ausschalten.

13.11.7 Test-Nachricht senden

Das Gerät ermöglicht Ihnen, durch Senden einer Test-Nachricht die Einstellungen zu prüfen.

Voraussetzung:
- Die E-Mail-Einstellungen sind vollständig festgelegt.
- Die Funktion *E-Mail-Benachrichtigung* ist eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Mail-Server*.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Verbindung testen*.
- ☐ Wählen Sie in der Dropdown-Liste *Empfänger*, an welche Empfänger das Gerät die E-Mail sendet.
- ☐ Legen Sie im Feld *Nachrichtentext* den Text der Test-Nachricht fest.
- ☐ Klicken Sie die Schaltfläche *Ok*, um die Test-Nachricht zu senden.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging email test msgtype <urgent|non-urgent> TEXT`	Eine E-Mail-Nachricht mit dem Inhalt `TEXT` an die Empfänger senden.

Wenn Sie keine Fehlermeldung sehen und die Empfänger die E-Mail erhalten, sind die Einstellungen im Gerät korrekt festgelegt.

13.12 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 geräteinterne Ereignisse schreibt.
- Audit Trail
  Protokolliert erfolgreiche 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 das Command Line Interface oder kopieren Sie die Dateien für den späteren Zugriff auf einen externen Server.
- *Support-Informationen herunterladen*
  Diese Schaltfläche ermöglicht Ihnen, Systeminformationen als ZIP-Archiv herunterzuladen.

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

13.12.1 Globale Einstellungen

Über diesen Dialog aktivieren oder deaktivieren Sie die jeweiligen Ziele, an die das Gerät Berichte sendet, zum Beispiel Konsole, Syslog-Server oder Verbindung zum Command Line Interface. 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 > 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 `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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 Funktion *Protokolliere SNMP-Get-Requests* ein.
  Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld `An`.
- Um SNMP-Schreib-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die Funktion *Protokolliere SNMP-Set-Requests* ein.
  Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld `An`.
- Wählen Sie den gewünschten Schweregrad für die Get- und Set-Anfragen.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Sofern aktiv, protokolliert das Gerät Änderungen an der Konfiguration, die über das Command Line Interface 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 > Global*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *CLI-Logging* das Optionsfeld `An`.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Das Gerät ermöglicht Ihnen, die folgenden Systeminformationen in einer ZIP-Datei auf Ihrem PC speichern:

- `audittrail.html`
- `config.xml`
- `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 .
  Nach kurzer Zeit können Sie das ZIP-Archiv herunterladen.
- Wählen Sie das Verzeichnis aus, in welchem Sie die Support-Information speichern.
- Klicken Sie die Schaltfläche *Ok*.

13.12.2 Syslog

Das Gerät bietet Ihnen die Möglichkeit, Nachrichten zu geräteinternen Ereignissen an einen oder mehrere Syslog-Server (bis zu 8) zu senden. Zusätzlich schließen Sie SNMP-Anfragen des Geräts 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 oder den *Hostname* des Syslog-Servers ein.
- ☐ Legen Sie in Spalte *Ziel-UDP-Port* den TCP- oder 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 benötigt, 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 `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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 > Global*.
- ☐ Um SNMP-Lese-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die Funktion *Protokolliere SNMP-Get-Requests* ein.
  Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld `An`.
- ☐ Um SNMP-Schreib-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die Funktion *Protokolliere SNMP-Set-Requests* ein.
  Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld `An`.
- ☐ Wählen Sie den gewünschten Schweregrad für die Get- und Set-Anfragen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging host add 1 addr 10.0.1.159 severity 3`	Der Liste der Syslog-Server einen neuen Empfänger hinzufügen. Der Wert `3` legt den Schweregrad des Ereignisses fest, welches das Gerät protokolliert. Der Wert `3` bedeutet `error`.
`logging syslog operation`	Funktion *Syslog* einschalten.
`exit`	In den Privileged-EXEC-Modus wechseln.
`show logging host`	Syslog-Host-Einstellungen anzeigen.

```
No.    Server IP       Port   Max. Severity   Type        Status
-----  --------------- -----  --------------  ----------  -------
1      10.0.1.159      514    error           systemlog   active
```

