HIRSCHMANN
A BELDEN BRAND

Hirschmann Automation and Control GmbH

# GRS103 HiOS-2S Rel. 10.6.00



## Referenz-Handbuch

Grafische Benutzeroberfläche

## Anwender-Handbuch

Konfiguration

Security

HIRSCHMANN
A BELDEN BRAND

# Referenz-Handbuch

## Grafische Benutzeroberfläche
## GREYHOUND Switch GRS103
## HiOS-2S



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.

© 2026 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** | 7 |
| | **Über dieses Handbuch** | 9 |
| | **Legende** | 10 |
| | **Hinweise zur grafischen Benutzeroberfläche** | 11 |
| | Sprachumschaltung | 11 |
| | Banner | 12 |
| | Menübereich | 13 |
| | Dialogbereich | 15 |
| **1** | **Grundeinstellungen** | 19 |
| 1.1 | System | 19 |
| 1.2 | Module | 25 |
| 1.3 | Netzwerk | 27 |
| 1.3.1 | Global | 28 |
| 1.3.2 | IPv4 | 30 |
| 1.3.3 | IPv6 | 34 |
| 1.4 | Out-of-Band via USB | 38 |
| 1.5 | Software | 40 |
| 1.6 | Laden/Speichern | 45 |
| 1.7 | Externer Speicher | 59 |
| 1.8 | Port | 62 |
| 1.9 | Power over Ethernet | 68 |
| 1.9.1 | PoE Global | 69 |
| 1.9.2 | PoE Port | 71 |
| 1.10 | Restart | 74 |
| **2** | **Zeit** | 77 |
| 2.1 | Grundeinstellungen | 77 |
| 2.2 | SNTP | 81 |
| 2.2.1 | SNTP Client | 82 |
| 2.2.2 | SNTP Server | 86 |
| **3** | **Gerätesicherheit** | 89 |
| 3.1 | Benutzerverwaltung | 89 |
| 3.2 | Authentifizierungs-Liste | 99 |
| 3.3 | Management-Zugriff | 102 |
| 3.3.1 | Server | 103 |
| 3.3.2 | IP-Zugriffsbeschränkung | 117 |
| 3.3.3 | Web | 121 |
| 3.3.4 | Command Line Interface | 122 |
| 3.3.5 | SNMPv1/v2 Community | 124 |
| 3.4 | Pre-Login-Banner | 125 |
| 3.5 | SSH Bekannte Hosts | 126 |

| | | |
|---|---|---|
| **4** | **Netzsicherheit** | 129 |
| 4.1 | Netzsicherheit Übersicht | 129 |
| 4.2 | Port-Sicherheit | 131 |
| 4.3 | 802.1X | 137 |
| 4.3.1 | 802.1X Global | 138 |
| 4.3.2 | 802.1X Port-Konfiguration | 140 |
| 4.3.3 | 802.1X Port-Clients | 146 |
| 4.3.4 | 802.1X EAPOL-Portstatistiken | 148 |
| 4.3.5 | 802.1X Verlauf Port-Authentifizierung | 150 |
| 4.3.6 | 802.1X Integrierter Authentifikations-Server (IAS) | 152 |
| 4.4 | RADIUS | 154 |
| 4.4.1 | RADIUS Global | 156 |
| 4.4.2 | RADIUS Authentication-Server | 158 |
| 4.4.3 | RADIUS Accounting-Server | 162 |
| 4.4.4 | RADIUS Authentication Statistiken | 164 |
| 4.4.5 | RADIUS Accounting-Statistiken | 166 |
| 4.5 | DoS | 167 |
| 4.5.1 | DoS Global | 168 |
| 4.6 | ACL | 171 |
| 4.6.1 | ACL IPv4-Regel | 172 |
| 4.6.2 | ACL MAC-Regel | 176 |
| 4.6.3 | ACL Zuweisung | 179 |
| **5** | **Switching** | 183 |
| 5.1 | Switching Global | 183 |
| 5.2 | Lastbegrenzer | 186 |
| 5.3 | Filter für MAC-Adressen | 189 |
| 5.4 | IGMP-Snooping | 192 |
| 5.4.1 | IGMP-Snooping Global | 193 |
| 5.4.2 | IGMP-Snooping Konfiguration | 195 |
| 5.4.3 | IGMP-Snooping Erweiterungen | 199 |
| 5.4.4 | IGMP Snooping-Querier | 202 |
| 5.4.5 | IGMP Snooping Multicasts | 205 |
| 5.5 | MRP-IEEE | 206 |
| 5.5.1 | MRP-IEEE Konfiguration | 207 |
| 5.5.2 | MRP-IEEE Multiple MAC Registration Protocol | 208 |
| 5.5.3 | MRP-IEEE Multiple VLAN Registration Protocol | 213 |
| 5.6 | GARP | 216 |
| 5.6.1 | GMRP | 217 |
| 5.6.2 | GVRP | 219 |
| 5.7 | QoS/Priority | 220 |
| 5.7.1 | QoS/Priority Global | 221 |
| 5.7.2 | QoS/Priorität Port-Konfiguration | 222 |
| 5.7.3 | 802.1D/p Zuweisung | 224 |
| 5.7.4 | IP-DSCP-Zuweisung | 226 |
| 5.7.5 | Queue-Management | 228 |
| 5.8 | VLAN | 229 |

5.8.1 VLAN Global . . . 230
5.8.2 VLAN Konfiguration . . . 231
5.8.3 VLAN Port . . . 234
5.8.4 VLAN Voice . . . 236
5.9 L2-Redundanz . . . 239
5.9.1 MRP . . . 240
5.9.2 Spanning Tree . . . 244
5.9.2.1 Spanning Tree Global . . . 245
5.9.2.2 Spanning Tree Port . . . 252
5.9.3 Link-Aggregation . . . 259
5.9.4 Link-Backup . . . 266

**6 Diagnose** . . . 271
6.1 Statuskonfiguration . . . 271
6.1.1 Gerätestatus . . . 272
6.1.2 Sicherheitsstatus . . . 277
6.1.3 Signalkontakt . . . 284
6.1.3.1 Signalkontakt 1 / Signalkontakt 2 . . . 285
6.1.4 MAC-Benachrichtigung . . . 290
6.1.5 Alarme (Traps) . . . 292
6.1.5.1 Trap V3 Benutzerverwaltung . . . 293
6.1.5.2 Trap Ziele . . . 297
6.2 System . . . 300
6.2.1 Systeminformationen . . . 301
6.2.2 Hardware-Zustand . . . 302
6.2.3 Konfigurations-Check . . . 303
6.2.4 IP-Adressen Konflikterkennung . . . 305
6.2.5 ARP . . . 309
6.2.6 Selbsttest . . . 311
6.3 Syslog . . . 313
6.4 Ports . . . 316
6.4.1 SFP . . . 317
6.4.2 TP-Kabeldiagnose . . . 318
6.4.3 Port-Monitor . . . 320
6.4.4 Auto-Disable . . . 330
6.4.5 Port-Mirroring . . . 334
6.5 LLDP . . . 337
6.5.1 LLDP Konfiguration . . . 338
6.5.2 LLDP Topologie-Erkennung . . . 342
6.6 Bericht . . . 346
6.6.1 Bericht Global . . . 347
6.6.2 Persistentes Ereignisprotokoll . . . 352
6.6.3 System-Log . . . 355
6.6.4 Audit-Trail . . . 356

**7 Erweitert** . . . 357
7.1 DHCP . . . 357
7.1.1 DHCP Server . . . 357

7.1.1.1 DHCP-Server Global . . . 358
7.1.1.2 DHCP-Server Pool . . . 360
7.1.1.3 DHCP-Server Lease-Tabelle . . . 367
7.2 DHCP-L2-Relay . . . 368
7.2.1 DHCP-L2-Relay Konfiguration . . . 370
7.2.2 DHCP-L2-Relay Statistiken . . . 373
7.3 Industrie-Protokolle . . . 374
7.3.1 IEC 61850/MMS . . . 375
7.3.2 Modbus TCP . . . 378
7.4 Command Line Interface . . . 380

**A** **Stichwortverzeichnis** . . . 381

**B** **Technische Unterstützung** . . . 387

**C** **Leserkritik** . . . 388

# 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“, das ausschließlich in englischer Sprache verfügbar ist, enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Geräts über das Command Line Interface.

Das Benutzerhandbuch „Sicherheit“, das ausschließlich in englischer Sprache verfügbar ist, bietet eine Einführung in die Planung der Systemsicherheit und die Entwicklung von Richtlinien. Es enthält eine detaillierte Auflistung der Sicherheitsmaßnahmen für das Gerät. Es beschreibt außerdem, wie ein geschütztes Gerät die Sicherheit und Verfügbarkeit Ihres Netzes verbessern kann. Sein Anhang enthält Details zu Hardware-Sicherheitssiegeln sowie einen Leitfaden zur Passwortstärke.

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:

| | |
|---|---|
| • <br> – | Listenpunkt<br>Listenpunkt – zweite Ebene |
| ▶ | Wert eines Parameters |
| ☐ | Handlungsschritt |
| 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

## Sprachumschaltung

Die grafische Benutzeroberfläche des Geräts ermöglicht Ihnen, die Anzeigesprache umzuschalten. Wenn Sie auf der Anmeldeseite die Sprache explizit wählen, fügt der Webbrowser einen Parameter `locale` zum URL in der Adressleiste hinzu, zum Beispiel `?locale=de`.

Ohne explizite Auswahl einer Anzeigesprache richtet sich die Anzeigesprache nach der bevorzugten Sprache für Webseiten (auch Website oder Content genannt) in den Einstellungen des Webbrowsers. Bei nicht unterstützten bevorzugten Sprachen zeigt das Gerät die grafische Benutzeroberfläche in Englisch (USA).

Die Anzeigesprache bestimmt auch das Anzeigeformat von Datums- und Zeitangaben.

Details:
- Wenn die bevorzugte Sprache für Webseiten Deutsch ist, zeigt das Gerät die grafische Benutzeroberfläche in Deutsch. Dies schließt Datums- und Zeitangaben im deutschen Format `DD.MM.YYYY, HH:MM:SS` ein.
  Beispiel: `20.05.2026, 12:34:56`
- Wenn die bevorzugte Sprache für Webseiten eine andere als Deutsch ist, zeigt das Gerät die grafische Benutzeroberfläche in Englisch (USA). Dies schließt Datums- und Zeitangaben im US-Format `MMM DD, YYYY, HH:MM:SS {AM|PM}` ein.
  Beispiel: `May 20, 2026, 12:34:56 PM`

# Banner

Das Banner zeigt die folgenden Informationen:



Blendet den Menübereich ein oder aus.

Hersteller-Logo

Zeigt das Hersteller-Logo.

Name des Dialogs

Zeigt den Namen des gegenwärtig im Dialogbereich angezeigten Dialogs.



Zeigt, dass der Webbrowser 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 nichtflüchtigen Speicher (*NVM*) abweichen. Das Banner zeigt das Symbol, sobald Sie die Einstellungen angewendet, diese jedoch noch nicht im nichtflüchtigen 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*.

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 den Eintrag klicken, meldet dies den gegenwärtig angemeldeten Benutzer ab. Danach öffnet sich der Login-Dialog.

# Menübereich

Um den Menübereich ein- oder auszublenden, klicken Sie im Banner die Schaltfläche  .

Der Menübereich ist wie folgt unterteilt:
- Symbolleiste
- Menübaum

## Symbolleiste

Die Symbolleiste zeigt die folgenden Informationen:

Geräte-Software

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



Zeigt ein Textfeld, um nach einem Schlüsselwort zu suchen. Wenn Sie ein Zeichen oder eine Zeichenkette eingeben, 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 auf. Der Menübaum zeigt dann jeden Menüeintrag auf jeder Ebene.

Um wieder den eingeklappten Menübaum anzuzeigen, klicken Sie die Schaltfläche  . Der Menübaum zeigt dann ausschließlich Menüeinträge der ersten 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 visuelle Eigenschaften:

- Schreibgeschützte Bedienelemente
  - mittel-dunkler Rand
  - heller Hintergrund (Kontrollkästchen, Optionsfelder)
  - schattierter Hintergrund (Eingabefelder)
- Editierbare Bedienelemente
  - dunkler Rand
  - heller Hintergrund

## 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 die Änderung noch nicht angewendet haben. Die geänderten Einstellungen sind noch nicht wirksam.

## Standard-Schaltflächen

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



Wendet die von Ihnen geänderten Einstellungen im Gerät an.

Informationen darüber, wie das Gerät die geänderten Einstellungen auch nach einem Neustart beibehält, finden Sie im Abschnitt „Einstellungen speichern” auf Seite 16.

Verwirft nicht gespeicherte Änderungen im gegenwärtigen Dialog. Setzt die Werte in den Feldern auf die im Gerät angewendeten Einstellungen zurück.

### Einstellungen speichern

Beim Anwenden der Einstellungen speichert das Gerät die geänderten Einstellungen vorläufig. 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 nichtflüchtigen 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 Tabellenzeile 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:

- Tabellenzeilen filtern
- Tabellenzeilen sortieren
- Mehrere Tabellenzeilen auswählen

### Tabellenzeilen filtern

Der Filter ermöglicht Ihnen, die Anzahl der angezeigten Tabellenzeilen zu verringern.



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

### Tabellenzeilen sortieren

Die Reihenfolge der Tabellenzeilen können Sie ändern. Ein Symbol zeigt den Sortierstatus, sobald Sie den Tabellenkopf klicken.



Die Zeilen der Tabelle sind anhand der Einträge der betreffenden Spalte in absteigender Reihenfolge sortiert.

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



Die Zeilen der Tabelle sind anhand der Einträge der betreffenden Spalte in aufsteigender Reihenfolge sortiert.

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.

### Mehrere Tabellenzeilen auswählen

Sie haben die Möglichkeit, mehrere Tabellenzeilen auf einmal auszuwählen und eine Aktion auf die ausgewählten Tabellenzeilen anzuwenden.

- ☐ Um in der Tabelle einzelne Zeilen auszuwählen, markieren Sie das Kontrollkästchen ganz links in der gewünschten Tabellenzeile.
- ☐ Um in der Tabelle jede Zeile auszuwählen, markieren Sie das Kontrollkästchen ganz links im Tabellenkopf.

Sobald Sie mehrere Tabellenzeilen gewählt haben, können Sie eine Aktion auf jede dieser Tabellenzeilen gleichzeitig anwenden, zum Beispiel:

- die Werte in einer Tabellenspalte eingeben oder ändern
- mehrere Tabellenzeilen entfernen

# 1 Grundeinstellungen

Das Menü enthält die folgenden Dialoge:

- System
- Module
- Netzwerk
- Out-of-Band via USB
- Software
- Laden/Speichern
- Externer Speicher
- Port
- Power over Ethernet
- Restart

## 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 ein Alarm vorliegt, wechselt die Hintergrundfarbe zu rot. Andernfalls bleibt 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 jeweiligen 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 löst einen Alarm aus, wenn Sie an ein Gerät, das die Überwachung von 2 redundanten Netzteilen unterstützt, lediglich ein Netzteil anschließen. Um diesen 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 ein Alarm vorliegt, wechselt die Hintergrundfarbe zu rot. Andernfalls bleibt 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 jeweiligen 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 ein Alarm vorliegt, wechselt die Hintergrundfarbe zu rot. Andernfalls bleibt die Hintergrundfarbe grün.

Die Parameter, die das Gerät überwacht, legen Sie fest im Dialog *Diagnose* > *Statuskonfiguration* > Signalkontakt > *Signalkontakt 1*/*Diagnose* > *Statuskonfiguration* > *Signalkontakt* > *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 jeweiligen 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 1*/*Diagnose* > *Statuskonfiguration* > *Signalkontakt* > Signalkontakt 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 Generieren eines digitalen Zertifikats 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 Fully Qualified Domain Name (FQDN). Aus Kompatibilitätsgründen ist es empfehlenswert, ausschließlich 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*
- *IEC 61850/MMS*

Standort

Legt den gegenwärtigen oder geplanten Standort fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
  Das Gerät akzeptiert die folgenden Zeichen:
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Ansprechpartner

Legt den Ansprechpartner für dieses Gerät fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
  Das Gerät akzeptiert die folgenden Zeichen:
  - `0..9`
  - `a..z`
  - `A..Z`
  - `!#$%&'()*+,-./:;<=>?@[\\]^_`{}~`

Gerätetyp

Zeigt die Produktbezeichnung des Grundgeräts.

Netzteil 1
Netzteil 2

Zeigt den Status des Netzteils am betreffenden Spannungsversorgungs-Anschluss.

Mögliche Werte:

- *vorhanden*
- *nicht erkannt*
- *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 Schwellenwerte für die Temperatur aktivieren Sie im Dialog *Diagnose* > Statuskonfiguration > *Gerätestatus*.

Obere Temp.-Grenze [°C]

Legt den oberen Schwellenwert für die Temperatur in °C fest.

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 Schwellenwert für die Temperatur in °C fest.

Mögliche Werte:

- `-99..99` (ganze Zahl)
  Wenn die Temperatur 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 ein Alarm vor. Für Details siehe Rahmen *Geräte-Status*.

Power



Wenn das Gerät 2 redundante Netzteile unterstützt: Lediglich eine Versorgungsspannung liegt an.



Wenn das Gerät ein Netzteil unterstützt: Die Versorgungsspannung liegt an.

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

ACA



Kein externer Speicher (*ENVM*) angeschlossen.



Der externe Speicher (*ENVM*) ist angeschlossen, jedoch nicht betriebsbereit.



Der externe Speicher (*ENVM*) ist angeschlossenen und betriebsbereit.

**Status Port**

Dieser Rahmen zeigt eine vereinfachte Ansicht der Ports zum Zeitpunkt der letzten Anzeigeaktualisierung. Den Port-Status erkennen Sie an der Markierung.

In der Grundansicht zeigt der Rahmen lediglich Ports mit aktivem Link. Wenn Sie die Schaltfläche  klicken, zeigt der Rahmen sämtliche Ports.

- Neben der Port-Nummer steht die Port-Übertragungsrate.
- Wenn Sie den Mauszeiger über dem Port-Symbol positionieren oder darauf tippen, zeigt ein Tooltip detaillierte Informationen zum Port-Status.

Grüne Hintergrundfarbe

Port mit aktivem Link.

Graue Hintergrundfarbe

Port mit inaktivem Link.

Gelbe Hintergrundfarbe

Port, an dem das Gerät einen nicht unterstützten SFP-Transceiver oder eine nicht unterstützte Datenrate erkannt hat.

Gestrichelte Umrandung

Port ist aufgrund einer Redundanzfunktion im Zustand *Blocking*.

# 1.2 Module

[ Grundeinstellungen > Module ]

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

Solange die Spalte *Status Ethernet-Modul* den Wert `configurable` zeigt, können Sie das Modul einrichten 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, richtet das Gerät das Modul mit seinen Voreinstellungen ein. 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 richtet das Modul automatisch anhand der Voreinstellungen ein und erkennt die Modul-Parameter.
- ☐ Um die grafische Benutzeroberfläche zu aktualisieren, klicken Sie die Schaltfläche .
  Die Spalte *Status Ethernet-Modul* zeigt für das installierte Ethernet-Modul den Wert `physical`.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

### Steckplatz aktivieren/deaktivieren

Auf einem inaktiven Steckplatz erkennt das Gerät das installierte Modul und ermöglicht Ihnen, die Ports einzurichten. Das Modul stellt auf einem inaktivem Steckplatz keine Verbindungen ins Netz her.

Führen Sie die folgenden Schritte aus:

- ☐ Wählen Sie die Tabellenzeile 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu 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 *Status Ethernet-Modul* zeigt für das zuvor entfernte Modul den Wert `configurable`.
- ☐ Wählen Sie die Tabellenzeile des zuvor entfernten Moduls.
- ☐ Klicken Sie die Schaltfläche .
  Die Spalte *Status Ethernet-Modul* 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen



Ethernet-Modul entfernen

Entfernt das markierte Ethernet-Modul aus der Tabelle.

Ethernet-Modul

Zeigt die Nummer des Steckplatzes, auf den sich die Tabellenzeile bezieht.

Aktiv

Aktiviert/deaktiviert den Steckplatz.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Der Steckplatz ist aktiv. Das Gerät erkennt das in diesem Steckplatz installierte Modul.
- `unmarkiert`
  Der Steckplatz ist inaktiv.

Typ

Zeigt den Typ 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 die Anzahl der Ports, die 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.

Status Ethernet-Modul

Zeigt den Status des Steckplatzes.

Mögliche Werte:

- *physical*
  Im Steckplatz ist ein Modul installiert.
- *configurable*
  Der Steckplatz ist leer und bereit zum Einrichten.
- *remove*
  Der Steckplatz ist leer und inaktiv.
- *fix*
  Das Modul kann nicht entfernt werden.

## 1.3 Netzwerk

[ Grundeinstellungen > Netzwerk ]

Das Menü enthält die folgenden Dialoge:

- Global
- IPv4
- IPv6

# 1.3.1 Global

[ Grundeinstellungen > Netzwerk > Global ]

Dieser Dialog ermöglicht Ihnen, die VLAN- und HiDiscovery-Einstellungen festzulegen, die für den Zugriff über das Netz auf das Management des Geräts erforderlich sind.

### Management-Schnittstelle

Dieser Rahmen ermöglicht Ihnen, das VLAN festzulegen, in dem das Management des Geräts erreichbar ist.

MAC-Adresse

Zeigt die MAC-Adresse des Geräts. Mit der MAC-Adresse ist das Management des Geräts über das Netz erreichbar.

### 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 > Netzwerk > IPv4 ]

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

### Konfiguration

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.

**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.

### Management-Schnittstelle

VLAN-ID

Legt das VLAN fest, in dem das Management des Geräts über das Netz erreichbar ist. Das Management des Geräts ist ausschließlich über Ports erreichbar, die Mitglied dieses VLANs sind.

Mögliche Werte:

- `1..4042` (Voreinstellung: `1`)
  Die Dropdown-Liste enthält ausschließlich die VLANs, die im Dialog *Switching > VLAN > Konfiguration* bereits eingerichtet sind.

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.
  oder
  Wählen Sie den Eintrag *VLAN-Port-Einstellungen nicht ändern*, um die Port-VLAN-Einstellungen beizubehalten. Diese Option ist sinnvoll, wenn die VLANs bereits eingerichtet sind.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Gerät weist dem Port die VLAN-Einstellungen zu:
  - Der Port ist 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 Zeit ist das Gerät über den gewählten Port im gewählten Management-VLAN erreichbar.

### 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 der Server entsprechend eingerichtet ist, 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.

Lease-Time [s]

Zeigt die verbleibende Zeit in Sekunden, bevor die IP-Adresse, die dem Management des Geräts vom DHCP-Server zugewiesen wurde, ihre Gültigkeit verliert.

Um die Anzeige zu aktualisieren, klicken Sie die Schaltfläche .

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 folgender DHCP-Optionen:
  - `Option 66: TFTP server name`
    `Option 67: Boot file name`
    Das Gerät lädt mittels Trivial File Transfer Protocol (TFTP) 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.

# 1.3.3 IPv6

[ Grundeinstellungen > Netzwerk > IPv6 ]

In diesem Dialog legen Sie die IPv6-Einstellungen fest, die für den Zugriff über das -Netz auf das Management des Geräts erforderlich sind.

## Funktion

Funktion

Aktiviert/deaktiviert das IPv6-Protokoll im Gerät.

Sie können IPv4 und IPv6 gleichzeitig im Gerät betreiben. Das wird durch die Verwendung von Dual IP Layer, auch Dual Stack genannt, ermöglicht.

Mögliche Werte:

- *An* (Voreinstellung)
  IPv6 ist eingeschaltet.
- *Aus*
  IPv6 ist ausgeschaltet.
  Wenn das Gerät ausschließlich IPv4 verwenden soll, deaktivieren Sie IPv6 im Gerät.

## Konfiguration

Dynamische IP-Adresszuweisung

Legt fest, aus welcher Quelle das Management des Geräts seine IPv6-Parameter erhält.

Mögliche Werte:

- *Kein*
  Das Gerät erhält seine IPv6-Parameter durch manuelle Zuweisung.
  Sie können maximal 4 IPv6-Adressen manuell festlegen. Sie können Loopback-, Link-Local- und Multicast-Adressen nicht als statische IPv6-Adressen festlegen.
- *Auto* (Voreinstellung)
  Das Gerät erhält seine IPv6-Parameter durch dynamische Zuweisung. Das Gerät erhält maximal 2 IPv6-Adressen.
  Ein Beispiel ist der Router Advertisement Daemon (radvd). Der radvd verwendet *Router Solicitation*- und *Router Advertisement*-Nachrichten zur automatischen Einrichtung einer IPv6-Adresse. Die *Router Solicitation*- und *Router Advertisement*-Nachrichten werden im RFC 4861 beschrieben.
- *DHCPv6*
  Das Gerät erhält seine IPv6-Parameter von einem DHCPv6-Server.
- *Alle*
  Wenn das Optionsfeld *Alle* ausgewählt ist, dann erhält das Gerät seine IPv6-Parameter durch dynamische und manuelle Zuweisung.

### Management-Schnittstelle

VLAN-ID

Legt das VLAN fest, in dem das Management des Geräts über das Netz erreichbar ist. Das Management des Geräts ist ausschließlich über Ports erreichbar, die Mitglied dieses VLANs sind.

Mögliche Werte:

- `1..4042` (Voreinstellung: `1`)
  Die Dropdown-Liste enthält ausschließlich die VLANs, die im Dialog *Switching > VLAN > Konfiguration* bereits eingerichtet sind.

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.
  oder
  Wählen Sie den Eintrag *VLAN-Port-Einstellungen nicht ändern*, um die Port-VLAN-Einstellungen beizubehalten. Diese Option ist sinnvoll, wenn die VLANs bereits eingerichtet sind.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Gerät weist dem Port die VLAN-Einstellungen zu:
  - Der Port ist 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 Zeit ist das Gerät über den gewählten Port im gewählten Management-VLAN erreichbar.

### DHCP

Client-ID

Zeigt die DHCPv6-Client-ID, die das Gerät an den DHCPv6-Server sendet. Wenn der Server entsprechend eingerichtet ist, dann erhält das Client-Gerät eine IPv6-Adresse für diese DHCPv6-Client-ID.

Die vom DHCPv6-Server empfangene IPv6-Adresse hat den *Prefix-Länge*-Wert `128`. Gemäß RFC 8415 kann ein DHCPv6-Server gegenwärtig nicht dazu verwendet werden, *Gateway-Adresse*- oder *Prefix-Länge*-Informationen bereitzustellen.

Das Gerät kann ausschließlich eine IPv6-Adresse vom DHCPv6-Server erhalten.

### IP-Parameter

Gateway-Adresse

Legt die IPv6-Adresse eines Routers fest, über den das Gerät andere Geräte außerhalb des eigenen Netzes erreicht.

Mögliche Werte:

- Gültige IPv6-Adresse (außer Loopback- und Multicast-Adressen)

**Anmerkung:**
Wenn das Optionsfeld *Auto* ausgewählt ist und Sie einen Router Advertisement Daemon (radvd) verwenden, dann erhält das Gerät automatisch eine Link-Local-Adresse als *Gateway-Adresse*, die eine höhere Metrik hat als die manuell eingestellte *Gateway-Adresse*.

### Erkennung doppelter Adressen

In diesem Feld können Sie die Anzahl der aufeinanderfolgenden *Neighbor Solicitation*-Nachrichten festlegen, die das Gerät mit der Funktion *Erkennung doppelter Adressen* sendet. Diese Funktion wird verwendet, um die Eindeutigkeit einer IPv6-Unicast-Adresse auf dem Interface festzustellen.

Anzahl der Nachbarn

Legt die Anzahl der *Neighbor Solicitation*-Nachrichten fest, die das Gerät mit der Funktion *Erkennung doppelter Adressen* sendet.

Mögliche Werte:

- `0`
  Die Funktion ist ausgeschaltet.
- `1..5` (Voreinstellung: `1`)

Wenn die Funktion *Erkennung doppelter Adressen* erkennt, dass eine IPv6-Adresse auf einem Link nicht eindeutig ist, dann protokolliert das Gerät dieses Ereignis nicht in der Log-Datei (System Log).

### Tabelle

Diese Tabelle zeigt eine Liste der IPv6-Adressen, die für das Management des Geräts eingerichtet sind.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Prefix

Zeigt den Präfix einer IPv6-Adresse in verkürzter Schreibweise. Der Präfix zeigt die Bits am linken Rand einer IPv6-Adresse, den Netzanteil der Adresse.

Prefix-Länge

Zeigt die Präfixlänge der IPv6-Adresse.

Im Gegensatz zu einer IPv4-Adresse verwendet eine IPv6-Adresse keine Subnetzmaske, um den Teil der Adresse zu kennzeichnen, der zum Subnetz gehört. Diese Funktion übernimmt die Präfixlänge in IPv6.

Mögliche Werte:

- `0..128`

IP-Adresse

Zeigt die gesamte IPv6-Adresse in verkürzter Schreibweise.

Die verkürzte Schreibweise wird automatisch auf jede IPv6-Adresse angewendet, unabhängig davon, aus welcher Quelle das Management des Geräts seine IPv6-Parameter erhält.

Mögliche Werte:

- Gültige IPv6-Adresse
  Für die Verwendung einer IPv6-Adresse in einer URL gilt die folgende URL-Syntax: `https://[<ipv6_address>]`.

Weitere Informationen zu den Verkürzungsregeln und Adresstypen in IPv6 finden Sie im Anwender-Handbuch „Konfiguration“.

EUI-Option

Legt fest, ob die Funktion *EUI-Option* auf die IPv6-Adresse angewendet wird.

Wenn Sie dieses Kontrollkästchen markieren, wird die Interface-ID der IPv6-Adresse automatisch festgelegt. Das Gerät verwendet die MAC-Adresse des Interface, erweitert um die Werte `ff` und `fe` zwischen Byte 3 und Byte 4, um eine 64 Bit lange Interface-ID zu generieren.

Sie können diese Option ausschließlich für IPv6-Adressen wählen, deren Präfixlänge `64` entspricht.

Mögliche Werte:

- `markiert`
  Die Funktion *EUI-Option* ist aktiv.
- `unmarkiert` (Voreinstellung)
  Die Funktion *EUI-Option* ist inaktiv.

Ursprung

Legt fest, auf welche Weise das Gerät seine IPv6-Parameter erhalten hat.

Mögliche Werte:

- *Autoconf*
  Das Gerät hat die IPv6-Adresse durch dynamische Zuweisung erhalten, wenn das Optionsfeld *Auto* ausgewählt ist.
- *Manuell*
  Das Gerät hat die IPv6-Adresse durch manuelle Zuweisung erhalten.
- *DHCP*
  Das Gerät hat die IPv6-Adresse von einem DHCPv6-Server erhalten.
- *Linklayer*
  Das Gerät legt automatisch eine Link-Local-IPv6-Adresse fest. Die Link-Local-Adresse kann nicht geändert werden.

Status

Zeigt den gegenwärtigen Status der IPv6-Adresse.

Mögliche Werte:

- *aktiv*
  Die IPv6-Adresse ist aktiv.
- *notInService*
  Die IPv6-Adresse ist inaktiv.
- *notReady*
  Die IPv6-Adresse ist festgelegt, aber gegenwärtig nicht aktiv, da noch einige Konfigurationsparameter fehlen.

**Anmerkung:**
Wenn die IPv6-Adresse manuell festgelegt wird, können Sie manuell zwischen Status *aktiv* und Status *notInService* wechseln. Wählen Sie dazu in der Dropdown-Liste in Spalte *Status* den gewünschten Status für die entsprechende Tabellenzeile.

## 1.4 Out-of-Band via USB

[ Grundeinstellungen > Out-of-Band via USB ]

Das Gerät verfügt über eine USB-Netzschnittstelle, die Ihnen Out-of-Band-Zugriff auf das Management des Geräts ermöglicht. Bei hoher In-Band-Last auf den Switching-Ports haben Sie über die USB-Netzschnittstelle dennoch Zugriff auf das Management des Geräts.

Das Gerät ermöglicht Ihnen über die USB-Netzschnittstelle den Zugriff auf das Management des Geräts mit den folgenden Protokollen:

- HTTP
- HTTPS
- SSH
- Telnet
- SNMP
- FTP
- TFTP
- SFTP
- SCP

Beim Zugriff auf das Management des Geräts gibt es folgende Einschränkungen:

- Die Management-Station ist direkt an den USB-Port angeschlossen.
- Die USB-Netzschnittstelle unterstützt keine der folgenden Merkmale:
  - Pakete mit Prioritäts-Tag
  - Pakete mit *VLAN*-Tag
  - *DHCP-L2-Relay*
  - *LLDP*
  - *DiffServ*
  - *ACL*
  - *Industrie-Protokolle*

In diesem Dialog ermöglicht Ihnen das Gerät, die IP-Parameter zu ändern und die USB-Netzschnittstelle bei Bedarf auszuschalten.

### Funktion

Funktion

Schaltet die USB-Netzschnittstelle ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Das Gerät ermöglicht Ihnen den Zugriff auf das Management des Geräts über die USB-Netzschnittstelle.
- *Aus*
  Das Gerät unterbindet den Zugriff auf das Management des Geräts über die USB-Netzschnittstelle.

### Management-Schnittstelle

Gerät MAC-Adresse

Zeigt die MAC-Adresse der USB-Netzschnittstelle.

Host MAC-Adresse

Zeigt die MAC-Adresse der angeschlossenen Management-Station.

### IP-Parameter

Vergewissern Sie sich, dass das IP-Subnetz dieser Netzschnittstelle sich nicht mit einem Subnetz überschneidet, das mit einem anderen Interface des Gerätes verbunden ist:

- Management-Interface

IP-Adresse

Legt die IP-Adresse fest, mit der das Management des Geräts über die USB-Netzschnittstelle erreichbar ist.

Mögliche Werte:

- Gültige IPv4-Adresse
  (Voreinstellung: `192.168.248.100`)
  Das Gerät weist diese IP-Adresse, um 1 erhöht, der Management-Station zu, die mit dem Gerät verbunden ist.
  Beispiel: `192.168.248.100` für die USB-Netzschnittstelle, `192.168.248.101` für die Management-Station.

Netzmaske

Legt die Netzmaske fest.

Mögliche Werte:

- Gültige IPv4-Netzmaske
  (Voreinstellung: `255.255.255.0`)

# 1.5 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:**
Bevor Sie die Geräte-Software aktualisieren, beachten Sie 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 Systemstart.

Ausgeführte Version

Zeigt Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Systemstart 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 bei der letzten Software-Aktualisierung oder nach Klicken der Schaltfläche *Wiederherstellen* in den Backup-Bereich kopiert.

Wiederherstellen

Das Gerät vertauscht die Images der Geräte-Software und dementsprechend die in den Feldern *Gespeicherte Version* und *Backup-Version* angezeigten Werte.

Beim nächsten Systemstart lädt das Gerät die im Feld *Gespeicherte Version* angezeigte Geräte-Software.

Bootcode

Zeigt Versionsnummer und Erstellungsdatum des Bootcodes.

### Software-Update

Das Gerät ermöglicht Ihnen, die Geräte-Software an dieser Stelle zu aktualisieren, wenn ein geeignetes Image der Geräte-Software außerhalb des Geräts verfügbar ist. Wenn ein geeignetes Image der Geräte-Software auf dem ausgewählten externen Speicher (*ENVM*) gespeichert ist, verwenden Sie die Tabelle auf der Registerkarte *Dateisystem* weiter unten.

URL

Legt Pfad und Dateiname des Images der Geräte-Software fest, mit dem Sie die Geräte-Software aktualisieren.

Das Gerät bietet Ihnen folgende Möglichkeiten, die Geräte-Software zu aktualisieren:

- Software-Aktualisierung vom PC

  Ziehen Sie die Datei von Ihrem PC oder Netzlaufwerk in den ⬆-Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.
- Software-Aktualisierung über FTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Wenn sich die Datei auf einem FTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>[:Port]/<Dateiname>`
- Software-Aktualisierung über TFTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Wenn sich die Datei auf einem TFTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Software-Aktualisierung über SCP oder SFTP
  Wenn sich die Datei auf einem SCP- oder SFTP-Server befindet, dann legen Sie den URL in einer der folgenden Formen fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Klicken Sie die Schaltfläche *Start*, um das Fenster *Anmeldeinformationen* zu öffnen. In diesem Fenster geben Sie *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

  Denken Sie daran, den SCP- oder SFTP-Server zunächst als bekannten Host für SSH einzurichten, bevor das Gerät das erste Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.

Start

Aktualisiert die Geräte-Software.

- Um während des Software-Updates beim Management des Geräts angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ dazu können Sie, bevor Sie das Software-Update starten, einen ausreichend großen Wert im Dialog *Gerätesicherheit > Management-Zugriff > Web*, Feld *Webinterface-Session Timeout [min]* festlegen.
- Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
- Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software. Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

### Hochladen unsignierter Geräte-Software erlauben

Aktiviert/deaktiviert die Option, dass das Gerät das Hochladen einer unsignierten Geräte-Software erlaubt. Der Zweck dieser Einstellung ist, das Hochladen einer Geräte-Software zuzulassen, die keine kryptografische Signatur hat.

Mögliche Werte:

- `markiert`
  Das Gerät erlaubt das Hochladen einer unsignierten Geräte-Software.
  Das Hochladen einer unsignierten Geräte-Software kann ein Sicherheitsrisiko darstellen. Wenn Sie dem Urheber vertrauen, können Sie die unsignierte Geräte-Software hochladen.
- `unmarkiert` (Voreinstellung)
  Das Gerät erlaubt ausschließlich das Hochladen einer signierten Geräte-Software.

### Secure Boot eingeschaltet

Aktiviert einen Modus, in dem das Gerät ausschließlich mit einem Software-Image bootet, das eine gültige kryptografische Signatur aufweist.

Mögliche Werte:

- `markiert`
  Während des Systemstarts bootet das Gerät ausschließlich mit einem Image der Geräte-Software, das eine gültige kryptografische Signatur aufweist.
  Sobald die Betriebsart aktiviert ist, kann man sie nicht wieder deaktivieren:
  - Das Kontrollkästchen ist dauerhaft ausgegraut.
  - Sie können kein Downgrade auf eine Software-Version früher als 10.3.03 durchführen.
  - Das Kontrollkästchen *Hochladen unsignierter Geräte-Software erlauben* ist dauerhaft ausgeblendet.
- `unmarkiert` (Voreinstellung)
  Beim Systemstart bootet das Gerät mit einem beliebigen Image der Geräte-Software, unabhängig davon, ob das Image der Geräte-Software kryptografisch signiert ist oder nicht. Im Fall eines kryptografisch signierten Images der Geräte-Software muss dessen Signatur jedoch gültig sein.

## [Dateisystem]

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Update Firmware

Aktualisiert die Geräte-Software, wenn auf dem externen Speicher (*ENVM*) ein geeignetes Image der Geräte-Software gespeichert ist. Voraussetzung ist, dass eine Tabellenzeile ausgewählt ist, für welche die Spalte *Datei Ort* den Wert *usb* zeigt.

- Um während des Software-Updates beim Management des Geräts angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ dazu können Sie, bevor Sie das Software-Update starten, einen ausreichend großen Wert im Dialog *Gerätesicherheit > Management-Zugriff > Web*, Feld *Webinterface-Session Timeout [min]* festlegen.
- Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
- Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software. Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

Datei Ort

Zeigt den Speicherort der Geräte-Software.

Mögliche Werte:

- *ram*
  Flüchtiger Speicher des Geräts
- *flash*
  Nichtflüchtiger Speicher (*NVM*) des Geräts
- *usb*
  Externer USB-Speicher (ACA21/ACA22)

Index

Zeigt den Index der Geräte-Software.

Die Index-Nummer der Geräte-Software im Flash-Speicher hat die folgende Bedeutung:

- 1
  Beim nächsten Systemstart lädt das Gerät diese Geräte-Software.
- 2
  Diese Geräte-Software hat das Gerät bei der letzten Software-Aktualisierung in den Backup-Bereich kopiert.

Dateiname

Zeigt den geräteinternen Dateinamen der Geräte-Software.

Firmware

Zeigt Versionsnummer und Erstellungsdatum der Geräte-Software.

# 1.6 Laden/Speichern

[ Grundeinstellungen > Laden/Speichern ]

Dieser Dialog ermöglicht Ihnen, die Einstellungen des Geräts dauerhaft 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 nichtflüchtigen 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

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Löschen

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

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

Speichern

Speichert die vorläufig angewendeten Einstellungen in dem als „ausgewählt“ gekennzeichneten Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*).

Wenn im Dialog *Grundeinstellungen > Externer Speicher* das Kontrollkästchen in Spalte *Sichere Konfiguration beim Speichern* markiert ist, dann speichert das Gerät eine Kopie des Konfigurationsprofils im externen Speicher (*ENVM*).



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 nichtflüchtigen Speicher (*NVM*) zu speichern.

- ☐ Klicken Sie die Dropdown-Liste *Profilname* und geben Sie im Suchfeld den Namen ein, unter dem Sie das Konfigurationsprofil speichern möchten (maximal 32 Zeichen).
  - ☐ Um ein bereits vorhandenes Konfigurationsprofil zu überschreiben, wählen Sie in den Suchergebnissen den gewünschten Eintrag.
  - ☐ Um das Konfigurationsprofil unter einem neuen Namen zu speichern, klicken Sie den Link *Erstellen* unterhalb des Suchfelds.

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 Hinzufügen 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 nichtflüchtigen 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 Systemstart 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 nichtflüchtigen 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 externen Speicher (*ENVM*).

☐ 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 diese in den ↑-Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.
  – Import über FTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Wenn sich die Datei auf einem FTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>[:Port]/<Dateiname>`

- Import über TFTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Wenn sich die Datei auf einem TFTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Import über SCP oder SFTP
  Wenn sich die Datei auf einem SCP- oder SFTP-Server befindet, dann legen Sie den URL in einer der folgenden Formen fest:
  `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
  Klicken Sie die Schaltfläche *Start*, um das Fenster *Anmeldeinformationen* zu öffnen. In diesem Fenster geben Sie *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`
  Denken Sie daran, den SCP- oder SFTP-Server zunächst als bekannten Host für SSH einzurichten, bevor das Gerät das erste Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.

☐ 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 *Speicherort* legen Sie den Speicherort für das Konfigurationsprofil fest. Voraussetzung ist, dass in der Dropdown-Liste *Select source* der Eintrag *PC/URL* ausgewählt ist.

▶ *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 nichtflüchtigen 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 über FTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  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 über TFTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  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 über SCP oder SFTP
  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>`
    Klicken Sie die Schaltfläche *Ok*, um das Fenster *Anmeldeinformationen* zu öffnen. In diesem Fenster geben Sie *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

  Denken Sie daran, den SCP- oder SFTP-Server zunächst als bekannten Host für SSH einzurichten, bevor das Gerät das erste Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit* > SSH Bekannte Hosts.

Running-Config als Skript speichern

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.

Running-Config aus Skript laden

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 diese in den -Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.
- Import über FTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Wenn sich die Datei auf einem FTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
  `ftp://<Benutzername>:<Passwort>@<IP-Adresse>[:Port]/<Dateiname>`

- Import über TFTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Wenn sich die Datei auf einem TFTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Import über SCP oder SFTP
  Wenn sich die Datei auf einem SCP- oder SFTP-Server befindet, dann legen Sie den URL in einer der folgenden Formen fest:
  `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
  Denken Sie daran, den SCP- oder SFTP-Server zunächst als bekannten Host für SSH einzurichten, bevor das Gerät das erste Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit* > SSH Bekannte Hosts.

Auf Lieferzustand zurücksetzen...

Setzt die Geräteeinstellungen auf die Voreinstellungen zurück.

- Das Gerät löscht die gespeicherten Konfigurationsprofile aus dem flüchtigen Speicher (*RAM*) und aus dem nichtflüchtigen Speicher (*NVM*).
- Das Gerät löscht das vom Webserver im Gerät verwendete digitale Zertifikat.
- Das Gerät löscht den vom SSH-Server im Gerät verwendeten RSA-Schlüssel (Host Key).
- Ist ein externer Speicher (*ENVM*) angeschlossen, löscht das Gerät die auf dem externen Speicher gespeicherten Konfigurationsprofile.
- Nach kurzer Zeit startet das Gerät neu und verwendet dann die Werkseinstellungen.

Auf Default-Zustand zurücksetzen

Löscht die gegenwärtigen Betriebseinstellungen (`running config`) aus dem flüchtigen Speicher (*RAM*).

Speicherort

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* (nichtflüchtiger Speicher des Geräts)
  Aus dem nichtflüchtigen Speicher lädt das Gerät das „ausgewählte“ Konfigurationsprofil beim Systemstart oder beim Anwenden der Funktion *Konfigurationsänderungen rückgängig machen*.
  Der nichtflüchtige Speicher bietet Platz für mehrere Konfigurationsprofile, abhängig von der Anzahl der im Konfigurationsprofil gespeicherten Einstellungen. Das Gerät verwaltet im nichtflüchtigen Speicher maximal 20 Konfigurationsprofile.
  Sie können ein Konfigurationsprofil in den flüchtigen Speicher (*RAM*) laden. Führen Sie dazu die folgenden Schritte aus:
  - ☐ Wählen Sie die Tabellenzeile 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 im Dialog *Grundeinstellungen > Externer Speicher* das Kontrollkästchen *Sichere Konfiguration beim Speichern* markiert ist.

Profilname

Zeigt die Bezeichnung des Konfigurationsprofils.

Mögliche Werte:

- `running-config`
  Bezeichnung des Konfigurationsprofils im flüchtigen Speicher (*RAM*).
- `config`
  Bezeichnung des werksseitig vorhandenen Konfigurationsprofils im nichtflüchtigen Speicher (*NVM*).
- benutzerdefinierter Name
  Das Gerät ermöglicht Ihnen, ein Konfigurationsprofil mit benutzerdefiniertem Namen zu speichern. Wählen Sie dazu die Tabellenzeile 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...*.

Letzte Änderung (UTC)

Zeigt den Zeitpunkt der koordinierten Weltzeit (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 Systemstart oder beim Anwenden der Funktion *Konfigurationsänderungen rückgängig machen* in den flüchtigen Speicher (*RAM*).
  - Wenn Sie die Schaltfläche 💾 klicken, speichert das Gerät die vorläufig angewendeten Einstellungen in diesem Konfigurationsprofil.
- `unmarkiert`
  Ein anderes Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

Verschlüsselung

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.

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.

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.

### Externer Speicher

Ausgewählter externer Speicher

Zeigt den Typ des externen Speichers (*ENVM*).

Mögliche Werte:

- *usb*
  Externer USB-Speicher (ACA21/ACA22)

Status

Zeigt den Betriebszustand des externen Speichers (*ENVM*).

Mögliche Werte:

- *notPresent*
  Kein externer Speicher (*ENVM*) angeschlossen.
- *removed*
  Jemand hat den externen Speicher (*ENVM*) während des Betriebs aus dem Gerät entfernt.
- *ok*
  Der externe Speicher (*ENVM*) ist angeschlossenen und betriebsbereit.
- *outOfMemory*
  Der Speicherplatz im externen Speicher (*ENVM*) ist belegt.
- *genericErr*
  Das Gerät hat einen Fehler erkannt.

### 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 nichtflüchtigen 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 nichtflüchtigen Speicher (*NVM*) ausschließlich dann, wenn dieses unverschlüsselt ist.

Wenn im Dialog *Grundeinstellungen > Externer Speicher* die Spalte *Konfigurations-Priorität* den Wert `erste` 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 Eingeben 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 nichtflüchtigen Speicher (*NVM*) und im externen Speicher (*ENVM*) anzuwenden.

**Anmerkung:**
Wenden Sie diese Funktion ausschließlich dann an, wenn maximal ein Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) des Geräts gespeichert ist. Entscheiden Sie sich vor dem Hinzufügen 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 ersetzen, zum Beispiel weil das Gerät nicht mehr funktioniert, 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 nicht mehr funktionierenden Gerät verwendet haben.

- ☐ Installieren Sie im neuen Gerät den externen Speicher (*ENVM*) aus dem nicht mehr funktionierenden Gerät.
- ☐ Starten Sie das neue Gerät neu.
  Beim nächsten Systemstart lädt das Gerät das Konfigurationsprofil mit den Einstellungen des nicht mehr funktionierenden Geräts vom externen Speicher (*ENVM*). Das Gerät kopiert die Einstellungen in den flüchtigen Speicher (*RAM*) und in den nichtflüchtigen Speicher (*NVM*).

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 nichtflüchtigen Speicher (*NVM*) und im externen Speicher (*ENVM*) 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 nichtflüchtigen 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 nichtflüchtige 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. Die gegenwärtigen Einstellungen, die lediglich zwischengespeichert 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 nichtflüchtigen 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 nichtflüchtigen 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 (*ENVM*) von den Einstellungen des „ausgewählten“ Konfigurationsprofils im nichtflüchtigen 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 (*ENVM*) 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 nichtflüchtigen 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
  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

Das Gerät bietet Ihnen folgende Möglichkeiten, um die Datei auf dem Remote-Server zu sichern:

- Backup über FTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Um die Datei auf einem FTP-Server zu sichern, legen Sie den URL zur Datei in der folgenden Form fest:
  `ftp://<IP-Adresse>[:Port]/<Pfad>/<Dateiname>`
- Backup über TFTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Um die Datei auf einem TFTP-Server zu sichern, legen Sie den URL zur Datei in der folgenden Form fest:
  `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
- Backup über SCP oder SFTP
  Um die Datei auf einem SCP- oder SFTP-Server zu sichern, legen Sie den URL zur Datei in der folgenden Form fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Klicken Sie die Schaltfläche *Start*, um das Fenster *Anmeldeinformationen* zu öffnen.

  Denken Sie daran, den SCP- oder SFTP-Server zunächst als bekannten Host für SSH einzurichten, bevor das Gerät das erste Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit* > SSH Bekannte Hosts.