`configure`	In den Konfigurationsmodus wechseln.
`logging snmp-requests get operation`	SNMP-Get-Anfragen protokollieren.
`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 `notice`.
`logging snmp-requests set operation`	SNMP-SET-Anfragen protokollieren.
`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 `notice`.
`exit`	In den Privileged-EXEC-Modus wechseln.
`show logging snmp`	SNMP-Logging-Einstellungen anzeigen.

```
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

13.12.3 System-Log

Das Gerät ermöglicht Ihnen, 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:

- ☐ Um den Inhalt des Protokolls zu aktualisieren, klicken Sie die Schaltfläche ↻.
- ☐ Um den Inhalt des Protokolls als HTML-Datei zu speichern, klicken Sie die Schaltfläche .
- ☐ Um den Inhalt des Protokolls zu löschen, klicken Sie die Schaltfläche 🗑.
- ☐ Um den Inhalt des Protokolls nach Suchbegriffen zu durchsuchen, verwenden Sie die Suchfunktion Ihres Web-Browsers.

Anmerkung: Sie haben die Möglichkeit, auch protokollierte Ereignisse an einen oder mehrere Syslog-Server zu senden.

13.12.4 Syslog über TLS

Transport Layer Security ist ein kryptografisches Protokoll, das entwickelt wurde, um Kommunikationssicherheit über ein Rechnernetz zu unterstützen. Das vorrangige Ziel des TLS-Protokolls besteht darin, Datenschutz und Datenintegrität zwischen 2 kommunizierenden Computeranwendungen herzustellen.

Nach der Initiierung einer Datenverbindung mit einem Syslog-Server über einen TLS-Handshake validiert das Gerät das vom Server empfangene Zertifikat. Zu diesem Zweck übertragen Sie das PEM-Zertifikat von einem Remote-Server oder vom externen Speicher oder aus dem externen Speicher auf das Gerät. Vergewissern Sie sich, dass die konfigurierte IP-Adresse oder der DNS-Name des Servers mit den im Zertifikat enthaltenen Informationen übereinstimmt. Sie finden die Informationen in den Feldern „Allgemeiner Name“ oder „Alternativer Name des Betreffs“ des Zertifikates.

Das Gerät sendet die TLS-verschlüsselten Syslog-Nachrichten über den TCP-Port, der in Spalte *Ziel-UDP-Port* festgelegt ist.

Anmerkung: Legen Sie die IP-Adresse oder den DNS-Namen des Servers dahingehend fest, dass sie/er der IP-Adresse bzw. dem DNS-Namen im Serverzertifikat entspricht. Die Werte sind im Zertifikat als „Allgemeiner Name“ oder als „Alternativer Name des Betreffs“ angegeben.

Beispiel

Das vorliegende Beispiel beschreibt die Konfiguration der Funktion *Syslog*. Wenn Sie die folgenden Schritte ausführen, ermöglicht Ihnen das Gerät, TLS-verschlüsselte Syslog-Nachrichten über den TCP-Port zu senden, der in Spalte *Ziel-UDP-Port* festgelegt ist.

Syslog-Nachrichten, die von einem Gerät an einen Syslog-Server gesendet werden, passieren ggf. unsichere Netze. Um einen Syslog-Server über TLS zu konfigurieren, übertragen Sie das CA-Zertifikat auf das Gerät.

Anmerkung: Um die Änderungen nach dem Laden eines neuen Zertifikates zu übernehmen, starten Sie die Funktion *Syslog* neu.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Syslog*.
- ☐ Um eine Datenverbindung mit den Syslog-Servern zu initiieren, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Das Gerät validiert das empfangene Zertifikat. Das Gerät authentifiziert außerdem den Server und beginnt mit dem Senden von Syslog-Nachrichten.

- ☐ Übertragen Sie das PEM-Zertifikat vom Remote-Server oder aus dem externen Speicher auf das Gerät.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`logging host add 1 addr 192.168.3.215`	Index `1` dem Syslog-Server mit IPv4-Adresse `192.168.3.215` hinzufügen.

`logging host modify 1 port 6512 type systemlog`	Portnummer `6512` festlegen und Ereignisse in der Log-Datei (System Log) protokollieren.
`logging host modify 1 transport tls`	Für den Übertragungstyp `tls` festlegen.
`logging host modify 1 severity informational`	Ereignis-Typ festlegen, der als `informational` in der Log-Datei (System Log) protokolliert wird.
`exit`	In den Privileged-EXEC-Modus wechseln.
`copy syslogcacert evmm`	CA-Zertifikate aus dem externen Speicher auf das Gerät kopieren.
`show logging host`	Syslog-Host-Einstellungen anzeigen.

13.12.5 Audit Trail

Der Dialog *Diagnose > Bericht > Audit-Trail* enthält Systeminformationen sowie Änderungen, die über Command Line Interface und SNMP an dem Gerät vorgenommen wurden. Bei Änderungen der Gerätekonfiguration zeigt der Dialog, wer zu welchem Zeitpunkt welche Änderungen vorgenommen hat.

Der Dialog *Diagnose > Syslog* ermöglicht Ihnen, bis zu 8 Syslog-Server festzulegen, an die das Gerät Audit Trails sendet.

Die folgende Liste enthält Protokollereignisse:
- Änderungen an Konfigurationsparametern
- Kommandos (mit Ausnahme der `show`-Kommandos) im Command Line Interface
- Kommando `logging audit-trail <string>` im Command Line Interface, das den Kommentar protokolliert
- Automatische Änderungen der Systemzeit
- Watchdog-Ereignisse
- Sperren eines Benutzers nach mehreren fehlgeschlagenen Login-Versuchen
- Benutzeranmeldung über das Command Line Interface (lokal oder remote)
- Manuelle, benutzerinitiierte Abmeldung
- Zeitgesteuerte Abmeldung nach einer benutzerdefinierten Zeitspanne der Inaktivität im Command Line Interface.
- Dateiübertragung, einschließlich Firmware-Update
- Konfigurationsänderungen über HiDiscovery
- Automatische Konfiguration oder Firmware-Updates über den externen Speicher
- Gesperrter Zugriff auf das Management des Geräts aufgrund von ungültigen Anmeldedaten
- Neustart
- Öffnen und Schließen von SNMP über HTTPS-Tunnel
- Ermittelte Stromausfälle

13.13 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 Kommando `debug` zugegriffen werden. Weitere Informationen zur Funktion TCPDump finden Sie im Referenz-Handbuch „Command Line Interface“.

13.14 Datenverkehr beobachten

Das Gerät ermöglicht Ihnen, Datenpakete, die das Gerät durchlaufen, an einen Ziel-Port weiterzuleiten. Dort können Sie die Datenpakete überwachen und auswerten.

Das Gerät bietet Ihnen folgende Möglichkeiten:
- Port-Mirroring
- VLAN-Mirroring
- Remote SPAN

13.14.1 Port-Mirroring

Die Funktion *Port-Mirroring* ermöglicht Ihnen, die Datenpakete von physischen Quell-Ports zu einem physischen Ziel-Port zu kopieren.

Mit einem am Ziel-Port angeschlossenen Analysator, zum Beispiel RMON-Probe, überwachen Sie die auf den Quell-Ports gesendeten und empfangen Datenpakete. Die Funktion hat keine Auswirkungen auf den über die Quell-Ports laufenden Datenstrom.

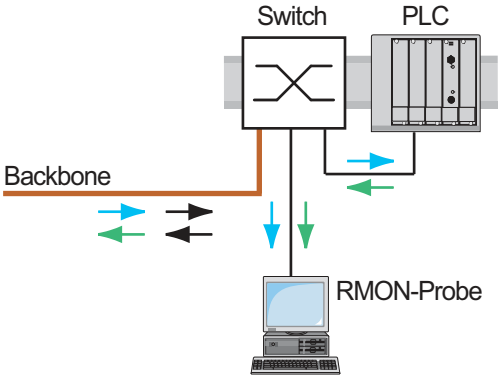


Abb. 75: Beispiel

Das Gerät vermittelt auf dem Ziel-Port ausschließlich die von den Quell-Ports kopierten Datenpakete.

Um über den Ziel-Port auf das Management des Geräts zuzugreifen, markieren Sie vor Einschalten der Funktion *Port-Mirroring* das Kontrollkästchen *Management erlauben*. Das Gerät ermöglicht Benutzern den Zugriff auf das Management des Geräts über den Ziel-Port, ohne die aktive *Port-Mirroring*-Session zu unterbrechen.

Anmerkung: Das Gerät dupliziert auf dem Ziel-Port Multicasts, Broadcasts und unbekannte Unicasts.

Die VLAN-Einstellungen auf dem Ziel-Port bleiben unverändert. Voraussetzung für den Zugriff auf des Management des Geräts über den Ziel-Port ist, dass der Ziel-Port Mitglied im Management-VLAN ist.

Funktion Port-Mirroring einschalten

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Legen Sie die Quell-Ports fest.
  Markieren Sie das Kontrollkästchen in Spalte *Eingeschaltet* für die gewünschten Ports.
- ☐ Legen Sie den Ziel-Port fest.
  Wählen Sie im Rahmen *Ziel-Port*, Dropdown-Liste *Primärer Port* den gewünschten Port.
  Die Dropdown-Liste zeigt ausschließlich die verfügbaren Ports. Bereits als Quell-Port festgelegte Ports sind nicht verfügbar.
- ☐ Falls erforderlich, 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 Ziel-Port auf das Management des Geräts zuzugreifen:
  Markieren Sie im Rahmen *Ziel-Port* das Kontrollkästchen *Management erlauben*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Um die Funktion *Port-Mirroring* zu deaktivieren und die Voreinstellungen wiederherzustellen, klicken Sie die Schaltfläche 🗑.

13.14.2 VLAN-Mirroring

Die Funktion *VLAN-Mirroring* ermöglicht Ihnen, den empfangenen Datenstrom in einem bestimmten VLAN auf einen ausgewählten Ziel-Port zu spiegeln. Das Gerät kopiert lediglich die Daten im VLAN und sendet die Originaldaten an die vorgesehenen Empfänger. Das Gerät kann beispielsweise Daten auf einen Network Analyzer spiegeln, der mit dem Ziel-Port verbunden ist.

Ausschließlich eine Funktion kann jeweils aktiv sein, entweder die Funktion *VLAN-Mirroring* oder die Funktion *Port-Mirroring*. Wenn Sie VLAN 0 als Quell-VLAN auswählen, ist die Funktion *VLAN-Mirroring* inaktiv. Um die Funktion *VLAN-Mirroring* zu deaktivieren, heben Sie für den Quell-Port die Markierung des Kontrollkästchens in Spalte *Eingeschaltet* auf.

Überschreitet der am gespiegelten VLAN empfangene Datenstrom die maximale Bandbreite des Ziel-Ports, verwirft das Gerät einige Pakete, um die maximale Bandbreite des Ziel-Ports zu erfassen. Das Gerät verwirft zwar einige Pakete, spiegelt aber weiterhin Pakete im festgelegten VLAN.

Wenn Sie die PVID auf einem Port als die Quell-VLAN-ID festlegen, spiegelt das Gerät die empfangenen unmarkierten Pakete, die kein VLAN-Tag enthalten. In diesem Fall spiegelt das Gerät das Paket exakt so, wie es das Paket empfangen hat.

Beispiel-Konfiguration

In dieser Beispielkonfiguration spiegelt Sw 4 die an VLAN 20 empfangenen Daten auf einen Network Analyzer auf dem Ziel-Port.

Um das VLAN-Mirroring an Sw 4 zu konfigurieren, gehen Sie folgendermaßen vor:
- ☐ Erzeugen Sie das gespiegelte VLAN.
- ☐ Konfigurieren Sie das VLAN-Mirroring.

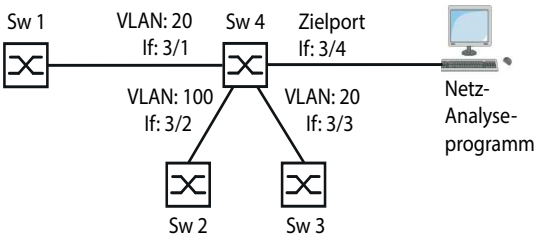


Abb. 76: Beispielkonfiguration für VLAN-Mirroring

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  - ☐ 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 in Spalte *Name* den Wert `VLAN-Mirroring-Port` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Funktion *Port-Mirroring* deaktivieren:
  Heben Sie die Markierung jedes Kontrollkästchens in Spalte *Eingeschaltet* auf.
- ☐ Ziel-Port festlegen:
  Legen Sie im Rahmen *Ziel-Port* den Wert `3/4` fest.
- ☐ Datenquelle festlegen:
  Legen Sie im Rahmen *VLAN-Mirroring*, Feld *Quell-VLAN-ID* den Wert `20` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 20`	VLAN `20` auf dem Gerät erzeugen.
`name 20 VLAN mirroring port`	Dem VLAN `20` den Namen `VLAN mirroring port` zuweisen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.

`monitor session 1 source vlan 20`	VLAN-Mirroring-Sitzung `1` erzeugen, wobei VLAN `20` die Quelle ist.
`monitor session 1 destination interface 3/4`	Als Ziel-Port Port `3/4` festlegen.
`monitor session 1 mode`	VLAN-Mirroring-Sitzung `1` festlegen.

13.14.3 Remote SPAN

Der Remote Switch Port Analyzer (RSPAN) ermöglicht dem Netzadministrator, gespiegelte Daten über verschiedene Geräte hinweg an einen Ziel-Port weiterzuleiten. Der Netzadministrator kann die Daten analysieren oder von einem zentralen Ort aus eine Diagnose für die im Netzwerk erkannten Fehler durchführen. Das Gerät ermöglicht dem Netzadministrator, Daten aus 1 zentralen Quelle oder aus mehreren Quellen zu analysieren.

Die gespiegelten Daten durchqueren das Netz an einem festgelegten VLAN. Jedes RSPAN-Gerät verwendet dasselbe RSPAN-VLAN zum Weiterleiten gespiegelter Daten. Außerdem kann jeder Port, mit Ausnahme der gespiegelten Ports, ein Mitglied des RSPAN-VLAN sein.

Abhängig von der Menge der Daten und der Port-Bandbreite kann das Gerät einen Teil der gespiegelten Daten verwerfen. Um den Verlust von gespiegelten Datenpaketen zu reduzieren, verwenden Sie Gigabit-Ports und/oder LAG-Schnittstellen, um die RSPAN-Daten an das Zielgerät weiterzuleiten.

Der Netzadministrator konfiguriert die für RSPAN verwendeten Geräte in Abhängigkeit der verschiedenen Rollen. RSPAN verwendet die folgenden Gerätekonfigurationen:

- Ein Quellgerät spiegelt und markiert die Daten mit der RSPAN-VLAN-ID und leitet die Daten ausschließlich an den Ziel-Port des Quellgeräts weiter. Im Quellgerät legen Sie im Feld *Ziel-VLAN-ID* das RSPAN-VLAN fest.
  Wenn das Quellgerät die Uplink-Daten und die RSPAN-Daten über dieselbe Datenverbindung weiterleitet, benötigt das Gerät einen Reflektor-Port. Der Reflektor-Port markiert die RSPAN-VLAN-Daten mit der RSPAN-VLAN-ID. Anschließend leitet der Reflektor-Port die markierten Daten an das Zielgerät weiter. Hierfür verbindet der Netzadministrator 2 Ports am Quellgerät über ein Ethernet-Kabel miteinander.
- Ein Zielgerät aggregiert die mit der RSPAN-VLAN-ID markierten Daten und leitet die Daten an den Ziel-Port weiter. Im Zielgerät legen Sie im Feld *Quell-VLAN-ID* das RSPAN-VLAN fest. Der normale Datenstrom kann den Port gemeinsam mit den RSPAN-VLAN-Daten verwenden.
- Ein Zwischengerät flutet die mit der RSPAN-VLAN-ID markierten Daten zu den Ports mit RSPAN-VLAN-Mitgliedschaft. In einem Zwischengerät legen Sie im Feld *VLAN-ID* das RSPAN-VLAN fest. Das Gerät kann die RSPAN-VLAN-Daten über eine LAG-Verbindung an das RSPAN-Zielgerät übermitteln.

Das Gerät kann RSPAN-Daten über ein MRP-Ring-Netz an das Zielgerät weiterleiten, sofern das Ziel-Ring-Gerät kein Ring-Mitglied ist. Das Gerät ist außerdem in der Lage, RSPAN-Daten über eine LAG-Instanz weiterzuleiten, sofern die LAG-Ports keine Ziel-Ports sind.

Anmerkung: Um bei der Verwendung der Funktion *RSPAN* eine fehlerhafte Erkennung von Loops zu vermeiden, gehen Sie folgendermaßen vor. Wenn Sie über verschiedene Pfade für Uplink-Daten und RSPAN-Daten eine Verbindung zu den benachbarten Geräten herstellen, vergewissern Sie sich, dass das Spanning-Tree-Protokoll an beiden Ports der RSPAN-Datenverbindungen deaktiviert ist. Wenn Sie einen Reflektor-Port verwenden, vergewissern Sie sich, dass das Spanning-Tree-Protokoll an den Datenverbindungen deaktiviert ist, die RSPAN-Daten übertragen.

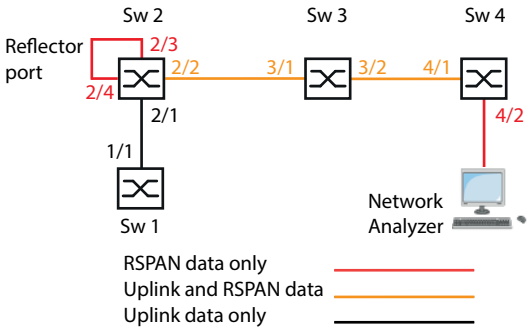
In den folgenden Beispielen möchte der Netzadministrator den Datenstrom zu einem Network Analyzer spiegeln, der sich innerhalb des Netzes befindet. Die Beispiele demonstrieren die verschiedenen Methoden zum Integrieren des Quellgeräts in Ihr Netz.

In den Beispielen möchte der Netzadministrator die Datenpakete von Switch 1, die Switch 2 auf Port 2/1 empfängt, an den Network Analyzer spiegeln, der mit Switch 4 verbunden ist. Der Netzadministrator hat für die RSPAN-VLAN-ID VLAN 30 festgelegt.

Anmerkung: Verwenden Sie ausschließlich RSPAN-fähige Geräte zum Weiterleiten der RSPAN-Daten.

Beispiel 1

In dem Beispiel konfigurieren Sie einen Reflektor-Port an Switch 2. Verbinden Sie mit einem Ethernet-Kabel die Ports 2/3 und 2/4. Die Verbindungen zwischen Switch 2, Switch 3 und Switch 4 übertragen sowohl den RSPAN-Datenstrom als auch den Uplink-Datenstrom. Führen Sie anschließend die folgenden Schritte aus:



Konfigurieren Sie Switch 2 als Port-Mirroring-Quelle.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert 30 fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert RSPAN_VLAN fest.
- ☐ Port 2/2 als Mitglied des RSPAN-VLANs festlegen:
  Legen Sie für VLAN 30 in Spalte *2/2* den Wert T fest.
- ☐ Das Weiterleiten von Management-Paketen an Port 2/4 blockieren:
  Legen Sie für VLAN 1 in Spalte *2/4* den Wert – fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Ziel-Port festlegen:
  Legen Sie im Rahmen *Ziel-Port* den Wert 2/3 fest.
- ☐ RSPAN-VLAN festlegen:
  Legen Sie im Rahmen *RSPAN*, Feld *VLAN-ID* den Wert 30 fest.
- ☐ Ziel-VLAN festlegen:
  Legen Sie im Rahmen *RSPAN*, Feld *Ziel-VLAN-ID* den Wert 30 fest.
- ☐ Datenquelle festlegen:
  Markieren Sie für Port 2/1 das Kontrollkästchen in Spalte *Eingeschaltet*.

- ☐ Richtung festlegen:
  Legen Sie für Port `2/1` in Spalte *Typ* den Wert `txrx` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Funktion *Spanning Tree* auf Port `2/4` deaktivieren:
  Heben Sie für Port `2/4` die Markierung des Kontrollkästchens in Spalte *STP aktiv* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN `30` auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN `30` den Namen `RSPAN_VLAN` zuweisen.
`rspan-vlan 30`	VLAN `30` als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`monitor session 1 source add interface 2/1`	Port `2/1` als Quell-Port zu Sitzung `1` hinzufügen.
`monitor session 1 destination interface 2/3`	Port `2/3` als Quell-Port zu Sitzung `1` hinzufügen.
`monitor session 1 destination remote vlan 30`	VLAN-Mirroring-Sitzung `1` erzeugen. Die Quelle ist VLAN `30`.
`monitor session 1 mode`	VLAN-Mirroring-Sitzung `1` aktivieren.
`interface 2/2`	In den Interface-Konfigurationsmodus von Interface `2/2` wechseln.
`vlan participation include 30`	Festlegen, dass Port `2/2` ein Mitglied von VLAN `30` ist.
`vlan tagging 30`	Festlegen, dass Port `2/2` Daten von VLAN `30` weiterleitet.
`exit`	In den Konfigurationsmodus wechseln.
`interface 2/4`	In den Interface-Konfigurationsmodus von Interface `2/4` wechseln.
`vlan participation auto 1`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`spanning-tree mode disable`	STP auf dem Port deaktivieren.
`exit`	In den Konfigurationsmodus wechseln.

Konfigurieren Sie Switch 3 als Zwischengerät.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert `30` fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert `RSPAN_VLAN` fest.
- ☐ Port `3/2` als Mitglied des RSPAN-VLANs festlegen:
  Legen Sie für VLAN `30` in Spalte *3/2* den Wert `T` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN `30` auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN `30` den Namen `RSPAN_VLAN` zuweisen.
`rspan-vlan 30`	VLAN `30` als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 3/2`	In den Interface-Konfigurationsmodus von Interface `3/2` wechseln.
`vlan participation include 30`	Festlegen, dass Port `3/2` ein Mitglied von VLAN `30` ist.
`vlan tagging 30`	Festlegen, dass Port `3/2` Daten von VLAN `30` weiterleitet.
`exit`	In den Konfigurationsmodus wechseln.

Konfigurieren Sie Switch 4 als Zielgerät.

Führen Sie die folgenden Schritte aus:

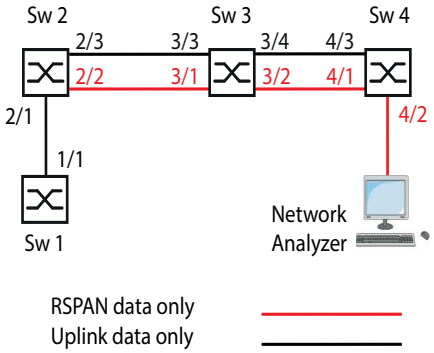
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert `30` fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert `RSPAN_VLAN` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Ziel-Port festlegen:
  Legen Sie im Rahmen *Ziel-Port* den Wert `4/2` fest.
- ☐ RSPAN-VLAN festlegen:
  Legen Sie im Rahmen *RSPAN*, Feld *VLAN-ID* den Wert `30` fest.

- Datenquelle festlegen:
  Legen Sie im Rahmen *RSPAN*, Feld *Quell-VLAN-ID* den Wert `30` fest.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN `30` auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN `30` den Namen `RSPAN_VLAN` zuweisen.
`rspan-vlan 30`	VLAN `30` als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`monitor session 1 source remote vlan 30`	VLAN `30` als RSPAN-Datenquelle festlegen.
`monitor session 1 destination interface 4/2`	Als Ziel-Port Port `4/2` festlegen.
`monitor session 1 mode`	VLAN-Mirroring-Sitzung `1` aktivieren.

Beispiel 2

In diesem Beispiel leitet das Netz die RSPAN-Daten und die Uplink-Daten über parallele Pfade vom Quellgerät zum Zielgerät weiter.



Konfigurieren Sie Switch 2 als Port-Mirroring-Quelle.

Führen Sie die folgenden Schritte aus:

- Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- VLAN hinzufügen:
  Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert `30` fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert `RSPAN_VLAN` fest.
- Port `2/3` als Nicht-Mitglied des RSPAN-VLANs festlegen:
  Legen Sie für VLAN `30` in Spalte *2/3* den Wert `–` fest.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Ziel-Port festlegen:
  Legen Sie im Rahmen *Ziel-Port* den Wert `2/2` fest.
- ☐ Ziel-VLAN festlegen:
  Legen Sie im Rahmen *RSPAN*, Feld *Ziel-VLAN-ID* den Wert `30` fest.
- ☐ Datenquelle festlegen:
  Markieren Sie für Port `2/1` das Kontrollkästchen in Spalte *Eingeschaltet*.
- ☐ Richtung festlegen:
  Legen Sie für Port `2/1` in Spalte *Typ* den Wert `txrx` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN `30` auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN `30` den Namen `RSPAN_VLAN` zuweisen.
`rspan-vlan 30`	VLAN `30` als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`monitor session 1 source add interface 2/1`	Port `2/1` als Quell-Port zu Sitzung `1` hinzufügen.
`monitor session 1 destination interface 2/3`	Port `2/3` als Quell-Port zu Sitzung `1` hinzufügen.
`monitor session 1 destination remote vlan 30`	VLAN-Mirroring-Sitzung `1` erzeugen. Die Quelle ist VLAN `30`.
`monitor session 1 mode`	VLAN-Mirroring-Sitzung `1` aktivieren.
`interface 2/3`	In den Interface-Konfigurationsmodus von Interface `2/3` wechseln.
`vlan participation auto 30`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`exit`	In den Konfigurationsmodus wechseln.

Konfigurieren Sie Switch 3 als Zwischengerät.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert `30` fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert `RSPAN_VLAN` fest.
- ☐ Port `3/1` als Nicht-Mitglied des Management-VLANs festlegen:
  Legen Sie für VLAN `1` in Spalte *3/1* den Wert `-` fest.
- ☐ Port `3/2` als Nicht-Mitglied des Management-VLANs festlegen:
  Legen Sie für VLAN `1` in Spalte *3/2* den Wert `-` fest.

- ☐ Port 3/2 als Mitglied des RSPAN-VLANs festlegen:
  Legen Sie für VLAN 30 in Spalte *3/2* den Wert T fest.
- ☐ Port 3/3 als Nicht-Mitglied des RSPAN-VLANs festlegen:
  Legen Sie für VLAN 30 in Spalte *3/3* den Wert – fest.
- ☐ Port 3/4 als Nicht-Mitglied des RSPAN-VLANs festlegen:
  Legen Sie für VLAN 30 in Spalte *3/4* den Wert – fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Funktion *Spanning Tree* auf Port 3/1 deaktivieren:
  Heben Sie für Port 3/1 die Markierung des Kontrollkästchens in Spalte *STP aktiv* auf.
- ☐ Funktion *Spanning Tree* auf Port 3/2 deaktivieren:
  Heben Sie für Port 3/2 die Markierung des Kontrollkästchens in Spalte *STP aktiv* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN 30 auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN 30 den Namen RSPAN_VLAN zuweisen.
`rspan-vlan 30`	VLAN 30 als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 3/1`	In den Interface-Konfigurationsmodus von Interface 3/1 wechseln.
`vlan participation auto 1`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`spanning-tree mode disable`	STP auf dem Port deaktivieren.
`exit`	In den Konfigurationsmodus wechseln.
`interface 3/2`	In den Interface-Konfigurationsmodus von Interface 3/2 wechseln.
`vlan participation include 30`	Festlegen, dass Port 3/2 ein Mitglied von VLAN 30 ist.
`vlan tagging 30`	Festlegen, dass Port 3/2 Daten von VLAN 30 weiterleitet.
`vlan participation auto 1`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`spanning-tree mode disable`	STP auf dem Port deaktivieren.
`exit`	In den Konfigurationsmodus wechseln.
`interface 3/3`	In den Interface-Konfigurationsmodus von Interface 3/3 wechseln.
`vlan participation auto 30`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`exit`	In den Konfigurationsmodus wechseln.
`interface 3/4`	In den Interface-Konfigurationsmodus von Interface 3/4 wechseln.
`vlan participation auto 30`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`exit`	In den Konfigurationsmodus wechseln.

Konfigurieren Sie Switch 4 als Zielgerät.

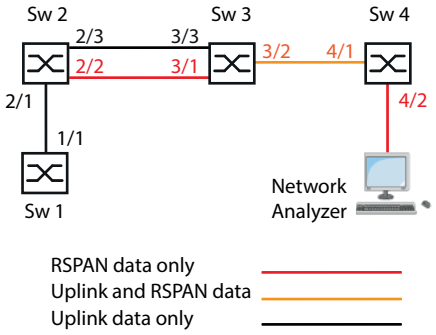
Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert `30` fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert `RSPAN_VLAN` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Ziel-Port festlegen:
  Legen Sie im Rahmen *Ziel-Port* den Wert `4/2` fest.
- ☐ Datenquelle festlegen:
  Legen Sie im Rahmen *RSPAN*, Feld *Quell-VLAN-ID* den Wert `30` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Funktion *Spanning Tree* auf Port `4/1` deaktivieren:
  Heben Sie für Port `4/1` die Markierung des Kontrollkästchens in Spalte *STP aktiv* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN `30` auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN `30` den Namen `RSPAN_VLAN` zuweisen.
`rspan-vlan 30`	VLAN `30` als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`monitor session 1 destination interface 4/2`	Als Ziel-Port Port `4/2` festlegen.
`monitor session 1 source remote vlan 30`	VLAN `30` als RSPAN-Datenquelle festlegen.
`monitor session 1 mode`	VLAN-Mirroring-Sitzung `1` aktivieren.
`interface 4/1`	In den Interface-Konfigurationsmodus von Interface `4/1` wechseln.
`spanning-tree mode disable`	STP auf dem Port deaktivieren.
`exit`	In den Konfigurationsmodus wechseln.

Beispiel 3

Im Beispiel sendet das Quell-Gerät Switch 2 die Uplink- und die RSPAN-Daten an das Zwischengerät Switch 3. Das Zwischengerät Switch 3 leitet den kombinierten Datenverkehr anschließend über eine einzelne Datenverbindung weiter an das Zielgerät Switch 4.



Konfigurieren Sie Switch 2 als Port-Mirroring-Quelle.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert `30` fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert `RSPAN_VLAN` fest.
- ☐ Port `2/3` als Mitglied des RSPAN-VLANs festlegen:
  Legen Sie für VLAN `30` in Spalte *2/3* den Wert `-` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Ziel-Port festlegen:
  Legen Sie im Rahmen *Ziel-Port* den Wert `2/2` fest.
- ☐ Ziel-VLAN festlegen:
  Legen Sie im Rahmen *RSPAN*, Feld *Ziel-VLAN-ID* den Wert `30` fest.
- ☐ Datenquelle festlegen:
  Markieren Sie für Port `2/1` das Kontrollkästchen in Spalte *Eingeschaltet*.
- ☐ Richtung festlegen:
  Legen Sie für Port `2/1` in Spalte *Typ* den Wert `txrx` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN `30` auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN `30` den Namen `RSPAN_VLAN` zuweisen.
`rspan-vlan 30`	VLAN `30` als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.

`configure`	In den Konfigurationsmodus wechseln.
`monitor session 1 destination interface 2/2`	Port `2/3` als Quell-Port zu Sitzung `1` hinzufügen.
`monitor session 1 destination remote vlan 30`	VLAN-Mirroring-Sitzung `1` erzeugen. Die Quelle ist VLAN `30`.
`monitor session 1 source add interface 2/1`	Port `2/1` als Quell-Port zu Sitzung `1` hinzufügen.
`monitor session 1 mode`	VLAN-Mirroring-Sitzung `1` aktivieren.
`interface 2/3`	In den Interface-Konfigurationsmodus von Interface `2/3` wechseln.
`vlan participation auto 30`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`exit`	In den Konfigurationsmodus wechseln.

Konfigurieren Sie Switch 3 als Zwischengerät.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert `30` fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert `RSPAN_VLAN` fest.
- ☐ Port `3/1` als Nicht-Mitglied des Management-VLANs festlegen:
  Legen Sie für VLAN `1` in Spalte *3/1* den Wert `-` fest.
- ☐ Port `3/2` als Mitglied des RSPAN-VLANs festlegen:
  Legen Sie für VLAN `30` in Spalte *3/2* den Wert `T` fest.
- ☐ Port `3/3` als Nicht-Mitglied des Management-VLANs festlegen:
  Legen Sie für VLAN `1` in Spalte *3/3* den Wert `-` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Funktion *Spanning Tree* auf Port `3/1` deaktivieren:
  Heben Sie für Port `3/1` die Markierung des Kontrollkästchens in Spalte *STP aktiv* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN `30` auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN `30` den Namen `RSPAN_VLAN` zuweisen.
`rspan-vlan 30`	VLAN `30` als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 3/1`	In den Interface-Konfigurationsmodus von Interface `3/1` wechseln.

`vlan participation auto 1`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`spanning-tree mode disable`	STP auf dem Port deaktivieren.
`exit`	In den Konfigurationsmodus wechseln.
`interface 3/2`	In den Interface-Konfigurationsmodus von Interface `3/2` wechseln.
`vlan participation include 30`	Festlegen, dass Port `3/2` ein Mitglied von VLAN `30` ist.
`vlan tagging 30`	Festlegen, dass Port `3/2` Daten von VLAN `30` weiterleitet.
`exit`	In den Konfigurationsmodus wechseln.
`interface 3/3`	In den Interface-Konfigurationsmodus von Interface `3/3` wechseln.
`vlan participation auto 30`	Der Port wird bei entsprechender Anfrage Teilnehmer in diesem VLAN.
`exit`	In den Konfigurationsmodus wechseln.

Konfigurieren Sie Switch 4 als Zielgerät.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ VLAN hinzufügen:
  Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
  Legen Sie im Feld *VLAN-ID* den Wert `30` fest.
  Klicken Sie die Schaltfläche *Ok*.
  Legen Sie in Spalte *Name* den Wert `RSPAN_VLAN` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Ziel-Port festlegen:
  Legen Sie im Rahmen *Ziel-Port* den Wert `4/2` fest.
- ☐ Datenquelle festlegen:
  Legen Sie im Rahmen *RSPAN*, Feld *Quell-VLAN-ID* den Wert `30` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`vlan add 30`	VLAN `30` auf dem Gerät erzeugen.
`name 30 RSPAN_VLAN`	Dem VLAN `30` den Namen `RSPAN_VLAN` zuweisen.
`rspan-vlan 30`	VLAN `30` als RSPAN-VLAN festlegen.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.

`monitor session 1 destination interface 4/2`	Als Ziel-Port Port `4/2` festlegen.
`monitor session 1 source remote vlan 30`	VLAN `30` als RSPAN-Datenquelle festlegen.
`monitor session 1 mode`	VLAN-Mirroring-Sitzung `1` aktivieren.

13.15 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, zum Beispiel 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 Geräts.

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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`selftest action task log-only`	Nachricht an das Ereignisprotokoll senden, wenn eine Aufgabe missglückt ist.
`selftest action resource send-trap`	Bei Ressourcen-Mangel einen SNMP-Trap senden.
`selftest action software send-trap`	Bei Verlust der Software-Integrität einen SNMP-Trap senden.
`selftest action hardware reboot`	Neustart des Geräts bei Beeinträchtigung der Hardware.

Das Deaktivieren dieser Funktionen ermöglicht Ihnen, die Zeit zu verkürzen, die zum Neustarten des Geräts nach einem Kaltstart erforderlich ist. Diese Optionen finden Sie im Dialog *Diagnose > System > Selbsttest*, Rahmen *Konfiguration*.

- Kontrollkästchen *RAM-Test*
  Aktiviert/deaktiviert den RAM-Selbsttest während eines Kaltstarts.

- Kontrollkästchen *SysMon1 ist verfügbar*
  Aktiviert/deaktiviert den System Monitor 1 während eines Kaltstarts.
- Kontrollkästchen *Bei Fehler Default-Konfiguration laden*
  Aktiviert/deaktiviert das Laden der Standard-Gerätekonfiguration, falls dem Gerät beim Neustart keine lesbare Konfiguration zur Verfügung steht.

Die folgenden Einstellungen sperren Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.

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

Dies ist zum Beispiel dann der Fall, wenn sich das Passwort des zu ladenden Konfigurationsprofils von dem im Gerät festgelegten Passwort unterscheidet. Um das Gerät wieder entsperren zu lassen, wenden Sie sich an Ihren Vertriebspartner.

Führen Sie die folgenden Schritte aus:

`selftest ramtest`	RAM-Selbsttest bei einem Kaltstart aktivieren.
`no selftest ramtest`	RAM-Selbsttest deaktivieren.
`selftest system-monitor`	System Monitor 1 aktivieren.
`no selftest system-monitor`	System Monitor 1deaktivieren.
`show selftest action`	Die durchzuführenden Maßnahmen bei einer Beeinträchtigung des Geräts anzeigen.

```
Cause     Action
--------- ----------
task      reboot
resource  reboot
software  reboot
hardware  reboot
```

`show selftest settings`	Die Selbsttest-Einstellungen anzeigen.