Zugangsdaten setzen

Öffnet das Fenster *Anmeldeinformationen*, das Ihnen beim Eingeben 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
!#$%&'()*+,-./:;<=>?@[\\]^_`{}~
```

# 1.7 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.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Typ

Zeigt den Typ des externen Speichers (*ENVM*).

Mögliche Werte:

- *usb*
  Externer USB-Speicher (ACA21/ACA22)

Status

Zeigt den Betriebszustand des externen Speichers (*ENVM*).

Mögliche Werte:

- *notPresent*
  Kein externer Speicher (*ENVM*) angeschlossen.
- *removed*
  Jemand hat den externen Speicher (*ENVM*) während des Betriebs aus dem Gerät entfernt.
- *ok*
  Der externe Speicher (*ENVM*) ist angeschlossenen und betriebsbereit.
- *outOfMemory*
  Der Speicherplatz im externen Speicher (*ENVM*) ist belegt.
- *genericErr*
  Das Gerät hat einen Fehler erkannt.

Schreibbar

Zeigt, ob das Gerät Schreibzugriff auf den externen Speicher (*ENVM*) hat.

Mögliche Werte:

- markiert
  Das Gerät hat Schreibzugriff auf den externen Speicher (*ENVM*).
- unmarkiert
  Das Gerät hat ausschließlich Lesezugriff auf den externen Speicher (*ENVM*). Möglicherweise ist für den externen Speicher ein Schreibschutz aktiviert.

### Automatisches Software-Update

Aktiviert/deaktiviert die automatische Aktualisierung der Geräte-Software während des Systemstarts.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Gerät aktualisiert die Geräte-Software, wenn sich folgende Dateien im externen Speicher (*ENVM*) befinden:
  - die Datei des Geräte-Software-Images
  - eine Textdatei `startup.txt` mit dem Inhalt `autoUpdate=<Dateiname_des_Software-Images>.bin`
- `unmarkiert`
  Keine automatische Aktualisierung der Geräte-Software während des Systemstarts.

### SSH-Key automatisch uploaden

Aktiviert/deaktiviert das Laden des RSA-Schlüssels vom externen Speicher (*ENVM*) beim Systemstart.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Laden des RSA-Schlüssels ist aktiviert.
  Beim Systemstart lädt das Gerät den RSA-Schlüssel vom externen Speicher (*ENVM*), 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 nichtflüchtigen Speicher (*NVM*) vorhandenen Schlüssel.

### Konfigurations-Priorität

Legt fest, von welchem Speicher das Gerät beim Neustart das Konfigurationsprofil lädt.

Mögliche Werte:

- *inaktiv*
  Das Gerät lädt das Konfigurationsprofil aus dem nichtflüchtigen Speicher (*NVM*).
- *erste*
  Das Gerät lädt das Konfigurationsprofil vom externen Speicher (*ENVM*).
  Findet das Gerät auf dem externen Speicher (*ENVM*) kein Konfigurationsprofil, lädt es das Konfigurationsprofil aus dem nichtflüchtigen Speicher (*NVM*).

**Anmerkung:**
Beim Laden des Konfigurationsprofils aus dem externen Speicher (*ENVM*) überschreibt das Gerät die Einstellungen des „ausgewählten“ Konfigurationsprofils im nichtflüchtigen Speicher (*NVM*).

Wenn die Spalte *Konfigurations-Priorität* den Wert `erste` 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 Speichern einer Kopie im externen Speicher (*ENVM*).

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Speichern einer Kopie ist aktiviert. Wenn Sie im Dialog *Grundeinstellungen > Laden/Speichern* die Schaltfläche klicken, speichert das Gerät eine Kopie des Konfigurationsprofils auf dem aktiven externen Speicher (*ENVM*).
- `unmarkiert`
  Das Speichern einer Kopie ist deaktiviert. Das Gerät speichert 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.

# 1.8 Port

[ Grundeinstellungen > Port ]

Dieser Dialog ermöglicht Ihnen, Einstellungen für die einzelnen Ports festzulegen. Der Dialog zeigt außerdem Betriebsmodus, Zustand der Verbindung, Bitrate und Duplex-Modus für jeden Port.

Der Dialog enthält die folgenden Registerkarten:
- [Konfiguration]
- [Statistiken]
- [Eingehende Netzlast]

## [Konfiguration]

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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 physisch eingeschaltet oder ausgeschaltet ist.

Mögliche Werte:

- `markiert`
  Der Port ist physisch eingeschaltet.
- `unmarkiert`
  Der Port ist physisch ausgeschaltet.
  Wenn der Port ausgeschaltet ist, obwohl das Kontrollkästchen *Port an* markiert ist, bedeutet dies, dass der Port durch eine andere Funktion ausgeschaltet wurde, zum Beispiel durch *Auto-Disable* oder *Port-Monitor*. Die Einstellungen der Funktion *Auto-Disable* legen Sie im Dialog *Diagnose > Ports > Auto-Disable* fest. Die Einstellungen der Funktion *Port-Monitor* legen Sie im Dialog *Diagnose > Ports > Port-Monitor* fest.

Autoneg.

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 mittels Auto-Negotiation selbständig aus und erkennt die Belegung der Anschlüsse des Twisted-Pair-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*festlegen.
- Ausgegraute Darstellung
  Keine automatische Auswahl des Betriebsmodus.

Manuelle Konfiguration

Legt den Betriebsmodus des Ports fest, wenn die Funktion *Autoneg.* ausgeschaltet ist.

Mögliche Werte:

- `10M HDX`
  Halbduplex-Verbindung
- `10M FDX`
  Vollduplex-Verbindung
- `100M HDX`
  Halbduplex-Verbindung
- `100M FDX`
  Vollduplex-Verbindung
- `1G 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.
- `10M HDX`
  Halbduplex-Verbindung
- `10M FDX`
  Vollduplex-Verbindung
- `100M HDX`
  Halbduplex-Verbindung
- `100M FDX`
  Vollduplex-Verbindung
- `1G 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

Legt die Belegung der Anschlüsse eines Twisted-Pair-Ports fest.

Voraussetzung ist, dass die Funktion *Autoneg.* ausgeschaltet ist.

Mögliche Werte:

- *`mdi`*
  Das Gerät vertauscht das Sende- und Empfangsleitungspaar auf dem Port.
- *`mdix`* (Voreinstellung auf Twisted-Pair-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 über ein gekreuztes Kabel anschließen, stellt das Gerät den Port automatisch von *`mdix`* auf *`mdi`*.
- *`unsupported`* (Voreinstellung auf optischen Ports oder Twisted-Pair-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 Sendeunterbrechungen 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

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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
  Wenn das Gerät eine Link-Status-Änderung erkennt, sendet es einen SNMP-Trap.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

Power-State

Legt fest, ob der Port physisch eingeschaltet oder ausgeschaltet ist, nachdem Sie den Port in der Spalte *Port an* deaktiviert haben.

Mögliche Werte:

- `markiert`
  Das Gerät lässt den Port physisch eingeschaltet, wenn das Kontrollkästchen *Port an* nicht markiert ist. Ein Gerät, das an diesem Port angeschlossen ist, erkennt weiterhin den aktiven Link.
- `unmarkiert` (Voreinstellung)
  Der Port ist physisch ausgeschaltet. Der physische Zustand des Ports wird ausschließlich durch die Einstellung in Spalte *Port an* beeinflusst.

Energie sparen

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.

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*
  - *Unicasts empfangen*
  - *Multicasts empfangen*
  - *Broadcasts empfangen*
- Anzahl der vom Gerät gesendeten oder vermittelten Datenpakete/Bytes
  - *Gesendete Pakete*
  - *Gesendete Oktets*
  - *Unicasts gesendet*
  - *Multicasts gesendet*
  - *Broadcasts gesendet*
- 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 > Restart* die Schaltfläche *Port-Statistiken leeren*.

## [Eingehende Netzlast]

Diese Registerkarte zeigt die Eingangsnetzlast auf den einzelnen Ports.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des Ports.

Netzlast [%]

Zeigt die gegenwärtige Netzlast in Prozent, bezogen auf den in Spalte *Kontroll-Intervall [s]* festgelegten Zeitabstand.

Die Auslastung ist das Verhältnis zwischen der empfangenen Datenmenge und der maximal möglichen Datenmenge bei der gegenwärtig eingestellten Datenrate.

Unterer Schwellenwert [%]

Legt den unteren Schwellenwert für die Benachrichtigung bezüglich der Netzlast fest. Wenn die Netzlast auf dem Port diesen Wert unterschreitet, dann ändert sich der Status des Kontrollkästchens in Spalte *Alarm* auf `markiert`.

Mögliche Werte:

- `0.00..100.00` (Voreinstellung: `0.00`)

Der Wert `0` oder `0.00` deaktiviert den unteren Schwellenwert für die Benachrichtigung.

Oberer Schwellenwert [%]

Legt den oberen Schwellenwert für die Benachrichtigung bezüglich der Netzlast fest. Wenn die Netzlast auf dem Port diesen Wert überschreitet, dann ändert sich der Status des Kontrollkästchens in Spalte *Alarm* auf `markiert`.

Mögliche Werte:

- `0.00..100.00` (Voreinstellung: `0.00`)

Der Wert `0` oder `0.00` deaktiviert den oberen Schwellenwert für die Benachrichtigung.

Kontroll-Intervall [s]

Legt die Zeitspanne in Sekunden fest, innerhalb der das Gerät die Netzlast ermittelt und gegebenenfalls begrenzt.

Mögliche Werte:

- `1..3600` (Voreinstellung: `30`)

Alarm

Kennzeichnet den Alarmzustand für die Netzlast.

Mögliche Werte:

- `markiert`
  Die Netzlast auf dem Port liegt unter dem in Spalte *Unterer Schwellenwert [%]* oder über dem in Spalte *Oberer Schwellenwert [%]* festgelegten Wert. Das Gerät sendet einen SNMP-Trap. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
- `unmarkiert`
  Die Netzlast auf dem Port liegt zwischen dem unteren und oberen Schwellenwert für die Benachrichtigung.

## 1.9 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 von den angeschlossenen Geräten angeforderte Leistungen die verfügbare Leistung überschreitet, geht das Gerät beim Abschalten der für die Ports bereitgestellten Leistungen nach der eingerichteten Priorität vor. Beim Abschalten der für die Ports bereitgestellten Leistung beginnt das Gerät mit den Ports, für die Sie eine niedrige Priorität eingerichtet haben. Wenn mehrere Ports die selbe Priorität haben, schaltet das Gerät die Leistung an den Ports mit den höchsten Nummern zuerst ab.

Das Menü enthält die folgenden Dialoge:

- PoE Global
- PoE Port

# 1.9.1 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 Schwellenwert 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.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Modul

Gerätemodule, auf die sich die Tabellenzeilen beziehen.

Budget konfigurierte Leistung [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 *Budget max. Leistung [W]*.

Budget max. Leistung [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

Schwellenwert [%]

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

Mögliche Werte:

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

Trap senden

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

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv. Voraussetzung ist, dass im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
  Wenn der Stromverbrauch des Moduls den benutzerdefinierten Schwellenwert überschreitet, sendet das Gerät einen SNMP-Trap.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

## 1.9.2 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 gespeiste Geräte für einen festgelegten Zeitraum aus.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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 im 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 gespeisten Geräte.

Mögliche Werte:

- `ausgeschaltet`
  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`
  Das Gerät im befindet sich im Zustand *TEST ERROR*.
- `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:

- `class0`
- `class1`
- `class2`
- `class3`
- `class4`

class0
class1
class2
class3
class4

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..30`

Verbrauch [mA]

Zeigt den am Port abgegebenen Strom in Milliampere.

Mögliche Werte:

- `0..600`

Limit Leistung [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..30` (Voreinstellung: `0`)
  Sie können den Wert in Schritten von 0,1 W festlegen.

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`)

## 1.10 Restart

[ Grundeinstellungen > Restart ]

Dieser Dialog ermöglicht Ihnen, das Gerät neu zu starten, Port-Zähler und die MAC-Adresstabelle (Forwarding Database) zurückzusetzen sowie Log-Dateien zu löschen.

## Restart

Kaltstart...

Öffnet das Fenster *Restart*, um einen sofortigen oder einen verzögerten Neustart des Geräts auszulösen.

Wenn sich das Konfigurationsprofil im flüchtigen Speicher (*RAM*) und das „ausgewählte“ Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) unterscheiden, zeigt das Gerät das Fenster *Warnung*.

- ☐ Um die Einstellungen dauerhaft zu speichern, klicken Sie im Fenster *Warnung* die Schaltfläche *Ja*.
- ☐ Um die geänderten Einstellungen zu verwerfen, klicken Sie im Fenster *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 den RAM-Selbsttest 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.

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.

## Schaltflächen

FDB leeren

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 leeren

Entfernt aus der ARP-Tabelle die dynamisch eingerichteten Adressen.

Siehe Dialog *Diagnose > System > ARP*.

Port-Statistiken leeren

Setzt die Zähler der Portstatistik auf `0`.

Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Statistiken*.

IGMP-Snooping Daten leeren

Entfernt die IGMP-Snooping-Einträge und setzt den Zähler im Rahmen *Information* auf `0`.

Siehe Dialog *Switching > IGMP-Snooping > Global*.

Log-Datei leeren

Entfernt die protokollierten Einträge aus der Log-Datei.

Siehe Dialog *Diagnose > Bericht > System-Log*.

Persistente Log-Datei leeren

Entfernt die Log-Dateien vom externen Speicher (*ENVM*).

Siehe Dialog *Diagnose > Bericht > Persistentes Ereignisprotokoll*.

# 2 Zeit

Das Menü enthält die folgenden Dialoge:
- Grundeinstellungen
- SNTP

## 2.1 Grundeinstellungen

[ Zeit > Grundeinstellungen ]

Das Gerät ist mit einer gepufferten Hardware-Uhr ausgestattet. Diese Uhr behält die korrekte Zeit bei, wenn die Stromversorgung ausfällt oder Sie das Gerät vom Stromnetz trennen. Nach dem Systemstart steht die korrekte Uhrzeit wieder 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]

**Anmerkung:**
Das Anzeigeformat für Datums- und Zeitangaben wird durch die Sprache der grafischen Benutzeroberfläche bestimmt. Sie können die Sprache umschalten, siehe „Sprachumschaltung” auf Seite 11.

### [Global]

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

#### Konfiguration

Systemzeit (UTC)

Zeigt Datum und Uhrzeit als Koordinierte Weltzeit (UTC), das heißt, ohne den im Feld *Lokaler Offset [min]* festgelegten Wert.

Setze Zeit vom PC

Das Gerät übernimmt die Uhrzeit Ihrer Management-Station als Systemzeit.

Systemzeit

Zeigt den Tag und die Ortszeit: *Systemzeit* = *Systemzeit (UTC)* + *Lokaler Offset [min]* + *Sommerzeit*

Zeitquelle

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 eingeschaltet und das Gerät ist durch einen *SNTP*-Server synchronisiert.
  Siehe Dialog *Zeit > SNTP*.

Lokaler Offset [min]

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

Mögliche Werte:

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

## [Sommerzeit]

In dieser Registerkarte schalten Sie die Funktion *Sommerzeit* ein/aus. Beginn und Ende der Sommerzeit wählen Sie anhand eines vordefinierten Profils aus. Alternativ dazu legen Sie diese Einstellungen individuell fest. Während der Sommerzeit stellt das Gerät die Ortszeit um eine Stunde vor.

### Funktion

Sommerzeit

Schaltet den *Sommerzeit*-Modus ein/aus.

Mögliche Werte:

- *An*
  Die *Sommerzeit*-Modus ist eingeschaltet.
  Das Gerät stellt die Uhr automatisch auf Sommerzeit und wieder zurück.
- *Aus* (Voreinstellung)
  Die *Sommerzeit*-Modus ist ausgeschaltet.

Die Sommerzeit-Einstellungen legen Sie in den Rahmen *Sommerzeit Beginn* und *Sommerzeit Ende* fest.

Profil...

Öffnet das Fenster *Profil...*, um ein vordefiniertes Profil für Beginn und Ende der Sommerzeit auszuwählen. Das Auswählen eines Profils überschreibt die in den Rahmen *Sommerzeit Beginn* und *Sommerzeit Ende* festgelegten Einstellungen.

Mögliche Werte:

- *EU*
  Sommerzeit-Einstellungen, die in der Europäischen Union gelten.
- *USA*
  Sommerzeit-Einstellungen, die in den Vereinigen Staaten gelten.

### Sommerzeit Beginn

In diesem Rahmen legen Sie den Zeitpunkt fest, zu dem das Gerät die Uhr von Normalzeit auf Sommerzeit vorstellt. In den ersten 3 Feldern legen Sie den Tag für den Beginn der Sommerzeit fest. Im letzten Feld legen Sie den Zeitpunkt fest.

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 den Zeitpunkt fest, zu dem das Gerät die Uhr auf Sommerzeit vorstellt.

Mögliche Werte:

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

### Sommerzeit Ende

In diesem Rahmen legen Sie den Zeitpunkt fest, zu dem das Gerät die Uhr von Sommerzeit auf Normalzeit zurückstellt. In den ersten 3 Feldern legen Sie den Tag für das Ende der Sommerzeit fest. Im letzten Feld legen Sie den Zeitpunkt fest.

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 den Zeitpunkt fest, zu dem das Gerät die Uhr auf Normalzeit zurückstellt.

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.

Mittels SNTP-Client-Funktion ermöglicht Ihnen das Gerät, die lokale Systemuhr mit einem externen NTP- oder SNTP-Server zu synchronisieren.

Als SNTP-Server stellt das Gerät die Zeitinformation anderen Geräten im Netz 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 Zeitinformationen von einem externen NTP- oder SNTP-Server und stimmt die lokale Systemuhr auf die Zeit des Zeit-Servers ab.

### Funktion

Funktion

Schaltet die Funktion *Client* im Gerät ein/aus. Beachten Sie die Einstellung des Kontrollkästchens *Deaktiviere Client nach erfolgreicher Synchronisierung* im Rahmen *Konfiguration*.

Mögliche Werte:

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

### Zustand

Zustand

Zeigt den Zustand der *Client*-Funktion.

Mögliche Werte:

- *ausgeschaltet*
  Der SNTP-Client ist nicht in Betrieb.
- *notSynchronized*
  Der SNTP-Client ist in Betrieb.
  Die lokale Systemuhr ist nicht auf einen externen NTP- oder SNTP-Server abgestimmt.
- *synchronizedToRemoteServer*
  Der SNTP-Client ist in Betrieb.
  Die lokale Systemuhr ist auf einen externen NTP- oder SNTP-Server abgestimmt.

## Konfiguration

Modus

Legt fest, ob das Gerät die Zeitinformationen von einem im Gerät eingerichteten externen NTP- oder SNTP-Server aktiv anfordert (Modus *unicast*) oder auf die Zeitinformationen von einem beliebigen NTP- oder SNTP-Server passiv wartet (Modus *broadcast*).

Mögliche Werte:

- *unicast* (Voreinstellung)
  Das Gerät bezieht die Zeitinformationen ausschließlich von einem der eingerichteten NTP- oder SNTP-Server. Das Gerät sendet Unicast-Anfragen an den externen SNTP- oder NTP-Server und wertet die Antwort des Servers aus.
- *broadcast*
  Das Gerät bezieht die Zeitinformationen von einem beliebigen NTP- oder SNTP-Server. Das Gerät wertet die Broadcasts oder Multicasts von diesem Server aus.

Request-Intervall [s]

Legt das Intervall in Sekunden fest, in dem das Gerät Zeitinformationen von einem externen NTP- oder SNTP-Server anfordert.

Mögliche Werte:

- `5..3600` (Voreinstellung: `30`)

Broadcast-Recv Timeout [s]

Legt die Zeit in Sekunden fest, die das Gerät im Modus *broadcast* wartet, bevor es im Feld *Zustand* den Wert von *syncToRemoteServer* auf *notSynchronized* ändert, wenn es keine Broadcast-Pakete empfängt. Siehe Rahmen *Zustand*.

Mögliche Werte:

- `128..2048` (Voreinstellung: `320`)

Deaktiviere Client nach erfolgreicher Synchronisierung

Aktiviert/deaktiviert das automatische Ausschalten der *SNTP Client*-Funktion, nachdem das Gerät seine lokale Systemuhr erfolgreich abgestimmt hat.

Mögliche Werte:

- `markiert`
  Das automatische Ausschalten der *SNTP Client*-Funktion ist aktiv.
  Das Gerät schaltet die *SNTP Client*-Funktion aus, nachdem es seine lokale Systemuhr erfolgreich abgestimmt hat.
- `unmarkiert` (Voreinstellung)
  Das automatische Ausschalten der *SNTP Client*-Funktion ist inaktiv.
  Das Gerät lässt die *SNTP Client*-Funktion eingeschaltet, nachdem es seine lokale Systemuhr erfolgreich abgestimmt hat.

### Tabelle

In der Tabelle können Sie die Einstellungen für bis zu 4 externe NTP- oder SNTP-Server festlegen. Nach Einschalten der Funktion sendet das Gerät Anfragen an den in der ersten Tabellenzeile eingerichteten Server.

Wenn der externe NTP- oder SNTP-Server nicht antwortet, sendet das Gerät seine Anfrage an den in der nächsten Tabellenzeile eingerichteten Server. Wenn das Gerät keine Antwort empfängt, sendet es zyklisch Anfragen an jeden eingerichteten NTP- oder SNTP-Server, bis es eine gültige Zeit von einem dieser Server erhält. Das Gerät stimmt seine lokale Systemuhr auf den ersten antwortenden NTP- oder SNTP-Server ab, auch wenn ein in der Tabelle weiter oben stehender Server später wieder erreichbar ist.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Fügt eine Tabellenzeile hinzu.

Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht.

Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen. Wenn Sie eine Tabellenzeile löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie eine Tabellenzeile hinzufügen, schließt das Gerät die erste Lücke.

Name

Legt einen Namen für den externen NTP- oder SNTP-Server fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

IP-Adresse

Legt die IP-Adresse des externen NTP- oder SNTP-Servers fest.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)
- Gültige IPv6-Adresse

Ziel UDP-Port

Legt den UDP-Port fest, auf dem der externe NTP- oder SNTP-Server auf Anfragen wartet.

Mögliche Werte:

- `1..65535 (2¹⁶-1)` (Voreinstellung: `123`)

Status

Zeigt den Zustand der Verbindung zwischen dem Gerät und dem externen NTP- oder SNTP-Server.

Mögliche Werte:

- *erfolgreich*
  Das Gerät hat die lokale Systemuhr erfolgreich auf den externen NTP- oder SNTP-Server abgestimmt.
- *badDateEncoded*
  Die Synchronisierung war nicht erfolgreich. Die empfangene Zeitinformation enthält Protokollfehler.
- *other*
  Die Synchronisierung war nicht erfolgreich.
  - Für den externen NTP- oder SNTP-Server ist die IP-Adresse `0.0.0.0` festgelegt.
    oder
  - Das Gerät verwendet einen anderen externen NTP- oder SNTP-Server.
- *requestTimedOut*
  Die Synchronisierung war nicht erfolgreich. Das Gerät hat keine Antwort vom externen NTP- oder SNTP-Server erhalten.
- *serverKissOfDeath*
  Die Synchronisierung war nicht erfolgreich. Der externe NTP- oder SNTP-Server ist überlastet. Das Gerät ist aufgefordert, seine Systemuhr auf einen anderen NTP- oder SNTP-Server abzustimmen. Steht kein anderer NTP- oder SNTP-Server zur Verfügung, prüft das Gerät in Abständen, die größer sind als der Wert im Feld *Request-Intervall [s]*, ob der Server noch überlastet ist.
- *serverUnsychronized*
  Die Synchronisierung war nicht erfolgreich. Der externe NTP- oder SNTP-Server ist nicht auf eine Referenzzeitquelle abgestimmt.
- *versionNotSupported*
  Die Synchronisierung war nicht erfolgreich. Die SNTP-Versionen des Clients und des Servers sind nicht kompatibel.

Aktiv

Aktiviert/deaktiviert die Verbindung zum externen NTP- oder SNTP-Server.

Mögliche Werte:

- `markiert`
  Die Verbindung zum externen NTP- oder SNTP-Server ist aktiviert.
  Das Gerät hat die Möglichkeit, auf den Server zuzugreifen.
- `unmarkiert` (Voreinstellung)
  Die Verbindung zum externen NTP- oder SNTP-Server ist deaktiviert.
  Das Gerät hat nicht die Möglichkeit, auf den Server zuzugreifen.

## 2.2.2 SNTP Server

[Zeit > SNTP > Server]

In diesem Dialog legen Sie die Einstellungen fest, mit denen das Gerät als SNTP-Server arbeitet. Als SNTP-Server stellt das Gerät die Zeitinformation anderen Geräten im Netz zur Verfügung. Das Gerät stellt die koordinierte Weltzeit (UTC) ohne Berücksichtigung lokaler Zeitunterschiede zur Verfügung.

Bei entsprechender Einstellung arbeitet der SNTP-Server des Geräts im Broadcast-Modus. Im Broadcast-Modus stellt das Gerät die Zeitinformationen anderen Geräten im Netz durch Senden von Broadcasts oder Multicasts zur Verfügung.

### Funktion

Funktion

Schaltet die Funktion *Server* im Gerät ein/aus. Beachten Sie die Einstellung des Kontrollkästchens *Server deaktivieren bei lokaler Zeitquelle* im Rahmen *Konfiguration*.

Mögliche Werte:

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

### Zustand

Zustand

Zeigt den Zustand der Funktion *Server* im Gerät.

Mögliche Werte:

- *ausgeschaltet*
  Der SNTP-Server ist nicht in Betrieb.
- *notSynchronized*
  Der SNTP-Server ist in Betrieb.
  Die lokale Systemuhr ist nicht auf eine Referenzzeitquelle abgestimmt.
- *syncToLocal*
  Der SNTP-Server ist in Betrieb.
  Die lokale Systemuhr ist auf die Hardware-Uhr des Geräts abgestimmt.
- *syncToRefclock*
  Der SNTP-Server ist in Betrieb.
  Die lokale Systemuhr ist auf eine externe Referenzzeitquelle abgestimmt.
- *syncToRemoteServer*
  Der SNTP-Server ist in Betrieb.
  Die lokale Systemuhr ist auf einen externen NTP- oder SNTP-Server abgestimmt, der in einer Kaskade dem Gerät übergeordnet ist.

### Konfiguration

UDP-Port

Legt den UDP-Port fest, auf dem das Gerät Anfragen erwartet.

Mögliche Werte:

- `1..65535 (2¹⁶-1)` (Voreinstellung: `123`)

Broadcast Admin-Modus

Aktiviert/deaktiviert den Broadcast-Modus.

Mögliche Werte:

- `markiert`
  Das Gerät sendet SNTP-Pakete als Broadcasts oder Multicasts.
  Das Gerät antwortet außerdem auf SNTP-Anfragen im Unicast-Modus.
- `unmarkiert` (Voreinstellung)
  Das Gerät antwortet auf SNTP-Anfragen im Unicast-Modus, sendet jedoch selbst keine Broadcast-Pakete.

Broadcast Ziel-Adresse

Legt die Ziel-IP-Adresse fest, an die das Gerät im Broadcast-Modus die SNTP-Pakete sendet.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)
  Broadcast- und Multicast-Adressen sind zulässig.

Broadcast UDP-Port

Legt den UDP-Port fest, über den das Gerät im Broadcast-Modus die SNTP-Pakete sendet.

Mögliche Werte:

- `1..65535 (2¹⁶-1)` (Voreinstellung: `123`)

Broadcast VLAN-ID

Legt das VLAN fest, an welches das Gerät im Broadcast-Modus die SNTP-Pakete sendet.

Mögliche Werte:

- `0`
  Das Gerät sendet die SNTP-Pakete in demselben VLAN, in dem auch der Zugriff auf das Management des Geräts erfolgt. Siehe Dialog *Grundeinstellungen > Netzwerk > Global*.
- `1..4042` (Voreinstellung: `1`)

Broadcast Sende-Intervall [s]

Legt das Intervall in Sekunden fest, in dem das Gerät SNTP-Pakete sendet.

Mögliche Werte:

- `64..1024` (Voreinstellung: `128`)

Server deaktivieren bei lokaler Zeitquelle

Aktiviert/deaktiviert das Ausschalten der *SNTP Server*-Funktion, wenn die lokale Systemuhr nicht auf eine andere externe Zeitreferenz abgestimmt ist.

Mögliche Werte:

- `markiert`
  Das automatische Ausschalten der *SNTP Server*-Funktion ist aktiv.
  Wenn das Gerät seine lokale Systemuhr auf eine externe Zeitreferenz abgestimmt hat, dann lässt es die *SNTP Server*-Funktion eingeschaltet. Andernfalls schaltet das Gerät die *SNTP Server*-Funktion aus.
- `unmarkiert` (Voreinstellung)
  Das automatische Ausschalten der *SNTP Server*-Funktion ist inaktiv.
  Das Gerät lässt die *SNTP Server*-Funktion eingeschaltet, unabhängig davon, ob es seine lokale Systemuhr auf eine externe Zeitreferenz abgestimmt hat.
  Wenn die lokale Systemuhr nicht mit einer externen Zeitreferenz synchronisiert ist, dann informiert das Gerät den Client im SNTP-Paket darüber, dass seine Systemuhr lokal abgestimmt ist.

# 3 Gerätesicherheit

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

## 3.1 Benutzerverwaltung

[ Gerätesicherheit > Benutzerverwaltung ]

Das Gerät ermöglicht Benutzern den Zugriff auf sein Management, wenn diese sich mit gültigen Zugangsdaten anmelden.

In diesem Dialog verwalten Sie die Benutzer der lokalen Benutzerverwaltung. Außerdem legen Sie hier die folgenden Einstellungen fest:
- Einstellungen für das Login
- Einstellungen für das Speichern der Passwörter
- Passwortrichtlinien-Einstellungen für gültige Passwörter

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 aufeinanderfolgenden erfolglosen 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 Command Line Interface über die serielle Verbindung ist die Anzahl erfolgloser Login-Versuche unbegrenzt.

Mögliche Werte:

▶ `0..5` (Voreinstellung: `0`)

Wenn sich der Benutzer nacheinander ein weiteres Mal erfolglos 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 beim Management des Geräts anzumelden.

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`)

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`)

Benutzer automatisch entsperren

Aktiviert/deaktiviert die automatische Entsperrung von Benutzerkonten, die das Gerät aufgrund der festgelegten Anzahl aufeinanderfolgender fehlgeschlagener Anmeldeversuche gesperrt hat. Siehe Feld *Login-Versuche* im Rahmen *Konfiguration*.

Mögliche Werte:

- `markiert`
  Die Entsperrung der Benutzerkonten ist aktiviert. Das Gerät entsperrt ein gesperrtes Benutzerkonto nach Ablauf der in Spalte *Timer für automatische Entsperrung [min]* festgelegten Zeit.
- `unmarkiert` (Voreinstellung)
  Die Entsperrung der Benutzerkonten ist deaktiviert. Ein gesperrtes Benutzerkonto bleibt gesperrt, bis ein Administrator es entsperrt.

### Passwort-Richtlinien

Dieser Rahmen ermöglicht Ihnen, Richtlinien für gültige Passwörter festzulegen. Das Gerät verwendet diese Richtlinie zur Überprüfung eines neuen oder geänderten Passworts, sofern die Passwortrichtlinienprüfung für das jeweilige Passwort aktiviert ist.

Die Einstellungen wirken sich auf die Passwörter in Spalte *Passwort* aus, sofern das entsprechende Kontrollkästchen in Spalte *Richtlinien überprüfen* aktiviert 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.

**Anmerkung:**
Zulässige Sonderzeichen sind: `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`

### 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 16.

Schaltflächen

 Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Benutzername* legen Sie die Bezeichnung des Benutzerkontos fest.
  Mögliche Werte:
  ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

 Löschen

Entfernt die ausgewählte Tabellenzeile.

Benutzername

Zeigt die Bezeichnung des Benutzerkontos.

Um ein Benutzerkonto hinzuzufügen, klicken Sie die Schaltfläche  .

Aktiv

Aktiviert/deaktiviert das Benutzerkonto.

Mögliche Werte:

▶ `markiert`
Das Benutzerkonto ist aktiv. Das Gerät akzeptiert die Anmeldung eines Benutzers am Management des Geräts mit diesem Benutzernamen.

▶ `unmarkiert` (Voreinstellung)
Das Benutzerkonto ist inaktiv. Das Gerät verweigert die Anmeldung eines Benutzers am Management des Geräts mit diesem Benutzernamen.

Wenn ausschließlich 1 Benutzerkonto mit der Zugriffsrolle *`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. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Um den *Passwort*-Wert zu ändern, klicken Sie das entsprechende Feld. Das Gerät öffnet einen Dialog zum Eingeben/Ändern des Passworts, siehe „Dialog zur Eingabe/Änderung des Passworts” auf Seite 96.

Wenn Sie das Passwort zum ersten Mal festlegen, verwendet das Gerät dasselbe Passwort auch in den Spalten *Passwort SNMP-Authentifizierung* und *Passwort SNMP-Verschlüsselung*.

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

Mögliche Werte:

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

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. Dazu verwendet das Gerät einen Dialog zur Änderung/Eingabe des Passworts, siehe „Dialog zur Eingabe/Änderung des Passworts" auf Seite 96.

Das Gerät überprüft stets die Mindestlänge des Passworts, auch wenn das Kontrollkästchen in Spalte *Richtlinien überprüfen*`nicht markiert` ist. Die erforderliche Mindestlänge des Passworts legen Sie im Rahmen *Konfiguration* fest.

Rolle

Legt die Zugriffsrolle fest, die den Zugriff des Benutzers auf die einzelnen Funktionen des Geräts steuert.

Mögliche Werte:

- *unauthorized*
  Der Benutzer ist gesperrt, das Gerät verweigert die Anmeldung des Benutzers beim Management des Geräts.
  Weisen Sie diesen Wert zu, um das Benutzerkonto vorübergehend zu sperren. Wenn beim Zuweisen einer anderen Zugriffsrolle ein Fehler auftritt, dann weist das Gerät dem Benutzerkonto diese Zugriffsrolle 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 Zugriffsrolle 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 nacheinander erfolglos versucht, sich anzumelden.
- `unmarkiert` (ausgegraut) (Voreinstellung)
  Das Benutzerkonto ist entsperrt. Der Benutzer hat Zugriff auf das Management des Geräts.

Timer für automatische Entsperrung [min]

Legt die Zeit in Minuten fest, nach deren Ablauf das Gerät ein gesperrtes Benutzerkonto entsperrt. Diese Einstellung ist ausschließlich wirksam, wenn das Kontrollkästchen *Benutzer automatisch entsperren* im Rahmen *Konfiguration* markiert ist.

Der Timer startet, sobald das Gerät das Konto aufgrund der festgelegten Anzahl aufeinanderfolgender fehlgeschlagener Anmeldeversuche sperrt. Siehe Feld *Login-Versuche* im Rahmen *Konfiguration*.

Mögliche Werte:

- `1..720` (Voreinstellung: `30`)

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.

**Anmerkung:**
Das Gerät überprüft stets die Mindestlänge des Passworts, auch wenn das Kontrollkästchen in Spalte *Richtlinien überprüfen*`nicht markiert` ist.

SNMP-Authentifizierung

Legt den Algorithmus fest, den das Gerät für die Authentifizierung des gewählten SNMPv3-Benutzers anwendet.

Mögliche Werte:

- *`hmacmd5`* (Voreinstellung)
  MD5
- *`hmacsha`*
  SHA-1
- *`hmacsha256`*
  SHA-256

Passwort SNMP-Authentifizierung

Legt das Passwort fest, welches das Gerät beim Zugriff des Benutzers mittels SNMPv3 anwendet. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Um den *Passwort SNMP-Authentifizierung*-Wert zu ändern, klicken Sie das entsprechende Feld. Das Gerät öffnet einen Dialog zum Eingeben/Ändern des Passworts, siehe „Dialog zur Eingabe/Änderung des Passworts" auf Seite 96.

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

- Für die gegenwärtige Spalte ermöglicht 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 den Algorithmus fest, den das Gerät anwendet, um SNMPv3-Nachrichten des ausgewählten SNMPv3-Benutzers zu verschlüsseln.

Mögliche Werte:

- *kein*
  Keine Verschlüsselung.
- *des* (Voreinstellung)
  DES
- *aesCfb128*
  AES-128
- *aesCfb256*
  AES-256

Passwort SNMP-Verschlüsselung

Legt das Passwort fest, welches das Gerät zur Verschlüsselung beim Zugriff des Benutzers mittels SNMPv3 anwendet. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Um den *Passwort SNMP-Verschlüsselung*-Wert zu ändern, klicken Sie das entsprechende Feld. Das Gerät öffnet einen Dialog zum Eingeben/Ändern des Passworts, siehe „Dialog zur Eingabe/Änderung des Passworts" auf Seite 96.

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

- Für die gegenwärtige Spalte ermöglicht 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
- !#$%&'()*+,-./:;<=>?@[\]^_`{}~

### Dialog zur Eingabe/Änderung des Passworts

Wenn Sie ein Passwortfeld klicken, zeigt das Gerät einen Dialog zur Passwortänderung. In diesem Dialog können Sie ein gültiges Passwort festlegen, indem er Ihnen die erforderlichen Passwortkriterien zeigt. Der Dialog gibt Ihnen Rückmeldung darüber, welche Kriterien das aktuell eingegebene Passwort erfüllt.

- Der Dialog prüft, ob das eingegebene Passwort die erforderliche Passwortlänge erfüllt.
  - Diese Überprüfung ist stets aktiv.
- Der Dialog prüft, ob das eingegebene Passwort der Passwortrichtlinie entspricht.
  - Diese Überprüfung ist ausschließlich dann aktiv, wenn Sie das Kontrollkästchen *Richtlinien überprüfen* für das entsprechende Passwortfeld aktiviert haben.
- Der Dialog überprüft, ob das eingegebene Passwort nur zulässige Zeichen enthält.
  - Diese Überprüfung ist stets aktiv.
- Der Dialog hilft, Tippfehler beim Passwort zu vermeiden, indem er Sie auffordert, das Passwort zweimal einzugeben.
  - Diese Überprüfung ist stets aktiv.

Passwortlänge (min.):

Dieses Dialogelement zeigt die erforderliche Mindestlänge des Passworts.

- Wenn das aktuell eingegebene Passwort die erforderliche Mindestlänge erfüllt:
  - Das Gerät zeigt links neben dem Text *Passwortlänge (min.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Passwortlänge (min.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

**Anmerkung:**
Diese Überprüfung ist stets aktiv.

Passwortlänge (max.):

Dieses Dialogelement zeigt die erforderliche Maximallänge des Passworts.

- Wenn das Passwort die erforderliche Maximallänge erfüllt:
  - Das Gerät zeigt links neben dem Text *Passwortlänge (max.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Passwortlänge (max.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

**Anmerkung:**
Diese Überprüfung ist stets aktiv.

Großbuchstaben (min.):

Dieses Dialogfeld zeigt die erforderliche Mindestanzahl an Großbuchstaben im Passwort.

- Wenn das Passwort die erforderliche Mindestanzahl an Großbuchstaben enthält:
  - Das Gerät zeigt links neben dem Text *Großbuchstaben (min.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Großbuchstaben (min.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

**Anmerkung:**
Diese Überprüfung ist ausschließlich dann aktiv, wenn Sie das Kontrollkästchen *Richtlinien überprüfen* für das entsprechende Passwortfeld aktiviert haben.

Kleinbuchstaben (min.):

Dieses Dialogfeld zeigt die erforderliche Mindestanzahl an Kleinbuchstaben im Passwort.

- Wenn das Passwort die erforderliche Mindestanzahl an Kleinbuchstaben enthält:
  - Das Gerät zeigt links neben dem Text *Kleinbuchstaben (min.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Kleinbuchstaben (min.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

**Anmerkung:**
Diese Überprüfung ist ausschließlich dann aktiv, wenn Sie das Kontrollkästchen *Richtlinien überprüfen* für das entsprechende Passwortfeld aktiviert haben.

Ziffern (min.):

Dieses Dialogfeld zeigt die erforderliche Mindestanzahl an Ziffern im Passwort.

- Wenn das Passwort die erforderliche Mindestanzahl an Ziffern enthält:
  - Das Gerät zeigt links neben dem Text *Ziffern (min.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Ziffern (min.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

**Anmerkung:**
Diese Überprüfung ist ausschließlich dann aktiv, wenn Sie das Kontrollkästchen *Richtlinien überprüfen* für das entsprechende Passwortfeld aktiviert haben.

Sonderzeichen (min.):

Dieses Dialogfeld zeigt die erforderliche Mindestanzahl an Sonderzeichen im Passwort.

- Wenn das Passwort die erforderliche Mindestanzahl an Sonderzeichen enthält:
  - Das Gerät zeigt links neben dem Text *Sonderzeichen (min.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Sonderzeichen (min.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

**Anmerkung:**
Zulässige Sonderzeichen sind: `!#$%&'()*+,-./:;<=>?@[\]^_`{}~`
Diese Überprüfung ist ausschließlich dann aktiv, wenn Sie das Kontrollkästchen *Richtlinien überprüfen* für das entsprechende Passwortfeld aktiviert haben.

Enthält nur erlaubte Zeichen

Dieses Dialogelement zeigt, ob das Passwort nur zulässige Zeichen enthält:

- Falls ja:
  - Das Gerät zeigt links neben dem Text *Enthält nur erlaubte Zeichen* ein grünes Häkchen
  - Das Gerät zeigt den Text *Enthält nur erlaubte Zeichen* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Neues Passwort

Geben Sie hier das neue oder geänderte Passwort ein. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Das in diesem Feld eingegebene Passwort muss mit dem Wert im Feld *Passwort bestätigen* übereinstimmen.

Passwort bestätigen

Bestätigt das neue oder geänderte Passwort. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Das in diesem Feld eingegebene Passwort muss mit dem Wert im Feld *Neues Passwort* übereinstimmen.

Ok

Das Klicken dieser Schaltfläche schließt den Dialog und übernimmt das Passwort in das Passwortfeld des darunterliegenden Dialogs, vorausgesetzt:

- Das aktuell eingegebene Passwort erfüllt alle erforderlichen Kriterien.
- Der *Passwort bestätigen*-Wert stimmt mit dem *Neues Passwort*-Wert überein.

Abbrechen

Das Klicken dieser Schaltfläche bricht den Dialog ab und lässt das Passwort im darunterliegenden Dialog unverändert.

# 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
- 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 16.

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

Schaltflächen

 Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Name* legen Sie den Namen der Liste fest.
  Mögliche Werte:
  ▶ Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Löschen

Entfernt die ausgewählte Tabellenzeile.

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 Liste hinzuzufügen, 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 erfolglos ist.

Mögliche Werte:

- *`lokal`* (Voreinstellung)
  Das Gerät authentifiziert die Benutzer mittels lokaler 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 Anmeldung des Benutzers beim Management des Geräts oder lehnt die Anmeldung 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 beim Management des Geräts 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 beim Management des Geräts anzumelden.

- Wenn die erste Richtlinie in der Authentifizierungsliste *radius* ist und das Gerät die Anmeldung ablehnt, wird die Anmeldung sofort verweigert, ohne dass das Gerät versucht, den Benutzer über eine andere Richtlinie anzumelden.
  Bleibt die Antwort des RADIUS-Servers aus, versucht das Gerät die Authentifizierung des Benutzers mit der nächsten Richtlinie.
- Wenn die erste Richtlinie in der Authentifizierungsliste *reject* ist, lehnen die Geräte die Benutzeranmeldung sofort ab, ohne eine andere Richtlinie anzuwenden.
- Vergewissern Sie sich, dass die Authentifizierungsliste `defaultV24AuthList` mindestens eine Richtlinie enthält, die vom Wert *reject* abweicht.

▶ *ias*
Das Gerät authentifiziert die sich mittels 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 > IAS*.
Der Authentifizierungliste `defaultDot1x8021AuthList` können Sie ausschließlich diesen Wert zuweisen.

### Zugeordnete Anwendungen

Zeigt die zugeordneten Anwendungen. Wenn Benutzer mit der betreffenden Anwendung auf das Gerät zugreifen, wendet das Gerät die festgelegten Richtlinien für die Authentifizierung an.

Um der Liste eine andere Anwendung zuzuordnen oder die Zuordnung aufzuheben, klicken Sie die Schaltfläche . Das Gerät ermöglicht Ihnen, jede Anwendung genau einer Liste zuzuordnen.

### Aktiv

Aktiviert/deaktiviert die Liste.

Mögliche Werte:

▶ `markiert` (Voreinstellung)
Die Liste ist aktiviert. Das Gerät wendet die Richtlinien dieser Liste an, wenn Benutzer mit der betreffenden Anwendung auf das Gerät zugreifen.

▶ `unmarkiert`
Die Liste ist deaktiviert.

# 3.3 Management-Zugriff

[ Gerätesicherheit > Management-Zugriff ]

Das Menü enthält die folgenden Dialoge:

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

## 3.3.1 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 16.

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 (SSH) 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`
  Zugriff mittels SNMP-Version 1 ist aktiv.
  - Die Community-Namen legen Sie fest im Dialog *Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community*.
- `unmarkiert` (Voreinstellung)
  Zugriff mittels SNMP-Version 1 ist inaktiv.

SNMPv2

Aktiviert/deaktiviert den Zugriff auf das Gerät per SNMP Version 2.

Mögliche Werte:

- `markiert`
  Zugriff mittels SNMP-Version 2 ist aktiv.
  - Die Community-Namen legen Sie fest im Dialog *Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community*.
- `unmarkiert` (Voreinstellung)
  Zugriff mittels SNMP-Version 2 ist inaktiv.

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 (2¹⁶-1)` (Voreinstellung: `161`)

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 Einstellungen zu speichern.
- ☐ Starten Sie das Gerät neu.

## [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*
  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* (Voreinstellung)
  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 Management des Geräts ausschließlich mittels Command Line Interface über die serielle Verbindung 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 (2¹⁶-1)` (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 beim Management des Geräts angemeldeten Benutzers.

Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers beim Management des Geräts 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 Fingerabdruck dieses Schlüssels. Der Fingerabdruck 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 Fingerabdrücke zu vergleichen. Wenn die Zeichenfolgen übereinstimmen, dann ist der Client mit dem korrekten Server verbunden.

Das Gerät ermöglicht Ihnen, den RSA-*Host Key* direkt im Gerät zu generieren. Alternativ dazu können Sie Ihren eigenen privaten Schlüssel im PEM-Format auf das Gerät übertragen.

Darüber hinaus kann das Gerät beim Systemstart einen RSA-*Host Key* laden, der auf dem externen Speicher (*ENVM*) abgelegt ist. 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 Management des Geräts ausschließlich mittels Command Line Interface über die serielle Verbindung 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 (2¹⁶-1)` (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 beim Management des Geräts angemeldeten Benutzers trennt das Gerät nach dieser Zeit die Verbindung.

Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers beim Management des Geräts wirksam.

Mögliche Werte:

- `0`
  Deaktiviert die Funktion. Die Verbindung bleibt bei Inaktivität aufgebaut.
- `1..160` (Voreinstellung: `5`)

### Signatur

RSA vorhanden

Zeigt, ob ein RSA-*Host Key* im Gerät vorhanden ist.

Mögliche Werte:

- `markiert`
  Der RSA-*Host Key* ist vorhanden.
- `unmarkiert`
  Der RSA-*Host Key* ist nicht vorhanden.

Erstellen

Generiert einen RSA-*Host Key* im Gerät. Voraussetzung ist, dass der *SSH*-Server ausgeschaltet ist.

Länge des generierten Schlüssels:

- 2048 Bit (RSA)

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

Alternativ dazu können Sie Ihren eigenen privaten Schlüssel im PEM-Format auf das Gerät übertragen. Siehe Rahmen *Key-Import*.

Löschen

Löscht den RSA-*Host Key* vom Gerät. Voraussetzung ist, dass der SSH-Server ausgeschaltet ist.

Betriebszustand

Zeigt, ob das Gerät gegenwärtig einen RSA-*Host Key* generiert.

Möglicherweise hat ein anderer Benutzer diese Aktion ausgelöst.

Mögliche Werte:

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

### Fingerabdruck

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

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

Fingerabdruck Typ

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

Mögliche Werte:

- `md5`
  Das Feld *RSA-Fingerabdruck* zeigt den Fingerabdruck als hexadezimalen MD5-Hash.
- `sha256` (Voreinstellung)
  Das Feld *RSA-Fingerabdruck* zeigt den Fingerabdruck als Base64-codierten SHA-256-Hash.

RSA-Fingerabdruck

Zeigt den Fingerabdruck des RSA-*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.

### Key-Import

URL

Legt Pfad und Dateiname Ihres eigenen RSA-Keys fest.

Das Gerät akzeptiert den Schlüssel, wenn er 2048, 3072 oder 4096 Bit lang ist.

Das Gerät bietet Ihnen folgende Möglichkeiten, die Datei auf das Gerät zu übertragen:

- Import vom PC
  Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie diese in den -Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.

- Import über FTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  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 über TFTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  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 über SCP oder SFTP
  Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  - `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Klicken Sie die Schaltfläche *Start*, um das Fenster *Anmeldeinformationen* zu öffnen. In diesem Fenster geben Sie *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`

  Denken Sie daran, den SCP- oder SFTP-Server zunächst als bekannten Host für SSH einzurichten, bevor das Gerät das erste Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit* > SSH Bekannte Hosts.

Start

Überträgt die im Feld *URL* festgelegte Datei auf das Gerät.

Damit die Änderungen nach dem Übertragen eines digitalen Zertifikats auf das Gerät wirksam werden, schalten Sie die Funktion *SSH-Server* aus und wieder ein. Siehe Rahmen *Funktion*.

## [HTTP]

Diese Registerkarte ermöglicht Ihnen, das Hypertext Transfer Protocol (HTTP) für den Webserver 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 Hypertext Transfer Protocol (HTTP), verwenden Sie stattdessen das Hypertext Transfer Protocol Secure (HTTPS).

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 die Funktion *HTTP* ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Die Funktion *HTTP* ist eingeschaltet.
  Der Zugriff auf das Management des Geräts ist möglich über eine unverschlüsselte *HTTP*-Verbindung.
  Wenn die Funktion *HTTPS* ebenfalls eingeschaltet ist, leitet das Gerät die Anfrage für eine *HTTP*-Verbindung automatisch auf eine verschlüsselte *HTTPS*-Verbindung um.
- *Aus*
  Die Funktion *HTTP* ist ausgeschaltet.
  Wenn die Funktion *HTTPS* eingeschaltet ist, ist der Zugriff auf das Management des Geräts über eine verschlüsselte *HTTPS*-Verbindung möglich.

**Anmerkung:**
Wenn die Funktionen *HTTP* und *HTTPS* ausgeschaltet sind, können Sie die Funktion *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 (2¹⁶-1)` (Voreinstellung: `80`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

## [HTTPS]

Diese Registerkarte ermöglicht Ihnen, das Hypertext Transfer Protocol Secure(HTTPS) für den Webserver 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 digitale Zertifikat selbst zu generieren oder ein vorhandenes digitale Zertifikat auf das Gerät zu übertragen.

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 die Funktion *HTTPS* ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Die Funktion *HTTPS* ist eingeschaltet.
  Der Zugriff auf das Management des Geräts ist möglich über eine verschlüsselte *HTTPS*-Verbindung.
  Wenn kein digitales Zertifikat vorhanden ist, generiert das Gerät ein digitales Zertifikat, bevor es die Funktion *HTTPS* einschaltet.
- *Aus*
  Die Funktion *HTTPS* ist ausgeschaltet.
  Wenn die Funktion *HTTP* eingeschaltet ist, ist der Zugriff auf das Management des Geräts möglich über eine unverschlüsselte *HTTP*-Verbindung.

**Anmerkung:**
Wenn die Funktionen *HTTP* und *HTTPS* ausgeschaltet sind, können Sie die Funktion *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 (2¹⁶-1)` (Voreinstellung: `443`)
  Ausnahme: Port `2222` ist für interne Funktionen reserviert.

### Zertifikat

Wenn das Gerät ein digitales Zertifikat verwendet, das nicht von einer dem Webbrowser bekannten Zertifizierungsstelle (Certification Authority, CA) signiert ist, dann zeigt der Webbrowser möglicherweise eine Warnung an, bevor er die grafische Benutzeroberfläche lädt.

Um diese Warnung abzustellen, haben Sie die folgenden Möglichkeiten:
- Übertragen Sie auf das Gerät ein digitales Zertifikat, dessen Zertifizierungsstelle (Certification Authority, CA) Ihrem Webbrowser bekannt ist. Dies kann zusätzlich erfordern, dass Sie die Zertifizierungsstelle (Certification Authority, CA) Ihrem Webbrowser oder Betriebssystem bekannt machen.
- Als Übergangslösung können Sie auch eine Ausnahmeregel für das existierende Geräte-Zertifikat in Ihrem Webbrowser hinzufügen.

Vorhanden

Zeigt, ob ein digitales Zertifikat im Gerät vorhanden ist.

Mögliche Werte:

- `markiert`
  Ein digitales Zertifikat ist vorhanden.
- `unmarkiert`
  Das digitale Zertifikat wurde entfernt.

Erstellen

Generiert ein digitales Zertifikat im Gerät.

Bis zum Neustart verwendet der Webserver das vorherige Zertifikat.

Damit der Webserver das neu generierte digitale Zertifikat verwendet, starten Sie den Webserver neu. Der Neustart des Webserver ist ausschließlich über das Command Line Interface möglich.

Sie können ein digitales Zertifikat auf das Gerät übertragen. Siehe Rahmen *Zertifikat-Import*.

Löschen

Löscht 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 digitales Zertifikat.
- *delete*
  Das Gerät löscht gegenwärtig ein digitales Zertifikat.
- *generate*
  Das Gerät generiert gegenwärtig ein digitales Zertifikat.

### Fingerabdruck

Der Fingerabdruck 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 Fingerabdruck so lange, bis Sie den Server neu starten.

Fingerabdruck Typ

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

Mögliche Werte:

- `sha1`
  Das Feld *Fingerabdruck* zeigt den SHA1-Fingerabdruck des digitalen Zertifikats.
- `sha256` (Voreinstellung)
  Das Feld *Fingerabdruck* zeigt den SHA1-Fingerabdruck des digitalen Zertifikats.

Fingerabdruck

Hexadezimale Zeichenfolge des vom Server verwendeten digitalen Zertifikats.

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

### Zertifikat-Import

URL

Legt Pfad und Dateiname des digitalen Zertifikats fest.

Das Gerät akzeptiert digitale Zertifikate mit den folgenden Eigenschaften:

- X.509-Format
- `.PEM` Dateinamenserweiterung
- Base64-kodiert und umschlossen von den Zeilen
  - `-----BEGIN PRIVATE KEY-----`
    …
    `-----END PRIVATE KEY-----`
    oder
  - `-----BEGIN CERTIFICATE-----`
    …
    `-----END CERTIFICATE-----`
- RSA-Schlüssel mit einer Länge von 2048, 3072 oder 4096 Bit

Das Gerät bietet Ihnen folgende Möglichkeiten, die Datei auf das Gerät zu übertragen:

- Import vom PC
  Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie diese in den ↑-Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.

- Import über FTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  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]/<Pfad>/<Dateiname>`
- Import über TFTP
  Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  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 über SCP oder SFTP
  Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
  - `scp://` oder `sftp://<IP-Adresse>[:Port]/<Pfad>/<Dateiname>`
    Klicken Sie die Schaltfläche *Start*, um das Fenster *Anmeldeinformationen* zu öffnen. In diesem Fenster geben Sie *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
  - `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>[:Port]/<Pfad>/<Dateiname>`

  Denken Sie daran, den SCP- oder SFTP-Server zunächst als bekannten Host für SSH einzurichten, bevor das Gerät das erste Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit* > SSH Bekannte Hosts.

Start

Überträgt die im Feld *URL* festgelegte Datei auf das Gerät.

Damit die Änderungen nach dem Übertragen eines digitalen Zertifikats auf das Gerät wirksam werden, schalten Sie die Funktion *HTTPS server* aus und wieder ein. Siehe Rahmen *Funktion*.

# 3.3.2 IP-Zugriffsbeschränkung

[ Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung ]

Dieser Dialog ermöglicht Ihnen, den Zugriff auf das Management des Geräts für ausgewählte Anwendungen von einem festgelegten IP-Adressbereich aus zu beschränken.

- Wenn die Funktion ausgeschaltet ist, dann ist der Zugriff auf das Management des Geräts unbeschränkt. Jeder kann mit einer beliebigen Anwendung und von einer beliebigen IP-Adresse aus auf das Management des Geräts zugreifen.
- Bei eingeschalteter Funktion ist der Zugriff beschränkt. Jeder hat Zugriff auf das Management des Geräts ausschließlich unter den folgenden Bedingungen:
  - Mindestens eine Regel ist aktiv.
    und
  - Sie greifen mit einer erlaubten Anwendung von einem zugelassenen IP-Adressbereich aus auf das Gerät zu, wie in der Regel festgelegt.

### Funktion

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.

**Anmerkung:**
Bevor Sie die Funktion aktivieren, vergewissern Sie sich, dass die Tabelle mindestens eine aktive Regel enthält, welche Ihnen Zugriff auf das Management des Geräts gewährt. Andernfalls ist der Zugriff auf das Management des Geräts ausschließlich mittels Command Line Interface über die serielle Verbindung möglich.

▶ *Aus* (Voreinstellung)
Die Funktion *IP-Zugriffsbeschränkung* ist ausgeschaltet.

### Tabelle

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

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen


Hinzufügen

Fügt eine Tabellenzeile hinzu.


Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Wenn Sie eine Tabellenzeile löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie eine Tabellenzeile hinzufügen, schließt das Gerät die erste 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`)
  Ein Beispiel: Um den Zugriff von einer einzelnen IP-Adresse aus zu beschränken, legen Sie den Wert `255.255.255.255` fest.

HTTP

Aktiviert/deaktiviert den HTTP-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  HTTP-Zugriff ist aktiviert. Der Zugriff ist von dem nebenstehenden IP-Adressbereich aus möglich.
- `unmarkiert`
  HTTP-Zugriff ist inaktiv.

HTTPS

Aktiviert/deaktiviert den HTTPS-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  HTTPS-Zugriff ist aktiv. Der Zugriff ist von dem nebenstehenden IP-Adressbereich aus möglich.
- `unmarkiert`
  HTTPS-Zugriff ist inaktiv.

SNMP

Aktiviert/deaktiviert den SNMP-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  SNMP-Zugriff ist aktiv. Der Zugriff ist von dem nebenstehenden IP-Adressbereich aus möglich.
- `unmarkiert`
  SNMP-Zugriff ist inaktiv.

Telnet

Aktiviert/deaktiviert den Telnet-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Telnet-Zugriff ist aktiv. Zugriff ist von dem nebenstehenden IP-Adressbereich aus möglich.
- `unmarkiert`
  Telnet-Zugriff ist inaktiv.

SSH

Aktiviert/deaktiviert den SSH-Zugriff.

Mögliche Werte:

- `markiert` (Voreinstellung)
  SSH-Zugriff ist aktiv. Der Zugriff ist von dem nebenstehenden IP-Adressbereich aus möglich.
- `unmarkiert`
  SSH-Zugriff ist inaktiv.

IEC 61850/MMS

Aktiviert/deaktiviert den Zugriff auf den MMS-Server.

Mögliche Werte:

- `markiert` (Voreinstellung)
  IEC 61850/MMS-Zugriff ist aktiv. Zugriff ist von dem nebenstehenden IP-Adressbereich aus möglich.
- `unmarkiert`
  IEC 61850/MMS-Zugriff ist inaktiv.

Modbus TCP

Aktiviert/deaktiviert den Zugriff auf den *Modbus TCP*-Server.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Modbus TCP-Zugriff ist aktiv. Zugriff ist von dem nebenstehenden IP-Adressbereich aus möglich.
- `unmarkiert`
  Modbus TCP-Zugriff ist inaktiv.

Aktiv

Aktiviert/deaktiviert die Tabellenzeile.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Tabellenzeile ist aktiv. Das Gerät schränkt den Zugriff auf das Management des Geräts auf den festgelegten IP-Adressbereich für ausgewählte Anwendungen ein.
- `unmarkiert`
  Die Tabellenzeile ist inaktiv. Das Gerät schränkt den Zugriff auf das Management des Geräts von dem festgelegten IP-Adressbereich aus für ausgewählte Anwendungen nicht ein.

## 3.3.3 Web

[ Gerätesicherheit > Management-Zugriff > Web ]

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

### Konfiguration

Webinterface-Session Timeout [min]

Legt die Timeout-Zeit in Minuten fest. Bei Inaktivität beendet das Gerät nach dieser Zeit die Sitzung des beim Management des Geräts angemeldeten Benutzers.

Mögliche Werte:

- `0..160` (Voreinstellung: `5`)

Der Wert `0` deaktiviert die Funktion, der Benutzer bleibt bei Inaktivität angemeldet.

## 3.3.4 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 Schließen inaktiver Sitzungen des Command Line Interface über die serielle Verbindung zu aktivieren.

Sie können mittels Command Line Interface wie folgt auf das Management des Geräts zugreifen:
- durch eine serielle Verbindung über die USB-C-Schnittstelle
- per SSH über Ethernet

#### 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
  – `%s` Produktname kurz
  – `%t` Uhrzeit
Voreinstellung: `(GRS)`

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 mittels Command Line Interface über die serielle Verbindung beim Management des Geräts angemeldet ist.

Mögliche Werte:

▶ `0..160` (Voreinstellung: `5`)
Der Wert `0` deaktiviert die Funktion, der Benutzer bleibt bei Inaktivität beim Management des Geräts angemeldet.

Eine Änderung des Werts wird bei erneuter Anmeldung eines Benutzers beim Management des Geräts 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 Einstellungen des Geräts. 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 beim Management des Geräts 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>`

# 3.3.5 SNMPv1/v2 Community

[ Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community ]

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

Anwendungen senden Anfragen mittels SNMPv1/v2 mit einem Community-Namen im SNMP-Datenpaket-Header. Abhängig vom Community-Namen (siehe Spalte *Community*) erhält die Anwendung die Berechtigung *Lesen* oder *Lesen und Schreiben*.

Den Zugriff auf das Gerät mittels 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 16.

Community

Zeigt die Berechtigung für SNMPv1/v2-Zugriff auf das Gerät.

Mögliche Werte:

- `Write`
  Für Anfragen mit dem eingegebenen Community-Namen erhält die Anwendung die Berechtigung *Lesen und Schreiben*.
- `Read`
  Für Anfragen mit dem eingegebenen Community-Namen erhält die Anwendung die Berechtigung *Lesen*.

Name

Legt den Community-Namen für die nebenstehende Berechtigung fest.

Mögliche Werte:

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

  `private` (Voreinstellung für die Berechtigung *Lesen und Schreiben*)
  `public` (Voreinstellung für die Berechtigung *Lesen*)

# 3.4 Pre-Login-Banner

[ Gerätesicherheit > Pre-Login-Banner ]

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

Die Benutzer sehen den Text im Login-Dialog der grafischen Benutzeroberfläche und im Command Line Interface. Benutzer, die sich mit SSH beim Management des Geräts anmelden, sehen den Text – unabhängig 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, speichert das Gerät diesen Text.

### 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>`

# 3.5 SSH Bekannte Hosts

[ Gerätesicherheit > SSH Bekannte Hosts ]

Das Gerät lässt SSH-basierte Verbindungen ausschließlich zu Remote-Servern zu, die dem Gerät bekannt sind. Im Lieferzustand ist kein Remote-Server als bekannter Host im Gerät eingerichtet.

In diesem Dialog machen Sie die Remote-Server durch die Fingerabdrücke ihrer öffentlichen Schlüssel bekannt. Sie können bis zu 50 Einträge bestehend aus Server-Adresse und Fingerabdruck des öffentlichen Schlüssels einrichten. Das Gerät prüft die Identität des Remote-Servers, indem es den Fingerabdruck des öffentlichen Schlüssels, der auf dem Gerät gespeichert ist, mit dem Fingerabdruck vergleicht, der aus dem öffentlichen Schlüssel berechnet wurde, den der Remote-Server tatsächlich gesendet hat. Wenn der berechnete Fingerabdruck des öffentlichen Schlüssels nicht mit dem gespeicherten Fingerabdruck des öffentlichen Schlüssels übereinstimmt, beendet das Gerät die Verbindung.

Wenn auf einem Remote-Server mehrere Schlüssel für unterschiedliche Verschlüsselungsalgorithmen eingerichtet sind, fügen Sie jeden Fingerabdruck eines öffentlichen Schlüssels als separaten Eintrag hinzu.

**Anmerkung:**
Vergewissern Sie sich, dass die Fingerabdrücke der öffentlichen Schlüssel, die Sie auf dem Gerät speichern, aus einer vertrauenswürdigen Quelle stammen, zum Beispiel vom Administrator des SSH-Servers.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Index* legen Sie die Index-Nummer fest.
  Mögliche Werte:
  ▶ `1..50`
  Das Gerät ermöglicht Ihnen, bis zu 50 bekannte Hosts festzulegen.
- Im Feld *Adresse* legen Sie die Adresse des Servers fest. Wenn der Server sowohl mittels IP-Adresse als auch mittels DNS-Name erreichbar ist, fügen Sie für jeden Adresstyp eine eigene Tabellenzeile hinzu.
  Mögliche Werte:
  – Gültige IPv4-Adresse
  – Gültige IPv6-Adresse
  – DNS-Hostname

- Im Feld *Key-Fingerabdruck* legen Sie den Fingerabdruck des öffentlichen Schlüssels des Servers fest.
  Sie können den Fingerabdruck des öffentlichen Schlüssels des Servers zum Beispiel wie folgt ermitteln:
  – vom Administrator eines bekannten SSH-Servers
  – aus der Fehlermeldung nach einem fehlgeschlagenen Software-Update im Dialog *Software* aufgrund der Abweichung zwischen dem im Gerät gespeicherten Fingerabdruck des öffentlichen Schlüssels und dem Fingerabdruck, der aus dem öffentlichen Schlüssel berechnet wird, den der Remote-Server tatsächlich gesendet hat.
    Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.

  Mögliche Werte:
  ▶ Base64-codierte SHA-256-Hash-Sequenz mit einer Länge von 43 oder 44 Zeichen
- Im Feld *Key-Typ* legen Sie den Algorithmus fest, der für die Generierung des öffentlichen Schlüssels des Servers verwendet wurde. Sie können den *Key-Typ*-Wert gleichzeitig und mit der gleichen Methode ermitteln, mit der Sie den Fingerabdruck des öffentlichen Schlüssels erhalten haben.
  Wenn Sie versehentlich einen anderen Algorithmus wählen, kann das Gerät den öffentlichen Schlüssel nicht mittels Fingerabdruck des öffentlichen Schlüssels identifizieren.
  Mögliche Werte:
  ▶ *dsa*
  ▶ *rsa*
  ▶ *ecdsa*
  ▶ *ed25519*

Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Adresse

Zeigt die Adresse des Servers.

Mögliche Werte:
▶ Gültige IPv4-Adresse
▶ Gültige IPv6-Adresse
▶ DNS-Hostname

Key-Fingerabdruck

Legt den Fingerabdruck des öffentlichen Schlüssels des Servers fest.

Mögliche Werte:
▶ Base64-codierte SHA-256-Hash-Sequenz mit einer Länge von 43 oder 44 Zeichen
Um den Fingerabdruck des öffentlichen Schlüssels zu ändern, heben Sie zunächst die Markierung des Kontrollkästchens in Spalte *Aktiv* auf.

Key-Typ

Zeigt den Algorithmus, der zum Generieren des öffentlichen Schlüssels des Servers verwendet wurde.

Mögliche Werte:

- *dsa*
- *rsa*
- *ecdsa*
- *ed25519*

Aktiv

Aktiviert/deaktiviert die Tabellenzeile.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Tabellenzeile ist aktiv.
  Das Gerät betrachtet den in dieser Tabellenzeile eingerichteten Server als bekannt. Wenn Sie eine Datei von einem externen Server auf das Gerät übertragen oder umgekehrt, prüft das Gerät anhand dieses Fingerabdrucks des öffentlichen Schlüssels die Identität des externen Servers.
- `unmarkiert`
  Die Tabellenzeile ist inaktiv.
  Das Gerät betrachtet den in dieser Tabellenzeile eingerichteten Server als unbekannt. Wenn Sie eine Datei von einem externen Server auf das Gerät übertragen oder umgekehrt, beendet das Gerät die Verbindung zu diesem Server.

# 4 Netzsicherheit

Das Menü enthält die folgenden Dialoge:

- Netzsicherheit Übersicht
- Port-Sicherheit
- 802.1X
- RADIUS
- DoS
- 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 eingerichteten *ACL*-Regeln
  Siehe Dialog *Netzsicherheit > ACL*.

### Schaltflächen



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



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

Um die Ebenen wieder einzuklappen, klicken Sie die Schaltfläche . Die Übersicht zeigt dann ausschließlich die erste 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 VLAN-ID und Absender-MAC-Adresse, bevor es ein Datenpaket vermittelt.
  Das Gerät vermittelt ein empfangenes Datenpaket ausschließlich dann, wenn das VLAN 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 16.

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 135.

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 betreiben, empfehlen wir, die Markierung des Kontrollkästchens für die Ring-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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
  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.

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 Fenster *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 Fenster *Wizard* verknüpft sind sowie die Obergrenze für *statische Einträge*. Der untere Teil des Fensters *Wizard* zeigt die Einträge im Detail, sofern vorhanden.

Löscht 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

Fügt einen *statischen Eintrag* hinzu, der auf den in den Feldern *VLAN-ID* und *MAC-Adresse* festgelegten Werten basiert. 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 erwünschten 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 erwünschten 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

[ Netzsicherheit > 802.1X ]

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 mittels 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 Verlauf Port-Authentifizierung
- 802.1X Integrierter Authentifikations-Server (IAS)

# 4.3.1 802.1X Global

[ Netzsicherheit > 802.1X > Global ]

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

### Funktion

Funktion

Schaltet die Funktion *802.1X* ein/aus.

Mögliche Werte:

- *An*
  Die Funktion *802.1X* ist eingeschaltet.
  Das Gerät prüft den Zugriff angeschlossener Endgeräte auf das Netz.
  Die Port-basierte Zugriffskontrolle ist eingeschaltet.
- *Aus* (Voreinstellung)
  Die Funktion *802.1X* 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-Konfiguration*, Spalte *Zugewiesene VLAN-ID* festgelegten VLAN zugewiesen.

VLAN dynamisch erstellen

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 richtet das VLAN ein, falls es nicht existiert.
- `unmarkiert` (Voreinstellung)
  Das automatische Einrichten von VLANs ist inaktiv.
  Existiert das zugewiesene VLAN nicht, bleibt der Port dem ursprünglichen VLAN zugewiesen.

Monitor-Mode

Aktiviert/deaktiviert den Monitor-Modus.

Mögliche Werte:

- `markiert`
  Der Monitor-Modus ist eingeschaltet.
  Das Gerät überwacht die Authentifizierung und hilft bei der Fehlerdiagnose. Wenn sich ein Endgerät erfolglos anmeldet, gewährt das Gerät dem Endgerät Zugriff auf das Netz.
- `unmarkiert` (Voreinstellung)
  Der Monitor-Modus ist ausgeschaltet.

**Information**

Monitor-Mode Clients

Zeigt, wie vielen Endgeräten das Gerät trotz erfolgloser Anmeldung Zugriff auf das Netz gewährt hat.

Voraussetzung ist, dass im Rahmen *Konfiguration* die Funktion *Monitor-Mode* aktiv ist.

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 mithilfe des Protokolls 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-Konfiguration ]

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

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des Ports.

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.

Status Authentifizierung

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.

Zugewiesene VLAN-ID

Zeigt das VLAN, 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`)

Das VLAN, das der Authenticator den Ports zugewiesen hat, finden Sie im Dialog *Netzsicherheit > 802.1X > Port-Clients*.

Grund

Zeigt den Grund für die Zuweisung des VLANs. 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`

Das VLAN, das der Authenticator den Ports für einen Supplikanten zugewiesen hat, finden Sie im Dialog *Netzsicherheit > 802.1X > Port-Clients*.

Gast VLAN-ID

Legt das VLAN fest, das der Authenticator dem Port zuweist, wenn sich das Endgerät während der in Spalte *Intervall Gast-VLAN*festgelegten Zeit nicht 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 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.
- `1..4042`

Unauthenticated VLAN-ID

Legt das VLAN fest, das 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.

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 *Periode Reauthentifizierung [s]*.
  Diese Einstellung ist außer Kraft gesetzt, wenn der Authenticator dem Endgerät eine Voice-, Unauthenticated- oder Gast-VLAN zugewiesen hat.
- `unmarkiert` (Voreinstellung)
  Periodische Authentifizierungsanforderungen sind inaktiv.
  Das Gerät behält die Anmeldung des Endgeräts bei.

Periode Reauthentifizierung [s]

Legt die Zeitspanne in Sekunden fest, nach welcher der Authenticator periodisch das Endgerät auffordert, sich erneut anzumelden.

Mögliche Werte:

- `1..65535 (2¹⁶-1)` (Voreinstellung: `3600`)

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 (2¹⁶-1)` (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 (2¹⁶-1)` (Voreinstellung: `30`)

Timeout Supplikant [s]

Legt die Zeitspanne in Sekunden fest, innerhalb welcher der Authenticator auf die Anmeldung des Endgeräts wartet.

Mögliche Werte:

- `1..65535 (2¹⁶-1)` (Voreinstellung: `30`)

Timeout Server [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 (2¹⁶-1)` (Voreinstellung: `30`)

Requests (max.)

Legt fest, wie viele Male der Authenticator das Endgerät auffordert, sich anzumelden, bis die in Spalte *Timeout Supplikant [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`)

Intervall Gast-VLAN

Zeigt die Zeitspanne in Sekunden, 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.

Der Wert in dieser Spalte ist das Dreifache des in Spalte *Sendeperiode [s]* festgelegten Werts.

Status

Zeigt den gegenwärtigen Zustand des Authenticators (`Authenticator PAE state`).

Mögliche Werte:

- *initialize*
- *disconnected*
- *connecting*
- *authenticating*
- *authenticated*
- *aborting*
- *held*
- *forceAuth*
- *forceUnauth*

Backend Status Authentifizierung

Zeigt den gegenwärtigen Zustand der Verbindung zum Authentifizierungs-Server (`Backend Authentication state`).

Mögliche Werte:

- *request*
- *response*
- *erfolgreich*
- *fail*
- *timeout*
- *idle*
- *initialize*

Port initialisieren

Aktiviert/deaktiviert das Initialisieren des Ports, um die Zugriffskontrolle auf dem Port zu aktivieren oder in den Initialzustand zurückzusetzen. Wenden Sie diese Funktion ausschließlich dann an, wenn für den Port in Spalte *Port-Kontrolle* der Wert *auto* festgelegt ist.

Mögliche Werte:

- `markiert`
  Das Initialisieren des Ports ist aktiv.
  Sobald die Initialisierung abgeschlossen ist, ändert das Gerät den Wert wieder auf `unmarkiert`.
- `unmarkiert` (Voreinstellung)
  Das Initialisieren des Ports ist inaktiv.
  Das Gerät behält den gegenwärtigen Port-Status bei.

Reauthentifizieren

Aktiviert/deaktiviert die einmalige Authentifizierungsanforderung.

Wenden Sie diese Funktion ausschließlich dann an, wenn für den Port in Spalte *Port-Kontrolle* der Wert *auto* festgelegt ist.

Das Gerät 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.

## 4.3.3 802.1X Port-Clients

[Netzsicherheit > 802.1X > 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 16.

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 das VLAN, das der Authenticator dem Port nach erfolgreicher Authentifizierung des Endgeräts zugewiesen hat.

VLAN 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-Konfiguration*, Spalte *Port-Kontrolle* der Wert `auto` festgelegt ist.

Der Authentication-Server weist dem Gerät die Timeout-Zeit per RADIUS zu. Der Wert `0` bedeutet, dass der Authentication-Server kein Timeout zugewiesen hat.

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 > 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 16.

Schaltflächen

Statistiken zurücksetzen

Setzt die Statistiken der ausgewählten Tabellenzeilen zurück.

Port

Zeigt die Nummer des Ports.

Empfangene

Zeigt, wie viele EAPOL-Datenpakete insgesamt das Gerät auf dem Port empfangen hat.

Gesendete

Zeigt, wie viele EAPOL-Datenpakete insgesamt das Gerät auf dem Port gesendet hat.

Start

Zeigt, wie viele EAPOL-Start-Datenpakete das Gerät auf dem Port empfangen hat.

Logoff

Zeigt, wie viele EAPOL-Logoff-Datenpakete das Gerät auf dem Port empfangen hat.

Response/ID

Zeigt, wie viele EAP-Response/Identity-Datenpakete das Gerät auf dem Port empfangen hat.

Response

Zeigt, wie viele gültige EAP-Response-Datenpakete das Gerät auf dem Port empfangen hat (ohne EAP-Response/Identity-Datenpakete).

Request/ID

Zeigt, wie viele EAP-Request/Identity-Datenpakete das Gerät auf dem Port empfangen hat.

Request

Zeigt, wie viele gültige EAP-Request-Datenpakete das Gerät auf dem Port empfangen hat (ohne EAP-Request/Identity-Datenpakete).

Invalid

Zeigt, wie viele EAPOL-Datenpakete mit unbekanntem Frame-Typ das Gerät auf dem Port empfangen hat.

Fehlerhaft Empfangene

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 Verlauf Port-Authentifizierung

[ Netzsicherheit > 802.1X > Verlauf Port-Authentifizierung ]

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 16.

Schaltflächen

Löschen

Entfernt die ausgewählte Tabellenzeile.

Port

Zeigt die Nummer des Ports.

Zeit

Zeigt den Zeitpunkt, zu dem der Authenticator das Endgerät authentifiziert hat.

Vorhanden seit

Zeigt die Zeit, die verstrichen ist, seit das Gerät diesen Log-Eintrag generiert hat.

MAC-Adresse

Zeigt die MAC-Adresse des Endgeräts.

VLAN-ID

Zeigt die ID des VLAN, das dem Endgerät vor der Anmeldung zugewiesen war.

Status

Zeigt den Zustand der Authentifizierung auf dem Port.

Mögliche Werte:

- *erfolgreich*
  Die Authentifizierung war erfolgreich.
- *Fehler*
  Die Authentifizierung war nicht erfolgreich.

Zugriff

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.

VLAN Typ

Zeigt die Art des VLAN, das der Authenticator dem Port zugewiesen hat.

Mögliche Werte:

- *default*
- *radius*
- *unauthenticatedVlan*
- *guestVlan*
- *monitorVlan*
- *notAssigned*

Grund

Zeigt den Grund für die Zuweisung des VLANs und den VLAN-Typ.

# 4.3.6 802.1X Integrierter Authentifikations-Server (IAS)

[ Netzsicherheit > 802.1X > IAS ]

Der Integrierte Authentifikationsserver (IAS) ermöglicht Ihnen, Endgeräte mithilfe des Protokolls 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 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Benutzername* legen Sie den Namen des Benutzerkontos auf dem Endgerät fest.

Löschen

Entfernt die ausgewählte Tabellenzeile.

Benutzername

Zeigt den Namen des Benutzerkontos auf dem Endgerät.

Um ein Benutzerkonto hinzuzufügen, klicken Sie die Schaltfläche .

Passwort

Legt das Passwort fest, mit dem sich der Benutzer authentifiziert. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Um den *Passwort*-Wert zu ändern, klicken Sie das entsprechende Feld. Das Gerät öffnet einen Dialog zum Eingeben/Ändern des Passworts, siehe „[Dialog zur Eingabe/Änderung des Passworts]” auf Seite 153.

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 mittels Protokoll 802.1X mit diesen Zugangsdaten anzumelden.
- `unmarkiert` (Voreinstellung)
  Die Zugangsdaten sind inaktiv.

## [Dialog zur Eingabe/Änderung des Passworts]

Wenn Sie ein Passwortfeld klicken, zeigt das Gerät einen Dialog zur Passwortänderung. In diesem Dialog können Sie ein gültiges Passwort festlegen, indem er Ihnen die erforderlichen Passwortkriterien zeigt. Der Dialog gibt Ihnen Rückmeldung darüber, welche Kriterien das aktuell eingegebene Passwort erfüllt.

- Der Dialog prüft, ob das eingegebene Passwort die erforderliche Passwortlänge erfüllt.
- Der Dialog überprüft, ob das eingegebene Passwort nur zulässige Zeichen enthält.
- Der Dialog hilft, Tippfehler beim Passwort zu vermeiden, indem er Sie auffordert, das Passwort zweimal einzugeben.

Passwortlänge (min.):

Dieses Dialogelement zeigt die erforderliche Mindestlänge des Passworts.

- Wenn das aktuell eingegebene Passwort die erforderliche Mindestlänge erfüllt:
  - Das Gerät zeigt links neben dem Text *Passwortlänge (min.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Passwortlänge (min.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Passwortlänge (max.):

Dieses Dialogelement zeigt die erforderliche Maximallänge des Passworts.

- Wenn das Passwort die erforderliche Maximallänge erfüllt:
  - Das Gerät zeigt links neben dem Text *Passwortlänge (max.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Passwortlänge (max.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Enthält nur erlaubte Zeichen

Dieses Dialogelement zeigt, ob das Passwort nur zulässige Zeichen enthält:

- Falls ja:
  - Das Gerät zeigt links neben dem Text *Enthält nur erlaubte Zeichen* ein grünes Häkchen
  - Das Gerät zeigt den Text *Enthält nur erlaubte Zeichen* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Neues Passwort

Geben Sie hier das neue oder geänderte Passwort ein. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Das in diesem Feld eingegebene Passwort muss mit dem Wert im Feld *Passwort bestätigen* übereinstimmen.

Passwort bestätigen

Bestätigt das neue oder geänderte Passwort. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Das in diesem Feld eingegebene Passwort muss mit dem Wert im Feld *Neues Passwort* übereinstimmen.

Ok

Das Klicken dieser Schaltfläche schließt den Dialog und übernimmt das Passwort in das Passwortfeld des darunterliegenden Dialogs, vorausgesetzt:

- Das aktuell eingegebene Passwort erfüllt alle erforderlichen Kriterien.
- Der *Passwort bestätigen*-Wert stimmt mit dem *Neues Passwort*-Wert überein.

Abbrechen

Das Klicken dieser Schaltfläche bricht den Dialog ab und lässt das Passwort im darunterliegenden Dialog unverändert.

## 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. Dies ermöglicht Ihnen, 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 der Benutzer.

Den in der Antwort eines RADIUS-Servers übertragenen Service-Type weist das Gerät wie folgt einer im Gerät vorhandenen Zugriffsrolle 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 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Index* legen Sie die Index-Nummer fest.
- Im Feld *Adresse*legen Sie die IP-Adresse des Servers fest.