```
Selftest settings
-----------------
Test RAM on cold start.......................enabled
System Monitor 1............................enabled
Boot default configuration on error.........enabled
```

13.16 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. 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

13.17 Netzüberwachung mit sFlow

SFlow ist ein Standardprotokoll zur Überwachung von Netzen. Das Gerät stellt diese Funktion bereit, um Netzaktivitäten sichtbar zu machen, und ermöglicht auf diese Weise ein effektives Management und eine effektive Steuerung von Netzressourcen.

Das *SFlow*-Überwachungssystem besteht aus einem in das Gerät eingebetteten *SFlow*-Agenten und einem zentralen *SFlow*-Kollektor. Der Agent nutzt für die Erfassung von Datenverkehrsstatistiken die Abtasttechnologie. *SFlow*-Instanzen, die mit einzelnen Datenquellen im Agenten verbunden sind, führen die Abtastung von Paketflüssen und Zählern durch. Der Agent verwendet *SFlow*-Datagramme, um die abgetasteten Verkehrsstatistiken zur Analyse an den *SFlow*-Kollektor weiterzuleiten.

Der Agent verwendet 2 Methoden zur Abtastung: die statistische, paketbasierte Abtastung von Paketflüssen und die zeitbasierte Abtastung von Zählern. Ein *SFlow*-Datagramm enthält beide Stichprobenarten. Die Abtastung von Paketflüssen sendet auf der Grundlage der Abtastrate einen konstanten, jedoch beliebigen Datagramm-Strom an den Kollektor. Bei der zeitbasierten Abtastung fragt der Agent die Zähler zum Befüllen der Datagramme in einem festgelegten Intervall ab.

Das Gerät implementiert Datagramm-Version 5 für den *SFlow*-Agenten.

Die benutzerdefinierten *SFlow*-Funktionen sind:

- Sampler-Konfiguration, Abtastung von Paketflüssen:
  - Portnummer der Datenquelle zum Abtasten physischer Ports
  - Kennziffer des mit dem Sampler verknüpften Empfängers
  - Abtastrate
    Das Gerät zählt die Pakete von empfangenen Daten. Wenn der Zähler die benutzerdefinierte Anzahl erreicht, tastet der Agent das Paket ab.
    Bereich: `256..65535`
    `0` = Funktion inaktiv
  - Header-Größe in abzutastenden Bytes
    Bereich: `20..256`
- Poller-Konfiguration, Abtastung der Zähler:
  - Portnummer der Datenquelle, verfügbar für physische Ports
  - Kennziffer des mit dem Poller verknüpften Empfängers
  - Intervall in Sekunden zwischen den Stichproben
    Bereich: `0..86400`
- Empfängerkonfiguration, bis zu 8 Einträge:
  - Besitzername zur Kontrolle eines *SFlow*-Eintrages
  - Timeout in Sekunden, bis das Abtasten angehalten wird und das Gerät den Empfänger sowie den Sampler und den Poller freigibt
  - Datagram-Größe
  - IP-Adresse
  - Portnummer

Konfigurieren Sie zunächst einen verfügbaren Empfänger, um den *SFlow*-Agenten für eine Überwachungssitzung zu konfigurieren. Konfigurieren Sie anschließend eine Abtastrate, um das Abtasten von Paketflüssen durchzuführen. Konfigurieren Sie zudem ein Abfrageintervall für das Abtasten von Zählern.

Das Unternehmen XYZ beispielsweise möchte den Datenfluss auf einem Gerät überwachen. Die IP-Adresse für den Remote-Server mit dem -Kollektor lautet `10.10.10.10`. XYZ benötigt eine Stichprobe der ersten 256 Bytes von jedem 300. Paket. Darüber hinaus benötigt XYZ eine alle 400 Sekunden durchgeführte Zählerabfrage.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > SFlow > Empfänger*.
- ☐ Fügen Sie in Spalte *Name* den Wert `XYZ` als Namen der Person oder Organisation ein, die den Empfänger steuert.
- ☐ Legen Sie für die IP-Adresse des Remote-Servers, auf dem die *SFlow*-Kollektor-Software ausgeführt wird, in Spalte *IP-Adresse* den Wert `10.10.10.10` fest.
- ☐ Öffnen Sie den Dialog *Diagnose > SFlow > Konfiguration*, Registerkarte *Sampler*.
- ☐ Wählen Sie in Spalte *Empfänger* die Index-Nummer des in den vorigen Schritten festgelegten Empfängers aus.
- ☐ Legen Sie in Spalte *Abtastrate* den Wert `300` fest.
- ☐ Legen Sie in Spalte *Max. Header-Größe [Byte]* den Wert `256` fest.
- ☐ Öffnen Sie den Dialog *Diagnose > SFlow > Konfiguration*, Registerkarte *Poller*.
- ☐ Wählen Sie in Spalte *Empfänger* die Index-Nummer des in den vorigen Schritten festgelegten Empfängers aus.
- ☐ Legen Sie in Spalte *Intervall [s]* den Wert `400` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`sflow receiver 1 owner XYZ ip 10.10.10.10`	Einen *SFlow*-Empfänger konfigurieren.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`sflow sampler receiver 1 rate 300`	Zuweisen eines *SFlow*-Samplers an dem Port zu einem zuvor konfigurierten Empfänger mit einer Abtastrate von `300`.
`sflow sampler maxheadersize 256`	Einstellen der maximalen Header-Größe des *SFlow*-Samplers auf den Wert `256`.
`sflow poller receiver 1interval 400`	Zuweisen des *SFlow*-Poller zu dem zuvor konfigurierten Empfänger und zum Abtasten der Daten für `400` s.

14 Erweiterte Funktionen des Geräts

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 vermittelt 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 ermöglicht Ihnen, 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 ermöglicht Ihnen, 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 eine 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 ermöglicht Ihnen außerdem, 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 ermöglicht Ihnen Lücken in den IP-Adressbereichen.

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 dazu 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 `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dhcp-server pool add 1 static 192.168.23.42`	Eintrag mit Index `1` erzeugen. IP-Adresse `192.168.23.42` zum statischen Pool hinzufügen.
`dhcp-server pool modify 1 mode interface 1/1`	Statische Adresse des Eintrags mit Index `1` zu Interface `1/1` zuweisen.
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	IP-Adresse in Index `1` zu dem Gerät mit der MAC-Adresse `00:24:E8:D6:50:51` zuweisen.
`dhcp-server pool mode 1`	Pool-Eintrag mit Index `1` aktivieren.
`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`	DHCP-Server global aktivieren.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`dhcp-server operation`	Funktion *DHCP Server* für diesen Port aktivieren.

14.1.3 Beispiel: DHCP-Server – Dynamischer IP-Adressbereich

Das Gerät ermöglicht Ihnen, 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 dazu 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 `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	Dynamischen Pool mit einem IP-Bereich von `192.168.23.92` bis `192.168.23.142` einfügen.
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	Lease Time in Sekunden bzw. als unbegrenzt einfügen.
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	Dynamischen Pool mit einem IP-Bereich von `192.168.23.172` bis `192.168.23.180` einfügen.
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	Lease Time in Sekunden bzw. als unbegrenzt einfügen.
`dhcp-server pool mode 2`	Pool-Eintrag mit Index `2` aktivieren.
`dhcp-server pool mode 3`	Pool-Eintrag mit Index `3` aktivieren.
`dhcp-server operation`	DHCP-Server global aktivieren.
`interface 2/1`	In den Interface-Konfigurationsmodus von Interface `2/1` wechseln.
`dhcp-server operation`	Funktion *DHCP Server* für diesen Port aktivieren.

14.2 DHCP-L2-Relay

Ein Netzadministrator verwendet den DHCP-Schicht-2-*Relay-Agenten*, um DHCP-Client-Informationen hinzuzufügen. Schicht-3-*Relay-Agenten* und DHCP-Server benötigen diese Informationen, um einem Client eine Adresse und 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 Geräten im Netz 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 Geräte im Netz zwischen dem Client und dem Schicht-3-*Relay-Agenten* oder DHCP-Server, zum Beispiel Switches. In diesem Fall stellt das Gerät einen Schicht-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.

14.2.1 Circuit- und Remote-IDs

In einer IPv4-Umgebung fügt das Gerät die *Circuit-ID* und die *Remote-ID* 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-*Relay-Agenten* wieder an den ursprünglichen Client zurückzuleiten. 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* ermöglicht Ihnen, die Funktion auf den aktiven Ports und in den VLANs zu aktivieren. Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*. Klicken Sie anschließend die Schaltfläche ✓.

Das Gerät leitet DHCPv4-Pakete mit *Option 82*-Information an diejenigen 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 Funktion *DHCP-L2-Relay*, lassen das Kontrollkästchen in Spalte *Gesicherter Port* jedoch unmarkiert. Auf diesen Ports verwirft das Gerät DHCPv4-Pakete mit *Option 82*-Information.

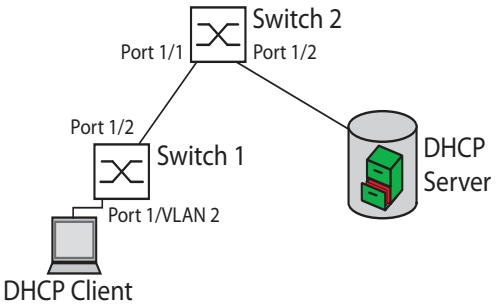


Abb. 77: Beispiel: DHCP-Schicht-2-Netz

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-ID*.
- 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 `An`.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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 `An`.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Vergewissern Sie sich, dass VLAN 2 vorhanden ist. Führen Sie dann an Switch 1 die folgenden Schritte aus:

- Richten Sie das VLAN 2 ein und legen Sie Port `1/1` als Mitglied des VLAN 2 fest.

`enable`	In den Privileged-EXEC-Modus wechseln.
`vlan database`	In den VLAN-Konfigurationsmodus wechseln.
`dhcp-l2relay circuit-id 2`	Circuit-ID und DHCP-Option-82 in VLAN `2` aktivieren.

`dhcp-l2relay remote-id ip 2`	IP-Adresse des Geräts als Remote-ID in VLAN `2` festlegen.
`dhcp-l2relay mode 2`	Funktion *DHCP-L2-Relay* in VLAN `2` aktivieren.
`exit`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`dhcp-l2relay mode`	Funktion *DHCP-L2-Relay* auf dem Port aktivieren.
`exit`	In den Konfigurationsmodus wechseln.
`interface 1/2`	In den Interface-Konfigurationsmodus von Interface `1/2` wechseln.
`dhcp-l2relay trust`	Port als *Gesicherter Port* festlegen.
`dhcp-l2relay mode`	Funktion *DHCP-L2-Relay* auf dem Port aktivieren.
`exit`	In den Konfigurationsmodus wechseln.
`dhcp-l2relay mode`	Funktion *DHCP-L2-Relay* auf dem Gerät einschalten.

Führen Sie an Switch 2 die folgenden Schritte aus:

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`dhcp-l2relay trust`	Port als *Gesicherter Port* festlegen.
`dhcp-l2relay mode`	Funktion *DHCP-L2-Relay* auf dem Port aktivieren.
`exit`	In den Konfigurationsmodus wechseln.
`interface 1/2`	In den Interface-Konfigurationsmodus von Interface `1/2` wechseln.
`dhcp-l2relay trust`	Port als *Gesicherter Port* festlegen.
`dhcp-l2relay mode`	Funktion *DHCP-L2-Relay* auf dem Port aktivieren.
`exit`	In den Konfigurationsmodus wechseln.
`dhcp-l2relay mode`	Funktion *DHCP-L2-Relay* auf dem Gerät einschalten.

14.3 Gerät als DNS-Client verwenden

Der DNS-Client fordert die DNS-Server dazu auf, die Host-Namen und IP-Adressen von Geräten im Netz aufzulösen. Der DNS-Client konvertiert Namen von Geräten, ähnlich einem Telefonbuch, in IP-Adressen. Wenn der DNS-Client die Aufforderung erhält, einen neuen Namen aufzulösen, führt er die Abfrage der Informationen zunächst in seiner internen statischen Datenbank und anschließend in den zugewiesenen DNS-Servern durch. Der DNS-Client speichert die abgefragten Informationen in einem Cache-Speicher für zukünftige Anfragen.

Das Gerät ermöglicht Ihnen, den DNS-Client vom DHCP-Server über das Management-VLAN zu konfigurieren. Das Gerät ermöglicht Ihnen außerdem, die Hostnamen statisch den IP-Adressen zuzuordnen.

Der DNS-Client bietet folgende Benutzerfunktionen:
- DNS-Server-Liste mit Platz für bis zu 4 DNS-IP-Adressen.
- Mapping von statischen Host-Namen zu IP-Adressen mit Platz für bis zu 64 konfigurierbare statische Hosts
- Host-Cache mit Platz für 128 Einträge

14.3.1 Beispiel: DNS-Server konfigurieren

Geben Sie den Namen für den DNS-Client an, und konfigurieren Sie diesen so, dass er einen DNS-Server dazu auffordert, Host-Namen aufzulösen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DNS > Client > Statisch*.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Konfigurationsquelle* den Wert `user` fest.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Domänen-Name* den Wert `device1` fest.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche ⊞.
- ☐ Legen Sie in Spalte *Adresse* den Wert `192.168.3.5` als IPv4-Adresse des DNS-Servers fest.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Öffnen Sie den Dialog *Erweitert > DNS > Client > Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dns client source user`	Festlegen, dass der Benutzer die Einstellungen des DNS-Clients manuell festlegt.
`dns client domain-name device1`	Zeichenfolge `device1` als eindeutigen Domänennamen für das Gerät festlegen.
`dns client servers add 1 ip 192.168.3.5`	Hinzufügen eines DNS-Namensservers mit einer IPv4-Adresse von `192.168.3.5` als Index `1`.
`dns client adminstate`	Funktion *DNS-Client* global einschalten.

Konfigurieren Sie den DNS-Client so, dass er statische Hosts mit IP-Adressen abbildet. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DNS > Client > Statische Hosts*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche ⊞.
- ☐ Fügen Sie in Spalte *Name* den Wert `example.com` ein.
  Dabei handelt es sich um den Namen eines Geräts im Netz.
- ☐ Legen Sie in Spalte *IP-Adresse* den Wert `192.168.3.9` fest.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`dns client host add 1 name example.com ip 192.168.3.9`	Statischen Host `example.com` mit IP-Adresse `192.168.3.9` hinzufügen.
`dns client adminstate`	Funktion *DNS-Client* global einschalten.

14.4 Digitales I/O-Modul

Verwenden Sie diese Funktion für die Überwachung von Remote-Kontakten. Für Eingänge und Ausgänge wird eine zyklische Anwendung ausgeführt, die die Werte der konfigurierten Eingänge auf Fern- oder lokalen I/O-Modulen abruft und diese Werte auf die Ausgänge spiegelt. Das Gerät fragt die lokalen Eingänge ab, um ihren Status einzustellen. Wenn diese Funktion aktiviert ist, erzeugt das Gerät Ereignisprotokoll-Einträge und SNMP-Traps für Änderungen der Ein- und Ausgangswerte.

14.4.1 Digitale I/O-Signale verwalten

Das digitale I/O-Modul bietet folgende Benutzerfunktionen:

- steuerbare Eingänge am Stromversorgungsmodul
- Spiegeln eines Ausgangs auf einen Eingang (1:1)
- Spiegeln desselben Eingangs auf verschiedene Ausgänge (1:N-Spiegelung)
- konfigurierbares Aktualisierungsintervall sowohl für Eingänge als auch für Ausgänge für die Statusaktualisierung
- Das Gerät sendet SNMP-Anfragen, um den Status von entfernten oder lokalen Eingängen abzurufen.

Beispiel

Eine leuchtende Lampe im Kontrollraum zeigt, dass eine Schranktür geöffnet ist. Die IP-Adresse des Schrankgeräts lautet 192.168.0.11. Eingang 1 an einem I/O-Modul in Steckplatz 3 leitet den Status des Schranktürkontakts weiter. Ausgang 4 an einem I/O-Modul in Steckplatz 2 des Kontrollraumgeräts empfängt den Status des Kontakts und schaltet eine Lampe ein, wenn die Tür geöffnet ist. Bei dem Status des Türkontakts handelt es sich um einen Eingang, der für andere Geräte verfügbar ist.

Konfigurieren Sie das Schrankgerät so, dass es das Signal vom Türkontakt empfängt. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > Digital-IO Modul*, Registerkarte *IO-Eingang*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`digital-input admin-state`	Aktivieren der Eingangsfunktion auf dem Gerät.

Aktivieren Sie am Kontrollraumgerät die Eingangs- und Ausgangsfunktion, und spiegeln Sie Eingang 1 an Modul 3 des Schrankgeräts auf Ausgang 4 am I/O-Modul in Steckplatz 2.

- ☐ Öffnen Sie den Dialog *Erweitert > Digital-IO Modul*, Registerkarte *IO-Ausgang*.
- ☐ Legen Sie in Spalte *Quell-Adresse* den Wert `192.168.0.11` fest.
- ☐ Legen Sie für *Output-ID* = `2/4` in Spalte *Input-ID* den Wert `3/1` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`digital-output mirror io 2/4 192.168.0.11:161 3/1`	Modul 3, Eingang 1 des Schrankgeräts auf Steckplatz 2, Ausgang 4 spiegeln.
`digital-output admin-state`	Aktivieren der Ausgangsfunktion auf dem Gerät.
`digital-input admin-state`	Aktivieren der Eingangsfunktion auf dem Gerät.

14.5 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 Funktion *GARP* registriert oder entfernt, wird der Teilnehmer auf der Grundlage spezifischer Regeln geändert. Bei den Teilnehmern handelt es sich um eine Reihe erreichbarer Endgeräte und Geräte im Netz. 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.

14.5.1 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 Geräte im Netz und Endgeräte bereitstellt. Die Geräte registrieren Informationen zur Gruppenmitgliedschaft mit den Geräten, die mit demselben LAN-Segment verbunden sind. Die Funktion *GARP* ermöglicht den Geräten außerdem, die Informationen über Geräte im Netz hinweg zu verbreiten, die erweiterte Filterdienste unterstützen.

Anmerkung: Vergewissern Sie sich vor dem Einschalten der Funktion *GMRP*, dass die Funktion *MMRP* ausgeschaltet ist.

Das folgende Beispiel beschreibt die Konfiguration der Funktion *GMRP*. Das Gerät unterstützt eingeschränktes Multicast-Flooding für einen ausgewählten Port. Führen Sie dazu 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`garp gmrp operation`	Funktion *GMRP* auf dem Port einschalten.
`exit`	In den Konfigurationsmodus wechseln.
`garp gmrp operation`	Funktion *GMRP* global einschalten.

14.5.2 GVRP konfigurieren

Verwenden Sie die Funktion *GVRP*, 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 Funktion *GVRP* dynamisch VLANs auf Geräten, die über 802.1Q-Trunk-Ports angeschlossen sind.

Das folgende Beispiel beschreibt die Konfiguration der Funktion *GVRP*. Das Gerät ermöglicht Ihnen, VLAN-Konfigurationsinformationen mit anderen *GVRP*-Geräten auszutauschen. Führen Sie dazu 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 3/1`	In den Interface-Konfigurationsmodus von Interface `3/1` wechseln.
`garp gvrp operation`	Funktion *GVRP* auf dem Port einschalten.
`exit`	In den Konfigurationsmodus wechseln.
`garp gvrp operation`	Funktion *GVRP* global einschalten.

14.6 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.

14.6.1 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 auf dem 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.

14.6.2 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.

14.6.3 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*) ermöglicht Ihnen, 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 Funktion *MMRP* 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.

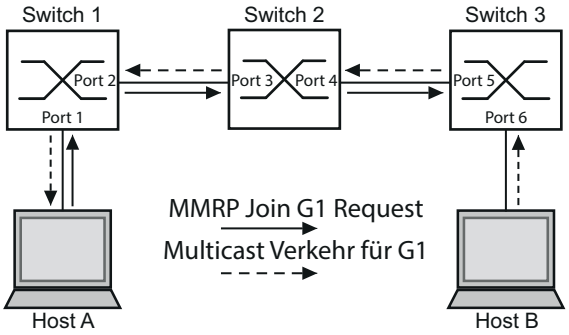


Abb. 78: MMRP-Netz für MAC-Adressen-Registrierung

Schalten Sie die *MMRP*-Funktion auf den Switches ein. Führen Sie dazu 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 1 und Port 2.
- Um Port 3 und Port 4 als *MMRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 2 das Kontrollkästchen in Spalte *MMRP* für Port 3 und Port 4.
- Um Port 5 und Port 6 als *MMRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 3 das Kontrollkästchen in Spalte *MMRP* für Port 5 und Port 6.
- 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 *An*.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Um die *MMRP*-Ports an Switch 1 einzuschalten, verwenden Sie die folgenden Kommandos. Schalten Sie die Funktion *MMRP* und Ports an den Switches 2 und 3 ein, indem sie in den Kommandos die entsprechenden Interfaces ersetzen.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`mrp-ieee mmrp operation`	Funktion *MMRP* auf dem Port einschalten.
`interface 1/2`	In den Interface-Konfigurationsmodus von Interface `1/2` wechseln.
`mrp-ieee mmrp operation`	Funktion *MMRP* auf dem Port einschalten.
`exit`	In den Konfigurationsmodus wechseln.
`mrp-ieee mrp periodic-state-machine`	Funktion *Periodische State-Machine* global einschalten.
`mrp-ieee mmrp operation`	Funktion *MMRP* global einschalten.

14.6.4 MVRP

Das Multiple-VLAN-Registration-Protokoll (*MVRP*) ist eine MRP-Anwendung, die Dienste für die dynamische VLAN-Registrierung und -rücknahme bietet.

Die Funktion *MVRP* 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 Funktion *MVRP* 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. Wenn an den Switches STP eingeschaltet ist, sind die Ports, die Switch 1 und Switch 4 verbinden, zur Vermeidung von Loops im „Discarding“-Status.

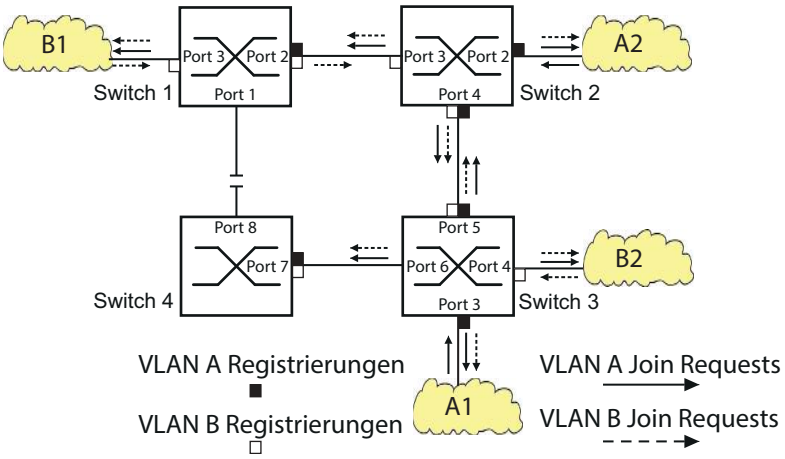


Abb. 79: MVRP-Beispiel-Netz für VLAN-Registrierung

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.

Schalten Sie MVRP auf den Switches ein. Führen Sie dazu 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 1 bis 3.
- Um die Ports 2 bis 4 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 2 das Kontrollkästchen in Spalte *MVRP* für die Ports 2 bis 4.

- Um die Ports 3 bis 6 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 3 das Kontrollkästchen in Spalte *MVRP* für die Ports 3 bis 6.
- Um Port 7 und Port 8 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 4 das Kontrollkästchen in Spalte *MVRP* für Port 7 und Port 8.
- Um die Registrierung der VLANs zu aufrecht zu erhalten, schalten Sie die *Periodische State-Machine* ein.
  Wählen Sie im Rahmen *Konfiguration* das Optionsfeld *An*.
- Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Um die *MVRP*-Ports an Switch 1 einzuschalten, verwenden Sie die folgenden Kommandos. Schalten Sie die Funktionen *MVRP* und Ports an den Switches 2, 3 und 4 ein, indem Sie in den Kommandos die entsprechenden Interfaces ersetzen.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`interface 1/1`	In den Interface-Konfigurationsmodus von Interface `1/1` wechseln.
`mrp-ieee mvrp operation`	Funktion *MVRP* auf dem Port einschalten.
`interface 1/2`	In den Interface-Konfigurationsmodus von Interface `1/2` wechseln.
`mrp-ieee mvrp operation`	Funktion *MVRP* auf dem Port einschalten.
`exit`	In den Konfigurationsmodus wechseln.
`mrp-ieee mvrp periodic-state-machine`	Funktion *Periodische State-Machine* global einschalten.
`mrp-ieee mvrp operation`	Funktion *MVRP* global einschalten.

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 zu kommunizieren.

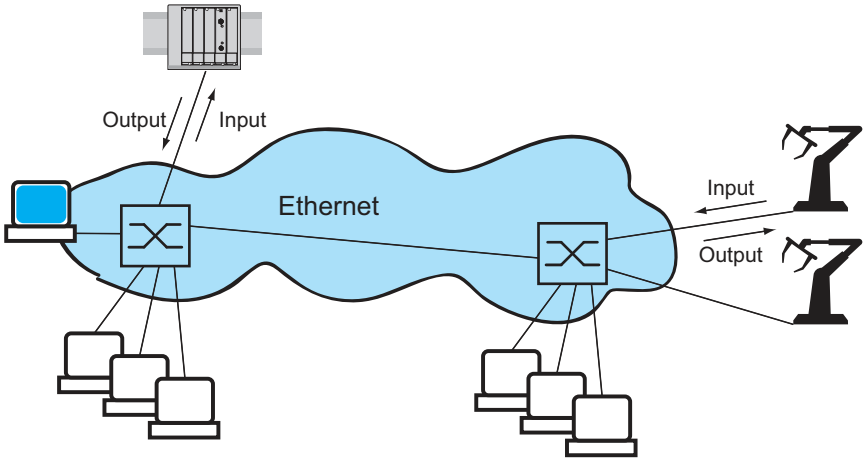


Abb. 80: Beispiel für die Kommunikation.

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 Geräts sowie die Systemstruktur in maschinell verarbeitbarer Form. Die mit SCL beschriebenen Eigenschaften des Geräts 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.

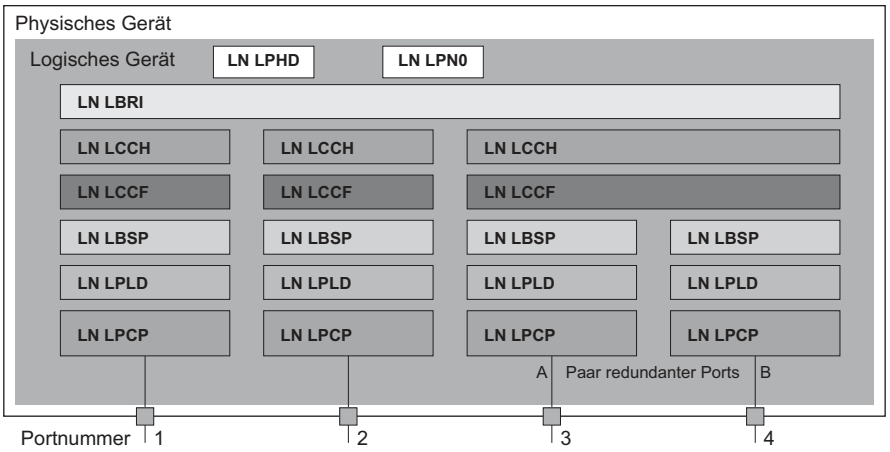


Abb. 81: Bridge-Modell nach Technical Report IEC 61850 90-4

Tab. 50: Klassen des Bridge-Modells nach TR IEC61850 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 Geräts ab.
`LN LCCH`	Logischer Knoten `Communication Channel`: Definiert den logischen `Communication Channel`, der aus einem oder mehreren physischen Geräteports besteht.

Tab. 50: Klassen des Bridge-Modells nach TR IEC61850 90-4 (Forts.)

Klasse	Beschreibung
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.

15.1.2 Integration in ein Steuerungssystem

Vorbereitung des Geräts

Führen Sie die folgenden Schritte aus:

- ☐ 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 *An* und klicken die Schaltfläche ✓.
  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.

IEC61850/MMS bietet keine Authentifizierungsmechanismen. Wenn der Schreibzugriff für IEC61850/MMS eingeschaltet ist, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Geräts zu ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Geräts und zu Ausfällen im Netz.

HINWEIS

GEFAHR DES UNAUTORISIERTEN ZUGRIFFS AUF DAS GERÄT

Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (zum Beispiel Firewall, VPN etc.) getroffen haben, um die Möglichkeit eines unbefugten Zugriffs zu verringern.

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 ermöglicht Ihnen, mit Hilfe der grafischen Benutzeroberfläche die ICD-Datei herunterzuladen. Diese Datei enthält die mit SCL beschriebenen Eigenschaften des Geräts 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 ⬇.

Gerät überwachen

Der im Gerät integrierte IEC61850/MMS-Server ermöglicht Ihnen, mehrere Stati des Geräts per Report Control Block (RCB) zu überwachen. Bis zu 5 MMS-Clients können sich gleichzeitig für einen Report Control Block anmelden.

Das Gerät ermöglicht Ihnen, die folgenden Zustände zu überwachen:

Tab. 51: Mit IEC 61850/MMS überwachbare Stati des Geräts

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 des RCB-Objekts `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.

Tab. 51: Mit IEC 61850/MMS überwachbare Stati des Geräts (Forts.)

Klasse	RCB-Objekt	Beschreibung
LN LBRI	RstpRoot	Ändert sich, wenn das Gerät die Rolle der Root-Bridge übernimmt oder abgibt.
	RstpTopoCnt	Ändert sich, wenn sich die Topologie auf Grund eines Wechsels der Root-Bridge ändert.
LN LCCH	ChLiv	Ändert sich, wenn sich der Link-Status des physischen Ports ändert.
LN LPCP	PhyHealth	Ändert sich, wenn sich der Link-Status des physischen Ports ändert.

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 Funktion *Modbus TCP* ermöglicht Ihnen, 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.

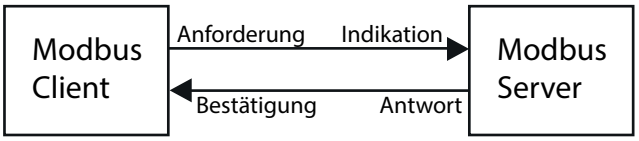


Abb. 82: Modbus TCP/IP Client/Server-Modus

Um Daten zwischen dem Client und dem Server auszutauschen, verwendet das Client/Server-Modell 4 Nachrichtentypen:

- Modbus TCP/IP-Anfrage; der Client erzeugt eine Informationsanforderung und sendet sie an den Server.
- Modbus TCP/IP-Hinweis; der Server empfängt eine Anfrage als Hinweis, dass ein Client Informationen anfordert.
- Modbus TCP/IP-Antwort; wenn die angeforderten Informationen verfügbar sind, sendet der Server eine Antwort mit den angeforderten Informationen. Wenn die angeforderten Informationen nicht verfügbar sind, sendet der Server eine Ausnahmeantwort, um den Client über den während der Verarbeitung erkannten Fehler zu benachrichtigen. Die Ausnahmeantwort enthält einen Ausnahmecode, der die Ursache des erkannten Fehlers angibt.
- Modbus TCP/IP-Bestätigung; der Client empfängt eine Antwort vom Server mit den angeforderten Informationen.

15.2.2 Unterstützte Funktionen und Speicherzuordnung

Das Gerät unterstützt Funktionen mit den öffentlichen Codes `0x03` (`Read Holding Registers`) und `0x05` (`Write Single Coil`). Die Codes ermöglichen Ihnen, in den Registern gespeicherte Informationen zu lesen, zum Beispiel Systeminformationen einschließlich Systemname, Systemstandort, Software-Version, IP-Adresse und MAC-Adresse. Die Codes ermöglichen Ihnen außerdem, die Port-Informationen und die Port-Statistik zu lesen. Der Code `0x05` ermöglicht Ihnen, 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, codiert 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

Tab. 52: 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
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

Port-Statistik

Tab. 53: 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
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

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.

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 Geräts zu ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Geräts und zu Ausfällen im Netz.

HINWEIS

GEFAHR DES UNAUTORISIERTEN ZUGRIFFS AUF DAS GERÄT

Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (zum Beispiel Firewall, VPN etc.) getroffen haben, um die Möglichkeit eines unbefugten Zugriffs zu verringern.

Die Nichtbeachtung dieser Anweisungen kann zu Geräteschäden führen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung*.
- ☐ Fügen Sie einen neuen Tabelleneintrag hinzu. Klicken Sie dazu die Schaltfläche ⊞.
- ☐ Legen Sie den IP-Adressbereich in der Zeile fest, in der die Spalte *Index* den Wert `2` hat. Fügen Sie dazu die folgenden Werte ein:
  - In Spalte *Adresse*: `10.17.1.0`
  - In Spalte *Netzmaske*: `255.255.255.248`
- ☐ Vergewissern Sie sich, dass das Kontrollkästchen in Spalte *Modbus TCP* markiert ist.
- ☐ Aktivieren Sie den IP-Adressbereich. Markieren Sie dazu das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*.
- ☐ Vergewissern Sie sich, dass das Kontrollkästchen für den Parameter *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 `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Wenn Sie die Funktion *Modbus TCP* einschalten, erkennt die Funktion *Sicherheitsstatus* die Aktivierung und zeigt einen Alarm im Dialog *Grundeinstellungen > System*, Rahmen *Sicherheits-Status*.

`enable`	In den Privileged-EXEC-Modus wechseln.
`network management access add 2`	Eintrag für den Adressbereich im Netz erzeugen. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: `2`.
`network management access modify 2 ip 10.17.1.0`	IP-Adresse festlegen.
`network management access modify 2 mask 29`	Netzmaske festlegen.
`network management access modify 2 modbus-tcp enable`	Festlegen, dass das Gerät *Modbus TCP* Zugriff auf das Management des Geräts ermöglicht.
`network management access operation`	IP-Zugriffsbeschränkung einschalten.
`configure`	In den Konfigurationsmodus wechseln.
`security-status monitor modbus-tcp-enabled`	Festlegen, dass das Gerät die Aktivierung des *Modbus TCP*-Servers überwacht.
`modbus-tcp operation`	*Modbus TCP*-Server einschalten.
`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`	Die Sicherheitsstatus-Einstellungen anzeigen.

```
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
```

Die Regeln für den eingeschränkten Management-Zugriff für Index 1 anzeigen.

```
Restricted management access settings
-------------------------------------
Index.......................................1
IP Address..................................10.17.1.0
Prefix Length...............................29
HTTP........................................yes
SNMP........................................yes
Telnet......................................yes
SSH.........................................yes
HTTPS.......................................yes
IEC61850-MMS................................yes
Modbus TCP/IP...............................yes
Active......................................[x]
```

15.3 EtherNet/IP

EtherNet/IP ist ein weltweit eingesetztes industrielles Kommunikationsprotokoll, das von der Open DeviceNet Vendor Association (ODVA) gepflegt wird. Es basiert auf den Protokollen *TCP/IP* und *UDP/IP* über Ethernet. *EtherNet/IP* wird von führenden Herstellern unterstützt und bietet daher eine breite Grundlage für den effektiven Datenverkehr im Industriebereich.

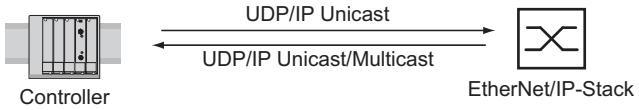


Abb. 83: EtherNet/IP-Netz

EtherNet/IP erweitert die Standard-Ethernet-Protokolle um das Industrieprotokoll CIP (Common Industrial Protocol). *EtherNet/IP* implementiert CIP in der Sitzungsschicht und darüber und passt CIP der spezifischen *EtherNet/IP*-Technologie in der Transportschicht und darunter an. Bei Automatisierungsanwendungen implementiert *EtherNet/IP* CIP auf Anwendungsebene. Daher ist *EtherNet/IP* optimal für den Bereich der industriellen Steuerungstechnik geeignet.

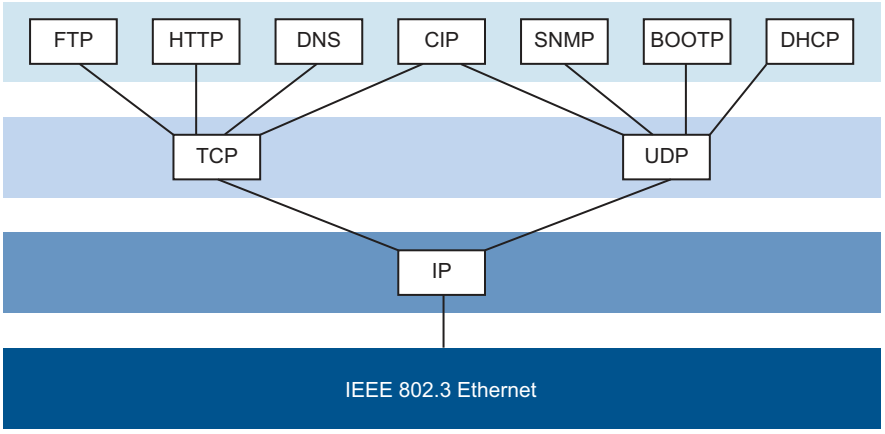


Abb. 84: IEEE802.3 EtherNet/IP

EtherNet/IP treffen Sie insbesondere in den USA und im Verbindung mit Rockwell-Steuerungen an.

Weitere Informationen zu EtherNet/IP finden Sie auf der ODVA-Webseite unter www.odva.org.

15.3.1 Integration in ein Steuerungssystem

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Global*.
  Vergewissern Sie sich, dass die Funktion *IGMP-Snooping* eingeschaltet ist.
- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > EtherNet/IP*.
  Vergewissern Sie sich, dass die Funktion *EtherNet/IP* eingeschaltet ist.
- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > EtherNet/IP*.
- ☐ Um das EDS als ZIP-Archiv auf Ihrem PC zu speichern, klicken Sie *Download*.
  Das ZIP-Archiv enthält die *EtherNet/IP*-Konfigurationsdatei und das Symbol, über das eine Verbindung zwischen der Steuerung und dem Gerät konfiguriert wird.

Konfiguration einer SPS am Beispiel der Rockwell-Software

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie das „EDS Hardware Installation Tool“ von RSLinx.
- ☐ Fügen Sie mit dem „EDS Hardware Installation Tool“ die EDS-Datei hinzu.
- ☐ Starten Sie den Dienst „RSLinx“ neu, damit RSLinx die EDS-Datei des Geräts übernimmt.
- ☐ Prüfen Sie mit RSLinx, ob RSLinx das Gerät erkannt hat.
- ☐ Öffnen Sie Ihr Logix 5000 - Projekt.
- ☐ Binden Sie das Gerät als neues Modul (Generic Ethernet Module) am Ethernet-Port des Controllers ein.

Tab. 54: Einstellungen zum Einbinden eines Generic Ethernet Module

Einstellung	I/O-Verbindung	Input only	Listen only
Comm Format	Data - DINT	Data - DINT	Input data - DINT - Run/Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	2	2	2
Input Size	7	7	7
Output Assembly Instance	1	254	255
Output Size	1	0	0
Configuration Assembly Instance	3	3	3
Configuration Size	0	0	0

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

Anmerkung: Die Überwachung der I/O-Verbindung zur CPU des Geräts kann bei einem erkannten Fehler zum potenziellen Systemausfall führen. Berücksichtigen Sie bei der Überwachung deshalb nicht die I/O-Verbindung zur CPU.

Die I/O-Verbindung zwischen der speicherprogrammierbaren Steuerung (SPS) und dem Gerät kann durch ein Management-Programm unterbrochen werden. Beispielsweise kann eine Netzmanagementstation die CPU des Geräts mit Echtzeitdaten (RT-Daten) mit einer höheren Priorität auslasten. In diesem Fall kann das Gerät weiterhin Datenpakete senden oder empfangen, und das System bleibt betriebsbereit.

Beispiel zur Integration aus der Sample Code Library

Die Sample Code Library ist eine Web-Seite von Rockwell. Sie hat das Ziel, den Anwendern einen Platz zu bieten, an welchem sie ihre besten Architekturintegrations-Anwendungen austauschen können.

Suchen Sie auf der Webseite samplecode.rockwellautomation.com nach der „Catalog Number“ 9701. Das ist die Katalognummer für ein Beispiel zur Integration des Hirschmann-Geräts in RS Logix 5000 Rel. 16, SPS-Firmware Release 16.

15.3.2 EtherNet/IP-Entity-Parameter

Die folgenden Absätze identifizieren die Objekte und Operationen, die das Gerät unterstützt.

Unterstützte Operationen

Tab. 55: Übersicht über die unterstützten Etnernet/IP-Requests für die Objektinstanzen.

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: USINT VlanId ARRAY of: 6 USINT Mac DWORD Port-Mask	–

Identity-Objekt

Das Gerät unterstützt das Identity-Objekt (Class Code 0x01) von *EtherNet/IP*. Die Hersteller-ID von Hirschmann lautet 634. Zur Kennzeichnung des Produkttyps „Hirschmann“ verwendet 44 (0x2C) die ID Managed Ethernet Switch.

Tab. 56: Instanz-Attribute (ausschließlich Instanz 1 ist verfügbar)

Id	Attribute	Access Rule	Data type	Description
0x1	Vendor ID	Get	UINT	Hirschmann634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type

Tab. 56: Instanz-Attribute (ausschließlich Instanz 1 ist verfügbar) (Forts.)

Id	Attribute	Access Rule	Data type	Description
0x4	Revision	Get	STRUCT of: USINT Major USINT Minor	Revision of the EtherNet/IP implementation, 2.1.
0x5	Status	Get	WORD	Support for the following Bit status only: 0: Owned (always 1) 2: Configured (always 1) 4: Extend Device Status 5: 6: 7: 0x3: No I/O connection established 0x7: At least one I/O connection established, all in idle mode.
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Hirschmann" + product family + product ID + software variant.

TCP/IP Interface Object

Das Gerät unterstützt ausschließlich Instanz 1 des TCP/IP-Objektes (Class Code 0xF5) von *EtherNet/IP*.

In Abhängigkeit vom Schreibzugriff-Status speichert das Gerät die vollständige Konfiguration im Flash-Speicher des Geräts. Das Speichern der Konfigurationsdatei kann bis zu 10 Sekunden in Anspruch nehmen. Wird der Speichervorgang unterbrochen, zum Beispiel durch Ausfall des Netzteils, ist der Betrieb des Geräts wahrscheinlich nicht möglich.

Anmerkung: Das Gerät reagiert auf die Konfigurationsänderung `Get Request` mit einer `Response`, selbst wenn der Speichervorgang für die Konfiguration noch nicht abgeschlossen ist.

Tab. 57: Class-Attribute

Id	Attribute	Access Rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances currently created: 1

Tab. 58: Attribute der Instanz 1

Id	Attribute	Access Rule	Data type	Description
0x1	Status	Get	DWORD	0: Interface Status (0=Interface not configured, 1=Interface contains valid config)
				6: ACD status (default 0)
				7: ACD fault (default 0)
0x2	Interface Capability flags	Get	DWORD	0: BOOTP Client
				1: DNS Client
				2: DHCP Client
				3: DHCP-DNS Update
				4: Configuration setable (within CIP) Other bits reserved (0)
				7: ACD capable (0=not capable, 1=capable)
0x3	Config Control	Set/Get	DWORD	0: 0x0=using stored config 1: 0x1=using BOOTP 2: 0x2=using DHCP 3:
				4: One device uses DNS for name lookup (always 0 because it is not supported) Other bits reserved (0)
0x4	Physical Link Object	Get	STRUCT of:	Path to the Physical Link Object, always {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
			UINT PathSize	
			EPATH Path	
0x5	Interface Configuration	Set/Get	STRUCT of:	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
			UDINT IpAddress	
			UDINT Netmask	
			UDINT GatewayAddress	
			UDINT NameServer1	
			UDINT NameServer2	
			STRING DomainName	
0x6	Host Name	Set/Get	STRING	Host Name (for DHCP DNS Update)
0x7	Safety Network Number			Not supported
0x8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets Range 1..255 (default = 1)

Tab. 58: Attribute der Instanz 1 (Forts.)

Id	Attribute	Access Rule	Data type	Description
0x9	Mcast Config	Get/Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable (default)
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters

Tab. 59: Hirschmann-Erweiterungen des TCP/IP-Interface-Objekts

Id	Attribute	Access Rule	Data type	Description
0x64	Cable Test	Set/Get	STRUCT of: USINT Interface USINT Status	Interface Status (1=Active, 2=Success, 3=Failure, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMin-Length
			USINT CableMax-Length
			USINTCableFailure-Location
				100BASE:{
				{Interface, CablePair1, CableS-tatus, CableMinLength, CableMax-Length, CableFailureLocation}
				{Interface, CablePair2, CableS-tatus, CableMinLength, CableMax-Length, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableS-tatus, CableMinLength, CableMax-Length, CableFailureLocation}
				{Interface, CablePair2, CableS-tatus, CableMinLength, CableMax-Length, CableFailureLocation}
				{Interface, CablePair3, CableS-tatus, CableMinLength, CableMax-Length, CableFailureLocation}
				{Interface, CablePair4, CableS-tatus, CableMinLength, CableMax-Length, CableFailureLocation}
				}

Ethernet-Link-Objekt

Die Informationen in den folgenden Tabellen sind Teil des Ethernet-Link-Objekts. Um auf die Informationen zuzugreifen, verwenden Sie die folgenden Werte:

- Class(####)
- Instance(###)
- Attribute(#)

Legen Sie mindestens eine Instanz für das Gerät fest, zum Beispiel Instanz 1 als Instanz des CPU-Ethernet-Interfaces (Class Code 0xF6) von *EtherNet/IP*.

Tab. 60: Instanz-Attribute

Id	Attribute	Access Rule	Data type	Description
0x1	Interface Speed	Get	UDINT	Used interface speed in MBit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.
0x2	Interface Flags	Get	DWORD	Interface Status Flags: 0: Link State (0=No link, 1=Link) 1: Duplex mode (0=Half, 1=Full) 2: 3: 4: Auto-Negotiation Status 0x0=Auto-Negotiation in progress 0x1=Auto-Negotiation failed 0x2=Failed but speed detected 0x3=Auto-Negotiation success 0x4=No Auto-Negotiation 5: Manual configuration require reset (always 0 because it is not needed) 6: Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface
0x4	Interface Counters	Get	STRUCT of: UDINT MibIICounter1 UDINT MibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EtherneMib Counter1 UDINT EtherneMib Counter2 …	Alignment Errors, FCS Errors, Single Collision, Multiple Collision, SQE Test Errors, Deferred Transmissions, Late Collisions, Excessive Collisions, MAC TX Errors, Carrier Sense Errors, Frame Too Long, MAC RX Errors

Tab. 60: Instanz-Attribute (Forts.)

Id	Attribute	Access Rule	Data type	Description
0x6	Interface Control	Get/Set	STRUCT of:	Control Bits:
			WORD ControlBits	0: Auto-negotiation enable/disable (0=disable, 1=enable)
				1: Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInter-face Speed	Interface speed in MBits/s: 10,100,…, if Auto-negotiation disabled
0x7	Interface type	Get	USINT	Type of interface: 0: Unknown interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber
0x8	Interface state	Get	USINT	Current state of the interface: 0: Unknown interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing
0x9	Admin State	Set/Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface
0xA	Interface label	Get	SHORT-STRING	Human readable ID

Tab. 61: Hirschmann-Erweiterungen des Ethernet-Link-Objekts

Id	Attribute	Access Rule	Data type	Description
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: Link state (0=link down, 1=link up)
				1: Link admin state (0=disabled, 1=enabled)
				8: Access violation alarm (read-only)
				9: Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpper-Threshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Upper Limit.
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLower-Threshold can be accessed. Utilization in percentage (Unit 1%=100). RX Inter-face Utilization Lower Limit.

Tab. 61: Hirschmann-Erweiterungen des Ethernet-Link-Objekts (Forts.)

Id	Attribute	Access Rule	Data type	Description
0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/second
0x6A	Ethernet Interface Description	Get/Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.
0x6B	Port Monitor	Get/Set	DWORD	0: Link Flap (0=Off, 1=On)
				1: CRC/Fragment (0=Off, 1=On)
				2: Duplex Mismatch (0=Off, 1=On)
				3: Overload-Detection (0=Off, 1=On)
				4: Link-Speed/ Duplex Mode (0=Off, 1=On)
				5: Deactivate port action (0=Off, 1=On)
				6: Send trap action (0=Off, 1=On)
				7: Active Condition (displays which condition caused an action to occur) 8: 9: 10: 11: 00001_B: Link Flap 00010_B: CRC/Fragments 00100_B: Duplex Mismatch 01000_B: Overload-Detection 10000_B: Link-Speed/ Duplex mode
				12: Reserved (always 0)
				13: Reserved (always 0)
				14: Reserved (always 0)
				15: Reserved (always 0)
0x6C	Quick Connect	Get/Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, then the device sets the port speed to 100FD, disables Auto-Negotiation, and Spanning Tree on the interface.

Tab. 61: Hirschmann-Erweiterungen des Ethernet-Link-Objekts (Forts.)

Id	Attribute	Access Rule	Data type	Description
0x6D	SFP Diagnostics	Get	STRUCT of:	
			STRING Module-Type	
			SHORT-STRING SerialNumber	
			USINT Connector	
			USINT Supported	
			DINT Temperature	in °C
			DINT TxPower	in mW
			DINT RxPower	in mW
			DINT RxPower	in dBm
			DINT TxPower	in dBm

Tab. 62: Zuweisung der Ports zu den Ethernet Link Object Instances

Ethernet Port	Ethernet Link Object Instance
CPU	1
Modul 1 / Port 1	2
Modul 1 / Port 2	3
Modul 1 / Port 3	4
Modul 1 / Port 4	5
…	…

Anmerkung: Die Anzahl der Ports ist von der verwendeten Hardware abhängig. Das Ethernet-Link-Objekt existiert ausschließlich dann, wenn das Modul eingesteckt und der Port angeschlossen ist.

Switch-Agent-Objekt

Das Gerät unterstützt das Hirschmann-spezifische Ethernet-Switch-Agent-Objekt (Class Code 0x95) für die Gerätekonfigurations- und Informationsparameter mit Instanz 1.

Tab. 63: Class-Attribute

Id	Attribute	Access Rule	Data type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=failed)
				1:	Device Security Status (0=ok, 1=failed)
				2:	Power Supply 1 (0=ok, 1=failed)
				3:	Power Supply 2 (0=ok, 1=failed or not existing)
				4:	Reserved
				5:	Reserved
				6:	Signal Contact 1 (0=closed, 1=open)
				7:	Signal Contact 2 (0=closed, 1=open or not existing)
				8:	Reserved
				9:	Temperature (0=ok, 1=failure)
				10:	Module removed (1=removed)
				11:	ACA21/ACA22 removed (1=removed)
				12:	ACA31 removed (1=removed)
				13:	Reserved
				14:	Reserved
				15:	Reserved
				16:	Reserved
				17:	Reserved
				18:	Reserved
				19:	Reserved
				20:	Reserved
				21:	Reserved
				22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29:	Reserved
				30:	Reserved
				31:	Connection Error (1=failure)

Tab. 63: Class-Attribute (Forts.)

Id	Attribute	Access Rule	Data type	Description
0x2	Switch Temperature	Get	STRUCT of:	
			INT TemperatureF	in °F
			INT TemperatureC	in °C
0x3	Reserved	Get	UDINT	Reserved for future use (always 0)
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0: IGMP Snooping (0=disabled, 1=enabled)
				1: IGMP Querier (0=disabled, 1=enabled)
				2: IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier)
				3:
				4: IGMP Querier Packet Version 5: Off=0 IGMP Querier disabled 6: V1=1 7: V2=2 V3=3
				8: Treatment of Unknown Multicasts: 9: 0=Send To All Ports 10: 1=Send To Query Ports 2=Discard
0x6	Switch Existing Ports	Get	ARRAY of:	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)
			DWORD	
0x7	Switch Port Control	Get/Set	ARRAY of:	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)
			DWORD	
0x8	Switch Ports Mapping	Get	ARRAY of:	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist
			USINT	

Tab. 63: Class-Attribute (Forts.)

Id	Attribute	Access Rule	Data type	Description
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.)
				0: Flash Save Configuration In Progress/Flash Write In Progress
				1: Flash Save Configuration Failed/Flash Write Failed
				4: Configuration changed (configuration not in sync. between running configuration

Das Hirschmann-spezifische Ethernet-Switch-Agent-Objekt bietet Ihnen den zusätzlichen herstellerspezifischen Dienst mit dem Service Code 0x35 zum Speichern der Switch-Konfiguration. Wenn Sie über Ihren PC eine Anfrage zum Speichern einer Gerätekonfiguration senden, sendet das Gerät nach dem Speichern der Konfiguration im Flash-Speicher eine Antwort.

Basis-Switch-Objekt

Das Basis-Switch-Objekt stellt die Schnittstelle auf CIP-Anwendungsebene zu grundlegenden Statusinformationen für einen Managed Ethernet Switch (Revision 1) bereit.

Ausschließlich Instanz 1 des Basis-Switch Class Code 0x51 ist verfügbar.

Tab. 64: Instanz-Attribute

Id	Attribute	Access Rule	Data type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of:	Port Mask
			DWORD	
0x7	Global Port Admin State	Get	ARRAY of:	Port Admin Status
			DWORD	
0x8	Global Port link Status	Get	ARRAY of:	Port Link Status
			DWORD	
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure

Tab. 64: Instanz-Attribute (Forts.)

Id	Attribute	Access Rule	Data type	Description
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default=300) 0=Learning off
0xC	Temperature C	Get	DINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	DINT	Switch temperature in degrees Fahrenheit

Dienste, Verbindungen, I/O-Daten

Das Gerät unterstützt die folgenden Verbindungstypen und Parameter.

Tab. 65: Einstellungen für die Integration eines neuen Moduls

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

Tab. 66: I/O-Datenstruktur des Geräts

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm[2]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Access Violation Alarm[3]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT

Tab. 66: I/O-Datenstruktur des Geräts (Forts.)

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connec enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

1. Die voreingestellte Größe der Port-Bitmasken beträgt 32 Bit (DWORD). Für Geräte mit mehr als 28 Ports wurden die Port-Bitmasken auf n * DWORD erweitert.
2. Die Alarm-Einstellungen für die Netzlast legen Sie fest im Dialog *Grundeinstellungen > Port*, Registerkarte *Netzlast*. Der obere Grenzwert ist der Wert, bei dem die Alarmbedingung aktiv wird. Der untere Grenzwert ist der Wert, bei dem die Alarmbedingung inaktiv wird.
3. Die Alarm-Einstellungen für die Zugriffsverletzungen legen Sie fest im Dialog *Netzsicherheit > Port-Sicherheit*. Der obere Grenzwert ist der Wert, bei dem die Alarmbedingung aktiv wird. Der untere Grenzwert ist der Wert, bei dem die Alarmbedingung inaktiv wird.

Tab. 67: Zuordnung der Datentypen zu Bit-Größen

Objekt-Typ	Bit-Größe
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

15.4 PROFINET

PROFINET ist ein weltweit eingesetztes industrielles Kommunikationsprotokoll. Es basiert auf den Protokollen *TCP/IP* und *UDP/IP* über Ethernet. Dies ist ein wichtiger Aspekt, um die Anforderungen an Konsistenz von der Management-Ebene bis hinunter in die Feldebene zu erfüllen.

PROFINET ergänzt die vorhandene Profibus-Technologie für Anwendungen, die eine schnelle Datenkommunikation und die Nutzung industrieller IT-Funktionen erfordern.

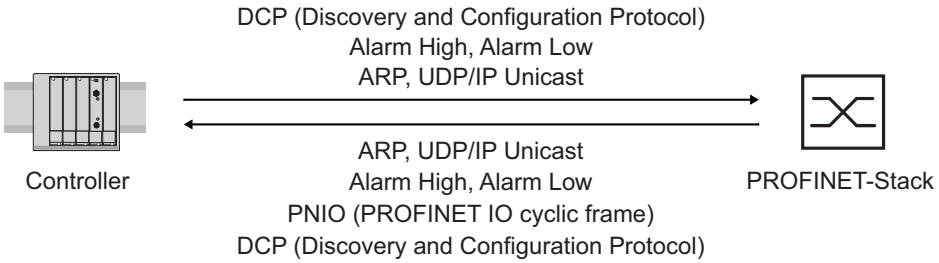


Abb. 85: Kommunikation zwischen Controller und dem Gerät

PROFINET treffen Sie insbesondere in Europa und bei Siemens-Steuerungen an.

PROFINET benutzt die Gerätebeschreibungssprache GSDML (Generic Station Description Markup Language, basierend auf XML), um Geräte und deren Eigenschaften maschinell verarbeitbar zu beschreiben. Die Gerätebeschreibung finden Sie in der GSD (Generic Station Description-) Datei des Geräts.

Weitere Informationen zu PROFINET finden Sie auf der Webseite der PROFIBUS-Organisation unter www.profibus.com.

Die Geräte sind konform zur Klasse B für *PROFINET*.

15.4.1 Gerätemodelle für PROFINET-GSDML-Version 2.3

Das Gerät erzeugt GSDML-Dateien im Format GSDML V.2.3. In der GSDML-Datei ist das Gerät gemäß GSDML-Norm V.2.2 modelliert.

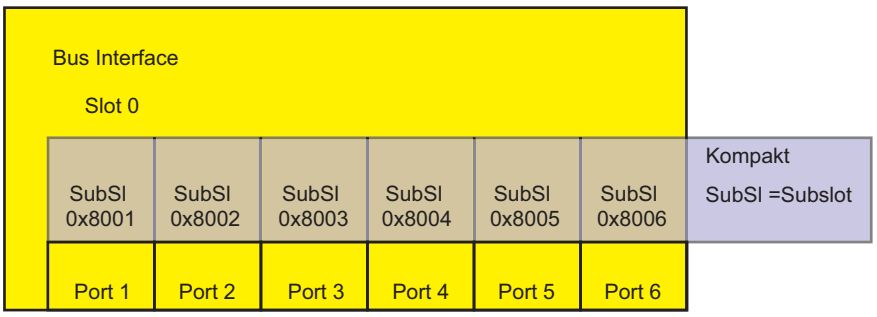


Abb. 86: Kompaktes Gerät

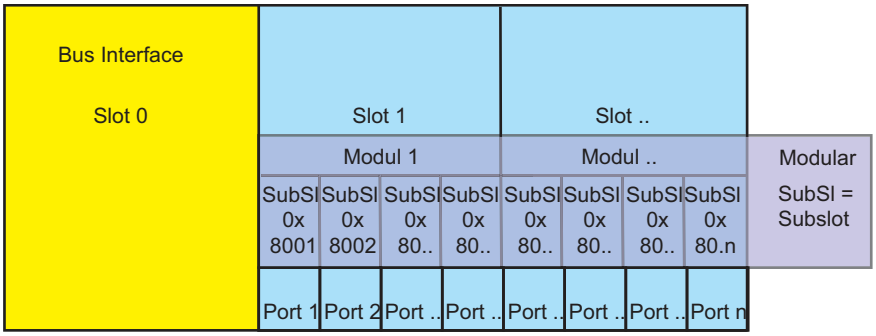


Abb. 87: Modulares Gerät

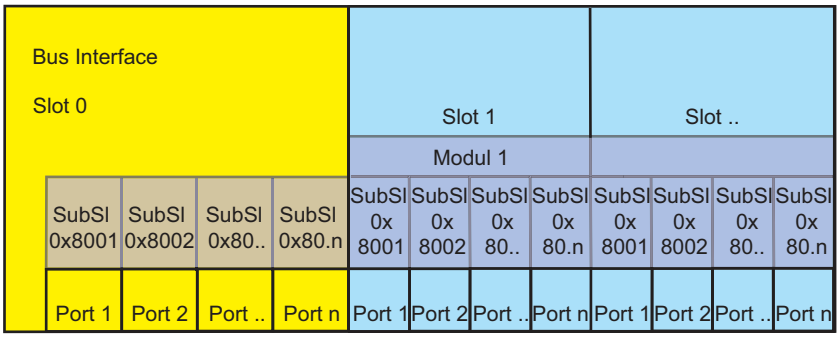


Abb. 88: Kombigerät

15.4.2 Grafische Benutzeroberfläche und Command Line Interface

Wenn Sie das Gerät erfolgreich in einer *PROFINET*-Umgebung eingerichtet haben, stellt die PROFINET-IO-Steuerung eine Applikationsrelation (AR) zu dem Gerät her.

Nachdem der Benutzer sich mittels des Command Line Interface eingeloggt hat, zeigt das Gerät eine Meldung, dass eine Applikationsrelation aktiv ist. Im Dialog *PROFINET* zeigt die grafische Benutzeroberfläche entsprechende Informationen, z.B. die Anzahl der laufenden Applikationsrelationen (AR).

Wenn das Gerät in einem MRP-Ring als *Ring-Manager* arbeitet, dann stellt es die AR nach dem Neustart des Geräts nicht automatisch her. Sie können die AR in diesem Fall durch Ausschalten des MRP-Ringports im Gerät einrichten. Dadurch stellt das Gerät die AR her, der MRP-Ring schließt sich von selbst.

Wenn die AR bereits hergestellt ist, dann lassen Sie die MRP-Ports eingeschaltet, solange diese Ports *PROFINET*-Pakete vermitteln.

15.4.3 Gerät in ein Steuerungssystem integrieren

Gerät vorbereiten

Zuerst installieren Sie das Gerät, schließen es an und konfigurieren es. Dann integrieren Sie das Gerät in ein Steuerungssystem. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.
- ☐ Vergewissern Sie sich, dass im Feld *Systemname* ein gültiger Name für das Gerät festgelegt ist.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netz > IPv4*.
- ☐ Wählen Sie im Rahmen *Management-Schnittstelle* das Optionsfeld `Lokal`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarten *Global* und *Port*.
- ☐ Konfigurieren Sie die Alarmeinstellung für die Alarme, die Sie überwachen wollen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > PROFINET*.
- ☐ Laden Sie die GSD(ML)-Datei zusammen mit dem Symbol auf Ihren lokalen Rechner herunter.
- ☐ Um die Funktion *PROFINET* einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Voreingestellte Werte ändern

Funktionen mit direktem Einfluss auf die Funktion *PROFINET* erfordern das Ändern folgender voreingestellter Werte. Wenn Sie das Gerät in einer speziell erhältlichen *PROFINET*-Variante erworben haben, dann sind diese Werte bereits voreingestellt:

PROFINET	Dialog *Erweitert > Industrie-Protokolle > PROFINET* • *Funktion* = `An` • *Stationsname* = "" (leerer String)

Netz	Dialog *Grundeinstellungen > Netz > Global* • *HiDiscovery Protokoll v1/v2Zugriff* = `readOnly` Dialog *Grundeinstellungen > Netz > IPv4* • *Zuweisung IP-Adresse* = `Lokal` • *IP-Adresse* = `0.0.0.0` • *Netzmaske* = `0.0.0.0` • *Gateway-Adresse* = `0.0.0.0`