- Legen Sie im Feld *Secret* das Shared Secret fest. Der *RADIUS*-Authentication-Server verwendet dieses Shared Secret, um zu verifizieren, dass die Anfrage von einem vertrauenswürdigen und nicht von einem manipulierten Gerät stammt.
  Wenn Sie das Feld *Secret* leer lassen, führt dies dazu, dass der *RADIUS*-Authentication-Server jede Anfrage stillschweigend verwirft.
  Mögliche Werte:
  ▶ Alphanumerische ASCII-Zeichenfolge mit 1..64 Zeichen
  Das Gerät akzeptiert die folgenden Zeichen:
  ```
  a..z
  A..Z
  0..9
  !#$%&'()*+,-./:;<=>?@[\\]^_`{}~
  ```

Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

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 (2¹⁶-1)` (Voreinstellung: `1812`)

Secret

Legen Sie einen geheimen Schlüsselwert fest, mit dem sich das Gerät beim Authentication-Server anmeldet. Das Gerät zeigt ●●●●● (Punkte) anstelle des geheimen Schlüsselwerts.

Um den geheimen Schlüsselwert zu ändern, klicken Sie das betreffende Feld. Das Gerät öffnet einen Dialog zum Eingeben/Ändern des geheimen Schlüsselwerts, siehe „[Dialog zur Eingabe/Änderung des geheimen Schlüsselwerts]" auf Seite 160.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..64 Zeichen

Den geheimen Schlüsselwert 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 Authentication-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.

## [Dialog zur Eingabe/Änderung des geheimen Schlüsselwerts]

Wenn Sie auf das Feld eines geheimen Schlüsselwerts klicken, zeigt das Gerät einen Dialog zur Änderung des geheimen Schlüsselwerts. In diesem Dialog können Sie einen geheimen Schlüsselwert festlegen, indem er Ihnen die erforderlichen Kriterien für geheimen Schlüsselwerte zeigt. Der Dialog gibt Ihnen Rückmeldung darüber, welche Kriterien der aktuell eingegebene geheime Schlüsselwert erfüllt.

- Der Dialog prüft, ob der eingegebene geheime Schlüsselwert die erforderliche Länge für geheime Schlüsselwerte erfüllt.
- Der Dialog überprüft, ob der eingegebene geheime Schlüsselwert nur zulässige Zeichen enthält.
- Der Dialog hilft, Tippfehler beim geheimen Schlüsselwert zu vermeiden, indem er Sie auffordert, den geheimen Schlüsselwert zweimal einzugeben.

Passwortlänge (min.):

Dieses Dialogelement zeigt die erforderliche Mindestlänge des geheimen Schlüsselwerts.

- Wenn der aktuell eingegebene geheime Schlüsselwert die erforderliche Mindestlänge erfüllt:
  - Das Gerät zeigt links neben dem Text *Passwortlänge (min.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Passwortlänge (min.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Passwortlänge (max.):

Dieses Dialogelement zeigt die erforderliche Maximallänge des geheimen Schlüsselwerts.

- Wenn der geheime Schlüsselwert die erforderliche Maximallänge erfüllt:
  - Das Gerät zeigt links neben dem Text *Passwortlänge (max.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Passwortlänge (max.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Enthält nur erlaubte Zeichen

Dieses Dialogelement zeigt, ob der geheime Schlüsselwert nur zulässige Zeichen enthält:

- Falls ja:
  - Das Gerät zeigt links neben dem Text *Enthält nur erlaubte Zeichen* ein grünes Häkchen
  - Das Gerät zeigt den Text *Enthält nur erlaubte Zeichen* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Neues Passwort

Geben Sie hier den neuen oder geänderten geheimen Schlüsselwert ein. Das Gerät zeigt ●●●●● (Punkte) anstelle des geheimen Schlüsselwerts.

Der hier eingegebene geheime Schlüsselwert muss mit dem Wert im Feld *Passwort bestätigen* übereinstimmen.

Passwort bestätigen

Bestätigt den neuen oder geänderten geheimen Schlüsselwert. Das Gerät zeigt ●●●●● (Punkte) anstelle des geheimen Schlüsselwerts.

Der hier eingegebene geheime Schlüsselwert muss mit dem Wert im Feld *Neues Passwort* übereinstimmen.

Ok

Das Klicken dieser Schaltfläche schließt den Dialog und übernimmt den geheimen Schlüsselwert in das geheime Schlüsselwert-Feld des darunterliegenden Dialogs, vorausgesetzt:

- Der aktuell eingegebene geheime Schlüsselwert erfüllt alle erforderlichen Kriterien.
- Der *Passwort bestätigen*-Wert stimmt mit dem *Neues Passwort*-Wert überein.

Abbrechen

Das Klicken dieser Schaltfläche bricht den Dialog ab und lässt den geheimen Schlüsselwert im darunterliegenden Dialog unverändert.

# 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 Dialog *Netzsicherheit > RADIUS > Global* die Funktion *Accounting* aktiv 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 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- Im Feld *Index* legen Sie die Index-Nummer fest.
- Im Feld *Adresse*legen Sie die IP-Adresse des Servers fest.
- Legen Sie im Feld *Secret* das Shared Secret fest. Der *RADIUS*-Accounting-Server verwendet dieses Shared Secret, um zu verifizieren, dass die Anfrage von einem vertrauenswürdigen und nicht von einem manipulierten Gerät stammt.
  Wenn Sie das Feld *Secret* leer lassen, kann dies zu Sicherheitsrisiken führen oder dazu, dass der *RADIUS*-Accounting-Server Pakete verwirft.
  Mögliche Werte:
  ▶ Alphanumerische ASCII-Zeichenfolge mit 1..64 Zeichen
  Das Gerät akzeptiert die folgenden Zeichen:
  ```
  a..z
  A..Z
  0..9
  !#$%&'()*+,-./:;<=>?@[\\]^_`{}~
  ```

Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

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 (2¹⁶-1)` (Voreinstellung: `1813`)

Secret

Legen Sie einen geheimen Schlüsselwert fest, mit dem sich das Gerät beim Accounting-Server anmeldet. Das Gerät zeigt ●●●●● (Punkte) anstelle des geheimen Schlüsselwerts.

Um den geheimen Schlüsselwert zu ändern, klicken Sie das betreffende Feld. Das Gerät öffnet einen Dialog zum Eingeben/Ändern des geheimen Schlüsselwerts, siehe „[Dialog zur Eingabe/Änderung des geheimen Schlüsselwerts]" auf Seite 160.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..64 Zeichen

Den geheimen Schlüsselwert erfahren Sie vom Administrator des Accounting-Servers.

Aktiv

Aktiviert/deaktiviert die Verbindung zum Accounting-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 Tabellenzeile.

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 16.

Name

Zeigt den Namen des Servers.

IP-Adresse

Zeigt die IP-Adresse des Servers.

Zeit Round-Trip

Zeigt den Zeitabstand in Hundertstelsekunden zwischen der zuletzt empfangenen Antwort des Servers (Access-Reply/Access-Challenge) und dem zugehörigen gesendeten Datenpaket (Access-Request).

Access-Anfragen

Zeigt, wie viele Access-Datenpakete das Gerät an den Server gesendet hat. Der Wert berücksichtigt keine Wiederholungen.

Wiederholt gesendete Access-Anfragen

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 Tabellenzeile.

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 16.

Name

Zeigt den Namen des Servers.

IP-Adresse

Zeigt die IP-Adresse des Servers.

Zeit Round-Trip

Zeigt den Zeitabstand in Hundertstelsekunden zwischen der zuletzt empfangenen Antwort des Servers (Accounting-Response) und dem zugehörigen gesendeten Datenpaket (Accounting-Request).

Accounting-Anfragen

Zeigt, wie viele Accounting-Request-Datenpakete das Gerät an den Server gesendet hat. Der Wert berücksichtigt keine Wiederholungen.

Wiederholt gesendete Accounting-Anfragen

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, bestimmte Dienste oder Geräte funktionsunfähig zu machen. 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.

**Anmerkung:**
Wir empfehlen, die Filter zu aktivieren, um das Sicherheitsniveau des Geräts zu erhöhen.

### 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.

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 Schutz

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 Schutz

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 Schutz

Aktiviert/deaktiviert den L4-Port-Schutz.

Der L4-Port-Schutz erkennt eingehende TCP- und UDP-Datenpakete, bei denen Quell-Port-Nummer und Ziel-Port-Nummer identisch sind, und verwirft diese.

Mögliche Werte:

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

Min.-Header-Size Filter

Aktiviert/deaktiviert den Minimal-Header-Filter.

Der Minimal-Header-Filter vergleicht den TCP-Header von eingehenden Datenpaketen. Wenn der mit 4 multiplizierte Daten-Offset-Wert kleiner ist als die minimale TCP-Header-Größe, dann verwirft der Filter die Datenpakete.

Mögliche Werte:

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

Min. 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

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`)

## 4.6 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.
- *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 eine Regel und legen Sie die Einstellungen der Regel fest. Siehe Dialog *Netzsicherheit > ACL > IPv4-Regel* oder Dialog *Netzsicherheit > ACL > MAC-Regel*.
- ☐ Weisen Sie die Access-Control-Liste den Ports und VLANs des Geräts zu. Siehe Dialog *Netzsicherheit > ACL > Zuweisung*.

Das Menü enthält die folgenden Dialoge:

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

# 4.6.1 ACL IPv4-Regel

[ 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 numerisch niedrigsten 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

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.

- In der Dropdown-Liste *Gruppenname* wählen Sie den Namen der Access-Control-Liste, zu der die Regel gehört, oder fügen Sie einen neuen Namen hinzu.
  Um einen bereits vorhandenen Namen zu verwenden: Geben Sie den Namen in das Suchfeld ein, dann wählen Sie den gewünschten Eintrag in den Suchergebnissen.
  Um einen Namen hinzuzufügen: Geben Sie den Namen in das Suchfeld ein, dann klicken Sie den Link *Erstellen* unterhalb des Suchfelds. Folgende Regeln gelten:
  – Sie können eine ASCII-Zeichenfolge mit 1..31 Zeichen eingeben.
  – Das erste Zeichen ist stets ein Buchstabe.
  – Das Gerät akzeptiert die folgenden Zeichen:
    ```
    a..z
    A..Z
    0..9
    -._
    ```
- 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 Indexwert zuerst an.

Löschen

Entfernt die ausgewählte Tabellenzeile.

Gruppenname

Zeigt den Namen der Access-Control-Liste. Die Access-Control-Liste enthält die Regeln.

Den Namen legen Sie beim Hinzufügen einer Tabellenzeile fest.

Index

Zeigt die Nummer der Regel innerhalb der Access-Control-Liste. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Enthält die Access-Control-Liste mehrere Regeln, wendet das Gerät die Regel mit dem numerisch niedrigsten 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 abhängig vom Wert in den folgenden Feldern an:
  - *Quelle IP-Adresse*, *Ziel IP-Adresse*, *Protokoll*
  - *DSCP*, *TOS-Priorität*, *TOS-Maske*
  - *Paket fragmentiert*

Quelle 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 Schicht-4-Protokoll-Typ der Datenpakete fest, auf die das Gerät die Regel anwendet. Das Gerät wendet die Regel ausschließlich auf Datenpakete an, die den festgelegten Wert im Feld *Protocol* 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

Quelle TCP/UDP-Port

Legt den Quell-Port der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte *Protokoll* der Wert `TCP` oder `UDP` festgelegt ist.

Mögliche Werte:

- `any` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Quell-Port auszuwerten.
- `1..65535 (2¹⁶-1)`
  Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten Quell-Port enthalten.

Ziel TCP/UDP-Port

Legt den Ziel-Port der IP-Datenpakete fest, auf die das Gerät die Regel anwendet. Voraussetzung ist, dass in Spalte *Protokoll* der Wert `TCP` oder `UDP` festgelegt ist.

Mögliche Werte:

- `any` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes IP-Datenpaket an, ohne den Ziel-Port auszuwerten.
- `1..65535 (2¹⁶-1)`
  Das Gerät wendet die Regel ausschließlich auf IP-Datenpakete an, die den festgelegten Ziel-Port enthalten.

Aktion

Legt fest, wie das Gerät die IP-Datenpakete verarbeitet, wenn es die Regel anwendet.

Mögliche Werte:

- *`permit`* (Voreinstellung)
  Das Gerät vermittelt die IP-Datenpakete.
- *`deny`*
  Das Gerät verwirft die IP-Datenpakete.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog *Diagnose > Bericht > System-Log*.

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiv.
  Voraussetzung ist, dass im Dialog *Netzsicherheit > ACL > Zuweisung* die Access-Control-Liste einem VLAN oder Port zugewiesen ist.
  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.

## 4.6.2 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 numerisch niedrigsten Wert in Spalte *Index*.

Das Gerät ermöglicht Ihnen, nach folgenden Kriterien zu filtern:
- Quell- oder Ziel-MAC-Adresse eines Datenpakets

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.
- In der Dropdown-Liste *Gruppenname* wählen Sie den Namen der Access-Control-Liste, zu der die Regel gehört, oder fügen Sie einen neuen Namen hinzu.
  Um einen bereits vorhandenen Namen zu verwenden: Geben Sie den Namen in das Suchfeld ein, dann wählen Sie den gewünschten Eintrag in den Suchergebnissen.
  Um einen Namen hinzuzufügen: Geben Sie den Namen in das Suchfeld ein, dann klicken Sie den Link *Erstellen* unterhalb des Suchfelds. Folgende Regeln gelten:
  – Sie können eine ASCII-Zeichenfolge mit 1..31 Zeichen eingeben.
  – Das erste Zeichen ist stets ein Buchstabe.
  – Das Gerät akzeptiert die folgenden Zeichen:
    ```
    a..z
    A..Z
    0..9
    -._
    ```
- 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 Indexwert zuerst an.

Löschen

Entfernt die ausgewählte Tabellenzeile.

Gruppenname

Zeigt den Namen der Access-Control-Liste. Die Access-Control-Liste enthält die Regeln.

Den Namen legen Sie beim Hinzufügen einer Tabellenzeile fest.

Index

Zeigt die Nummer der Regel innerhalb der Access-Control-Liste. Sie legen die Index-Nummer fest, wenn Sie eine Tabellenzeile hinzufügen.

Enthält die Access-Control-Liste mehrere Regeln, wendet das Gerät die Regel mit dem numerisch niedrigsten Wert zuerst an.

Alle Pakete filtern

Legt fest, auf welche MAC-Datenpakete das Gerät die Regel anwendet.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Gerät wendet die Regel auf jedes MAC-Datenpaket an.
- `unmarkiert`
  Das Gerät wendet die Regel auf MAC-Datenpakete abhängig vom Wert in den folgenden Feldern an:
  - *Quelle MAC-Adresse*
  - *Ziel MAC-Adresse*

Quelle 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.

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.

Log

Aktiviert/deaktiviert die Protokollierung in der Log-Datei. Siehe Dialog *Diagnose > Bericht > System-Log*.

Mögliche Werte:

- `markiert`
  Die Protokollierung ist aktiv.
  Voraussetzung ist, dass im Dialog *Netzsicherheit > ACL > Zuweisung* die Access-Control-Liste einem VLAN oder Port zugewiesen ist.
  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.

## 4.6.3 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.

Das Gerät ermöglicht Ihnen, bis zu 50 ACLs mit einer bestimmten Anzahl an Regeln festzulegen. Die Anzahl an Regeln, die Sie den Ports und VLANs tatsächlich zuweisen können, ist möglicherweise kleiner als die Anzahl der im Gerät festgelegten Regeln. Ein Beispiel im Anwender-Handbuch „Konfiguration“ veranschaulicht die Faktoren, die sich auf die mögliche Anzahl auswirken, die Sie tatsächlich zuweisen können.

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*) Datenpakete anzuwenden.

**Anmerkung:**
Bevor Sie die Funktion einschalten, vergewissern Sie sich, dass mindestens eine aktive Tabellenzeile 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 mittels Command Line Interface über die serielle Verbindung möglich.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen


Hinzufügen

Öffnet das Fenster *Erstellen*, um einem Port oder einem VLAN eine Regel zuzuweisen.
- In der Dropdown-Liste *Port/VLAN* wählen Sie den Port oder das VLAN, auf den/das das Gerät die Regel anwendet.
- Im Feld *Priorität* legen Sie die Reihenfolge fest, in der das Gerät die Regeln auf den Datenstrom anwendet.

- In der Dropdown-Liste *Richtung* wählen Sie aus, ob das Gerät die Regel auf empfangene Datenpakete oder auf zu sendende Datenpakete anwendet.
- In der Dropdown-Liste *Gruppenname* wählen Sie die Regel, welche das Gerät dem Port oder VLAN zuweist.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

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, dass das Gerät die Access-Control-Liste auf empfangene Datenpakete anwendet. Das Gerät kann die Access-Control-Listen ausschließlich auf empfangene Datenpakete anwenden.

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 (2³²-1)`

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.

# 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 für die Einträge in der MAC-Adresstabelle (Forwarding Database) ändern
- Flusskontrolle im Gerät einschalten
- Funktion *VLAN-Unaware Modus* aktivieren

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 überflüssige Datenpakete.

Der in IEEE 802.3 definierte Flusskontrollmechanismus sorgt dafür, dass durch einen Pufferüberlauf auf einem Port keine Datenpakete verloren gehen. Kurz bevor der Pufferspeicher eines Ports 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 dann für die Dauer der Signalisierung keine Datenpakete. Auf einem Uplink-Port führt dies möglicherweise zu unerwünschten Sendeunterbrechungen im übergeordneten Netzsegment („Wandering Backpressure“). Der Flusskontrollmechanismus verringert das Netz somit auf die Bandbreite, die das langsamste Gerät im Netz verarbeiten kann.

Gemäß 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`. Datenpakete mit einer VLAN-ID=`0` heißen *Priority Tagged Frames*. 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 die Funktion *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 MAC-Adresstabelle (Forwarding Database).

Die MAC-Adresstabelle (Forwarding Database) 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 Modus, in dem das Gerät die VLAN-ID ignoriert und die Datenpakete unverändert vermittelt. Das Gerät wertet weiterhin die Prioritätsinformation in den Datenpaketen aus.

Auf den angeschlossenen Endgeräten erfordern lediglich einige wenige Anwendungen Empfangen von Datenpaketen mit einer VLAN-ID=`0`. Wenn die Anwendungen im Netz dies erfordern, dann aktivieren Sie die Funktion.

Mögliche Werte:

- `markiert`
  Das Gerät arbeitet gemäß IEEE 802.1Q im Modus *VLAN-unaware*:
  - Das Gerät ignoriert die VLAN-Einstellungen im Gerät und die VLAN-ID in den Datenpaketen. Das Gerät vermittelt die Datenpakete anhand ihrer Ziel-MAC-Adresse.
  - Das Gerät wertet die im VLAN-Tag der Datenpakete enthaltene Prioritätsinformation aus.
  - Das Gerät ignoriert die in den Dialogen *Switching > VLAN > Konfiguration* und *Switching > VLAN > Port* festgelegten VLAN-Einstellungen.

  **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)
  Das Gerät arbeitet gemäß IEEE 802.1Q im Modus *VLAN-aware*:
  - Das Gerät wertet das VLAN-Tag in den Datenpaketen aus.
  - Das Gerät vermittelt die Datenpakete anhand ihrer Ziel-MAC-Adresse oder Ziel-IP-Adresse im jeweiligen VLAN.
  - Das Gerät wertet die im Datenpaket enthaltene Prioritätsinformation aus.
  - Wenn das Gerät ein Datenpaket mit einer VLAN-ID=`0` empfängt, weist es dem Datenpaket die VLAN-ID des Ports zu. Siehe Dialog *Switching > VLAN > Port*.

# 5.2 Lastbegrenzer

[ Switching > Lastbegrenzer ]

Das Gerät ermöglicht Ihnen, die Anzahl der Datenpakete an den Ports zu begrenzen, um auch bei hohem Datenaufkommen einen stabilen Betrieb zu ermöglichen. Wenn die Anzahl der Datenpakete auf einem Port den Schwellenwert überschreitet, dann verwirft das Gerät die überschüssigen Datenpakete 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 Schwellenwert legt fest, welchen maximalen Verkehr der Port eingangsseitig vermittelt. Wenn die Anzahl der Datenpakete auf einem Port den festgelegten Schwellenwert überschreitet, dann verwirft das Gerät die überschüssigen Datenpakete auf diesem Port.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des Ports.

Schwellenwert

Legt den Schwellenwert fest für Broadcast-, Multicast- und Unicast-Datenpakete auf diesem Port:

Mögliche Werte:

- `0` (Voreinstellung)
  Die Funktion *Lastbegrenzer* ist auf diesem Port deaktiviert.
- `1..24414` bei 100 Mbit/s
  `1..244140` bei 1000 Mbit/s
  - Wenn in Spalte *Einheit* der Wert `Prozent` festgelegt ist, dann legen Sie einen prozentualen Wert zwischen `1` und `100` fest.
  - Wenn in Spalte *Einheit* der Wert `pps` festgelegt ist, dann legen Sie einen absoluten Wert fest. Die Lastbegrenzerfunktion berechnet den Schwellenwert auf Grundlage von 512 Byte großen Datenpaketen.

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

Einheit

Legt die Einheit für den Schwellenwert fest:

Mögliche Werte:

- *Prozent* (Voreinstellung)
  Der Schwellenwert ist festgelegt in Prozent der Datenrate des Ports.
- *pps*
  Der Schwellenwert ist festgelegt in Datenpaketen pro Sekunde.

Broadcast Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Broadcast-Datenpakete.

Mögliche Werte:

- markiert
- unmarkiert (Voreinstellung)

Bei Überschreiten des Schwellenwerts verwirft das Gerät auf diesem Port die Überlast an Broadcast-Datenpaketen.

Multicast Modus

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Multicast-Datenpakete.

Mögliche Werte:

- markiert
- unmarkiert (Voreinstellung)

Bei Überschreiten des Schwellenwerts verwirft das Gerät auf diesem Port die Überlast an Multicast-Datenpaketen.

Unknown unicast mode

Aktiviert/deaktiviert die Lastbegrenzerfunktion für empfangene Unicast-Datenpakete mit unbekannter Zieladresse.

Mögliche Werte:

- markiert
- unmarkiert (Voreinstellung)

Bei Überschreiten des Schwellenwerts verwirft das Gerät auf diesem Port die Überlast an Unicast-Datenpaketen.

## [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 16.

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 MAC-Adresstabelle (Forwarding Database) anzuzeigen und zu bearbeiten. Adressfilter legen die Vermittlungsweise der Datenpakete im Gerät anhand der Ziel-MAC-Adresse fest.

Jede Tabellenzeile 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 die Zieladresse eines Datenpakets enthält, dann vermittelt das Gerät das Datenpaket vom empfangenden Port an den in der Tabellenzeile festgelegten Port.
- Existiert keine Tabellenzeile für die Zieladresse, vermittelt das Gerät das Datenpaket vom empfangenden Port an jeden anderen Port.

### Tabelle

Um die gelernten MAC-Adressen aus der MAC-Adresstabelle (Forwarding Database) zu entfernen, klicken Sie im Dialog *Grundeinstellungen > Restart* die Schaltfläche *FDB leeren*.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.
- Im Feld *MAC-Adresse* legen Sie die Ziel-MAC-Adresse fest.
- Im Feld *VLAN-ID* legen Sie die VLAN-ID fest.
- Im Listenfeld wählen Sie die Ports aus.
  - Wenn die Ziel-MAC-Adresse eine Unicast-Adresse ist, wählen Sie genau einen Port aus.
  - Wenn die Ziel-MAC-Adresse eine Multicast- oder Broadcast-Adresse ist, wählen Sie einen oder mehrere Ports aus.
  - Wählen Sie keinen Port aus, um einen *Discard*-Filter hinzuzufügen. Das Gerät verwirft Datenpakete mit der in der Tabellenzeile festgelegten Ziel-MAC-Adresse.

Löschen

Entfernt die ausgewählte Tabellenzeile.

FDB leeren

Löscht die MAC-Adressen, die in Spalte *Status* den Wert *Learned* haben, aus der Forwarding-Tabelle (FDB).

MAC-Adresse

Zeigt die Ziel-MAC-Adresse, auf die sich die Tabellenzeile bezieht.

VLAN-ID

Zeigt die ID des VLANs, auf das sich die Tabellenzeile bezieht.

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:

- `Static`
  Manuell eingerichteter Adressfilter
  Der Adressfilter bleibt dauerhaft eingerichtet.
  Sie können einen Adressfilter mit dem Status `Static` bearbeiten oder löschen.
- *Mgmt*
  MAC-Adresse des Geräts
  Der Adressfilter ist gegen Veränderungen geschützt.
- *Learned*
  Automatisch eingerichteter Adressfilter
  Das Gerät hat den Filter anhand empfangener Datenpakete eingerichtet.
  Das Gerät löscht einen Adressfilter mit dem Status *Learned* nach einer bestimmten Zeit (*Aging-Time [s]*), wenn das Gerät keine Datenpakete mehr von der relevanten MAC-Adresse empfängt.
  Um einen Adressfilter mit dem Status *Learned* zu bearbeiten oder zu löschen, setzen Sie zunächst seinen Status auf `Static` und speichern diese Änderung im flüchtigen Speicher.
- *GMRP*
  Multicast-Adressfilter automatisch eingerichtet durch GMRP.
- *IGMP*
  Adressfilter automatisch eingerichtet durch IGMP-Snooping.
- *MRP-MMRP*
  Multicast-Adressfilter automatisch eingerichtet durch MMRP.
- *Other*
  Statischer Adressfilter
  Eine der folgenden Gerätefunktionen hat die Zieladresse eingerichtet:
  - *802.1X*
  - *Port-Sicherheit*

<Port-Nummer>

Zeigt, wie der betreffende Port Datenpakete an die Zieladresse sendet, die in der Spalte ganz links angegeben ist. Die Tabellenzelle enthält eine Abkürzung. Wenn Sie den Mauszeiger über einer Tabellenzelle positionieren oder darauf tippen, zeigt ein Tooltip den vollständigen Text.

Mögliche Werte:

- `-`
  Tooltip: `-`
  Der Port sendet keine Datenpakete an die Zieladresse.
- `L`
  Tooltip: `Learned`
  Der Port sendet Datenpakete an die Zieladresse.
  Das Gerät hat den Filter anhand empfangener Datenpakete automatisch eingerichtet.
- *US*
  Tooltip: *Unicast static*
  Der Port sendet Datenpakete an die Unicast-Zieladresse.
  Ein Benutzer hat den Filter eingerichtet.

- *MS*
  Tooltip: *Multicast static*
  Der Port sendet Datenpakete an die Multicast-Zieladresse.
  Ein Benutzer hat den Filter eingerichtet.
- *FA*
  Tooltip: *Forward all*
  Der Port sendet alle Multicast-Datenpakete.
  Das Gerät hat den Filter anhand empfangener Datenpakete automatisch eingerichtet.
- *IL*
  Tooltip: *IGMP learned*
  Der Port sendet Datenpakete an die Multicast-Zieladresse.
  Die *IGMP-Snooping*-Funktion im Gerät hat den Filter eingerichtet.
- *MS/IL*
  Tooltip: *Multicast static/IGMP learned*
  Der Port sendet Datenpakete an die Multicast-Zieladresse.
  Ein Benutzer hat den Filter eingerichtet. Zusätzlich hat die *IGMP-Snooping*-Funktion im Gerät den Filter eingerichtet.
- *GL*
  Tooltip: *GMRP learned*
  Der Port sendet Datenpakete an die Multicast-Zieladresse.
  Die *GMRP*-Funktion im Gerät hat den Filter eingerichtet.
- *GFA*
  Tooltip: *GMRP forward all*
  Der Port sendet Multicast-Datenpakete mit Gruppen-Adressen.
  Ein Benutzer hat den Filter eingerichtet, oder die *GMRP*-Funktion im Gerät hat den Filter eingerichtet.
- *MS/GL*
  Tooltip: *Multicast static/GMRP learned*
  Der Port sendet Datenpakete an die Multicast-Zieladresse.
  Ein Benutzer hat den Filter eingerichtet. Zusätzlich hat die *GMRP*-Funktion im Gerät den Filter eingerichtet.
- *ML*
  Tooltip: *MMRP learned*
  Der Port sendet Datenpakete an die Multicast-Zieladresse.
  Die *MMRP*-Funktion im Gerät hat den Filter eingerichtet.
- *MS/ML*
  Tooltip: *Multicast static/MMRP learned*
  Der Port sendet Datenpakete an die Multicast-Zieladresse.
  Ein Benutzer hat den Filter eingerichtet. Zusätzlich hat die *MMRP*-Funktion im Gerät den Filter eingerichtet.

# 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) generiert.
- Die am IGMP-Snooping beteiligten Geräte im Netz leiten die IGMP-Queries weiter.

Das Gerät verknüpft die IGMP-Reports mit den Einträgen in seiner MAC-Adresstabelle (Forwarding Database). Tritt ein Multicast-Empfänger einer Multicast-Gruppe bei, fügt das Gerät für diesen Port eine Tabellenzeile im Dialog *Switching > Filter für MAC-Adressen* hinzu. Das Gerät entfernt die Tabellenzeile, wenn der Multicast-Empfänger die Multicast-Gruppe verlässt.

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, die Funktion *IGMP-Snooping* im Gerät einzuschalten und die Funktion pro Port und pro VLAN einzurichten.

### 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) and 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

Löscht die IGMP-Snooping-Einträge und setzt den Zähler im Rahmen *Information* auf `0`.

Verarbeitete Multicast Controls

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, um die MAC-Adresstabelle (Forwarding Database) zur Vermittlung der Multicast-Datenpakete einzurichten.

Mögliche Werte:

- `0..2147483647 (2³¹-1)`

Mit der Schaltfläche *IGMP-Snooping Daten leeren* im Dialog *Grundeinstellungen > Restart* 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 und die Funktion pro Port und pro VLAN einzurichten.

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

### [VLAN-ID]

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

#### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

VLAN-ID

Zeigt die ID des VLANs, auf das sich die Tabellenzeile bezieht.

Aktiv

Aktiviert/deaktiviert die Funktion *IGMP-Snooping* für dieses VLAN.

Voraussetzung ist, dass die Funktion *IGMP-Snooping* global eingeschaltet 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 MAC-Adresstabelle (Forwarding Database) 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. 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`)

Admin-Modus Fast-Leave

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 MAC-Adresstabelle (Forwarding Database).
- `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 richten Sie die Funktion *IGMP-Snooping* für jeden Port ein.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des Ports.

Aktiv

Aktiviert/deaktiviert die Funktion *IGMP-Snooping* auf dem Port.

Voraussetzung ist, dass die Funktion *IGMP-Snooping* global eingeschaltet ist.

Mögliche Werte:

- `markiert` (Voreinstellung)
  IGMP-Snooping ist auf diesem Port eingeschaltet. Der Port ist für den Multicast-Datenstrom angemeldet.
- `unmarkiert`
  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 MAC-Adresstabelle (Forwarding Database) 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. 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`)

Admin-Modus Fast-Leave

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 MAC-Adresstabelle (Forwarding Database).
- `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.

Statischer Query-Port

Aktiviert/deaktiviert den *Statischer Query-Port*-Modus.

Mögliche Werte:

- `markiert`
  Der *Statischer Query-Port*-Modus ist aktiv.
  Der Port ist ein statischer Query-Port in den eingerichteten VLANs.
- `unmarkiert` (Voreinstellung)
  Der *Statischer 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, auf die sich die Tabellenzeile bezieht.

## 5.4.3 IGMP-Snooping Erweiterungen

[ Switching > IGMP-Snooping > Snooping Erweiterungen ]

Dieser Dialog ermöglicht Ihnen, für ein VLAN einen Port auszuwählen und den Port einzurichten.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen


Wizard

Öffnet das Fenster *Wizard*, das Sie beim Auswählen und Einrichten der Ports unterstützt. Siehe „[Wizard: IGMP-Snooping Erweiterungen]” auf Seite 200.

VLAN-ID

Zeigt die ID des VLANs, auf das sich die Tabellenzeile bezieht.

<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 eingerichteter Query-Port.
- `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, sowie an statisch eingerichtete Query-Ports.
  Um diesen Wert zuzuweisen, führen Sie die folgenden Schritte aus:
  - ☐ Öffnen Sie das Fenster *Wizard*.
  - ☐ Markieren Sie auf der Seite *Konfiguration* das Kontrollkästchen *Statisch*.
- `A` = Automatic
  Das Gerät hat den Port als Query-Port erkannt. Voraussetzung ist, dass der Port als *Learn by LLDP* eingerichtet ist.

- `P` = Learn by LLDP (manual setting)
  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 auf der Seite *Konfiguration* das Kontrollkästchen *`Learn by LLDP`*.
- `F` = Forward All (manual setting)
  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 auf der Seite *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.

Mögliche Werte:

- *`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 Einrichten der Ports.

Das Fenster *Wizard* führt Sie durch die folgenden Schritte:
- Auswahl VLAN/Port
- Konfiguration

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

### Auswahl VLAN/Port

VLAN-ID

Auswahl der VLAN-ID.

Port

Auswahl der Ports.

### Konfiguration

VLAN-ID

Zeigt die ausgewählte VLAN-ID.

Port

Zeigt die Nummer der ausgewählten Ports.

Statisch

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 vermittelt einen Multicast-Stream lediglich an die Ports, an denen ein Multicast-Empfänger angeschlossen ist.

Um zu erkennen, an welchen Ports Multicast-Empfänger angeschlossen sind, sendet das Gerät auf den Ports in einem bestimmten Intervall Query-Datenpakete. 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 sowohl global als auch für die existierenden VLANs einzurichten.

### 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 16.

VLAN-ID

Zeigt die ID des VLANs, auf das sich die Tabellenzeile bezieht.

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.

IP-Adresse

Legt die IP-Adresse fest, die das Gerät als Absenderadresse in generierte *General Query*-Datenpakete einfügt. Verwenden Sie die Adresse des Multicast-Routers.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)

Protokoll-Version

Zeigt die Version des Internet Group Management Protocols (IGMP) der *General Query*-Datenpakete.

Mögliche Werte:

- `1`
  IGMP v1
- `2` (Voreinstellung)
  IGMP v2
- `3`
  IGMP v3

Max. Antwortzeit

Zeigt die Zeit in Sekunden, in der die Mitglieder einer Multicast-Gruppe auf ein Query-Datenpaket antworten. 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 vermittelt auch Datenpakete mit bekannten Multicast-Adressen an die Query-Ports.

### Konfiguration

Unbekannte Multicasts

Legt fest, wie das Gerät die Datenpakete unbekannter Multicast-Adressen vermittelt.

Mögliche Werte:

- *Verwerfen*
  Das Gerät verwirft Datenpakete mit unbekannter MAC-Multicast-Adresse.
- *An alle Ports senden* (Voreinstellung)
  Das Gerät vermittelt Datenpakete mit unbekannter MAC-Multicast-Adresse an jeden Port.
- *An Query-Ports senden*
  Das Gerät vermittelt Datenpakete mit unbekannter MAC-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 16.

VLAN-ID

Zeigt die ID des VLANs, auf das sich die Tabellenzeile bezieht.

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-Protokoll (MRP-IEEE) als Ersatz für das Generic Attribute Registration Protocol (GARP) ein. Zudem änderte und ersetzte der IEEE-Normungsausschuss 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 beschränken. Um den Verkehr zu beschränken, 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 Datenpakete 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-IEEE-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 *LeaveAll*- oder *Leave*-Ereignis legen Sie – auch im Fall einer verlorenen Nachricht – für den `≥ (2x JoinTime) + 60`-Timer den Wert *Leave* fest.
- Um das Aufkommen an *Rejoin*-Datenpaketen zu minimieren, welche das Gerät nach einem *LeaveAll*-Ereignis generiert, legen Sie den Wert für den *LeaveAll*-Timer größer als den Wert des *Leave*-Timers fest.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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 generiert.

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.

Ein Beispiel für die Arbeitsweise von MMRP ist eine 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 16.

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 16.

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 vermittelt die Datenpakete, welche für die im MMRP registrierten Multicast-MAC-Adressen bestimmt sind, in das VLAN. Das Gerät vermittelt die Datenpakete an Ports, die MMRP dynamisch eingerichtet hat, oder an Ports, 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 Datenpakete, 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 (MMRPDUs) aus, um den Zustand der Geräte an einem aktiven MMRP-Port aufrecht zu erhalten. Diese Registerkarte ermöglicht Ihnen, für jeden Port die Statistiken der vermittelten MMRP-Datenpakete zu überwachen.

### Information

Schaltflächen

Statistiken zurücksetzen

Setzt die Zähler der Port-Statistiken und die Werte in Spalte *Letzte empfangene MAC-Adresse* zurück.

MMRP-PDU gesendet

Zeigt die Anzahl der an das Gerät übermittelten MMRPDUs.

MMRP-PDU empfangen

Zeigt die Anzahl der vom Gerät empfangenen MMRPDUs.

Bad-Header PDU empfangen

Zeigt die Anzahl der vom Gerät empfangenen MMRPDUs mit fehlerhaftem Header.

Bad-Format PDU empfangen

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 16.

Port

Zeigt die Nummer des Ports.

MMRP-PDU gesendet

Zeigt die Anzahl der an den Port übermittelten MMRPDUs.

MMRP-PDU empfangen

Zeigt die Anzahl der vom Port empfangenen MMRPDUs.

Bad-Header PDU empfangen

Zeigt die Anzahl der vom Port empfangenen MMRPDUs mit fehlerhaftem Header.

Bad-Format PDU empfangen

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 MAC-Adresse, von welcher der Port zuletzt 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 Einrichten von VLANs ermöglicht. Wenn Sie zum Beispiel ein VLAN an einem aktiven MVRP-Port einrichten, verteilt das Gerät die VLAN-Informationen an andere Geräte mit eingeschaltetem MVRP. Anhand der erhaltenen Informationen generiert 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 s 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 16.

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.

Eingeschränkte VLAN-Registrierung

Aktiviert/deaktiviert die Funktion *Eingeschränkte VLAN-Registrierung* auf diesem Port.

Mögliche Werte:

- `markiert`
  Bei eingeschalteter Funktion und vorhandenem statischem VLAN-Registrierungseintrag ermöglicht Ihnen das Gerät, ein dynamisches VLAN für diesen Eintrag hinzuzufügen.
- `unmarkiert` (Voreinstellung)
  Schaltet die Funktion *Eingeschränkte VLAN-Registrierung* auf diesem Port aus.

## [Statistiken]

Geräte in einem LAN tauschen Multiple VLAN Registration Protocol Data Units (MVRPDUs) aus, um den Zustand der VLANs an aktiven Ports aufrecht zu erhalten. Diese Registerkarte ermöglicht Ihnen, die MVRP-Datenpakete zu überwachen.

### Information

Schaltflächen

Statistiken zurücksetzen

Setzt die Zähler der Port-Statistiken und die Werte in Spalte *Letzte empfangene MAC-Adresse* zurück.

MVRP-PDU gesendet

Zeigt die Anzahl der an das Gerät übermittelten MVRPDUs.

MVRP-PDU empfangen

Zeigt die Anzahl der vom Gerät empfangenen MVRPDUs.

Bad-Header PDU empfangen

Zeigt die Anzahl der vom Gerät empfangenen MVRPDUs mit fehlerhaftem Header.

Bad-Format PDU empfangen

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.

Fehler Message-Queue

Zeigt die Anzahl der vom Gerät blockierten MVRPDUs.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des Ports.

MVRP-PDU gesendet

Zeigt die Anzahl der an den Port übermittelten MVRPDUs.

MVRP-PDU empfangen

Zeigt die Anzahl der vom Port empfangenen MVRPDUs.

Bad-Header PDU empfangen

Zeigt die Anzahl der vom Gerät auf dem Port empfangenen MVRPDUs mit fehlerhaftem Header.

Bad-Format PDU empfangen

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 erfolglosen Registrierungsversuche auf dem Port.

Letzte empfangene MAC-Adresse

Zeigt die MAC-Adresse, von welcher der Port zuletzt MVRPDUs empfangen hat.

## 5.6 GARP

[ Switching > GARP ]

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

Wird ein Attribut für einen Teilnehmer gemäß dem GARP registriert oder wieder ausgetragen, 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 802.1D 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 16.

Port

Zeigt die Nummer des Ports.

GMRP aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an *GMRP*.

Voraussetzung ist, dass die Funktion *GMRP* global eingeschaltet 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 oder Generic VLAN Registration Protocol (GVRP) 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 Einrichtung 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 einrichtet. 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 hinzuzufügen 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 ausgeschaltet 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 16.

Port

Zeigt die Nummer des Ports.

GVRP aktiv

Aktiviert/deaktiviert die Teilnahme des Ports an *GVRP*.

Voraussetzung ist, dass die Funktion *GVRP* global eingeschaltet 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, *Port-Priorität*).

**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

# 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 Precedence*-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 16.

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 höherer oder mit niedrigerer 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 16.

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`<br>Normale Daten ohne Priorisierung |
| `1` | 0 | `Background`<br>Zeitunkritische Daten und Hintergrunddienste |
| `2` | 1 | `Standard`<br>Normale Daten |
| `3` | 3 | `Excellent Effort`<br>Wichtige Daten |
| `4` | 4 | `Controlled Load`<br>Zeitkritische Daten mit hoher Priorität |

| VLAN-Priorität | Verkehrsklasse | Inhaltskennzeichnung gemäß IEEE 802.1D |
|---|---|---|
| 5 | 5 | Video<br>Bildübertragung mit Verzögerungen und Jitter <100 ms |
| 6 | 6 | Voice<br>Sprachübertragung mit Verzögerungen und Jitter <10 ms |
| 7 | 7 | Network Control<br>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 16.

DSCP Wert

Zeigt den DSCP-Wert.

Traffic-Klasse

Legt die *Verkehrsklasse* fest, die dem DSCP-Wert zugewiesen ist.

Mögliche Werte:

- `0..7`
  `0`ist der Warteschlange mit der niedrigsten Priorität zugewiesen.
  `7`ist der Warteschlange mit der höchsten Priorität zugewiesen.

### 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 |
| 46 | EF | 5 |

| DSCP-Wert | DSCP-Name | Verkehrsklasse |
|---|---|---|
| 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.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 16.

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 %.

# 5.8 VLAN

[ Switching > VLAN ]

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

- Hohe Flexibilität
  - Mit VLAN verteilen Sie den Datenpakete 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 der Datenpakete auf einzelne logische Netze erschwert ungewolltes Abhören und härtet das System gegen Angriffe, wie MAC-Flooding oder MAC-Spoofing.

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

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

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

Das Gerät priorisiert den empfangenen Datenstrom in folgender Reihenfolge:

- Voice-VLAN
- Port-basiertes VLAN

Das Menü enthält die folgenden Dialoge:

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

## 5.8.1 VLAN Global

[ 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 > Netzwerk > Global* das VLAN 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 1 ist dauerhaft im Gerät eingerichtet.

## 5.8.2 VLAN Konfiguration

[ Switching > VLAN > Konfiguration ]

In diesem Dialog verwalten Sie die VLANs. Um ein VLAN einzurichten, fügen Sie eine weitere Tabellenzeile hinzu. 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 richtet das Gerät dynamische VLANs ein:
  – *MRP*: Wenn Sie den Ring-Ports ein noch nicht eingerichtetes VLAN zuweisen, dann richtet das Gerät dieses VLAN ein.
  – *MVRP*: Das Gerät richtet ein VLAN auf Grundlage der Meldungen benachbarter Geräte ein.

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

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen.

Im Feld *VLAN-ID* legen Sie die VLAN-ID fest.

Löschen

Entfernt die ausgewählte Tabellenzeile.

VLAN-ID

ID des VLANs.

Das Gerät unterstützt bis zu 128 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*. Siehe Dialog *Netzsicherheit > 802.1X*.
- *permanent*
  VLAN eingerichtet durch den Benutzer.
  oder
  VLAN eingerichtet durch Funktion *MRP*. Siehe Dialog *Switching > L2-Redundanz > MRP*.
  Wenn Sie die Einstellungen im nichtflüchtigen 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.

Name

Legt die Bezeichnung des VLANs fest.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..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. Andernfalls brechen die Verbindungen zum Management des Geräts ab, sobald Sie die Änderungen anwenden. Der Zugriff auf das Management des Geräts ist dann ausschließlich mittels Command Line Interface über die serielle Verbindung 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 inaktiver Funktion *VLAN-Unaware Modus* Datenpakete vermittelt, 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).
- Die VLAN-ID im VLAN-Tag des Datenpakets unterscheidet sich von der VLAN-ID des Ports.

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

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des Ports.

Port VLAN-ID

Legt die VLAN-ID fest, welche das Gerät den empfangenen Datenpaketen zuweist, die kein VLAN-Tag enthalten.

Voraussetzungen:
- In Spalte *Akzeptierte Datenpakete* ist der Wert `admitAll` festgelegt.

Mögliche Werte:
- `1..4042` (Voreinstellung: `1`)
  Ein bereits eingerichtetes VLAN

Wenn Sie die Funktion *MRP* verwenden und den Ring-Ports kein VLAN zugewiesen ist, legen Sie hier für die Ring-Ports den Wert `1`fest. Andernfalls weist das Gerät den Ring-Ports den Wert automatisch zu.

Akzeptierte Datenpakete

Legt fest, ob der Port empfangene Datenpakete ohne VLAN-Tag überträgt oder verwirft.

Mögliche Werte:
- `admitAll` (Voreinstellung)
  Der Port akzeptiert Datenpakete sowohl mit als auch ohne VLAN-Tag.
- `admitOnlyVlanTagged`
  Der Port akzeptiert ausschließlich Datenpakete, die mit einer VLANID ≥ `1` markiert sind.

Ingress-Filtering

Aktiviert/deaktiviert die Eingangsfilterung.

Mögliche Werte:

- `markiert`
  Die Eingangsfilterung ist aktiv.
  Das Gerät vergleicht die im Datenpaket enthaltene VLAN-ID mit den VLANs, in denen der Port Mitglied ist. Siehe Dialog *Switching > VLAN > Konfiguration*. Stimmt die VLAN-ID im Datenpaket mit einem dieser VLANs überein, vermittelt das Gerät das Datenpaket. Andernfalls verwirft das Gerät das Datenpaket.
- `unmarkiert` (Voreinstellung)
  Die Eingangsfilterung ist inaktiv.
  Das Gerät vermittelt empfangene Datenpakete, ohne die VLAN-ID zu vergleichen. Demzufolge vermittelt das Gerät auch Datenpakete in VLANs, in denen der Port nicht Mitglied ist.

# 5.8.4 VLAN Voice

[ Switching > VLAN > Voice ]

Verwenden Sie die Voice-VLAN-Funktion, um auf einem Port die Sprach- und Datenpakete bezüglich VLAN und/oder Priorität zu trennen. Ein wesentlicher Nutzen von Voice-VLAN ist, bei hoher Auslastung des Ports 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 eingerichteten Voice-VLANs hinzu. Die Mitgliedergruppe enthält entweder „getaggte“ oder „ungetaggte“ Mitglieder. Die Markierung ist abhängig vom Voice-VLAN-Interface-Modus (*vlan*, *dot1p-priority*, *kein*, *untagged*).

Ein weiterer Nutzen der Voice-VLAN-Funktion liegt darin, dass das VoIP-Telefon Informationen zu VLAN-ID und Priorität mittels LLDP-MED vom Gerät erhält. Infolgedessen sendet das VoIP-Telefon Sprachdatenpakete entweder mit VLAN-Tag, mit Prioritätsmarkierung oder ohne VLAN-Tag. 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 *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 16.

Port

Zeigt die Nummer des Ports.

Modus Voice-VLAN

Legt fest, ob der Port empfangene Datenpakete ohne Voice-VLAN-Tag oder mit Voice-VLAN-Prioritätsinformationen überträgt oder verwirft.

Mögliche Werte:

- *ausgeschaltet* (Voreinstellung)
  Deaktiviert die Funktion *Voice* für diese Tabellenzeile.
- *kein*
  Ermöglicht dem IP-Telefon, seine eigene Konfiguration zum Senden von Sprachdatenpaketen ohne VLAN-Tag 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.

Modus Data-Priority

Legt den Trust-Modus für die Datenpakete auf dem jeweiligen Port fest.

Das Gerät verwendet diesen Modus für Datenpakete im Voice-VLAN, wenn es ein VoIP-Telefon und einen PC erkennt, die das gleiche Kabel für die Datenübertragung verwenden.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Datenpakete haben normale Priorität, wenn Sprachdatenpakete auf dem Interface anliegen.
- `unmarkiert`
  Die Datenpakete haben die Priorität `0`, wenn Sprachdatenpakete auf dem Interface anliegen und in Spalte *Modus Voice-VLAN* der Wert *dot1p-priority* festgelegt ist. 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 VLAN-ID fest, auf die sich die Tabellenzeile bezieht. Um Datenpakete an dieses VLAN unter Verwendung dieses Filters zu vermitteln, legen Sie in Spalte *Modus Voice-VLAN* den Wert `vlan` fest.

Mögliche Werte:

- `1..4042` (Voreinstellung: `0`)

Priorität

Legt die Voice-VLAN-Priorität des Ports fest.

Voraussetzungen:

- In Spalte *Modus Voice-VLAN* ist der Wert `dot1p-priority` festgelegt.

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 Precedence*-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 *Modus Voice-VLAN* auf `dot1p-priority` setzen, benötigen Sprachgeräte eine Authentifizierung.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Wenn die Funktion im Dialog *Netzsicherheit > 802.1X > 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 > Global*.
- `unmarkiert`

# 5.9 L2-Redundanz

[ Switching > L2-Redundanz ]

Das Menü enthält die folgenden Dialoge:

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

# 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 Media Redundancy Protocol (MRP) gemäß IEC 62439 unterstützen.

Die Ringstruktur eines MRP-Rings wandelt sich zurück in eine Linienstruktur, wenn eine Teilstrecke nicht in Betrieb ist. Sie können die maximale Wiederherstellungszeit festlegen.

Das *Ring-Manager*-Gerät schließt die Enden eines Backbones in Linienstruktur zu einem redundanten Ring.

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

### 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.

Nachdem Sie die Parameter für den MRP-Ring eingerichtet haben, schalten Sie hier die Funktion ein.

Mögliche Werte:

- *An*
  Die Funktion *MRP* ist eingeschaltet.
  Nachdem Sie die Geräte im MRP-Ring eingerichtet haben, ist die Redundanz aktiv.
- *Aus* (Voreinstellung)
  Die Funktion *MRP* ist ausgeschaltet.

### Ring-Port 1/Ring-Port 2

Port

Legt den Port fest, der als Ring-Port arbeitet.

Mögliche Werte:

- `<Port-Nummer>`

Funktion

Zeigt den Betriebszustand des Ring-Ports.

Mögliche Werte:

- *forwarding*
  Der Port ist eingeschaltet, Verbindung vorhanden.
- *blocked*
  Der Port ist blockiert, Verbindung vorhanden.
- *ausgeschaltet*
  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 das *Ring-Manager*-Gerät auf den primären Ring-Port zurück.
- `unmarkiert` (Voreinstellung)
  Die Backup-Funktion für *Ring-Port 2* ist deaktiviert. Ist der Ring geschlossen, sendet das *Ring-Manager*-Gerät weiterhin Daten an den sekundären Ring-Port.

### Konfiguration

Ring-Manager

Schaltet die Funktion *Ring-Manager* ein/aus.

Wenn sich an jedem Ende der Linie ein Gerät befindet, dann aktivieren Sie diese Funktion.

Mögliche Werte:

- *An*
  Die Funktion *Ring-Manager* ist eingeschaltet.
  Das Gerät arbeitet als *Ring-Manager*.
  Um unerwartetes Verhalten zu vermeiden, schalten Sie die Funktion nicht auf einem Gerät ein, auf dem die Funktion *RCP* eingeschaltet ist.
- *Aus* (Voreinstellung)
  Die Funktion *Ring-Manager* ist ausgeschaltet.
  Das Gerät arbeitet ausschließlich als *Ring-Client*.

Domänen-Name

Legt den Namen der MRP-Domäne fest, zu der das Gerät gehört.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..255 Zeichen
  Sie können einen beliebigen Namen festlegen. Durch Eingabe eines aussagekräftigen Namens können Sie die Verwaltung von MRP-Domains vereinfachen.

Ring-Rekonfiguration

Legt die max. Umschaltzeit in Millisekunden bei der Rekonfiguration des Rings fest. Diese Einstellung ist ausschließlich dann wirksam, wenn das Gerät als *Ring-Manager* arbeitet.

Mögliche Werte:

- *500ms*
- *200ms* (Voreinstellung)

Kürzere Umschaltzeiten stellen höhere Anforderungen an die Reaktionszeit jedes einzelnen Geräts im Ring. Verwenden Sie kleinere Werte als *500ms* ausschließlich dann, wenn die anderen Geräte im Ring ebenfalls diese kürzere Umschaltzeit unterstützen.

VLAN-ID

Legt die VLAN-ID fest, die Sie den Ring-Ports zuweisen.

Mögliche Werte:

- `0` (Voreinstellung)
  Kein VLAN zugewiesen.
  Weisen Sie im Dialog *Switching > VLAN > Konfiguration* für VLAN `1` den Ring-Ports den Wert `U` zu.
- `1..4042`
  VLAN zugewiesen.
  Wenn Sie den Ring-Ports ein nicht vorhandenes VLAN zuweisen, dann richtet das Gerät dieses VLAN automatisch ein. Im Dialog *Switching > VLAN > Konfiguration* fügt das Gerät eine Tabellenzeile für das VLAN hinzu und weist den Ring-Ports den Wert `T`zu.

Advanced-Modus

Aktiviert/deaktiviert den *Advanced-Modus* für schnelle Umschaltzeiten.

Mögliche Werte:

- `markiert` (Voreinstellung)
  *Advanced-Modus* aktiv.
  MRP-fähige Hirschmann-Geräte unterstützen diesen Modus.
- `unmarkiert`
  *Advanced-Modus* inaktiv.
  Wählen Sie diese Einstellung, wenn ein anderes Gerät im Ring keine Unterstützung für diesen Modus bietet.

Domänen-ID

Zeigt eine 16-Byte-Folge in Dezimalschreibweise, welche die MRP-Domäne identifiziert, zu der das Gerät gehört.

### Information

Information

Zeigt den Zustand des Rings.

Mögliche Werte:

- *Redundanz verfügbar. Ring ist geschlossen.*
  Normaler Betrieb. Die Bestandteile des Rings arbeiten wie vorgesehen.
- *Konfigurationsfehler: Ring-Port Verbindung fehlerhaft*
  Das Gerät hat einen Link-Fehler an einem Ring-Port erkannt. Vergewissern Sie sich, dass in den Rahmen *Ring-Port 1* und *Ring-Port 2* der richtige Port gewählt ist.
- *Redundanz nicht verfügbar. Ring ist geöffnet. Prüfe die Ring-Clients.*
  Das Gerät hat keinen Konfigurationsfehler erkannt, jedoch ist keine Redundanz verfügbar.
- *Redundanz nicht verfügbar. Mindestens ein Ring-Port ist deaktiviert.*
  Mindestens ein Ring-Port ist ausgeschaltet. Vergewissern Sie sich, dass beide Ports eingeschaltet sind. Siehe Dialog *Grundeinstellungen > Port*.
- *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 an einem der Ring-Ports.

Zeitpunkt der letzten Ringöffnung

Zeigt den Zeitpunkt (Datum und Uhrzeit), zu dem das Gerät zuletzt einen offenen Ring erkannt hat. Das Feld zeigt einen gültigen Wert, wenn das Gerät als *Ring-Manager* arbeitet.

Anzahl der Ringöffnungen

Zeigt, wie oft das Gerät einen offenen Ring erkannt hat. Das Feld zeigt einen gültigen Wert, wenn das Gerät als *Ring-Manager* arbeitet.

## 5.9.2 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.

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

Das Menü enthält die folgenden Dialoge:

- Spanning Tree Global
- Spanning Tree Port

# 5.9.2.1 Spanning Tree Global

[ 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

Zeigt das für die Funktion *Spanning Tree* verwendete Protokoll:

Mögliche Werte:

- *rstp*
  Das Protokoll RSTP ist aktiv.
  Mit RSTP (IEEE 802.1Q-2005) arbeitet die Funktion *Spanning Tree* auf der darunterliegenden physikalischen Schicht.

### 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` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

### Bridge-Konfiguration

Bridge-ID

Zeigt die *Bridge-Identifikation* des Geräts.

Das Gerät mit dem numerisch niedrigsten Wert für die *Bridge-Identifikation* 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 (2¹⁵)`)

Um das Gerät zur *Root-Bridge* zu machen, weisen Sie dem Gerät den numerisch niedrigsten 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 Rapid Spanning Tree Protocol (RSTP) handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus.

Die Funktion *Spanning Tree* verwendet den Parameter, um den Wechsel zwischen den Zuständen `ausgeschaltet`, `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 eingeben, 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, also 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*.

Die Funktion *Spanning Tree* verwendet den Parameter, um die Gültigkeit von STP-BPDUs in Sekunden festzulegen.

Tx holds

Begrenzt die maximale Übertragungsrate für das Senden von BPDUs.

Mögliche Werte:

- `1..40` (Voreinstellung: `10`)

Sendet das Gerät eine BPDU, inkrementiert 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 generierte 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

Aktiviert/deaktiviert die Funktion *BPDU-Guard* im Gerät.

Mit dieser Funktion hilft das Gerät, das 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 dazu 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

Root-ID

Zeigt die *Bridge-Identifikation* 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 Rapid Spanning Tree Protocol (RSTP) handeln die Bridges Zustandswechsel ohne vorgegebene Verzögerung aus.

Die Funktion *Spanning Tree* verwendet den Parameter, um den Wechsel zwischen den Zuständen `ausgeschaltet`, `discarding`, `learning`, `forwarding` zu verzögern.

Max age

Legt die von der *Root-Bridge* bereitstellte maximal zulässige Astlänge fest, also die Anzahl der Geräte bis zur *Root-Bridge*.

Mögliche Werte:

- `6..40` (Voreinstellung: `20`)

Die Funktion *Spanning Tree* 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`
  Das Gerät übernimmt die Rolle der *Root-Bridge*.
- `1..200000000 (2× 10⁸)`

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>`

# 5.9.2.2 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]

## [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-Redundanz-protokollen 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 16.

Port

Zeigt die Nummer des Ports.

STP aktiv

Aktiviert/deaktiviert die Funktion *Spanning Tree* auf dem Port.

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.
- *ausgeschaltet*
  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.
- *ausgeschaltet*
  Der Port ist inaktiv. Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.

Port-Pfadkosten

Legt die Pfadkosten des Ports fest.

Mögliche Werte:

- `0..200000000 (2× 10⁸)` (Voreinstellung: `0`)

Mit dem Wert `0` ermittelt das Gerät automatisch die Pfadkosten abhängig von der Datenrate des Ports.

Port-Priorität

Legt die Priorität des Ports fest.

Mögliche Werte:

- `0..240` in 16er-Schritten (Voreinstellung: `128`)

Der Wert repräsentiert die ersten 4 Bits der Port-ID.

Empfangene Bridge-ID

Zeigt die *Bridge-Identifikation* 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 erkannten 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 erkannten 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 erkannten 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 Verbindungsaufbau 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 Funktion *BPDU-Guard* 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 16.

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, das 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

Aktiviert/deaktiviert die Überwachung von *Topology Change*-Meldungen auf dem Port. Mit dieser Einstellung hilft das Gerät, das Netz vor Angriffen mit STP-BPDUs zu schützen, die versuchen, die Topologie zu verändern.

Mögliche Werte:

- `markiert`
  Die Überwachung von *Topology Change*-Meldungen ist aktiv.
  - 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 aktivierter Funktion *TCN-Guard*.
    Beispiel: Das Gerät empfängt eine bessere Pfadinformation zur *Root-Bridge*.
- `unmarkiert` (Voreinstellung)
  Die Überwachung von *Topology Change*-Meldungen ist inaktiv.
  Empfängt das Gerät STP-BPDUs mit *Topology Change*-Flag, löscht es die MAC-Adresstabelle (Forwarding Database) des Ports und vermittelt die *Topology Change*-Notifications.

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 *Switching > L2-Redundanz > Spanning Tree > Port* ist bei diesem Port das Kontrollkästchen in Spalte *Admin-Edge Port* markiert.
- Im Dialog *Switching > L2-Redundanz > Spanning Tree > Global* ist die Funktion *BPDU-Guard* 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*.

## 5.9.3 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.

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 Link Aggregation Control Protocol (LACP) nicht 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.

Das Gerät ermöglicht Ihnen, bis zu 2 Link-Aggregation-Gruppen einzurichten.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile für ein LAG-Interface hinzuzufügen oder um 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.

Nachdem Sie ein LAG-Interface eingerichtet haben, fügt das Gerät das LAG-Interface der Tabelle im Dialog *Grundeinstellungen > Port*, Registerkarte *Statistiken* hinzu.

Löschen

Entfernt die ausgewählte Tabellenzeile.

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 nicht betriebsbereit.
- *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.
- `unmarkiert`
  Das LAG-Interface ist inaktiv.

STP aktiv

Aktiviert/deaktiviert die Funktion *Spanning Tree* auf diesem LAG-Interface. Voraussetzung ist, dass im Dialog *Switching > L2-Redundanz > Spanning Tree > Global* die Funktion *Spanning Tree* eingeschaltet ist.

Die Funktion *Spanning Tree* können Sie auch im Dialog *Switching > L2-Redundanz > Spanning Tree > Port* auf den LAG-Interfaces aktivieren/deaktivieren.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *Spanning Tree* ist auf diesem LAG-Interface aktiv.
- `unmarkiert`
  Die Funktion *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.

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* aktiv ist.

Mögliche Werte:

- `1..x` (Voreinstellung: `1`)
  Der Maximalwert ist abhängig von der Anzahl der physischen Ports, die dem LAG-Interface zugewiesen sind.

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. Voraussetzung ist, dass im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
  Wenn das Gerät eine Link-Status-Änderung erkennt, sendet es einen SNMP-Trap.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

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 (2¹⁶-1)`
  Den korrespondierenden Wert für die physischen Ports legen Sie in Spalte *LACP port actor admin key* fest.

Port

Zeigt die Nummer des 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 (2¹⁶-1)`
  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 Einträge.

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 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 IEEE 802.1AX-2014.

# 5.9.4 Link-Backup

[ Switching > L2-Redundanz > Link-Backup ]

Mit Link Backup richten Sie Paare von redundanten Links ein. Jedes Paar besteht aus einem *Primären Port* und einem *Backup-Port*. Der *Primäre Port* leitet die Datenpakete weiter, bis das Gerät einen Fehler ermittelt. Wenn das Gerät einen Fehler auf dem *Primären Port* ermittelt, vermittelt die Link-Backup-Funktion die Datenpakete über den *Backup-Port*.

Der Dialog ermöglicht Ihnen außerdem, eine Fail-Back-Funktion einzurichten. Wenn Sie die Funktion *Fail back* aktivieren und der *Primär-Port* in den Normalbetrieb zurückkehrt, blockiert das Gerät zunächst die Datenpakete am *Backup-Port* und vermittelt die Datenpakete dann an den *Primär-Port*. 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 16.

Schaltflächen

Hinzufügen

Fügt eine Tabellenzeile hinzu.

Löschen

Entfernt die ausgewählte Tabellenzeile.

Primärer Port

Zeigt den *Primären Port* des Interface-Paares. Wenn Sie die Funktion Link-Backup einschalten, ist dieser Port für die Weiterleitung der Datenpakete verantwortlich.

Mögliche Werte:

- Physische Ports

Backup-Port

Zeigt den *Backup-Port*, an den das Gerät die Datenpakete vermittelt, wenn es auf dem *Primären Port* einen Fehler erkennt.

Mögliche Werte:

- Physische 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, Weiterleitung der Datenpakete.
- *blocking*
  Der Link ist vorhanden, keine Abschaltung, keine Weiterleitung der Datenpakete.
- *down*
  Das Kabel ist ausgesteckt, der Port ist ausgeschaltet, die Verbindung auf dem Port ist unterbrochen, oder eine Funktion im Gerät hat den Port ausgeschaltet.
- *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, Weiterleitung der Datenpakete.
- *blocking*
  Der Link ist vorhanden, keine Abschaltung, keine Weiterleitung der Datenpakete.
- *down*
  Das Kabel ist ausgesteckt, der Port ist ausgeschaltet, die Verbindung auf dem Port ist unterbrochen, oder eine Funktion im Gerät hat den Port ausgeschaltet.
- *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 der 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 die Datenpakete 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 der 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 Datenpakete entsprechend der Paar-Konfiguration weiter.
- `unmarkiert` (Voreinstellung)
  Das Link-Backup-Paar ist deaktiviert. Die Ports leiten die Datenpakete entsprechend den Grundeinstellungen weiter.

### Erstellen

Primärer Port

Legt den *Primären Port* des Backup-Interface-Paares fest. Im Normalbetrieb ist dieser Port verantwortlich für die Weiterleitung der Datenpakete.

Mögliche Werte:

- Physische Ports

Backup-Port

Legt den *Backup-Port* fest, an den das Gerät die Datenpakete vermittelt, wenn es auf dem *Primären Port* einen Fehler ermittelt.

Mögliche Werte:

- Physische Ports außer dem Port, den Sie als *Primären Port* festlegen.

# 6 Diagnose

Das Menü enthält die folgenden Dialoge:
- Statuskonfiguration
- System
- Syslog
- Ports
- LLDP
- Bericht

## 6.1 Statuskonfiguration

[ 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 *Geräte-Status*.

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:

- *ok*
- *error*
  Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen.

### 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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
  Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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 den festgelegten oberen Schwellenwert überschreitet oder den festgelegten unteren Schwellenwert unterschreitet, wechselt der Wert im Rahmen *Geräte-Status* auf *error*.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Schwellenwerte für die Temperatur 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 Ethernet-Module.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn Sie ein Ethernet-Modul aus dem Gerät entfernen.
  Weiter unten haben Sie die Möglichkeit, die zu überwachenden Ethernet-Module einzeln auszuwählen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Externer Speicher wurde entfernt

Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers (`ENVM`).

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn Sie den aktiven externen Speicher (`ENVM`) 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 (`ENVM`).

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 (`ENVM`).
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Ring-Redundanz

Aktiviert/deaktiviert die Überwachung der Ringredundanz.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  In folgenden Situationen wechselt der Wert im Rahmen *Geräte-Status* auf `error`:
  - Das Gerät arbeitet als Redundanz-Manager. Die Redundanzfunktion des Geräts verwendet die alternative Verbindung. Eine Redundanzreserve ist nicht länger vorhanden.
  - Das Gerät als Ringteilnehmer hat einen Fehler in seinen Ringredundanz-Einstellungen erkannt.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Netzteil 1
Netzteil 2

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 Ethernet-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 16.

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 *Verbindungs-fehler* markieren.

## [Status]

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Zeitstempel

Zeigt Datum und Uhrzeit des Ereignisses.

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:

- *ok*
- *error*
  Das Gerät zeigt diesen Wert, um einen ermittelten Fehler für eine der überwachten Parameter anzuzeigen.

#### 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. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
  Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.
- `unmarkiert` (Voreinstellung)
  Das Senden von SNMP-Traps ist inaktiv.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 16.

Passwort-Voreinstellung unverändert

Aktiviert/deaktiviert die Überwachung des Passworts für das lokal eingerichtete Benutzerkonto `admin`.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie für das Benutzerkonto `admin` das voreingestellte Passwort unverändert verwenden.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Das Passwort legen Sie fest im Dialog *Gerätesicherheit > Benutzerverwaltung*.

Min. Passwort-Länge kürzer als 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 1 über die serielle Schnittstelle möglich

Aktiviert/deaktiviert die Überwachung der Option zum Starten des System Monitors 1.

Wenn aktiv, können Sie den System Monitor 1 über die serielle Verbindung beim Systemstart starten.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Option zum Starten des System Monitors 1 aktivieren.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.
  Der Wert im Rahmen *Sicherheits-Status* bleibt unverändert, wenn Sie die Option zum Starten des System Monitors 1 aktivieren.

Sie aktivieren/deaktivieren die Option zum Starten des System Monitors 1 im Dialog*Diagnose > System > Selbsttest*.

Speichern des Konfigurationsprofils auf dem externen Speicher möglich

Aktiviert/deaktiviert die Überwachung des Konfigurationsprofils im externen Speicher (`ENVM`).

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 (`ENVM`) aktiv ist.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Das Speichern des Konfigurationsprofils im externen Speicher (*Grundeinstellungen > Externer Speicher*) aktivieren/deaktivieren Sie im Dialog `ENVM`.

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 > Netzwerk > Global* ein/aus.

Unverschlüsselte Konfiguration vom externen Speicher laden

Aktiviert/deaktiviert die Überwachung des Ladens unverschlüsselter Konfigurationsprofile vom externen Speicher (*ENVM*).

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 (*ENVM*) zu laden.
  Der Rahmen *Sicherheits-Status* im Dialog *Grundeinstellungen > System* zeigt einen Alarm, wenn folgende Voraussetzungen erfüllt sind:
  - Das im externen Speicher (*ENVM*) gespeicherte Konfigurationsprofil ist unverschlüsselt. und
  - Die Spalte *Konfigurations-Priorität* im Dialog *Grundeinstellungen > Externer Speicher* hat den Wert `erste`.
- `unmarkiert`
  Die Überwachung ist inaktiv.

IEC 61850/MMS aktiv

Aktiviert/deaktiviert die Überwachung der Funktion *IEC 61850/MMS*.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *IEC 61850/MMS* einschalten.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion *IEC 61850/MMS* schalten Sie im Dialog *Erweitert > Industrie-Protokolle > IEC 61850/MMS*, Rahmen *Funktion*ein/aus.

Self-signed HTTPS-Zertifikat vorhanden

Aktiviert/deaktiviert die Überwachung des digitalen Zertifikats des HTTP-Servers.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn der HTTPS-Server ein selbst generiertes 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.

Secure Boot ist inaktiv

Aktiviert/deaktiviert die Überwachung der Funktion Secure Boot.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Bis Sie die Funktion Secure Boot aktivieren, wird im Rahmen *Sicherheits-Status* weiterhin der Wert `error` angezeigt. Sobald aktiviert, wechselt der Wert `ok`.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Funktion Secure Boot aktivieren Sie im Dialog *Grundeinstellungen > Software*, Rahmen *Software-Update*.

Support-Modus ist aktiv

Aktiviert/deaktiviert die Überwachung der Funktion Support-Modus.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Überwachung ist aktiv.
  Wenn sich der Wert im Rahmen *Sicherheits-Status* aufgrund dieser Einstellung in `error` ändert, wenden Sie sich an den Hersteller.
- `unmarkiert`
  Die Überwachung ist inaktiv.

## [Port]

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 16.

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 16.

Zeitstempel

Zeigt Datum und Uhrzeit des Ereignisses.

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 in der Dropdown-Liste *Modus* der Eintrag *Manuelle Einstellung* ausgewählt ist.

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. Voraussetzung ist, dass im Dialog *Diagnose* > Statuskonfiguration > *Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
  Das Gerät sendet einen SNMP-Trap, wenn es an den überwachten Funktionen eine Änderung erkennt.
- unmarkiert (Voreinstellung)
  Das Senden von SNMP-Traps ist inaktiv.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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 den festgelegten oberen Schwellenwert überschreitet oder den festgelegten unteren Schwellenwert unterschreitet.
- `unmarkiert`
  Die Überwachung ist inaktiv.

Die Schwellenwerte für die Temperatur 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 Ethernet-Module.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn Sie ein Ethernet-Modul aus dem Gerät entfernen.
  Weiter unten haben Sie die Möglichkeit, die zu überwachenden Ethernet-Module einzeln auszuwählen.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Externer Speicher wurde entfernt

Aktiviert/deaktiviert die Überwachung des aktiven externen Speichers (*ENVM*).

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn Sie den aktiven externen Speicher (*ENVM*) 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 (*ENVM*).

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 (*ENVM*).
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Ring-Redundanz

Aktiviert/deaktiviert die Überwachung der Ringredundanz.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  In folgenden Situationen öffnet der Signalkontakt:
  - Das Gerät arbeitet als Redundanz-Manager. Die Redundanzfunktion des Geräts verwendet die alternative Verbindung. Eine Redundanzreserve ist nicht länger vorhanden.
  - Das Gerät als Ringteilnehmer hat einen Fehler in seinen Ringredundanz-Einstellungen erkannt.
- `unmarkiert` (Voreinstellung)
  Die Überwachung ist inaktiv.

Netzteil 1
Netzteil 2

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 Ethernet-Moduls.

Mögliche Werte:

- `markiert`
  Die Überwachung ist aktiv.
  Der Signalkontakt öffnet, wenn Sie dieses Ethernet-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 16.

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 16.

Zeitstempel

Zeigt Datum und Uhrzeit des Ereignisses.

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 (Forwarding Database). 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 (2³¹-1)` (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 16.

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.

  Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
- `unmarkiert` (Voreinstellung)
  Die Funktion *MAC-Benachrichtigung* ist auf dem Port inaktiv.

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

Status letzte MAC

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 das Senden eines SNMP-Traps als Reaktion auf bestimmte Ereignisse.

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

- *Diagnose > Statuskonfiguration > Gerätestatus*
- *Diagnose > Statuskonfiguration > Sicherheitsstatus*
- *Diagnose > Statuskonfiguration > MAC-Benachrichtigung*

Das Menü enthält die folgenden Dialoge:

- Trap V3 Benutzerverwaltung
- Trap Ziele

# 6.1.5.1 Trap V3 Benutzerverwaltung

[ Diagnose > Statuskonfiguration > Alarme (Traps) > Trap V3 Benutzerverwaltung ]

In diesem Dialog legen Sie die SNMPv3-Trap-Benutzer fest, welche SNMP-Traps an das/die Trap-Ziel(e) senden können. Das Gerät unterstützt verschlüsselte SNMPv3-Traps sowie Authentifizierung für das Senden.

SNMPv3-Trap-Benutzer haben die Berechtigung, SNMPv3-Traps an die festgelegten SNMPv3-Trap-Destinations zu senden.

SNMPv3-Trap-Benutzer sind ausschließlich für das Senden von SNMPv3-Traps an SNMPv3-Trap-Destinations bestimmt. Die SNMPv3-Trap-Benutzer unterscheiden sich von den im Gerät eingerichteten Benutzerkonten. Verwechseln Sie diese nicht. Siehe Dialog *Gerätesicherheit > Benutzerverwaltung*.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen. Das Gerät fügt maximal 10 SNMPv3-Trap-Benutzer mit den Parametern hinzu, die Sie in diesem Fenster festlegen.

- In der Dropdown-Liste *Zu klonender Benutzer* wählen Sie das Benutzerkonto, von dem das Gerät die Authentifizierungseinstellungen klont.
  Wählen Sie obligatorisch eines der im Gerät eingerichteten Benutzerkonten aus. Benutzerkonten für das Gerät richten Sie im Dialog *Gerätesicherheit > Benutzerverwaltung* ein.
- Im Feld *Trap Benutzer Name* legen Sie den Namen für den SNMPv3-Trap-Benutzer fest.
  Mögliche Werte:
  - Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
- In der Dropdown-Liste *Trap Benutzer Auth Protokoll* wählen Sie den Algorithmus, welchen das Gerät für diesen Benutzer zur Authentifizierung der SNMPv3-Traps anwendet. Die verfügbaren Werte sind abhängig vom Algorithmus, welcher für den zu klonenden Benutzer festgelegt ist.
  Mögliche Werte:
  - *kein* (Voreinstellung)
    Keine Authentifizierung.
  - *hmacmd5*
    MD5
  - *hmacsha*
    SHA-1
  - *hmacsha256*
    SHA-256
- Im Feld *Trap Benutzer Auth Passwort* legen Sie das Passwort fest, welches das Gerät zusammen mit dem gewählten Algorithmus für die Authentifizierung der SNMPv3-Traps anwendet. Erforderlich, wenn in der Dropdown-Liste *Trap Benutzer Auth Protokoll* ein anderer Eintrag als *kein* ausgewählt ist.
  Mögliche Werte:
  - Alphanumerische ASCII-Zeichenfolge mit 8..64 Zeichen

- In der Dropdown-Liste *Trap Benutzer Priv Protokoll* wählen Sie den Algorithmus, welchen das Gerät für diesen Benutzer zur Verschlüsselung der SNMPv3-Traps anwendet. Voraussetzung ist, dass in der Dropdown-Liste *Trap Benutzer Auth Protokoll* ein anderer Eintrag als *kein* ausgewählt ist. Die verfügbaren Werte sind abhängig vom Algorithmus, welcher für den zu klonenden Benutzer festgelegt ist.
  Mögliche Werte:
  - *kein* (Voreinstellung)
    Keine Verschlüsselung.
  - *des*
    DES
  - *aesCfb128*
    *AES-128*
  - *aesCfb256*
    *AES-256*
- Im Feld *Trap Benutzer Priv Passwort* legen Sie das Passwort fest, welches das Gerät zusammen mit dem gewählten Algorithmus zum Verschlüsseln der SNMPv3-Traps anwendet. Erforderlich, wenn in der Dropdown-Liste *Trap Benutzer Priv Protokoll* ein anderer Eintrag als *kein* ausgewählt ist.
  Mögliche Werte:
  - Alphanumerische ASCII-Zeichenfolge mit 8..64 Zeichen

Wenn Sie die Schaltfläche *Ok* klicken, fügt das Gerät die Tabellenzeile für den SNMPv3 Trap-Benutzer hinzu. Wenn Sie in der Dropdown-Liste *Trap Benutzer Auth Protokoll* oder *Trap Benutzer Priv Protokoll* einen anderen Eintrag als *kein* gewählt haben, öffnet sich zunächst das Fenster *Anmeldeinformationen*. Dann geben Sie das/die erforderliche(n) Passwort(e) ein. Auch wenn Sie ein falsches Passwort eingeben, fügt das Gerät den SNMPv3-Trap-Benutzer hinzu. Wenn das Gerät SNMPv3-Traps sendet, kann das Trap-Ziel diese jedoch nicht entschlüsseln.

 Löschen

Entfernt die ausgewählte Tabellenzeile.

SNMPv3 Notification Benutzer

Zeigt den Namen des SNMPv3-Trap-Benutzers.

Authentifizierung

Zeigt das Protokoll für das Senden von SNMPv3-Traps mit Authentifizierung im Kontext des SNMPv3-Trap-Benutzers.

Auth Passwort

Legt das Authentifizierungspasswort des SNMPv3-Trap-Benutzers fest. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Um das Passwort zu ändern, klicken Sie in das betreffende Feld. Das Gerät öffnet einen Dialog zum Eingeben/Ändern des Passworts, siehe „[Dialog zur Eingabe/Änderung des Passworts]" auf Seite 295.

Um das Passwort zu ändern, fügen Sie einen weiteren SNMPv3-Trap-Benutzer hinzu und löschen dann den bestehenden.

Privacy

Zeigt das Protokoll, welches das Gerät für diesen Benutzer zur Verschlüsselung der SNMPv3-Traps verwendet.

Priv Passwort

Legt das Datenschutz- (Verschlüsselungs-) Passwort des SNMPv3-Trap-Benutzers fest. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Um das Passwort zu ändern, klicken Sie in das betreffende Feld. Das Gerät öffnet einen Dialog zum Eingeben/Ändern des Passworts, siehe „[Dialog zur Eingabe/Änderung des Passworts]" auf Seite 295.

Um das Passwort zu ändern, fügen Sie einen weiteren SNMPv3-Trap-Benutzer hinzu und löschen dann den bestehenden.

Status Benutzer

Zeigt den Status des SNMPv3-Trap-Benutzers.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Der SNMPv3-Trap-Benutzer ist aktiv.
- `unmarkiert`
  Der SNMPv3-Trap-Benutzer ist inaktiv.

## [Dialog zur Eingabe/Änderung des Passworts]

Wenn Sie ein Passwortfeld klicken, zeigt das Gerät einen Dialog zur Passwortänderung. In diesem Dialog können Sie ein gültiges Passwort festlegen, indem er Ihnen die erforderlichen Passwortkriterien zeigt. Der Dialog gibt Ihnen Rückmeldung darüber, welche Kriterien das aktuell eingegebene Passwort erfüllt.

- Der Dialog prüft, ob das eingegebene Passwort die erforderliche Passwortlänge erfüllt.
- Der Dialog überprüft, ob das eingegebene Passwort nur zulässige Zeichen enthält.
- Der Dialog hilft, Tippfehler beim Passwort zu vermeiden, indem er Sie auffordert, das Passwort zweimal einzugeben.

Passwortlänge (min.):

Dieses Dialogelement zeigt die erforderliche Mindestlänge des Passworts.

- Wenn das aktuell eingegebene Passwort die erforderliche Mindestlänge erfüllt:
  - Das Gerät zeigt links neben dem Text *Passwortlänge (min.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Passwortlänge (min.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Passwortlänge (max.):

Dieses Dialogelement zeigt die erforderliche Maximallänge des Passworts.

- Wenn das Passwort die erforderliche Maximallänge erfüllt:
  - Das Gerät zeigt links neben dem Text *Passwortlänge (max.):* ein grünes Häkchen
  - Das Gerät zeigt den Text *Passwortlänge (max.):* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Enthält nur erlaubte Zeichen

Dieses Dialogelement zeigt, ob das Passwort nur zulässige Zeichen enthält:

- Falls ja:
  - Das Gerät zeigt links neben dem Text *Enthält nur erlaubte Zeichen* ein grünes Häkchen
  - Das Gerät zeigt den Text *Enthält nur erlaubte Zeichen* in grüner Schrift.
- Andernfalls:
  - Das Gerät zeigt links neben dem Text ein rotes Ausrufezeichen (!) an.
  - Das Gerät zeigt den Text in roter Schrift.

Neues Passwort

Geben Sie hier das neue oder geänderte Passwort ein. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Das in diesem Feld eingegebene Passwort muss mit dem Wert im Feld *Passwort bestätigen* übereinstimmen.

Passwort bestätigen

Bestätigt das neue oder geänderte Passwort. Das Gerät zeigt ●●●●● (Punkte) anstelle des Passworts.

Das in diesem Feld eingegebene Passwort muss mit dem Wert im Feld *Neues Passwort* übereinstimmen.

Ok

Das Klicken dieser Schaltfläche schließt den Dialog und übernimmt das Passwort in das Passwortfeld des darunterliegenden Dialogs, vorausgesetzt:

- Das aktuell eingegebene Passwort erfüllt alle erforderlichen Kriterien.
- Der *Passwort bestätigen*-Wert stimmt mit dem *Neues Passwort*-Wert überein.

Abbrechen

Das Klicken dieser Schaltfläche bricht den Dialog ab und lässt das Passwort im darunterliegenden Dialog unverändert.

# 6.1.5.2 Trap Ziele

[Diagnose > Statuskonfiguration > Alarme (Traps) > Trap Ziele]

In diesem Dialog legen Sie die Trap-Ziele fest, an die das Gerät SNMP-Traps sendet.

Für SNMPv3 gelten die folgenden Kriterien:
- Das Gerät sendet SNMPv3-Traps an das für den betreffenden SNMPv3-Trap-Benutzer festgelegte Trap-Ziel.
- Das Gerät unterstützt maximal 10 Trap-Ziele für SNMPv3.

### Funktion

Funktion

Schaltet das Senden von SNMP-Traps ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Das Senden von SNMP-Traps ist eingeschaltet.
- *Aus*
  Das Senden von SNMP-Traps ist ausgeschaltet.

### SNMPv1/v2-Trap-Community

Name

Legt die Community-Zeichenfolge fest, die das Gerät in jedem SNMPv1/v2-Trap zur Authentifizierung an das Trap-Ziel sendet.

Mögliche Werte:

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

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen



Hinzufügen

Öffnet das Fenster *Erstellen*, um eine Tabellenzeile hinzuzufügen. Damit richten Sie ein Trap-Ziel im Gerät ein.

- Im Feld *Name* legen Sie einen Namen für das Trap-Ziel fest.
  Mögliche Werte:
  - Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen
- In der Dropdown-Liste *Typ* wählen Sie die SNMP-Version, die das Gerät zum Senden von SNMP-Traps an das Trap-Ziel verwendet.
  Mögliche Werte:
  - `V1`
    SNMP Version 1
    Verwenden Sie diese Einstellung nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  - `V3`
    SNMP Version 3
- Im Feld *Adresse* legen Sie IP-Adresse und Port des Trap-Ziels fest.
  Mögliche Werte:
  - `<IPv4-Adresse>:<Port>`
    Wenn Sie keinen Port festlegen, fügt das Gerät automatisch den Port `162` dem Trap-Ziel hinzu.
- In der Dropdown-Liste *SNMPv3 Trap Benutzer* wählen Sie den SNMPv3-Trap-Benutzer, in dessen Kontext das Gerät SNMPv3-Traps an das Trap-Ziel sendet.
  Voraussetzung ist, dass Sie in der Dropdown-Liste *Typ* den Eintrag `V3` wählen.
  Sie wählen einen der Benutzer, die Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps) > Trap V3 Benutzerverwaltung* eingerichtet haben.
- In der Dropdown-Liste *Sicherheitsstufe* wählen Sie, ob das Gerät die SNMPv3-Traps verschlüsselt sendet und ob vor dem Senden eine Authentifizierung erforderlich ist.
  Voraussetzung ist, dass Sie in der Dropdown-Liste *Typ* den Eintrag `V3` wählen.
  Mögliche Werte:
  - *`noAuthNoPriv`*
    Das Gerät sendet unverschlüsselte SNMPv3-Traps ohne Authentifizierung.
    Verwenden Sie diese Einstellung nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  - *`authNoPriv`*
    Das Gerät sendet unverschlüsselte SNMPv3-Traps.
    Der Benutzer muss sich vor dem Senden von SNMPv3-Traps authentifizieren.
  - *`authPriv`*
    Das Gerät sendet verschlüsselte SNMPv3-Traps.
    Der Benutzer muss sich vor dem Senden von SNMPv3-Traps authentifizieren.



Löschen

Entfernt die ausgewählte Tabellenzeile.

Name

Zeigt den Namen, den Sie für das Trap-Ziel (Trap-Host) festgelegt haben.

SNMP Protokoll

Zeigt die SNMP-Version, die das Gerät verwendet, um SNMP-Traps an das Trap-Ziel zu senden.

Adresse

Legt IP-Adresse und Port des Trap-Ziels (Trap-Host) fest.

Mögliche Werte:

- `<IPv4-Adresse>:<Port>`
  Wenn Sie keinen Port festlegen, fügt das Gerät automatisch den Port `162` dem Trap-Ziel hinzu.

SNMPv3 Trap Benutzer

Legt den SNMPv3-Trap-Benutzer fest, den das Gerät verwendet, um SNMPv3-Traps an das Trap-Ziel zu senden.

Sie wählen einen der SNMPv3-Trap-Benutzer, die Sie im Dialog *Diagnose* > *Statuskonfiguration* > Alarme (Traps) > *Trap V3 Benutzerverwaltung* eingerichtet haben.

Sicherheitsstufe

Legt fest, ob das Gerät die SNMPv3-Traps verschlüsselt sendet und ob vor dem Senden eine Authentifizierung erforderlich ist.

Mögliche Werte:

- *noAuthNoPriv*
  Das Gerät sendet unverschlüsselte SNMPv3-Traps ohne Authentifizierung.
  Verwenden Sie diese Einstellung nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
- *authNoPriv*
  Das Gerät sendet unverschlüsselte SNMPv3-Traps.
  Der Benutzer muss sich vor dem Senden von SNMPv3-Traps authentifizieren.
- *authPriv*
  Das Gerät sendet verschlüsselte SNMPv3-Traps.
  Der Benutzer muss sich vor dem Senden von SNMPv3-Traps authentifizieren.

Typ

Zeigt den Typ der Benachrichtigung.

Aktiv

Aktiviert/deaktiviert das Senden von SNMP-Traps an das Trap-Ziel.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Das Senden von SNMP-Traps an das Trap-Ziel ist aktiv.
- `unmarkiert`
  Das Senden von SNMP-Traps an dieses 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

Speichert die HTML-Seite auf Ihrem PC mittels Webbrowser-Dialog.

# 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 16.

Flash-Region

Zeigt den Namen des Parameters, zum Beispiel für den betreffenden Speicherbereich.

Beschreibung

Zeigt eine Beschreibung für den Parameter.

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, welche die Leistungsfähigkeit der Kommunikation zwischen dem Gerät und den erkannten Nachbargeräten beeinflussen.

**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 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.

### Konfiguration

Starte Konfigurations-Check...

Startet die Prüfung und aktualisiert 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.

### Information

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.

Wenn im Gerät mehr als 39 VLANs eingerichtet sind, dann zeigt der Dialog fortwährend 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.

Information

Zeigt, wie viele Abweichungen des Levels `INFORMATION` das Gerät beim Konfigurations-Check erkannt hat.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.



Zeigt detaillierte Informationen über die erkannten Abweichungen im Bereich unterhalb der Tabellenzeile. Um die detaillierten Informationen wieder auszublenden, klicken Sie die Schaltfläche  . Wenn Sie das Symbol in der Kopfzeile der Tabelle klicken, blenden Sie die detaillierten Informationen für jede Tabellenzeile ein oder aus.

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.
- *Warnung*
  Die Leistungsfähigkeit der Kommunikation zwischen den beiden Geräten kann beeinträchtigt sein.
- *Fehler*
  Die Kommunikation zwischen den beiden Geräten ist beeinträchtigt.

Nachricht

Zeigt eine Zusammenfassung der erkannten Abweichungen.

# 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.

### Information

Konflikt erkannt

Zeigt, ob gegenwärtig ein Adresskonflikt besteht.

Mögliche Werte:

- `markiert`
  Das Gerät erkennt einen Adresskonflikt.
- `unmarkiert`
  Das Gerät erkennt keinen Adresskonflikt.

### Konfiguration

Erkennung 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 *Erkennung Verzögerung [ms]* festgelegten zeitlichen Abstand. Empfängt das Gerät auf diese Datenpakete eine Antwort, liegt ein Addresskonflikt vor.
  - Erkennt das Gerät keinen Adresskonflikt, sendet es 2 Gratuitous-ARP-Datenpakete als Announcement. Diese Datenpakete sendet das Gerät auch dann, wenn die Adresskonflikt-Erkennung ausgeschaltet ist.
  - Ist die IP-Adresse bereits im Netz vorhanden, wechselt das Gerät zurück zu den zuvor verwendeten IP-Parametern (falls möglich).
    Erhält das Gerät seine IP-Parameter von einem DHCP-Server, sendet es eine DHCPDECLINE-Nachricht an den DHCP-Server zurück.
  - Das Gerät prüft jeweils nach der im Feld *Rückfallverzögerung [s]* festgelegten Zeit, ob der Adresskonflikt weiterhin besteht. Erkennt das Gerät 10 Adresskonflikte nacheinander, verlängert es die Wartezeit bis zur nächsten Prüfung auf 60 s.
  - Sobald das Gerät den Adresskonflikt behebt, geht das Management des Geräts wieder ans Netz.
- *passiv*
  Passive Adresskonflikt-Erkennung. Das Gerät analysiert den Datenstrom 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 *Erkennung 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.

Erkennung 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` (Voreinstellung)
  Das Senden von SNMP-Traps ist aktiv. Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
  Das Gerät sendet einen SNMP-Trap, wenn es einen Adresskonflikt erkennt.
- `unmarkiert`
  Das Senden von SNMP-Traps ist inaktiv.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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.

Das Gerät kann IPv4 und IPv6-Adressen anzeigen. Bei IPv6 ermittelt das Gerät die Adressen benachbarter Geräte mithilfe des Neighbor Discovery Protocol (NDP).

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

ARP-Tabelle leeren

Löscht die dynamisch eingerichteten Adressen aus der ARP-Tabelle.

Port

Zeigt die Nummer des Ports.

IP-Adresse

Zeigt die IPv4-Adresse oder die IPv6-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:
- Den RAM-Selbsttest aktivieren/deaktivieren, den das Gerät beim Systemstart ausführt.
- Aktiviert/deaktiviert die Option zum Starten des System Monitors 1 während des Systemstarts.
- Festlegen, wie sich das Gerät im verhält, wenn es einen Fehler erkennt.

### 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, den das Gerät während des Systemstarts ausführt.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Der RAM-Speicher-Test ist aktiviert. Während des Systemstarts testet das Gerät den RAM-Speicher.
- `unmarkiert`
  Der RAM-Speicher-Test ist deaktiviert. Dies verkürzt die Startzeit des Geräts.

SysMon1 ist verfügbar

Aktiviert/deaktiviert die Option zum Starten des System Monitors 1 während des Systemstarts.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Während des Systemstarts zeigt das Startmenü den Eintrag System Monitor 1.
  Um den System Monitor 1 tatsächlich zu starten, versetzen Sie das Gerät in den Recovery-Modus.
- `unmarkiert`
  Während des Systemstarts zeigt das Startmenü keinen Eintrag System Monitor 1.
  Niemand kann den System Monitor 1 starten.

Der System Monitor 1 bietet Funktionen zur Wiederherstellung der Einstellungen des Geräts.

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 mittels Command Line Interface über die serielle Verbindung möglich.
  Um das Gerät wieder über das Netz erreichbar zu machen, starten Sie den System Monitor 1 und setzen die Einstellungen zurück. Nach dem Systemstart verwendet das Gerät die Werkseinstellungen.

### Tabelle

In dieser Tabelle legen Sie fest, wie sich das Gerät verhält, wenn es einen Fehler erkennt.

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen" auf Seite 16.

Ursache

Ursachen erkannter Fehler, 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:

- *logOnly*
  Das Gerät protokolliert den Fehler in der Log-Datei. Siehe Dialog *Diagnose > Bericht > System-Log*.
- *sendTrap*
  Das Gerät sendet einen SNMP-Trap.
  Voraussetzung ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
- *reboot* (Voreinstellung)
  Das Gerät löst einen Neustart aus.

# 6.3 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.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Hinzufügen

Fügt eine Tabellenzeile hinzu.

Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

Wenn Sie eine Tabellenzeile löschen, bleibt eine Lücke in der Nummerierung. Wenn Sie eine Tabellenzeile hinzufügen, schließt das Gerät die erste 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`)
- Gültige IPv6-Adresse

Ziel UDP-Port

Legt den UDP-Port fest, auf dem der Syslog-Server die Log-Einträge erwartet.

Mögliche Werte:

- `1..65535 (2¹⁶-1)` (Voreinstellung: `514`)

Transport Typ

Zeigt den Transporttyp, den das Gerät verwendet, um Ereignisse an den Syslog-Server zu senden.

Mögliche Werte:

- *udp*
  Das Gerät sendet die Ereignisse über den in Spalte *Ziel UDP-Port* festgelegten UDP-Port.

Min. Schweregrad

Legt den Mindest-Schweregrad der Ereignisse fest. Das Gerät sendet einen Log-Eintrag für Ereignisse mit diesem Schweregrad und mit dringlicheren Schweregraden an den Syslog-Server.

Mögliche Werte:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (Voreinstellung)
- *notice*
- *informational*
- *debug*

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.

Mögliche Werte:

- `markiert`
  Das Gerät sendet Ereignisse zum Syslog-Server.
- `unmarkiert` (Voreinstellung)
  Die Übermittlung der Ereignisse zum Syslog-Server ist deaktiviert.

# 6.4 Ports

[ Diagnose > Ports ]

Das Menü enthält die folgenden Dialoge:

- SFP
- TP-Kabeldiagnose
- Port-Monitor
- Auto-Disable
- Port-Mirroring

## 6.4.1 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 16.

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.

# 6.4.2 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 feststellt, zeigt es auch die geschätzte Entfernung zu der Stelle, an der es das Problem erkannt hat.

Um verlässliche Ergebnisse zu erhalten, verwenden Sie die Funktion *TP-Kabeldiagnose* für Twisted-Pair-Kabel, die mindestens 10 Meter lang sind.

**Anmerkung:**
Dieser Test unterbricht den Datenstrom vorübergehend auf dem betreffenden Port.

### Information

Port

Zeigt die Nummer des Ports.

Starte Kabeldiagnose...

Öffnet das Fenster *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 das Fenster *Port auswählen*.
- *erfolgreich*
  Das Gerät hat einen Test erfolgreich ausgeführt.
- *Fehler*
  Das Gerät hat erkannt, dass der Test unterbrochen wurde.
- *nicht initialisiert*
  Das Gerät hat noch keinen Test ausgeführt.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Kabelpaar

Zeigt das Kabelpaar, auf das sich diese Tabellenzeile 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 inaktiv 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 von einem Kabelende zum anderen oder zu einer Unterbrechung des Kabels.

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.

## 6.4.3 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 16.

#### 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 eine Tabellenzeile, 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 die Überwachung von auf dem Port erkannten 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 erkannte 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 Tabellenzeile 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 ist, dass im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* die Funktion *Alarme (Traps)* eingeschaltet und mindestens ein Trap-Ziel festgelegt ist.
- *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 16.

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 16.

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 Rate erkannter Fragmentfehler.
- 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 16.

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 Rate erkannter Fragmentfehler (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 (10⁶)` (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-Schwellenwerte.
- 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 einen Port nicht, wenn der Port in einer der folgenden Rollen arbeitet:
- Mitglied einer Link-Aggregation-Gruppe

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des Ports.

Typ

Legt den Typ der Datenpakete fest, den das Gerät beim Überwachen der Last auf dem Port berücksichtigt.

Mögliche Werte:

- *alle*
  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.

Einheit

Legt die Einheit der Datenrate fest.

Mögliche Werte:

- *pps* (Voreinstellung)
  Pakete pro Sekunde
- *kbps*
  Kbit pro Sekunde
  Voraussetzung ist, dass in Spalte *Typ* der Wert *alle* festgelegt ist.

Unterer Schwellenwert

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 (10⁷)` (Voreinstellung: `0`)

Oberer Schwellenwert

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 (10⁷)` (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 16.

Port

Zeigt die Nummer des Ports.

10M 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.

10M 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.

100M 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.

100M 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.

1G 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.

# 6.4.4 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 16.

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 eine Tabellenzeile, 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 (2³²-1)`
  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*.
- `DOT1S`
  *BPDU-Guard*
  Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.

Grund

Zeigt den überwachten Parameter, der zum Ausschalten des Ports geführt hat.

Mögliche Werte:

- *`kein`*
  Kein überwachter Parameter.
  Der Port ist eingeschaltet.
- *`Link-Änderungen`*
  Zu viele Linkänderungen. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Link-Änderungen*.
- *`CRC-/Fragment Fehler`*
  Zu viele CRC-/Fragmentfehler erkannt. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *CRC/Fragmente*.
- *`Duplex-Mismatch Erkennung`*
  Duplex-Mismatch erkannt. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Global*.
- *`BPDU-Rate`*
  STP-BPDUs empfangen. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- *`MAC-basierte Port-Sicherheit`*
  Zu viele Datenpakete von unerwünschten Absendern. Siehe Dialog *Netzsicherheit > Port-Sicherheit*.

- *Überlast-Erkennung*
  Überlast. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Überlast-Erkennung*.
- *Speed-Duplex*
  Unerlaubte Kombination von Geschwindigkeit und Duplex-Modus erkannt. Siehe Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Link-Speed-/Duplex-Mode Erkennung*.

Aktiv

Zeigt, ob der Port aufgrund einer Überschreitung der Parameter gegenwärtig ausgeschaltet ist.

Mögliche Werte:

- `markiert`
  Der Port ist gegenwärtig ausgeschaltet.
- `unmarkiert`
  Der Port ist eingeschaltet.

## [Status]

Diese Registerkarte zeigt, für welche überwachten Parameter die Funktion *Auto-Disable* aktiv ist.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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 Dialog *Diagnose > Ports > Port-Monitor*.
- *network security*
  Der Parameter gehört zu den Funktionen im Dialog *Netzsicherheit*.
- *l2 redundancy*
  Der Parameter gehört zu den Funktionen im Dialog *Switching > L2-Redundanz*.

Auto-Disable

Zeigt, ob die Funktion *Auto-Disable* für den nebenstehenden Parameter aktiv/inaktiv 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.

# 6.4.5 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 am Ziel-Port angeschlossen Analyzer oder einer *RMON-Probe* 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 im Dialog auf die Voreinstellung zurück und stellt die zuvor angewendeten Einstellungen wieder her.

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
- Uplink-Port, auf welchem ein Redundanzprotokoll auf Schicht-2 aktiv ist

Mögliche Werte:

- `-` (Voreinstellung)
  Kein Ziel-Port ausgewählt.
- `<Port-Nummer>`
  Nummer des Ziel-Ports. Das Gerät kopiert die Datenpakete von den Quell-Ports auf diesen Port.

Auf dem Ziel-Port fügt das Gerät den Datenpaketen, die der Quell-Port sendet, ein VLAN-Tag hinzu. Datenpakete, die der Quell-Port empfängt, sendet der Ziel-Port ohne Änderungen.

**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 überflüssige 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:

- `-` (Voreinstellung)
  Kein Ziel-Port ausgewählt.
- `<Port-Nummer>`
  Nummer des Ziel-Ports. Das Gerät kopiert die Datenpakete von den Quell-Ports auf diesen Port.

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.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Quelle Port

Zeigt die Nummer des Ports.

Aktiv

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.

Auf dem Ziel-Port fügt das Gerät den Datenpaketen, die der Quell-Port sendet, ein VLAN-Tag hinzu. Datenpakete, die der Quell-Port empfängt, sendet der Ziel-Port ohne Änderungen.

Mögliche Werte:

- *`kein`* (Voreinstellung)
  Keine Datenpakete.
- *`tx`*
  Datenpakete, die der Quell-Port sendet.
- *`rx`*
  Datenpakete, die der Quell-Port empfängt.
- *`txrx`*
  Datenpakete, die der Quell-Port sendet.

**Anmerkung:**
Mit der Einstellung *`txrx`* kopiert das Gerät jedes übertragene Datenpaket. 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.

# 6.5 LLDP

[ Diagnose > LLDP ]

Das Gerät ermöglicht Ihnen, Informationen über benachbarte Geräte zu sammeln. Dazu nutzt das Gerät das Link Layer Discovery Protocol (LLDP). Diese Informationen ermöglichen einer Netzmanagement-Station, die Struktur des Netzes darzustellen.

Dieses Menü ermöglicht Ihnen, die Topologie-Erkennung einzurichten und die empfangenen Informationen in Tabellenform anzuzeigen.

Das Menü enthält die folgenden Dialoge:

- LLDP Konfiguration
- LLDP Topologie-Erkennung

## 6.5.1 LLDP Konfiguration

[ Diagnose > LLDP > Konfiguration ]

Dieser Dialog ermöglicht Ihnen, die Topologie-Erkennung für jeden Port einzurichten.

### Funktion

Funktion

Schaltet die Funktion *LLDP* ein/aus.

Mögliche Werte:

- *An* (Voreinstellung)
  Die Funktion *LLDP* ist eingeschaltet.
  Die Topologie-Erkennung mit LLDP ist im 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 (2¹⁵)` (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 das Senden von aufeinanderfolgenden LLDP-Datenpaketen fest, nachdem sich die Einstellungen des Geräts geändert haben.

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 16.

Port

Zeigt die Nummer des Ports.

Funktion

Legt fest, ob der Port LLDP-Datenpakete überträgt.

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.
- *ausgeschaltet*
  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`)

Modus FDB

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 MAC-Adresstabelle (Forwarding Database) für diesen Port vorhanden ist.
- *`beide`*
  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`*.

## 6.5.2 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 gesendeten 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. Diese Informationen ermöglichen einer Netzmanagement-Station, die Struktur des 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 MAC-Adresstabelle (Forwarding Database) 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 angeschlossene Gerät je eine Zeile.

#### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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 MAC-Adresstabelle (Forwarding Database).
- `unmarkiert`
  Das angeschlossene Gerät unterstützt aktiv LLDP.

Nachbar-Adresse

Zeigt die IPv4-Adresse oder den Hostnamen, mit der/dem der Zugriff auf das Management des Nachbargeräts möglich ist.

Nachbar IPv6-Adresse

Zeigt die IPv6-Adresse, mit welcher 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 aktiv 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 16.

Port

Zeigt die Nummer des Ports.

Geräteklasse

Zeigt die Geräteklasse des über Fernverbindung angeschlossen Geräts.

Mögliche Werte:

- *notDefined*
  Das Gerät weist Funktionsmerkmale auf, welche durch keine der *LLDP-MED*-Klassen abgedeckt sind.
- *endpointClass1*
  Das Gerät weist die Funktionsmerkmale *endpointClass1* auf.
- *endpointClass2*
  Das Gerät weist die Funktionsmerkmale *endpointClass2* auf.
- *endpointClass3*
  Das Gerät weist die Funktionsmerkmale *endpointClass3* auf.
- *networkConnectivity*
  Das Gerät verfügt über Anschlussmöglichkeiten für das Netz.

VLAN-ID

Zeigt die Erweiterung für die VLAN-Kennung des entfernten Systems, welches an diesen Port angeschlossen ist (gemäß IEEE 802.3).

- 0
  Pakete mit Prioritäts-Tag
  Ausschließlich die 802.1D-Priorität ist von Bedeutung und das Gerät verwendet die voreingestellte VLAN-Kennung des Eingangs-Ports.
- 1..4042
  gültige Port-VLAN-ID

Priorität

Zeigt den Wert der *802.1D Priority*, welche dem an diesen Port angeschlossenen entfernten System zugeordnet ist.

DSCP

Zeigt den Wert der *Differentiated Service Code Point (DSCP)*, welche dem an diesen Port angeschlossenen entfernten System zugeordnet ist.

Status Unknown-Bit

Zeigt den *Unknown Bit Status* des eingehenden Verkehrs.

Mögliche Werte:

- *true*
  Die Netz-Richtlinie für den festgelegten Anwendungstyp ist gegenwärtig unbekannt. In diesem Fall ignoriert das Gerät die Schicht-2-Priorität und den Wert des Feldes *DSCP*.
- *false*
  Kennzeichnet eine festgelegte Netz-Richtlinie.

Status Tagged-Bit

Zeigt den sog. „Tagged Bit Status“.

Mögliche Werte:

- *true*
  Die Anwendung verwendet ein markiertes VLAN.
- *false*
  Das Gerät greift für die spezifische Anwendung auf unmarkierten VLAN-Betrieb zurück. In diesem Fall ignoriert das Gerät sowohl die VLAN-ID als auch die Schicht-2-Prioritätsfelder. Der DSCP-Wert auf Schicht 3 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.

# 6.6 Bericht

[ Diagnose > Bericht ]

Das Menü enthält die folgenden Dialoge:

- Bericht Global
- Persistentes Ereignisprotokoll
- System-Log
- Audit-Trail

## 6.6.1 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

Generiert ein ZIP-Archiv, das Sie mit dem Webbrowser 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 350.

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 350.

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 generiert, 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 separaten Syslog-Server-Eintrag hinzuzufügen.
- ☐ 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.

Logge SNMP Get-Requests

Schaltet die Protokollierung für den Empfang von *SNMP Get Requests* ein/aus.

Mögliche Werte:

- *An*
  Die Protokollierung ist eingeschaltet.
  Das Gerät protokolliert jeden empfangenen *SNMP Get Request* 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.

Logge SNMP Set-Requests

Schaltet die Protokollierung für den Empfang von *SNMP Set Requests* ein/aus.

Mögliche Werte:

- *An*
  Die Protokollierung ist eingeschaltet.
  Das Gerät protokolliert jeden empfangenen *SNMP Set Request* 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 empfangenen *SNMP Get Requests* protokolliert. Weitere Informationen finden Sie unter „Bedeutung der Ereignis-Schweregrade” auf Seite 350.

Mögliche Werte:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning*
- *notice* (Voreinstellung)
- *informational*
- *debug*

Schweregrad Set-Request

Legt den Schweregrad des Ereignisses fest, welches das Gerät bei empfangenen *SNMP Set Requests* protokolliert. Weitere Informationen finden Sie unter „Bedeutung der Ereignis-Schweregrade” auf Seite 350.

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 350.

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*-Protokoll chronologisch aufgezeichneten Systemereignisse und gespeicherten Änderungen durch die Benutzer. |
| `config.xml` | XML | Enthält die im „ausgewählten“ Konfigurationsprofil gespeicherten Einstellungen des Geräts. Der Dateiname entspricht dem Namen des gegenwärtig „ausgewählten“ Konfigurationsprofils. |
| `defaultconfig.xml` | XML | Enthält die Voreinstellungen des Geräts. |
| `runningconfig.xml` | XML | Enthält die gegenwärtigen Betriebseinstellungen des Geräts. |
| `script` | TEXT | Enthält die Ausgaben des Kommandos `show running-config script`. |
| `supportinfo.html` | HTML | 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 |

| Schweregrad | Bedeutung |
|---|---|
| *error* | Fehlerhafter Zustand |
| *warning* | Warnung |
| *notice* | Signifikanter, normaler Zustand |
| *informational* | Informierende Nachricht |
| *debug* | Debug-Nachricht |

# 6.6.2 Persistentes Ereignisprotokoll

[ Diagnose > Bericht > Persistentes Ereignisprotokoll ]

Das Gerät ermöglicht Ihnen, die Log-Einträge in einer Datei im externen Speicher (*ENVM*) dauerhaft 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 in einer neu generierten Datei.

In der Tabelle zeigt das Gerät die im externen Speicher (*ENVM*) 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 (*ENVM*) ausreichend Speicherplatz verfügbar.

**Anmerkung:**
Vergewissern Sie sich, dass ein externer Speicher (*ENVM*) angeschlossen ist. Um festzustellen, ob ein externer Speicher (*ENVM*) 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 *Externer Speicher wurde entfernt* im Dialog *Diagnose* > Statuskonfiguration > *Gerätestatus*.

### Funktion

Funktion

Schaltet die Funktion *Persistentes Ereignisprotokoll* ein/aus.

Aktivieren Sie die Funktion ausschließlich dann, wenn der externe Speicher (*ENVM*) 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 (*ENVM*).
- *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 in einer neu generierten 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 (*ENVM*) 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 (*ENVM*).

Mögliche Werte:

- *emergency*
- *alert*
- *critical*
- *error*
- *warning* (Voreinstellung)
- *notice*
- *informational*
- *debug*

Ziel der Log-Datei

Legt den Typ des externen Speichers für die Protokollierung fest.

Mögliche Werte:

- *usb*
  Externer USB-Speicher (ACA21/ACA22)

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen

Persistente Log-Datei leeren

Löscht die Log-Dateien aus dem externen Speicher (*ENVM*).

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht.

Mögliche Werte:

- `1..25`

Das Gerät legt diese Nummer automatisch fest.

Dateiname

Zeigt den Dateinamen der Log-Datei im externen Speicher (*ENVM*).

Mögliche Werte:

- `messages`
- `messages.X`

Datei-Größe [Byte]

Zeigt die Größe der Log-Datei im externen Speicher (*ENVM*) in Bytes.

## 6.6.3 System-Log

[ Diagnose > Bericht > System-Log ]

Dieser Dialog zeigt die System-Log-Datei. Das Gerät protokolliert geräteinterne Ereignisse in der System-Log-Datei. Das Gerät behält die protokollierten Ereignisse auch nach einem Neustart bei.

Um die Datei System-Log zu durchsuchen, verwenden Sie die Suchfunktion Ihres Webbrowsers.

Der Dialog ermöglicht Ihnen, eine Kopie der System-Log-Datei auf Ihren Computer herunterzuladen. Das Gerät stellt die herunterzuladende Datei im HTML-Format bereit.

Schaltflächen



Log-Datei speichern

Lädt eine Kopie der System-Log-Datei gemäß den Einstellungen des Webbrowsers auf Ihren Computer herunter.



Log-Datei leeren

Leert die System-Log-Datei im Gerät.

## 6.6.4 Audit-Trail

[ Diagnose > Bericht > Audit-Trail ]

Dieser Dialog zeigt den 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 Webbrowsers.

Das Gerät protokolliert Systemereignisse und schreibende Benutzeraktionen auf das Gerät. Dies ermöglicht Ihnen, nachzuvollziehen, WER WANN WAS im Gerät ändert. Voraussetzung ist, dass Ihrem Benutzerkonto die Zugriffsrolle *auditor* oder *administrator* zugewiesen ist.

Unter anderem protokolliert das Gerät die folgenden Benutzeraktionen:
- Anmeldung eines Benutzers beim Management des Geräts 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 zu vieler aufeinanderfolgender 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 Aktualisierungen der Geräte-Software
- Konfigurationsänderungen mittels HiDiscovery
- Aktualisierung der Geräte-Software und automatisches Konfigurieren des Geräts über den externen Speicher (*ENVM*)
- 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 Zugriff auf den System Monitor 1 während des Systemstarts möglich. Ein Angreifer, der sich physisch Zugriff auf das Gerät verschafft, kann mittels des System Monitors 1 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 Zugriff auf den System Monitor 1. Siehe Dialog *Diagnose > System > Selbsttest*, Kontrollkästchen *SysMon1 ist verfügbar*.

Schaltflächen



Audit-Trail Datei speichern

Speichert die HTML-Seite auf Ihrem PC mittels Webbrowser-Dialog.

# 7 Erweitert

Das Menü enthält die folgenden Dialoge:
- DHCP
- Industrie-Protokolle
- Command Line Interface

## 7.1 DHCP

[ Erweitert > DHCP ]

Das Menü enthält die folgenden Dialoge:
- DHCP Server
- DHCP-L2-Relay

### 7.1.1 DHCP Server

[ Erweitert > DHCP > DHCP Server ]

Das Dynamic Host Configuration Protocol (DHCP) ermöglicht einem Server, den Geräten im Netz (Clients) die IP-Einstellungen zuzuweisen. Der DHCP-Server speichert und weist die verfügbaren IP-Adressen zu, sowie weitere Einstellungen, falls festgelegt.

Der DHCP-Server im Gerät wartet auf dem UDP-Port 67 auf Anfragen und antwortet den Client-Geräten auf dem UDP-Port 68. Wenn das Gerät einen DHCP-Request empfängt, validiert es die zuzuweisende IP-Adresse, bevor es dem anfragenden Client-Gerät die IP-Adresse und andere IP-Einstellungen zuweist.

Das Menü enthält die folgenden Dialoge:
- DHCP-Server Global
- DHCP-Server Pool
- DHCP-Server Lease-Tabelle

# 7.1.1.1 DHCP-Server Global

[Erweitert > DHCP > DHCP Server > Global]

Dieser Dialog ermöglicht Ihnen, die Funktion *DHCP Server* global, oder nach Bedarf pro Port, zu aktivieren..

### Funktion

Funktion

Schaltet die Funktion *DHCP Server* des Geräts global ein/aus.

Mögliche Werte:

- *An*
- *Aus* (Voreinstellung)

### Konfiguration

IP-Probe

Aktiviert/deaktiviert das Prüfen auf eindeutige IP-Adressen. Vor dem Zuweisen einer IP-Adresse sendet das Gerät ein *ICMP Echo Request*-Paket, um zu prüfen, ob diese IP-Adresse bereits im Netz verwendet wird.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *IP-Probe* ist aktiv.
- `unmarkiert`
  Die Funktion *IP-Probe* ist inaktiv.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des physischen Ports, auf dem das Gerät auf DHCP-Anfragen wartet und den Client-Geräten antwortet.

DHCP-Server aktiv

Aktiviert/deaktiviert die Funktion *DHCP Server* auf diesem Port.

Voraussetzung ist, dass Sie die Funktion global aktivieren.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Die Funktion *DHCP Server* ist aktiv.
- `unmarkiert`
  Die Funktion *DHCP Server* ist inaktiv.

# 7.1.1.2 DHCP-Server Pool

[ Erweitert > DHCP > DHCP Server > Pool ]

In diesem Dialog legen Sie die Einstellungen fest, um Client-Geräten, von denen das Gerät eine DHCP-Anfrage erhält, eine bestimmte IP-Adresse zuzuweisen.

Abhängig davon, an welchem physischen Port das anfragende Client-Gerät angeschlossen ist oder in welchem VLAN es Mitglied ist, weist das Gerät eine IP-Adresse aus einem bestimmten Pool (Adressbereich) zu. Die MAC-Adresse des anfragenden Client-Geräts ist ein weiteres Merkmal dafür, aus welchem Pool das Gerät eine IP-Adresse zuweist.

Falls festgelegt, verarbeitet das Gerät weitere Informationen, um dem Client-Gerät eine IP-Adresse aus einem bestimmten Pool zuzuweisen. Dies können zum Beispiel folgende Informationen im DHCP-Request sein:
- *Circuit ID*
- *Class ID*
- *Client ID*
- *Remote ID*

Das Gerät stellt bis zu 128 Pools zur Verfügung. Bis zu 1000 Client-Geräte können ihre IP-Einstellungen vom Gerät erhalten.

Das Gerät verwaltet die IP-Einstellungen in zwei Arten von Pools.
- Statische Pools
  Um einem bestimmten Gerät stets dieselbe IP-Adresse zuzuweisen, verwaltet das Gerät die betreffenden IP-Einstellungen in einem Pool, dessen Adressbereich genau eine IP-Adresse umfasst.
  Statische Pools sind zum Beispiel dazu geeignet, einem Server, NAS oder Drucker eine feste IP-Adresse zuzuweisen.
- Dynamische Pools
  Um IP-Adressen aus einem bestimmten Adressbereich zuzuweisen, verwaltet das Gerät die betreffenden IP-Einstellungen in einem Pool, dessen Adressbereich mehrere IP-Adressen umfasst.
  Dynamische Pools sind zum Beispiel dazu geeignet, Client-Geräten, die zu einem bestimmten VLAN gehören, eine bestimmte IP-Adresse zuzuweisen.

Zusätzlich zu den IP-Einstellungen kann das Gerät den Client-Geräten weitere Parameter (DHCP-Optionen) zuweisen. Das Zuweisen solcher Parameter ist ein eleganter Weg, um die Client-Geräte bereits beim Beziehen ihrer IP-Einstellungen automatisch einzurichten. Das Gerät ermöglicht Ihnen, solche Parameter für jeden Pool festzulegen.

Das Gerät ermöglicht Ihnen, die Boot-Parameter für PXE-konforme Clients festzulegen, damit diese ein Bootloader-Image von einem TFTP-Server herunterladen und starten können. Mögliche Anwendungen sind das Starten einer Installationsumgebung, eines Rettungssystems oder eines Live-Systems über das Netz.

Um die PXE-Boot-Erweiterung für einen bestimmten Pool zu aktivieren, fügen Sie die folgenden Werte zu den Pool-Einstellungen hinzu:
- *Vendor Identifier*
- *Client System Architecture*
- URL zu einer Bootloader-Image-Datei auf einem TFTP-Server

Das Gerät erwartet die Informationen für *Vendor Identifier* und *Client System Architecture* in zusammengefasster Form als *Class Identifier* im DHCP-Optionsfeld 60. Wenn ein PXE-konformes Client-Gerät eine *DHCP Discover*-Nachricht mit einem passenden *Class Identifier* im DHCP-Optionsfeld 60 als Broadcast sendet, antwortet das Gerät mit den im betreffenden Pool festgelegten Einstellungen.

**Anmerkung:**
Das Gerät prüft nicht die Integrität, Authentizität und Verfügbarkeit der TFTP-Server und der Bootloader-Image-Dateien. Verwenden Sie die PXE-Boot-Erweiterung ausschließlich dann, wenn Sie dem Übertragungsnetz vertrauen. Andernfalls können unerwünschtes Verhalten und Sicherheitsrisiken die Folge sein.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Schaltflächen


Hinzufügen

Fügt eine Tabellenzeile hinzu.


Löschen

Entfernt die ausgewählte Tabellenzeile.

Index

Zeigt die Index-Nummer, auf die sich die Tabellenzeile bezieht. Das Gerät weist den Wert automatisch zu, wenn Sie eine Tabellenzeile hinzufügen.

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-Bereich Start

Legt die feste IP-Adresse für einen statischen Pool oder die erste IP-Adresse eines Adressbereichs fest.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)

IP-Bereich Ende

Legt die letzte IP-Adresse eines Adressbereichs fest. Für einen statischen Pool behalten Sie die Voreinstellung bei oder fügen Sie den gleichen Wert ein, der in der Spalte *IP-Bereich Start* festgelegt ist.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)

Port

Legt die Nummer des physischen Ports fest, an den das anfragende Client-Gerät angeschlossen ist.

Mögliche Werte:

- *Alle* (Voreinstellung)
  Das Gerät weist dem anfragenden Client-Gerät eine IP-Adresse zu, unabhängig davon, auf welchem Port das lokale Gerät die DHCP-Anfrage empfängt.
- `<Port-Nummer>`
  Das Gerät weist dem anfragenden Client-Gerät ausschließlich dann eine IP-Adresse zu, wenn das lokale Gerät die DHCP-Anfrage auf dem festgelegten Port empfängt.
  Voraussetzung ist, dass in der Dropdown-Liste in der Spalte *VLAN-ID* der Eintrag `-` ausgewählt ist.

VLAN-ID

Legt das VLAN fest, auf das sich die Tabellenzeile bezieht. Voraussetzung ist, dass in der Dropdown-Liste in der Spalte *Port* der Eintrag *Alle* ausgewählt ist.

Mögliche Werte:

- `-` (Voreinstellung)
- `1..4042`
  Der Wert `1` entspricht dem VLAN, in dem das Management des Geräts in der Voreinstellung erreichbar ist.

MAC-Adresse

Legt die MAC-Adresse des anfragenden Client-Geräts fest.

Mögliche Werte:

- `-` (Voreinstellung)
  Bei der IP-Adresszuweisung ignoriert der Server diese Variable.
- Gültige Unicast-MAC-Adresse
  Legen Sie den Wert mit Doppelpunkt-Trennzeichen fest, zum Beispiel `00:11:22:33:44:55`.

DHCP-Relay

Legt die IP-Adresse des DHCP-Relays fest, über das Clients ihre Anfrage an den DHCP-Server senden. Empfängt das Gerät eine DHCP-Anfrage über ein anderes DHCP-Relay, ignoriert es diese DHCP-Anfrage.

Mögliche Werte:

- – (Voreinstellung)
  Kein DHCP-Relay festgelegt.
- Gültige IPv4-Adresse
  IP-Adresse des DHCP-Relays.

Client-ID

Legt den benutzerdefinierten Bezeichner für den Client anstelle der MAC-Adresse fest.

Mögliche Werte:

- – (Voreinstellung)
  Das Gerät ignoriert den Parameter während der Zuweisung einer IP-Adresse aus dem Pool.
- Folge von hexadezimalen Zeichenpaaren mit 1..254 Paaren, getrennt durch ein Leerzeichen.
  Beispiel: `41 42 43 44 4F`

**Anmerkung:**
Wenn Sie hohe Sicherheitsanforderungen haben und den Clients nicht bedingungslos vertrauen möchten, ziehen Sie in Betracht, die *Remote-ID* oder die *Circuit-ID* statt der *Client-ID* zu benutzen. Die *Remote-ID* und die *Circuit-ID* werden von einem DHCP-Relay eingefügt und sind dadurch schwerer zu fälschen.

Remote-ID

Legt die *Remote-ID* fest. Das DHCP-Relay fügt die *Remote-ID* in die DHCP-Anfrage ein.

Mögliche Werte:

- – (Voreinstellung)
  Das Gerät ignoriert den Parameter während der Zuweisung einer IP-Adresse aus dem Pool.
- Folge von hexadezimalen Zeichenpaaren mit 1..254 Paaren, getrennt durch ein Leerzeichen.
  Beispiel: `41 42 43 44 4F`

Circuit-ID

Legt die *Circuit-ID* fest. Das DHCP-Relay fügt die *Circuit-ID* in die DHCP-Anfrage ein.

Mögliche Werte:

- – (Voreinstellung)
  Das Gerät ignoriert den Parameter während der Zuweisung einer IP-Adresse aus dem Pool.
- Folge von hexadezimalen Zeichenpaaren mit 1..254 Paaren, getrennt durch ein Leerzeichen.
  Beispiel: `41 42 43 44 4F`

Vendor-ID

Legt den *Vendor Identifier* fest. Sofern festgelegt, aktiviert das Gerät die PXE-Boot-Erweiterung für den betreffenden Pool. Verwenden Sie diese Einstellung ausschließlich dann, wenn Sie die Bootloader-Image-Datei über vertrauenswürdige Netze übertragen.

Wenn ein PXE-konformes Client-Gerät eine *DHCP Discover*-Nachricht mit einem passenden *Class Identifier* im DHCP-Optionsfeld 60 als Broadcast sendet, antwortet das Gerät mit den im betreffenden Pool festgelegten Einstellungen.

Ein passender *Class Identifier* enthält folgende Informationen:

- Die hier festgelegte Zeichenfolge.
- Den in Spalte *Client-Architektur* gewählten Wert.

Mögliche Werte:

- `-` (Voreinstellung)
  Die PXE-Boot-Erweiterung für den betreffenden Pool ist inaktiv.
  Das Gerät ignoriert den *Class Identifier* im DHCP-Optionsfeld 60 empfangener *DHCP Discover*-Nachrichten.
- Alphanumerische ASCII-Zeichenfolge mit 1..9 Zeichen

Client-Architektur

Legt die *Client System Architecture* fest. Sofern festgelegt, aktiviert das Gerät die PXE-Boot-Erweiterung für den betreffenden Pool. Verwenden Sie diese Einstellung ausschließlich dann, wenn Sie die Bootloader-Image-Datei über vertrauenswürdige Netze übertragen.

Wenn ein PXE-konformes Client-Gerät eine *DHCP Discover*-Nachricht mit einem passenden *Class Identifier* im DHCP-Optionsfeld 60 als Broadcast sendet, antwortet das Gerät mit den im betreffenden Pool festgelegten Einstellungen.

Ein passender *Class Identifier* enthält folgende Informationen:

- Die in Spalte *Vendor-ID* festgelegte Zeichenfolge.
- Den hier gewählten Wert.

Mögliche Werte:

- `intel-x86pc` (Voreinstellung)
  Intel x86-Architektur, die verbreitete Architektur für die meisten Desktop-PCs und Server
- `nec-pc98`
  NECs PC-98-Serie, eine PC-Serie basierend auf der x86-Architektur
- `efi-itanium`
  Intel Itanium 64-Bit-Prozessorarchitektur mit EFI (Extensible Firmware Interface)
- `dec-alpha`
  DEC-Alpha-Prozessorarchitektur
- `arc-x86`
  Advanced RISC Computing, eine in bestimmten Systemen verwendete Variante der x86-Architektur
- `intel-lean-client`
  Intel-Architektur für Thin Clients
- `efi-ia32`
  Intel-Architektur 32-Bit mit EFI, die üblicherweise auf älteren Intel-Prozessoren (32-Bit-Version von x86) zum Einsatz kommt
- `efi-bc`
  Boot-Continuity-Plattform, die EFI verwendet

- *efi-xscale*
  Intel Xscale, eine Mikroprozessorserie auf Basis der ARM-Architektur, die in Embedded-Systemen zum Einsatz kommt
- *efi-x86-64*
  x86-64-Architektur, auch bekannt als AMD64 oder Intel 64, mit EFI

Hirschmann-Gerät

Aktiviert/deaktiviert die Hirschmann-Multicasts. Wenn das Gerät in diesem IP-Adressbereich lediglich Client-Geräte von Hirschmann bedient, dann aktivieren Sie diese Funktion.

Mögliche Werte:

- `markiert`
  In diesem IP-Adressbereich bedient das Gerät ausschließlich Client-Geräte von Hirschmann. Die Hirschmann-Multicasts sind aktiviert.
- `unmarkiert` (Voreinstellung)
  In diesem IP-Adressbereich bedient das Gerät Client-Geräte unterschiedlicher Hersteller. Die Hirschmann-Multicasts sind deaktiviert.

Konfigurations-URL

Legt den URL zu einer Datei fest, die zusätzliche Einstellungen für die Inbetriebnahme des Client-Geräts enthält.

Wenn Sie in Spalte *Vendor-ID* einen Wert festgelegt und in Spalte *Client-Architektur* einen Wert gewählt haben, verweist der URL auf eine Bootloader-Image-Datei auf einem TFTP-Server. Ein PXE-konformer Client startet mittels der Datei, die unter dem URL bereitgestellt ist.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 0..70 Zeichen
  Wenn Sie dieses Feld leer lassen, lässt das Gerät dieses Optionsfeld in der *DHCP Offer*-Nachricht leer.
  Beispiel: `tftp://192.168.1.10/pfad/datei.name`

Lease-Time [s]

Legt den befristeten Zeitraum in Sekunden fest, für den das Gerät jede IP-Adresse vergibt.

Das Client-Gerät ist dafür verantwortlich, die IP-Adresse vor Ablauf der Frist zu erneuern. Wenn das Client-Gerät seine IP-Adresse nicht rechtzeitig erneuert, gelangt die IP-Adresse zurück in den Adress-Pool.

Mögliche Werte:

- `60..220752000 (2555 d)` (Voreinstellung: `86400`)
- `4294967295 (2³²-1)`
  Verwenden Sie diesen Wert für zeitlich unbegrenzte Vergaben und für Vergaben mittels 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 (Voreinstellung: `0.0.0.0`)

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 (Voreinstellung: `255.255.255.0`)

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 (Voreinstellung: `0.0.0.0`)

NTP-Server

Legt die IP-Adresse eines externen NTP-Servers fest.

Steht hier der Wert `0.0.0.0`, wird der DHCP-Nachricht kein Optionsfeld hinzugefügt.

Mögliche Werte:

- Gültige IPv4-Adresse (Voreinstellung: `0.0.0.0`)

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 (Voreinstellung: `0.0.0.0`)

Hostname

Legt den Hostnamen 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

# 7.1.1.3 DHCP-Server Lease-Tabelle

[ Erweitert > DHCP > DHCP Server > Lease-Tabelle ]

Dieser Dialog zeigt für jeden Port die gegenwärtig zugewiesenen IP-Adressen.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

Port

Zeigt die Nummer des Ports, über den das Gerät, dem die IP-Adresse zugewiesen ist, angeschlossen ist.

IP-Adresse

Zeigt die IP-Adresse, auf welche sich die Tabellenzeile bezieht.

Status

Zeigt die Phase der Vergabe.

Gemäß DHCP-Standard gibt es beim Zuweisen einer IP-Adresse 4 Schritte: Discovery (Client sendet Anfrage an Server), Offer (Server bietet IP-Adresse an), Request (Client fordert IP-Adresse an) sowie Acknowledgement (Server bestätigt IP-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*
  Der 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, wie lange die zugewiesene IP-Adresse noch gültig ist.

Vergeben an MAC-Adresse

Zeigt die MAC-Adresse des Geräts, dem die IP-Adresse zugewiesen ist.

Gateway

Zeigt die Gateway-IP-Adresse des Geräts, dem die IP-Adresse zugewiesen ist.

Client-ID

Zeigt die *Client-ID* des Geräts, dem die IP-Adresse zugewiesen ist.

Remote-ID

Zeigt die *Remote-ID* des Geräts, dem die IP-Adresse zugewiesen ist.

Circuit-ID

Zeigt die *Circuit-ID* des Geräts, dem die IP-Adresse zugewiesen ist.

## 7.2 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-ID oder einer benutzerdefinierten Gerätebeschreibung. Bei einer Client-ID handelt es sich um einen benutzerdefinierten Systemnamen für das Gerät.

Das DHCPv6-Protokoll verwendet einen *Relay-Agenten*, um *Relay-Agent*-Optionen zu DHCPv6-Paketen hinzuzufügen, die zwischen einem Client und einem DHCPv6-Server ausgetauscht werden. Der Lightweight-DHCPv6-Relay-Agent (LDRA) wird im RFC 6221 beschrieben.

Der LDRA verarbeitet 2 Arten von Nachrichten:

- *Relay-Forward*-Nachrichten
  Der *Relay-Agent* leitet *Relay-Forward*-Nachrichten weiter, die eindeutige Informationen über den Client enthalten. Die Informationen über den Client beinhalten die Peer-Adresse, also die IPv6-Link-Local-Adresse des Client und die *Interface-ID*-Information. Die *Interface-ID*-Information, auch *Option 18* genannt, stellt Informationen zur Verfügung, die das Interface identifizieren, über das die Client-Anfrage gesendet wurde.
- *Relay-Reply*-Nachrichten
  Der DHCPv6-Server sendet *Relay-Reply*-Nachrichten. Der *Relay-Agent* überprüft die Nachrichten, um die Informationen aus der ursprünglichen *Relay-Forward*-Nachricht aufzunehmen. Wenn die Informationen gültig sind, dann leitet der *Relay-Agent* das Paket an den Client weiter.

Das Menü enthält die folgenden Dialoge:

- DHCP-L2-Relay Konfiguration
- DHCP-L2-Relay Statistiken

# 7.2.1 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.

Die *Option 82*-Informationen sind auf die DHCPv4-L2-Relay-Funktion beschränkt. Die DHCPv6-L2-Relay-Funktion verwendet *Option 18*-Informationen für den Paketaustausch zwischen dem Client und dem DHCPv6-Server. Das Gerät verwirft DHCPv6-Pakete, die an einem Port empfangen werden, der keine *Option 18*-Informationen enthält.

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

### Funktion

Funktion

Schaltet die DHCP-L2-Relay-Funktion des Geräts global ein oder aus.

Wenn diese Funktion eingeschaltet ist, können DHCPv4-L2-Relay-Funktionen und DHCPv6-L2-Relay-Funktionen gleichzeitig im Gerät betrieben werden.

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 16.

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.
  Das Gerät akzeptiert DHCPv6-Pakete mit *Option 18*-Informationen.
- `unmarkiert` (Voreinstellung)
  Das Gerät verwirft DHCPv4-Pakete, die an einem ungesicherten Port empfangen werden, der *Option 82*-Informationen enthält.
  Das Gerät verwirft DHCPv6-Pakete, die an einem Port empfangen werden, der keine *Option 18*-Informationen enthält.

## [VLAN-ID]

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

VLAN-ID

VLAN, auf das sich die Tabellenzeile 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. Das Feld *Remote-ID* zeigt die Zeichenfolge, die das Gerät als *Remote-ID* verwendet.

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 Eintrag wählen, geben Sie in Spalte *Remote-ID* eine beliebige Zeichenfolge ein.

Remote-ID

Zeigt die *Remote-ID*, welche das Gerät für dieses VLAN verwendet. Geben Sie eine beliebige Zeichenfolge ein, wenn in der Dropdown-Liste *Remote-ID Typ* der Eintrag *other* ausgewählt ist.

Mögliche Werte:

- Alphanumerische ASCII-Zeichenfolge mit 1..32 Zeichen

Das Gerät schreibt ASCII-Code-Werte in das Paket. Wenn in der Dropdown-Liste *Remote-ID Typ* der Eintrag *client-id* oder *other* ausgewählt ist, dann verarbeitet das Gerät den ASCII-Code der Zeichen. Wenn Sie zum Beispiel die Zeichenfolge `abc` eingeben, schreibt das Gerät den Wert `616263` in das Paket.

Wenn das Gerät die eingegebene Zeichenfolge nicht akzeptiert, führen Sie die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche  , um die nicht gespeicherten Änderungen im gegenwärtigen Dialog zu verwerfen.
- ☐ Wählen Sie in der Dropdown-Liste *Remote-ID Typ* den Eintrag *other*.
- ☐ Klicken Sie die Schaltfläche  , ohne die Zeichenfolge zu ändern.
- ☐ Geben Sie die beliebige Zeichenfolge ein.

## 7.2.2 DHCP-L2-Relay Statistiken

[ Erweitert > DHCP-L2-Relay > Statistiken ]

Das Gerät überwacht den Datenstrom auf den Ports und zeigt die Ergebnisse in tabellarischer Form.

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

Die DHCPv6-Relay-Optionen werden in der Statistik-Tabelle nicht angezeigt.

### Tabelle

Informationen zum Anpassen des Erscheinungsbilds der Tabelle finden Sie unter „Arbeiten mit Tabellen” auf Seite 16.

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.

# 7.3 Industrie-Protokolle

[ Erweitert > Industrie-Protokolle ]

Das Menü enthält die folgenden Dialoge:

- IEC 61850/MMS
- Modbus TCP

# 7.3.1 IEC 61850/MMS

[ Erweitert > Industrie-Protokolle > IEC 61850/MMS ]

IEC 61850/MMS ist ein von der International Electrotechnical Commission (IEC) genormtes 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:**
IEC 61850/MMS bietet keine Authentifizierungsmechanismen. Wenn der Schreibzugriff für IEC 61850/MMS eingeschaltet ist, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Geräts zu ändern. Dies kann zu fehlerhaften Einstellungen im Gerät führen und möglicherweise Unterbrechungen im Netz zur Folge haben.
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 *IEC 61850/MMS*-Server ein/aus.

Mögliche Werte:

- *An*
  Der *IEC 61850/MMS*-Server ist eingeschaltet.
- *Aus* (Voreinstellung)
  Der *IEC 61850/MMS*-Server ist ausgeschaltet.
  Die IEC 61850-MIBs bleiben zugänglich.

### Information

Status

Zeigt den gegenwärtigen Status des *IEC 61850/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.

CID-Datei herunterladen

Kopiert die CID-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 Einstellungen des Geräts mittels Protokoll IEC 61850/MMS zu ändern.
- `unmarkiert` (Voreinstellung)
  Der Schreibzugriff auf den MMS-Server ist deaktiviert. Der MMS-Server ist mit Lesezugriff erreichbar.

IED-Name

Legt den Namen des Intelligent Electronic Device (IED) fest, auch bekannt als Technical-Key.

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 (2¹⁶-1)` (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`)

# 7.3.2 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 eine Anwendung mit Mensch-Maschine-Schnittstelle sowie die Speicherzuordnungstabelle. Die unterstützten Objekte und die Speicherzuordnung finden Sie in den Tabellen im Anwender-Handbuch „Konfiguration“.

Im Dialog können Sie die Funktion einschalten, den Schreibzugriff aktivieren und festlegen, auf welchem TCP-Port die Mensch-Maschine-Schnittstelle auf Daten wartet. Darüber hinaus können Sie die Anzahl der Sitzungen festlegen, die gleichzeitig geöffnet sein dürfen.

**Anmerkung:**
Das Aktivieren des *Modbus TCP*-Schreibzugriffs kann ein Sicherheitsrisiko verursachen, da das Protokoll keine Benutzerzugriffe authentifiziert.

Um das Sicherheitsrisiko zu verringern, legen Sie im Dialog *Gerätesicherheit > Management-Zugriff* den IP-Adressbereich fest. Bevor Sie die Funktion einschalten, geben Sie ausschließlich die IP-Adressen ein, die 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 kann ein Sicherheitsrisiko verursachen, da das Protokoll keine Benutzerzugriffe authentifiziert.

Mögliche Werte:

- `markiert` (Voreinstellung)
  Der Lese-/Schreibzugriff für den *Modbus TCP*-Server ist aktiv. Dies ermöglicht Ihnen, die Einstellungen des Geräts mittels Funktion *Modbus TCP* 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 Command Line Interface

[ Erweitert > CLI ]

Dieser Dialog ermöglicht Ihnen, mit dem Command Line Interface auf das Gerät zuzugreifen.

Voraussetzungen:
- Im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH* ist der SSH-Server eingeschaltet.
- 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 Webbrowser eine SSH-fähige Client-Anwendung findet, dann stellt der SSH-fähige Client eine Verbindung mit dem SSH-Protokoll zum Management des Geräts her.

# A Stichwortverzeichnis

**0-9**
802.1D/p-Mapping . . . 224
802.1X . . . 99, 137

**A**
Access-Control-Listen . . . 171
ACL . . . 171
Adresskonflikt-Erkennung . . . 305
Aging-Time . . . 183
Alarm . . . 292
Anforderungsintervall . . . 83
ARP . . . 305
ARP-Tabelle . . . 75, 309
Audit-Trail . . . 356
Ausgangs-Lastbegrenzer . . . 186
Auslastung . . . 67
Authentifizierungs-Historie . . . 150
Authentifizierungs-Liste . . . 99
Auto-Disable . . . 132, 133, 248, 323, 324, 330

**B**
Benutzerverwaltung . . . 89
Betriebszeit . . . 22, 302
Bridge . . . 245

**C**
CLI . . . 122
Command Line Interface . . . 122
Community-Namen . . . 124

**D**
Default Gateway . . . 365
DHCP L2 Relay . . . 368
DHCP-Server . . . 357
DHCPv6-L2-Relay . . . 368
Digitales Zertifikat . . . 21, 50, 115, 282
DoS . . . 167
DSCP . . . 226
Duplicate Address Detection . . . 36

**E**
EAPOL . . . 148
Eingangs-Lastbegrenzer . . . 186
Einstellungen . . . 45
Einstellungen zurücksetzen . . . 50
ENVM . . . 43, 50, 53, 59, 353
Ereignis-Schweregrad . . . 350
Ethernet-Modul . . . 275, 287, 289
Ethernet-Module . . . 274
Externer Speicher . . . 23, 43, 50, 53, 59, 274, 280, 288, 353

**F**
FDB (MAC-Adresstabelle) . . . 75, 189
Fingerprint . . . 110, 115
Flash-Speicher . . . 43, 302
Flusskontrolle . . . 183

**G**
GARP . . . . . 216
Geräte-Software . . . . . 40
Geräte-Software Backup . . . . . 40
Gerätestatus . . . . . 19, 272
GMRP . . . . . 217
Guards . . . . . 257
GVRP . . . . . 219

**H**
Hardware-Uhr . . . . . 77
Hardware-Zustand . . . . . 302
HiDiscovery . . . . . 28, 281, 356
Host Key . . . . . 110
HTML . . . . . 301, 355
HTTP . . . . . 111
HTTPS . . . . . 112
HTTP-Server . . . . . 279

**I**
IAS . . . . . 99, 152
IEC 61850/MMS . . . . . 282, 375
IEEE 802.1X . . . . . 99
IGMP-Snooping . . . . . 76, 192
Industrial HiVision . . . . . 9, 105
Ingress Filtering . . . . . 235
Integrierter Authentifikations-Server . . . . . 99, 152
IP-Adressen Konflikterkennung . . . . . 305
IP-DSCP-Mapping . . . . . 226
IPv4-Regel . . . . . 172
IP-Zugriffsbeschränkung . . . . . 117

**K**
Kabeldiagnose . . . . . 318
Konfigurations-Check . . . . . 303
Konfigurationsprofil . . . . . 16, 45

**L**
L2 Relay (DHCP) . . . . . 368
Laden/Speichern . . . . . 45
Lastbegrenzer . . . . . 186
Link-Aggregation . . . . . 259
Link-Backup . . . . . 266
Link-Status . . . . . 273, 287
LLDP . . . . . 337
Logdatei . . . . . 74, 76, 355
Login-Banner . . . . . 123, 125
Loops . . . . . 244

**M**
MAC-Adress-Filter . . . 189
MAC-Adresstabelle (Forwarding Database) . . . 75, 189
MAC-Flooding . . . 131
MAC-Regel . . . 176
MAC-Spoofing . . . 133
Management-VLAN . . . 28
Management-Zugriff . . . 28, 34, 117
Manufacturing Message Specification . . . 375
Media Redundancy Protocol . . . 240
MMRP . . . 208
MMS . . . 375
Modbus TCP . . . 282, 378
Module . . . 274
MRP . . . 240
MRP-IEEE . . . 206
MRP-IEEE-Konfiguration . . . 207
MVRP . . . 213

**N**
Netzlast . . . 67
Netzteil . . . 21, 275, 288
Neustart . . . 74
NVM . . . 16, 43, 50

**O**
Out-of-Band-Management-Port . . . 38

**P**
Passwort . . . 278
Passwort-Länge . . . 90, 278
Passwortrichtlinie . . . 90
Persistente Log-Datei . . . 76
Persistentes Ereignisprotokoll . . . 352
PoE . . . 68
Port-basierte Zugriffskontrolle . . . 137
Port-Clients . . . 146
Port-Konfiguration . . . 140, 222
Port-Mirroring . . . 334
Port-Monitor . . . 330
Port-Priorität . . . 222
Portsicherheit . . . 131
Port-Statistiken . . . 76, 148
Port-VLAN . . . 234
Power over Ethernet . . . 68
Pre-Login-Banner . . . 125

**Q**
Queue-Management . . . 228
Queues . . . 221

**R**

RADIUS . . . . . 99, 154
RAM . . . . . 50
RAM-Selbsttest . . . . . 311
Relay (DHCP) . . . . . 368
Ringredundanz . . . . . 274, 288
Ringstruktur . . . . . 240
Root-Bridge . . . . . 245
RSTP . . . . . 244, 245

**S**

Schulungsangebote . . . . . 387
Schwellenwerte Netzlast . . . . . 186
Schweregrad . . . . . 350
Secure Boot . . . . . 42, 282
Secure Shell (SSH) . . . . . 107
Selbsttest . . . . . 311
Serielle Schnittstelle . . . . . 280
SFP-Modul . . . . . 317
Sicherheitsstatus . . . . . 20, 277
Signalkontakt . . . . . 20, 284
SNMP-Server . . . . . 105, 280
SNMP-Traps . . . . . 65, 70, 133, 245, 263, 273, 277, 286, 292, 307, 323
SNMPv1/v2 . . . . . 124
SNTP . . . . . 81
SNTP-Client . . . . . 82
SNTP-Server . . . . . 86
Software-Aktualisierung . . . . . 40
Software-Backup . . . . . 40
Sommerzeit . . . . . 78
Spanning Tree Protocol . . . . . 244
SSH-Server . . . . . 107
Standard-Gateway . . . . . 365
Support-Informationen . . . . . 347
Support-Informationen (ZIP-Archiv) . . . . . 350
Syslog . . . . . 313
System Monitor 1 . . . . . 311
Systeminformationen . . . . . 301
System-Log . . . . . 355
Systemzeit . . . . . 77

**T**

Technische Fragen . . . . . 387
Technische Unterlagen . . . . . 387
Technische Unterstützung . . . . . 387
Telnet-Server . . . . . 106, 279
Temperatur . . . . . 22, 273, 287
Topologie-Erkennung . . . . . 342
Traps . . . . . 65, 70, 133, 245, 263, 273, 277, 286, 292, 307, 323
Trap-Ziel . . . . . 297
Trust Modus . . . . . 222
Twisted-Pair . . . . . 318

**U**

Unaware-Modus . . . . . 183
Unsignierte Geräte-Software (Hochladen zulassen) . . . . . 42
USB-Netzschnittstelle . . . . . 38

**V**

Verschlüsselung . . . . . 45
Virtual Local Area Network . . . . . 229
VLAN . . . . . 30, 35, 229
VLAN Konfiguration . . . . . 231
VLAN-Ports . . . . . 234
VLAN-Unaware-Modus . . . . . 183

**W**

Warteschlange (Queue) . . . . . 221
Watchdog . . . . . 45, 55
Webserver . . . . . 111, 112
Werkseinstellungen . . . . . 50

**Z**

Zähler-Reset . . . . . 74
Zertifikat . . . . . 21, 50, 114, 115, 282
ZIP-Archiv mit Support-Informationen . . . . . 350
Zugriffsbeschränkung . . . . . 117
Zugriffskontrolle . . . . . 137
Zurücksetzen auf Werkseinstellungen . . . . . 50

# B Technische 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.belden.com.

Technische Unterstützung erhalten Sie unter my.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/services/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 IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Deutschland

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

# Anwender-Handbuch

## Konfiguration
## GREYHOUND Switch GRS103
## HiOS-2S



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.

© 2026 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

**Ersetzen eines Geräts** . . . 13

**1 Benutzeroberflächen** . . . 15
1.1 Grafische Benutzeroberfläche . . . 15
1.1.1 Systemanforderungen . . . 15
1.1.2 Zugriff auf das Management des Geräts . . . 16
1.2 Command Line Interface . . . 17
1.2.1 Zugriff auf das Management des Geräts über die serielle Verbindung . . . 17
1.2.2 Zugriff auf das Management des Geräts mittels SSH . . . 19
1.2.3 Modus-basierte Kommando-Hierarchie . . . 21
1.2.4 Ausführen eines Kommandos . . . 25
1.2.5 Aufbau eines Kommandos . . . 25
1.2.6 Beispiele für Kommandos . . . 28
1.2.7 Eingabeprompt . . . 29
1.2.8 Tastaturkombinationen . . . 30
1.2.9 Eingabehilfen . . . 32
1.2.10 Anwendungsfälle . . . 33
1.2.11 Service-Shell . . . 34
1.3 System Monitor 1 . . . 37
1.3.1 Systemanforderungen . . . 37
1.3.2 Zugriff auf das Management des Geräts . . . 37
1.4 Eine Begrüßungsmitteilung vor Anmeldung des Benutzers zeigen . . . 40
1.5 Eine Begrüßungsmitteilung nach Anmeldung des Benutzers zeigen . . . 41

**2 IP-Parameter festlegen** . . . 43
2.1 Grundlagen IP Parameter . . . 43
2.1.1 IPv4 . . . 43
2.1.2 IPv6 . . . 47
2.2 IP-Parameter mit dem Command Line Interface festlegen . . . 52
2.2.1 IPv4 . . . 52
2.2.2 IPv6 . . . 53
2.3 IP-Parameter mit HiDiscovery festlegen . . . 55
2.4 IP-Parameter mit grafischer Benutzeroberfläche festlegen . . . 57
2.4.1 IPv4 . . . 57
2.4.2 IPv6 . . . 58
2.5 IP-Parameter mit BOOTP festlegen . . . 59
2.6 IP-Parameter mit DHCP festlegen . . . 60
2.6.1 IPv4 . . . 60
2.6.2 IPv6 . . . 62
2.7 Erkennung von Adresskonflikten verwalten . . . 63
2.7.1 Aktive und passive Erkennung . . . 63
2.8 Funktion Erkennung doppelter Adressen . . . 64

**3 Zugriff auf das Gerät . . . 65**
3.1 Erste Anmeldung (Passwortänderung) . . . 65
3.2 Authentifizierungs-Listen . . . 66
3.2.1 Anwendungen . . . 66
3.2.2 Richtlinien . . . 66
3.2.3 Authentifizierungs-Listen verwalten . . . 66
3.2.4 Einstellungen anpassen . . . 67
3.3 Benutzerverwaltung . . . 69
3.3.1 Berechtigungen . . . 69
3.3.2 Benutzerkonten verwalten . . . 71
3.3.3 Voreingestellte Benutzerkonten . . . 72
3.3.4 Voreingestellte Passwörter ändern . . . 72
3.3.5 Neues Benutzerkonto einrichten . . . 73
3.3.6 Automatische Entsperrung von Benutzerkonten . . . 74
3.3.7 Benutzerkonto deaktivieren . . . 76
3.3.8 Richtlinien für Passwörter anpassen . . . 77
3.4 SNMP-Zugriff . . . 79
3.4.1 SNMPv1/v2-Zugriff . . . 79
3.4.2 SNMPv3-Zugriff . . . 79
3.4.3 SNMPv3-Traps . . . 80
3.5 Out-of-Band-Zugriff . . . 83
3.5.1 IP-Parameter festlegen . . . 83
3.5.2 USB-Netzschnittstelle ausschalten . . . 84

**4 Die Systemzeit im Netz synchronisieren . . . 85**
4.1 Uhrzeit einstellen . . . 85
4.2 Sommerzeit automatisch umschalten . . . 87
4.2.1 Sommerzeiteinstellung mittels vordefinierter Profile . . . 87
4.2.2 Sommerzeit manuell einstellen . . . 87
4.3 Die Zeit im Netz mit SNTP synchronisieren . . . 89
4.3.1 Vorbereitung . . . 90
4.3.2 Einstellungen des SNTP-Clients festlegen . . . 90
4.3.3 Einstellungen des SNTP-Servers festlegen . . . 92

**5 Konfigurationsprofile verwalten . . . 93**
5.1 Geänderte Einstellungen erkennen . . . 93
5.1.1 Flüchtiger Speicher (RAM) und nichtflüchtiger Speicher ( NVM ) . . . 93
5.1.2 Externer Speicher ( ENVM ) und nichtflüchtiger Speicher ( NVM ) . . . 94
5.2 Einstellungen speichern . . . 95
5.2.1 Konfigurationsprofil im Gerät speichern . . . 95
5.2.2 Konfigurationsprofil im externen Speicher ( ENVM ) speichern . . . 97
5.2.3 Konfigurationsprofil auf einem Remote-Server sichern . . . 97
5.2.4 Konfigurationsprofil exportieren . . . 98
5.3 Einstellungen laden . . . 100
5.3.1 Konfigurationsprofil aktivieren . . . 100
5.3.2 Konfigurationsprofil aus dem externen Speicher ( ENVM ) laden . . . 100
5.3.3 Konfigurationsprofil importieren . . . 102
5.4 Gerät auf Voreinstellung zurücksetzen . . . 105
5.4.1 Mit grafischer Benutzeroberfläche oder Command Line Interface . . . 105
5.4.2 Mittels System Monitor 1 . . . 105

**6 Geräte-Software aktualisieren . . . 107**
6.1 Laden einer früheren Version der Geräte-Software . . . 107

6.2 Software-Aktualisierung vom PC . . . 108
6.3 Software-Aktualisierung von einem Server . . . 109
6.3.1 Software-Aktualisierung über FTP . . . 109
6.3.2 Software-Aktualisierung über TFTP . . . 110
6.3.3 Software-Aktualisierung über SFTP . . . 111
6.3.4 Software-Aktualisierung über SCP . . . 113
6.4 Software-Aktualisierung aus dem externen Speicher ( ENVM ) . . . 115
6.4.1 Manuell – durch den Administrator initiiert . . . 115
6.4.2 Automatisch – durch das Gerät initiiert . . . 115

**7 Ports konfigurieren . . . 117**
7.1 Port ein-/ausschalten . . . 117
7.2 Betriebsart wählen . . . 118

**8 Unterstützung beim Schutz vor unberechtigtem Zugriff . . . 119**
8.1 SNMPv1/v2-Community ändern . . . 119
8.2 SNMPv1/v2 ausschalten . . . 120
8.3 HTTP ausschalten . . . 121
8.4 Telnet ausschalten . . . 122
8.5 HiDiscovery-Zugriff ausschalten . . . 123
8.6 Zugriffe auf das Management des Geräts beschränken . . . 124
8.6.1 Zugriffe aus einem bestimmten IP-Adressbereich einschränken . . . 124
8.7 Session-Timeouts anpassen . . . 126
8.8 Nicht verwendete Module deaktivieren . . . 128
8.9 SSH-Einstellungen anpassen . . . 129
8.9.1 RSA-Host-Key im Gerät generieren . . . 129
8.9.2 Einen extern generierten privaten RSA-Schlüssel auf das Gerät übertragen . . . 130
8.10 SSH-Hosts im Gerät bekannt machen . . . 133

**9 Datenverkehr kontrollieren . . . 137**
9.1 Unterstützung beim Schutz vor DoS-Attacken . . . 137
9.1.1 Filter für TCP- und UDP-Pakete . . . 138
9.1.2 Filter für IP-Pakete . . . 142
9.1.3 Filter für ICMP-Pakete . . . 142
9.2 ACL . . . 144
9.2.1 Erzeugen und Bearbeiten von IPv4-Regeln . . . 145
9.2.2 Erzeugen und Konfigurieren einer IP-ACL im Command Line Interface . . . 147
9.2.3 Erzeugen und Bearbeiten von MAC-Regeln . . . 147
9.2.4 Erzeugen und Konfigurieren einer MAC-ACL im Command Line Interface . . . 148
9.2.5 Zuweisen von ACLs zu Ports oder VLANs . . . 149
9.2.6 Maximale Anzahl zuweisbarer Regeln . . . 149

**10 Netzlaststeuerung . . . 151**
10.1 Gezielte Paketvermittlung . . . 151
10.1.1 Lernen der MAC-Adressen . . . 151
10.1.2 Aging gelernter MAC-Adressen . . . 151
10.1.3 Statische Adresseinträge . . . 152
10.2 Multicasts . . . 155
10.2.1 Beispiel für eine Multicast-Anwendung . . . 155
10.2.2 IGMP-Snooping . . . 155
10.3 Lastbegrenzung . . . 160

10.4 QoS/Priorität . . . 161
10.4.1 Beschreibung Priorisierung . . . 161
10.4.2 Behandlung empfangener Prioritätsinformationen . . . 162
10.4.3 VLAN-Tagging . . . 163
10.4.4 IP ToS (Type of Service) . . . 164
10.4.5 Handhabung der Verkehrsklassen . . . 164
10.4.6 Queue-Management . . . 165
10.4.7 Management-Priorisierung . . . 166
10.4.8 Priorisierung einstellen . . . 166
10.5 Flusskontrolle . . . 171
10.5.1 Flusskontrolle bei Halbduplex-Verbindung . . . 171
10.5.2 Flusskontrolle bei Vollduplex-Verbindung . . . 172
10.5.3 Flusskontrolle einrichten . . . 172

**11 VLANs** . . . 173
11.1 Beispiele für ein VLAN . . . 173
11.1.1 Anwendungsbeispiel für ein einfaches Port-basiertes VLAN . . . 174
11.1.2 Anwendungsbeispiel für ein komplexes VLAN-Setup . . . 178
11.2 Gast-VLAN / Unauthentifiziertes VLAN . . . 183
11.3 RADIUS-VLAN-Zuordnung . . . 185
11.4 Voice-VLAN erzeugen . . . 186
11.5 VLAN-Unaware-Modus . . . 187

**12 Redundanz** . . . 189
12.1 Netz-Topologie vs. Redundanzprotokolle . . . 189
12.1.1 Netz-Topologien . . . 189
12.1.2 Redundanzprotokolle . . . 190
12.1.3 Kombinationen von Redundanzprotokollen . . . 191
12.2 Media Redundancy Protocol (MRP) . . . 192
12.2.1 Netzstruktur . . . 192
12.2.2 Rekonfigurationszeit . . . 193
12.2.3 Advanced-Modus . . . 193
12.2.4 Voraussetzungen für MRP . . . 193
12.2.5 Erweiterte Informationen . . . 194
12.2.6 Anwendungsbeispiel für einen MRP-Ring . . . 196
12.3 Spanning Tree . . . 200
12.3.1 Grundlagen . . . 200
12.3.2 Regeln für die Erstellung der Baumstruktur . . . 204
12.3.3 Beispiele . . . 206
12.4 Rapid Spanning Tree Protokoll . . . 209
12.4.1 Port-Rollen . . . 209
12.4.2 Port-Stati . . . 210
12.4.3 Spanning Tree Priority Vector . . . 211
12.4.4 Schnelle Rekonfiguration . . . 211
12.4.5 Gerät konfigurieren . . . 212
12.4.6 Guards . . . 214
12.5 Link-Aggregation . . . 218
12.5.1 Funktionsweise . . . 218
12.5.2 Link-Aggregation Beispiel . . . 218
12.6 Link-Backup . . . 220
12.6.1 Beschreibung Fail-Back . . . 220
12.6.2 Anwendungsbeispiel für die Funktion Link-Backup . . . 221

**13 Funktionsdiagnose . . . 223**
13.1 SNMP-Traps senden . . . 223
13.1.1 SNMP-Traps für Konfigurationsaktivitäten . . . 223
13.1.2 SNMP-Trap-Einstellung . . . 224
13.1.3 ICMP-Messaging . . . 224
13.2 Gerätestatus überwachen . . . 225
13.2.1 Ereignisse, die überwacht werden können . . . 226
13.2.2 Gerätestatus konfigurieren . . . 226
13.2.3 Gerätestatus anzeigen . . . 228
13.3 Sicherheitsstatus . . . 229
13.3.1 Ereignisse, die überwacht werden können . . . 229
13.3.2 Konfigurieren des Sicherheitsstatus . . . 230
13.3.3 Anzeigen des Sicherheitsstatus . . . 232
13.4 Out-of-Band-Signalisierung . . . 233
13.4.1 Signalkontakt steuern . . . 233
13.4.2 Gerätestatus und Sicherheitsstatus überwachen . . . 234
13.5 Portereignis-Zähler . . . 237
13.5.1 Erkennen der Nichtübereinstimmung der Duplex-Modi . . . 237
13.6 Auto-Disable . . . 239
13.7 SFP-Zustandsanzeige . . . 242
13.8 Topologie-Erkennung . . . 243
13.8.1 Anzeige der Topologie-Erkennung . . . 243
13.8.2 LLDP-MED . . . 244
13.9 Erkennen von Loops . . . 245
13.10 Berichte . . . 246
13.10.1 Globale Einstellungen . . . 246
13.10.2 Syslog . . . 248
13.10.3 System-Log . . . 249
13.10.4 Audit Trail . . . 251
13.11 Netzanalyse mit TCPDump . . . 253
13.12 Überwachung des Datenstroms mit Port-Mirroring . . . 254
13.12.1 Funktion Port-Mirroring einschalten . . . 255
13.13 Selbsttest . . . 256
13.14 Kupferkabeltest . . . 258

**14 Erweiterte Funktionen des Geräts . . . 259**
14.1 DHCP-Server . . . 259
14.1.1 Einstellungen, welche der Server den Clients zuweist . . . 259
14.1.2 Pools . . . 260
14.1.3 Eine Preboot-eXecution-Environment (PXE) einrichten . . . 262
14.2 DHCP-L2-Relay . . . 265
14.2.1 Circuit- und Remote-IDs . . . 265
14.2.2 DHCP-L2-Relay-Konfiguration . . . 266
14.3 Funktion GARP . . . 269
14.3.1 GMRP konfigurieren . . . 269
14.3.2 GVRP konfigurieren . . . 270
14.4 MRP-IEEE . . . 271
14.4.1 MRP-IEEE-Funktion . . . 271
14.4.2 MRP-IEEE-Timer . . . 272
14.4.3 MMRP . . . 272
14.4.4 MVRP . . . 274

**15 Industrieprotokolle** . . . 277
15.1 IEC 61850/MMS . . . 278
15.1.1 Switch-Modell für IEC 61850 . . . 278
15.1.2 Integration in ein Steuerungssystem . . . 279
15.2 Funktion Modbus TCP . . . 282
15.2.1 Modbus TCP/IP Client/Server-Modus . . . 282
15.2.2 Unterstützte Funktionen und Speicherzuordnung . . . 282
15.2.3 Anwendungsbeispiel für die Funktion Modbus TCP . . . 287

**A Konfigurationsumgebung einrichten** . . . 291
A.1 DHCP/BOOTP-Server einrichten . . . 291
A.2 DHCP-Server Option 82 einrichten . . . 294
A.3 HTTPS-Zertifikat . . . 297
A.3.1 Konflikte bei der Zertifikatsvalidierung . . . 297
A.3.2 HTTPS-Zertifikatsverwaltung . . . 297
A.3.3 Zugang über HTTPS . . . 298

**B Anhang** . . . 301
B.1 Literaturhinweise . . . 301
B.2 Management Information BASE (MIB) . . . 302
B.3 Liste der RFCs . . . 304
B.4 Zugrundeliegende IEEE-Normen . . . 307
B.5 Zugrundeliegende IEC-Normen . . . 308
B.6 Zugrundeliegende ANSI-Normen . . . 309
B.7 Technische Daten . . . 310
B.7.1 Switching . . . 310
B.7.2 VLAN . . . 310
B.7.3 Access-Control-Listen (ACL) . . . 310
B.8 Copyright integrierter Software . . . 311
B.9 Verwendete Abkürzungen . . . 312

**C Stichwortverzeichnis** . . . 315

**D Technische Unterstützung** . . . 321

**E Leserkritik** . . . 322

# 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“, das ausschließlich in englischer Sprache verfügbar ist, enthält detaillierte Information zur Bedienung der einzelnen Funktionen des Geräts über das Command Line Interface.

Das Benutzerhandbuch „Sicherheit“, das ausschließlich in englischer Sprache verfügbar ist, bietet eine Einführung in die Planung der Systemsicherheit und die Entwicklung von Richtlinien. Es enthält eine detaillierte Auflistung der Sicherheitsmaßnahmen für das Gerät. Es beschreibt außerdem, wie ein geschütztes Gerät die Sicherheit und Verfügbarkeit Ihres Netzes verbessern kann. Sein Anhang enthält Details zu Hardware-Sicherheitssiegeln sowie einen Leitfaden zur Passwortstärke.

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:

| | |
|---|---|
| • <br> – | Listenpunkt<br>Listenpunkt – zweite Ebene |
| ▶ | Wert eines Parameters |
| ☐ | Handlungsschritt |
| 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 Geräts

Das Gerät bietet die folgenden Plug-and-Play-Lösungen für den Austausch eines Geräts durch ein Gerät desselben Typs, zum Beispiel zur vorbeugenden Wartung oder wenn ein Fehler erkannt wurde.

- Das neue Gerät lädt das Konfigurationsprofil des ersetzten Geräts vom externen Speicher (*ENVM*).
  Siehe „Konfigurationsprofil aus dem externen Speicher (ENVM) laden” auf Seite 100.
- Das neue Gerät erhält seine IP-Adresse mittels DHCP *Option 82*.
  Siehe „DHCP-L2-Relay” auf Seite 265.
  Siehe „DHCP-Server Option 82 einrichten” auf Seite 294.

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 digitales Zertifikat auf das Gerät zu übertragen.
  Siehe „HTTPS-Zertifikatsverwaltung” auf Seite 297.
- 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 „Einen extern generierten privaten RSA-Schlüssel auf das Gerät übertragen” auf Seite 130.

# 1 Benutzeroberflächen

Das Gerät ermöglicht Ihnen den Zugriff auf das Management des Geräts über folgende Benutzeroberflächen:

| Benutzeroberfläche | Berechtigung erforderlich | Erreichbar über … | Voraussetzung |
|---|---|---|---|
| Grafische Benutzeroberfläche | Ja | Ethernet | Webbrowser |
| Command Line Interface | Ja | Ethernet | SSH-Client |
| | | Serielle Schnittstelle | VT100-Terminalemulation |
| System Monitor 1 | Nein | Serielle Schnittstelle | |

Die Berechtigung für Zugriffe auf das Management des Geräts wird wie folgt erteilt:
- Durch ein auf dem Gerät eingerichtetes Benutzerkonto
  Siehe „Benutzerverwaltung” auf Seite 69.
- Ein Remote-Server erteilt die Berechtigung
  – RADIUS

Dieses Kapitel enthält die folgenden Themen:
▶ Grafische Benutzeroberfläche
▶ Command Line Interface
▶ System Monitor 1
▶ Eine Begrüßungsmitteilung vor Anmeldung des Benutzers zeigen
▶ Eine Begrüßungsmitteilung nach Anmeldung des Benutzers zeigen

## 1.1 Grafische Benutzeroberfläche

### 1.1.1 Systemanforderungen

Um mittels grafischer Benutzeroberfläche auf das Management des Geräts zuzugreifen, benötigen Sie einen Webbrowser mit HTML5-Unterstützung.

Webbrowser und andere Drittanbieter-Software validieren routinemäßig die Gültigkeit digitaler Zertifikate. Wenn Ihr Webbrowser eine Meldung zeigt, die auf einen Konflikt bei der Validierung des digitalen Zertifikats des Geräts hinweist, führen Sie die folgenden Schritte aus:
- ☐ Prüfen Sie, ob das digitale Zertifikat des Geräts noch gültig ist.
- ☐ Prüfen Sie, ob Ihr Webbrowser den Algorithmus, mit dem das digitale Zertifikat generiert wurde, nicht mehr als vertrauenswürdig einstuft.

Um den Konflikt bei der Validierung zu beheben, generieren Sie das digitale Zertifikat im Gerät mit der neuesten Gerätesoftware noch einmal. Alternativ dazu können Sie ein digitales Zertifikat extern mittels zeitgemäßer Signaturalgorithmen generieren. Übertragen Sie das neue digitale Zertifikat auf das Gerät.

### 1.1.2 Zugriff auf das Management des Geräts

Voraussetzung für Zugriffe auf das Management des Geräts ist, dass im Gerät die IP-Parameter eingerichtet sind. Siehe „IP-Parameter festlegen” auf Seite 43.

Führen Sie die folgenden Schritte aus:

- ☐ Starten Sie den Webbrowser auf der Management-Station.
- ☐ Fügen Sie die IP-Adresse des Geräts in das Adressfeld des Webbrowsers ein.
  Der Webbrowser 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 den entsprechenden Link oben rechts.
- ☐ Geben Sie Benutzername und Passwort ein.
  - –
  - – Der voreingestellte Benutzername ist `admin`.
  - – Das voreingestellte Passwort ist `private`.
    Wenn Sie bei der Ersteinrichtung des Geräts das voreingestellte Passwort eingeben, werden Sie aufgefordert, ein neues Passwort einzugeben.
    Siehe „Erste Anmeldung (Passwortänderung)” auf Seite 65.
- ☐ Klicken Sie die Schaltfläche *Login*.
  Wenn das Gerät die von Ihnen eingegebenen Anmeldedaten akzeptiert, sind Sie im Management des Geräts angemeldet.

# 1.2 Command Line Interface

IT-Spezialisten finden im Command Line Interface die gewohnte Umgebung zum Konfigurieren von IT-Geräten. Als erfahrener Benutzer oder Administrator kennen Sie die Grundlagen der Vernetzung und wissen, wie man Hirschmann-Geräte einsetzt.

Sie können mittels Command Line Interface wie folgt auf das Management des Geräts zugreifen:

- Über die serielle Verbindung
  Siehe „Zugriff auf das Management des Geräts über die serielle Verbindung” auf Seite 17.
- Über das Netz mittels Secure Shell (SSH)
  Siehe „Zugriff auf das Management des Geräts mittels SSH” auf Seite 19.

Informationen zur Montage und Inbetriebnahme des Geräts finden Sie im Anwender-Handbuch „Installation“.

## 1.2.1 Zugriff auf das Management des Geräts über die serielle Verbindung

Für Zugriffe auf das Management des Geräts verbinden Sie eine Management-Station mit VT100-Terminalemulation mit der seriellen Schnittstelle des Geräts.

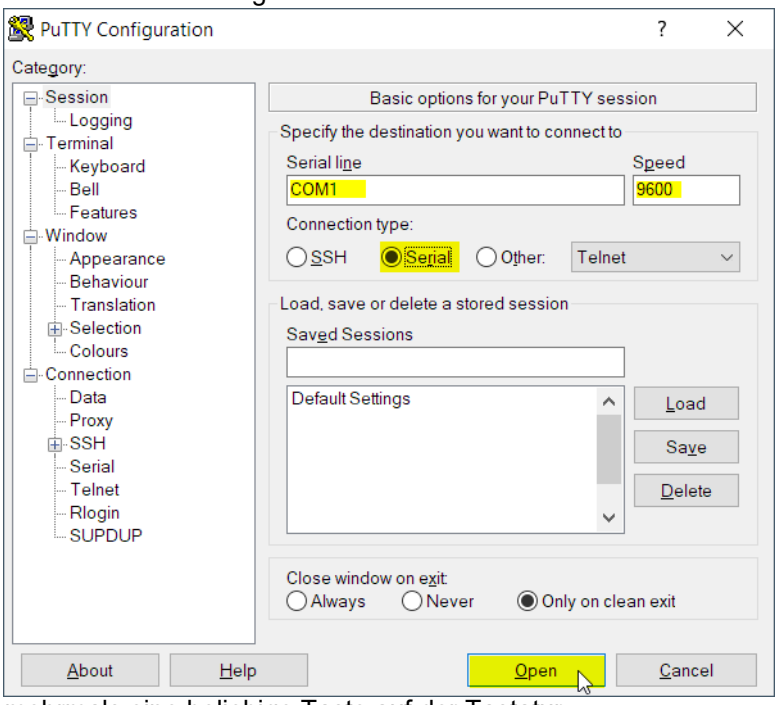
| Einstellungen für VT100-Terminalemulation | |
|---|---|
| Speed | 9600 bit/s |
| Data | 8 bit |
| Stopbit | 1 bit |
| Parity | None |
| Handshake | None |

Das folgende Beispiel führt Sie anhand der Anwendung *PuTTY* als VT100-Terminalemulation durch die erforderlichen Schritte. Sie können die Anwendung *PuTTY* hier herunterladen: www.chiark.greenend.org.uk/~sgtatham/putty/.

Führen Sie die folgenden Schritte aus:

- ☐ Verbinden Sie die Management-Station mit der seriellen Schnittstelle des Geräts.
- ☐ Starten Sie auf der Management-Station die VT100-Terminalemulation.

☐ Richten Sie die serielle Verbindung ein. Klicken Sie anschließend die Schaltfläche *Open*.




☐ Drücken Sie mehrmals eine beliebige Taste auf der Tastatur.
Nach wenigen Sekunden zeigt die VT100-Terminalemulation den Anmeldebildschirm.

☐ Geben Sie Benutzername und Passwort ein.

– Der voreingestellte Benutzername ist `admin`.
– Das voreingestellte Passwort ist `private`.
Wenn Sie bei der Ersteinrichtung des Geräts das voreingestellte Passwort eingeben, werden Sie aufgefordert, ein neues Passwort einzugeben. Siehe „Erste Anmeldung (Passwortänderung)” auf Seite 65.

Sie sind im Management des Geräts angemeldet.