VLAN	Dialog *Switching > Global* • *VLAN-Unaware-Modus*=`markiert`
LLDP	Dialog *Diagnose > LLDP > Konfiguration* • *Sende-Intervall [s]* = `5` • *Sende-Verzögerung [s]* = `1`

SPS konfigurieren

Die folgende Ausführung bezieht sich auf die Konfiguration der SPS am Beispiel der Software Simatic S7 von Siemens und setzt voraus, dass Sie mit der Bedienung der Software vertraut sind.

Das Gerät unterstützt auch Engineering-Stationen anderer Hersteller, wie PC Worx von Phoenix Contact

In der Voreinstellung der SPS erkennt die SPS die Unterbrechung der I/O-Verbindung zum Gerät als Fehler. Die SPS betrachtet 3 Echtzeitpakete, die nacheinander in der SPS oder im Gerät fehlen, als Unterbrechung. Dies führt laut Voreinstellung zum Anlagenausfall. Um diese Voreinstellung zu ändern, führen Sie Step7-Programmierungsmaßnahmen durch.

Anmerkung: Die Überwachung der I/O-Verbindung zur CPU des Geräts kann bei einem erkannten Fehler zum potenziellen Systemausfall führen. Berücksichtigen Sie bei der Überwachung deshalb nicht die I/O-Verbindung zur CPU.

Der Datenverkehr für das Gerätemanagement kann die I/O-Verbindung zwischen der SPS und dem Gerät unterbrechen. Beispielsweise kann eine Netzmanagementstation die CPU des Geräts mit Echtzeitdaten höherer Priorität auslasten. In diesem Fall bleibt das System betriebsbereit, weil das Gerät weiterhin Datenpakete senden oder empfangen kann.

GSDML-Datei bereitstellen

Zum Erzeugen von GDSML-Dateien und der Symbole bietet Ihnen das Hirschmann-Gerät folgende Möglichkeit:

▶ Sie können die grafische Benutzeroberfläche im Dialog *Erweitert > Industrie-Protokolle >* PROFINET verwenden, um die GSDML-Datei und das Symbol des Geräts herunterzuladen.

15.4.4 Gerät in die Konfiguration einbinden

Gerät einbinden

Führen Sie die folgenden Schritte aus:

☐ Öffnen Sie die Anwendung *Simatic Manager* über Simatic S7.

☐ Öffnen Sie Ihr Projekt.

- Wechseln Sie in die Hardware-Konfiguration.
- Installieren Sie die GSD(ML)-Datei:
  Klicken Sie im Menü die Einträge *Options > Install GSD File*.
  Wählen Sie die zuvor auf Ihrem PC gespeicherte GSD-Datei.
  Simatic S7 installiert die Datei zusammen mit dem Symbol.
  Sie finden das neue Gerät unter:
  PROFINET IO > Additional Field Devices > Switching Devices > Hirschmann..
  oder unter
  PROFINET IO > Additional Field Devices > Network Components > Hirschmann..
- Ziehen Sie das Gerät per Drag-and-Drop auf das Buskabel.

Gerät umbenennen

Führen Sie die folgenden Schritte aus:
- Markieren Sie das Gerät.
- Klicken Sie im Menü die Einträge *PLC > Ethernet > Edit Ethernet Node*.
- Fügen Sie im Dialog *Edit Ethernet Node*, Rahmen *Assign device name* den Namen des Geräts in Feld *Device name* ein.
- Klicken Sie die Schaltfläche *Browse…*.
  Wählen Sie das Gerät.
  Klicken Sie die Schaltfläche *OK*.
- Legen Sie den Namen des Geräts fest.
  Klicken Sie die Schaltfläche *Assign Name*.
- Klicken Sie die Schaltfläche *Close*.
- Rechtsklicken Sie in der Hardware-Konfiguration das Gerät und wählen Sie in der Dropdown-Liste den Eintrag *Object properties*.
- Fügen Sie denselben Namen ein, der im Dialog *Edit Ethernet Node* festgelegt ist.
- Klicken Sie die Schaltfläche *Ethernet*.
  Fügen Sie die IP-Parameter ein.
  Um das Fenster *Properties - Ethernet interface...* zu schließen, klicken Sie die Schaltfläche *OK*.
- Um das Fenster *Properties* zu schließen, klicken Sie die Schaltfläche *OK*.

Das Gerät wurde in die Konfiguration aufgenommen.

IO-Zyklus konfigurieren

Führen Sie die folgenden Schritte aus:
- Klicken Sie das Gerät in der Hardware-Konfiguration.
- Rechtsklicken Sie im Dialog *Slot/Module View* die Zeile X1 / /PN-IO.
- Wählen Sie in der Dropdown-Liste den Eintrag *Object properties*.
- Öffnen Sie im Fenster *Properties* die Registerkarte *IO Cycle*.
- Wählen Sie im Rahmen *Update Time*, Feld *Update time[ms]*, die erforderliche Aktualisierungszeit in ms für den IO-Zyklus aus.
- Wählen Sie im Rahmen *Watchdog Time*, Feld *Number of accepted update cycles with missing IO data*, die erforderliche Anzahl für den I/O-Zyklus aus.
- Um das Fenster *Properties* zu schließen, klicken Sie die Schaltfläche *OK*.

Medienredundanz konfigurieren

Führen Sie die folgenden Schritte aus:
- Linksklicken Sie das Gerät in der Hardware-Konfigurationen.
- Rechtsklicken Sie im Dialog *Slot/Module View* die Zeile X1 / /PN-IO.
- Wählen Sie in der Dropdown-Liste den Eintrag *Object properties*.

- ☐ Öffnen Sie im Fenster *Properties* die Registerkarte *Media Redundancy*.
- ☐ Wählen Sie im Rahmen *MRP Configuration*, Feld *Domain*, die erforderliche MRP-Domäne für den Knoten.
- ☐ Wählen Sie im Rahmen *MRP Configuration* im Feld *Role* die erforderliche Rolle des Knotens im Ring.
- ☐ Wählen Sie in den Feldern *Ring Port 1* und *Ring Port 2* die aktiven MRP-Ring-Ports aus.
- ☐ Um das Fenster *Properties* zu schließen, klicken Sie die Schaltfläche *OK*.

Anmerkung: Wenn bereits eine Applikationsrelation besteht, schalten Sie keinen der MRP-Ring-Ports mittels der I/O-Module (PROFINET) aus.

Module für modulare Geräte hinzufügen

Führen Sie den folgenden Schritt aus:

- ☐ Ziehen Sie per Drag-and-Drop ein Modul aus der Bibliothek zu einem Steckplatz (Slot). Simatic S7 fügt die Ports über die Moduleigenschaften hinzu.

Geräteeigenschaft konfigurieren

Führen Sie die folgenden Schritte aus:

- ☐ In Steckplatz 0 fügen Sie die Einstellungen für das gesamte Gerät ein.
- ☐ Wählen Sie das Gerät.
- ☐ Rechtsklicken Sie Steckplatz 0.
  Um das gesamte Gerät zu konfigurieren, wählen Sie *Object properties*.
- ☐ Öffnen Sie im Fenster *Properties* die Registerkarte *Parameters*.

Port-Eigenschaften konfigurieren

Bei den modularen Geräten stellen die Steckplätze 1 bis n die Module dar. Die Ports werden als Untersteckplätze/Untermodule dargestellt.

Bei den nichtmodularen Geräten stellen die Untersteckplätze 1 bis n in Steckplatz 0 die Ports dar.

Konfigurieren Sie die Port-Alarme. Führen Sie dazu die folgenden Schritte aus:

- ☐ Rechtsklicken Sie einen Port, 1 bis n, und wählen Sie *Object properties*.
- ☐ Öffnen Sie im Fenster *Properties* die Registerkarte *Parameters*.
- ☐ Wählen Sie die gewünschten Alarme und schließen Sie das Fenster.

Sonderfall: *LinkDown*-Alarm:

Der *LinkDown*-Alarm setzt sich zusammen aus der UND-Verknüpfung

- des Hirschmann-spezifischen Status für Verbindungsfehler und
- der Simatic S7-spezifischen Option für die Verbindung.

Aktivieren Sie den *LinkDown*-Alarms. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie im Dialog *Properties* die Registerkarte *Parameters* (Hirschmann-spezifisch).
- ☐ Um den Parameter *Alarms* einzuschalten, wählen Sie in Spalte *Value* den Wert `On`.
- ☐ Schalten Sie den Parameter *Link state monitoring* ein und wählen Sie in Spalte *Value* die Option `Generate diagnosis alarm when link goes down`.
- ☐ Öffnen Sie die Registerkarte *Options*.
- ☐ Um die Link-Überwachung zu aktivieren, wählen Sie eine feste Einstellung für den Port im Rahmen *Connection*, Feld *Transmission medium/duplex*.

Verbindungs-Optionen konfigurieren

Führen Sie die folgenden Schritte aus:
- ☐ Rechtsklicken Sie einen Port, 1 bis n, und wählen Sie *Object properties*.
- ☐ Öffnen Sie im Dialog *Properties* die Registerkarte *Options*.
- ☐ Wählen Sie im Rahmen *Connection*, Feld *Transmission medium/duplex*, die gewünschte Einstellung für den Port.
- ☐ Um das Fenster *Properties* zu schließen, klicken Sie die Schaltfläche *OK*.

Wenn Sie die Port-Einstellung in einen anderen Wert als `Automatic settings` ändern, schaltet das Gerät den Port über einen kurzen Zeitraum aus. Wenn Sie den Port auf einem Pfad zwischen dem I/O-Controller und dem I/O-Gerät platziert haben, kann die Unterbrechung möglicherweise zu einem Fehler bei der Herstellung einer Applikationsrelation führen. Treffen Sie die folgenden Vorkehrungen, bevor Sie die Port-Einstellung ändern:

Anmerkung: Bevor Sie *RSTP* auf bestimmten Ports ausschalten, stellen Sie sicher, dass dies nicht zu Loops führt.

Deaktivieren Sie *RSTP* an den Geräteports zwischen dem I/O-Controller und dem I/O-Gerät.

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *STP aktiv* für die betreffenden Ports.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Planen Sie die Topologie. Führen Sie dazu die folgenden Schritte aus:
- ☐ Rechtsklicken Sie einen Port, 1 bis n, und wählen Sie *Object properties*.
- ☐ Öffnen Sie im Dialog *Properties* die Registerkarte *Topology*.
- ☐ Wählen Sie im Rahmen *Partners*, Feld *Partner port*, die gewünschte Einstellung für den Partner-Port.
- ☐ Um das Fenster *Properties* zu schließen, klicken Sie die Schaltfläche *OK*.

Tauschen von Geräten

Hirschmann-Geräte unterstützen die Funktion des Gerätetauschs mit einer Engineering-Station.

Beim Tauschen gleicher Geräte weist die Engineering-Station dem neuen Gerät die Parameter des ursprünglichen Geräts zu.

Die Funktion des Gerätetausches mit Simatic S7 erfordert folgende Voraussetzungen:
- ▶ S7 300 mit SW Stand ab V2.7 (gegenwärtig für CPU 319 verfügbar) oder S7 400 mit SW Stand ab V5.2
- ▶ Hirschmann-Gerät mit SW Release ab 05.0.00
- ▶ Die Nachbargeräte unterstützen LLDP
- ▶ Topologie (=Nachbarschaftsbeziehungen) ist konfiguriert und auf SPS geladen

Voraussetzungen für das Ersatzgerät:
- Das Ersatzgerät ist genau vom gleichen Typ wie das ursprüngliche Gerät.
- Das Ersatzgerät ist genau an der gleichen Stelle im Netz (gleiche Ports und Nachbargeräte) angeschlossen.
- Das Ersatzgerät verfügt über eine *PROFINET*-Standardkonfiguration:
  - Systemname = "" (leerer String)
  - IP-Adresse = 0.0.0.0
    Netzmaske = 0.0.0.0
    Gateway-Adresse = 0.0.0.0
    oder
    DHCP ist aktiviert
  - *PROFINET* ist aktiviert

Wenn diese Voraussetzungen erfüllt sind, weist die Engineering-Station dem Ersatzgerät automatisch die Parameter des ursprünglichen Geräts (Gerätename, IP-Parameter und Konfigurationsdaten) zu.

Führen Sie die folgenden Schritte aus:
- ☐ Notieren Sie sich die Port-Belegungen des ursprünglichen Geräts. Entfernen Sie das ursprüngliche Gerät aus dem System.
  Daraufhin erkennt die SPS einen Fehler.
- ☐ Setzen Sie das Ersatzgerät an der gleichen Stelle im Netz ein. Wenn Sie die Ports wieder verbinden, vergewissern Sie sich, dass die Port-Belegungen denen des ursprünglichen Geräts entsprechen.
  Die SPS findet das Ersatzgerät und konfiguriert es in der gleichen Weise wie das ursprüngliche Gerät.
  Die SPS erkennt danach den ordnungsgemäßen Betrieb.
- ☐ Setzen Sie gegebenenfalls die SPS wieder auf `Run`.

Module tauschen

Der *PROFINET*-Stack im Gerät erkennt eine Änderung der angeschlossenen Module und meldet die Änderung an die Engineering-Station. Wenn ein zuvor konfiguriertes Modul aus dem Gerät entfernt wird, meldet die Engineering-Station einen Fehler. Wenn ein konfiguriertes Modul, das gefehlt hat, angeschlossen wird, beseitigt die Engineering-Station die Fehlermeldung.

Topologie-Erkennung

Nachdem Sie die Topologie-Erkennung gestartet haben, sucht die Engineering-Station nach angeschlossenen Geräten.

Projektierung der Topologie

Simatic S7 bietet Ihnen die Möglichkeit, die Topologie zu konfigurieren und entsprechend zu überwachen. Simatic S7 stellt Verbindungsparameter (Qualität und Einstellungen) in einer farbigen Grafik dar.

Kommunikationsdiagnose

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

Portstatistiken ausgeben

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

15.4.5 PROFINET-Parameter

Alarme

Das Gerät unterstützt Alarme auf Geräte- und Port-Ebene.

Tab. 68: Unterstützte Alarme

Alarme auf Geräte-ebene	Änderung des Gerätestatus
	Ausfall des redundanten Netzteils
	Ausfall/Entfernen des ACA
Alarme auf Port-Ebene	Änderung des Link-Status
	Überschreiten der festgelegten Übertragungsrate

Record-Parameter

Das Gerät bietet Datensätze für:
- Geräte-Parameter
- Gerätestatus
- Port-Status/Port-Parameter

Tab. 69: Geräte-Parameter

Byte	Content	Access	Value	Meaning
0	Send alarm if status changes	rw	0	Do not send an alarm.
			1	Send an alarm if the status of device changes.
1	Power Alarm	rw	0	Do not send an alarm.
			1	When a power supply fails, send an alarm.
2	ACA Alarm	rw	0	Do not send an alarm.
			1	When the ACA is removed, send an alarm.
3	Module Alarm	rw	0	Do not send an alarm.
			1	When the module connections are changed, send an alarm.

Tab. 70: Gerätestatus

Byte	Content	Access	Value	Meaning
0	Device status	ro	0	Unavailable
			1	OK
			2	Error

Tab. 70: Gerätestatus

Byte	Content	Access	Value	Meaning
1	Power supply unit 1	ro	0	Unavailable
			1	OK
			2	Error
2	Power supply unit 2	ro	0	OK
			1	Unavailable
			2	Error
3	Power supply unit 3	ro	0	Unavailable
			1	OK
			2	Error
4	Power supply unit 4	ro	0	Unavailable
			1	OK
			2	Error
5	Power supply unit 5	ro	0	Unavailable
			1	OK
			2	Error
6	Power supply unit 6	ro	0	Unavailable
			1	OK
			2	Error
7	Power supply unit 7	ro	0	Unavailable
			1	OK
			2	Error
8	Power supply unit 8	ro	0	Unavailable
			1	OK
			2	Error
9	Signal contact 1	ro	0	Unavailable
			1	Closed
			2	Open
10	Signal contact 2	ro	0	Unavailable
			1	Closed
			2	Open
11	Temperature	ro	0	Unavailable
			1	OK
			2	Threshold value for temperature exceeded or not reached.
12	Fan	ro	0	Unavailable
			1	OK
			2	Fan failure
13	Module removal	ro	0	Unavailable
			1	OK
			2	A module has been removed.

Tab. 70: Gerätestatus

Byte	Content	Access	Value	Meaning
14	ACA removed	ro	0	Unavailable
			1	OK
			2	The ACA has been removed.
15	Not used		0	
			1	
			2	
16	Not used		0	
			1	
			2	
17	Connection	ro	0	Unavailable
			1	OK
			2	Connection failure

Tab. 71: Port-Status/Port-Parameter

Byte	Content	Access	Value	Meaning
0	Report port error	rw	0	Do not send an alarm.
			1	When one of the port alarm reasons represented by bytes 4 .. 10 occurs, send an alarm.
1	Report connection error	rw	0	Do not send an alarm.
			1	Send alarm if the connection has failed.
2	Transmission rate too high	rw	0	Do not send an alarm.
			1	When the threshold values for the transmission rate are exceed, send an alarm.
3	Port on	rw	0	Unavailable
			1	Port enabled
			2	Port disabled
4	Link status	ro	0	Unavailable
			1	Connection exists
			2	Connection interrupted
5	Bit rate	ro	0	Unavailable
			1	Unknown
			2	10 MBit/s
			2	100 MBit/s
			2	1000 MBit/s
6	Duplex	ro	0	Unavailable
			1	Half duplex
			2	Full duplex
7	Autonegotiation	ro	0	Unavailable
			1	Disabled
			2	Enabled

I/O Data

Die Bit-Zuordnung für die I/O-Daten entnehmen Sie der folgenden Tabelle.

Tab. 72: Geräte-I/O-Daten

Direction	Byte	Bit	Meaning
	Bit values:	0	OK or unavailable
		1	Reason for report exists
Input	0	General	
		0	Device status
		1	Signal contact 1
		2	Signal contact 2
		3	Temperature
		4	Fan
		5	Module removal
		6	ACA removed
		7	Not used
Input	1	Power supply status	
		0	Power supply unit 1
		1	Power supply unit 2
		2	Power supply unit 3
		3	Power supply unit 4
		4	Power supply unit 5
		5	Power supply unit 6
		6	Power supply unit 7
		7	Power supply unit 8
Input	2	Supply voltage status	
		0	Not used
		1	Not used
		2	Connection error
		3	Not used
		4	Not used
		5	Not used
		6	Not used
		7	Not used
Output			Not defined

Tab. 73: Port-I/O-Daten (Input)

Direction	Byte	Bit	Meaning
	Bit values:	0	No connection
		1	Active connection

Tab. 73: Port-I/O-Daten (Input)

Direction	Byte	Bit	Meaning
Input	0	Connection status for ports 1 to 8	
		0	Port 1
		1	Port 2
		2	Port 3
		3	Port 4
		4	Port 5
		5	Port 6
		6	Port 7
		7	Port 8
Input	1	Connection status for ports 9 to 16	
		0	Port 9
		1	Port 10
		2	Port 11
		3	Port 12
		4	Port 13
		5	Port 14
		6	Port 15
		7	Port 16
Input	n	Connection for port (n x 8) + 1 to port (n x 8) + 8	
		0	Port (n x 8) + 1
		1	Port (n x 8) + 2
		2	Port (n x 8) + 3
		3	Port (n x 8) + 4
		4	Port (n x 8) + 5
		5	Port (n x 8) + 6
		6	Port (n x 8) + 7
		7	Port (n x 8) + 8

Tab. 74: Port-I/O-Daten (Output)

Direction	Byte	Bit	Meaning
	Bit values:	0	Port activated
		1	Port not activated
Output	0	Status "Port activated" for ports 1 to 8	
		0	Port 1 activated
		1	Port 2 activated
		2	Port 3 activated
		3	Port 4 activated
		4	Port 5 activated
		5	Port 6 activated
		6	Port 7 activated
		7	Port 8 activated

Tab. 74: Port-I/O-Daten (Output)

Direction	Byte	Bit	Meaning
Output	1	Status "Port activated" for ports 9 to 16	
		0	Port 9 activated
		1	Port 10 activated
		2	Port 11 activated
		3	Port 12 activated
		4	Port 13 activated
		5	Port 14 activated
		6	Port 15 activated
		7	Port 16 activated
Output	n	Status "Port activated" for port (n x 8) + 1 to port (n x 8) + 8	
		0	Port (n x 8) + 1 activated
		1	Port (n x 8) + 2 activated
		2	Port (n x 8) + 3 activated
		3	Port (n x 8) + 4 activated
		4	Port (n x 8) + 5 activated
		5	Port (n x 8) + 6 activated
		6	Port (n x 8) + 7 activated
		7	Port (n x 8) + 8 activated

15.5 OPC UA-Server

Die *Open Platform Communications United Architecture* (*OPC UA*) ist ein Protokoll für die industrielle Kommunikation und beschreibt eine Vielzahl von *OPC UA* Informationsmodellen. Das Protokoll *OPC UA* ist ein standardisiertes Protokoll für den sicheren und zuverlässigen Datenaustausch im Bereich der industriellen Automatisierung und in anderen Industriezweigen.

Das Protokoll *OPC UA* bietet einen sehr flexiblen und anpassungsfähigen Mechanismus zur Übertragung der Daten zwischen Geräten im Bereich der industriellen Automatisierung, Überwachungseinrichtungen und Sensoren. Das Protokoll *OPC UA* verwendet eine standardisierte Schnittstelle, zum Beispiel *HTTPS*, wodurch sich das Protokoll einfach in bestehende Managementsysteme integrieren lässt. Das Gerät, das als *OPC UA*-Server arbeitet, vermittelt die Daten der angeschlossenen Endgeräte, vom einfachen Verfügbarkeitsstatus bis hin zu großen Mengen an komplexen industriellen Daten.

Die folgende Abbildung zeigt die *OPC UA*-Informationsmodell-Daten der angeschlossenen Endgeräte, die dem *OPC UA*-Client zur Verfügung stehen.

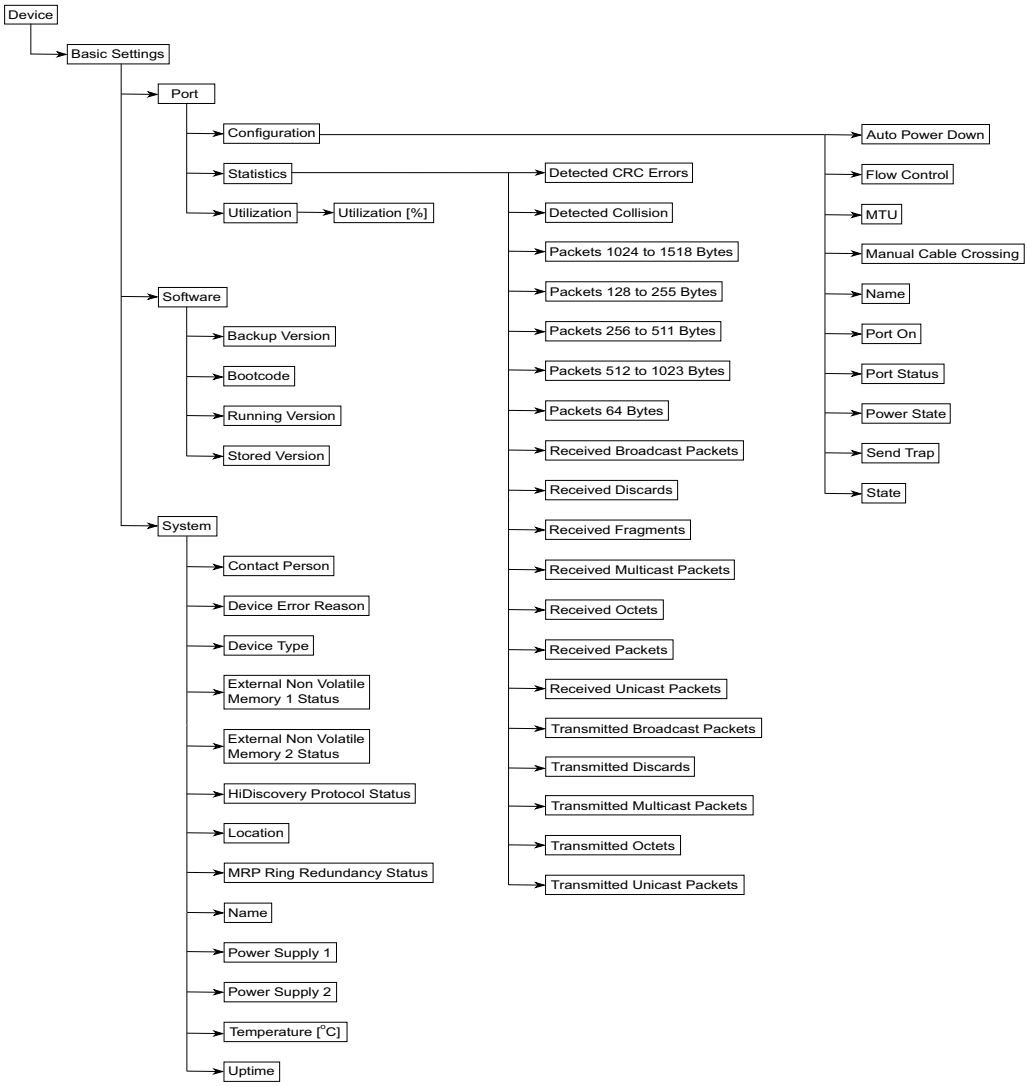


Abb. 89: OPC UA-Informationsmodell

Tab. 75: Objekte im OPC-UA-Informationsmodell

Objekt	Beschreibung
`Automatisches Ausschalten`	Legt fest, wie sich der Port verhält, wenn kein Kabel angeschlossen ist.
`Port an`	Aktiviert/deaktiviert den Port.
`Power-State (Port aus)`	Legt fest, ob der Port physikalisch eingeschaltet oder ausgeschaltet ist, wenn Sie den Port mit der Funktion *Port an* deaktivieren.
`Zustand`	Zeigt, ob der Port gegenwärtig physikalisch eingeschaltet oder ausgeschaltet ist.
`Status Port`	Zeigt den Vermittlungsstatus des Ports.

Tab. 76: Werte der Objekte im OPC-UA-Informationsmodell

Objekt	Wert	Beschreibung
Device Error Reason	1	None
	2	Power supply
	3	Link failure
	4	Temperature
	5	Fan failure
	6	Module removal
	7	External non volatile memory removal
	8	External non volatile memory not in synchronization
	9	Ring redundancy
External Non Volatile Memory 1 Status	1	Not present
	2	Removed
	3	Ok
	4	Out of memory
	5	Generic error
External Non Volatile Memory 2 Status	1	Not present
	2	Removed
	3	Ok
	4	Out of memory
	5	Generic error
HiDiscovery Protocol Status	1	Enabled
	2	Disabled
MRP Ring Redundancy Status	1	Available
	2	Not available
Power Supply 1	1	Present
	2	Defective
	3	Not installed
	4	Unknown
Power Supply 2	1	Present
	2	Defective
	3	Not installed
	4	Unknown

Tab. 76: Werte der Objekte im OPC-UA-Informationsmodell

Objekt	Wert	Beschreibung
Auto Power Down	1	Auto power down
	2	No power save
	3	Energy efficient ethernet
	4	Unsupported
Flow Control	1	Enabled
	2	Disabled
Manual Cable Crossing	1	Medium dependent interface
	2	Medium dependent interface crossover
	3	Auto medium dependent interface crossover
	4	Unsupported
Port On	1	Up
	2	Down
	3	Testing
Power State	1	Enabled
	2	Disabled
Send Trap	1	Enabled
	2	Disabled
State	1	Up
	2	Down
Port Status	1	Up
	2	Down
	3	Testing
	4	Unknown
	5	Dormant
	6	Not present
	7	Lower layer down

Das Gerät, das als *OPC UA*-Server arbeitet, verarbeitet die Daten des *OPC UA*-Informationsmodells und überträgt sie auf sicherem Wege an die *OPC UA*-Client-Anwendung. Der *OPC UA*-Server und der *OPC UA*-Client kommunizieren in einer Sitzung miteinander.

Das Gerät, das als *OPC UA*-Server arbeitet, verteilt die überwachten Daten des *OPC UA*-Informationsmodells. Der Benutzer des *OPC UA*-Clients wählt aus einer Liste der IEC-Variablen diejenigen Elemente aus, welche die *OPC UA*-Client-Anwendung überwachen soll. Die *OPC UA*-Client-Anwendung fordert die Daten des *OPC UA*-Informationsmodells beim als *OPC UA*-Server arbeitenden Gerät an und verwendet die Daten des festgelegten *OPC UA*-Benutzerkontos.

Das Gerät richtet eine *OPC UA*-Sitzung ein, indem es zunächst die Richtlinie für eine sichere Verbindung aushandelt. Über diese sichere Verbindung sendet der *OPC UA*-Client die Anmeldedaten des *OPC UA*-Benutzerkontos. Danach authentifiziert der *OPC UA*-Server im Gerät den *OPC UA*-Client. Wenn die Anmeldedaten gültig sind, gewährt das Gerät dem *OPC UA*-Client Zugriff auf seine *OPC UA Server*-Funktion.

Das Gerät bietet ein rollenbasiertes Authentifizierungs- und Verschlüsselungskonzept, mit dem es den Zugriff auf seinen *OPC UA*-Server gezielt steuert. Der *OPC UA*-Client kann diejenigen Befehle und Funktionen nutzen, die mit dem im Gerät eingerichteten *OPC UA*-Benutzerkonto verknüpft sind.

15.5.1 OPC UA-Server einschalten

In der Voreinstellung ist die Funktion *OPC UA Server* ausgeschaltet. Im Dialog *Erweitert > Industrie-Protokolle > OPC UA Server* können Sie die Funktion *OPC UA Server* einschalten. Außerdem können Sie die maximale Anzahl gleichzeitiger *OPC UA*-Sitzungen festlegen. In der Voreinstellung sind die Werte für die Felder *Listening-Port* und *Sitzungen (max.)* bereits festgelegt. Das Authentifizierungs- und Verschlüsselungsprotokoll für *OPC UA*-Benutzer legen Sie auf globaler Ebene fest.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > OPC UA Server*.
- ☐ Um die Funktion *OPC UA Server* einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Ändern Sie die TCP-Portnummer im Feld *Listening-Port*, falls erforderlich.
- ☐ Falls erforderlich, ändern Sie im Feld *Sitzungen (max.)* die Anzahl der *OPC UA*-Sitzungen, die gleichzeitig eingerichtet sein können.
- ☐ Wählen Sie im Feld *Security-Policy* das Authentifizierungs- und Verschlüsselungsprotokoll.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
  Der Dialog zeigt das Fenster *Um die Änderungen anzuwenden, starten Sie den OPC/UA-Server neu. Jetzt neu starten?*.
- ☐ Um die Änderungen anzuwenden, klicken Sie die Schaltfläche *Yes*.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`opc-ua operation`	*OPC UA Server*-Server einschalten.
`opc-ua port <1..65535>`	TCP-Portnummer ändern, falls erforderlich.
`opc-ua sessions <1..5>`	Festlegen, wie viele *OPC UA*-Sitzungen gleichzeitig aufgebaut sein können.
`opc-ua security-policy none | basic128rsa15 | basic256 | basic256sha256`	Authentifizierungs- und Verschlüsselungsprotokoll festlegen.
`show opc-ua global`	Die *OPC UA*-Server-Einstellungen anzeigen.