```
                    Copyright (c) 2011-2026 Hirschmann Automation and Control GmbH

                                    All rights reserved

                                GRS103 Release HiOS-2S-10.6.00

                                (Build date 2026-10-03 09:35)


                    System Name   :  GRS103-ECE555d6e764
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    USB IP        :  192.168.248.100
                    USB Mask      :  255.255.255.0
                    System Time   :  2026-10-05 12:47:17


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.

GRS>
```

*Abb. 1: Start-Bildschirm des Command Line Interfaces*

### 1.2.2 Zugriff auf das Management des Geräts mittels SSH

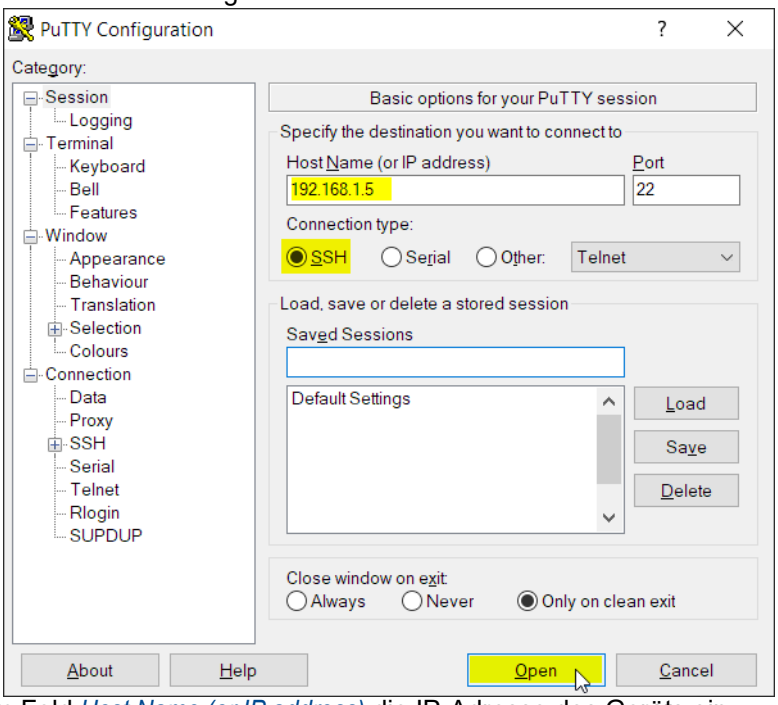
Voraussetzung für Zugriffe auf das Management des Geräts ist, dass im Gerät die IP-Parameter eingerichtet sind. Siehe „IP-Parameter festlegen” auf Seite 43.

Das folgende Beispiel führt Sie anhand der Anwendung *PuTTY* als SSH-Client durch die erforderlichen Schritte. Sie können die Anwendung *PuTTY* hier herunterladen: www.chiark.greenend.org.uk/~sgtatham/putty/. Alternativ dazu können Sie das Kommando `ssh` verwenden, welches zu OpenSSH gehört.

Führen Sie die folgenden Schritte aus:

- ☐ Verbinden Sie die Management-Station über das Ethernet-Netz mit dem Gerät.
- ☐ Starten Sie auf der Management-Station die SSH-Client-Anwendung.

☐ Richten Sie die SSH-Verbindung ein.

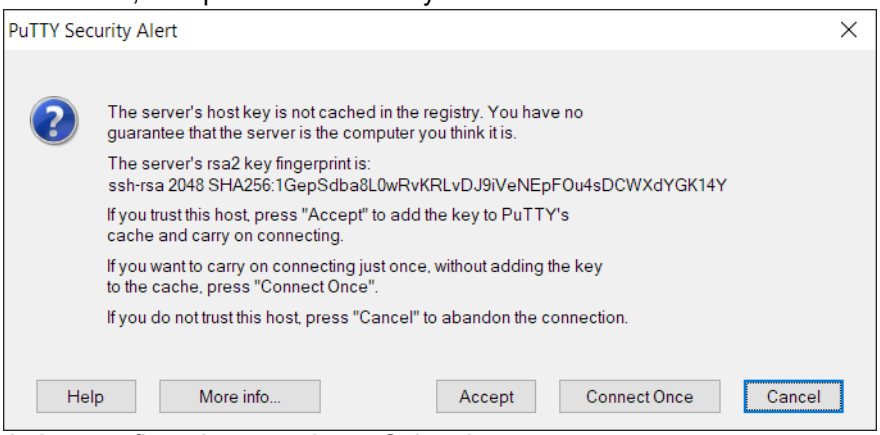



☐ Geben Sie im Feld *Host Name (or IP address)* die IP-Adresse des Geräts ein.
☐ Wählen Sie in der Optionsliste *Connection type* das Optionsfeld *SSH*.
☐ Klicken Sie die Schaltfläche *Open*.
Wenn Sie die Management-Station erstmals mit dem Gerät verbinden, zeigt die SSH-Client-Anwendung eine *Host Key*-Prüfungsmeldung.

☐ Prüfen Sie den Fingerabdruck des Keys, den der SSH-Server des Geräts sendet.

**Anmerkung:**
Auf dem Gerät können Sie den Fingerabdruck des *Host Keys* mit dem Kommando `show ssh server` oder im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH* anzeigen.

☐ Um fortzufahren, akzeptieren Sie den Key.




Der Verbindungsaufbau dauert mehrere Sekunden.

☐ Geben Sie Benutzername und Passwort ein.
– Der voreingestellte Benutzername ist `admin`.
– Das voreingestellte Passwort ist `private`.
Wenn Sie bei der Ersteinrichtung des Geräts das voreingestellte Passwort eingeben, werden Sie aufgefordert, ein neues Passwort einzugeben. Siehe „Erste Anmeldung (Passwortänderung)" auf Seite 65.

Sie sind im Management des Geräts angemeldet.

```
login as: admin
admin@192.168.1.5's password:


                    Copyright (c) 2011-2026 Hirschmann Automation and Control GmbH

                                  All rights reserved

                               GRS103 Release HiOS-2S-10.6.00

                               (Build date 2026-10-03 09:35)


                    System Name   :  GRS103-ECE555d6e764
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  EC:E5:55:01:02:03
                    USB IP        :  192.168.248.100
                    USB Mask      :  255.255.255.0
                    System Time   :  2026-10-05 12:47:17


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.

GRS>
```

*Abb. 2: Start-Bildschirm des Command Line Interfaces*

### 1.2.3 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 ermöglicht Ihnen, diese Kommandos auch im *Privileged Exec* Modus auszuführen.

Die folgende Abbildung zeigt die Modi des Command Line Interfaces.

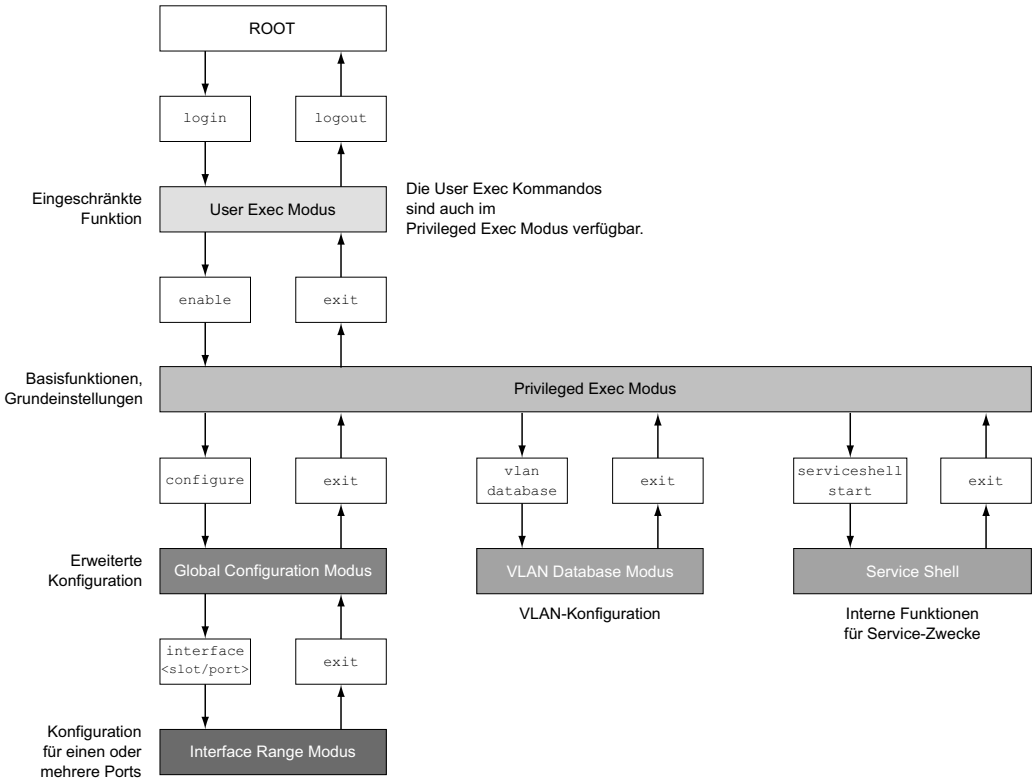



*Abb. 3: Aufbau des Command Line Interfaces*

Das Command Line Interface unterstützt, abhängig von der Berechtigungsstufe (User Level), die folgenden Modi:

- *User Exec* Modus
  Nach Anmelden beim Management des Geräts mit dem Command Line Interface befinden Sie sich im *User Exec* Modus. Der *User Exec* Modus enthält einen begrenzten Umfang an Kommandos.
  Kommando-Prompt: `(GRS) >`
- *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 beim Management des Geräts anmelden. Vom *Privileged Exec* Modus aus sind auch die Kommandos des *User Exec* Modus ausführbar.
  Kommando-Prompt:`(GRS) #`
- VLAN-Modus
  Der VLAN-Modus enthält VLAN-bezogene Kommandos.
  Kommando-Prompt: `(GRS) (VLAN)#`
- Service-Shell
  Die Service-Shell dient ausschließlich 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: `(GRS) (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 physischen Ports des Gerätes
    Kommando-Prompt: `(GRS) ((interface) all)#`
    Beispiel: Beim Wechsel vom *Global Config* Modus in den *Interface Range* Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (GRS) (config)#interface all
    (GRS) ((Interface)all)#
    ```
  - Einzelner Port an einem Interface
    Kommando-Prompt: `(GRS) (interface <slot/port>)#`
    Beispiel: Beim Wechsel vom *Global Config* Modus in den *Interface Range* Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (GRS) (config)#interface 2/1
    (GRS) (interface 2/1)#
    ```
  - Eine Portreihe an einem Interface
    Kommando-Prompt: `(GRS) (interface <interface range> )#`
    Beispiel: Beim Wechsel vom *Global Config* Modus in den *Interface Range* Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (GRS) (config)#interface 1/2-1/4
    (GRS) ((Interface)1/2-1/4)#
    ```
  - Eine Auflistung von einzelnen Ports
    Kommando-Prompt: `(GRS) (interface <interface list>)#`
    Beispiel: Beim Wechsel vom *Global Config* Modus in den *Interface Range* Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (GRS) (config)#interface 1/2,1/4,1/5
    (GRS) ((Interface)1/2,1/4,1/5)#
    ```
  - Eine Auflistung von Portreihen und einzelnen Ports
    Kommando-Prompt: `(GRS) (interface <complex range>)#`
    Beispiel: Beim Wechsel vom *Global Config* Modus in den *Interface Range* Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (GRS) (config)#interface 1/2-1/4,1/6-1/9
    (GRS) ((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. 1: 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:<br>`(GRS) >logout`<br>`Are you sure (Y/N) ?y` |
| *Privileged Exec* Modus | Aus dem *User Exec* Modus geben Sie den Befehl `enable` ein.<br>`(GRS) >enable`<br>`(GRS) #` | Um den *Privileged Exec* Modus zu beenden und in den *User Exec* Modus zurückzukehren, geben Sie `exit` ein:<br>`(GRS) #exit`<br>`(GRS) >` |
| VLAN-Modus | Aus dem *Privileged Exec* Modus geben Sie den Befehl `vlan database` ein.<br>`(GRS) #vlan database`<br>`(GRS) (Vlan)#` | Um den VLAN-Modus zu beenden und in den *Privileged Exec* Modus zurückzukehren, geben Sie `exit` ein oder drücken Sie <STRG>+<Z>.<br>`(GRS) (Vlan)#exit`<br>`(GRS) #` |
| *Global Config* Modus | Aus dem *Privileged Exec* Modus geben Sie den Befehl `configure` ein.<br>`(GRS) #configure`<br>`(GRS) (config)#`<br>Aus dem *User Exec* Modus geben Sie Befehl `enable` und dann im *Privileged Exec* Modus den Befehl `Configure` ein.<br>`(GRS) >enable`<br>`(GRS) #configure`<br>`(GRS) (config)#` | Um den *Global Config* Modus zu beenden und in den *Privileged Exec* Modus zurückzukehren, geben Sie `exit` ein:<br>`(GRS) (config)#exit`<br>`(GRS) #`<br>Um anschließend den *Privileged Exec* Modus zu beenden und in den *User Exec* Modus zurückzukehren, geben Sie erneut `exit` ein:<br>`(GRS) #exit`<br>`(GRS) >` |
| *Interface Range* Modus | Aus dem *Global Config* Modus geben Sie den Befehl `interface {all\|<slot/port>\|<interface range> \|<interface list>\|<complex range>}` ein.<br>`(GRS) (config)#interface <slot/port>`<br>`(GRS) (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 <STRG>+<Z>.<br>`(GRS) (interface slot/port)#exit`<br>`(GRS) #` |

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.

```
(GRS)>
  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.

(GRS)>
```

*Abb. 4: Kommandos im User Exec Modus*

## 1.2.4 Ausführen eines Kommandos

### Syntaxanalyse

Nach Anmelden beim Management des Geräts mit dem Command Line Interface befinden Sie sich im *User Exec* Modus. Das Command Line Interface gibt das `(GRS)>` Prompt auf dem Bildschirm aus.

Wenn Sie ein Kommando eingeben und die <Enter> 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:

```
(GRS)>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.

## 1.2.5 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. 2: 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. |
| `[Choice1 \| Choice2]` | Eine senkrechte Linie, eingeschlossen in Klammern, zeigt eine Auswahlmöglichkeit. Wählen Sie einen Wert.<br>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>` | Durch Drücken der <Enter>-Taste fügen Sie einen Zeilenumbruch ein. |

Die folgende Liste zeigt mögliche Parameterwerte innerhalb des Command Line Interface:

*Tab. 3: 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. 4: 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:

```
*(GRS)#cli prompt Device name
Error: Invalid command 'name'

*(GRS)#cli prompt 'Device name'

*(Device name)#
```

### 1.2.6 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 den Zeitüberschreitungs-Wert des RADIUS Servers festzulegen.

```
(GRS) (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.

```
(GRS) (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.

## 1.2.7 Eingabeprompt

### Kommandomodus

Das Command Line Interface zeigt durch das Eingabeprompt, in welchem der Modi Sie sich befinden:

- `(GRS) >`
  *User Exec* Modus
- `(GRS) #`
  *Privileged Exec* Modus
- `(GRS) (config)#`
  *Global Config* Modus
- `(GRS) (Vlan)#`
  VLAN Database mode
- `(GRS) ((Interface)all)#`
  *Interface Range* Modus / Alle Ports des Geräts
- `(GRS) ((Interface)2/1)#`
  *Interface Range* Modus / Einzelner Port auf einem Interface
- `(GRS) ((Interface)1/2-1/4)#`
  *Interface Range* Modus / Eine Reihe von Ports auf einem Interface
- `(GRS) ((Interface)1/2,1/4,1/5)#`
  *Interface Range* Modus / Eine Auflistung von einzelnen Ports
- `(GRS) ((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.
  `*(GRS)>`
- Rautezeichen `#`
  Ein Rautezeichen `#` zu Beginn des Eingabeprompts zeigt, dass sich die Boot-Parameter von den Parametern während der Bootphase unterscheiden.
  `*#(GRS)>`
- Ausrufezeichen `!`
  Ein Ausrufezeichen `!` zu Beginn des Eingabeprompts zeigt: Das Passwort für das Benutzerkonto `admin` stimmt mit dem Lieferzustand überein.
  `!(GRS)>`

### Wildcards

Das Gerät ermöglicht Ihnen, den Prompt der Befehlszeile zu ändern.

Das Command Line Interface unterstützt die folgenden Platzhalter:

*Tab. 5: Verwendung von Wildcards am Eingabeprompt des Command Line Interfaces*

| Wildcard | Beschreibung |
|---|---|
| `%d` | Systemdatum |
| `%t` | Systemzeit |

*Tab. 5: Verwendung von Wildcards am Eingabeprompt des Command Line Interfaces*

| Wildcard | Beschreibung |
|---|---|
| %i | IP-Adresse des Geräts |
| %m | MAC-Adresse des Gerätes |
| %p | Produktbezeichnung des Geräts |

```
!(GRS)>enable

!(GRS)#cli prompt %i

!192.168.1.5#cli prompt (GRS)%d

!*(GRS)2026-10-05#cli prompt (GRS)%d%t

!*(GRS)2026-10-05 12:47:17#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

### 1.2.8 Tastaturkombinationen

Die folgenden Tastaturkombinationen erleichtern Ihnen die Arbeit mit dem Command Line Interface:

*Tab. 6: Tastenkombinationen im Command Line Interface*

| Tastaturkombination | Beschreibung |
|---|---|
| <STRG> + <H>, <Zurück (Backspace)> | Letztes Zeichen löschen |
| <STRG> + <A> | Zum Zeilenanfang gehen |
| <STRG> + <E> | Zum Zeilenende gehen |
| <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>, <LEERTASTE> | 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:

```
(GRS) #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

(GRS) #
```

*Abb. 5: Auflisten der Tastenkombinationen mit dem Help-Kommando*

## 1.2.9 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:
  ```
  (GRS) (Config)#lo
  (GRS) (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 `(GRS) >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:

```
!*#(GRS)(Config)#show?

   show          Display device options and settings.
```

## 1.2.10 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:

- ☐ Geben Sie `enable` ein, um in den *Privileged Exec* Modus zu wechseln.
- ☐ 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:

- Voraussetzungen für die Ausführung des Kommandos:
  - Sie befinden sich im *Global Config*-Modus.
    Siehe „Modus-basierte Kommando-Hierarchie” auf Seite 21.
  - Sie haben die Zugriffsrolle *administrator*.

Syntax der Kommandos und Parameter: Siehe „Aufbau eines Kommandos” auf Seite 25.

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`

### 1.2.11 Service-Shell

Die Service-Shell dient ausschließlich 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 nichtflüchtigen Speichers (*NVM*), **kann dazu führen, dass Ihr Gerät nicht mehr funktioniert**.

#### Service-Shell starten

Voraussetzung ist, dass Sie sich im *User Exec*-Modus befinden: `(GRS) >`

Führen Sie die folgenden Schritte aus:
- ☐ Geben Sie `enable` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - ☐ Geben Sie `e` ein und drücken die <Tabulator>-Taste.
- ☐ Geben Sie `serviceshell start` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - ☐ Geben Sie `ser` ein und drücken die <Tabulator>-Taste.
  - ☐ Geben Sie `s` ein und drücken die <Tabulator>-Taste.

```
!GRS >enable

!*GRS #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 (2026-10-05 12:47:17 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

#### Mit der Service Shell arbeiten

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:
☐ Geben 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:
☐ Geben Sie `exit` ein und drücken die <Enter>-Taste.

### Service-Shell dauerhaft 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: `(GRS) >`

Führen Sie die folgenden Schritte aus:
☐ Geben Sie `enable` ein und drücken die <Enter>-Taste.
Um den Aufwand beim Tippen zu reduzieren:
☐ Geben Sie `e` ein und drücken die <Tabulator>-Taste.

- ☐ Geben Sie `serviceshell deactivate` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - ☐ Geben Sie `ser` ein und drücken die <Tabulator>-Taste.
  - ☐ Geben Sie `dea` ein und drücken die <Tabulator>-Taste.
- ☐ **Dieser Schritt ist unumkehrbar!**
  Drücken Sie die <Y>-Taste.

```
!GRS >enable

!*GRS #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 1

Der System Monitor 1 bietet Funktionen zur Wiederherstellung der Einstellungen des Geräts. Wenn die Option zum Zugriff auf System Monitor 1 während des Systemstarts aktiv ist, siehe Dialog *Diagnose > System > Selbsttest*, können Sie während des Systemstarts den System Monitor 1 starten. Voraussetzung ist, dass die Management-Station über die serielle Verbindung mit dem Gerät verbunden ist.

Im System Monitor 1 erledigen Sie beispielsweise folgende Aufgaben:
- Betriebssystem verwalten und Image der Geräte-Software prüfen
- Betriebssystem starten
- Konfigurationsprofile löschen, Gerät auf den Lieferzustand zurücksetzen
- Bootcode-Information prüfen

## 1.3.1 Systemanforderungen

Für Zugriffe auf das Management des Geräts verbinden Sie eine Management-Station mit VT100-Terminalemulation mit der USB-C-Schnittstelle des Geräts.

| Einstellungen für VT100-Terminalemulation | |
|---|---|
| Speed | `9600 bit/s` |
| Data | `8 bit` |
| Stopbit | `1 bit` |
| Parity | `None` |
| Handshake | `None` |

## 1.3.2 Zugriff auf das Management des Geräts

Während des Systemstarts ist die serielle Verbindung zum Gerät über die USB-C-Schnittstelle nicht verfügbar. Deshalb funktioniert der Zugriff auf System Monitor 1 anders als bei anderen Hirschmann-Geräten.

Um in den System Monitor 1 zu wechseln, führen Sie die folgenden Schritte aus:
- ☐ „Gerät in den Recovery-Modus versetzen” auf Seite 37
- ☐ „In den System Monitor 1 wechseln” auf Seite 38

### Gerät in den Recovery-Modus versetzen

Erforderliches Zubehör:
- Externer Speicher (empfohlen: ACA21/ACA22)
- USB-C-zu-USB-A-Adapter (wenn Sie einen anderen als den empfohlenen externen Speicher (*ENVM*) verwenden)

Führen Sie die folgenden Schritte aus:
- ☐ Stecken Sie den externen Speicher (*ENVM*) in die Management-Station ein.
- ☐ Erstellen Sie eine leere Datei `recovery.txt` im Stammverzeichnis des externen Speichers (*ENVM*).

- ☐ Stecken Sie den externen Speicher (*ENVM*) in das Gerät.
- ☐ Starten Sie das Gerät neu.
- ☐ Beobachten Sie die LEDs, während des Startvorgangs des Geräts. Wenn die LED *Status* abwechselnd rot und grün blinkt, ist das Gerät erfolgreich in den Recovery-Modus versetzt.

  **Anmerkung:**
  Die Beschreibung der Anzeigeelemente finden Sie im Anwender-Handbuch Installation.

- ☐ Entfernen Sie den externen Speicher aus dem Gerät.

### In den System Monitor 1 wechseln

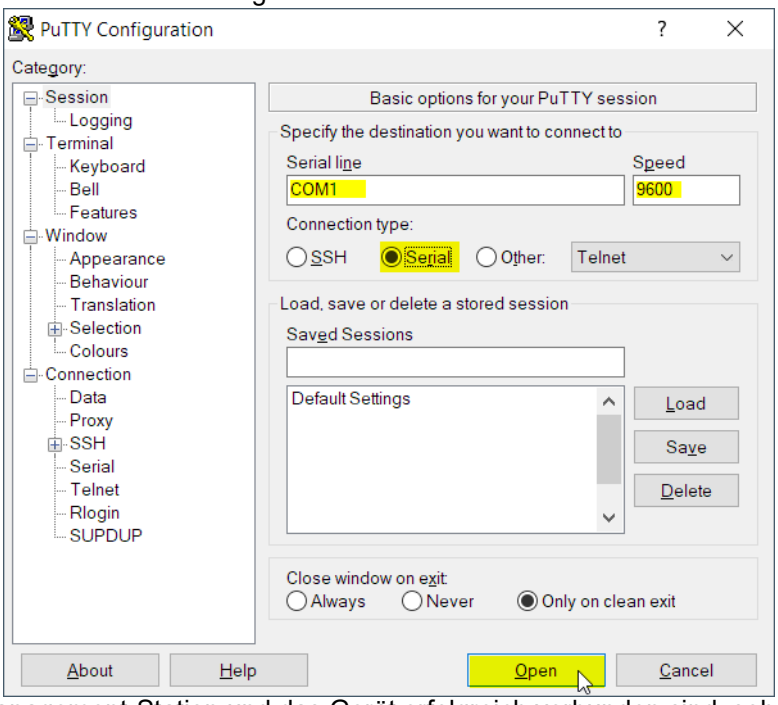
Erforderliches Zubehör:

- USB-Kabel, um die Management-Station mit der USB-C-Schnittstelle des Geräts zu verbinden
- Management-Station mit VT100-Terminalemulation

Führen Sie die folgenden Schritte aus:

- ☐ Verbinden Sie die Management-Station über das USB-Kabel mit dem Gerät.
- ☐ Starten Sie auf der Management-Station die VT100-Terminalemulation.

☐ Richten Sie die serielle Verbindung ein. Klicken Sie anschließend die Schaltfläche *Open*.




Wenn die Management-Station und das Gerät erfolgreich verbunden sind, sehen Sie einen leeren Bildschirm.

☐ Drücken Sie die <Enter>-Taste.
Nach wenigen Sekunden zeigt die VT100-Terminalemulation den System Monitor 1.

```
System Monitor 1
(Selected OS: ...-10.6 (2026-10-03 09:35))

1  Manage operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

☐ Wählen Sie durch Eingabe der Ziffer den gewünschten Menüpunkt aus.
☐ Um ein Untermenü zu verlassen und zum Hauptmenü zurückzukehren, drücken Sie die <ESC>-Taste.

**Anmerkung:**
Wenn Sie den externen Speicher (*ENVM*) dauerhaft im Gerät eingesteckt lassen möchten, löschen Sie zunächst die Datei `recovery.txt` aus dem Stammverzeichnis des externen Speichers (*ENVM*).

# 1.4 Eine Begrüßungsmitteilung vor Anmeldung des Benutzers zeigen

Sie können eine Begrüßungsmitteilung einrichten, die das Gerät zeigt, bevor sich ein Benutzer beim Management des Geräts anmeldet.

Unabhängig davon können Sie auch eine Post-Login-Begrüßungsmitteilung einrichten. Das Gerät zeigt die Post-Login-Begrüßungsmitteilung, nachdem sich ein Benutzer mittels Command Line Interface beim Management des Geräts angemeldet hat. Siehe „Eine Begrüßungsmitteilung nach Anmeldung des Benutzers zeigen” auf Seite 41.

Geben Sie aus Sicherheitsgründen möglichst wenige Informationen ein. Vermeiden Sie jegliche Informationen, die einem unbefugten Benutzer helfen könnten. Im Zweifelsfall schließen Sie einen angemessenen Kompromiss auf der Grundlage Ihrer Sicherheitsrichtlinien.

Das folgende Beispiel zeigt, wie Sie die Pre-Login-Begrüßungsmitteilung einrichten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Pre-Login-Banner*.
- ☐ Geben Sie im Feld *Banner-Text* die gewünschte Zeichenfolge ein, zum Beispiel `Willkommen! Sie benötigen bestimmte Berechtigungen, um auf das Management des Geräts zugreifen zu können.`
- ☐ Schalten Sie die Funktion *Pre-Login-Banner* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `system pre-login-banner text "Welcome! You need certain permissions to access the device management."` | Legen Sie die Zeichenfolge fest, die das Gerät zeigt, bevor sich ein Benutzer beim Management des Geräts anmeldet. Setzen Sie die Zeichenfolge in Anführungszeichen. Das Gerät zeigt die Zeichenfolge ohne Anführungszeichen an. |
| `system pre-login-banner operation` | Die Funktion für das Banner vor der Anmeldung einschalten. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

# 1.5 Eine Begrüßungsmitteilung nach Anmeldung des Benutzers zeigen

Sie können eine Begrüßungsmitteilung einrichten, die das Gerät zeigt, nachdem sich ein Benutzer mittels Command Line Interface beim Management des Geräts angemeldet hat.

Unabhängig davon können Sie auch eine Pre-Login-Begrüßungsmitteilung einrichten. Das Gerät zeigt die Pre-Login-Begrüßungsmitteilung, bevor sich ein Benutzer beim Management des Geräts anmeldet. Siehe „Eine Begrüßungsmitteilung vor Anmeldung des Benutzers zeigen” auf Seite 40.

Das folgende Beispiel zeigt, wie Sie die Post-Login-Begrüßungsmitteilung einrichten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > CLI*, Registerkarte *Login-Banner*.
- ☐ Geben Sie im Feld *Banner-Text* die gewünschte Zeichenfolge ein, zum Beispiel `Willkommen im Command Line Interface!`.
- ☐ Schalten Sie die Funktion *Login-Banner* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `cli banner text "Welcome to the Command Line Interface!"` | Die Zeichenfolge festlegen, die das Gerät zeigt, nachdem sich ein Benutzer beim Management des Geräts angemeldet hat. Setzen Sie die Zeichenfolge in Anführungszeichen. Das Gerät zeigt die Zeichenfolge ohne Anführungszeichen an. |
| `cli banner operation` | Die Funktion für das Banner nach der Anmeldung einschalten. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

# 2 IP-Parameter festlegen

Bei der Erstinstallation des Geräts legen Sie die IP-Parameter fest.

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 (*ENVM*) gespeichert haben.
- Verwendung von BOOTP.
  Wählen Sie diese In-Band-Methode, um das installierte Gerät über BOOTP einzurichten. Hierzu benötigen Sie einen BOOTP-Server. Der BOOTP-Server weist dem Gerät die Konfigurationsdaten anhand der MAC-Adresse des Geräts zu. Der DHCP-Modus ist der Standardmodus für den Bezug der Konfigurationsdaten.
- Konfiguration über DHCP.
  Wählen Sie diese In-Band-Methode, um die Einrichtung des installierten Geräts über DHCP vorzunehmen. Hierzu benötigen Sie einen DHCP-Server. Der DHCP-Server weist dem Gerät die Konfigurationsdaten anhand der MAC-Adresse oder des Systemnamens des Geräts 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.

RFC 1340 aus dem Jahr 1992 definiert 5 Klassen von IP-Adressen.

*Tab. 7: IP-Adressklassen*

| Klasse | Netzadresse | Hostadresse | Adressbereich |
|---|---|---|---|
| A | 1 Byte | 3 Bytes | 0.0.0.0..127.255.255.255 |
| B | 2 Bytes | 2 Bytes | 128.0.0.0..191.255.255.255 |
| C | 3 Bytes | 1 Byte | 192.0.0.0..223.255.255.255 |
| D | | | 224.0.0.0..239.255.255.255 |
| E | | | 240.0.0.0..255.255.255.255 |

Der erste Byte einer IP-Adresse ist die Netzadresse. Der Regulierungsausschuss für die weltweite Zuweisung von Netzadressen ist Internet Assigned Numbers Authority (IANA). 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

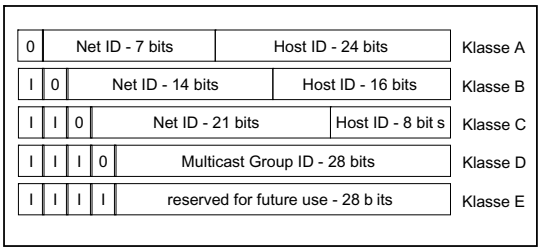



*Abb. 6: Bitdarstellung der IP-Adresse*

Ist das erste Bit einer IP-Adresse 0, gehört sie zur Klasse A. Das erste Oktett ist kleiner als 128.

Ist das erste Bit einer IP-Adresse 1 und das zweite Bit 0, gehört sie zur Klasse B. Das erste Oktett ist zwischen 128 und 191.

Sind die ersten 2 Bits einer IP-Adresse 1, gehört sie zur Klasse C. Das erste Oktett ist größer als 191.

Die Vergabe der Adresse des Hosts (*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), welche 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

### Wie man die Netzmaske verwendet

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?

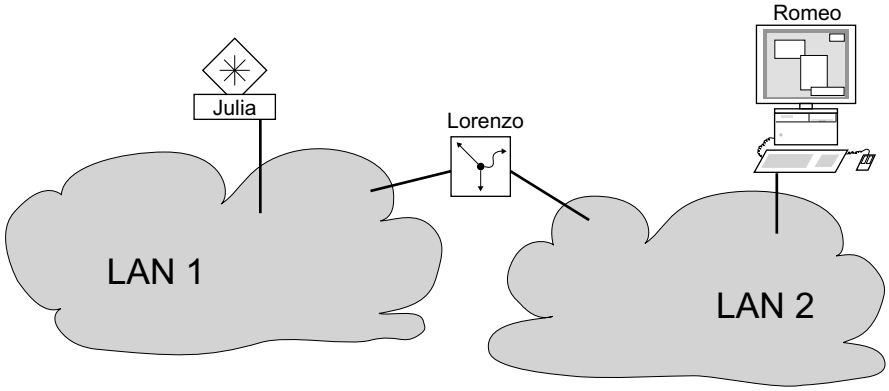



*Abb. 7: Management-Agent durch Router von der Netz-Management-Station getrennt*

Die Netz-Management-Station „Romeo” möchte Daten an den Management-Agenten „Julia” senden. 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 senden? 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 $(2^8-2)$ Adressen war zu klein und die Klasse B mit maximal 65534 $(2^{16}-2)$ Adressen war für die meisten Anwender zu groß, was zu einer ineffektiven Nutzung der vorhandenen Klasse-B-Adressen führte.

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 zur Lösung dieses Problems das Classless Inter-Domain Routing (CIDR). Das CIDR überwindet diese Klassenschranken und unterstützt klassenlose IP-Adressbereiche.

Mit CIDR legen Sie die Anzahl der Bits fest, welche den IP-Adressbereich kennzeichnen. Hierzu stellen Sie den IP-Adressbereich in binärer Form dar und zählen die Maskenbits, welche die Netzmaske kennzeichnen. 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. Supernetting ermöglicht Ihnen, Adressbereiche der Klasse B sehr fein zu untergliedern.

## 2.1.2 IPv6

### Grundlagen IP Parameter

Das Internet Protocol Version 6 (IPv6) ist die neue Version des Internet Protocol Version 4 (IPv4). Die Implementierung von IPv6 war notwendig, da die IPv4-Adressen aufgrund der großen Verbreitung des Internets nicht ausreichen. Das IPv6-Protokoll wird in RFC 8200 beschrieben.

Unterschiede zwischen IPv6 und IPv4 sind unter anderem:
- Darstellung und Länge der Adresse
- Keine Broadcast-Adressen
- Vereinfachung der Header-Struktur
- Fragmentierung erfolgt nur durch den Source Host
- Zusätzliche Möglichkeiten zur Erkennung von Paketflüssen im Netz

IPv4 und IPv6-Protokolle können im Gerät parallel betrieben werden. Das wird durch die Verwendung von Dual IP Layer, auch Dual Stack genannt, ermöglicht.

**Anmerkung:**
Wenn Sie das Gerät ausschließlich mit der Funktion IPv4 betreiben möchten, dann deaktivieren Sie die Funktion IPv6 im Gerät.

Im Gerät hat das IPv6-Protokoll folgende Einschränkungen:
- Sie können maximal 8 IPv6-Unicast-Adressen folgendermaßen festlegen:
  - 4 IPv6-Adressen durch manuelle Konfiguration
  - 2 IPv6-Adressen, wenn das Optionsfeld *Auto* ausgewählt ist
  - 1 IPv6-Adresse durch den DHCPv6-Server
  - 1 Link-Local-Adresse
- Die Funktion IPv6 kann ausschließlich im Management-Interface aktiviert werden. Alle konfigurierbaren IPv6-Adressen können gleichzeitig auf dem Interface verwendet werden.
- Mit den IPv6-Adressen kann die Management-IP-Adresse des Geräts festgelegt werden. Andere Dienste, bei denen IPv6-Adressen verwendet werden können, sind beispielsweise SNTP, SYSLOG, DNS und LDAP.

### Darstellung der Adresse

Die IPv6-Adresse besteht aus 128 Bits. Sie besteht aus 8 Blöcken mit 4 hexadezimalen Zahlen. Jeder Block stellt 16 Bits dar. Die 16-Bit-Blöcke werden durch Doppelpunkte (:) getrennt. Die Groß- und Kleinschreibung müssen Sie bei IPv6-Adressen nicht beachten.

Gemäß RFC 4291 ist das bevorzugte Format für eine IPv6-Adresse x:x:x:x:x:x:x:x. Jedes „x“ besteht aus 4 Hexadezimalwerten und stellt einen 16-Bit-Block dar. Ein Beispiel für die bevorzugte Schreibweise von IPv6-Adressen ist in der untenstehenden Abbildung zu sehen.

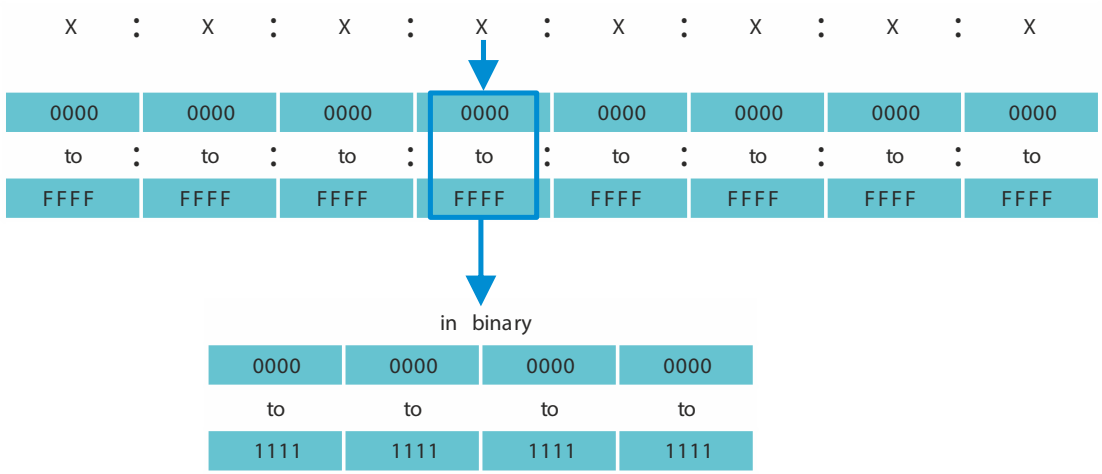



*Abb. 8: Darstellung der IPv6-Adresse*

Wie Sie der untenstehenden Abbildung entnehmen können, enthält eine IPv6-Adresse viele Nullen. Um IPv6-Adressen zu kürzen, die 0 Bits enthalten, müssen 2 Schreibregeln befolgt werden:

- Die erste Regel ist, führende Nullen in jedem 16-Bit-Block wegzulassen. Diese Regel bezieht sich ausschließlich auf führende Nullen und nicht auf angehängte Nullen in einem 16-Bit-Block. Wenn die angehängten Nullen ebenfalls weggelassen werden, dann ist die Adresse nicht mehr eindeutig.
- Bei der zweiten Regel werden die Nullen durch eine spezielle Syntax gekürzt. Sie können 2 Doppelpunkte nacheinander („::“) verwenden, um aufeinanderfolgende 16-Bit-Blöcke, die ausschließlich Nullen enthalten, zu ersetzen. Das Zeichen „::“ darf ausschließlich einmal in einer Adresse verwendet werden. Wenn das Zeichen „::“ mehr als einmal in der Darstellung einer Adresse verwendet wird, dann kann aus dieser Notation mehr als eine mögliche Adresse entwickelt werden.

Wenn beide Regeln angewendet werden, ist das Ergebnis die verkürzte Schreibweise.

In der untenstehenden Tabelle sehen Sie 2 Beispiele, wie diese Regeln angewendet werden:

*Tab. 8: Verkürzung von IPv6-Adressen*

| | |
|---|---|
| Bevorzugt | CC03:0000:0000:0000:0001:AB30:0400:FF02 |
| Keine führenden Nullen | CC03: 0: 0: 0: 1:AB30: 400:FF02 |
| Verkürzt | CC03::1:AB30:400:FF02 |

*Tab. 8: Verkürzung von IPv6-Adressen*

| | |
|---|---|
| Bevorzugt | 2008:00B7:0000:DEF0:DDDD:0000:E604:0001 |
| Keine führenden Nullen | 2008: B7: 0:DEF0:DDDD: 0:E604: 1 |
| Verkürzt | 2008:B7::DEF0:DDDD:0:E604:1 |

### Präfixlänge

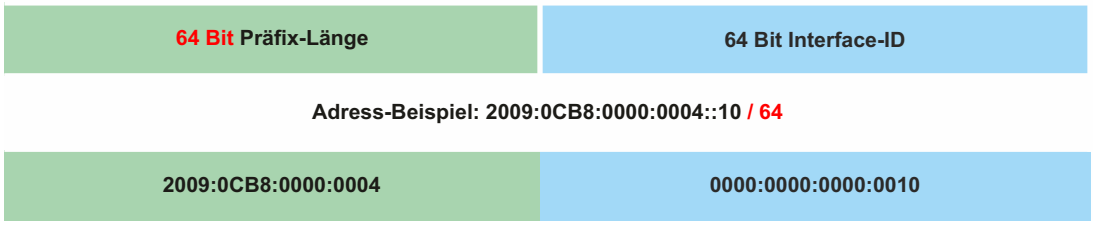
Im Gegensatz zu einer IPv4-Adresse verwendet eine IPv6-Adresse keine Subnetzmaske, um den Teil der Adresse zu kennzeichnen, der zum Subnetz gehört. Stattdessen nutzt das IPv6-Protokoll dafür die Präfixlänge.

Die Präfixe von IPv6-Adressen werden ähnlich geschrieben wie die Präfixe von IPv4-Adressen in Classless Inter-Domain Routing (CIDR):

`<IPv6-Adresse>/<Präfixlänge>`

Die Präfixlänge beträgt `0..128`. Die typische Präfixlänge von IPv6 für LANs und andere Netzwerktypen beträgt /64. Das bedeutet, dass der Netzanteil der Adresse 64 Bits lang ist. Die übrigen 64 Bits stellen die Interface-ID dar, ähnlich dem Host-Anteil der IPv4-Adresse.

In der untenstehenden Abbildung sehen Sie ein Beispiel für die Zuweisung von Präfixlängen in Bits.




### Arten von Adressen

Die Arten von IPv6-Adressen werden im RFC 4291 beschrieben.

Die Arten von IPv6-Adressen sind anhand ihrer höherwertigen Bits zu erkennen, wie in folgender Tabelle definiert:

*Tab. 9: Arten von IPv6-Adressen*

| Art der Adresse | Binärpräfix | IPv6-Notation |
|---|---|---|
| Nicht spezifiziert | 00...0 (128 bits) | ::/128 |
| Loopback | 00...1 (128 bits) | ::1/128 |
| Multicast | 11111111 | FF00::/8 |
| Link-Local-Unicast | 1111111010 | FE80::/10 |
| Global Unicast | (everything else) | |

### Nicht spezifizierte Adresse

Die IPv6-Adresse, bei der jedes Bit auf 0 gesetzt ist, nennt man unspezifizierte Adresse, was 0.0.0.0 in IPv4 entspricht. Die nicht spezifizierte Adresse zeigt das Fehlen einer Adresse an. Sie wird gewöhnlich als Quelladresse verwendet, wenn noch keine eigene Adresse feststeht.

**Anmerkung:**
Die nicht spezifizierte Adresse kann keinem Interface zugewiesen werden. Sie kann nicht als Zieladresse verwendet werden.

### Loopback-Adresse

Die Unicast-Adresse 0:0:0:0:0:0:0:1 nennt man Loopback-Adresse. Die Loopback-Adresse kann von einem Gerät dazu verwendet werden, ein IPv6-Paket an sich selbst zu senden. Die Loopback-Adresse kann keinem physischen Interface zugewiesen werden.

### Multicast-Adresse

IPv6 hat keine Broadcast-Adresse im Gegensatz zu IPv4. Doch es gibt eine IPv6-Multicast-Adresse „all nodes“, die im Wesentlichen das gleiche Ergebnis liefert.

Eine IPv6-Multicast-Adresse wird verwendet, um ein IPv6-Paket an mehrere Empfänger zu senden. Der Aufbau einer Multicast-Adresse ist folgendermaßen: Die nächsten 4 Bits zeigen den Scope der Multicast-Adresse an (wie weit das Paket übermittelt wird):

- Die ersten 8 Bits sind auf FF gesetzt.
- Die nächsten 4 Bits zeigen die zeitliche Begrenzung der Adresse an: 0 bedeutet permanent und 1 bedeutet temporär.
- Die nächsten 4 Bits bestimmen den Geltungsbereich (Scope) der Multicast-Adresse. Damit wird bestimmt, wie weit die Pakete im Netzwerk übermittelt werden.

### Link-Local-Adresse

Die Link-Local-Adresse wird verwendet, um mit anderen Geräten über denselben Link zu kommunizieren. „Link“ bezieht sich auf ein Subnetz. Router leiten Pakete mit Link-Local-Adressen als Quelle oder Ziel nicht an andere Links weiter.

Link-Local-Adressen werden verwendet, um Pakete über einen einzelnen Link zu vermitteln, wenn keine Router vorhanden sind oder bei Scopes wie automatische Adresskonfiguration und Neighbor-Discovery. Sie haben das folgende Format:

*Tab. 10: Format der Link-Local-Adresse*

| 10 Bits | 54 Bits | 64 Bits |
|---|---|---|
| 1111111010 | 0 | Interface-ID |

Die Link-Local-Adresse ist festgelegt und nicht veränderbar.

### Globale Unicast-Adresse

Eine Global-Unicast-Adresse ist global eindeutig und kann über das Internet geroutet werden. Diese Art von Adressen entsprechen den öffentlichen IPv4-Adressen. Gegenwärtig werden ausschließlich Global-Unicast-Adressen mit den ersten drei Bits 001 oder 2000::/3 zugewiesen.

Eine Global-Unicast-Adresse hat 3 Bereiche:
- Global-Routing-Präfix
- Subnetz-ID
- Interface-ID

Der Global-Routing-Präfix ist der Netzanteil der Adresse.

Als Subnetz-ID wird die Identifikation eines Subnetzes innerhalb einer Organisation angegeben. Sie ist bis zu 16 Bits lang. Die Länge der Subnetz-ID wird durch die Länge des Global-Routing-Präfixes bestimmt.

Die Interface-ID identifiziert ein Interface eines bestimmten Knotens. Es wird Interface-ID genannt, da ein Host mehrere Interfaces haben kann, von denen jedes eine oder mehrere IPv6-Adressen hat.

Das allgemeine Format für IPv6-Global-Unicast-Adressen ist in der untenstehenden Abbildung dargestellt.

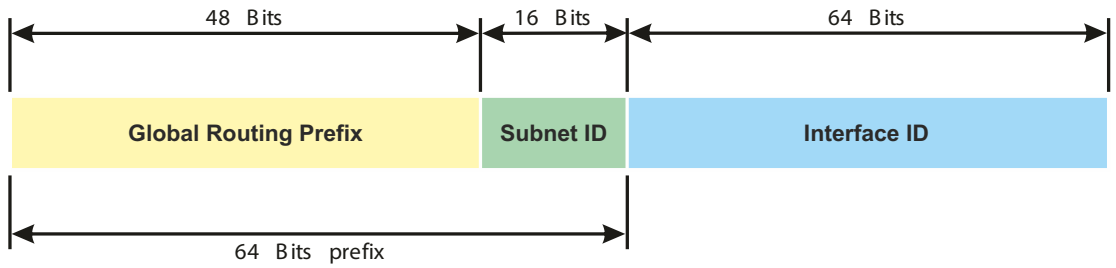



*Abb. 9: Allgemeines Format der IPv6-Global-Unicast-Adresse*

# 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

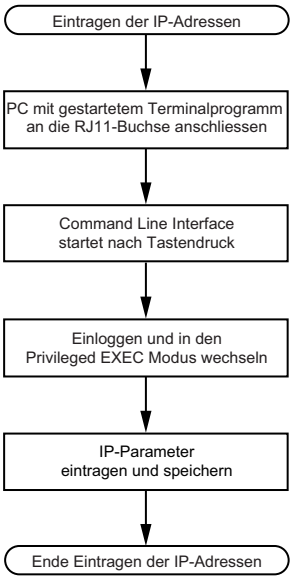
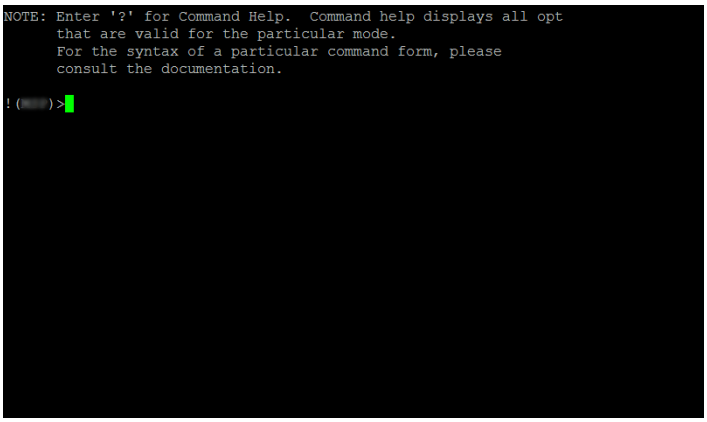



*Abb. 10: Ablaufdiagramm Eintragen der IP-Adressen*

**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 einrichten 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.

- ☐ Geben Sie die IP-Parameter ein.
  - Lokale IP-Adresse
    In der Voreinstellung ist die lokale IP-Adresse `0.0.0.0`.
  - Netzmaske
    Wenn Sie das Netz in Subnetze aufgeteilt haben und diese mit einer Netzmaske identifizieren, geben 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 „Wie man die Netzmaske verwendet").
    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 nichtflüchtigen Speicher (*NVM*) speichern. |

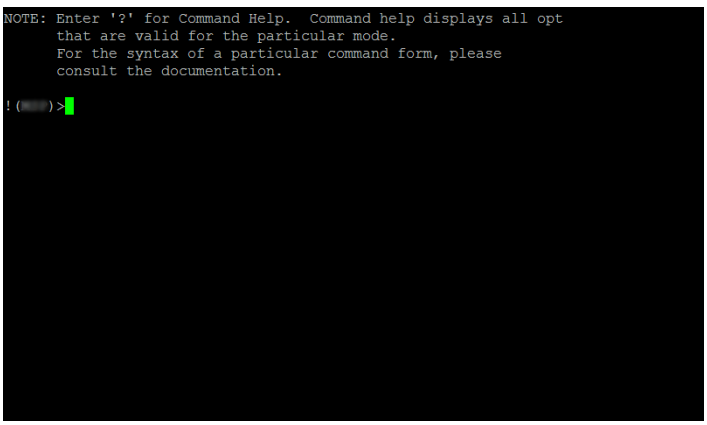
Nach Eingabe der IP-Parameter können Sie das Gerät über die grafische Benutzeroberfläche komfortabel einrichten.

### 2.2.2 IPv6

Das Gerät ermöglicht Ihnen, die IPv6-Parameter mittels Command Line Interface über die serielle Verbindung festzulegen. Um auf das Command Line Interface zuzugreifen, können Sie auch eine SSH-Verbindung unter Verwendung der IPv4-Management-Adresse nutzen.

Führen Sie die folgenden Schritte aus:

- ☐ Stellen Sie eine Verbindung zu dem Gerät her.
  Der Startbildschirm erscheint.



- ☐ Schalten Sie das IPv6-Protokoll ein, falls es ausgeschaltet ist.
- ☐ Geben Sie die IPv6-Parameter ein.
  - IPv6-Adresse
    Gültige IPv6-Adresse. Die IPv6-Adresse wird in einer verkürzten Schreibweise angezeigt.
  - Präfixlänge
    Im Gegensatz zu einer IPv4-Adresse verwendet eine IPv6-Adresse keine Subnetzmaske, um den Teil der Adresse zu kennzeichnen, der zum Subnetz gehört. Diese Funktion übernimmt in IPv6 die Präfixlänge (siehe auf Seite 49 „Präfixlänge").
  - Funktion *EUI-Option*
    Mit der *EUI-Option*-Funktion können Sie die Interface-ID der IPv6-Adresse automatisch festlegen. Das Gerät verwendet die MAC-Adresse des Interface, erweitert um die Werte `ff` und `fe` zwischen Byte 3 und Byte 4, um eine 64 Bit lange Interface-ID zu generieren.
    Sie können diese Option ausschließlich für IPv6-Adressen wählen, deren Präfixlänge `64` entspricht.
  - IPv6-Gateway-Adresse
    Die IPv6-Gateway-Adresse ist die Adresse eines Routers, über den das Gerät andere Geräte außerhalb des eigenen Netzes erreicht.
    Sie können alle IPv6-Adressen festlegen außer Loopback- und Multicast-Adressen.
    In der Voreinstellung ist die IPv6-Gateway-Adresse `::`.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `network ipv6 operation` | IPv6-Protokoll einschalten, falls es ausgeschaltet ist. In der Voreinstellung ist das IPv6-Protokoll aktiviert. |
| `network ipv6 address add 2001::1 64 eui-64` | IPv6-Adresse `2001::1` und Präfixlänge `64` zuweisen. Der Parameter `eui-64` ist optional.<br>Optional können Sie zusätzlich eine Gateway-Adresse zuweisen. |
| `copy config running-config nvm` | Aktuelle Einstellungen im „ausgewählten" Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) speichern. |

Nach Eingabe der IPv6-Parameter können Sie das Gerät über die grafische Benutzeroberfläche komfortabel einrichten. Für die Verwendung einer IPv6-Adresse in einer URL gilt die folgende URL-Syntax: `https://[<IPv6_Adresse>]`.

# 2.3 IP-Parameter mit HiDiscovery festlegen

Das HiDiscovery-Protokoll ermöglicht Ihnen, dem Gerät über das Ethernet IP-Parameter zuzuweisen.

Die anderen Parameter richten Sie komfortabel über die grafische Benutzeroberfläche ein.

Führen Sie die folgenden Schritte aus:
- ☐ Installieren Sie auf Ihrem Rechner das Programm HiDiscovery.
- ☐ Starten Sie das Programm HiDiscovery.

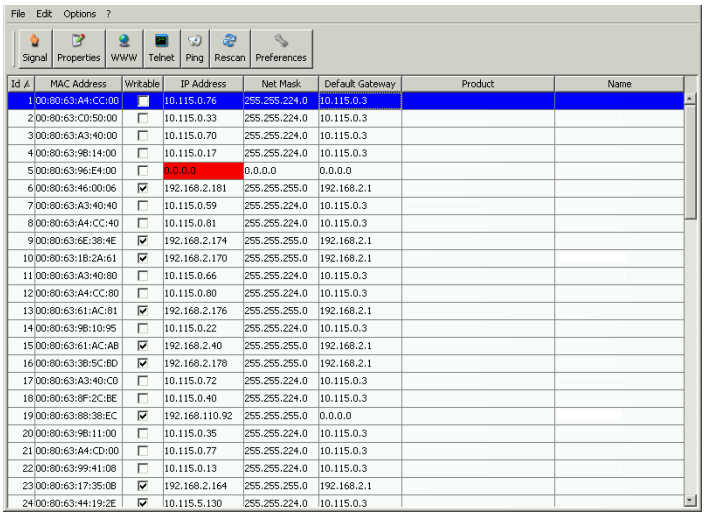



*Abb. 11: HiDiscovery*

Beim Start von HiDiscovery untersucht HiDiscovery automatisch das Netz nach Geräten, die das HiDiscovery-Protokoll unterstützen.

HiDiscovery benutzt die erste gefundene Netzschnittstelle des PCs. Wenn Ihr Computer über mehrere Netzschnittstellen verfügt, können Sie die gewünschte Netzschnittstelle in der Werkzeugleiste HiDiscovery auswählen.

HiDiscovery zeigt eine Zeile für jedes Gerät, das auf eine HiDiscovery-Protokoll-Abfrage reagiert.

HiDiscovery ermöglicht Ihnen 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.

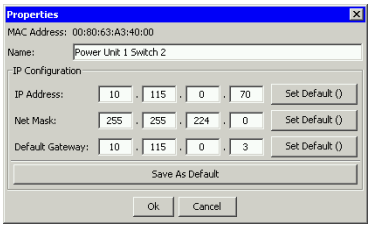



*Abb. 12: HiDiscovery – IP-Parameter-Zuweisung*

**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 > Netzwerk > Global*.

In diesem Dialog legen Sie das VLAN fest, in dem das Management des Geräts erreichbar ist, und richten den HiDiscovery-Zugang ein.

- ☐ 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 > Netzwerk > 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.

- ☐ Geben Sie im Rahmen *IP-Parameter* die IP-Adresse, die Netzmaske und das *Gateway* bei Bedarf ein.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

### 2.4.2 IPv6

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netzwerk > IPv6*.
- ☐ Das IPv6-Protokoll ist in der Voreinstellung aktiviert. Vergewissern Sie sich, dass das Optionsfeld *An* im Rahmen *Funktion* ausgewählt ist.
- ☐ Im Rahmen *Konfiguration* legen Sie fest, woher das Gerät seine IPv6-Parameter bezieht:
  - Wenn das Optionsfeld *Kein* ausgewählt ist, dann erhält das Gerät seine IPv6-Parameter durch manuelle Zuweisung.
    Sie können maximal 4 IPv6-Adressen manuell festlegen. Sie können Loopback-, Link-Local- und Multicast-Adressen nicht als statische IPv6-Adressen festlegen.
  - Wenn das Optionsfeld *Auto* ausgewählt ist, dann erhält das Gerät seine IPv6-Parameter durch dynamische Zuweisung, beispielsweise durch einen Router Advertisement Daemon (radvd).
    Das Gerät erhält maximal 2 IPv6-Adressen.
  - Wenn das Optionsfeld *DHCPv6* ausgewählt ist, dann erhält das Gerät seine IPv6-Parameter von einem DHCPv6-Server.
    Das Gerät kann ausschließlich eine IPv6-Adresse vom DHCPv6-Server erhalten.
  - Wenn das Optionsfeld *Alle* ausgewählt ist, dann erhält das Gerät seine IPv6-Parameter durch dynamische und manuelle Zuweisung.

**Anmerkung:**
Wenn Sie den Modus für die Zuweisung von IPv6-Adressen ändern, aktiviert das Gerät sofort den neuen Modus, wenn Sie die Schaltfläche ✓ klicken.

- ☐ Wenn nötig, geben Sie die *Gateway-Adresse* im Rahmen *IP-Parameter* ein.

  **Anmerkung:**
  Wenn das Optionsfeld *Auto* ausgewählt ist und Sie einen Router Advertisement Daemon (radvd) verwenden, dann erhält das Gerät automatisch eine Link-Local-Adresse als *Gateway-Adresse*, die eine höhere Metrik hat als die manuell eingestellte *Gateway-Adresse*.

- ☐ Im Rahmen *Erkennung doppelter Adressen* können Sie die Anzahl aufeinanderfolgender *Neighbor Solicitation*-Nachrichten festlegen, die das Gerät mit der Funktion *Erkennung doppelter Adressen* sendet (siehe auf Seite 64 „Funktion Erkennung doppelter Adressen").

Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

Legen Sie manuell eine IPv6-Adresse fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netzwerk > IPv6*.
- ☐ Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erstellen*.
  - ☐ Geben Sie die IPv6-Adresse in das Feld *IP-Adresse* ein.
  - ☐ Geben Sie die Präfixlänge der IPv6-Adresse in das Feld *Prefix-Länge* ein.
  - ☐ Klicken Sie die Schaltfläche *Ok*.
    Das Gerät fügt eine Tabellenzeile hinzu.

## 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 > Netzwerk >* IPv4 festgelegte 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 Dynamic Host Configuration Protocol (DHCP) 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 dauerhaft im nichtflüchtigen Speicher (*NVM*).

*Tab. 11: DHCP-Optionen, die das Gerät anfordert*

| Optionen | Bedeutung |
|---|---|
| 1 | Subnet Mask |
| 2 | Time Offset |
| 3 | Router |
| 4 | Time server |
| 12 | Hostname |
| 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 dazu kann der Client 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 Adresszuweisung).

In der Voreinstellung ist DHCP aktiviert. Solange DHCP aktiv ist, versucht das Gerät, eine IP-Adresse zu bekommen. Findet das Gerät nach einem Neustart keinen DHCP-Server, hat es keine IP-Adresse. Der Dialog *Grundeinstellungen > Netzwerk > IPv4* ermöglicht Ihnen, DHCP zu aktivieren oder zu 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.

### 2.6.2 IPv6

Das Dynamic Host Configuration Protocol version 6 (DHCPv6) ist ein Netzprotokoll, mit dem IPv6-Adressen dynamisch festgelegt werden. Dieses Protokoll ist das IPv6-Äquivalent zum Dynamic Host Configuration Protocol (DHCP) für IPv4. DHCPv6 ist im RFC 8415 beschrieben.

Das Gerät verwendet einen DHCP Unique Identifier (DUID), um eine Anfrage an den DHCPv6-Server zu senden. Im Gerät repräsentiert der DUID die *Client-ID*, die der DHCPv6-Server verwendet, um das Gerät zu identifizieren, das eine IPv6-Adresse angefordert hat.

Die *Client-ID* wird im Dialog *Grundeinstellungen > Netzwerk > IPv6* im Rahmen *DHCP* angezeigt.

Das Gerät kann ausschließlich eine IPv6-Adresse mit einer *Prefix-Länge* von 128 vom DHCPv6 erhalten. Keine *Gateway-Adresse*-Informationen werden bereitgestellt. Wenn nötig, können Sie die *Gateway-Adresse*-Informationen manuell festlegen.

In der Voreinstellung ist das DHCPv6-Protokoll deaktiviert. Sie können das Protokoll im Dialog *Grundeinstellungen > Netzwerk > IPv6* aktivieren oder deaktivieren. Vergewissern Sie sich, dass das Optionsfeld *DHCPv6* im Rahmen *Konfiguration* ausgewählt ist.

Wenn Sie eine IPv6-Adresse mit einer anderen *Prefix-Länge* als 128 dynamisch anfordern möchten, dann wählen Sie das Optionsfeld *Auto* aus. Ein Beispiel ist der Router Advertisement Daemon (radvd). Der radvd verwendet *Router Solicitation*- und *Router Advertisement*-Nachrichten, um automatisch eine IPv6-Adresse einzurichten.

In der Voreinstellung ist das Optionsfeld *Auto* ausgewählt. Sie können das Optionsfeld *Auto* im Dialog *Grundeinstellungen > Netzwerk > IPv6*, Rahmen *Konfiguration* auswählen oder die Auswahl aufheben.

Wenn das Optionsfeld *Alle* ausgewählt ist, dann erhält das Gerät seine IPv6-Parameter durch dynamische und manuelle Zuweisung.

# 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 Systemstart sowie die Durchführung regelmäßiger 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`
- *Erkennung Modus*: `aktiv und passiv`
- *Periodische ARP-Überprüfung senden*: `markiert`
- *Erkennung 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 festgelegten 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 festgelegte 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, welche 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.

# 2.8 Funktion Erkennung doppelter Adressen

Die Funktion *Erkennung doppelter Adressen* bestimmt die Eindeutigkeit einer IPv6-Unicast-Adresse auf einem Interface. Die Funktion wird ausgeführt, wenn eine IPv6-Adresse manuell oder mit den Methoden *DHCPv6* oder *Auto* eingerichtet wird. Die Funktion wird ebenfalls ausgeführt, wenn sich ein Verbindungsstatus ändert, zum Beispiel von inaktiv zu aktiv.

Die Funktion *Erkennung doppelter Adressen* verwendet *Neighbor Solicitation*- und *Neighbor Advertisement*-Nachrichten. Sie können einstellen, wie viele aufeinanderfolgende *Neighbor Solicitation*-Nachrichten das Gerät sendet. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netzwerk > IPv6*.
- ☐ Im Rahmen *Erkennung doppelter Adressen* legen Sie den nötigen Wert im Feld *Anzahl der Nachbarn* fest.
  Mögliche Werte:
  - `0`
    Die Funktion ist ausgeschaltet.
  - `1..5` (Voreinstellung: `1`)
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `network ipv6 dad-transmits <0..5>` | Anzahl von *Neighbor Solicitation*-Nachrichten einstellen, die das Gerät sendet.<br>Der Wert `0` deaktiviert die Funktion. |

**Anmerkung:**
Wenn die Funktion *Erkennung doppelter Adressen* erkennt, dass eine IPv6-Adresse auf einem Link nicht eindeutig ist, dann protokolliert das Gerät dieses Ereignis nicht in der Log-Datei (System Log).

# 3 Zugriff auf das Gerät

## 3.1 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 beim Management des Geräts anmelden.
- ☐ Melden Sie sich mit dem voreingestellten Passwort beim Management des Geräts 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 beim Management des Geräts anmelden, fordert Sie das Gerät auf, Ihr neues Passwort zu bestätigen.
- ☐ Melden Sie sich mit Ihrem neuen Passwort erneut beim Management des Geräts an.

**Anmerkung:**
Wenn Sie Ihr Passwort vergessen haben, dann wenden Sie sich an Ihren lokalen Support.

# 3.2 Authentifizierungs-Listen

Wenn ein Benutzer über eine bestimmte Verbindung auf das Management des Geräts zugreift, verifiziert das Gerät die Anmeldedaten des Benutzers durch eine Authentifizierungs-Liste, welche 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.

## 3.2.1 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 die 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`

## 3.2.2 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
- 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.

## 3.2.3 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.

☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

| | |
|---|---|
| `authlists disable defaultDot1x8021AuthList` | Authentifizierungs-Liste deaktivieren.`default-Dot1x8021AuthList`. |

### 3.2.4 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- oder TACACS+-Server weiter. Als Fallback-Lösung authentifiziert das Gerät die Benutzer über die lokale Benutzerverwaltung. Führen Sie dazu die folgenden Schritte aus:

☐ Erstellen Sie eine Authentifizierungs-Liste `loginGUI`.

☐ Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

☐ Klicken Sie die Schaltfläche .
Der Dialog zeigt das Fenster *Erstellen*.
- ☐ Geben Sie in das Feld *Name* eine aussagekräftige Bezeichnung ein.
  Geben Sie in diesem Beispiel den Namen `loginGUI` ein.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Gerät fügt eine Tabellenzeile hinzu.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `authlists add loginGUI` | Die Authentifizierungs-Liste `loginGUI` hinzufügen. |

☐ 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.

☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

| | |
|---|---|
| `authlists set-policy loginGUI radius local reject reject reject` | Die Richtlinien *radius*, *lokal* und *reject* der Authentifizierungs-Liste `loginGUI` zuweisen. |
| `show authlists` | Eingerichtete Authentifizierungs-Listen anzeigen. |

☐ 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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. |

# 3.3 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, mit einem RADIUS- oder mit einem TACACS+-Server im Netz. Damit das Gerät auf die Benutzerverwaltung zurückgreift, weisen Sie einer Authentifizierungsliste die Richtlinie `Lokal` zu, siehe Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

In der lokalen Benutzerverwaltung verwalten Sie die Benutzerkonten. Jedem Benutzer ist in aller Regel jeweils ein Benutzerkonto zugeordnet.

## 3.3.1 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.

**Anmerkung:**
Für das Command Line Interface gilt: Benutzer, denen ein bestimmtes Berechtigungsprofil zugeordnet ist, sind befugt, Kommandos und Funktionen aus diesem oder einem niedrigeren Berechtigungsprofil anzuwenden. Welche Kommandos einem Benutzer zur Verfügung stehen, hängt auch davon ab, in welchem Modus des Command Line Interface er sich gerade befindet. Siehe „Modus-basierte Kommando-Hierarchie” auf Seite 21.

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.

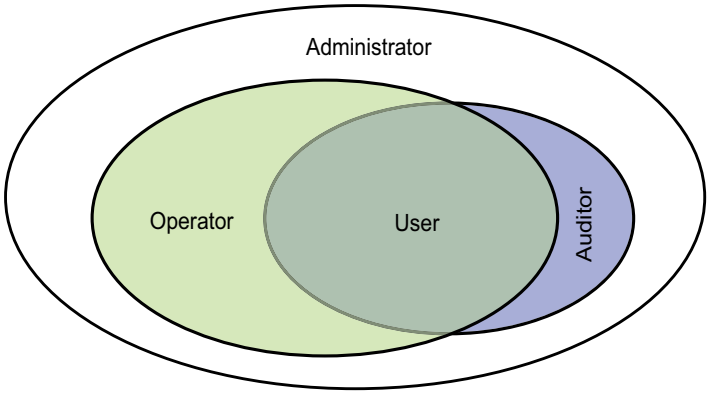



*Abb. 13: Berechtigungen für Benutzerkonten*

*Tab. 12: 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:<br>• Benutzerkonten hinzufügen, ändern und löschen<br>• Benutzerkonten aktivieren, deaktivieren und entsperren<br>• Jedes Passwort ändern<br>• Das Passwort-Management einrichten<br>• Systemzeit einstellen und ändern<br>• Dateien auf das Gerät laden, zum Beispiel Geräteeinstellungen, Zertifikate oder Images der Geräte-Software<br>• Einstellungen und sicherheitsbezogene Einstellungen auf den Lieferzustand zurück-setzen<br>• Den RADIUS- oder TACACS+-Server und die Authentifizierungslisten einrichten<br>• Skripte anwenden mit dem Command Line Interface<br>• CLI-Logging und SNMP-Logging ein- und ausschalten<br>• Externen Speicher aktivieren und deaktivieren<br>• System Monitor 1 aktivieren oder deaktivieren<br>• Dienste für den Zugriff auf das Management des Geräts (zum Beispiel SNMP) ein- und ausschalten.<br>• Zugriffsbeschränkungen auf die grafische Benutzeroberfläche oder das Command Line Interface auf Basis der IP-Adresse einrichten |
| *operator* | Der Benutzer ist berechtigt, das Gerät zu überwachen und zu konfigurieren, mit Ausnahme sicherheitsbezo-gener Einstellungen. | Sämtliche Tätigkeiten mit Lese-/Schreibzugriff mit Ausnahme der o.g. Tätigkeiten, die ausschließlich einem Administrator vorbehalten sind. |

*Tab. 12: 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.<br>• Als Administrator weisen Sie diese Berechtigung zu, um ein Benutzerkonto vorübergehend zu sperren.<br>• Wenn beim Zuweisen einer anderen Berechtigung ein Fehler erkannt wird, dann weist das Gerät dem Benutzerkonto diese Berechtigung zu. | Keine erlaubten Tätigkeiten. |

### 3.3.2 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.

### 3.3.3 Voreingestellte Benutzerkonten

In der Voreinstellung ist im Gerät das Benutzerkonto `admin` eingerichtet.

*Tab. 13: Einstellungen des voreingestellten Benutzerkontos*

| Parameter | Voreinstellung |
|---|---|
| *Benutzername* | `admin` |
| *Passwort* | `private` |
| *Rolle* | *`administrator`* |
| *Benutzer gesperrt* | `unmarkiert` |
| *Richtlinien überprüfen* | `unmarkiert` |
| *SNMP-Authentifizierung* | *`hmacmd5`* |
| *SNMP-Verschlüsselung* | *`des`* |

Ändern Sie das Passwort des Benutzerkontos `admin`, bevor Sie das Gerät im Netz zugänglich machen.

### 3.3.4 Voreingestellte Passwörter ändern

Um unerwünschte Eingriffe zu vermeiden, ändern Sie das Passwort des voreingestellten Benutzerkontos. Führen Sie dazu die folgenden Schritte aus:

☐ Ändern Sie das Passwort für das Benutzerkonto `admin`.

☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
Der Dialog zeigt die eingerichteten Benutzerkonten.

☐ Um eine festgelegte Mindestkomplexität für die Passwörter vorzuschreiben, 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 *Diagnose > Statuskonfiguration > Sicherheitsstatus*.

☐ Klicken Sie in der Tabellenzeile des betreffenden Benutzerkontos in das Feld *Passwort*.
Geben Sie ein 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.

☐ Wenden Sie die Einstellungen vorläufig an. 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. Auf diese Weise geben Sie eine höhere Mindestkomplexität für die Passwörter vor. |

**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. Geben Sie mindestens 6 Zeichen ein. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern. |

### 3.3.5 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 richten Sie das Benutzerkonto für einen Benutzer `USER` mit der Zugriffsrolle *operator* ein. Benutzer mit der Zugriffsrolle *operator* sind berechtigt, das Gerät zu überwachen und einzurichten, mit Ausnahme sicherheitsbezogener Einstellungen. Führen Sie dazu die folgenden Schritte aus:

☐ Erstellen Sie ein Benutzerkonto.

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Erstellen*.
- ☐ Geben Sie in das Feld *Benutzername* die Bezeichnung ein.
  In diesem Beispiel geben Sie dem Benutzerkonto die Bezeichnung `USER`.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Um eine festgelegte Mindestkomplexität für die Passwörter vorzuschreiben, markieren Sie das Kontrollkästchen in Spalte *Richtlinien überprüfen*.
  Das Gerät prüft das Passwort vor dem Speichern anhand der im Rahmen *Passwort-Richtlinien* festgelegten Richtlinien.
- ☐ Geben 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 Zugriffsrolle.
  In diesem Beispiel wählen Sie den Wert *operator*.
- ☐ Um das Benutzerkonto zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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` hinzufügen. |
| `users password-policy-check USER enable` | Für das Benutzerkonto `USER` das Prüfen des Passwortes anhand der festgelegten Richtlinien aktivieren. Auf diese Weise geben Sie eine höhere Mindestkomplexität für die Passwörter vor. |
| `users password USER SECRET` | Für das Benutzerkonto `USER` das Passwort `SECRET` festlegen. Geben Sie mindestens 6 Zeichen ein. |
| `users access-role USER operator` | Dem `USER`-Benutzerkonto die Zugriffsrolle *`operator`* zuweisen. |
| `users enable USER` | Benutzerkonto `USER` aktivieren. |
| `show users` | Eingerichtete Benutzerkonten anzeigen. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern. |

**Anmerkung:**
Denken Sie daran, das Passwort zuzuweisen, wenn Sie ein neues Benutzerkonto im Command Line Interface einrichten.

### 3.3.6 Automatische Entsperrung von Benutzerkonten

Wenn ein Benutzer die maximale Anzahl nacheinander fehlgeschlagener Anmeldeversuche überschreitet, sperrt das Gerät das Benutzerkonto. Wenn die automatische Entsperrung von Benutzerkonten eingeschaltet ist, entsperrt das Gerät gesperrte Benutzerkonten automatisch. Jedes Benutzerkonto wird entsperrt, sobald seine festgelegte Wartezeit abgelaufen ist. Ein Benutzer mit der Zugriffsrolle *`administrator`* kann ein Benutzerkonto manuell entsperren, bevor die automatische Entsperrung erfolgt.

Ausschließlich ein Benutzer mit der Zugriffsrolle *`administrator`* kann die automatische Entsperrung von Benutzerkonten ein-/ausschalten und die Wartezeit für die automatische Entsperrung ändern. Die Wartezeit ist für jedes Benutzerkonto individuell einstellbar.

**Anmerkung:**
Ein Benutzer kann nicht auf das Management des Geräts zugreifen, wenn das Benutzerkonto gesperrt ist. Um den kontinuierlichen Zugriff auf das Management des Geräts zu gewährleisten, sperrt das Gerät das letzte Benutzerkonto mit der Zugriffsrolle *`administrator`* nicht.

### Automatische Entsperrung von Benutzerkonten einschalten

Die Funktion *Benutzer automatisch entsperren* ist in der Voreinstellung ausgeschaltet. Um die Funktion einzuschalten, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
  Der Dialog zeigt die auf dem Gerät eingerichteten Benutzerkonten.
- ☐ Schalten Sie die Funktion *Benutzer automatisch entsperren* ein. Markieren Sie dazu im Rahmen *Konfiguration* das Kontrollkästchen *Benutzer automatisch entsperren*.
- ☐ Legen Sie in Spalte *Timer für automatische Entsperrung [min]* des betreffenden Benutzerkontos die gewünschte Wartezeit fest.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `passwords auto-unlock-users` | Die automatische Entsperrung von Benutzerkonten einschalten. |
| `user auto-unlock-timer USER1 40` | Eine Wartezeit von `40` Minuten für das Benutzerkonto `USER1` festlegen. Legen Sie die Wartezeit als ganze Zahl fest. Der Name des Benutzerkontos und die Wartezeit dienen ausschließlich als Beispiele. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

### Auswirkung auf gesperrte Benutzerkonten

Das Gerät setzt einen laufenden Timer in den folgenden Fällen zurück:

- Ausschalten und erneutes Einschalten der *Benutzer automatisch entsperren*-Funktion.
- Ändern der Wartezeit, während das betreffende Benutzerkonto gesperrt ist und der Timer läuft.

In diesen Fällen startet das Gerät den Timer mit der festgelegten Wartezeit erneut. Folglich bleibt das Konto gesperrt, bis die gesamte Wartezeit abgelaufen ist.

### Automatische Entsperrung von Benutzerkonten ausschalten

Wenn die automatische Entsperrung von Benutzerkonten ausgeschaltet ist, bleiben alle gegenwärtig gesperrten Benutzerkonten gesperrt, bis ein Benutzer mit der Zugriffsrolle *`administrator`* sie entsperrt. Um die automatische Entsperrung von Benutzerkonten auszuschalten, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
- ☐ Schalten Sie die Funktion *Benutzer automatisch entsperren* aus. Heben Sie dazu im Rahmen *Konfiguration* die Markierung des Kontrollkästchens auf.*Benutzer automatisch entsperren*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `no passwords auto-unlock-users` | Automatische Entsperrung von Benutzerkonten ausschalten. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern. |

### 3.3.7 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 Tabellenzeile des betreffenden Benutzerkontos die Markierung des Kontrollkästchens *Aktiv* auf.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 nichtflüchtigen 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 nichtflüchtigen Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern. |

### 3.3.8 Richtlinien für Passwörter anpassen

Das Gerät ermöglicht Ihnen zu prüfen, ob die Passwörter für die Benutzerkonten der vorgegebenen Richtlinie entsprechen. Wenn die Passwörter den Passwortregeln entsprechen, erreichen Sie eine höhere Komplexität der Passwörter.

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.

In der Voreinstellung 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 aufeinanderfolgende erfolglose 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 aufeinanderfolgenden erfolglosen 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 Command Line Interface über die serielle Verbindung ist die Anzahl erfolgloser Login-Versuche unbegrenzt.

☐ Legen Sie die Werte entsprechend Ihren Anforderungen fest.
  – Im Feld *Login-Versuche* legen Sie fest, wie oft ein Anwender versuchen kann, sich beim Management des Geräts anzumelden. 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` einzugeben.

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.

☐ Wenden Sie die Einstellungen vorläufig an. 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 nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

# 3.4 SNMP-Zugriff

Das Simple Network Management Protocol (SNMP) ermöglicht Ihnen, mit einem Netzmanagementsystem das Gerät über das Netz zu überwachen und seine Einstellungen zu ändern.

## 3.4.1 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 *Lesezugriff* und `private` für *Lese- und Schreibzugriff*. 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- und 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.

## 3.4.2 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 im Netzmanagementsystem anzupassen, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
  Der Dialog zeigt die eingerichteten Benutzerkonten.
- ☐ Klicken Sie in der Tabellenzeile des betreffenden Benutzerkontos in das Feld *SNMP-Authentifizierung*.
  Wählen Sie die gewünschte Einstellung.
- ☐ Klicken Sie in der Tabellenzeile des betreffenden Benutzerkontos in das Feld *SNMP-Verschlüsselung*.
  Wählen Sie die gewünschte Einstellung.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `users snmpv3 authentication <user> <auth type>` | Den Algorithmus festlegen, den das Gerät zum Authentifizieren des SNMPv3-Benutzers `<user>` anwendet.<br>Mögliche `<auth type>`-Werte:<br>• `md5`<br>• `sha1`<br>• `sha256` |
| `users snmpv3 encryption <user> <encryption type>` | Den Algorithmus festlegen, den das Gerät zum Verschlüsseln der SNMPv3-Nachrichten des SNMPv3-Benutzers `<user>` anwendet.<br>Mögliche `<encryption type>`-Werte:<br>• `des`<br>• `aescfb128`<br>• `aescfb256`<br>• `none` (keine Verschlüsselung) |
| `show users` | Die eingerichteten Benutzerkonten anzeigen. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

### 3.4.3 SNMPv3-Traps

SNMP Version 3 ermöglicht, dass das Gerät verschlüsselt mit einem Netzwerkmanagementsystem kommuniziert.

Richten Sie dazu die folgenden Rollen im Gerät ein:
- SNMPv3-Trap-Benutzer
- SNMPv3-Trap Hosts

### SNMPv3-Trap-Benutzer

Ein SNMPv3-Trap-Benutzer hat die Berechtigung, SNMPv3-Traps an die festgelegten SNMPv3-Trap-Hosts zu senden.

Ein SNMPv3-Trap-Benutzer ist ausschließlich für das Senden von SNMPv3-Traps an SNMPv3-Trap-Hosts bestimmt. Verwechseln Sie SNMPv3-Trap-Benutzer nicht mit Benutzerkonten für das Gerät. Siehe Abschnitt „Benutzerkonten verwalten” auf Seite 71.

Das Gerät unterstützt Verschlüsselung und Authentifizierung für das Senden von SNMPv3-Traps. Das Gerät ermöglicht Ihnen, maximal 10 SNMPv3-Trap-Benutzer einzurichten.

Das Gerät unterstützt die folgenden Authentifizierungs- und Verschlüsselungsmethoden:

- `auth-no-priv`
  Der Benutzer kann ausschließlich nach Authentifizierung SNMPv3-Traps senden. Das Gerät sendet die SNMPv3-Traps unverschlüsselt.
- `auth-priv`
  Der Benutzer kann ausschließlich nach Authentifizierung SNMPv3-Traps senden. Das Gerät sendet die SNMPv3-Traps verschlüsselt.
- `no-auth`
  Verwenden Sie diese Einstellung nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  Das Gerät sendet die SNMPv3-Traps unverschlüsselt ohne Authentifizierung.

Um einen SNMPv3-Trap-Benutzer hinzuzufügen, führen Sie die folgenden Schritte aus:

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `snmp notification user add <name1> auth-priv auth <authentication algorithm> <passphrase1> priv <encryption algorithm> <passphrase2>` | Den SNMPv3-Trap `<name1>`-Benutzer hinzufügen, mit Authentifizierung und Verschlüsselung.<br>• `<authentication algorithm>`<br>Mögliche Werte:<br>– `md5`<br>– `sha1`<br>– `sha256` (empfohlen)<br>• `<passphrase1>`<br>Passwort für die Authentifizierung<br>• `<encryption algorithm>`<br>Mögliche Werte:<br>– `des`<br>– `aescfb128`<br>– `aescfb256` (empfohlen)<br>• `<passphrase2>`<br>Passwort für die Verschlüsselung |
| `show snmp notification users` | Einstellungen für die SNMPv3-Trap-Benutzer zeigen. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

Um einen bestehenden SNMPv3-Trap-Benutzer zu modifizieren, löschen Sie den Benutzer und fügen Sie einen neuen Benutzer mit den gewünschten Einstellungen hinzu.

Um einen SNMPv3-Trap-Benutzer zu löschen, führen Sie die folgenden Schritte aus:

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `snmp notification user delete <name1>` | Den SNMPv3-Trap `<name1>`-Benutzer löschen. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern. |

### SNMPv3-Trap Hosts

Ein SNMPv3-Trap-Host ist das Ziel für einen SNMPv3-Trap, den das Gerät sendet.

Das Gerät unterstützt maximal 10 SNMP-Trap-Hosts.

Um einen SNMPv3-Trap-Host festzulegen, führen Sie die folgenden Schritte aus:

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `snmp notification host add <hostname1> a.b.c.d user <name2> auth-priv` | SNMPv3-Trap-Host `<hostname1>` hinzufügen<br>• Mit der IPv4-Adresse `<a.b.c.d>`<br>• Benutzername `<name2>`<br>• Mit Authentifizierung und Verschlüsselung |
| `show snmp notification hosts` | Einstellungen für den SNMPv3-Trap-Host zeigen. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern. |

Um einen bestehenden SNMPv3-Trap-Host zu modifizieren, löschen Sie den Host und fügen Sie einen neuen Host mit den gewünschten Einstellungen hinzu.

Um einen SNMPv3-Trap-Host zu löschen, führen Sie die folgenden Schritte aus:

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `snmp notification host delete <hostname1>` | Den SNMPv3-Trap-Host `<hostname1>` löschen. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil speichern. |

## 3.5 Out-of-Band-Zugriff

Das Gerät verfügt über einen separaten Port, der Ihnen Out-of-Band-Zugriff auf das Management des Geräts ermöglicht. Bei hoher In-Band-Last auf den Switching-Ports haben Sie über diesen separaten Port dennoch Zugriff auf das Management des Geräts.

Voraussetzung ist, dass Sie die Management-Station direkt an den USB-Port anschließen. Wenn Sie Microsoft Windows verwenden, installieren Sie gegebenenfalls den RNDIS-Treiber. Sobald Sie die Management-Station angeschlossen haben, kann diese über eine virtuelle Netzverbindung mit dem Management des Geräts kommunizieren.

In der Voreinstellung können Sie über diesen Port mit folgenden IP-Parametern auf das Management des Geräts zugreifen:

- *IP-Adresse* `192.168.248.100`
- *Netzmaske* `255.255.255.0`

Das Gerät ermöglicht Ihnen mittels folgender Protokolle den Zugriff auf das Management des Geräts:

- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP
- Industrieprotokolle
  - *IEC 61850/MMS*
  - *Modbus TCP*

### 3.5.1 IP-Parameter festlegen

Wenn Sie die Management-Station über den USB-Port anschließen, weist das Gerät die IP-Adresse der USB-Netzschnittstelle, um 1 erhöht, der Management-Station zu (in der Voreinstellung `192.168.248.101`). Das Gerät ermöglicht Ihnen, die IP-Parameter zu ändern, um das Gerät an die Anforderungen in Ihrer Umgebung anzupassen.

Vergewissern Sie sich, dass das IP-Subnetz dieser Netzschnittstelle sich nicht mit einem Subnetz überschneidet, das mit einem anderen Interface des Gerätes verbunden ist:

- Management-Interface

Wenn die Management-Station über den USB-Port auf das Management des Geräts zugreift, unterbricht das Gerät die Verbindung zur grafischen Benutzeroberfläche und zum Command Line Interface unmittelbar nachdem Sie die Änderungen durchgeführt haben.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Out-of-Band via USB*.
- ☐ Überschreiben Sie die IP-Adresse im Rahmen *IP-Parameter*, Feld *IP-Adresse*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