```
IEC62541 - OPC/UA server settings
--------------------------
IEC62541 - OPC/UA server operation..........enabled
Listening port..............................4840
Number of concurrent sessions...............5
Configured security-policy..................none
```

15.5.2 Ein OPC UA-Benutzerkonto einrichten

Der Dialog ermöglicht Ihnen die Verwaltung der *OPC UA*-Benutzerkonten, die erforderlich sind, um mit einer*OPC UA*-Client-Anwendung auf das Gerät zuzugreifen. Jeder *OPC UA*-Client-Benutzer benötigt ein aktives *OPC UA*>-Benutzerkonto, um Zugriff auf den *OPC UA*-Server des Geräts zu erhalten.

Im folgenden Beispiel werden wir ein *OPC UA*-Benutzerkonto für den *OPC UA*-Client-Benutzer `USER` einrichten, der Lesezugriff hat. Anschließend ist der `USER`-Benutzer berechtigt, die Daten des *OPC UA*-Informationsmodells zu überwachen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > OPC UA Server*.
- ☐ Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Fügen Sie in das Feld *Benutzername* die Bezeichnung `USER` ein.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Fügen Sie in das Feld *Passwort* das Passwort mit mindestens 6 Zeichen ein.
  In diesem Beispiel geben wir dem Benutzerkonto das Passwort `SECRET`.
- ☐ Wählen Sie in Spalte *Rolle* den Eintrag *read-only*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
  Der Dialog zeigt das Fenster *Um die Änderungen anzuwenden, starten Sie den OPC/UA-Server neu. Jetzt neu starten?*.
- ☐ Um die Änderungen anzuwenden, klicken Sie die Schaltfläche *Yes*.
  Der Dialog zeigt die eingerichteten *OPC UA*-Benutzerkonten.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`users add USER`	*OPC UA*-Benutzerkonto `USER` erzeugen.

`opc-ua users modify USER password`
`Enter NEW password: ****** (SECRET)`
`Confirm NEW password: ****** (SECRET)`
	Für das *OPC UA*-Benutzerkonto `USER` das Passwort `SECRET` einfügen und bestätigen. Fügen Sie das Passwort mit mindestens 6 Zeichen ein.

`opc-ua users modify USER access-role read-only`	Dem *OPC UA*-Benutzerkonto `USER` die Rolle *`read-only`* zuweisen.
`opc-ua users enable USER`	Benutzerkonto `USER` aktivieren.
`show opc-ua users`	Eingerichtete Benutzerkonten anzeigen.

```
User Name                  Access-Role      Status
-------------------------- ---------------- ------
user                       read-only        [x]
```

Anmerkung: Wenn Sie ein neues *OPC UA*-Benutzerkonto einrichten, denken Sie daran, auch das Passwort festzulegen.

15.5.3 Ein OPC UA-Benutzerkonto deaktivieren

Nach dem Deaktivieren des *OPC UA*-Benutzerkontos kann der Benutzer nicht mehr mit der *OPC UA Server*-Funktion auf das Gerät zugreifen. Das Deaktivieren eines *OPC UA*-Benutzerkontos ermöglicht, die Kontoeinstellungen beizubehalten und in Zukunft wieder zu verwenden. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > OPC UA Server*.
  Der Dialog zeigt die eingerichteten *OPC UA*-Benutzerkonten.
- ☐ Heben Sie in der Zeile des betreffenden *OPC UA*-Benutzerkontos die Markierung des Kontrollkästchens *Aktiv* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
  Der Dialog zeigt das Fenster *Um die Änderungen anzuwenden, starten Sie den OPC/UA-Server neu. Jetzt neu starten?*.
- ☐ Um die Änderungen anzuwenden, klicken Sie die Schaltfläche *Yes*.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`opc-ua users disable USER`	Benutzerkonto `USER` deaktivieren.
`show opc-ua users`	Eingerichtete Benutzerkonten anzeigen.

```
User Name                  Access-Role   Status
-------------------------- ------------- ------
user                       read-only     [ ]
```

`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern.

15.5.4 Ein OPC UA-Benutzerkonto löschen

Um die Einstellungen des *OPC UA*-Benutzerkontos dauerhaft zu deaktivieren, löschen Sie das *OPC UA*-Benutzerkonto. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > OPC UA Server*.
  Der Dialog zeigt die eingerichteten *OPC UA*-Benutzerkonten.
- ☐ Wählen Sie die Tabellenzeile des betreffenden Benutzerkontos *OPC UA*.
- ☐ Klicken Sie die Schaltfläche .
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
  Der Dialog zeigt das Fenster *Um die Änderungen anzuwenden, starten Sie den OPC/UA-Server neu. Jetzt neu starten?*.
- ☐ Um die Änderungen anzuwenden, klicken Sie die Schaltfläche *Yes*.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`opc-ua users delete USER`	Benutzerkonto `USER` löschen.

`show opc-ua users`	Eingerichtete Benutzerkonten anzeigen.
`save`	Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern.

```
User Name                  Access-Role   Status
-------------------------- ------------- ------
```

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 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.

Führen Sie die folgenden Schritte aus:

- ☐ Installieren Sie den DHCP-Server auf Ihrem PC.
  Führen Sie die Installation gemäß des Installationsassistenten durch.
- ☐ Starten Sie das Programm *haneWIN DHCP Server*.

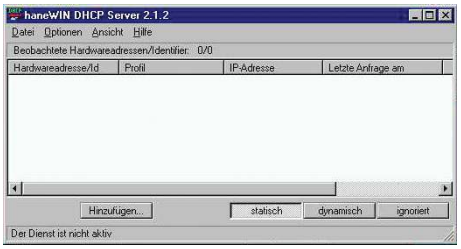


Abb. 90: Startfenster des Programms haneWIN DHCP Server

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.

- ☐ Klicken Sie im Menü die Einträge *Options > Preferences*, um das Fenster für die Programmeinstellungen zu öffnen.
- ☐ Wählen Sie die Registerkarte *DHCP*.
- ☐ Legen Sie die in der Abbildung dargestellten Einstellungen fest.

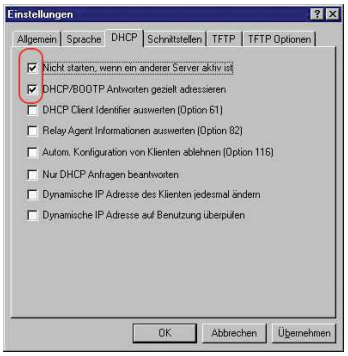


Abb. 91: DHCP-Einstellung

- ☐ Klicken Sie die Schaltfläche *OK*.
- ☐ Zur Eingabe der Konfigurationsprofile klicken Sie im Menü die Einträge *Options > Configuration Profiles*.

- Legen Sie den Namen für das neue Konfigurationsprofil fest.

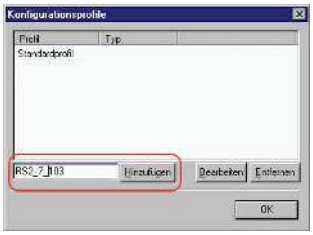


Abb. 92: Konfigurationsprofile hinzufügen

- Klicken Sie die Schaltfläche *Add*.
- Legen Sie die Netzmaske fest.

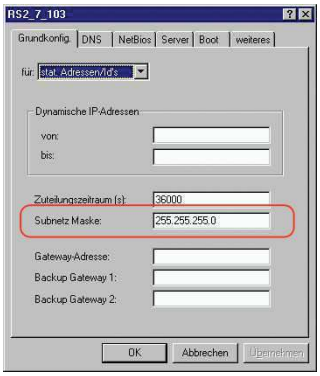


Abb. 93: Netzmaske im Konfigurationsprofil

- Klicken Sie die Schaltfläche *Apply*.
- Wählen Sie die Registerkarte *Boot*.
- Geben Sie die IP-Adresse Ihres tftp-Servers.
- Geben Sie den Pfad und den Dateinamen für die Konfigurationsdatei ein.

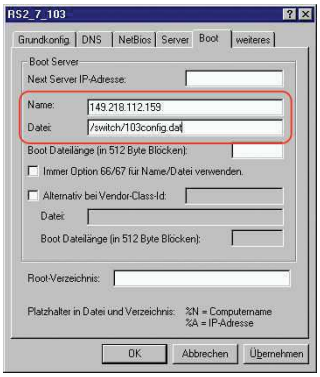


Abb. 94: Konfigurationsdatei auf dem tftp-Server

- Klicken Sie die Schaltfläche *Apply* und dann den Eintrag *OK*.

- Fügen Sie für jeden Gerätetyp ein Profil hinzu.
  Haben Geräte des gleichen Typs unterschiedliche Konfigurationen, dann fügen Sie für jede Konfiguration ein Profil hinzu.

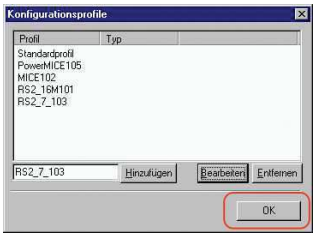


Abb. 95: Konfigurationsprofile verwalten

- Zum Beenden des Hinzufügens der Konfigurationsprofile klicken Sie die Schaltfläche *OK*.
- Zur Eingabe der statischen Adressen klicken Sie im Hauptfenster die Schaltfläche *Static*.

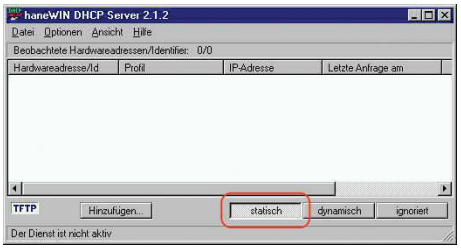


Abb. 96: Statische Adresseingabe

- Klicken Sie die Schaltfläche *Add*.

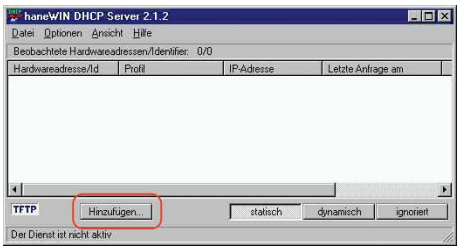


Abb. 97: Statische Adressen hinzufügen

- Geben Sie die MAC-Adresse des Geräts ein.
- Geben Sie die IP-Adresse des Geräts ein.

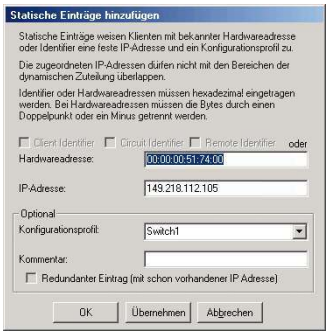


Abb. 98: Einträge für statische Adressen

- Wählen Sie das Konfigurationsprofil des Geräts.

- Klicken Sie die Schaltfläche *Apply* und dann den Eintrag *OK*.
- Fügen Sie für jedes Gerät, das vom DHCP-Server seine Parameter erhalten soll, einen Eintrag hinzu.

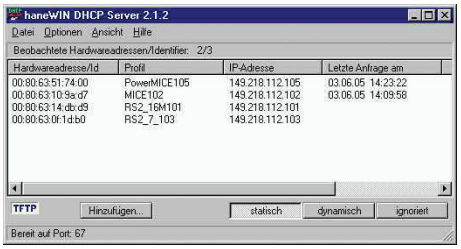


Abb. 99: DHCP-Server mit Einträgen

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 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.

Führen Sie die folgenden Schritte aus:

- ☐ Installieren Sie den DHCP-Server auf Ihrem PC.
  Führen Sie die Installation gemäß des Installationsassistenten durch.
- ☐ Starten Sie das Programm *haneWIN DHCP Server*.

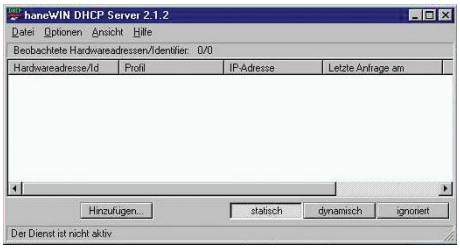


Abb. 100: Startfenster des Programms haneWIN DHCP Server

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.

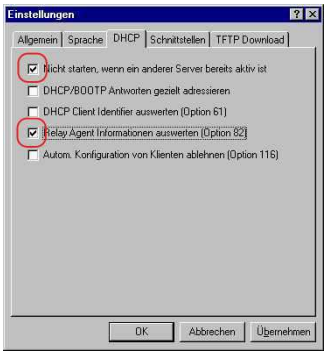


Abb. 101: DHCP-Einstellung

- Zur Eingabe der statischen Adressen klicken Sie die Schaltfläche *Add*.

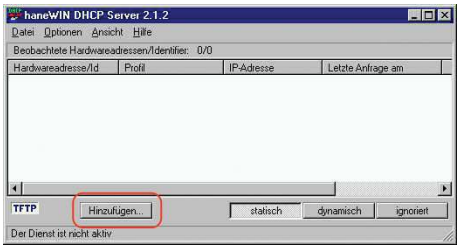


Abb. 102: Statische Adressen hinzufügen

- Markieren Sie das Kontrollkästchen *Circuit Identifier*.
- Markieren Sie das Kontrollkästchen *Remote Identifier*.

Abb. 103: Voreinstellung für die feste Adresszuweisung

- Legen Sie im Feld *Hardware address* 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 *Hardware address* festgelegten Port anschließen, die im Feld *IP address* 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 Geräts (zum Beispiel MAC-Adresse), an dem ein Gerät angeschlossen wird.

Abb. 104: Festlegen der Adressen

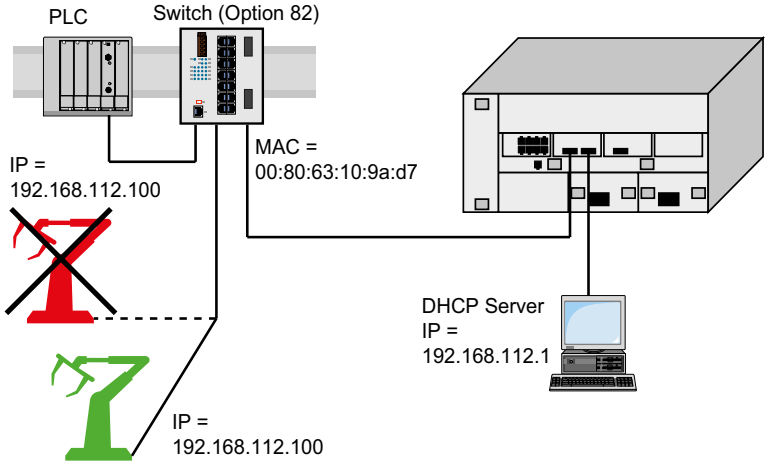


Abb. 105: Anwendungsbeispiel für den Einsatz von Option 82

A.3 SSH-Zugriff vorbereiten

Sie können sich über SSH mit dem Gerät verbinden. Führen Sie dazu die folgenden Schritte aus:

- Erzeugen Sie einen Schlüssel auf dem Gerät.
  oder
- Übertragen Sie Ihren 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 ermöglicht Ihnen, einen Schlüssel direkt auf dem Gerät zu erzeugen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Um den SSH-Server auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `Aus`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Um einen RSA-Schlüssel zu erzeugen, klicken Sie im Rahmen *Signatur* die Schaltfläche *Erzeugen*.
- ☐ Um den SSH-Server einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`ssh key rsa generate`	Einen neuen RSA-Schlüssel erzeugen.

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 rsa -f rsa.key -C '' -N ''
rsaparam -out rsaparam.pem 2048
```

Das Gerät ermöglicht Ihnen, Ihren eigenen Schlüssel auf das Gerät zu übertragen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Um den SSH-Server auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `Aus`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu 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.
- Um den SSH-Server einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Führen Sie die folgenden Schritte aus:
- Kopieren Sie den selbst erzeugten Schlüssel von Ihrem PC in den externen Speicher.
- Kopieren Sie den Schlüssel aus dem externen Speicher in das Gerät.

`enable`	In den Privileged-EXEC-Modus wechseln.
`copy sshkey envm <file name>`	Eigenen Schlüssel aus dem externen Speicher in das Gerät laden.