```
enable                                          In den Privileged-EXEC-Modus wechseln.
network usb parms 192.168.1.1 255.255.255.0     IP-Adresse 192.168.1.1 und Netzmaske
                                                255.255.255.0 für die USB-Netzschnittstelle fest-
                                                legen.
show network usb                                Einstellungen der USB-Netzschnittstelle anzeigen.
Out-of-band USB management settings
-----------------------------------
Management operation.....................enabled
IP address...............................192.168.1.1
Subnet mask..............................255.255.255.0
Host MAC address.........................64:60:38:1f:85:85
Device MAC address.......................64:60:38:1f:85:86

save                                            Einstellungen im nichtflüchtigen Speicher (nvm) im
                                                „ausgewählten" Konfigurationsprofil speichern.
```

### 3.5.2 USB-Netzschnittstelle ausschalten

In der Voreinstellung ist die USB-Netzschnittstelle eingeschaltet. Wenn Sie nicht möchten, dass jemand über den USB-Port auf das Management des Geräts zugreift, dann ermöglicht Ihnen das Gerät, die USB-Netzschnittstelle auszuschalten.

Wenn die Management-Station über den USB-Port auf das Management des Geräts zugreift, unterbricht das Gerät die Verbindung zur grafischen Benutzeroberfläche und zum Command Line Interface unmittelbar nachdem Sie die Änderungen durchgeführt haben.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Out-of-Band via USB*.
- ☐ Schalten Sie die USB-Netzschnittstelle aus.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

```
enable                                          In den Privileged-EXEC-Modus wechseln.
no network usb operation                        USB-Netzschnittstelle ausschalten.
Out-of-band USB management settings
-----------------------------------
Management operation.....................disabled
IP address...............................192.168.1.1
Subnet mask..............................255.255.255.0
Host MAC address.........................64:60:38:1f:85:85
Device MAC address.......................64:60:38:1f:85:86

save                                            Einstellungen im nichtflüchtigen 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
- Prozess-Steuerung

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 das Simple Network Time Protocol (SNTP) eine Genauigkeit im Millisekunden-Bereich. Die Genauigkeit ist abhängig von der Signallaufzeit.

## 4.1 Uhrzeit einstellen

Wenn Ihnen keine Referenzzeitquelle zur Verfügung steht, können Sie die Systemzeit im Gerät manuell einstellen.

Wenn Sie das für einige Zeit ausgeschaltete Gerät einschalten, stellt es die Uhr auf den 1. Januar 2026, 01:00 UTC+1. Nach dem Ausschalten puffert das Gerät die Einstellungen seiner Echtzeituhr für bis zu 24 Stunden.

Alternativ dazu können Sie das Gerät so einrichten, dass es die aktuelle Zeit mittels eines der folgenden Protokolle bezieht:
- Simple Network Time Protocol

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Zeit > Grundeinstellungen*.
- Das Feld *Systemzeit (UTC)* zeigt Datum und Uhrzeit der Systemuhr des Geräts bezogen auf die koordinierte Weltzeit (UTC). Die UTC ist weltweit gleich und berücksichtigt keine lokalen Zeitverschiebungen.
- Die Zeit im Feld *Systemzeit* ergibt sich aus der *Systemzeit (UTC)* zuzüglich dem Wert *Lokaler Offset [min]* sowie einer möglichen Verschiebung durch die Sommerzeit.
- ☐ Damit das Gerät die Zeit Ihres Computers 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 *Zeitquelle* zeigt den Ursprung der Zeitangabe. Das Gerät wählt automatisch die Quelle mit der höchsten Genauigkeit.
  Die Quelle ist zunächst `lokal`.
  Ist SNTP aktiviert und empfängt das Gerät ein gültiges SNTP-Paket, setzt es seine Zeitquelle auf `sntp`.
- Der Wert *Lokaler Offset [min]* legt die Differenz in Minuten zwischen der koordinierten Weltzeit (UTC) und der Ortszeit fest.

☐ Damit das Gerät die Zeitzone Ihres PCs ermittelt, klicken Sie die Schaltfläche *Setze Zeit vom PC*. Das Gerät berechnet die Differenz zwischen Ortszeit und koordinierter Weltzeit (UTC) 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.

☐ Wenden Sie die Einstellungen vorläufig an. 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>` | Differenz in Minuten zwischen der Ortszeit und der empfangenen koordinierten Weltzeit (UTC) eingeben. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

# 4.2 Sommerzeit automatisch umschalten

Wenn Sie das Gerät in einer Zeitzone mit Sommerzeitumstellung betreiben, ermöglicht Ihnen das Gerät, die Sommerzeitumstellung automatisch durchzuführen.

Wenn der *Sommerzeit*-Modus eingeschaltet ist, stellt das Gerät während der Sommerzeit seine Ortszeit um eine Stunde vor. Am Ende der Sommerzeit stellt das Gerät seine Ortszeit wieder um eine Stunde zurück.

## 4.2.1 Sommerzeiteinstellung mittels vordefinierter Profile

Das Gerät ermöglicht Ihnen, Beginn und Ende der Sommerzeit mittels vordefinierter Profile festzulegen.

Das Gerät enthält folgende vordefinierte Profile:

- *EU*
  Sommerzeiteinstellungen, die in der Europäischen Union gelten.
- *USA*
  Sommerzeiteinstellungen, die in den Vereinigen Staaten von Amerika gelten.

Führen Sie die folgenden Schritte aus, um das Profil *EU* für die Sommerzeiteinstellungen auszuwählen:

- ☐ Öffnen Sie den Dialog *Zeit > Grundeinstellungen*, Registerkarte *Sommerzeit*.
- ☐ Klicken Sie im Rahmen *Funktion* die Schaltfläche *Profil...*.
- ☐ Wählen Sie aus der Liste *Profil...* den Eintrag *EU*.
  Das Auswählen eines Profils überschreibt die in den Rahmen *Sommerzeit Beginn* und *Sommerzeit Ende* festgelegten Einstellungen.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `clock summer-time mode eu` | Modus *Sommerzeit* mit dem Profil `eu` einschalten. |

## 4.2.2 Sommerzeit manuell einstellen

Der Administrator des Netzwerks möchte die folgenden Sommerzeiteinstellungen festlegen:

*Sommerzeit Beginn*
- *Woche* = *letzte*
- *Tag* = *Sonntag*
- *Monat* = *März*
- *Systemzeit* = *02:00*

*Sommerzeit Ende*
- *Woche* = *letzte*

- *Tag* = *Sonntag*
- *Monat* = *Oktober*
- *Systemzeit* = 03:00

Führen Sie zu diesem Zweck die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Zeit > Grundeinstellungen*, Registerkarte *Sommerzeit*.
- ☐ Modus *Sommerzeit* einschalten.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Legen Sie im Rahmen *Sommerzeit Beginn* die folgenden Einstellungen fest:
  - *Woche* = *letzte*
  - *Tag* = *Sonntag*
  - *Monat* = *März*
  - *Systemzeit* = 02:00
- ☐ Legen Sie im Rahmen *Sommerzeit Ende* die folgenden Einstellungen fest:
  - *Woche* = *letzte*
  - *Tag* = *Sonntag*
  - *Monat* = *Oktober*
  - *Systemzeit* = 03:00
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `clock summer-time mode recurring` | Schalten Sie den Modus *Sommerzeit* ein. |
| `clock summer-time recurring start last sun mar 02:00` | Zeitpunkt festlegen, zu dem das Gerät die Uhr von Normalzeit auf Sommerzeit vorstellt.<br>• `last` *letzte* Woche des Monats festlegen.<br>• `sun` Wochentag *Sonntag* festlegen.<br>• `mar` Monat *März* festlegen.<br>• `02:00` Uhrzeit 02:00 festlegen. |
| `clock summer-time recurring end last sun oct 03:00` | Zeitpunkt festlegen, zu dem das Gerät die Uhr von Sommerzeit zurück auf Normalzeit stellt.<br>• `last` *letzte* Woche des Monats festlegen.<br>• `sun` Wochentag *Sonntag* festlegen.<br>• `oct` Monat *Oktober* festlegen.<br>• `03:00` Uhrzeit 03:00 festlegen. |

# 4.3 Die Zeit im Netz mit SNTP synchronisieren

Das Simple Network Time Protocol (SNTP) ermöglicht Ihnen, die Systemzeit im Netz zu synchronisieren. Das Gerät unterstützt die SNTP-Client- und die SNTP-Server-Funktion.

Der SNTP-Server stellt die koordinierte Weltzeit (UTC) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die UTC ist weltweit gleich und berücksichtigt keine lokalen Zeitverschiebungen.

SNTP ist eine vereinfachte Version des Network Time Protocol (NTP). 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.

In einer IPv6-Umgebung funktioniert der *Broadcast*-Betriebsmodus wie folgt:
- Der SNTP-Client ist ausschließlich für Nachrichten des SNTP-Servers empfangsbereit, deren IPv6 *Multicast*-Adresse auf `ff05::101` als IPv6-Zieladresse eingestellt ist.
- Der SNTP-Server sendet ausschließlich SNTP-Nachrichten an die *Multicast*-Adresse `ff05::101`. Der SNTP-Server sendet keine SNTP-Nachrichten mit der Link-Local-Adresse als IPv6-Quelladresse.

*Tab. 14: 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.

### 4.3.1 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.

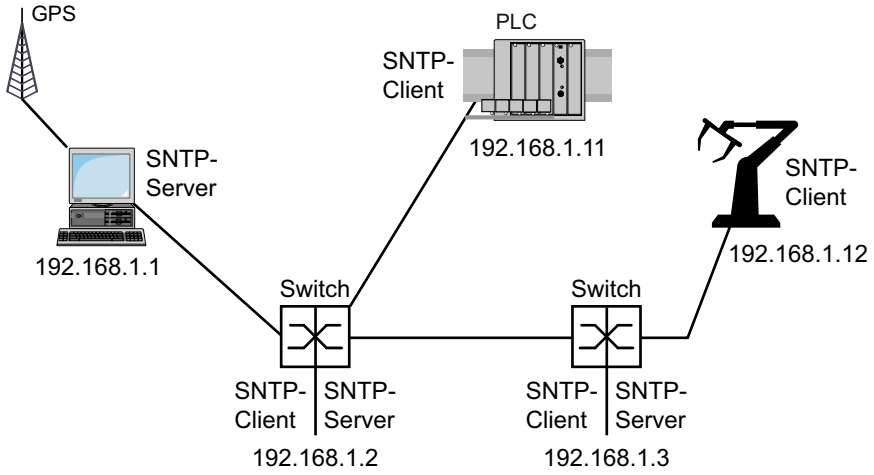



*Abb. 14: Beispiel für SNTP-Kaskade*

**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 eingerichtete SNTP-Server. Bleibt die Antwort des ersten SNTP-Servers aus, sendet der SNTP-Client seine Anfragen an den zweiten 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.

### 4.3.2 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 *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 eine Tabellenzeile hinzuzufügen, klicken Sie die Schaltfläche  .
- ☐ Legen Sie die Verbindungsdaten des SNTP-Servers fest.
- ☐ Schalten Sie die Funktion *Client* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .
- Das Feld *Zustand* zeigt den aktuellen Status der Funktion *Client*.

*Tab. 15: 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 *Client* | *Aus* | *An* | *An* | *An* | *An* |
| *Konfiguration*: *Modus* | `unicast` | `unicast` | `unicast` | `unicast` | `unicast` |
| *Request-Intervall [s]* | `30` | `30` | `30` | `30` | `30` |
| *Server*-Adresse(n) | – | `192.168.1.1` | `192.168.1.21`<br>`92.168.1.1` | `192.168.1.21`<br>`92.168.1.1` | `192.168.1.31`<br>`92.168.1.219`<br>`2.168.1.1` |

### 4.3.3 Einstellungen des SNTP-Servers festlegen

Beim Betrieb als SNTP-Server stellt das Gerät seine Systemzeit als koordinierte Weltzeit (UTC) im Netz zur Verfügung. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Zeit > SNTP > Server*.
- ☐ Schalten Sie die Funktion *Server* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Schalten Sie die Betriebsart *Broadcast* ein.
  Wählen Sie im Rahmen *Konfiguration* das Optionsfeld *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.
    In einer IPv6-Umgebung können Sie die IPv6-Adresse nicht festlegen, an die der SNTP-Server die SNTP-Pakete sendet. Der SNTP-Server verwendet die *Multicast*-Adresse `ff05::101` als IPv6-Zieladresse.
  - ☐ 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 das VLAN 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.

  **Anmerkung:**
  Mit Ausnahme des Felds *Broadcast Ziel-Adresse* sind die übrigen Einstellungen auf IPv4- und IPv6-SNTP-Server anwendbar.

- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .
- Das Feld *Zustand* zeigt den aktuellen Status der Funktion *Server*.

*Tab. 16: 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 *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` |

# 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 nichtflüchtigen Speicher (*NVM*) zu speichern. Um gegebenenfalls schnell auf andere Einstellungen umzuschalten, bietet der nichtflüchtige Speicher (*NVM* Platz für mehrere Konfigurationsprofile.

Wenn ein externer Speicher *ENVM* 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 nichtflüchtigen Speicher (*NVM*) bleibt dabei so lange unverändert, bis Sie die geänderten Einstellungen explizit speichern. Bis dahin unterscheiden sich die Konfigurationsprofile im flüchtigen und im nichtflüchtigen Speicher (*NVM*). 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 nichtflüchtigen 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 (*ENVM*) und nichtflüchtiger Speicher (*NVM*)

Sie können erkennen, ob die Einstellungen des „ausgewählten“ Konfigurationsprofils (*ENVM*) im externen Speicher von den Einstellungen des „ausgewählten“ Konfigurationsprofils im nichtflüchtigen 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 nichtflüchtigen Speicher (*NVM*).

### Konfigurationsprofil speichern

Das Gerät speichert die Einstellungen im „ausgewählten“ Konfigurationsprofil im nichtflüchtigen 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 nichtflüchtigen Speicher (nvm) enthaltenen Konfigurationsprofile anzeigen. |
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `save` | Einstellungen im nichtflüchtigen 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 fügt das Gerät im nichtflüchtigen Speicher (*NVM*) ein Konfigurationsprofil hinzu oder überschreibt ein vorhandenes.

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 nichtflüchtigen 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 nichtflüchtigen Speicher (`nvm`) speichern. Wenn vorhanden, überschreibt das Gerät ein namensgleiches Konfigurationsprofil. Das neue Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet. |

### Konfigurationsprofil auswählen

Wenn der nichtflüchtige 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 Systemstart 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.

- ☐ Wählen Sie die Tabellenzeile des gewünschten Konfigurationsprofils, das im nichtflüchtigen 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 nichtflüchtigen Speicher (`nvm`) enthaltenen Konfigurationsprofile anzeigen. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `config profile select nvm 1` | Konfigurationsprofil auswählen.<br>Orientieren Sie sich am nebenstehenden Namen des Konfigurationsprofils. |
| `save` | Einstellungen im nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

### 5.2.2 Konfigurationsprofil im externen Speicher (*ENVM*) speichern

Wenn ein externer Speicher (*ENVM*) 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 (*ENVM*) speichert.
- ☐ Um die Funktion zu deaktivieren, heben Sie die Markierung des Kontrollkästchens in Spalte *Sichere Konfiguration beim Speichern* auf.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `config envm config-save usb` | Funktion einschalten.<br>Beim Speichern eines Konfigurationsprofils speichert das Gerät eine Kopie im externen Speicher (*ENVM*).<br>`usb` = Externer USB-Speicher |
| `save` | Einstellungen im nichtflüchtigen 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 nichtflüchtigen 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 Remote-Server erforderlich sind.
- ☐ Schalten Sie die Funktion in der Optionsliste *Funktion* ein.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 {URL}` | Ziel-URL für das kopierte Konfigurationsprofil eingeben (max. 128 Zeichen). |
| `config remote-backup username {username}` | Benutzernamen eingeben für die Authentifizierung auf dem Remote-Server (max. 128 Zeichen). |
| `config remote-backup password {password}` | Benutzernamen für die Authentifizierung auf dem Remote-Server eingeben (max. 128 Zeichen). |
| `config remote-backup operation` | Funktion einschalten. |

Wenn die Übertragung zum Remote-Server scheitert, dann protokolliert das Gerät dieses Ereignis im 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 im Netz verfügbaren Server.
- Um die Datei auf einem SCP- oder SFTP-Server zu speichern, benötigen Sie zusätzlich Benutzername und Passwort für den Zugriff auf diesen Server.
- Denken Sie daran, den SCP- oder SFTP-Server dem Gerät bekannt zu machen, bevor das Gerät zum ersten Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Wählen Sie die Tabellenzeile 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>`
    Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  - ☐ 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>`
    Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  - ☐ 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>`
    Denken Sie daran, den SCP- oder SFTP-Server dem Gerät bekannt zu machen, bevor das Gerät zum ersten Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.
    Nach Klicken der Schaltfläche *Ok* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Konfigurationsprofil ist jetzt als XML-Datei am festgelegten Ort gespeichert.

| | |
|---|---|
| `show config profiles nvm` | Die im nichtflüchtigen 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.<br>Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen. |
| `copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>` | Das „ausgewählte" Konfigurationsprofil im nichtflüchtigen Speicher (`nvm`) auf einem SFTP-Server speichern. |
| `copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>` | Das Konfigurationsprofil `config3` im nichtflüchtigen Speicher (`nvm`) auf einem TFTP-Server speichern.<br>Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen. |
| `copy config nvm profile config3 remote ftp://<IP_address>[:port]/<path>/<file_name>` | Das Konfigurationsprofil `config3` im nichtflüchtigen Speicher (`nvm`) auf einem FTP-Server speichern.<br>Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen. |

# 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 nichtflüchtige Speicher des Geräts kann mehrere Konfigurationsprofile enthalten. Wenn Sie ein im nichtflüchtigen 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*.
- ☐ Wählen Sie die Tabellenzeile 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 nichtflüchtigen Speicher (`nvm`) enthaltenen Konfigurationsprofile anzeigen. |
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `copy config nvm profile config3 running-config` | Einstellungen des Konfigurationsprofils `config3` im nichtflüchtigen 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 (*ENVM*) laden

Wenn der externe Speicher (*ENVM*) angeschlossen ist, dann lädt das Gerät beim Systemstart automatisch ein Konfigurationsprofil aus dem externen Speicher (*ENVM*). Das Gerät ermöglicht Ihnen, diese Einstellungen wieder in einem Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) zu speichern.

Wenn der externe Speicher (*ENVM*) 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 Systemstart ein Konfigurationsprofil aus dem externen Speicher (*ENVM*) 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 `erste`.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `config envm load-priority usb first` | Funktion einschalten.<br>Beim Systemstart lädt das Gerät ein Konfigurationsprofil aus dem externen Speicher (*ENVM*).<br>`usb` = Externer USB-Speicher |
| `show config envm settings` | Einstellungen des externen Speichers (*ENVM*) anzeigen. |

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ---------------
usb    ok          [x]         [x]         first
```

| | |
|---|---|
| `save` | Die Einstellungen in einem Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) des Geräts speichern. |

Das Gerät ermöglicht Ihnen, mit dem Command Line Interface die Einstellungen aus dem externen Speicher (*ENVM*) in den nichtflüchtigen Speicher (*NVM*) zu kopieren.

| | |
|---|---|
| `show config profiles nvm` | Die im nichtflüchtigen 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 nichtflüchtigen Speicher (*NVM*) kopieren. |

Während des Systemstarts kann das Gerät außerdem automatisch ein Konfigurationsprofil aus einer Skriptdatei laden.

Voraussetzungen:
- Vergewissern Sie sich, dass der externe Speicher (*ENVM*) angeschlossen ist, bevor Sie das Gerät starten.
- Das Stammverzeichnis des externen Speichers (*ENVM*) enthält eine Textdatei `startup.txt` mit dem Inhalt `script=<Dateiname>`. Der Platzhalter `<Dateiname>` repräsentiert die Skriptdatei, die das Gerät während des Systemstarts ausführt.
- Das Stammverzeichnis des externen Speichers (*ENVM*) 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 (*ENVM*) 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 (*ENVM*). Sie haben die Möglichkeit, diese Funktion auszuschalten, wenn Sie den betreffenden Befehl in die Skriptdatei einfügen:

☐ `no config envm config-save usb`
Das Gerät speichert keine Kopie im externen USB-Speicher.

Enthält die Skriptdatei einen falschen Befehl, wendet das Gerät diesen Befehl während des Systemstarts nicht an. Das Gerät protokolliert das Ereignis im 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 eine Datei von einem Server zu importieren, benötigen Sie einen im Netz verfügbaren Server.
- Um eine Datei über SCP oder SFTP zu importieren, benötigen Sie zusätzlich Benutzername und Passwort für den Zugriff auf diesen Server.
- Denken Sie daran, den SCP- oder SFTP-Server dem Gerät bekannt zu machen, bevor das Gerät zum ersten Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.

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 externen Speicher (*ENVM*).

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 Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie diese in den ⬆-Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.
  - ☐ Wenn sich die Datei auf einem FTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
    `ftp://<Benutzername>:<Passwort>@<IP-Adresse>[:Port]/<Dateiname>`
    Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  - ☐ Wenn sich die Datei auf einem TFTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
    `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  - ☐ Wenn sich die Datei auf einem SCP- oder SFTP-Server befindet, dann legen Sie den URL 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>`
    Denken Sie daran, den SCP- oder SFTP-Server dem Gerät bekannt zu machen, bevor das Gerät zum ersten Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.
- ☐ 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 *Speicherort* 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 (*ENVM*). Führen Sie dazu die folgenden Schritte aus:

- ☐ Wählen Sie im Rahmen *Import profile from external memory* in der Dropdown-Liste *Profilname* den Namen des zu importierenden Konfigurationsprofils.
  Voraussetzung ist, dass der externe Speicher (*ENVM*) 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 nichtflüchtigen 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` | Einstellungen des Konfigurationsprofils, das auf einem FTP-Server gespeichert ist, importieren und aktivieren.<br>Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.<br>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` | Einstellungen des Konfigurationsprofils, das auf einem TFTP-Server gespeichert ist, importieren und aktivieren.<br>Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.<br>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` | Einstellungen des Konfigurationsprofils, das auf einem SFTP-Server gespeichert ist, importieren und aktivieren.<br>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 nichtflüchtigen Speicher (`nvm`) speichern.<br>Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen. |
| `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 nichtflüchtigen Speicher (`nvm`) speichern.<br>Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen. |

**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 Voreinstellung zurücksetzen

Wenn Sie die Einstellungen im Gerät auf den Lieferzustand zurücksetzen, dann löscht das Gerät die Konfigurationsprofile im flüchtigen Speicher und im nichtflüchtigen Speicher.

Wenn ein externer Speicher (*ENVM*) angeschlossen ist, dann löscht das Gerät auch die im externen Speicher (*ENVM*) 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 nichtflüchtigen Speicher (*NVM*).

Wenn ein externer Speicher (*ENVM*) angeschlossen ist, dann löscht das Gerät auch die im externen Speicher (*ENVM*) 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 (*ENVM*) und im nichtflüchtigen Speicher (*NVM*) löschen. Wenn ein externer Speicher (*ENVM*) angeschlossen ist, dann löscht das Gerät auch die im externen Speicher (*ENVM*) gespeicherten Konfigurationsprofile. Nach kurzer Zeit startet das Gerät neu und lädt die Werkseinstellungen. |

## 5.4.2 Mittels System Monitor 1

Führen Sie die folgenden Schritte aus:

- ☐ Um in den System Monitor 1 zu wechseln, gehen Sie vor wie in Kapitel „Zugriff auf das Management des Geräts” auf Seite 37 beschrieben.
- ☐ 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 nichtflüchtigen Speicher (*NVM*).
  Wenn ein externer Speicher (*ENVM*) angeschlossen ist, dann löscht das Gerät auch die im externen Speicher (*ENVM*) 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 Geräte-Software aktualisieren

Hirschmann arbeitet ständig an der Verbesserung und Weiterentwicklung der Software. Prüfen Sie regelmäßig, ob ein neuerer Stand der Geräte-Software Ihnen weitere Vorteile bietet. Informationen und Software-Downloads finden Sie auf den Hirschmann-Produktseiten im Internet unter catalog.belden.com.

Das Gerät bietet Ihnen folgende Möglichkeiten, die Geräte-Software zu aktualisieren:
- Laden einer früheren Version der Geräte-Software
- Software-Aktualisierung vom PC
- Software-Aktualisierung von einem Server
- Software-Aktualisierung aus dem externen Speicher (ENVM)

**Anmerkung:**
Die Einstellungen des Geräts bleiben erhalten, nachdem Sie die Geräte-Software aktualisiert haben.

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 beim Management des Geräts angemeldet 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 Systemstart geladen hat und gegenwärtig ausführt.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `show system info` | Systeminformationen anzeigen, wie Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Systemstart geladen hat und gegenwärtig ausführt. |

## 6.1 Laden einer früheren Version der Geräte-Software

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.

Wenn die Funktion Secure Boot aktiv ist, dann können Sie kein Downgrade auf eine Software-Version früher als 10.3.03 durchführen. Siehe Dialog *Grundeinstellungen > Software*, Rahmen *Software-Update*.

**Anmerkung:**
Die Einstellungen von Funktionen, die ausschließlich in der neueren Geräte-Software-Version zur Verfügung stehen, gehen verloren.

## 6.2 Software-Aktualisierung vom PC

Das Gerät ermöglicht Ihnen, die Geräte-Software zu aktualisieren, wenn ein geeignetes Image der Geräte-Software auf einem Datenträger gespeichert ist, den Sie von Ihrem PC aus erreichen.

Um während der Software-Aktualisierung beim Management des Geräts angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ dazu können Sie, bevor Sie die Software-Aktualisierung starten, einen ausreichend großen Wert im Dialog *Gerätesicherheit > Management-Zugriff > Web*, Feld *Webinterface-Session Timeout [min]* festlegen.

Führen Sie die folgenden Schritte aus:

- ☐ Navigieren Sie in das Verzeichnis, in welchem das Image der Geräte-Software gespeichert ist.
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Ziehen Sie die Datei in den -Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.
- ☐ Starten Sie die Software-Aktualisierung. Klicken Sie dazu die Schaltfläche *Start*.
  - Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
  - Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software.
    Sobald die Aktualisierung erfolgreich beendet ist, zeigt das Gerät eine Erfolgsmeldung. Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

# 6.3 Software-Aktualisierung von einem Server

Das Gerät ermöglicht Ihnen, seine Software zu aktualisieren, wenn Sie Zugriff auf einen Server haben, auf dem ein passendes Image der Geräte-Software gespeichert ist.

Das Gerät bietet Ihnen folgende Möglichkeiten, die Geräte-Software zu aktualisieren:
- Software-Aktualisierung über FTP
- Software-Aktualisierung über TFTP
- Software-Aktualisierung über SFTP
- Software-Aktualisierung über SCP

Um während der Software-Aktualisierung beim Management des Geräts angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ dazu können Sie, bevor Sie die Software-Aktualisierung starten, einen ausreichend großen Wert im Dialog *Gerätesicherheit > Management-Zugriff > Web*, Feld *Webinterface-Session Timeout [min]* festlegen.

## 6.3.1 Software-Aktualisierung über FTP

Diese Option ermöglicht Ihnen, die Geräte-Software mit einem Software-Image zu aktualisieren, welches das Gerät von einem FTP-Server abruft.

Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.

Voraussetzung ist, dass dem Benutzerkonto, das Sie zum Ausführen der Aktionen im Gerät verwenden, die Zugriffsrolle `administrator` zugewiesen ist.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Legen Sie im Rahmen *Software-Update*, Feld *URL* den URL zum Image der Geräte-Software in der folgenden Form fest:
  `ftp://Benutzer:Password@IP-Adresse:Port/Pfad/zum/Software_Image.bin`
  Sie können den URL auch ohne den Benutzernamen und das Passwort festlegen. In diesem Fall geben Sie diese in das *Anmeldeinformationen*-Fenster ein, nachdem Sie auf die Schaltfläche *Start* geklickt haben.
- ☐ Klicken Sie die Schaltfläche *Start*.
  - Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
  - Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software.
    Sobald die Aktualisierung erfolgreich beendet ist, zeigt das Gerät eine Information an, dass die Geräte-Software erfolgreich aktualisiert wurde.
    Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

```
enable

copy firmware remote ftp://
user:password@10.0.1.159:21/path/to/
software_image.bin system
```

In den Privileged-EXEC-Modus wechseln.

Übertragen des Images der Geräte-Software von einem FTP-Server in den Flash-Speicher des Geräts.

- `copy firmware remote`
  Übertragen des Images der Geräte-Software von einem entfernten Standort.
- `ftp://user:password@10.0.1.159:21/path/to/software_image.bin`
  URL des FTP-Servers, auf dem das Image der Geräte-Software gespeichert ist.
  Sie können den URL auch ohne den Benutzernamen und das Passwort festlegen. In diesem Fall fordert das Gerät Sie auf, die fehlenden Informationen nachträglich einzugeben.
  - `ftp://`
    Protokoll für die Dateiübertragung
  - `user`
    Name des Benutzerkontos auf dem FTP-Server
  - `password`
    Passwort für das Benutzerkonto
  - `10.0.1.159`
    IP-Adresse des FTP-Servers
  - `21`
    Standard-Port für FTP
  - `/path/to/`
    Der Pfad zum Image der Geräte-Software auf dem FTP-Server
  - `software_image.bin`
    Name des Images der Geräte-Software
- `system`
  Übertragen des kopierten Images der Geräte-Software in den Flash-Speicher.

### 6.3.2 Software-Aktualisierung über TFTP

Diese Option ermöglicht Ihnen, die Geräte-Software mit einem Software-Image zu aktualisieren, welches das Gerät von einem TFTP-Server abruft.

Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.

Voraussetzung ist, dass dem Benutzerkonto, das Sie zum Ausführen der Aktionen im Gerät verwenden, die Zugriffsrolle `administrator` zugewiesen ist.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Legen Sie im Rahmen *Software-Update*, Feld *URL* den URL zum Image der Geräte-Software in der folgenden Form fest:
  `tftp://IP-Adresse/Pfad/zum/Software_Image.bin`
- ☐ Klicken Sie die Schaltfläche *Start*.
  - Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
  - Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software.
    Sobald die Aktualisierung erfolgreich beendet ist, zeigt das Gerät eine Information an, dass die Geräte-Software erfolgreich aktualisiert wurde.
    Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

```
enable
```

In den Privileged-EXEC-Modus wechseln.

```
copy firmware remote tftp://0.0.1.159/
path/to/software_image.bin system
```

Übertragen des Images der Geräte-Software von einem TFTP-Server in den Flash-Speicher des Geräts.

- `copy firmware remote`
  Übertragen des Images der Geräte-Software von einem entfernten Standort.
- `tftp://10.0.1.159/path/to/software_image.bin`
  URL des TFTP-Servers, auf dem das Image der Geräte-Software gespeichert ist.
  - `tftp://`
    Protokoll für die Dateiübertragung
  - `10.0.1.159`
    IP-Adresse des TFTP-Servers
  - `/path/to/`
    Der Pfad zum Image der Geräte-Software auf dem TFTP-Server
  - `software_image.bin`
    Name des Images der Geräte-Software
- `system`
  Übertragen des kopierten Images der Geräte-Software in den Flash-Speicher.

### 6.3.3 Software-Aktualisierung über SFTP

Diese Option ermöglicht Ihnen, die Geräte-Software mit einem Software-Image zu aktualisieren, welches das Gerät von einem SFTP-Server abruft.

Voraussetzungen:
- Dem Benutzerkonto, das Sie zum Ausführen der Aktionen im Gerät verwenden, ist die Zugriffsrolle `administrator` zugewiesen.
- Der SFTP-Server ist dem Gerät bekannt. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Legen Sie im Rahmen *Software-Update*, Feld *URL* den URL zum Image der Geräte-Software in der folgenden Form fest:
  `sftp://Benutzer:Password@IP-Adresse/Pfad/zum/Software_Image.bin`
  Sie können den URL auch ohne den Benutzernamen und das Passwort festlegen. In diesem Fall geben Sie diese in das *Anmeldeinformationen*-Fenster ein, nachdem Sie auf die Schaltfläche *Start* geklickt haben.
- ☐ Klicken Sie die Schaltfläche *Start*.
  - Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
  - Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software.
    Sobald die Aktualisierung erfolgreich beendet ist, zeigt das Gerät eine Information an, dass die Geräte-Software erfolgreich aktualisiert wurde.
    Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

```
enable

copy firmware remote sftp://
user:password@10.0.1.159:21/path/to/
software_image.bin system
```

In den Privileged-EXEC-Modus wechseln.

Übertragen des Images der Geräte-Software von einem SFTP-Server in den Flash-Speicher des Geräts.

- `copy firmware remote`
  Übertragen des Images der Geräte-Software von einem entfernten Standort.
- `sftp://user:password@10.0.1.159:21/path/to/software_image.bin`
  URL des SFTP-Servers, auf dem das Image der Geräte-Software gespeichert ist.
  Sie können den URL auch ohne den Benutzernamen und das Passwort festlegen. In diesem Fall fordert das Gerät Sie auf, die fehlenden Informationen nachträglich einzugeben.
  - `sftp://`
    Protokoll für die Dateiübertragung
  - `user`
    Name des Benutzerkontos auf dem SFTP-Server
  - `password`
    Passwort für das Benutzerkonto
  - `10.0.1.159`
    IP-Adresse des SFTP-Servers
  - `/path/to/`
    Der Pfad zum Image der Geräte-Software auf dem SFTP-Server
  - `software_image.bin`
    Name des Images der Geräte-Software
- `system`
  Übertragen des kopierten Images der Geräte-Software in den Flash-Speicher.

### 6.3.4 Software-Aktualisierung über SCP

Diese Option ermöglicht Ihnen, die Geräte-Software mit einem Software-Image zu aktualisieren, welches das Gerät von einem SCP-Server abruft.

Voraussetzungen:
- Dem Benutzerkonto, das Sie zum Ausführen der Aktionen im Gerät verwenden, ist die Zugriffsrolle `administrator` zugewiesen.
- Der SCP-Server ist dem Gerät bekannt. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Legen Sie im Rahmen *Software-Update*, Feld *URL* den URL zum Image der Geräte-Software in der folgenden Form fest:
  `scp://Benutzer:Passwort@IP-Adresse/Pfad/zum/Software_Image.bin`
  Sie können den URL auch ohne den Benutzernamen und das Passwort festlegen. In diesem Fall geben Sie diese in das *Anmeldeinformationen*-Fenster ein, nachdem Sie auf die Schaltfläche *Start* geklickt haben.
- ☐ Klicken Sie die Schaltfläche *Start*.
  - Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
  - Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software.
    Sobald die Aktualisierung erfolgreich beendet ist, zeigt das Gerät eine Information an, dass die Geräte-Software erfolgreich aktualisiert wurde.
    Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