A.3.3 SSH-Client-Programm vorbereiten

Das Programm *PuTTY* ermöglicht Ihnen, auf das Gerät mit SSH zuzugreifen. Sie können die Software von www.putty.org herunterladen.

Führen Sie die folgenden Schritte aus:
- Starten Sie das Programm mit einem Doppelklick.

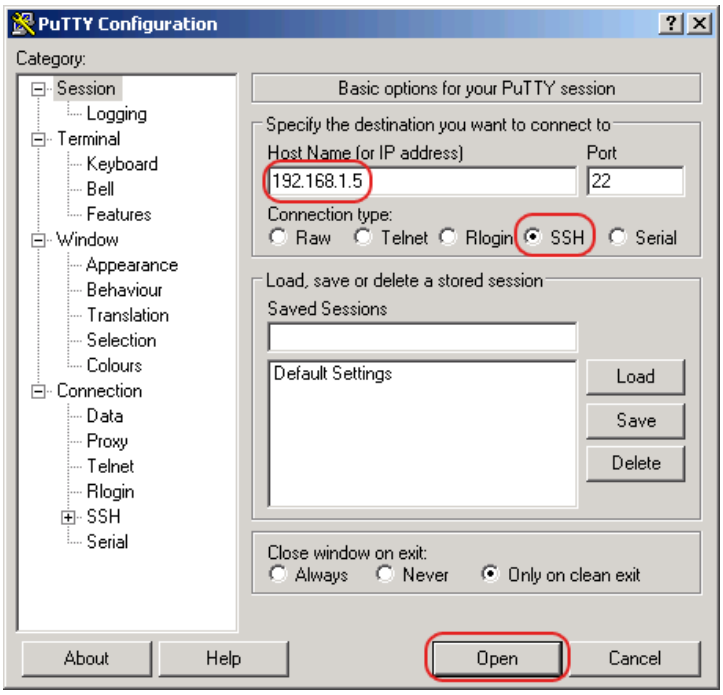


Abb. 106: PuTTY-Eingabemaske

- In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Geräts 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 und ermöglicht Ihnen, den Fingerabdruck des Schlüssels zu prüfen.

Abb. 107: Sicherheitsabfrage für den Fingerabdruck

Gegen Ende des Verbindungsaufbaus zeigt das Programm *PuTTY* eine Sicherheitsalarmmeldung und ermöglicht Ihnen, den Fingerabdruck des Schlüssels zu prüfen.

- Prüfen Sie den Fingerabdruck des Schlüssels, um sich zu vergewissern, dass Sie sich tatsächlich mit dem gewünschten Gerät verbunden haben.
- Stimmt der Fingerabdruck mit dem Ihres Schlüssels überein, dann klicken Sie die Schaltfläche *Yes*.

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 Geräts.

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. Um Validierungskonflikte mit Software von Drittanbietern zu beheben, übertragen Sie Ihr eigenes, aktuelles Zertifikat auf das Gerät oder generieren Sie das Zertifikat mit der neuesten Firmware.

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. Führen Sie dazu die folgenden Schritte aus:

- ☐ 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Starten Sie den HTTPS-Server neu, um den Schlüssel zu aktivieren. Führen Sie den Neustart des Servers über das Command Line Interface durch.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`https certificate generate`	Ein HTTPS-Zertifikat (X509/PEM) erzeugen.
`no https server`	Funktion *HTTPS* ausschalten.
`https server`	Funktion *HTTPS* einschalten.

☐ Das Gerät ermöglicht Ihnen auch, ein extern generiertes X.509/PEM-Zertifikat auf das Gerät zu übertragen:

- ☐ 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	In den Privileged-EXEC-Modus wechseln.
`copy httpscert envm <file name>`	HTTPS-Zertifikat aus dem externen nichtflüchtigen Speicher kopieren.
`configure`	In den Konfigurationsmodus wechseln.
`no https server`	Funktion *HTTPS* ausschalten.
`https server`	Funktion *HTTPS* einschalten.

Anmerkung: Um das Zertifikat nach der Erstellung oder Übertragung zu aktivieren, starten Sie das Gerät neu oder starten Sie den HTTPS-Server neu. Führen Sie den Neustart des HTTPS-Servers über das Command Line Interface durch.

A.4.2 Zugang über HTTPS

Die Voreinstellung für HTTPS-Datenverbindungen ist der TCP-Port `443`. Wenn Sie die HTTPS-Portnummer ändern, starten Sie anschließend das Gerät oder den HTTPS-Server neu. Damit wird die Änderung wirksam. Führen Sie dazu 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 `An`.
- ☐ Um über HTTPS auf das Gerät zuzugreifen, geben Sie in Ihrem Browser HTTPS statt HTTP und die IP-Adresse des Geräts ein.

`enable`	In den Privileged-EXEC-Modus wechseln.
`configure`	In den Konfigurationsmodus wechseln.
`https port 443`	Nummer des TCP-Ports festlegen, auf dem der Webserver HTTPS-Anfragen von den Clients entgegennimmt.
`https server`	Funktion *HTTPS* einschalten.
`show https`	Status des *HTTPS*-Servers und die Portnummer anzeigen.

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. Wenn Sie sich am Ende der Sitzung abmelden, beendet das Gerät die Datenverbindung.

B Anhang

B.1 Literaturhinweise

Eine kleine Auswahl an Büchern zu Netzwerk-Themen, geordnet nach Erscheinungsdatum (neueste zuerst):

- TSN – Time-Sensitive Networking (in Deutsch)
  Wolfgang Schulte
  VDE Verlag, 2020
  ISBN 978-3-8007-5078-8
- Time-Sensitive Networking For Dummies, Belden/Hirschmann Special Edition (in Englisch)
  Oliver Kleineberg und Axel Schneider
  Wiley, 2018
  ISBN 978-1-119-52791-6 (Print), ISBN 978-1-119-52799-2 (eBook)
  Fordern Sie Ihre kostenlose PDF-Kopie an unter https://www.belden.com/resources/knowledge/ebooks/time-sensitive-networking-for-dummies-lp
- IPv6: Grundlagen - Funktionalität - Integration (in Deutsch)
  Silvia Hagen
  Sunny Connection, 3. Auflage, 2016
  ISBN 978-3-9522942-3-9 (Print), ISBN 978-3-9522942-8-4 (eBook)
- IPv6 Essentials (in Englisch)
  Silvia Hagen
  O'Reilly, 3. Auflage, 2014
  ISBN 978-1-449-31921-2 (Print)
- TCP/IP Illustrated, Volume 1: The Protocols (2nd Edition) (in Englisch)
  W. R. Stevens und Kevin R. Fall
  Addison Wesley, 2011
  ISBN 978-0-321-33631-6
- Measurement, Control and Communication Using IEEE 1588 (in Englisch)
  John C. Eidson
  Springer, 2006
  ISBN 978-1-84628-250-8 (Print), ISBN 978-1-84628-251-5 (eBook)
- TCP/IP: Der Klassiker. Protokollanalyse. Aufgaben und Lösungen (in Deutsch)
  W. R. Stevens
  Hüthig-Verlag, 2008
  ISBN 978-3-7785-4036-7
- Optische Übertragungstechnik in der Praxis (in Deutsch)
  Christoph Wrobel
  Hüthig-Verlag, 3. Auflage, 2004
  ISBN 978-3-8266-5040-6

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 unter 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 Syntax-Begriffe:	
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 Hexadezimalzahl 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	Netzteil-Kennung (Nummer des Netzteils)
TimeTicks	Stopp-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 Hexadezimalzahl nach ISO/IEC 8802-3
Zähler	Ganze Zahl (0-2^{32}-1), deren Wert beim Auftreten bestimmter Ereignisse um `1` erhöht wird.

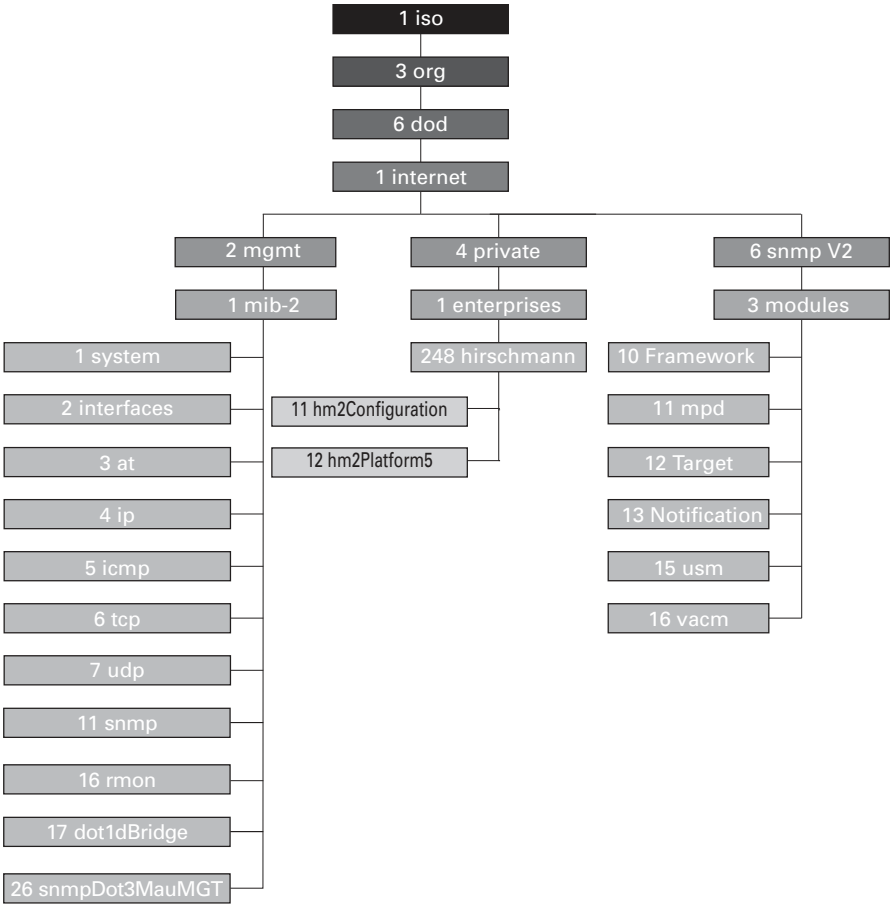


Abb. 108: Baumstruktur der Hirschmann-MIB

Wenn Sie von den Produktseiten im Internet ein Software-Update heruntergeladen haben, enthält das ZIP-Archiv mit der Gerätesoftware auch die MIBs.

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 2474	Definition of the Differentiated Services Field (DS Field) in the IPv4 and IPv6 Headers
RFC 2475	An Architecture for Differentiated Service
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 3621	Power Ethernet MIB
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)
RFC 5321	Simple Mail Transfer Protocol

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

15.5.5 Switching

Größe der MAC-Adress-Tabelle (inkl. statische Filter)	32768
Max. Anzahl statisch konfigurierter MAC-Adressfilter	100
Max. Anzahl der mit IGMP-Snooping lernbaren MAC-Adressfilter	1024
Max. Anzahl der MAC-Adresseinträge (MMRP)	512
Anzahl Warteschlangen	8 Queues
Einstellbare Port-Prioritäten	0..7
MTU (max. erlaubte Länge der Pakete, die ein Port empfangen oder senden kann)	12288 Bytes

15.5.6 VLAN

VLAN-ID-Bereich	1..4042
Anzahl der VLANs	max. 512 gleichzeitig pro Gerät max. 512 gleichzeitig pro Port

15.5.7 Access-Control-Listen (ACL)

Max. Anzahl der ACLs	100
Max. Anzahl der Regeln pro ACL	1023
Max. Anzahl der Regeln pro Port	1023
Anzahl der insgesamt konfigurierbaren Regeln	8184 (8 × 1023)
Max. Anzahl der VLAN-Zuweisungen	24
Max. Anzahl der Regeln, die ein Ereignis protokollieren	128
Max. Anzahl der Ingress-Regeln	1792
Max. Anzahl der Egress-Regeln	512

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	Name des externen Speichers
ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
EUI	Extended Unique Identifier
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
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 Stichwortverzeichnis

0-9
2-Switch-Kopplung, primäres Gerät 243
2-Switch-Kopplung, Standby-Gerät 245
802.1X 59

A
Advanced Mode 181, 184
AF 154
Aging-Time 137
Alarm 263, 374
Alarmeinstellung 368
Alarmnachrichten 261
Alternate-Port 205, 211
APNIC 44
ARIN 44
ARP 46
Assured Forwarding 154
Authentifizierungs-Liste 59
Automatische Konfiguration 108

B
Backup-Port 206, 211
Bandbreite 157
Baumstruktur (Spanning Tree) 201, 204
Benutzernamen 19, 22, 24
Berechtigungen 63
Bericht 294
Best-Master-Clock-Algorithmus 85
BOOTP 43
Boundary-Clock (PTP) 84
BPDU 200
BPDU Guard 210, 211
Bridge Identifier 197
Bridge Protocol Data Unit 200

C
CA-Zertifikat 298
CIDR 46
CIP 350
Class Selector 154
Classless Inter Domain Routing 46
Command Line Interface 18
Common Industrial Protocol 350

D

Datenpaketanforderungsintervall 351
Datensatz 371, 374
Datenverkehr 119
Defektes Gerät ersetzen 15
Delay (PTP) 85
Denial-of-Service 119
Designated Bridge 205
Designated Port 205, 210
Device Description Language (Gerätebeschreibungssprache) 366
DHCP 43
DHCP-L2-Relay 324
DHCP-Server 78, 82, 387, 391
Diameter (Spanning Tree) 199
Differentiated Services 154
DiffServ 143
DiffServ-Codepoint 154
Disabled-Port 206
DoS 119
DSCP 143, 152, 154

E

Echtzeit 143
Edge-Port 205, 210
EDS 350
EF 154
E-Mail Benachrichtigung 289
Engineering-Station 372
Engineering-System 369
Ereignisprotokoll 297
Erstinstallation 43
Erweiterte Informationen zu MRP 182
Erweiterte Informationen zu RCP 255
Erweiterte Informationen zur Ring-/Netz-Kopplung 234
Erweiterte Informationen, HIPER Ring 193
Erweiterte Informationen, MRP 182
EtherNet/IP-Website 350
Expedited Forwarding 154

F

Ferndiagnose 273
Flüchtiger Speicher (RAM) 87
Flusskontrolle 157
Funktionsüberwachung 273

G

GARP 331
Gateway 44, 48
Generic Ethernet Module 351
Generische Objektklassen 401
Gerätestatus 265
Global-Config-Modus 26, 27
GMRP 331
Grafische Benutzeroberfläche starten 17
Grandmaster (PTP) 85
Grenzwert 368
GSD 366, 368, 370
GSD-Datei 370
GSDML 366

H

HaneWin 387, 391
Hardware-Reset 261
Häufig gestellte Fragen 419
HiDiscovery 43
HIPER Ring, Erweiterte Informationen 193
HIPER Ring-Pakete 193
HIPER Ring-Paket-Priorisierung 194
HIPER-Ring 192
HiView 58
Hostadresse 44

I

IANA 44
IAS 59
IEC 61850 340
IEEE 802.1X 59
IEEE-MAC-Adresse 283
IGMP-Snooping 137, 350
Industrial HiVision 13
Instanzierung 401
Integrated authentication server 59
IP-Adresse 44, 48, 53
IP-Header 143, 145, 154
ISO/OSI-Schichtenmodell 46

K

Kommandobaum 29
Konfigurationsänderungen 261
Konfigurationsdatei 53
Konformitätsklasse 366

L

LACNIC 44
Laufzeitmessung (PTP) 85
LDAP 59
Leave-Nachricht 137
Link Aggration 178
Link-Überwachung 265, 273
Login-Dialog 17
Loop Guard 211, 213
Loops 244, 245, 249, 251

M

MAC-Adressen-Filter 133
MAC-Zieladresse 46
Mail-Benachrichtigung 289
MaxAge 200
MMS 340
Moduleigenschaften 371
Modus 108
MRP 178, 180, 181
MRP-over-LAG 188
MRP-Pakete 182
MRP-Paket-Priorisierung 183
Multicast 137

N
Nachricht 261
Netzlast 196, 197
Netzmanagement 54
Netzmanagementstation 373
Netzmaske 44, 48
NVM (permanenter Speicher) 87

O
Object Description 401
Object-ID 401
Objektklassen 401
ODVA 350
ODVA-Website 350
OpenSSH-Suite 21
Option 82 391
Ordinary-Clock (PTP) 85

P
Passwort 20, 22, 24
PC Worx 369
Permanenter Speicher (NVM) 87
Pfadkosten 198, 201
PHB 154
Polling 261
Port-Identifikation 197
Port-Mirroring 301
Port-Priorität 151
Port-Rollen (RSTP) 205
Port-Status 206
Precedence 154
Primär-Ring (RCP) 253
Priorität 145
Priority Tagged Frames 145
Privileged-Exec-Modus 26
PROFIBUS-Organisation 366
PTP 77
PTP-Domäne 86
PuTTY 18

Q
QoS 144
Query 137

R

RADIUS 59
RAM (flüchtiger Speicher) 87
Rapid Spanning Tree 178, 205
RCP 178
RCP, Anforderungen and die Topologie 256
RCP, erweiterte Informationen 255
RCP, Topologie der 2-Switch-Redundanten Kopplung 255
RCP, Topologieübersicht 255
RCP, Voraussetzungen 255
RCP-Pakete 256
Redundanz 196
Redundanz-Manager des Subrings 230
Referenzzeitquelle 77, 82, 85
Rekonfiguration 197
Rekonfigurationszeit (MRP) 181
Relaiskontakt 273
Report-Nachricht 137
RFC 403
Ring 180, 188
Ring-/Netzkopplung 178
Ring-/Netzkopplung, Anforderungen an die Verbindungs-Topologie 239
Ring-/Netz-Kopplung, Erweiterte Informationen 234
Ring-/Netzkopplung, Verbindungs-Topologie 2-Switch-Kopplung 235
Ring-/Netz-Kopplung, Verbindungs-Topologie 2-Switch-Kopplung mit Steuerleitung 236
Ring-/Netz-Kopplung, Verbindungs-Topologie der 1-Switch-Kopplung 234
Ring-/Netzkopplung-Pakete 237
Ring-/Netzkopplung-Paket-Priorisierung 239
Ring-Manager 180, 188
RIPE NCC 44
RM-Funktion 180, 188
RMON-Probe 301
Root Bridge 201
Root Guard 210, 213
Root-Pfad 202, 203
Root-Pfadkosten 197
Root-Port 205, 211
Router 44
RPI 351
RST BPDU 205, 207
RSTP 208
Ruhestromschaltung 273

S

Schulungsangebote 419
Schutzfunktionen (Guards) 210
Secure Shell 18, 21
Segmentierung 261
Sekundär-Ring (RCP) 253
Serielle Schnittstelle 18, 23
Service 294
Service Shell 26
Service Shell deaktivieren 39
SFP-Modul 282
Signalkontakt 273
Simatic S7 369
SNMP 261
SNMP-Trap 261, 263
SNTP 77
Software-Version 101
Sommerzeit 79
SSH 18, 21
Store and Forward 133
STP-BPDU 200
Strict-Priority 146
Subidentifier 401
Subnetz 48
Subring 178, 222
Subring-Manager 230
Symbol 350, 368, 370
Syslog über TLS 298
Systemanforderungen (grafische Benutzeroberfläche) 17

T

Tab-Completion 36
TCN Guard 211, 213
TCP/IP 350, 366
Technische Fragen 419
Topology-Change-Flag 211
ToS 143, 145, 154
Traffic Shaping 152
Transparent-Clock (PTP) 84
Trap 261, 263
Trap-Ziel-Tabelle 261
Type of Service 145

U

Übertragungssicherheit 261
UDP/IP 350, 366
Uhrzeit einstellen 77
Update 41
User-Exec-Modus 26

V

Verkehrsklasse 146, 151
Verzögerungszeit (MRP) 181
Video 146
VLAN 159
VLAN (HIPER-Ring) 192
VLAN-Priorität 150
VLAN-Tag 145, 159
VoIP 146
VT100 24

W

Warteschlange 146
Weighted Fair Queuing 146
Weighted Round Robin 146

Z

Ziel-Tabelle 261
Zugangsschutz 107

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 www.hirschmann.com.

Eine Liste von Telefonnummern und E-Mail-Adressen für direkten technischen Support durch Hirschmann finden Sie unter hirschmann-support.belden.com.

Sie finden auf dieser Website außerdem eine kostenfreie Wissensdatenbank sowie einen Download-Bereich für Software.

Technische Unterlagen

Die aktuellen Handbücher und Bedienungsanleitungen für Hirschmann-Produkte finden Sie unter doc.hirschmann.com.

Customer Innovation Center

Das Customer Innovation 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 www.belden.com/solutions/customer-innovation-center.
- Der Support reicht von der Inbetriebnahme über den Bereitschaftsservice bis zu Wartungskonzepten.

Mit dem Customer Innovation Center entscheiden Sie sich in jedem Fall gegen jeglichen Kompromiss. Das kundenindividuelle Angebot lässt Ihnen die Wahl, welche Komponenten Sie in Anspruch nehmen.

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 unterstützen uns, die Qualität und den Informationsgrad dieser Dokumentation noch zu steigern.

Ihre Beurteilung für dieses Handbuch:

	sehr gut	gut	befriedigend	mäßig	schlecht
Exakte Beschreibung	O	O	O	O	O
Lesbarkeit	O	O	O	O	O
Verständlichkeit	O	O	O	O	O
Beispiele	O	O	O	O	O
Aufbau	O	O	O	O	O
Vollständigkeit	O	O	O	O	O
Grafiken	O	O	O	O	O
Zeichnungen	O	O	O	O	O
Tabellen	O	O	O	O	O

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

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
  Deutschland

HIRSCHMANN

A BELDEN BRAND