```
enable

copy firmware remote scp://
user:password@10.0.1.159:21/path/to/
software_image.bin system
```

In den Privileged-EXEC-Modus wechseln.

Übertragen des Images der Geräte-Software von einem SCP-Server in den Flash-Speicher des Geräts.

- `copy firmware remote`
  Übertragen des Images der Geräte-Software von einem entfernten Standort.
- `user:password@10.0.1.159:21/path/to/soft-ware_image.bin`
  URL des SCP-Servers, auf dem das Image der Geräte-Software gespeichert ist.
  Sie können den URL auch ohne den Benutzer-namen und das Passwort festlegen. In diesem Fall fordert das Gerät Sie auf, die fehlenden Informationen nachträglich einzugeben.
  - `scp://`
    Protokoll für die Dateiübertragung
  - `user`
    Name des Benutzerkontos auf dem SCP-Server
  - `password`
    Passwort für das Benutzerkonto
  - `10.0.1.159`
    IP-Adresse des SCP-Servers
  - `/path/to/`
    Der Pfad zum Image der Geräte-Software auf dem SCP-Server
  - `software_image.bin`
    Name des Images der Geräte-Software
- `system`
  Übertragen des kopierten Images der Geräte-Software in den Flash-Speicher.

# 6.4 Software-Aktualisierung aus dem externen Speicher (*ENVM*)

## 6.4.1 Manuell – durch den Administrator initiiert

Das Gerät ermöglicht Ihnen, die Geräte-Software zu aktualisieren, wenn auf dem externen Speicher (*ENVM*) ein geeignetes Image der Geräte-Software gespeichert ist.

Um während der Software-Aktualisierung beim Management des Geräts angemeldet zu bleiben, bewegen Sie gelegentlich den Mauszeiger. Alternativ dazu können Sie, bevor Sie die Software-Aktualisierung starten, einen ausreichend großen Wert im Dialog *Gerätesicherheit > Management-Zugriff > Web*, Feld *Webinterface-Session Timeout [min]* festlegen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Vergewissern Sie sich, dass im Rahmen *Externer Speicher* der betreffende externe Speicher in der Dropdown-Liste *Ausgewählter externer Speicher* ausgewählt ist.
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Markieren Sie die Tabellenzeile, für welche die Spalte *Datei Ort* den Wert `usb` zeigt.
- ☐ Starten Sie die Software-Aktualisierung. Klicken Sie dazu die Schaltfläche .
  - Das Gerät überträgt die bisher verwendete Geräte-Software in den Backup-Speicherbereich.
  - Das Gerät überträgt die ausgewählte Datei in den Flash-Speicher und ersetzt die bisher verwendete Geräte-Software.
    Sobald die Aktualisierung erfolgreich beendet ist, zeigt das Gerät eine Erfolgsmeldung. Beim nächsten Systemstart startet das Gerät mit der Geräte-Software, die Sie übertragen haben.

## 6.4.2 Automatisch – durch das Gerät initiiert

Wenn sich folgende Dateien im externen Speicher (*ENVM*) befinden, aktualisiert das Gerät beim Systemstart die Geräte-Software automatisch:

- das Image der Geräte-Software
- eine Textdatei `startup.txt` mit dem Inhalt `autoUpdate=<Dateiname_des_Software-Images>.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:

- ☐ Übertragen Sie das neue Image der Geräte-Software in das Hauptverzeichnis des externen Speichers (*ENVM*). Verwenden Sie ausschließlich ein für das Gerät bestimmtes Image der Geräte-Software.
- ☐ Erstellen Sie eine Textdatei mit dem Namen `startup.txt` im Hauptverzeichnis des externen Speichers (*ENVM*).
- ☐ Öffnen Sie die Datei `startup.txt` im Texteditor und fügen Sie folgende Zeile ein: `autoUpdate=<Dateiname_des_Software-Images>.bin`
- ☐ Installieren Sie den externen Speicher (*ENVM*) im Gerät.

☐ Starten Sie das Gerät neu.
Während des Boot-Vorgangs prüft das Gerät automatisch folgende Kriterien:
- Ist ein externer Speicher (*ENVM*) angeschlossen?
- Befindet sich im Hauptverzeichnis des externen Speichers (*ENVM*) eine Datei `startup.txt`?
- Existiert das Image der Geräte-Software, welches in der Datei `startup.txt` festgelegt ist?
- Ist die Version des Images der Geräte-Software jünger als die Geräte-Software, die das Gerät gegenwärtig verwendet?

Wenn die Kriterien erfüllt sind, startet das Gerät die Aktualisierung.
Die gegenwärtig ausgeführte Geräte-Software kopiert das Gerät in den Backup-Bereich.
Sobald die Aktualisierung erfolgreich beendet ist, startet das Gerät selbstständig neu und lädt die neue Version der Geräte-Software.

☐ Kontrollieren Sie das Ergebnis der Aktualisierung. Die Log-Datei im Dialog *Diagnose > Bericht > System-Log* enthält eine der folgenden Meldungen:
- `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
  Software-Aktualisierung erfolgreich beendet
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
  Software-Aktualisierung abgebrochen
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
  Software-Aktualisierung aufgrund eines falschen Images der Geräte-Software abgebrochen
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Software-Aktualisierung abgebrochen, weil das Gerät das Image der Geräte-Software 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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` | Das Interface einschalten. |

# 7.2 Betriebsart wählen

In der Voreinstellung befinden sich die Ports im Betriebsmodus *Autoneg.*.

**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 *Autoneg.* auf.
  - ☐ Legen Sie in Spalte *Manuelle Konfiguration* die Betriebsart (Übertragungsgeschwindigkeit, Duplexbetrieb) fest.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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
- Zugriffe auf das Management des Geräts beschränken
- Session-Timeouts anpassen
- Nicht verwendete Module deaktivieren
- SSH-Einstellungen anpassen
- SSH-Hosts im Gerät bekannt machen

## 8.1 SNMPv1/v2-Community ändern

SNMPv1 und SNMPv2 arbeiten 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 die Funktion *SNMPv1* und/oder *SNMPv2* eingeschaltet ist, ermöglicht das Gerät jedem, der den *Community-Namen* kennt, den Zugriff auf das Gerät. Behandeln Sie die *Community-Namen* vertraulich.

Voreingestellt sind die *Community-Namen*`public` für *Lesezugriff* und `private` für *Lese- und Schreibzugriff*. Wenn Sie SNMPv1 oder SNMPv2 verwenden, dann ändern Sie den voreingestellten *Community-Namen*. 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 64 alphanumerische Zeichen.
  - Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
  - Legen Sie einen anderen *Community-Namen* fest als für *Lesezugriffe*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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- und Schreibzugriffe* festlegen. |
| `show snmp community` | Eingerichtete Communities anzeigen. |
| `save` | Einstellungen im nichtflüchtigen 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 nichtflüchtigen 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*.
- ☐ Schalten Sie das Protokoll *HTTP* aus.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 Webbrowsers geben 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*.
- ☐ Schalten Sie den *Telnet*-Server aus.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 den *Telnet*-Server ausschalten, dann ist der Zugriff auf das Management des Geräts ausschließlich mittels Command Line Interface über die serielle Verbindung 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*.
- ☐ Schalten Sie den *SSH*-Server ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 > Netzwerk > Global*.
- ☐ Um der HiDiscovery-Software die Schreibrechte zu entziehen, legen Sie im Rahmen *HiDiscovery Protokoll v1/v2*, Feld *Zugriff* den Wert `read-only` fest.
- ☐ Schalten Sie den HiDiscovery-Zugriff vollständig aus.
  Wählen Sie im Rahmen *HiDiscovery Protokoll v1/v2* das Optionsfeld `Aus`.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 Zugriffe auf das Management des Geräts beschränken

In der Voreinstellung kann ein jeder von einer beliebigen IP-Adresse und mit einem beliebigen Protokoll auf das Management des Geräts zugreifen. Das Gerät ermöglicht Ihnen, Zugriffe auf das Management des Geräts für ausgewählte Protokolle aus einem bestimmten IP-Adressbereich einzuschränken.

## 8.6.1 Zugriffe aus einem bestimmten IP-Adressbereich einschränken

Im folgenden Beispiel soll das Gerät 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 Fingerabdruck 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 die Tabellenzeile 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 eine Tabellenzeile 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 unerwünschten Protokolle. Die Kontrollkästchen in den Feldern *HTTPS*, *SNMP* und *Aktiv* bleiben markiert.

Adressbereich des Mobilfunknetzes:

- ☐ Um eine Tabellenzeile 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 unerwünschten Protokolle. Die Kontrollkästchen in den Feldern *SSH* und *Aktiv* bleiben markiert.

**Anmerkung:**
Bevor Sie die Zugriffsbeschränkung einschalten, vergewissern Sie sich, dass die Tabelle mindestens eine aktive Regel enthält, welche Ihnen Zugriff auf das Management des Geräts gewährt. Andernfalls ist der Zugriff auf das Management des Geräts ausschließlich mittels Command Line Interface über die serielle Verbindung möglich.

- ☐ Schalten Sie die Zugriffsbeschränkung ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `show network management access global` | Zeigen, ob die 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` | Eine Regel mit Index 2 für den Adressbereich des Firmennetzes hinzufügen. |
| `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.<br>Schritt für jedes unerwünschte Protokoll wiederholen. |
| `network management access add 3` | Eine Regel mit Index 3 für den Adressbereich des Mobilfunknetzes hinzufügen. |
| `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.<br>Schritt für jedes unerwünschte Protokoll wiederholen. |
| `no network management access status 1` | Voreingestellten Eintrag deaktivieren.<br>Dieser Eintrag ermöglicht Benutzern den Zugriff auf das Gerät von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle. |
| `network management access status 2` | Die Regel mit Index 2 für den Adressbereich des Firmennetzes aktivieren. |
| `network management access status 3` | Die Regel mit Index 3 für den Adressbereich des Mobilfunknetzes aktivieren. |
| `show network management access rules` | Eingerichtete Einträge anzeigen. |
| `network management access operation` | Die Zugriffsbeschränkung einschalten. |

# 8.7 Session-Timeouts anpassen

Das Gerät ermöglicht Ihnen, bei Inaktivität des 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 die 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 die 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 die 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 *Webinterface-Session Timeout [min]* die Timeout-Zeit in Minuten fest.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

# 8.9 SSH-Einstellungen anpassen

Im Lieferzustand verwendet der im Gerät integrierte SSH-Server einen selbstsignierten RSA-*Host Key*. Um das Sicherheitsniveau von SSH-Verbindungen zum Gerät zu erhöhen, können Sie den RSA-*Host Key* im Gerät wie folgt ersetzen:

- „RSA-Host-Key im Gerät generieren” auf Seite 129
- „Einen extern generierten privaten RSA-Schlüssel auf das Gerät übertragen” auf Seite 130

## 8.9.1 RSA-Host-Key im Gerät generieren

Das Gerät ermöglicht Ihnen, einen RSA-*Host Key* direkt im Gerät zu generieren und damit den gespeicherten RSA-*Host Key* zu ersetzen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Schalten Sie den *SSH*-Server aus.
  Wählen Sie dazu im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Klicken Sie im Rahmen *Signatur* die Schaltfläche *Erstellen*.
  Die Generierung des neuen RSA-*Host Keys* startet.
  Sie können den Vorgang überwachen, indem Sie die Schaltfläche ↻ klicken. Wenn der Wert im Feld *Betriebszustand* von *rsa* auf *kein* wechselt, ist der Vorgang abgeschlossen.
- ☐ Schalten Sie den *SSH*-Server ein.
  Wählen Sie dazu im Rahmen *Funktion* das Optionsfeld *An*.
  Der generierte RSA-*Host Key* ist sofort aktiv.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

Führen Sie die folgenden Kommandos ausschließlich dann aus, wenn Sie über die serielle Verbindung mit dem Management des Geräts verbunden sind. Wenn Sie über SSH verbunden sind, wird die Verbindung zum Management des Geräts unterbrochen.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `no ssh server` | Den *SSH*-Server ausschalten. |
| `ssh key rsa generate` | Den neuen RSA-*Host Key* generieren.<br>Dieser Vorgang dauert wenige Sekunden und endet ohne Rückmeldung.<br>Sie können den Vorgang überwachen, indem Sie das Kommando `show ssh server` ausführen. Wenn der Wert in der Zeile `SSH key operation status` von `rsa` auf `none` wechselt, ist der Vorgang abgeschlossen. |
| `ssh server` | *SSH*-Server einschalten.<br>Der generierte RSA-*Host Key* ist sofort aktiv. |

### 8.9.2 Einen extern generierten privaten RSA-Schlüssel auf das Gerät übertragen

Netzadministratoren können einen RSA-*Host Key* außerhalb des Geräts generieren, zum Beispiel mit dem Kommando `ssh-keygen`, das zu OpenSSH gehört. Optional können Sie den extern generierten RSA-Schlüssel von einer Zertifizierungsstelle (Certification Authority, CA) signieren lassen.

Um einen RSA-Schlüssel außerhalb des Geräts zu generieren, geben Sie auf der Management-Station folgendes Kommando ein: `ssh-keygen -b 4096 -t rsa -m PEM -N '' -f key_name`

- `-b 2048`
  Länge des Schlüssels
- `-t rsa`
  Art des Schlüssels
- `-m PEM`
  Format des Schlüssels
- `-N ''`
  Passphrase
- `-f key_name`
  Dateiname des Schlüssels
  Ersetzen Sie die Zeichenfolge `key_name` mit dem gewünschten Dateinamen.

Nachdem das Kommando ausgeführt ist, finden Sie im Dateisystem der Management-Station folgende Dateien:

- Privater Schlüssel (`key_name` ohne Dateiendung)
  Dieser Schlüssel ermöglicht dem SSH-Server im Gerät, sich gegenüber den SSH-Clients zu authentifizieren. Diesen Schlüssel übertragen Sie im weiteren Verlauf auf das Gerät. Bewahren Sie den privaten Schlüssel an einem vertrauenswürdigen, sicheren Ort auf, jedoch nicht an einem öffentlich zugänglichen oder gemeinsam genutzten Ort.
- Öffentlicher Schlüssel (`key_name` mit der Dateiendung `.pub`)
  Dieser Schlüssel ermöglicht den SSH-Clients, die Echtheit des SSH-Servers im Gerät zu prüfen.

Sie können den extern generierten privaten Schlüssel mit einer der folgenden Optionen auf das Gerät übertragen:

- Den privaten Schlüssel von der Management-Station oder einem Dateiserver mittels grafischer Benutzeroberfläche oder Command Line Interface direkt in das Gerät importieren.
  Siehe „Privaten Schlüssel direkt in das Gerät importieren” auf Seite 130.
- Den privaten Schlüssel über den externen Speicher mittels Command Line Interface auf das Gerät übertragen.
  Siehe „Privaten Schlüssel über den externen Speicher auf das Gerät übertragen” auf Seite 132.

#### Privaten Schlüssel direkt in das Gerät importieren

Sie können den privaten Schlüssel von der Management-Station oder einem Dateiserver mittels grafischer Benutzeroberfläche oder Command Line Interface direkt in das Gerät importieren. Stellen Sie sicher, dass sich der private Schlüssel nicht länger als für die Dauer der Übertragung notwendig auf dem Dateiserver befindet. Verschieben Sie den privaten Schlüssel unmittelbar nach der Übertragung an einen Ort, der nicht über das Netz erreichbar ist.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Schalten Sie den *SSH*-Server aus.
  Wählen Sie dazu im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

- ☐ Importieren Sie den privaten Schlüssel:
  - ☐ Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie diese in den ⬆-Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.
  - ☐ Wenn sich die Datei auf einem FTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
    `ftp://<Benutzername>:<Passwort>@<IP-Adresse>[:Port]/<Dateiname>`
    Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  - ☐ Wenn sich die Datei auf einem TFTP-Server befindet, dann legen Sie den URL in der folgenden Form fest:
    `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Verwenden Sie diese Methode nicht, wenn Sie Daten über nicht vertrauenswürdige Netze übertragen.
  - ☐ Wenn sich die Datei auf einem SCP- oder SFTP-Server befindet, dann legen Sie den URL 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>`
    Denken Sie daran, den SCP- oder SFTP-Server dem Gerät bekannt zu machen, bevor das Gerät zum ersten Mal auf den Server zugreift. Siehe Dialog *Gerätesicherheit > SSH Bekannte Hosts*.
- ☐ Klicken Sie die Schaltfläche *Start*.
  Die Dateiübertragung startet. Dieser Vorgang dauert wenige Sekunden.
- ☐ Verschieben Sie den privaten Schlüssel an einen Ort, der über das Netz nicht erreichbar ist.
- ☐ Schalten Sie den *SSH*-Server ein.
  Wählen Sie dazu im Rahmen *Funktion* das Optionsfeld *An*.
  Der importierte private Schlüssel ist sofort aktiv.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

Führen Sie die folgenden Kommandos ausschließlich dann aus, wenn Sie über die serielle Verbindung mit dem Management des Geräts verbunden sind. Wenn Sie über SSH verbunden sind, wird die Verbindung zum Management des Geräts unterbrochen.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `copy sshkey remote scp://192.168.1.1/path/to/priv_key_file nvm` | Den privaten Schlüssel mittels SCP von einer Management-Station mit der IP-Adresse 192.168.1.1 importieren.<br>Verschieben Sie den privaten Schlüssel unmittelbar nach der Übertragung an einen Ort, der nicht über das Netz erreichbar ist. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `no ssh server` | Den *SSH*-Server ausschalten. |
| `ssh server` | *SSH*-Server einschalten.<br>Der importierte private Schlüssel ist sofort aktiv. |

### Privaten Schlüssel über den externen Speicher auf das Gerät übertragen

Sie können den privaten Schlüssel über den externen Speicher mittels Command Line Interface auf das Gerät übertragen.

Vorbereitende Schritte:

- ☐ Kopieren Sie auf der Management-Station den privaten Schlüssel auf den mit der Management-Station verbundenen externen Speicher. Stellen Sie sicher, dass sich der private Schlüssel nicht länger als für die Dauer der Übertragung notwendig auf dem externen Speicher befindet. Löschen Sie den privaten Schlüssel sofort nach der Übertragung vom externen Speicher.
- ☐ Stecken Sie den externen Speicher in das Gerät.

Führen Sie die folgenden Kommandos ausschließlich dann aus, wenn Sie über die serielle Verbindung mit dem Management des Geräts verbunden sind. Wenn Sie über SSH verbunden sind, wird die Verbindung zum Management des Geräts unterbrechen.

Führen Sie die folgenden Schritte aus:

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `copy sshkey envm path/to/priv_key_file nvm` | Den privaten Schlüssel über den externen Speicher auf das Gerät übertragen (*ENVM*).<br>Löschen Sie den privaten Schlüssel sofort nach der Übertragung vom externen Speicher (*ENVM*). |
| `configure` | In den Konfigurationsmodus wechseln. |
| `no ssh server` | Den *SSH*-Server ausschalten. |
| `ssh server` | *SSH*-Server einschalten.<br>Der importierte private Schlüssel ist sofort aktiv. |

# 8.10 SSH-Hosts im Gerät bekannt machen

Das Gerät lässt SSH-basierte Verbindungen ausschließlich zu Remote-Servern zu, die dem Gerät bekannt sind. Im Lieferzustand ist kein Remote-Server als bekannter Host auf dem Gerät eingerichtet.

Beim Herunterladen eines Images der Geräte-Software oder beim Importieren eines Konfigurationsprofils über SCP oder SFTP verwenden diese Protokolle eine zugrundeliegende SSH-Verbindung. Für SSH machen Sie die Remote-Server mittels Fingerabdruck des öffentlichen Schlüssels bekannt. Das Gerät prüft die Identität des Remote-Servers, indem es den Fingerabdruck des öffentlichen Schlüssels, der auf dem Gerät gespeichert ist, mit dem Fingerabdruck vergleicht, der aus dem öffentlichen Schlüssel berechnet wurde, den der Remote-Server tatsächlich gesendet hat. Wenn der berechnete Fingerabdruck des öffentlichen Schlüssels nicht mit dem gespeicherten Fingerabdruck des öffentlichen Schlüssels übereinstimmt, beendet das Gerät die Verbindung.

Sie können den Fingerabdruck des öffentlichen Schlüssels des Remote-Servers und den Schlüsseltyp wie folgt herausfinden:
- Vom Administrator eines bekannten SSH-Servers.
  Nutzen Sie einen vertrauenswürdigen Kanal, um diese Daten zu empfangen.
- Aus der Fehlermeldung nach einem fehlgeschlagenen Software-Update im Dialog *Software*.
  Dies geschieht aufgrund der Nichtübereinstimmung zwischen dem im Gerät gespeicherten Fingerabdruck des öffentlichen Schlüssels und dem aus dem öffentlichen Schlüssel berechneten Fingerabdruck, den der Remote-Server tatsächlich gesendet hat.

Das Gerät bietet Ihnen folgende Einstellmöglichkeiten:
- SSH-Known-Hosts-Eintrag hinzufügen
- SSH-Known-Hosts-Eintrag aktualisieren
- SSH-Known-Hosts-Eintrag deaktivieren
- SSH-Known-Hosts-Eintrag löschen

### SSH-Known-Hosts-Eintrag hinzufügen

Sie können bis zu 50 Einträge bestehend aus Server-Adresse und Fingerabdruck des öffentlichen Schlüssels einrichten. Wenn auf einem Remote-Server mehrere Schlüssel für unterschiedliche Verschlüsselungsalgorithmen eingerichtet sind, fügen Sie jeden Fingerabdruck eines öffentlichen Schlüssels als separaten Eintrag hinzu.

Vergewissern Sie sich, dass die Fingerabdrücke der öffentlichen Schlüssel, die Sie auf dem Gerät speichern, aus einer vertrauenswürdigen Quelle stammen, zum Beispiel vom Administrator des SSH-Servers.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erstellen*.
- ☐ Legen Sie im Feld *Index* den Index-Wert fest. Weisen Sie einen eindeutigen Wert zu.
- ☐ Legen Sie im Feld *Adresse* die IP-Adresse (IPv4 oder IPv6) oder den DNS-Hostnamen des Remote-Servers fest.

- ☐ Geben Sie im Feld *Key-Fingerabdruck* den Fingerabdruck des öffentlichen Schlüssels des Remote-Servers ein.
- ☐ Wählen Sie in der Dropdown-Liste *Key-Typ* den Typ des Schlüssels. Dies ist der Algorithmus, den der Administrator des Remote-Servers zum Generieren des Server-Schlüsselpaars verwendet hat.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Gerät fügt eine Tabellenzeile hinzu.
  Ab sofort akzeptiert das Gerät das Herstellen einer Verbindung mit dem Remote-Server.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `ssh known-hosts add {index} address {ipv4 \| ipv6 \| dns} key-type {rsa \| dsa \| ecdsa \| ed25519} key-fingerprint {string_base64}` | Einen Eintrag mit Index, Adresse des Remote-Servers, Schlüsseltyp und Fingerabdruck des öffentlichen Schlüssels des Remote-Servers hinzufügen. |
| `show ssh known-hosts` | Die eingerichteten Einträge anzeigen. |
| `exit` | In den Privileged-EXEC-Modus wechseln. |

Um die Einstellungen dauerhaft zu speichern, siehe Abschnitt „Konfigurationsprofil speichern” auf Seite 95.

### SSH-Known-Hosts-Eintrag aktualisieren

Wenn sich der öffentliche Schlüssel des Remote-Servers ändert, dann ist in der betreffenden Tabellenzeile die Aktualisierung des Fingerabdrucks erforderlich.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*.
- ☐ Heben Sie die Markierung des Kontrollkästchens in Spalte *Aktiv* auf.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Geben Sie in Spalte *Key-Fingerabdruck* den neuen Fingerabdruck des öffentlichen Schlüssels des Remote-Servers ein.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Um den Eintrag zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `ssh known-hosts modify {index} status disable` | Den Eintrag deaktivieren. |
| `ssh known-hosts modify {index} key-fingerprint {string_base64}` | Den Eintrag mit der von Ihnen eingegebenen Indexnummer verändern. |
| `ssh known-hosts modify {index} status enable` | Den Eintrag aktivieren. |
| `show ssh known-hosts {index}` | Den aktualisierten Eintrag prüfen. |
| `exit` | In den Privileged-EXEC-Modus wechseln. |

Um die Einstellungen dauerhaft zu speichern, siehe Abschnitt „Konfigurationsprofil speichern” auf Seite 95.

### SSH-Known-Hosts-Eintrag deaktivieren

Sie deaktivieren einen Eintrag zum Beispiel dann, wenn der Serverschlüssel aufgrund der Rotation bald ungültig wird.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*.
- ☐ Heben Sie in der Tabellenzeile des betreffenden Eintrags die Markierung des Kontrollkästchens in Spalte *Aktiv* auf.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `ssh known-hosts modify {index} status disable` | Den Eintrag mit der von Ihnen eingegebenen Indexnummer deaktivieren. |
| `show ssh known-hosts {index}` | Prüfen, ob der Eintrag inaktiv ist. |
| `exit` | In den Privileged-EXEC-Modus wechseln. |

Um die Einstellungen dauerhaft zu speichern, siehe Abschnitt „Konfigurationsprofil speichern” auf Seite 95.

### SSH-Known-Hosts-Eintrag löschen

Wenn das Gerät einen Remote-Server nicht länger kontaktieren darf oder der öffentliche Schlüssel nicht mehr gültig ist, dann können Sie den betreffenden Eintrag löschen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*.
- ☐ Markieren Sie in der Tabellenzeile des betreffenden Eintrags das Kontrollkästchen in Spalte *Index*.

  Klicken Sie die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `ssh known-hosts delete {index}` | Den Eintrag mit der von Ihnen eingegebenen Indexnummer löschen. |
| `show ssh known-hosts {index}` | Prüfen, ob der Eintrag gelöscht wurde. |
| `SSH known hosts information` | |
| `---------------------------` | |
| `No entry.` | |
| `exit` | In den Privileged-EXEC-Modus wechseln. |

Um die Einstellungen dauerhaft zu speichern, siehe Abschnitt „Konfigurationsprofil speichern” auf Seite 95.

# 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 (ACL)

Das Gerät beobachtet und überwacht den Datenstrom. Aus den Ergebnissen der Beobachtung und Überwachung sowie aus den Regeln für die Netzsicherheit generiert 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

Denial-of-Service (DoS) ist ein Cyber-Angriff, der darauf abzielt, bestimmte Dienste oder Geräte funktionsunfähig zu machen. 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 des Netzes vor ungültigen oder gefälschten Datenpaketen, die auf bestimmte 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.

Sie können folgende Optionen festlegen, um das Gerät selbst und andere Geräte im Netz vor DoS-Angriffen zu schützen:
- 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 Schutz aktivieren
- Funktion TCP-SYN Schutz aktivieren
- Funktion L4-Port Schutz 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 Schutz 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 Schutz*, 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 Schutz* ausgeschaltet. Um die Funktion *TCP-Offset Schutz* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *TCP-Offset Schutz*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *TCP-Offset Schutz*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `dos tcp-offset` | Funktion *TCP-Offset Schutz* aktivieren. |
| `no dos tcp-offset` | Funktion *TCP-Offset Schutz* deaktivieren. |

### Funktion TCP-SYN Schutz aktivieren

Bei der *TCP SYN*-Methode sendet die angreifende Station Datenpakete, in denen das *TCP*-Flag *SYN* gesetzt ist und bei denen der L4- (Schicht 4-) Quell-Port <1024 ist. Das Gerät verwendet die Funktion *TCP-SYN Schutz*, um eingehende Datenpakete zu verwerfen, in denen das *TCP*-Flag *SYN* gesetzt ist und bei denen der L4- (Schicht 4-) Quell-Port <1024 ist.

In der Voreinstellung ist die Funktion *TCP-SYN Schutz* ausgeschaltet. Um die Funktion *TCP-SYN Schutz* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *TCP-SYN Schutz*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *TCP-SYN Schutz*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `dos tcp-syn` | Funktion *TCP-SYN Schutz* aktivieren. |
| `no dos tcp-syn` | Funktion *TCP-SYN Schutz* deaktivieren. |

### Funktion L4-Port Schutz 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 Schutz*, 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 Schutz* ausgeschaltet. Um die Funktion *L4-Port Schutz* zu aktivieren, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > DoS > Global*.
- ☐ Aktivieren Sie die Funktion *L4-Port Schutz*. Markieren Sie dazu im Rahmen *TCP/UDP* das Kontrollkästchen *L4-Port Schutz*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `dos l4-port` | Funktion *L4-Port Schutz* aktivieren. |
| `no dos l4-port` | Funktion *L4-Port Schutz* deaktivieren. |

### Funktion Min.-Header-Size Filter aktivieren

Das Gerät verwendet die Funktion *Min.-Header-Size Filter*, um den *TCP*-Header von empfangenen Datenpaketen zu prüfen. Das Gerät verwirft das Datenpaket, wenn (Daten-Offset-Wert × 4) < minimale *TCP*-Header-Größe ist.

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.

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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 Zieladressen 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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. |

# 9.2 ACL

In diesem Menü haben Sie die Möglichkeit, die Parameter für die Access-Control-Listen (ACL) einzugeben.

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)
- Quell- oder Ziel-Port eines Datenpakets (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 demselben Port oder derselben Link-Aggregation (LAG) sowohl eine IP-ACL als auch 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.

Das Gerät weist eine Besonderheit auf, wenn Sie einem Port sowohl eine IP-ACL als auch eine MAC-ACL und für die selbe Datenpaket-Richtung zuweisen möchten. In diesem speziellen Anwendungsfall weisen Sie die erste ACL dem gewünschten Port zu. Die zweite ACL weisen Sie einem VLAN zu, in dem der gewünschte Port Mitglied ist. Voraussetzung ist, dass das VLAN existiert. Wenn das VLAN nicht existiert, erstellen Sie es zuerst.

Führen Sie die folgenden Schritte aus:
- ☐ Weisen Sie die erste ACL dem Port zu. Dies kann die IP-ACL oder die MAC-ACL sein.
- ☐ Wenn der Port bereits Mitglied in einem VLAN ist, weisen Sie die zweite ACL diesem VLAN zu.
  - Dies schließt ist die Einrichtung ab.
- ☐ Wenn der Port in **keinem** VLAN Mitglied ist, richten Sie ein VLAN in dem Gerät ein, um es für den Port zu verwenden. Dann weisen Sie die zweite ACL diesem VLAN zu:
  - Erzeugen Sie ein neues VLAN mit einer VLAN-ID >1.
  - Wählen Sie die gewünschte VLAN-Tag-Einstellung `U` oder `T` für den Port.
  - Für die anderen Ports im Gerät, die mit dem gewünschten Port kommunizieren sollen: Fügen Sie diese Ports ebenfalls dem erstellten VLAN hinzu, mit der gewünschten VLAN-Tag-Einstellung `U` oder `T`.
  - Wenn Sie erwarten, dass Sie Datenpakete ohne VLAN-Tag an diesem Port empfangen, legen Sie für den Port eine Port VLAN-ID fest.
  - Für die anderen Ports in dem Gerät, die mit dem angegebenen Port kommunizieren sollen: Wenn Sie erwarten, dass Sie Datenpakete ohne VLAN-Tag an diesen Ports empfangen, legen Sie auch für diese Ports eine Port VLAN-ID fest.
  - Weisen Sie schließlich die zweite ACL diesem VLAN zu.

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 310.

**Anmerkung:**
Eine einzelne ACL können Sie beliebig vielen Port oder VLANs zuweisen.

Das Menü *ACL* enthält die folgenden Dialoge:
- *IPv4-Regel*
- *MAC-Regel*
- *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:
- Hinzufügen von neuen Gruppen und Regeln
- Hinzufügen von neuen Regeln zu vorhandenen Gruppen
- Bearbeiten einer vorhandenen Regel
- Aktivieren und Deaktivieren von Gruppen und Regeln
- Löschen von vorhandenen Gruppen und Regeln
- Ändern der Reihenfolge der vorhandenen Regeln

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > ACL > IPv4-Regel*.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Erstellen*.
- ☐ Klicken Sie die Dropdown-Liste *Gruppenname*, um den Namen der ACL (Gruppe) festzulegen.
  Geben Sie im Suchfeld den Namen ein.
  - ☐ Um einen bereits vorhandenen Namen zu verwenden: Geben Sie den Namen in das Suchfeld ein, dann wählen Sie den gewünschten Eintrag in den Suchergebnissen.
  - ☐ Um einen Namen hinzuzufügen: Geben Sie den Namen in das Suchfeld ein, dann klicken Sie den Link *Erstellen* unterhalb des Suchfelds.
- ☐ 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, wählen Sie die gewünschte Tabellenzeile und klicken die Schaltfläche .
- ☐ Bearbeiten Sie die Parameter der Regel in der Tabelle. Um einen Wert zu ändern, doppelklicken Sie in das betreffende Feld.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

**Anmerkung:**
Das Gerät ermöglicht Ihnen, in den Parametern *Quelle IP-Adresse* und *Ziel IP-Adresse* Platzhalter zu verwenden. Wenn Sie zum Beispiel `192.168.?.?` eingeben, lässt das Gerät Adressen zu, die mit `192.168` beginnen.

**Anmerkung:**
Voraussetzung für das Ändern der Werte in Spalte *Quelle 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 richten Sie ACLs ein, um die Kommunikation von Rechnern B und C zu Rechner A anhand der IP-Adresse (TCP/UDP-Port usw.) zu blockieren.

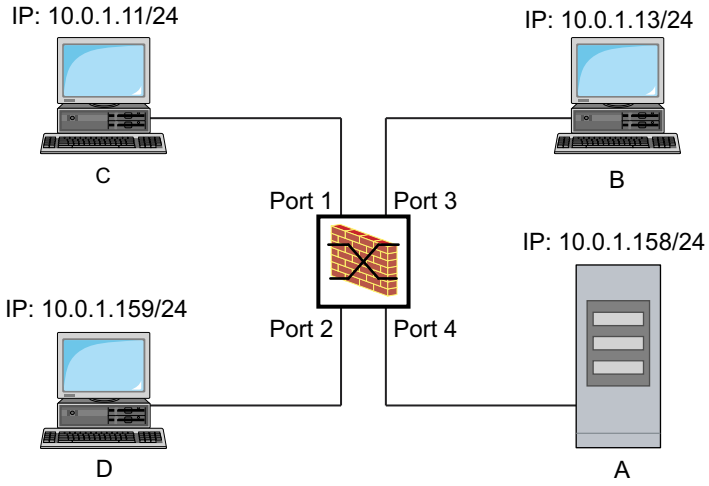



*Abb. 15: Anwendungsbeispiel für eine IP-ACL*

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:
- Hinzufügen 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 *Erstellen*.
- ☐ Klicken Sie die Dropdown-Liste *Gruppenname*, um den Namen der ACL (Gruppe) festzulegen.
  Geben Sie im Suchfeld den Namen ein.
  - ☐ Um einen bereits vorhandenen Namen zu verwenden: Geben Sie den Namen in das Suchfeld ein, dann wählen Sie den gewünschten Eintrag in den Suchergebnissen.
  - ☐ Um einen Namen hinzuzufügen: Geben Sie den Namen in das Suchfeld ein, dann klicken Sie den Link *Erstellen* unterhalb des Suchfelds.
- ☐ 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, wählen Sie die gewünschte Tabellenzeile und klicken die Schaltfläche  .
- ☐ Bearbeiten Sie die Parameter der Regel in der Tabelle. Um einen Wert zu ändern, doppelklicken Sie in das betreffende Feld.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

**Anmerkung:**
In den Feldern *Quelle 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 ACL anhand des Gruppennamens auswählen.

Führen Sie die folgenden Schritte aus:

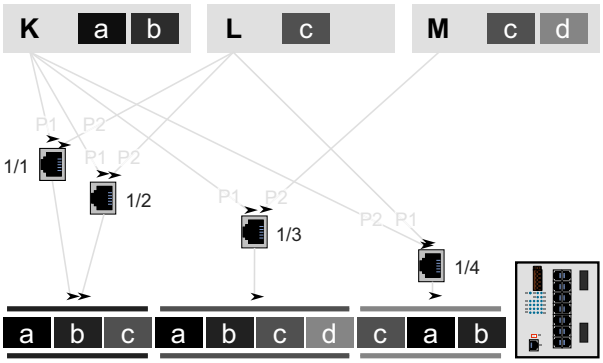
- ☐ Öffnen Sie den Dialog *Netzsicherheit > ACL > Zuweisung*.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Erstellen*.
  - ☐ Legen Sie im Feld *Port/VLAN* den gewünschten Port oder das gewünschte VLAN fest.
  - ☐ Legen Sie im Feld *Priorität* die Priorität fest.
  - ☐ Legen Sie 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

### 9.2.6 Maximale Anzahl zuweisbarer Regeln

Das Gerät ermöglicht Ihnen, bis zu 50 ACLs mit einer bestimmten Anzahl an Regeln festzulegen. Die Anzahl an Regeln, die Sie den Ports und VLANs tatsächlich zuweisen können, ist möglicherweise kleiner als die Anzahl der im Gerät festgelegten Regeln. Das folgende Beispiel veranschaulicht die Faktoren, welche die mögliche Anzahl beeinflussen, die Sie tatsächlich zuweisen können.

Im Gerät sind 3 ACLs mit insgesamt 4 Regeln festgelegt:
- ACL K mit den Regeln a und b
- ACL L mit der Regel c
- ACL M mit den Regeln c und d

Die ACLs und Regeln sind symbolisch benannt. Regeln mit demselben Namen enthalten dieselben Einstellungen.




Beim Zuweisen der ACLs zu den Ports 1/1 bis 1/4 schreibt das Gerät die in den ACLs enthaltenen Regeln mit der festgelegten Priorität in einen Speicherbereich der Hardware, den sich die Ports und VLANs teilen. Die Reihenfolge der Regeln zueinander wird durch die Indexnummer innerhalb der betreffenden ACL sowie durch die zugewiesene Priorität bestimmt.

- Ports 1/1 und 1/2
  Jedem Port sind 3 identische Regeln zugewiesen. Die Reihenfolge ist gleich, aufgrund der zugewiesenen Priorität.
  Das Gerät schreibt 3 Regeln in den Speicher der Hardware. Beide Ports verwenden dieselben Regeln.
- Port 1/3
  Die ersten 3 Regeln stimmen mit denen für Port 1/1 überein.
  Das Gerät schreibt die 3 Regeln noch einmal in den Speicher der Hardware, zusammen mit der zusätzlichen vierten Regel.
- Port 1/4
  Die Regeln stimmen mit denen für Port 1/1 überein.
  Das Gerät schreibt die 3 Regeln aufgrund der veränderten Reihenfolge noch einmal in den Speicher der Hardware.

| Port | Zugewiesene ACLs | Angewendete Regeln | Anzahl Regeln | Belegter Speicherplatz |
|---|---|---|---|---|
| 1/1 | K, L | a, b, c | 3 | 3 |
| 1/2 | K, L | a, b, c | 0 | 3 |
| 1/3 | K, M | a, b, c, d | 4 | 7 |
| 1/4 | L, K | c, a, b | 3 | 10 |

Fazit: Aufgrund von geringfügigen Unterschieden beim Zuweisen belegen 4 Regeln den Speicherplatz von 10 Regeln. Sie können den belegten Speicher optimieren, indem Sie selbst die Regeln geschickt organisieren.

# 10 Netzlaststeuerung

Das Gerät bietet Ihnen eine Reihe von Funktionen, die Ihnen helfen können, die Netzlast zu reduzieren:

- Gezielte Paketvermittlung
- Multicasts
- Lastbegrenzung
- Priorisierung - QoS
- Flusskontrolle

## 10.1 Gezielte Paketvermittlung

Durch gezielte Paketvermittlung reduziert das Gerät die Netzlast.

An jedem seiner Ports lernt das Gerät die Absender-MAC-Adresse empfangener Datenpakete. Die Kombination „Port und MAC-Adresse“ speichert das Gerät in seiner MAC-Adresstabelle (Forwarding Database).

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 (Forwarding Database) gespeichert ist. Ist die MAC-Adresse des Absenders noch unbekannt, generiert das Gerät einen Eintrag. Anschließend vergleicht das Gerät die Ziel-MAC-Adresse des Datenpakets mit den in der MAC-Adresstabelle (Forwarding Database) 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 (Forwarding Database). Ein Neustart oder das Zurücksetzen der MAC-Adresstabelle (Forwarding Database) löscht die Einträge in der MAC-Adresstabelle (Forwarding Database).

### 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 (Forwarding Database) 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 erstellen.

☐ 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 *Erstellen*.
– Legen Sie im Feld *MAC-Adresse* die Ziel-MAC-Adresse fest.
– Legen Sie im Feld *VLAN-ID* die VLAN-ID 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 *MAC-Adresse* eine Unicast-MAC-Adresse festgelegt haben.
  Markieren Sie einen oder mehrere Ports, wenn Sie im Feld *MAC-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*.

☐ Wenden Sie die Einstellungen vorläufig an. 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 hinzufügen, 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 hinzugefügten MAC-Adressfilter zuweisen. |
| `save` | Einstellungen im nichtflüchtigen 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 *`Static`*.

☐ Wenden Sie die Einstellungen vorläufig an. 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. Wählen Sie dazu die Tabellenzeile mit dem Wert *`Static`* in Spalte *Status* und klicken die Schaltfläche .

☐ Wenden Sie die Einstellungen vorläufig an. 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 nichtflüchtigen Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil speichern. |

☐ Gelernte MAC-Adressen löschen.

☐ Um die gelernten Adressen aus der MAC-Adresstabelle (Forwarding Database) zu löschen, klicken Sie die Schaltfläche 🗑 .
Alternativ dazu öffnen Sie den Dialog *Grundeinstellungen > Restart* und klicken die Schaltfläche *FDB leeren*.

| | |
|---|---|
| `clear mac-addr-table` | Die gelernten MAC-Adressen aus der MAC-Adresstabelle (Forwarding Database) 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 von den Multicast-Datenpaketen verursachte Netzlast reduzieren. 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 die Datenströme zwischen den Multicast-Routern und den Monitoren. Die Switches, die im Netz zwischen den Multicast-Routern und den Monitoren liegen, beobachten die IGMP-Datenpakete kontinuierlich (IGMP Snooping).

Switches registrieren Anmeldungen für den Empfang eines Multicast-Stroms (IGMP-Report). Daraufhin fügt das Gerät einen Eintrag in der MAC-Adresstabelle (Forwarding Database) hinzu 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, die IGMP-Datenpakete kontinuierlich zu überwachen und die eigenen Vermittlungseinstellungen für diese Datenpakete 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 (Forwarding Database). 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*.
- ☐ Schalten Sie die Funktion *IGMP-Snooping* ein.
  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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

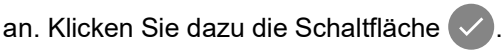
### IGMP-Querier-Funktion einstellen

Optional sendet das Gerät selbst aktive Query-Nachrichten. Alternativ dazu antwortet das Gerät auf Query-Nachrichten oder erkennt andere Multicast-Querier im Netz (Funktion *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 *Querier* des Geräts global ein oder aus.
- ☐ Um die Funktion *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 *IP-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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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:

- *Statisch*
  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` (für geLernt).
- *Learn by LLDP*
  Ein Port mit dieser Einstellung ermittelt automatisch andere Hirschmann-Geräte mittels Link Layer Discovery Protocol (LLDP). Das Gerät lernt dann von diesen Hirschmann-Geräten den IGMP-Query-Status auf diesem Port und richtet die *Querier*-Funktion dementsprechend ein. Der Eintrag `ALA` zeigt, dass die Funktion *Learn by LLDP* aktiv ist. Wenn das Gerät auf diesem Port in diesem VLAN ein anderes Hirschmann-Gerät gefunden hat, zeigt der Eintrag zusätzlich ein `A` (für Automatisch).
- *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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 einrichten

Das Gerät ermöglicht Ihnen, die Vermittlung von Multicast-Datenpaketen einzurichten. 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 vermittelt unbekannte Multicast-Daten an jeden Port.
- 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.

IGMP Snooping ignoriert ausdrücklich die folgenden Multicast-IP-Adressen, da deren zugeordnete Multicast-MAC-Adressen spezielle Funktionen haben:

*Tab. 18: Multicast-IP-Adressen, die von IGMP Snooping ignoriert werden*

| Multicast-IP-Adresse(n) | Multicast MAC-Adresse(n) | Protokolle (Block) |
|---|---|---|
| 224.0.0.0..224.0.0.255 | 01:00:5e:00:00:00..01:00:5e:00:00:ff | Local Network Control Block |
| 224.0.1.1 | 01:00:5e:00:01:01 | NTP/SNTP (Internetwork Control Block) |
| 224.0.1.129..224.0.1.132 | 01:00:5e:00:01:81..01:00:5e:00:01:84 | PTP (Internetwork Control Block) |
| 239.255.16.12 | 01:00:5e:7f:10:0c | HiDiscovery v2 (Administratively Scoped Block) |

**Anmerkung:**
Nach RFC 1112 (*Host Extensions for IP Multicasting*) werden bis zu 32 Multicast-IP-Adressen auf die selbe Multicast-MAC-Adresse abgebildet. Die Tabelle enthält nur die üblicherweise verwendete Multicast-IP-Adresse für eine Multicast-MAC-Adresse und lässt die 31 weiteren Multicast-IP-Adressen aus.

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.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

# 10.3 Lastbegrenzung

Die Lastbegrenzer-Funktion sorgt für einen stabilen Betrieb auch bei hohem Datenaufkommen, indem sie die Menge der Datenpakete auf den Ports begrenzt. Die Lastbegrenzung erfolgt individuell für jeden Port sowie getrennt für eingehende und ausgehende Datenpakete.

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-Datenpakete.

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 die Menge der ausgehenden Datenpakete anstatt der eingehenden Datenpakete. Die Ausgangs-Lastbegrenzung arbeitet durch die geräteinterne Pufferung der Datenpakete besser mit der TCP-Flusskontrolle 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 der Datenpakete:
  - 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 *Einheit* legen Sie fest, ob das Gerät die Schwellenwerte als Prozent der Port-Bandbreite oder als Datenpakete pro Sekunde interpretiert. Der Schwellenwert `0` deaktiviert den Lastbegrenzer.

☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

# 10.4 QoS/Priorität

QoS (Quality of Service) ist ein in 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 Datenpakete mit geringerer Priorität verzögerungsempfindliche Datenpakete stören. Zu den verzögerungsempfindlichen Datenpaketen zählen beispielsweise Sprach-, Video- und Echtzeitdaten.

## 10.4.1 Beschreibung Priorisierung

Zur Priorisierung der Datenpakete 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 empfangenden Ports.
- Die Priorität, die dem empfangenden Port zugewiesen ist.

Beide Klassifizierungskriterien sind konfigurierbar.

Bei der Verkehrsklassifizierung wendet das Gerät folgende Regeln an:

- Wenn der empfangende Port 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 empfangenden Ports.
- Wenn der empfangende Port 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 empfangenden Ports.
- Wenn der empfangende Port auf `untrusted` eingestellt ist, richtet sich das Gerät nach der Priorität des empfangenden Ports.

### 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 dauerhaft.
- *Weighted Fair Queuing*
  Die *Verkehrsklasse* erhält eine spezifische Bandbreite zugewiesen. Damit wird sichergestellt, dass das Gerät die Datenpakete dieser *Verkehrsklasse* sendet, auch wenn es viele Datenpakete in höheren *Verkehrsklassen* gibt.

## 10.4.2 Behandlung empfangener Prioritätsinformationen

Anwendungen kennzeichnen Datenpakete mit folgenden Priorisierungs-Informationen:

- VLAN-Priorität gemäß IEEE 802.1Q (Schicht 2)
- Type-of-Service (ToS) oder DiffServ (DSCP) bei VLAN Management IP-Paketen (Schicht 3)

Das Gerät ermöglicht Ihnen, diese Prioritätsinformation mit den folgenden Optionen 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 empfangenden Ports 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 empfangenden Ports.
- `untrusted`
  Das Gerät ignoriert die Prioritätsinformationen in Datenpaketen und weist den Paketen die Priorität des empfangenden Ports zu.

### 10.4.3 VLAN-Tagging

Für die Funktionen VLAN und Priorisierung sieht IEEE 802.1Q die Einbindung eines MAC-Frames 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“).

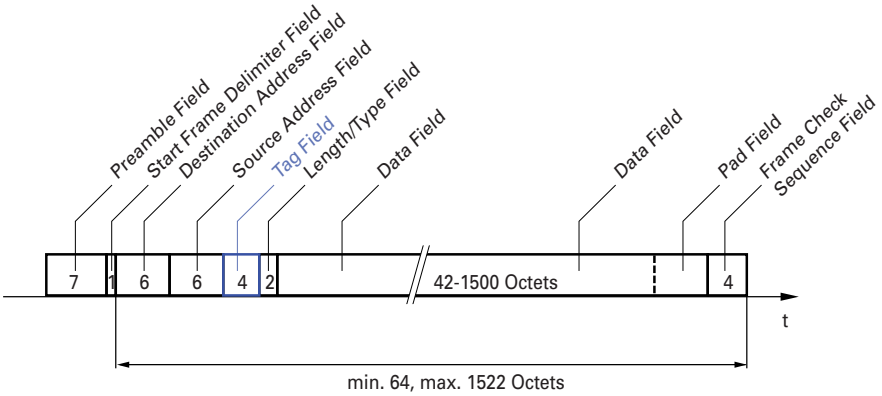



*Abb. 16: Ethernet-Datenpaket mit Tag*

Das Gerät wertet bei Datenpaketen mit VLAN-Tags folgende Informationen aus:

- Prioritätsinformation
- VLAN-Tag, sofern VLANs eingerichtet sind

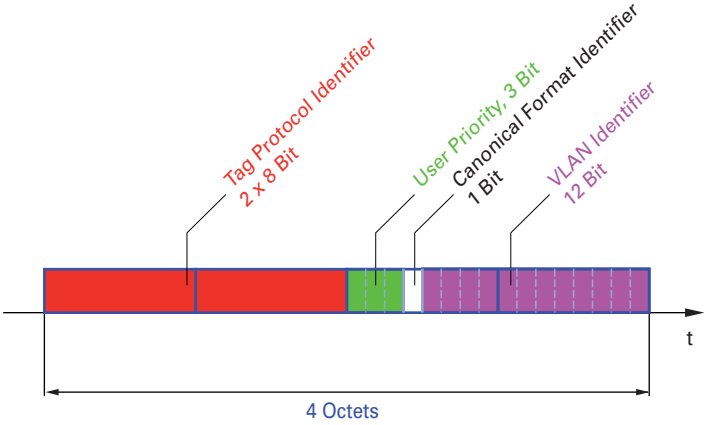



*Abb. 17: Aufbau des VLAN-Tag*

Ein Datenpaket, dessen VLAN-Tag eine Prioritätsinformation, aber keine VLAN-Information (VLAN-ID = 0) enthält, bezeichnet man als *Priority Tagged* Frame.

**Anmerkung:**
Netzprotokolle und Redundanzmechanismen nutzen die höchste *Verkehrsklasse* 7. Wählen Sie für Anwendungsdaten deshalb niedrigere *Verkehrsklassen*.

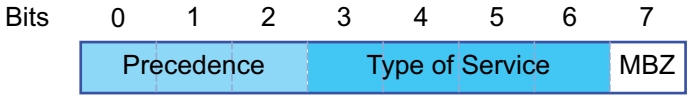
Beachten Sie beim Einsatz der VLAN-Priorisierung folgende Besonderheiten:

- 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 Ihnen eine Unterscheidung unterschiedlicher Dienstgüten. In der Praxis hat sich die Nutzung dieses Feldes jedoch nicht durchgesetzt.




*Tab. 19: 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 Datenpakete mit niedriger Priorität, wenn auf diesem Port viele Datenpakete mit hoher Priorität darauf warten, gesendet zu werden.

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

#### 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 *Strict Priority* für *Traffic-Klasse* = `3` zu aktivieren, gehen Sie wie folgt vor:
  - Markieren Sie das Kontrollkästchen in Spalte *Strict priority*.
- ☐ Um das *Weighted Fair Queuing* für *Traffic-Klasse* = `4` zu aktivieren, gehen Sie wie folgt vor:
  - Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
  - Legen Sie in Spalte *Min. Bandbreite [%]* den Wert `10` fest.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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. |

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------
0         5               weighted
1         20              weighted
2         30              weighted
3         0               strict
4         0               strict
5         0               strict
6         0               strict
7         0               strict
```

### 10.4.7 Management-Priorisierung

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.
- Wenden Sie die Einstellungen vorläufig an. 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.
- Wenden Sie die Einstellungen vorläufig an. 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` | Der VLAN-Priorität `0` die *Verkehrsklasse* `2` zuweisen. |
| `classofservice dot1p-mapping 1 2` | Der VLAN-Priorität `1` die *Verkehrsklasse* `2` zuweisen. |
| `vlan priority 1` | Für die *Port-Priorität* den Wert `1` festlegen. |

```
exit
```
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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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
 .             .
```

### 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 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 überflüssige Datenpakete.

Der in IEEE 802.3 definierte Flusskontrollmechanismus sorgt dafür, dass keine Datenpakete durch Pufferüberlauf auf einem Port verloren gehen. Kurz bevor der Pufferspeicher eines Ports 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. Dies führt dazu, dass der empfangende Port nicht mehr überlastet ist und die eingehenden Datenpakete verarbeiten kann.

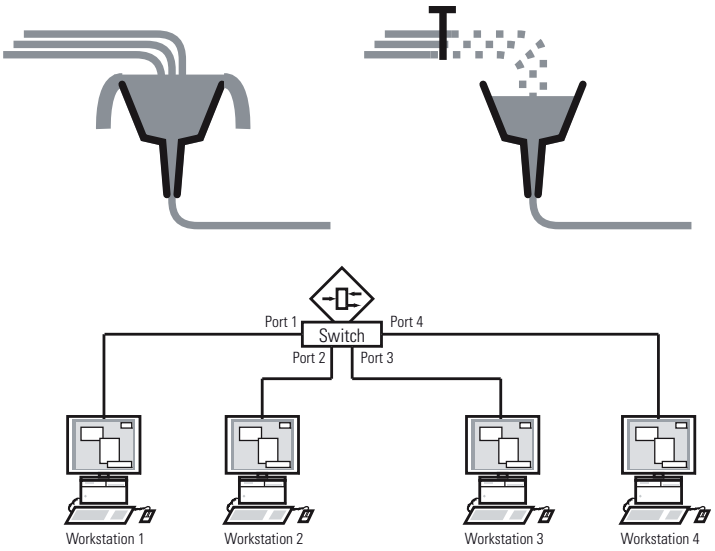



*Abb. 18: Beispiel für Flusskontrolle*

## 10.5.1 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.

### 10.5.2 Flusskontrolle bei Vollduplex-Verbindung

Im Beispiel besteht zwischen der Arbeitsstation 2 und dem Gerät eine Vollduplex-Verbindung.

Bevor die Sende-Warteschlange von Port 2 überläuft, sendet das Gerät eine Aufforderung an Arbeitsstation 2, beim Senden eine kleine Pause einzulegen.

### 10.5.3 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 physischen) 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 gemäß 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 vermittelt die Datenpakete wie üblich.
- Flexibilität
  Sie haben die Möglichkeit, Anwender-Arbeitsgruppen zu bilden, die – abgesehen vom physischen 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 Einrichtung der VLANs entweder Interface 1/6 oder die serielle Verbindung.

### 11.1.1 Anwendungsbeispiel für ein einfaches Port-basiertes VLAN

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.

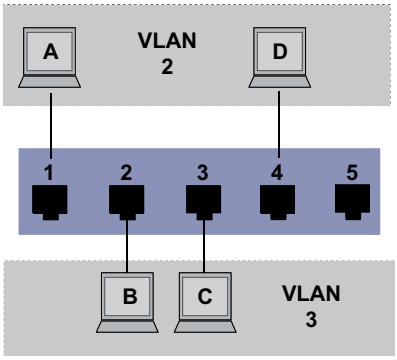



*Abb. 19: Beispiel für ein einfaches Port-basiertes VLAN*

Während der Einrichtung der VLANs fügen Sie für jeden Port Kommunikationsregeln hinzu, die Sie in einer Ingress-Tabelle (Eingang) und einer Egress-Tabelle (Ausgang) einrichten.

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 *Erstellen*.
- ☐ 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` auf `VLAN1`.
- ☐ Wiederholen Sie die vorherigen Schritte, um VLAN `3` mit dem Namen `VLAN3` hinzuzufügen.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `vlan database` | In den VLAN-Konfigurationsmodus wechseln. |
| `vlan add 2` | VLAN `2` hinzufügen. |
| `name 2 VLAN2` | Dem VLAN `2` den Namen `VLAN2` zuweisen. |
| `vlan add 3` | VLAN `3` hinzufügen. |
| `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............................. 128
Number of currently configured VLANs........... 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                    VLAN Type VLAN Creation Time
---- ------------------------------- --------- ------------------
1       VLAN1                        default    0 days, 00:00:05
2       VLAN2                        static     0 days, 02:44:29
3       VLAN3                        static     0 days, 02:52:26
```

☐ Ports einrichten

☐ Öffnen Sie den Dialog *Switching > VLAN > 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 im VLAN.
  Änderungen durch die Funktion *GVRP* sind erlaubt.

Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie den Wert `U` fest.

☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.

☐ Legen Sie in Spalte *Port VLAN-ID* das zugehörige VLAN fest:
`2` oder `3`

☐ Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie für die Ports, an welche ein Endgerät angeschlossen ist, in Spalte *Akzeptierte Datenpakete* den Wert *`admitAll`* fest.

☐ Wenden Sie die Einstellungen vorläufig an. 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 1/1 die Port-VLAN-ID 2 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 1/2 die Port-VLAN-ID 3 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. |
| `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 Anwendungsbeispiel für ein komplexes VLAN-Setup

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 zweiten Switch (im Beispiel rechts gezeichnet).

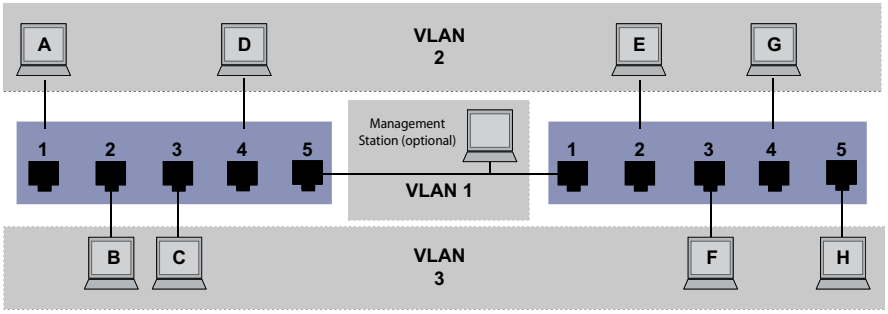



*Abb. 20: Beispiel für eine komplexere VLAN-Konfiguration*

Die Endgeräte der einzelnen VLANs (A bis H) erstrecken sich über 2 Vermittlungsgeräte (Switches). Derartige VLANs heißen deshalb verteilte VLANs. Zusätzlich ist eine optionale Netz-Management-Station abgebildet, die bei korrekter Einrichtung des zugehörigen VLANs Zugriff auf das Management der einzelnen Geräte im Netz 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)

In diesem Beispiel kommen Pakete mit VLAN-Tag für die 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 eingerichtete linke Gerät unter Anwendung der oben festgelegten 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 *Erstellen*.
- ☐ Legen Sie im Feld *VLAN-ID* das VLAN 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` auf `VLAN1`.
- ☐ Wiederholen Sie die vorherigen Schritte, um VLAN `3` mit dem Namen `VLAN3` hinzuzufügen.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `vlan database` | In den VLAN-Konfigurationsmodus wechseln. |
| `vlan add 2` | VLAN `2` hinzufügen. |
| `name 2 VLAN2` | Dem VLAN `2` den Namen `VLAN2` zuweisen. |
| `vlan add 3` | VLAN `3` hinzufügen. |
| `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............................. 128
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- ------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Ports einrichten

- ☐ Öffnen Sie den Dialog *Switching > VLAN > 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 im 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.

- ☐ Legen Sie in Spalte *Port VLAN-ID* das zugehörige VLAN fest: `1`, `2` oder `3`
- ☐ Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie für die Ports, an welche ein Endgerät angeschlossen ist, 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 ein Gast-VLAN an einem Port einrichten 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 einrichten 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 einrichten, 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 *Periode Reauthentifizierung [s]* festgelegte Zeit abläuft und Supplikanten auf dem Port vorhanden sind. Falls keine Supplikanten vorhanden sind, ordnet das Gerät den Port dem eingerichteten Gast-VLAN zu.

Das folgende Beispiel erläutert, wie Sie ein Gast-VLAN hinzufügen. Ein Nicht autorisiertes VLAN fügen Sie auf die gleiche Weise hinzu.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erstellen*.
- ☐ 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 *Erstellen*.
- ☐ 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 > Global*.
- ☐ Schalten Sie die Funktion *802.1X* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.

- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Netzsicherheit > 802.1X > 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*
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `vlan database` | In den VLAN-Konfigurationsmodus wechseln. |
| `vlan add 10` | VLAN `10` hinzufügen. |
| `vlan add 20` | VLAN `20` hinzufügen. |
| `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* 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 physischen 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 auf einem Port die Sprach- und Datenpakete bezüglich VLAN und/oder Priorität zu trennen. Ein wesentlicher Vorteil des Voice-VLANs liegt darin, dass ein hohes Datenaufkommen auf dem Port die Tonqualität eines IP-Telefons nicht beeinträchtigt.

Das Gerät verwendet die Quell-MAC-Adresse zur Identifizierung und Priorisierung des Sprachdatenstroms. Eine Identifizierung mittels MAC-Adresse verringert die Wahrscheinlichkeit, dass sich ein bösartiger Client mit dem Port verbindet und Sprachdatenpakete manipuliert.

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 VoIP-Telefon Sprachdatenpakete entweder mit VLAN-Tag, mit Prioritätsmarkierung oder ohne VLAN-Tag. 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 Datenpakete und versehen beide mit einer Priorisierung. Die Trennung der Datenpakete verbessert die Qualität des Sprachdatenstroms bei hohem Datenaufkommen.

- Wenn Sie bei dem Port den Modus *vlan* konfigurieren, ermöglicht dies 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 dies 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 legen sowohl die Voice-VLAN-ID wie auch die Priorität mit dem *vlan/dot1p-priority*-Modus fest. 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* einrichten, sendet dieses unmarkierte Pakete.
- Wenn Sie das Telefon mit dem Wert *kein* einrichten, verwendet dieses seine eigene Konfiguration zum Senden von Sprachdatenpaketen.

## 11.5 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. Gemäß IEEE 802.1Q legt diese Funktion fest, wie das Gerät Pakete mit VLAN-Tag verarbeitet.

Verwenden Sie den VLAN-Aware-Modus, um die benutzerdefinierte, vom Netzadministrator eingerichtete VLAN-Topologie anzuwenden. Beim Vermitteln von Paketen verwendet das Gerät das VLAN-Tag zusammen 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 empfangene Datenpakete unverändert weiterzuleiten. 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 de VLAN 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

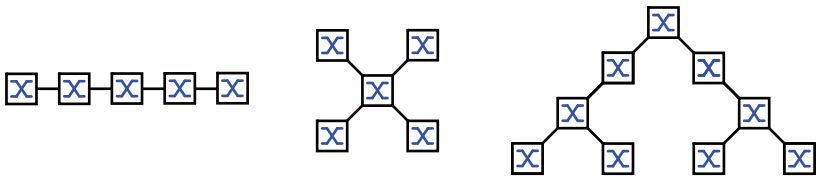


*Abb. 21: Netz mit Linien-, Stern- und Baum-Topologie*

Um die Kommunikation bei Erkennen eines Verbindungsausfalls 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. Bei Erkennen eines Verbindungsausfalls 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. Abhängig 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 physischer Schleifenbildung möglich. Ergebnis ist eine Maschen-Topologie.

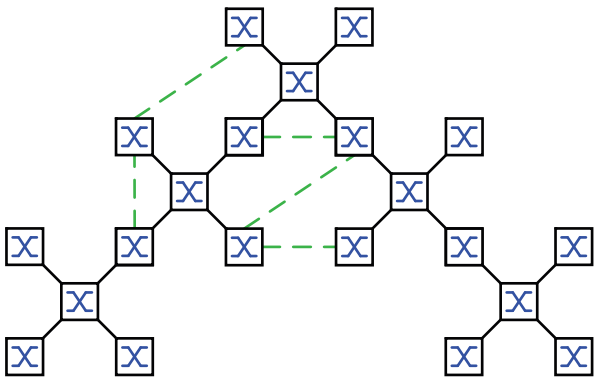


*Abb. 22: Maschen-Topologie: Baum-Topologie mit physischen Schleifen*

Für den Betrieb in dieser Netz-Topologie stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:
- Rapid Spanning Tree Protocol (RSTP)

### Ring-Topologie

In Netzen mit Linien-Topologie lassen sich Redundanzverfahren nutzen, indem Sie die Enden der Linie verbinden. Dadurch entsteht eine Ring-Topologie.

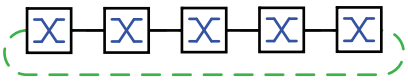


*Abb. 23: Ring-Topologie: Linien-Topologie mit verbundenen Enden*

Für den Betrieb in dieser Netz-Topologie stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:
- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree Protocol (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.<br>Ein MRP-Ring besteht aus bis zu 50 Geräten, die das Media Redundancy Protocol (MRP) nach IEC 62439 unterstützen.<br>Wenn Sie ausschließlich Hirschmann-Geräte einsetzen, sind bis zu 100 Geräte im MRP-Ring möglich. |
| RSTP | beliebige Struktur | Die Umschaltzeit ist abhängig von der Netz-Topologie und von Anzahl der Geräte.<br>• typ. < 1 s bei RSTP<br>• 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. |
| Link-Backup | beliebige Struktur | Wenn das Gerät einen Fehler auf dem primären Link erkannt hat, leitet das Gerät die Datenpakete zum Backup-Link um. Sie verwenden Link-Backup üblicherweise in Netzen von Dienstanbietern oder Unternehmen. |

**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 | Link-Aggreg. | Link-Backup |
|---|---|---|---|---|
| MRP | ▲ | — | — | — |
| RSTP | ▲ 1) | ▲ | — | — |
| Link-Aggreg. | — | ▲ 2) | ▲ | — |
| Link-Backup | ▲ | ▲ | ▲ | ▲ |

▲ Kombinierbar

○ Nicht kombinierbar

1) Eine redundante Kopplung zwischen diesen Netztopologien führt möglicherweise zu Loops.

2) Kombinierbar auf demselben Port

# 12.2 Media Redundancy Protocol (MRP)

Das Media Redundancy Protocol (MRP) ist eine seit Mai 2008 genormte Lösung für Ringredundanz im industriellen Umfeld.

MRP ist kompatibel zur redundanten Ring-Kopplung, unterstützt VLANs und zeichnet sich durch sehr kurze Rekonfigurationszeiten aus.

Ein MRP-Ring besteht aus bis zu 50 Geräten, die das Media Redundancy Protocol (MRP) nach IEC 62439 unterstützen. Wenn Sie ausschließlich Hirschmann-Geräte einsetzen, sind bis zu 100 Geräte im MRP-Ring möglich.

Wenn Sie den festgelegten MRP-Redundanz-Port (Fixed Backup) verwenden und das *Ring-Manager*-Gerät einen Ausfall des primären Ring-Links erkennt, vermittelt es 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 Ringredundanz ermöglicht Ihnen, hochverfügbare, ringförmige Netzstrukturen aufzubauen.

Mit der Funktion *Ring-Manager* können beide Enden eines Backbones in Linienstruktur zu einem redundanten Ring geschlossen werden. Das *Ring-Manager*-Gerät hält die redundante Strecke solange offen, wie die Linienstruktur intakt ist. Fällt ein Segment aus, schließt das *Ring-Manager*-Gerät sofort die redundante Strecke und die Linienstruktur ist wieder intakt.

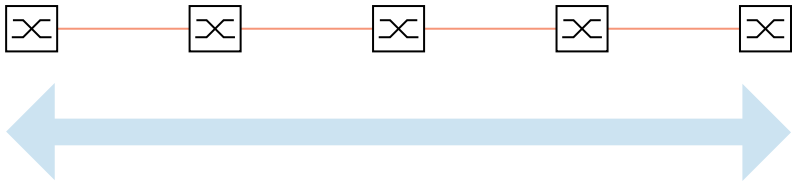


*Abb. 24: Linienstruktur*

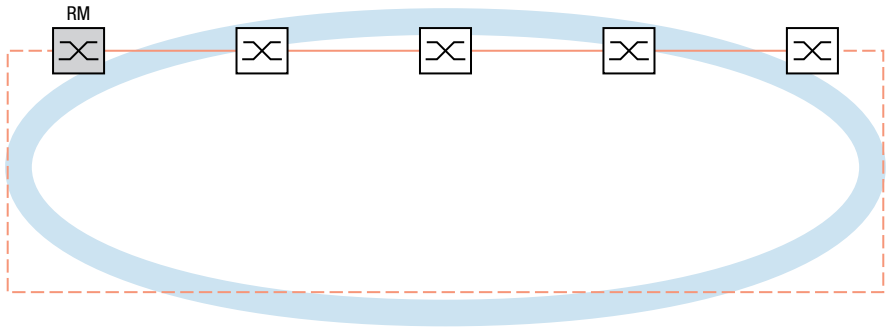



*Abb. 25: Redundante Ringstruktur*
*RM = Ring-Manager*
*—— Hauptleitung*
*- - - redundante Leitung*

### 12.2.2 Rekonfigurationszeit

Bei Erkennen des Ausfalls einer Teilstrecke wandelt das *Ring-Manager*-Gerät den MRP-Ring zurück in eine Linienstruktur. Die maximale Zeit für die Rekonfiguration der Strecke legen Sie im *Ring-Manager*-Gerät 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` einrichten.
Andernfalls sind die Geräte, die ausschließlich längere Verzögerungszeiten unterstützen, wegen Überlastung möglicherweise unerreichbar. Infolgedessen können Loops entstehen.

### 12.2.3 Advanced-Modus

Für noch kürzere als die festgelegte Rekonfigurationszeit bietet das Gerät den *Advanced-Modus*. Der *Advanced-Modus* beschleunigt die Link-Ausfall-Erkennung, wenn die Ringteilnehmer dem *Ring-Manager*-Gerät Unterbrechungen im Ring durch *Link Down*-Meldungen signalisieren.

Hirschmann-Geräte unterstützen *Link Down*-Meldungen. Aktivieren Sie deshalb generell im *Ring-Manager*-Gerät den *Advanced-Modus*.

Falls Sie Geräte einsetzen, die keine *Link Down*-Meldungen senden, rekonfiguriert das *Ring-Manager*-Gerät 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*-Gerät festgelegte Rekonfigurationszeit.
- Im Ring existiert genau ein *Ring-Manager*-Gerät.

Wenn Sie VLANs verwenden, richten Sie jeden Ring-Port mit folgenden Einstellungen ein:

- Ingress-Filtering deaktivieren, siehe Dialog *Switching > VLAN > Port*.
- Port-VLAN-ID (PVID) festlegen, siehe Dialog *Switching > VLAN > Port*.
  - PVID = `1`, wenn das Gerät die MRP-Datenpakete unmarkiert überträgt (VLAN-ID = `0` im Dialog *Switching > L2-Redundanz > MRP*)
    Durch die Einstellung PVID = `1` weist das Gerät die unmarkiert empfangenen Pakete automatisch dem VLAN 1 zu.
  - PVID = `any`, wenn das Gerät die MRP-Datenpakete in einem VLAN überträgt (VLAN-ID ≥`1` im Dialog *Switching > L2-Redundanz > MRP*)
- Egress-Regeln festlegen, siehe Dialog *Switching > VLAN > Konfiguration*.
  - `U` (untagged) für die Ring-Ports von VLAN 1, wenn das Gerät die MRP-Datenpakete unmarkiert überträgt (VLAN-ID = `0` im Dialog *Switching > L2-Redundanz > MRP*, der MRP-Ring ist keinem VLAN zugewiesen).
  - `T` (tagged), für die Ring-Ports in dem VLAN, das Sie dem MRP-Ring zuweisen. Wählen Sie `T`, wenn das Gerät die MRP-Datenpakete in einem VLAN überträgt (VLAN-ID ≥`1` im Dialog *Switching > L2-Redundanz > MRP*).

## 12.2.5 Erweiterte Informationen

### MRP-Pakete

Das Media Redundancy Protocol (MRP) verwendet *Test*-, *Link Change*- und *Topology Change*- (*FDB Flush*)-Pakete.

Das *Ring-Manager*-Gerät ist mit 2 Ring-Ports mit dem Ring verbunden. Solange alle Verbindungen im Ring funktionieren, setzt das *Ring-Manager*-Gerät einen seiner Ports, den redundanten Port, in den Zustand *blocking*. In diesem Zustand sendet und empfängt der redundante Port keine normalen (Nutzlast-) Datenpakete. Auf diese Weise verhindert das *Ring-Manager*-Gerät einen Loop.

Das *Ring-Manager*-Gerät sendet periodisch Testpakete von beiden Ring-Ports in den Ring. Die Testpakete sind spezielle Pakete. Das *Ring-Manager*-Gerät sendet und empfängt Testpakete auch am redundanten Port, obwohl der redundante Port normale Pakete blockiert. Das *Ring-Manager*-Gerät erwartet, die Testpakete am jeweils anderen Ring-Port zu empfangen. Wenn das *Ring-Manager*-Gerät für eine festgelegte Zeit keine erwarteten Testpakete empfängt, erkennt es einen Ring-Ausfall.

Wenn die *Advanced-Modus*-Funktion aktiv ist, reagiert das *Ring-Manager*-Gerät auch auf Link Down-Pakete. Voraussetzung ist, dass jedes Gerät im Ring in der Lage ist, ein *Link Change*-Paket zu senden, wenn sich die Verbindung zum jeweils nächsten Gerät im Ring ändert. Diese Pakete helfen dem *Ring-Manager*-Gerät dabei, schneller auf den Ausfall oder die Wiederherstellung einer Verbindung zu reagieren. Das *Ring-Manager*-Gerät empfängt die *Link Change*-Pakete auch an seinem redundanten Port.

Bei der Rekonfiguration des Rings löscht das *Ring-Manager*-Gerät seine MAC-Adresstabelle (Forwarding Database) und sendet *Topology Change*-Pakete an die am Ring teilnehmenden Geräte. Die *Topology Change*-Pakete veranlassen die anderen am Ring teilnehmenden Geräte dazu, ihre MAC-Adresstabelle (Forwarding Database) ebenfalls zu löschen. Dieses Verfahren hilft dabei, die Nutzlast-Pakete rascher über den neuen Pfad zu vermitteln. Dieses Verfahren wird angewendet, gleichgültig, ob die Ring-Rekonfiguration durch eine *Link Down*- oder eine *Link Up*-Meldung 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)<br>20 ms (für Ring-Wiederherstellungs-Zeit 200 ms) |
| | | Zeitüberschreitung für Empfang | 400 ms (für Ring-Wiederherstellungs-Zeit 500 ms)<br>160 ms (für Ring-Wiederherstellungs-Zeit 200 ms) |
| *Link Down*-Paket[2] | Ereignis-getrieben | Beim Verbindungs-Ausfall eines Ring-Ports. | - |
| *Topology Change*-Paket[3] | Ereignis-getrieben | Bei Rekonfiguration | - |

1. Ausschließlich vom *Ring-Manager*-Gerät versendet.
2. Gesendet von unterstützenden Ring-Teilnehmern.
3. Der Empfang eines *Topology Change*-Pakets veranlasst die unterstützenden, am Ring teilnehmenden Geräte dazu, ihre MAC-Adresstabelle (Forwarding Database) zu löschen.

### MRP-Paket-Priorisierung

Die am Ring teilnehmenden Geräte senden *Test*-, *Link Change*- und *Topology Change*-Pakete mit einer durch den Benutzer festlegbaren VLAN-ID. Das voreingestellte VLAN-ID ist 0. Die Geräte senden die Testpakete ohne VLAN-Tag und daher ohne Prioritäts- (Class of Service-) Information.

Um die Wiederherstellungszeit bei hoher Netzlast zu minimieren, können Sie ein VLAN-Tag und damit auch Prioritätsinformation zu diesen Paketen hinzufügen. Die Geräte vermitteln und senden diese Pakete dann mit der IEEE 802.1Q Class of Service-Priorität 7 (Netz-Steuerung).

Um die Testpakete zu priorisieren, führen Sie die folgenden Schritte auf dem *Ring-Manager*- und auf den *Ring-Client*-Geräten aus:

- ☐ Legen Sie die MRP-VLAN-ID auf einen Wert ≥1 fest.
- ☐ Legen Sie die Ring-Ports als T (Mitglied mit VLAN-Tag) dieses MRP-VLANs 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 dieses MRP-VLAN hinzu. Wenn das MRP-VLAN noch nicht existiert, richtet das Gerät automatisch dieses VLAN ein. Nach dem Festlegen einer neuen MRP-VLAN-ID prüfen Sie im Dialog *Switching > VLAN > Konfiguration* die VLAN- und Port-Einstellungen.

### 12.2.6 Anwendungsbeispiel für einen MRP-Ring

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.

Bei Erkennen eines Ausfalls des primären Ring-Links sendet das *Ring-Manager*-Gerät Daten auf dem sekundären Ring-Link. Bei Wiederherstellung des primären Links wechselt der sekundäre Link zurück in den Backup-Modus.

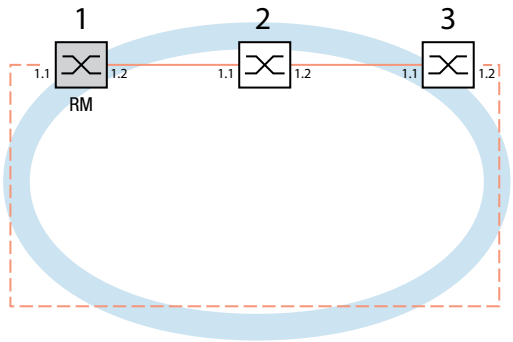



*Abb. 26: Beispiel für einen MRP-Ring*
*RM = Ring-Manager*
*—— Hauptleitung*
*- - - redundante Leitung*

Die folgende Beispielkonfiguration beschreibt die Konfiguration des *Ring-Manager*-Geräts (1). Richten Sie die 2 anderen Geräte (2 bis 3) in gleicher Weise ein, jedoch ohne die *Ring-Manager*-Funktion einzuschalten. Dieses Beispiel nutzt kein VLAN. Als Ring-Wiederherstellungszeit legen Sie den Wert `30ms` fest. Jedes Gerät unterstützt die Funktion *Advanced-Modus*.

- ☐ Bauen Sie das Netz nach Ihren Erfordernissen auf.
- ☐ Um die Ring-Wiederherstellungszeit für den Fall zu minimieren, wenn eine Verbindung nach einem Ausfall wiederhergestellt wird, richten Sie die Datenrate und den Duplex-Modus der Ring-Ports wie folgt ein:
  - Für 100 Mbit/s-TX-Ports deaktivieren Sie die Automatische Verbindungsaushandlung und richten Sie *100M FDX* manuell ein:
  - Für die anderen Port-Typen behalten Sie die Port-spezifischen Voreinstellungen bei.

**Anmerkung:**
Richten Sie jedes Gerät des MRP-Rings einzeln ein. 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. Richten Sie jeden Ringteilnehmer mit der gleichen MRP-Domänen-ID ein. Die MRP-Domänen-ID ist eine Folge aus 16 Ziffernblöcken (8-Bit-Werten).

Beim Konfigurieren mit der grafischen Benutzeroberfläche verwendet das Gerät den voreingestellten Wert („default domain“) `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

| | |
|---|---|
| `mrp domain add default-domain` | Eine MRP-Domäne mit der ID `default-domain` hinzufügen. |
| `mrp domain modify port primary 1/1` | Port `1/1` als Ring-Port *primary* festlegen. |
| `mrp domain modify port secondary 1/2` | Port `1/2` als *secondary*-Ring-Port festlegen. |

Schalten Sie den *Fixed backup*-Port ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ Schalten Sie die Funktion *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 *Primär-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 das *Ring-Manager*-Gerät den sekundären Port und hebt die Blockierung des *Primär-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 die Funktion *Ring-Manager* ein.
  Bei den anderen Geräten im Ring belassen Sie die Einstellung auf *Aus*.

| | |
|---|---|
| `mrp domain modify mode manager` | Gerät zum *Ring-Manager*-Gerät bestimmen. Bei den anderen Geräten im Ring belassen Sie die Voreinstellung. |

☐ Markieren Sie das Kontrollkästchen im Feld *Advanced-Modus*.

`mrp domain modify advanced-mode enabled` *Advanced-Modus* aktivieren.

☐ 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 das Netz entspricht, dann wählen Sie den Wert `500ms`.

☐ Aktivieren Sie die Funktion des MRP-Rings.

☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

`mrp domain modify operation enable` MRP-Ring aktivieren.

Wenn jeder Ring-Teilnehmer eingerichtet ist, schließen Sie die Linie, um den Ring herzustellen. 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.
- *ausgeschaltet*
  Der Port ist ausgeschaltet.
- *nicht verbunden*
  Keine Verbindung vorhanden.

Das Feld *Information* zeigt Meldungen zur Redundanzkonfiguration und mögliche Ursachen für erkannte Fehler.

Wenn das Gerät als *Ring-Client* oder als *Ring-Manager* arbeitet, sind folgende Meldungen möglich:
- *Redundanz verfügbar. Ring ist geschlossen.*
  Die Redundanz ist eingerichtet. Fällt eine Komponente des Rings aus, übernimmt die redundante Strecke deren Funktion.
- *Konfigurationsfehler: Ring-Port Verbindung fehlerhaft*
  Fehler in der Verkabelung der Ring-Ports erkannt.

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 sendet.
  Um die MRP-VLAN-ID zu setzen, richten Sie zuerst die VLANs und die zugehörigen Egress-Regeln im Dialog *Switching > VLAN > Konfiguration* ein.
  - 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 `1` die VLAN-Zugehörigkeit `U` (untagged) 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. |

# 12.3 Spanning Tree

**Anmerkung:**
Das Spanning Tree Protocol (STP) 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 innerhalb des Netzes führen. Um dies zu vermeiden, können Sie Spanning Tree einsetzen. 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 Ring-Topologie 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:**
Die Norm RSTP setzt voraus, 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 mit RSTP verloren.
Ein Gerät, das lediglich RSTP unterstützt, arbeitet mit MSTP-Geräten zusammen, indem es sich keiner MST-Region, sondern dem Common Spanning Tree (CST) zuweist.

## 12.3.1 Grundlagen

Da RSTP eine Weiterentwicklung des STP ist, gilt jede der folgenden Beschreibungen des STP auch für RSTP.

### 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, welche 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.
- Die Baumstruktur ist bis zur maximalen Netzausdehnung stabilisiert.
- Die Topologie stabilisiert sich innerhalb einer vorhersehbaren Zeit.
- Der Administrator kann die Topologie vorbestimmen und reproduzieren.
- Transparenz für die Endgeräte.
- Die Netzlast ist im Verhältnis zur verfügbaren Übertragungskapazität gering, da eine Baumstruktur eingerichtet wurde.

### Bridge-Parameter

Jede Bridge und ihre Verbindungen werden im Kontext von Spanning Tree eindeutig durch die folgenden Parameter beschrieben:
- *Bridge-Identifikation*
- *Root-Pfadkosten* der Bridge-Ports
- *Port-Identifikation*

### Bridge-Identifikation

Die *Bridge-Identifikation* besteht aus 8 Bytes. Die Bridge mit dem numerisch niedrigsten Wert für die *Bridge-Identifikation* besitzt die höchste Priorität.

Nach der ursprünglichen Norm 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.

In der neueren Norm 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. Folglich 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.

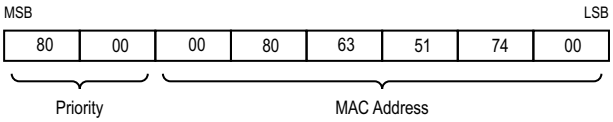



*Abb. 27: Bridge-Identifikation, Beispiel (Interpretation nach IEEE 802.1D-1998, Werte in Hexadezimalschreibweise)*

### Root-Pfadkosten

Jedem Pfad, der 2 Bridges miteinander verbindet, weisen die Bridges Kosten für die Übertragung (Pfadkosten) zu. Das Gerät bestimmt diesen Wert abhängig von der Datenrate (siehe Tabelle 29 auf Seite 202). 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* entsprechen der Summe der einzelnen Pfadkosten vom Port der angeschlossenen Bridge bis zur *Root-Bridge*.

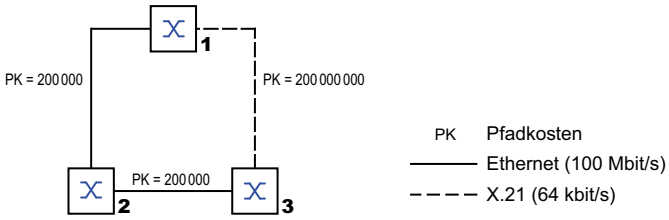



*Abb. 28: Pfadkosten*

*Tab. 29: Empfohlene Pfadkosten beim RSTP abhängig 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. Vergewissern Sie sich, dass Bridges, die mit IEEE 802.1D-1998 konform sind und ausschließlich 16-Bit-Werte für Pfadkosten unterstützen, als Pfadkosten den Wert 65535 (FFFFH) verwenden, wenn Sie diese zusammen mit Bridges benutzen, welche 32-Bit-Werte für die Pfadkosten unterstützen.

### Port-Identifikation

Nach der ursprünglichen Norm IEEE 802.1D-1998 besteht die *Port-Identifikation* aus 2 Bytes. Das niederwertigere Byte enthält die physische 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).

In der neueren Norm 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. Folglich 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).

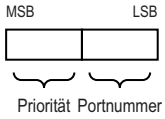



*Abb. 29: Port-Identifikation (Interpretation nach IEEE 802.1D-1998)*

### 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).

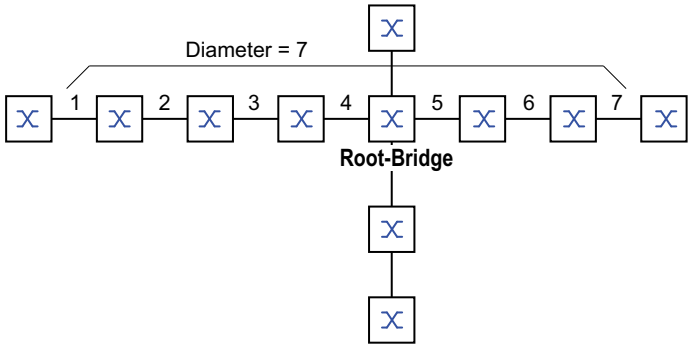



*Abb. 30: Definition „Diameter“*

Der im Netz erreichbare Netzdurchmesser beträgt MaxAge-1.

Im Lieferzustand ist MaxAge MaxAge = 20, der maximal erreichbare Diameter ist 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.

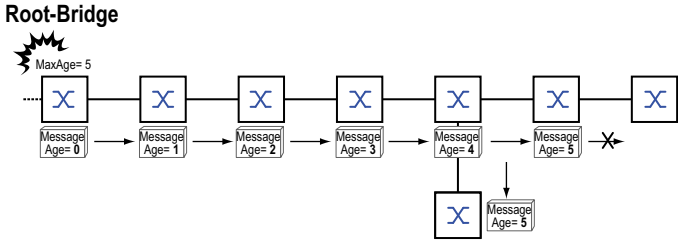



*Abb. 31: Übertragung einer STP-BPDU abhängig von MaxAge*

## 12.3.2 Regeln für die Erstellung der Baumstruktur

### Bridge-Information

Zur Berechnung der Baumstruktur benötigen die Bridges nähere Informationen über die anderen Bridges, die sich im Netz befinden.

Um diese Informationen zu erhalten, sendet jede Bridge eine BPDU (Bridge Protocol Data Unit) an andere Bridges.

Bestandteil einer BPDU ist unter anderem:
- *Bridge-Identifikation*
- *Root-Pfadkosten*
- *Port-Identifikation*

(siehe IEEE 802.1D)

### Aufbauen der Baumstruktur

Die Bridge mit dem numerisch niedrigsten Wert für die *Bridge-Identifikation* nennt man auch *Root-Bridge*. Diese Bridge 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. Hierzu verwendet die weiter von der Root entfernte Bridge die *Bridge Identifikation* der näher an der Root liegenden Bridge. Die weiter von der Root entfernte 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 29 auf Seite 203). Die Bridge blockiert dabei den Port, der zu dem Port mit der schlechteren ID führt. Eine numerisch höhere ID ist die logisch schlechtere. Haben 2 Ports die gleiche Priorität, hat der Port mit der höheren Port-Nr. die numerisch höhere ID; dies ist die logisch schlechtere.

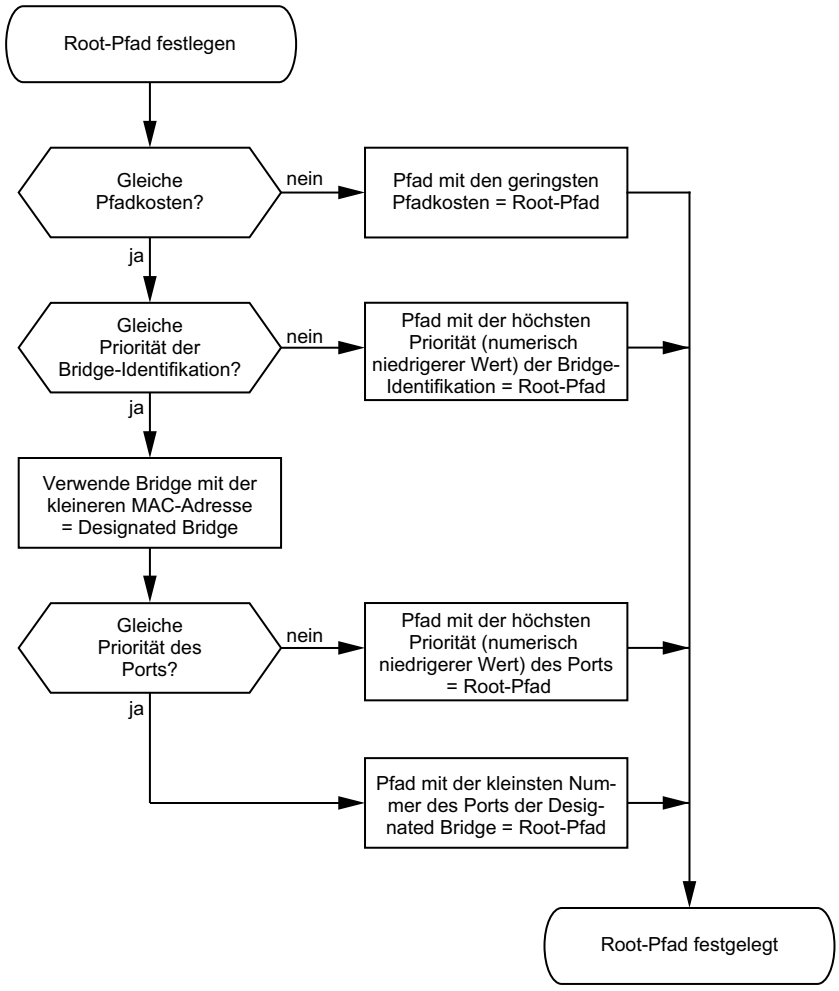



*Abb. 32: Flussdiagramm Root-Pfad festlegen*

## 12.3.3 Beispiele

### Beispiel für die Bestimmung des Root-Pfads

Anhand des Netzplanes kann man das Flussdiagramm (siehe Abbildung 32 auf Seite 205) zur Festlegung des Root-Paths nachvollziehen. Der Administrator hat für jede Bridge eine Priorität in der *Bridge-Identifikation* festgelegt. Die Bridge mit dem numerisch niedrigsten Wert 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 *Port-Identifikation* (Port 1 < Port 3).

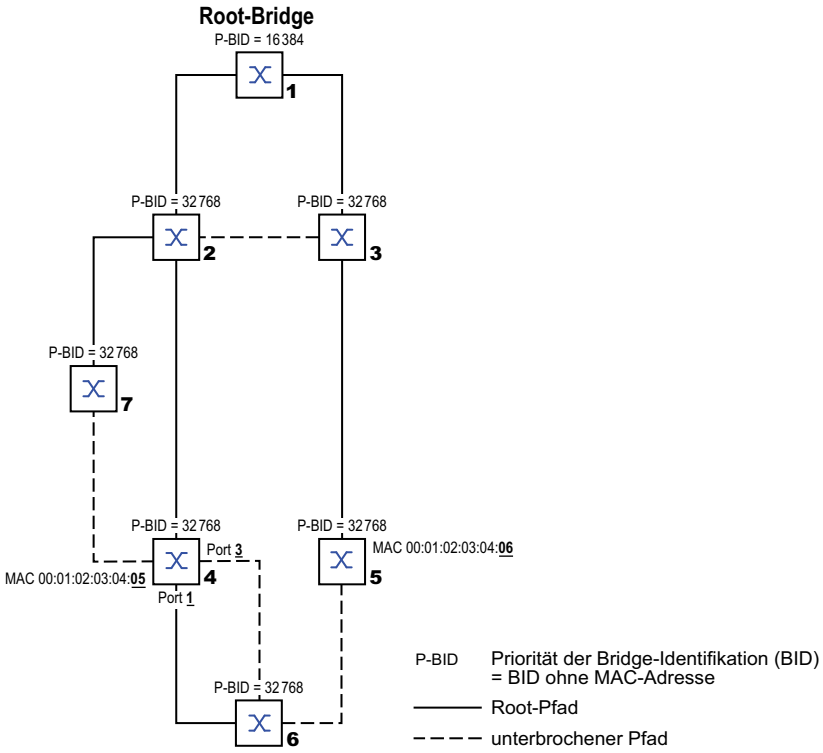



*Abb. 33: Beispiel eines Netzplans für die Bestimmung des Root-Pfads*

**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 32 auf Seite 205) 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 verursachen würde.

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 Wert 32768.

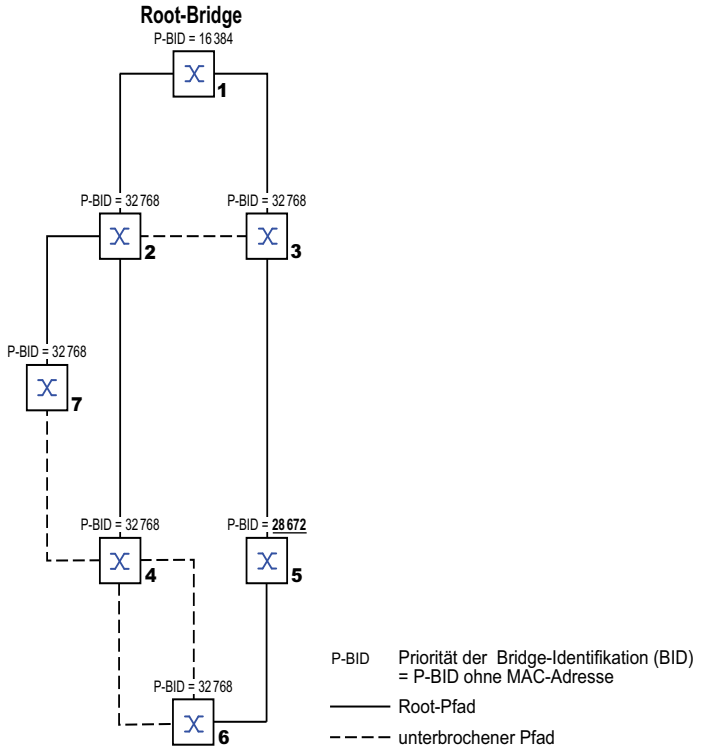



*Abb. 34: Beispiel eines Netzplans für die Manipulation des Root-Pfads*

### Beispiel für die Manipulation der Baumstruktur

Der Administrator 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, welche die *Root-Bridge* zu jeder anderen Bridge sendet.

Richtet der Administrator die Bridge 2 als *Root-Bridge* ein, 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.

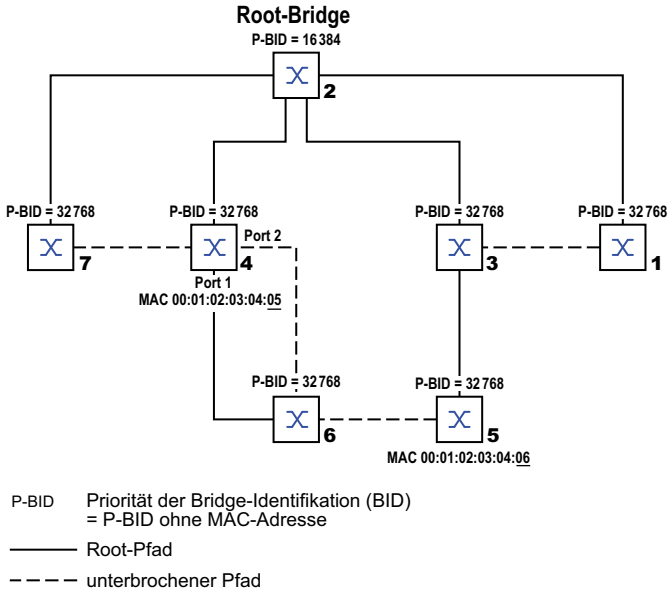



*Abb. 35: Beispiel für die Manipulation der Baumstruktur*

# 12.4 Rapid Spanning Tree Protokoll

Das Rapid Spanning Tree Protocol (RSTP) verwendet denselben Algorithmus zur Bestimmung der Baumstruktur wie Spanning Tree Protocol (STP). Wenn eine Verbindung oder eine Bridge ausfällt, bietet das Rapid Spanning Tree Protocol (RSTP) Mechanismen, welche die Rekonfiguration beschleunigen.

Eine zentrale Bedeutung erfahren in diesem Zusammenhang die Ports.

## 12.4.1 Port-Rollen

Das Rapid Spanning Tree Protocol (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 32 auf Seite 205.
  Die *Root-Bridge* selbst besitzt keinen *Root-Port*, sondern ausschließlich *Designated-Ports*.
- *Designated-Port*:
  Die Bridge in einem Netzsegment, welche den numerisch niedrigsten Wert für die *Root-Pfadkosten* hat, ist die *Designated-Bridge*.
  Haben mehrere Bridges die gleichen *Root-Pfadkosten*, übernimmt die Bridge mit dem numerisch niedrigsten Wert für die *Bridge-Identifikation* die Rolle der *Designated-Bridge*. Der *Designated-Port* an dieser Bridge ist der Port, der ein von der *Root-Bridge* wegführendes Netzsegment verbindet. Ist eine Bridge über mehr als einen 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*
  Jedes Netzsegment, in dem sich keine weiteren RSTP-Bridges befinden, ist mit genau einem *Designated-Port* verbunden. Dieser *Designated-Port* ist in diesem Fall auch ein *Edge-Port*. Ein *Edge-Port* ist dadurch gekennzeichnet, dass er keine *RST-BPDUs (Rapid Spanning Tree Bridge Protocol Data Units)* empfängt.
- *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 *Designated-Port* dieses Netzsegmentes (ohne RSTP-Bridges) ausfällt.
- Disabled-Port
  Dies ist ein Port, der innerhalb des Spanning-Tree-Protokolls keine Rolle spielt, also abgeschaltet ist oder keine Verbindung hat.

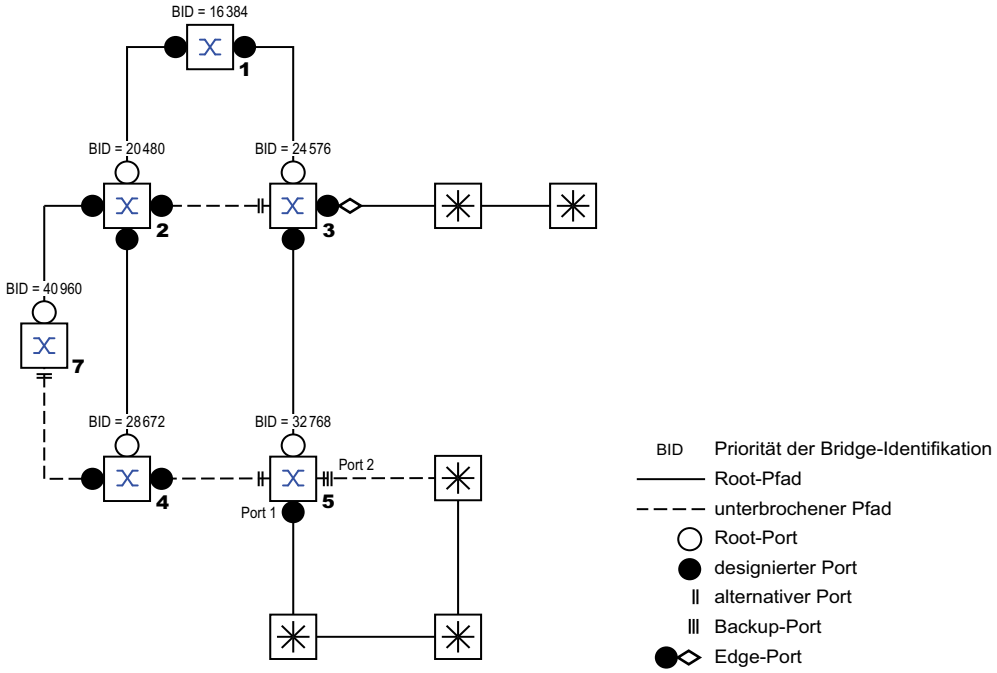



*Abb. 36: Port-Rollen-Zuweisung*

## 12.4.2 Port-Stati

Abhängig von der Baumstruktur und dem Status der ausgewählten Verbindungswege weist RSTP den Ports ihren Status zu.

*Tab. 30: Beziehung zwischen Werten für Port-Status 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 der MAC-Adresstabelle (Forwarding Database), keine Datenpakete außer STP-BPDUs

- *Learning*: Address Learning in der MAC-Adresstabelle (Forwarding Database) aktiv, keine Datenpakete außer STPBPDUs
- *Forwarding*: Address Learning in der MAC-Adresstabelle (Forwarding Database) aktiv, Senden und Empfangen jedes Paket-Typs (nicht ausschließlich STP-BPDUs)

### 12.4.3 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
- *Port-Identifikation* des Ports, durch den die Nachricht gesendet wurde
- *Port-Identifikation* 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.

### 12.4.4 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 *Alternate-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 *Alternate-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 Spanning Tree Protocol (STP) bestimmt das Alter der Einträge in der MAC-Adresstabelle (Forwarding Database) über die Aktualisierung der Kommunikation. Das Rapid Spanning Tree Protocol (RSTP) löscht sofort und gezielt die Einträge der Ports, die von einer Umkonfiguration betroffen sind.
- Reaktion auf Ereignisse:
  Ohne Zeitvorgaben entsprechen zu müssen, reagiert Rapid Spanning Tree Protocol (RSTP) sofort auf Ereignisse, zum Beispiel Unterbrechung und Wiederherstellung der Verbindung.

**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 (STP) verwenden oder Sie wählen eines der anderen in diesem Handbuch beschriebenen Redundanzverfahren.

### 12.4.5 Gerät konfigurieren

RSTP richtet die Netztopologie komplett selbstständig ein. Das Gerät mit dem numerisch niedrigsten Wert für die *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 im Gerät eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Schalten Sie die Funktion ein.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 numerisch niedrigeren Wert fest.
  Die Bridge mit dem numerisch niedrigsten Wert für die *Bridge-Identifikation* hat die höchste Priorität und wird zur *Root-Bridge* des Netzes.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 eingeben, 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-Identifikation* (*Bridge-Priorität* und MAC-Adresse) des jeweiligen Geräts sowie der *Root-Bridge*.
- Nummer des Ports, der zur *Root-Bridge* führt.
- Pfadkosten vom *Root-Port* des Geräts bis zur *Root-Bridge*.

Führen Sie die folgenden Schritte aus:

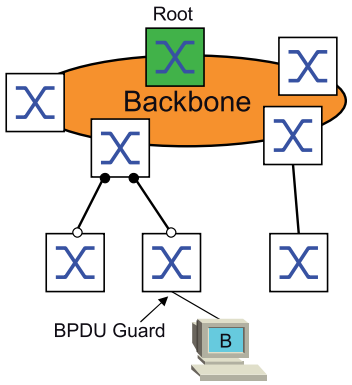
| | |
|---|---|
| `show spanning-tree global` | Zur Kontrolle die Parameter anzeigen. |

### 12.4.6 Guards

Das Gerät ermöglicht Ihnen, auf den Ports verschiedene Schutzfunktionen (Guards) zu aktivieren.

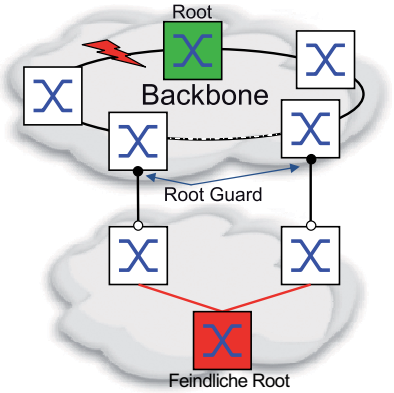
Folgende Schutzfunktionen helfen, das Netz vor Fehlkonfigurationen, Loops und Angriffen mit STP-BPDUs zu schützen:

- *BPDU-Guard* – für manuell festgelegte *Edge-Ports* (Ports, an welche ein Endgerät angeschlossen ist)
  Diese Schutzfunktion aktivieren Sie global im Gerät.




  Ports, an welche ein Endgerät angeschlossen ist, empfangen im Normalfall keine STP-BPDUs. Versucht ein Angreifer, auf diesem Port trotzdem STP-BPDUs einzuspeisen, deaktiviert das Gerät den Port.

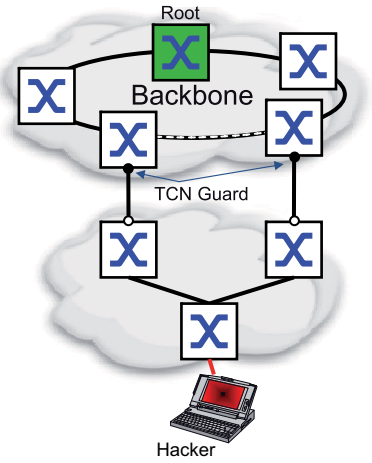
- *Root-Guard* – für *Designated-Ports*
  Diese Schutzfunktion aktivieren Sie für jeden Port separat.




  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`.

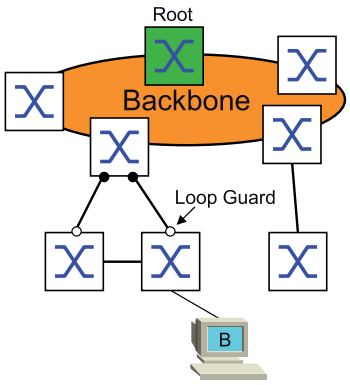
  Bleiben die STP-BPDUs mit besserer Pfadinformation zur *Root-Bridge* aus, setzt das Gerät den Status des Ports nach 2 × *Hello-Time [s]* wieder auf einen Wert gemäß Port-Rolle.

- *TCN-Guard* – für Ports, die STP-BPDUs mit *Topology Change*-Flag empfangen
  Diese Schutzfunktion aktivieren Sie für jeden Port separat.




  Bei eingeschalteter Schutzfunktion ignoriert das Gerät *Topology Change*-Flags in empfangenen STP-BPDUs. Der Inhalt der MAC-Adresstabelle (Forwarding Database) des Ports bleibt dadurch unverändert. Weitere Informationen in der BPDU, die eine Topologie-Änderung bewirken, verarbeitet das Gerät jedoch.

- *Loop-Guard* – für *Root-Ports*, *Alternate-Ports* und *Backup-Ports*
  Diese Schutzfunktion aktivieren Sie für jeden 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.

### Funktion BPDU-Guard aktivieren

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Markieren Sie das Kontrollkästchen *BPDU-Guard*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |

| | |
|---|---|
| `configure` | In den Konfigurationsmodus wechseln. |
| `spanning-tree bpdu-guard` | Funktion *BPDU-Guard* aktivieren. |
| `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 die Ports, an welche ein Endgerät angeschlossen ist, das Kontrollkästchen in Spalte *Admin-Edge Port*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `interface <slot/port>` | In den Interface-Konfigurationsmodus von Interface `<x/y>` wechseln. |
| `spanning-tree edge-port` | Den Port als *Edge-Port* (Port, an welchen ein Endgerät angeschlossen ist) kennzeichnen. |
| `show spanning-tree port <slot/port>` | 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 <slot/port>` | Zur Kontrolle die Parameter des Ports anzeigen. Der Wert des Parameters *BPDU guard effect* ist `enabled`. |

Setzen Sie den Zustand des Ports 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* (Port, an welchen ein Endgerät angeschlossen ist) auf.
    oder
  - Deaktivieren Sie die Funktion *BPDU-Guard*.
- ☐ Schalten Sie den Port wieder ein.

### Funktion Root-Guard / TCN-Guard / Loop-Guard aktivieren

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-Ports*, *Alternate-Ports* 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*.

- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `interface <slot/port>` | In den Interface-Konfigurationsmodus von Interface `<x/y>` wechseln. |
| `spanning-tree guard-root` | Die Funktion *Root-Guard* auf dem *Designated-Port* aktivieren. |
| `spanning-tree guard-tcn` | Die Funktion *TCN-Guard* auf dem Port aktivieren, der STP-BPDUs mit *Topology Change*-Flag empfängt. |
| `spanning-tree guard-loop` | Die Funktion *Loop-Guard* auf einem *Root-Port*, *Alternate-Port* oder *Backup-Port* aktivieren. |
| `exit` | Interface-Modus verlassen. |
| `show spanning-tree port <slot/port>` | Zur Kontrolle die Parameter des Ports anzeigen. |

# 12.5 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 einer 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 eingerichteten Links ein Link ausfällt, leiten die anderen Links in der Gruppe die Datenpakete weiter.

Die Voreinstellungen für eine neue *Link-Aggregation*-Instanz sind:
- In Spalte *Aktiv* ist das Kontrollkästchen markiert.
- In Spalte *Trap senden (Link-Up/Down)* ist das Kontrollkästchen markiert.
- In Spalte *Statische Link-Aggregation* ist das Kontrollkästchen unmarkiert.
- In Spalte *Aktive Ports (min.)* ist der Wert 1.

## 12.5.1 Funktionsweise

Das Gerät arbeitet mit dem Single-Switch-Verfahren. Das Single-Switch-Verfahren bietet Ihnen eine kostengünstige Möglichkeit, das 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 im Vollduplex-Modus arbeiten 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 2 Link-Aggregation-Gruppen einzurichten.

## 12.5.2 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.

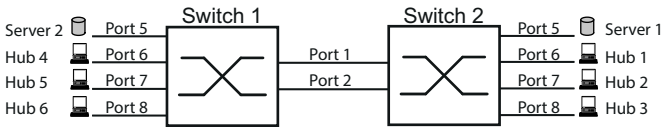



*Abb. 37: Link Aggregation Switch-zu-Switch-Netz*

Richten Sie Switch 1 and 2 über die grafische Benutzeroberfläche ein. 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 *Erstellen*.
- ☐ 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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` hinzufügen. |
| `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. |

# 12.6 Link-Backup

Link-Backup bietet einen redundanten Link für Datenpakete auf Schicht-2-Geräten. Wenn das Gerät einen Fehler auf dem primären Link erkannt hat, leitet das Gerät die Datenpakete 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 *Primär-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 Protocol (STP) auf den Link-Backup-Ports ausgeschaltet ist.

## 12.6.1 Beschreibung Fail-Back

Link-Backup ermöglicht Ihnen, eine Fail-Back-Option einzurichten. Wenn Sie die Funktion *Fail back* aktivieren und der *Primär-Port* in den Normalbetrieb zurückkehrt, blockiert das Gerät zunächst die Datenpakete am *Backup-Port* und vermittelt die Datenpakete dann an den *Primär-Port*. Dieser Prozess hilft zu vermeiden, dass das Gerät Loops im Netzwerk verursacht.

Wenn der *Primär-Port* zum Link-Up- und aktiven Zustand zurückkehrt, unterstützt das Gerät 2 Betriebsarten:
- Wenn Sie *Fail back* deaktivieren, bleibt der *Primär-Port* im Zustand `blocking`, bis der Backup-Link ausfällt.
- Wenn Sie *Fail back* aktivieren, und nachdem der *Fail-Back Verzögerung [s]* Timer abläuft, kehrt der *Primär-Port* in den Zustand `forwarding` zurück und der *Backup-Port* nimmt den Zustand „Down” an.

In den oben angeführten Fällen sendet der Port, der seinen Link dazu zwingt, Datenpakete zu vermitteln, zuerst ein *Topology Change*-Paket zum entfernten Gerät. Das *Topology Change*-Paket hilft dem entfernten Gerät dabei, die MAC-Adressen schnell wieder zu lernen.

### 12.6.2 Anwendungsbeispiel für die Funktion Link-Backup

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, vermittelt einer der Ports Datenpakete, der andere Port ist im Zustand *blocking*.

Der *Primär-Port* 2/3 auf Switch A ist der aktive Port und vermittelt Datenpakete zu Port 1 auf Switch B. Port 2/4 auf Switch A ist der *Backup-Port* und blockiert die Datenpakete.

Wenn Switch A den Port 2/3 aufgrund eines erkannten Fehlers deaktiviert, beginnt Port 2/4 auf Switch A damit, Datenpakete zu Port 2 auf Switch C zu vermitteln.

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 Port 2/4 zunächst die Datenpakete, dann beginnt Port 2/3, Datenpakete zu vermitteln.

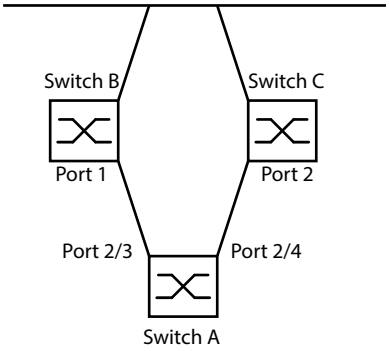



*Abb. 38: Link-Backup Beispiel-Netzwerk*

Die folgenden Tabellen enthalten Beispiele für Parameter, um Switch A einzurichten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Link-Backup*.
- ☐ Geben Sie ein neues Link-Backup-Paar in die Tabelle ein:
  - ☐ Klicken Sie die Schaltfläche .
    Der Dialog zeigt das Fenster *Erstellen*.
  - ☐ 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*.
- ☐ Schalten Sie die Funktion *Link-Backup* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.

| | |
|---|---|
| `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 hinzufügen, bei der Port `2/3` der *Primär-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 im 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
- Berichte
- Datenstrom auf einem Port überwachen (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 Traps festgelegt sind. Das Gerät ermöglicht Ihnen, die Trap-Ziel-Tabelle mit der Netz-Management-Station über SNMP einzurichten.

### 13.1.1 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 auf das Gerät übertragen 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.

### 13.1.2 SNMP-Trap-Einstellung

Das Gerät ermöglicht Ihnen, als Reaktion auf bestimmte Ereignisse einen SNMP-Trap zu senden. Richten Sie mindestens ein Trap-Ziel ein, 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 *Erstellen*.
- ☐ 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 berücksichtigt.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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* **(hardwareabhängig)**
- Dialog *Netzsicherheit > Port-Sicherheit*
- Dialog *Switching > L2-Redundanz > Link-Aggregation*
- Dialog *Diagnose > Statuskonfiguration > Gerätestatus*
- Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*
- Dialog *Diagnose > Statuskonfiguration > Signalkontakt*
- Dialog *Diagnose > Statuskonfiguration > MAC-Benachrichtigung*
- Dialog *Diagnose > System > IP-Adressen Konflikterkennung*
- Dialog *Diagnose > System > Selbsttest*
- Dialog *Diagnose > Ports > Port-Monitor*

### 13.1.3 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 einzurichten, 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 Sie das Gerät außerhalb der vom Benutzer festgelegten Schwellenwerte für die Temperatur betreiben
- Redundanzverlust (wenn das Gerät als *Ring-Manager* arbeitet)
- Unterbrechung der Link-Verbindung(en)
  Richten Sie für diese Funktion mindestens einen Port ein. In der Tabelle in der Registerkarte *Port*, Spalte *Verbindungsfehler melden* legen Sie fest, für welche Ports das Gerät eine Verbindungsunterbrechung an den Gerätestatus weitergibt. In der Voreinstellung ist die Verbindungsüberwachung inaktiv.
- Entfernen des externen Speichers (*ENVM*)
  Das Konfigurationsprofil im externen Speicher (*ENVM*) stimmt nicht mit den Einstellungen 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. 31: 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 den festgelegten oberen Schwellenwert überschreitet oder den festgelegten unteren Schwellenwert 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 den Geräteeinstellungen und dem im externen Speicher (*ENVM*) gespeicherten Konfigurationsprofil. |
| *Ring-Redundanz* | Aktivieren Sie diese Funktion, um das Vorhandensein der Ringredundanz zu überwachen. |
| *Netzteil 1*, *Netzteil 2* | 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*.
- ☐ Fügen Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* mindestens ein Trap-Ziel hinzu, das SNMP-Traps empfängt.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.
- ☐ Um die Temperatur zu überwachen, legen Sie im Rahmen *Systemdaten* die Schwellenwerte für die Temperatur fest.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 (*ENVM*) überwachen.<br>In folgenden Situationen wechselt der *Geräte-Status* auf *error*:<br>• Das Konfigurationsprofil existiert ausschließlich im Gerät.<br>• Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher (*ENVM*). |
| `device-status monitor envm-removal` | Aktiven externen Speicher (*ENVM*) 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` | Ringredundanz überwachen.<br>In folgenden Situationen wechselt der *Geräte-Status* auf *error*:<br>• Das Gerät arbeitet als Redundanz-Manager. Die Redundanzfunktion des Geräts verwendet die alternative Verbindung. Eine Redundanzreserve ist nicht länger vorhanden.<br>• Das Gerät als Ringteilnehmer hat einen Fehler in seinen Ringredundanz-Einstellungen erkannt. |
| `device-status monitor temperature` | Temperatur im Gerät überwachen. Wenn die Temperatur den festgelegten oberen Schwellenwert überschreitet oder den festgelegten unteren Schwellenwert unterschreitet, dann 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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. 32: 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 kürzer als 8* | Erstellen 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 1 über die serielle Schnittstelle möglich* | Das Gerät überwacht, ob der Start des System Monitors 1 über die serielle Verbindung während des Systemstarts möglich ist. |
| *Speichern des Konfigurationsprofils auf dem externen Speicher möglich* | Das Gerät überwacht die Möglichkeit, Einstellungen im externen nichtflüchtigen Speicher (*NVM*) zu speichern. |

*Tab. 32: 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. |
| *IEC 61850/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 generiertes 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .
- ☐ Fügen Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* mindestens ein Trap-Ziel hinzu, das SNMP-Traps empfängt.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `security-status monitor pwd-change` | Passwort für das lokal eingerichtete Benutzerkonto `admin` überwachen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie für das Benutzerkonto `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.<br>• *Großbuchstaben (min.)*<br>• *Kleinbuchstaben (min.)*<br>• *Ziffern (min.)*<br>• *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.<br>Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn mindestens eine der folgenden Bedingungen zutrifft:<br>• Die Funktion *SNMPv1* ist eingeschaltet.<br>• Die Funktion *SNMPv2* ist eingeschaltet.<br>• Die Verschlüsselung für SNMPv3 ist ausgeschaltet.<br>Die Verschlüsselung schalten Sie ein im Dialog *Gerätesicherheit > Benutzerverwaltung*, Feld *SNMP-Verschlüsselung*. |
| `security-status monitor sysmon-enabled` | Das Aktivieren der Funktion *System Monitor 1* im Gerät überwachen. |
| `security-status monitor extnvm-upd-enabled` | Das Aktivieren der Aktualisierung des externen nichtflüchtigen Speichers überwachen. |
| `security-status monitor iec61850-mms-enabled` | Funktion *IEC 61850/MMS* überwachen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *IEC 61850/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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 `1/1` 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` | Sicherheitsstatus und Einstellung zur Ermittlung des Sicherheitsstatus 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 Ihnen 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 Sie das Gerät außerhalb der vom Benutzer festgelegten Schwellenwerte für die Temperatur betreiben
- Ereignisse der Ringredundanz:
  Das Gerät arbeitet als Redundanz-Manager. Die Redundanzfunktion des Geräts verwendet die alternative Verbindung. Eine Redundanzreserve ist nicht länger vorhanden.
  Das Gerät als Ringteilnehmer hat einen Fehler in seinen Ringredundanz-Einstellungen erkannt.
  In der Voreinstellung ist die Ringredundanz-Überwachung inaktiv.
- Unterbrechung der Link-Verbindung(en)
  Richten Sie für diese Funktion mindestens einen Port ein. 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 (`ENVM`)
  Das Konfigurationsprofil im externen Speicher (`ENVM`) stimmt nicht mit den Einstellungen 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* in der Dropdown-Liste *Modus* den Eintrag `Manuelle Einstellung`.

- ☐ Öffnen Sie den Signalkontakt.
  Wählen Sie im Rahmen *Konfiguration* das Optionsfeld *offen*.
- ☐ Schließen Sie den Signalkontakt.
  Wählen Sie im Rahmen *Konfiguration* das Optionsfeld *geschlossen*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Fügen Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* mindestens ein Trap-Ziel hinzu, das SNMP-Traps empfängt.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Die Schwellenwerte 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 den festgelegten oberen Schwellenwert überschreitet oder den festgelegten unteren Schwellenwert unterschreitet. |
| `signal-contact 1 monitor ring-redundancy` | Ringredundanz überwachen.<br>In folgenden Situationen öffnet der Signalkontakt:<br>• Das Gerät arbeitet als Redundanz-Manager. Die Redundanzfunktion des Geräts verwendet die alternative Verbindung. Eine Redundanzreserve ist nicht länger vorhanden.<br>• Das Gerät als Ringteilnehmer hat einen Fehler in seinen Ringredundanz-Einstellungen erkannt. |
| `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 (*ENVM*) überwachen. Der Signalkontakt öffnet, wenn Sie den aktiven externen Speicher (*ENVM*) aus dem Gerät entfernen. |
| `signal-contact 1 monitor envm-not-in-sync` | Konfigurationsprofile im Gerät und im externen Speicher (*ENVM*) überwachen.<br>In folgenden Situationen öffnet der Signalkontakt:<br>• Das Konfigurationsprofil existiert ausschließlich im Gerät.<br>• Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher (*ENVM*). |
| `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. 33: 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 den festgelegten oberen Schwellenwert überschreitet oder den festgelegten unteren Schwellenwert 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 den Geräteeinstellungen und dem im externen Speicher (*ENVM*) gespeicherten Konfigurationsprofil. |
| *Ring-Redundanz* | Aktivieren Sie diese Funktion, um das Vorhandensein der Ringredundanz zu überwachen. |
| *Netzteil 1*, *Netzteil 2* | 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` | Die Einstellungen für den festgelegten Signalkontakt anzeigen. |

# 13.5 Portereignis-Zähler

Die Port-Statistiktabelle ermöglicht erfahrenen Netzadministratoren, mögliche Unterbrechungen im Netz zu finden.

Diese Tabelle zeigt die Inhalte verschiedener Ereigniszähler. Die Paketzähler summieren die Ereignisse aus Sende- und Empfangsrichtung. Im Dialog *Grundeinstellungen > Restart* können Sie die Ereigniszähler zurücksetzen.

*Tab. 34: Beispiele für die Angabe bekannter Schwächen*

| Zähler | Angabe bekannter möglicher Schwächen |
|---|---|
| Empfangene Fragmente | • Nicht funktionierender Controller des verbundenen Geräts<br>• Elektromagnetische Einkoppelung im Übertragungsmedium |
| CRC-Fehler | • Nicht funktionierender Controller des verbundenen Geräts<br>• Elektromagnetische Einkoppelung im Übertragungsmedium<br>• Nicht betriebsbereite Komponente im Netz |
| Kollisionen | • Nicht funktionierender Controller des verbundenen Geräts<br>• Netzausdehnung zu groß/Zeilen zu lang<br>• 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 > Restart* die Schaltfläche *Port-Statistiken leeren*.

## 13.5.1 Erkennen der Nichtübereinstimmung der Duplex-Modi

Wenn 2 direkt miteinander verbundene Ports unterschiedliche Duplex-Modi haben, treten möglicherweise Probleme auf. Diese möglichen Probleme sind schwierig zu erkennen. Das automatische Erkennen und Melden dieser Situation hat den Vorteil, dass nicht übereinstimmende Duplex-Modi erkannt werden, bevor mögliche 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 einem höheren bidirektionalen Datenstromniveau jedoch viele CRC-Fehler erkennt 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 Zähler von auf dem Port erkannten Fehlern abhängig 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:

- Duplex-Problem erkannt
  Nicht übereinstimmende Duplex-Modi.
- EMI
  Elektromagnetische Interferenz.
- Netzausdehnung
  Die Netzausdehnung ist zu groß bzw. sind zu viele Kaskadenhubs vorhanden.
- Kollisionen, *Late Collisions*
  Im Halbduplexmodus bedeuten Kollisionen Normalbetrieb.
  Im Vollduplex-Modus keine Erhöhung der Port-Zähler für Kollisionen oder *Late Collisions*.
- CRC-Fehler
  Das Gerät bewertet diese erkannten Fehler als nicht übereinstimmende Duplex-Modi im manuellen Vollduplex-Modus.

*Tab. 35: 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 | Mögliches 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 | Mögliches 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 | Mögliches Duplex-Problem, EMI |

# 13.6 Auto-Disable

Das Gerät kann einen Port aufgrund unterschiedlicher, vom Benutzer wählbarer Ereignisse ausschalten, zum Beispiel bei einem erkannten Fehler oder der Änderung einer Bedingung. Jedes dieser Ereignisse führt zur Abschaltung des Ports. Um den Port wieder in Betrieb zu nehmen, beseitigen Sie entweder die Ursache für die Abschaltung des Ports oder legen Sie einen Timer fest, der den Port automatisch wieder einschaltet.

Wenn das Gerät den Port ausschaltet, vermittelt es von und zu diesem Port keine Datenpakete mehr. Die Port-LED blinkt 3 Mal pro Periode grün und zeigt den Grund für das Ausschalten. Darüber hinaus generiert 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, generiert 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*)
- *Spanning Tree*
- *Port-Sicherheit*
- *Überlast-Erkennung* (Funktion *Port-Monitor*)
- *Link-Speed-/Duplex-Mode Erkennung* (Funktion *Port-Monitor*)

Im folgenden Beispiel richten Sie das Gerät so ein, dass es einen Port ausschaltet und anschließend automatisch wieder einschaltet, wenn es eine Überschreitung der im Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *CRC/Fragmente* festgelegten Schwellenwerte 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 Schwellenwerte mit Ihren Einstellungen für Port `1/1` übereinstimmen.
- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Global*.
- ☐ Schalten Sie die Funktion *Port-Monitor* ein.
  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 Schwellenwertüberschreitungen 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 richten die *Auto-Disable*-Funktion ein. 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* einrichten, 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, nach Ausschalten wegen erkannter Schwellenwertüberschreitungen den Port 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 Schwellenwertüberschreitungen 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 die Zeit abgelaufen ist. |

# 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 aktiv 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 Auto-Negotiation auf dem Port
- Einstellung für Medium-/Halb- und Vollduplex sowie für die Übertragungsrate des Ports
- 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. Diese Informationen ermöglichen der Netz-Management-Station, die Topologie des Netzes darzustellen.

Nicht-LLDP-fähige Geräte blockieren in der Regel die spezielle Multicast-LLDP-IEEE-MAC-Adresse, die zum Informationsaustausch verwendet wird. Nicht-LLDP-fähige 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 den 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.

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 MAC-Adresstabelle (Forwarding Database) enthält MAC-Adressen von Geräten, welche die Topologietabelle 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 DSCP (Differentiated Services Code Point)
- 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 Protokollelementen des Link Layer Discovery Protocol (LLDP) 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 sendet.

BPDU-Frames, die vom *Designated-Port* 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 Berichte

Im Folgenden werden die für Diagnosezwecke verfügbaren Berichte und Schaltflächen aufgeführt:

- System-Log-Datei
  Das Gerät protokolliert geräteinterne Ereignisse in der System-Log-Datei.
- 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 bleiben auch nach dem Ausschalten des Geräts 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 eingerichtete 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.

## 13.10.1 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.
- ☐ Schalten Sie die Funktion *Console-Logging* ein.
  Wählen Sie im Rahmen *Console-Logging* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

Wenn Sie die Protokollierung von SNMP-Anfragen aktivieren, protokolliert das Gerät die Anfragen im Syslog als Ereignisse. Die Funktion *Logge SNMP Get-Requests* protokolliert Benutzeranfragen nach Geräte-Konfigurationsinformationen. Die *Logge SNMP Set-Requests*-Funktion protokolliert Geräte-Einrichtungs-Ereignisse. 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 *Logge SNMP Get-Requests* ein.
  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 *Logge SNMP Set-Requests* ein.
  Wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld *An*.
- ☐ Wählen Sie den gewünschten Schweregrad für die Get- und Set-Anfragen.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 IEEE 1686 für intelligente elektronische Unterstationsgeräte zugrunde.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Bericht > Global*.
- ☐ Schalten Sie die Funktion *CLI-Logging* ein.
  Wählen Sie im Rahmen *CLI-Logging* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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`

Das Gerät benennt das ZIP-Archiv automatisch im Format `<IP-Adresse>_<Gerätename>.zip`.

Führen Sie die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche .
  Nach einiger Zeit können Sie das ZIP-Archiv herunterladen.
- ☐ Wählen Sie das Verzeichnis aus, in welchem Sie die Support-Information speichern.
- ☐ Klicken Sie die Schaltfläche *Ok*.

### 13.10.2 Syslog

Das Gerät ermöglicht Ihnen, 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 eine Tabellenzeile hinzuzufügen, klicken Sie die Schaltfläche  .
- ☐ Geben Sie in Spalte *IP-Adresse* die IP-Adresse des Syslog-Servers ein.
  Sie können eine gültige IPv4- oder IPv6-Adresse für den Syslog-Server festlegen.
- ☐ Legen Sie in Spalte *Ziel UDP-Port* den UDP-Port fest, auf dem der Syslog-Server die Log-Einträge erwartet.
- ☐ Legen Sie in Spalte *Min. Schweregrad* den Mindest-Schweregrad fest, den ein Ereignis benötigt, damit das Gerät einen Protokolleintrag an diesen Syslog-Server sendet.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Schalten Sie die Funktion *Syslog* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

Richten Sie im Rahmen *SNMP-Logging* die folgenden Einstellungen für SNMP-Lese- und Schreibanfragen ein:

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 *Logge SNMP Get-Requests* ein.
  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 *Logge SNMP Set-Requests* ein.
  Wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld *An*.
- ☐ Wählen Sie den gewünschten Schweregrad für die Get- und Set-Anfragen.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 Empfänger hinzufügen. Der Wert `3` legt den Schweregrad des Ereignisses fest, welches das Gerät protokolliert. Der Wert `3` bedeutet `error`. |
| `logging host add 2 addr 2001::1 severity 4` | Der Liste der Syslog-Server einen IPv6-Empfänger hinzufügen. Der Wert `4` bedeutet `warning`. |

```
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
2      2001::1        514    warning         systemlog   active
```

```
configure
```
In den Konfigurationsmodus wechseln.

```
logging snmp-requests get operation
```
Den Empfang von *SNMP Get Requests* protokollieren.

```
logging snmp-requests get severity 5
```
Der Wert `5` legt den Schweregrad des Ereignisses fest, welches das Gerät beim Empfang eines *SNMP Get Requests* protokolliert. Der Wert `5` bedeutet `notice`.

```
logging snmp-requests set operation
```
Den Empfang von *SNMP Set Requests* protokollieren.

```
logging snmp-requests set severity 5
```
Der Wert `5` legt den Schweregrad des Ereignisses fest, welches das Gerät beim Empfang eines *SNMP Set Requests* 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
```

### 13.10.3 System-Log

Das Gerät ermöglicht Ihnen, eine System-Log-Datei mit den Systemereignissen aufzurufen. In der Tabelle im Dialog *Diagnose > Bericht > System-Log* werden die protokollierten Ereignisse aufgeführt.

Sie haben die folgenden Möglichkeiten:
- Anzeigen und Aktualisieren der System-Log-Datei
- Nach Inhalten suchen
- Eine Kopie der System-Log-Datei herunterladen
- System-Log-Datei im Gerät leeren

Sie haben die Möglichkeit, auch protokollierte Ereignisse an einen oder mehrere Syslog-Server zu senden.

### Anzeigen und Aktualisieren der System-Log-Datei

Das Gerät protokolliert Ereignisse kontinuierlich in der System-Log-Datei. Die grafische Benutzeroberfläche aktualisiert die Anzeige der Ereignisse nicht automatisch. Wenn der Dialog bereits seit einiger Zeit geöffnet ist, aktualisieren Sie die Anzeige, um auch die zuletzt protokollierten Ereignisse anzuzeigen.

Führen Sie die folgenden Schritte aus:

- ☐ Aktualisieren Sie die Anzeige der System-Log-Datei in der grafischen Benutzeroberfläche. Klicken Sie dazu die Schaltfläche  .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `show logging buffered` | Die gespeicherten Protokolleinträge anzeigen. |

### Nach Inhalten suchen

Das Gerät protokolliert Ereignisse kontinuierlich in der System-Log-Datei. Nach einiger Zeit kann die Datei sehr viele Ereignisse enthalten.

Führen Sie die folgenden Schritte aus:

- ☐ Suchen Sie nach einem Schlüsselwort in der System-Log-Datei. Verwenden Sie dazu die Suchfunktion Ihres Webbrowsers.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `show logging buffered <filter>` | Die gespeicherten Protokolleinträge anzeigen. Sie können Schlüsselwörter für den Schweregrad, Ziffern oder Bereiche eingeben, die durch ein Komma getrennt sind. Beispiel: `emergency,alert-error,4,5-6` |

### Eine Kopie der System-Log-Datei herunterladen

Das Gerät protokolliert Ereignisse kontinuierlich in der System-Log-Datei. Nach einiger Zeit kann die Datei viele Ereignisse enthalten. In der grafischen Benutzeroberfläche können Sie eine Kopie der System-Log-Datei herunterladen, um die protokollierten Ereignisse auf Ihrem Computer zu analysieren. Mit dem Command Line Interface können Sie eine Kopie der System-Log-Datei im externen Speicher (*ENVM*) oder auf einem Remote-Server speichern.

Führen Sie die folgenden Schritte aus:

- ☐ Laden Sie eine Kopie der System-Log-Datei auf Ihren Computer herunter. Klicken Sie dazu die Schaltfläche  .
- ☐ Der Webbrowser speichert die Datei gemäß seinen Download-Einstellungen auf dem Computer. Wählen Sie gegebenenfalls den Speicherort für die Datei.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `copy eventlog buffered envm EXAMPLE` | Eine Kopie der System-Log-Datei unter dem Dateinamen `EXAMPLE` im externen Speicher (*ENVM*) speichern. |
| `copy eventlog buffered remote ftp://1.2.3.4/EXAMPLE` | Eine Kopie der System-Log-Datei unter dem Dateinamen `EXAMPLE` auf einem Remote-Server speichern. |

### System-Log-Datei im Gerät leeren

Das Gerät protokolliert Ereignisse kontinuierlich in der System-Log-Datei. Nach einiger Zeit kann die Datei viele Ereignisse enthalten. Wenn Sie an den protokollierten Ereignissen nicht länger interessiert sind, können Sie die System-Log-Datei im Gerät leeren.

Führen Sie die folgenden Schritte aus:

- ☐ Löschen Sie den Inhalt der System-Log-Datei. Klicken Sie dazu die Schaltfläche 🗑.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `clear logging buffered` | Die Log-Datei leeren. |

## 13.10.4 Audit Trail

Der Dialog *Diagnose > Bericht > Audit-Trail* enthält Systeminformationen sowie Änderungen an den Geräteeinstellungen, die über das Command Line Interface und SNMP an dem Gerät vorgenommen wurden. Bei Änderungen der Geräteeinstellungen 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 Aktualisierung der Geräte-Software
- Konfigurationsänderungen mittels HiDiscovery
- Automatische Konfiguration oder Aktualisierungen der Geräte-Software 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

# 13.11 Netzanalyse mit TCPDump

TCPDump ist ein UNIX-Hilfsprogramm für das Packet-Sniffing, das Netzadministratoren zum Aufzuspüren und Analysieren des Datenstroms in einem Netz verwenden. Das Aufspüren von Datenströmen dient unter anderem der Verifizierung der Konnektivität zwischen Hosts und der Analyse des Datenstroms, der das Netz durchquert.

TCPDump im 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“.

# 13.12 Überwachung des Datenstroms mit Port-Mirroring

Die Funktion *Port-Mirroring* ermöglicht Ihnen, die Datenpakete von physischen Quell-Ports zu einem physischen Ziel-Port zu kopieren. Port-Mirroring ist auch bekannt als Switched Port Analyzer (SPAN).

Mit einem am Ziel-Port angeschlossenen Analysator, zum Beispiel einer *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.

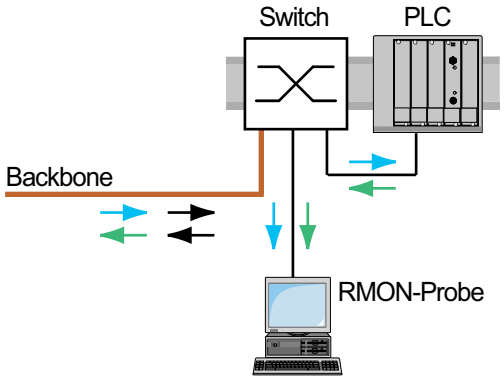



*Abb. 39: Anwendungsbeispiel für ein Port-Mirroring-Setup*

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.

### 13.12.1 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .

Um die Funktion *Port-Mirroring* zu deaktivieren und die Voreinstellungen wiederherzustellen, klicken Sie die Schaltfläche  .

# 13.13 Selbsttest

Das Gerät prüft beim Systemstart 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.

Richten Sie jede Kategorie so ein, dass sie eine Aktion auslöst, wenn das Gerät einen Integritätsverlust feststellt. 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 erkannter 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.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 die Option zum Starten des System Monitors 1 während des Systemstarts.
  - `markiert` (Voreinstellung)
    Während des Systemstarts zeigt das Startmenü den Eintrag System Monitor 1. Voraussetzung ist, dass die Management-Station über die serielle Verbindung mit dem Gerät verbunden ist.
    Um den System Monitor 1 tatsächlich zu starten, versetzen Sie das Gerät in den Recovery-Modus, siehe Abschnitt „Zugriff auf das Management des Geräts" auf Seite 37.
  - `unmarkiert`
    Während des Systemstarts zeigt das Startmenü keinen Eintrag System Monitor 1.
    Niemand kann den System Monitor 1 starten.
- Kontrollkästchen *Bei Fehler Default-Konfiguration laden*
  Aktiviert/deaktiviert das Laden der Standard-Gerätekonfiguration, falls dem Gerät beim Systemstart keine lesbare Konfiguration zur Verfügung steht.

Die folgenden Einstellungen sperren Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Systemstart 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` | Die Option zum Starten des System Monitors 1 aktivieren. Während des Systemstarts zeigt das Startmenü den Eintrag System Monitor 1. |
| `no selftest system-monitor` | Die Option zum Starten des System Monitors 1 deaktivieren. Während des Systemstarts zeigt das Startmenü keinen Eintrag System Monitor 1. |
| `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
```

# 13.14 Kupferkabeltest

Verwenden Sie diese Funktion, um ein Kupferkabel, das an einen Port angeschlossen ist, auf Kurzschluss oder Unterbrechungen zu prüfen. Der Test unterbricht den Datenstrom (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*
  Zeigt, dass das Kabel ordnungsgemäß funktioniert
- *offen*
  Zeigt, dass im Kabel eine Unterbrechung vorliegt
- *Kurzschluss*
  Zeigt, dass das Kabel einen Kurzschluss aufweist oder der Port inaktiv ist
- *unbekannt*
  Zeigt, dass das Kabel ungeprüft oder nicht angeschlossen ist

# 14 Erweiterte Funktionen des Geräts

## 14.1 DHCP-Server

Das Dynamic Host Configuration Protocol (DHCP) ermöglicht einem Server, den Geräten im Netz (Clients) die IP-Einstellungen zuzuweisen. Dadurch reduziert sich der Aufwand für die manuelle Einrichtung. Der DHCP-Server speichert und weist die verfügbaren IP-Adressen zu, sowie weitere Einstellungen, falls festgelegt.

Der Vorgang für die Zuweisung der IP-Einstellungen besteht aus 4 Phasen:
- *DISCOVER* gesendet vom DHCP-Client
- *OFFER* gesendet vom DHCP-Server
- *REQUEST* gesendet vom DHCP-Client
- *ACKNOWLEDGE* gesendet vom DHCP-Server

Der DHCP-Server im Gerät wartet auf dem UDP-Port 67 auf Anfragen und antwortet den Client-Geräten auf dem UDP-Port 68. Wenn das Gerät einen DHCP-Request empfängt, validiert es die zuzuweisende IP-Adresse, bevor es dem anfragenden Client-Gerät die IP-Adresse und andere IP-Einstellungen zuweist.

Das Gerät ermöglicht Ihnen, die Funktion *DHCP Server* global oder auf einzelnen physischen Ports zu aktivieren.

### 14.1.1 Einstellungen, welche der Server den Clients zuweist

Wenn das Gerät als DHCP-Server arbeitet, weist es den Client-Geräten die IP-Einstellungen anhand folgender Parameter zu:
- MAC-Adresse des Client-Geräts
- Physischer Port, an welchem das Client-Gerät angeschlossen ist
- VLAN, in welchem das Client-Gerät Mitglied ist

Das Gerät weist Client-Geräten die folgenden IP-Einstellungen zu:
- IP-Adresse
- Subnetzmaske
- Standard-Gateway, falls festgelegt
- Weitere Einstellungen für das Netz, falls festgelegt

### 14.1.2 Pools

Das Gerät speichert die IP-Einstellungen in zwei Arten von Pools.

- Statische Pools
  Um einem bestimmten Gerät stets dieselbe IP-Adresse zuzuweisen, speichert das Gerät die betreffenden IP-Einstellungen in einem Pool, dessen Adressbereich genau eine IP-Adresse umfasst.
  Statische Pools sind zum Beispiel dazu geeignet, einem Server, NAS oder Drucker eine feste IP-Adresse zuzuweisen.
- Dynamische Pools
  Um IP-Adressen aus einem bestimmten Adressbereich zuzuweisen, speichert das Gerät die betreffenden IP-Einstellungen in einem Pool, dessen Adressbereich mehrere IP-Adressen umfasst.
  Dynamische Pools sind zum Beispiel dazu geeignet, Client-Geräten, die zu einem bestimmten VLAN gehören, eine bestimmte IP-Adresse zuzuweisen.

#### Statischen Pool einrichten

Im folgenden Beispiel richten Sie das Gerät dahingehend ein, dass es einem bestimmten Client-Gerät, welches an einem bestimmten Port angeschlossen ist, die IP-Einstellungen aus einem bestimmten statischen Pool zuweist.

Der statische Pool ist anhand der folgenden Parameter einzurichten:

- MAC-Adresse des Client-Geräts: `ec:e5:55:d6:50:01`
- Physischer Port, an welchem das Client-Gerät am Server-Gerät angeschlossen ist: `1/1`
- IP-Adresse, die das Gerät dem Client-Gerät zuweisen soll: `192.168.23.42`
- Die zugewiesenen IP-Einstellungen sind 2 Tage lang gültig: `172800`

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DHCP > DHCP Server > Pool*.
- ☐ Fügen Sie eine Tabellenzeile hinzu. Klicken Sie dazu die Schaltfläche .
- ☐ Legen Sie für die Tabellenzeile die folgenden Einstellungen fest:
  - Spalte *IP-Bereich Start* = `192.168.23.42`
  - Spalte *Port* = `1/1`
  - Spalte *MAC-Adresse* = `ec:e5:55:d6:50:01`
  - Spalte *Lease-Time [s]* = `172800`
  - Spalte *Aktiv* = markiert
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .
- ☐ Öffnen Sie den Dialog *Erweitert > DHCP > DHCP Server > Global*.
- ☐ Vergewissern Sie sich, dass die DHCP-Funktion auf Port `1/1` aktiv ist.
  Falls noch nicht geschehen, markieren Sie für Port `1/1` das Kontrollkästchen in Spalte *DHCP-Server aktiv*.
- ☐ Aktivieren Sie den DHCP-Server global.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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` | Einen statischen Pool mit Index `1` mit der IP-Adresse `192.168.23.42` hinzufügen. |
| `dhcp-server pool modify 1 mode interface 1/1` | Den statischen Pool mit Index `1` dem physischen Port `1/1` zuweisen. |
| `dhcp-server pool modify 1 mode mac EC:E5:55:D6:50:01` | Den statischen Pool mit Index `1` einem Client-Gerät mit MAC-Adresse `EC:E5:55:D6:50:01` zuweisen. |
| `dhcp-server pool modify 1 leasetime 172800` | Die Lease Time für den statischen Pool mit Index `1` festlegen. |
| `dhcp-server pool mode 1 enable` | Den statischen Pool mit Index `1` einschalten. |
| `dhcp-server operation` | DHCP-Server global aktivieren. |
| `interface 1/1` | In den Interface-Konfigurationsmodus von Interface `1/1` wechseln. |
| `dhcp-server operation` | Die DHCP-Server-Funktion auf diesem Port aktivieren. |

### Dynamischen Pool einrichten

Im folgenden Beispiel richten Sie das Gerät dahingehend ein, dass es Client-Geräten, die an einen bestimmten Port angeschlossen sind, eine IP-Adresse aus einem bestimmten Adressbereich zuweist.

Der dynamische Pool ist anhand der folgenden Parameter einzurichten:
- Die MAC-Adresse des Client-Gerätes oder weitere Informationen aus der DHCP-Anfrage sind nicht auszuwerten.
- Physischer Port, an welchem die Client-Geräte am Server-Gerät angeschlossen sind: `1/2`
- Adressbereich, aus welchem das Gerät eine IP-Adresse an die Client-Geräte zuweist: `192.168.23.92..192.168.23.142`
- Die zugewiesenen IP-Einstellungen sind 2 Tage lang gültig: `172800`

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DHCP > DHCP Server > Pool*.
- ☐ Fügen Sie eine Tabellenzeile hinzu. Klicken Sie dazu die Schaltfläche .
- ☐ Legen Sie für die Tabellenzeile die folgenden Einstellungen fest:
  - Spalte *IP-Bereich Start* = `192.168.23.92`
  - Spalte *IP-Bereich Ende* = `192.168.23.142`
  - Spalte *Port* = `1/2`
  - Spalte *Lease-Time [s]* = `172800`
  - Spalte *Aktiv* = `Marked`
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .
- ☐ Öffnen Sie den Dialog *Erweitert > DHCP > DHCP Server > Global*.

- ☐ Vergewissern Sie sich, dass die DHCP-Funktion auf Port 1/2 aktiv ist.
  Falls noch nicht geschehen, markieren Sie für Port 1/2 das Kontrollkästchen in Spalte *DHCP-Server aktiv*.
- ☐ Aktivieren Sie den DHCP-Server global.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche .

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `dhcp-server pool add 2 dynamic 192.168.23.92 192.168.23.142` | Einen dynamischen Pool mit Index 2 mit einem Bereich von 192.168.23.92 bis 192.168.23.142 hinzufügen. |
| `dhcp-server pool modify 2 mode interface 1/2` | Den statischen Pool mit Index 2 dem physischen Port 1/2 zuweisen. |
| `dhcp-server pool modify 2 leasetime 172800` | Die Lease Time für den dynamischen Pool mit Index 2 festlegen. |
| `dhcp-server pool mode 2 enable` | Den dynamischen Pool mit Index 2 einschalten. |
| `dhcp-server operation` | DHCP-Server global aktivieren. |
| `interface 1/2` | In den Interface-Konfigurationsmodus von Interface 1/2 wechseln. |
| `dhcp-server operation` | Die DHCP-Server-Funktion auf diesem Port aktivieren. |

### 14.1.3 Eine Preboot-eXecution-Environment (PXE) einrichten

Das Gerät ermöglicht Ihnen, die Boot-Parameter für PXE-konforme Clients festzulegen, damit diese ein Bootloader-Image von einem TFTP-Server herunterladen und starten können. Mögliche Anwendungen sind das Starten einer Installationsumgebung, eines Rettungssystems oder eines Live-Systems über das Netz. Ein typischer Anwendungsfall ist ein Infotainment-Gerät, das ein über das Netz bereitgestelltes Betriebssystem startet.

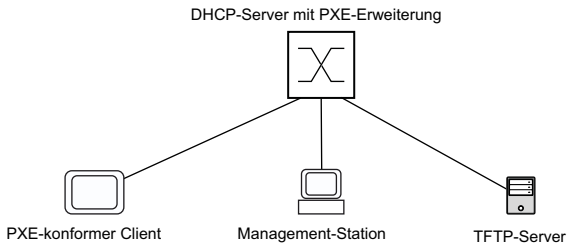



*Abb. 40: Einfacher Aufbau eines Preboot eXecution Environment (PXE)-Setups*

Um die PXE-Boot-Erweiterung für einen bestimmten Pool zu aktivieren, fügen Sie die folgenden Werte zu den Pool-Einstellungen hinzu:

- *Vendor Identifier*
- *Client System Architecture*
- URL zu einer Bootloader-Image-Datei auf einem TFTP-Server

Das Gerät erwartet die Informationen für *Vendor Identifier* und *Client System Architecture* in zusammengefasster Form als *Class Identifier* im DHCP-Optionsfeld 60. Wenn ein PXE-konformes Client-Gerät eine *DHCP Discover*-Nachricht mit einem passenden *Class Identifier* im DHCP-Optionsfeld 60 als Broadcast sendet, antwortet das Gerät mit den im betreffenden Pool festgelegten Einstellungen.

Ein PXE-konformes Client-Gerät benötigt ein Bootloader-Image, das zu seiner Hardware-Architektur passt. Berücksichtigen Sie bei der Planung, dass Sie mindestens einen Pool für jede erforderliche Hardware-Architektur benötigen.

**Anmerkung:**
Das Gerät prüft nicht die Integrität, Authentizität und Verfügbarkeit der TFTP-Server und der Bootloader-Image-Dateien. Verwenden Sie die PXE-Boot-Erweiterung ausschließlich dann, wenn Sie dem Übertragungsnetz vertrauen. Andernfalls können unerwünschtes Verhalten und Sicherheitsrisiken die Folge sein.

Im folgenden Beispiel möchte der Administrator des Netzes, dass Sie die PXE-Boot-Erweiterungsparameter für einen vorhandenen *DHCP-Server Pool*-Eintrag festlegen.

| | | |
|---|---|---|
| *Class Identifier* im DHCP-Optionsfeld 60 | *Vendor Identifier* | `vendor1` |
| | *Client System Architecture* | *`efi-x86-64`* |
| Bootloader-Image-Datei auf dem TFTP-Server | | `tftp://192.168.1.5/boot-efi-x86-64.img` |

Zum Ändern eines vorhandenen *DHCP-Server Pool*-Eintrags ist es erforderlich, den Pool zunächst zu deaktivieren. Informationen zum Einrichten eines DHCP-Server-Pools finden Sie in Abschnitt „Statischen Pool einrichten” auf Seite 260 oder „Dynamischen Pool einrichten” auf Seite 261. Nach dem Ändern des *DHCP-Server Pool*-Eintrags aktivieren Sie den Pool wieder.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DHCP > DHCP Server > Pool*.
- ☐ Deaktivieren Sie den *DHCP-Server Pool*-Eintrag. Heben Sie dazu die Markierung des Kontrollkästchens in Spalte *Aktiv* auf.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Geben Sie in Spalte*Vendor-ID* die Zeichenfolge `vendor1` ein.
- ☐ Wählen Sie in Spalte *Client-Architektur* den Eintrag *`efi-x86-64`* in der Dropdown-Liste.
- ☐ Geben Sie in Spalte *Konfigurations-URL* den URL ein: `tftp://192.168.1.5:/boot-efi-x86-64.img`.
- ☐ Aktivieren Sie den *DHCP-Server Pool*-Eintrag wieder. Markieren Sie dazu das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `dhcp-server pool mode 1 disable` | Pool `1` deaktivieren. |
| `dhcp-server pool modify 1 mode classid vendorid vendor1` | Die PXE-Boot-Erweiterung für Pool `1` einschalten und die Zeichenfolge `vendor1` als *Vendor Identifier* zuweisen. |
| `dhcp-server pool modify 1 mode classid architecture efi-x86-64` | Den Wert *`efi-x86-64`* als *Client System Architecture* festlegen. |

```
dhcp-server pool modify 1 option configpath
tftp://192.168.1.5:/boot-efi-x86-64.img
```

Den URL `tftp://192.168.1.5/boot-efi-x86-64.img` zur Bootloader-Image-Datei auf einem TFTP-Server festlegen.

```
dhcp-server pool mode 1 enable
```

Pool `1` wieder aktivieren.

```
show dhcp-server pool 1
```

Die Einstellungen zeigen, die für Pool `1` festgelegt sind.

```
DHCP Server Pool
----------------
Index.........................1
...
PXE Client Vendor ID............vendor1
PXE Client Architecture.........efi-x86-64
Configuration URL.............. tftp://192.168.1.5:/boot-efi-x86-64.img
...
```

# 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-Interfaces sowohl in den Client- als auch in den Server-Subnetzen besitzt und die Datenpakete 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.

Das DHCPv6-Protokoll verwendet einen *Relay-Agenten*, um *Relay-Agent*-Optionen zu DHCPv6-Paketen hinzuzufügen, die zwischen einem Client und einem DHCPv6-Server ausgetauscht werden. Der Lightweight-DHCPv6-Relay-Agent (LDRA) wird im RFC 6221 beschrieben.

Der LDRA verarbeitet 2 Arten von Nachrichten:
- Die erste Art von Nachrichten ist die *Relay-Forward*-Nachricht, die eindeutige Informationen über den Client enthält.
- Die zweite Art von Nachrichten ist die *Relay-Reply*-Nachricht, die der DHCPv6-Server an den *Relay-Agenten* sendet. Der *Relay-Agent* überprüft, ob die Nachricht die Informationen der ursprünglichen *Relay-Forward*-Nachricht enthält. Wenn die Nachricht gültig ist, sendet er das Paket an den Client.

Die *Relay-Forward*-Nachricht enthält *Interface-ID*-Informationen, auch *Option 18* genannt. Diese Option liefert Informationen zur Identifikation des Interface, über das die Client-Anfrage gesendet wurde. Das Gerät verwirft DHCPv6-Pakete, die keine *Option 18*-Informationen enthalten.

## 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 und DHCPv6-Pakete mit *Option 18*-Information an diejenigen Ports weiter, für die in Spalte *Aktiv* 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 und DHCPv6-Pakete mit *Option 18*-Information.

Eine Beispielkonfiguration für die DHCPv4-L2-Relay-Funktion ist unten abgebildet. Die Konfigurationsschritte für die DHCPv6-L2-Relay-Funktion sind ähnlich mit Ausnahme der *Circuit-ID*- und *Remote-ID*-Einträge, die ausschließlich für *Option 82* festgelegt werden können.

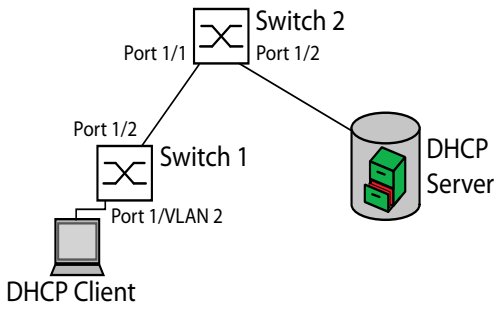



*Abb. 41: Beispiel: DHCP-Schicht-2-Netz*

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.
- ☐ Schalten Sie die Funktion *DHCP-L2-Relay* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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*.
- ☐ Schalten Sie die Funktion *DHCP-L2-Relay* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 VLAN 2 ein und fügen Sie Port 1/1 zu VLAN 2 hinzu.

| | |
|---|---|
| `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* im 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* im Gerät einschalten. |

# 14.3 Funktion GARP

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

Wird ein Attribut für einen Teilnehmer gemäß Funktion *GARP* registriert oder wieder ausgetragen, 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.

## 14.3.1 GMRP konfigurieren

Das GARP Multicast Registration Protocol (GMRP) ist ein Generic Attribute Registration Protocol (GARP), das einen Mechanismus für die dynamische Registrierung von Gruppenmitgliedschaften durch 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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. |

### 14.3.2 GVRP konfigurieren

Verwenden Sie die Funktion *GVRP*, um dem Gerät das Austauschen von VLAN-Konfigurationsinformationen mit anderen *GVRP*-fähigen Geräten zu ermöglichen. Auf diese Weise reduziert das Gerät unnötigen Verkehr von Broadcast- und unbekannten Unicast-Datenpaketen. Außerdem richtet die Funktion *GVRP* dynamisch VLANs auf Geräten ein, die über 802.1Q-Trunk-Ports verbunden sind.

Das folgende Beispiel beschreibt die Konfiguration der Funktion *GVRP*. Das Gerät ermöglicht Ihnen, VLAN-Konfigurationsinformationen mit anderen *GVRP*-fähigen Geräten auszutauschen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > GARP > GVRP*.
- ☐ Um VLAN-Konfigurationsinformationen mit anderen *GVRP*-fähigen Geräten auszutauschen, markieren Sie das Kontrollkästchen in Spalte *GVRP aktiv* für den Port.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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. |

# 14.4 MRP-IEEE

Die Erweiterung IEEE 802.1ak der Norm IEEE 802 1Q führte das Multiple-Registration-Protokoll (MRP-IEEE) als Ersatz für das Generic Attribute Registration Protocol (GARP) ein. Zudem änderte und ersetzte der IEEE-Normungsausschuss die *GARP*-Anwendungen, das GARP Multicast Registration Protocol (GMRP) und das GARP VLAN Registration Protocol (GVRP) mit dem Multiple MAC Registration Protocol (MMRP) und dem Multiple VLAN Registration Protocol (MVRP).

Um die Vermittlung der Datenpakete auf die erforderlichen Bereiche eines Netzes zu begrenzen, verteilen die MRP-IEEE-Anwendungen Attribut-Werte an Geräte mit eingeschaltetem MRP-IEEE innerhalb eines LANs. Die MRP-IEEE-Anwendungen registrieren und deregistrieren Multicast-Gruppenmitgliedschaften und VLAN-Kennungen.

**Anmerkung:**
Das Multiple Registration Protocol (MRP-IEEE) erfordert ein Loop-freies Netz. Um Loops im Netz zu vermeiden, verwenden Sie ein Netzprotokoll wie das Media Redundancy Protocol (MRP), Spanning Tree Protocol (STP) oder Rapid Spanning Tree Protocol (RSTP) mit MRP-IEEE.

## 14.4.1 MRP-IEEE-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 generiert MRP-IEEE-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-IEEE-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-Datenpakete entsteht.

### 14.4.2 MRP-IEEE-Timer

Die Timer-Voreinstellungen helfen, unnötige Attribut-Anmeldungen und -rücknahmen zu vermeiden. Die Timer-Einstellungen ermöglichen den Teilnehmern, MRP-IEEE-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 legen Sie – auch im Fall einer verlorenen Nachricht – für den *Leave*-Timer den Wert ≥ (2x JoinTime) + 60 in 1/100 s fest.
- Um das Aufkommen an *Rejoin*-Datenpaketen zu minimieren, welche das Gerät nach einem *LeaveAll*-Ereignis generiert, legen Sie den Wert für den *LeaveAll*-Timer größer als den Wert des *Leave*-Timers fest.

Die folgende Liste enthält verschiedene vom Gerät übertragene MRP-IEEE-Ereignisse.
- *Join*
  Steuert das Intervall für die Übertragung der nächsten *Join*-Nachricht.
- *Leave*
  Steuert den Zeitraum, den ein Switch vor dem Wechsel in den Rücknahme-Zustand im *Leave*-Zustand bleibt.
- *LeaveAll*
  Steuert die Frequenz, mit welcher der Switch *LeaveAll*-Nachrichten generiert.

Der Periodic-Timer löst nach Ablauf eine MRP-IEEE-Nachricht mit einem Join-Request aus, die der Switch an LAN-Teilnehmer sendet. Mit dieser Nachricht vermeiden Switches unnötige Rücknahmen.

### 14.4.3 MMRP

Wenn ein Gerät Broadcast-, Multicast- oder unbekannte Datenpakete auf einem Port empfängt, flutet das Gerät die Datenpakete an die anderen Ports. Dieser Vorgang beansprucht unnötig Bandbreite im LAN.

Das Multiple MAC Registration Protocol (MMRP) ermöglicht Ihnen, das Fluten von Datenpaketen 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-IEEE-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-Adress-Registration-Einträge beschränken so die Pakete auf die erforderlichen Segmente eines Loop-freien LANs.

Um Registrierungs- und Deregistrierungsstatus aufrecht zu erhalten und Datenpakete zu empfangen, erklärt ein Port periodisch sein Interesse. Jedes Gerät in einem LAN mit eingeschalteter Funktion *MMRP* führt eine Filterdatenbank und vermittelt die Datenpakete mit den Gruppen-MAC-Adressen an die aufgeführten Teilnehmer.

### MMRP einrichten

In diesem Beispiel erwartet Host A für die Gruppe G1 bestimmte Datenpakete. 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 Datenpaketen 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.

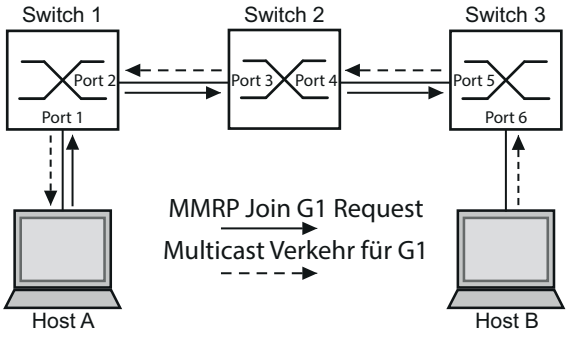



*Abb. 42: MMRP-Netz für MAC-Adressen-Registrierung*

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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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. |

### 14.4.4 MVRP

Das Multiple VLAN Registration Protocol (MVRP) ist eine MRP-IEEE-Anwendung, welche 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 die Informationen Auskunft, über welche Ports der Switch die Datenpakete 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 Zustand *discarding*.

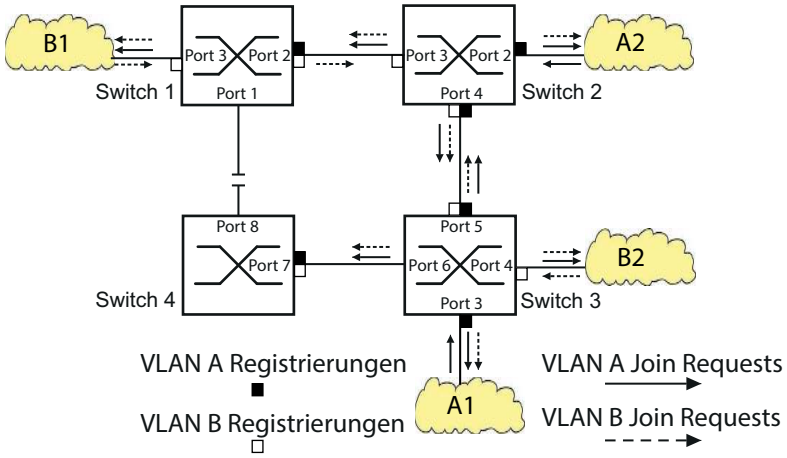



*Abb. 43: MVRP-Beispiel-Netz für VLAN-Registrierung*

Im MVRP-Beispiel-Netz senden die LANs zunächst eine Join-Anfrage an die Switches. Der Switch trägt die VLAN-Registrierung in die MAC-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 MAC-Adresstabelle (Forwarding Database) des empfangenden 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*.
- ☐ Schalten Sie die Funktion *MVRP* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 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 1990er-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.

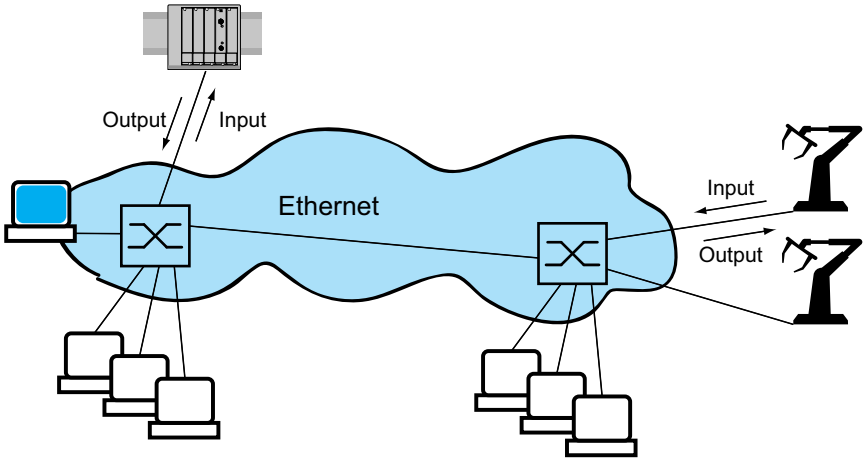



*Abb. 44: Beispiel für die Kommunikation.*

# 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 im 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 einzurichten.

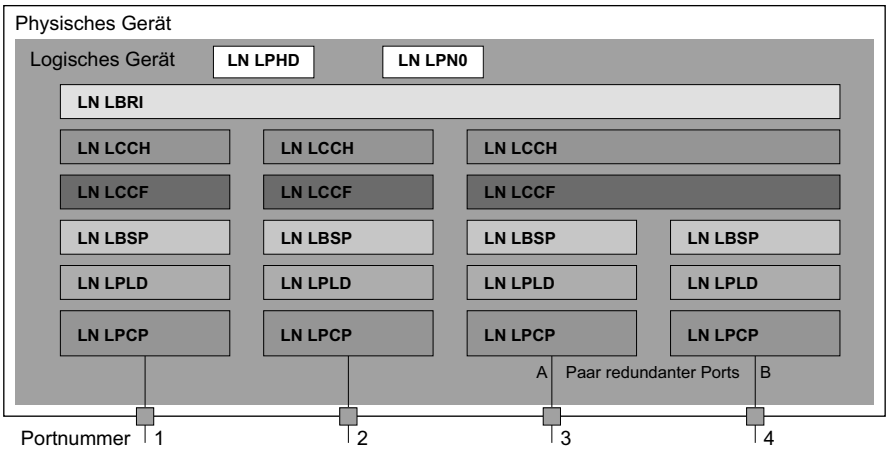



*Abb. 45: Bridge-Modell nach Technical Report IEC 61850 90-4*

*Tab. 36: Klassen des Bridge-Modells nach TR IEC 61850 90-4*

| Klasse | Beschreibung |
|---|---|
| LN LLN0 | Logischer Knoten Zero des IED Bridge:<br>Definiert die logischen Eigenschaften des Geräts. |
| LN LPHD | Logischer Knoten Physical Device des IED Bridge:<br>Definiert die physischen Eigenschaften des Geräts. |
| LN LBRI | Logischer Knoten Bridge:<br>Bildet generelle Einstellungen der Bridge-Funktionen des Geräts ab. |
| LN LCCH | Logischer Knoten Communication Channel:<br>Definiert den logischen Communication Channel, der aus einem oder mehreren physischen Ports besteht. |

*Tab. 36: Klassen des Bridge-Modells nach TR IEC 61850 90-4 (Forts.)*

| Klasse | Beschreibung |
|---|---|
| LN LCCF | Logischer Knoten Channel Communication Filtering:<br>Definiert die VLAN- und Multicast-Einstellungen für den übergeordneten Communication Channel. |
| LN LBSP | Logischer Knoten Port Spanning Tree Protocol:<br>Definiert die Spanning-Tree-Zustände und -Einstellungen für den jeweiligen physischen Port. |
| LN LPLD | Logischer Knoten Port Layer Discovery:<br>Definiert die LLDP-Zustände und -Einstellungen für den jeweiligen physischen Port. |
| LN LPCP | Logischer Knoten Physical Communication Port:<br>Repräsentiert den jeweiligen physischen Port. |

## 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 > IEC 61850/MMS*.
- ☐ Starten Sie den MMS-Server.

  Wählen Sie das Optionsfeld *An* im Rahmen *Funktion* und klicken Sie 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.

IEC 61850/MMS bietet keine Authentifizierungsmechanismen. Wenn der Schreibzugriff für IEC 61850/MMS eingeschaltet ist, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Geräts zu ändern. Dies kann zu fehlerhaften Einstellungen im Gerät führen und möglicherweise Unterbrechungen im Netz zur Folge haben.

**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.

**Das Nicht-Beachten 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 einzurichten.

☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > IEC 61850/MMS*.

☐ Um die ICD-Datei auf Ihren PC zu laden, klicken Sie die Schaltfläche ⬇.

### Gerät überwachen

Der im Gerät integrierte IEC 61850/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. 37: 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 Schwellenwerte für die Temperatur 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 Schwellenwerte für die Temperatur 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. 37: 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 Funktion 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 im 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.

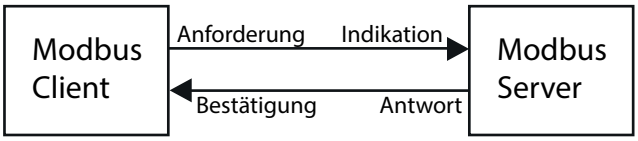



*Abb. 46: Modbus TCP/IP Client/Server-Modus*

Um Daten zwischen dem Client und dem Server auszutauschen, verwendet das Client/Server-Modell 4 Nachrichtentypen:

- Modbus TCP/IP-Anfrage; der Client generiert 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 Mbit/s
  - 3 = Fiber - 100 Mbit/s
  - 4 = Giga - 10/100/1000 Mbit/s (triple speed)
  - 5 = Giga - Copper 1000 Mbit/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 Adressen in den folgenden Tabellen ermöglichen dem Client, Port-Zähler zurückzusetzen und spezifische Informationen aus den Geräteregistern abzurufen.

*Tab. 38: System/Global Information*

| Address | Qty | Description | Min | Max | Step | Unit | Format |
|---|---|---|---|---|---|---|---|
| 0000 | 128 | System Name | - | - | - | - | String |
| 0080 | 128 | System Contact | - | - | - | - | String |
| 0100 | 128 | System Location | - | - | - | - | String |
| 0180 | 128 | Software Version | - | - | - | - | String |
| 0200 | 32 | OrderCode | - | - | - | - | String |
| 0220 | 16 | Serial Number | - | - | - | - | String |
| 0230 | 1 | IP Address[0] | 0 | 254 | 1 | - | F1 |
| 0231 | 1 | IP Address[1] | 0 | 254 | 1 | - | F1 |
| 0232 | 1 | IP Address[2] | 0 | 254 | 1 | - | F1 |
| 0233 | 1 | IP Address[3] | 0 | 254 | 1 | - | F1 |
| 0234 | 1 | NetMask[0] | 0 | 255 | 1 | - | F1 |
| 0235 | 1 | NetMask[1] | 0 | 255 | 1 | - | F1 |
| 0236 | 1 | NetMask[2] | 0 | 255 | 1 | - | F1 |
| 0237 | 1 | NetMask[3] | 0 | 255 | 1 | - | F1 |
| 0238 | 1 | GateWay[0] | 0 | 254 | 1 | - | F1 |
| 0239 | 1 | GateWay[1] | 0 | 254 | 1 | - | F1 |
| 023A | 1 | GateWay[2] | 0 | 254 | 1 | - | F1 |
| 023B | 1 | GateWay[3] | 0 | 254 | 1 | - | F1 |
| 023C | 3 | MacAddress | - | - | - | - | String |
| 023F | 1 | PowerAlarm1 | 0 | 1 | 1 | - | F2 |
| 0240 | 1 | PowerAlarm2 | 0 | 1 | 1 | - | F2 |
| 0241 | 1 | StpState | 0 | 1 | 1 | - | F1 |
| 0242 | 2 | Number of Ports | 1 | 64 | 1 | - | F1 |
| 0244 | 1 | Reset Counter (all Counter) | 0 | 1 | 1 | - | F1 |
| 0245 | 4 | Port Present Map | - | - | - | - | Bitmap |
| 0249 | 4 | Port Link Map | - | - | - | - | Bitmap |
| 024D | 4 | Port Stp State Map | - | - | - | - | Bitmap |
| 0251 | 4 | Port Activity Map | - | - | - | - | Bitmap |

*Tab. 39: Port-Informationen*

| Address | Qty | Description | Min | Max | Step | Unit | 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 |

*Tab. 40: Port-Statistik*

| Address | Qty | Description | Min | Max | Step | Unit | Format |
|---|---|---|---|---|---|---|---|
| 0800 | 2 | Port1 - Number of bytes received | 0 | 4294967295 ($2^{32}$-1) | 1 | - | F9 |
| 0802 | 2 | Port1 - Number of bytes sent | 0 | 4294967295 | 1 | - | F9 |
| 0804 | 2 | Port1 - Number of frames received | 0 | 4294967295 | 1 | - | F9 |
| 0806 | 2 | Port1 - Number of frames sent | 0 | 4294967295 | 1 | - | F9 |
| 0808 | 2 | Port1 - Total bytes received | 0 | 4294967295 | 1 | - | F9 |
| 080A | 2 | Port1 - Total frames received | 0 | 4294967295 | 1 | - | F9 |
| 080C | 2 | Port1 - Number of broadcast frames received | 0 | 4294967295 | 1 | - | F9 |
| 080E | 2 | Port1 - Number of multicast frames received | 0 | 4294967295 | 1 | - | F9 |
| 0810 | 2 | Port1 - Number of frames with CRC error | 0 | 4294967295 | 1 | - | F9 |
| 0812 | 2 | Port1 - Number of oversized frames received | 0 | 4294967295 | 1 | - | F9 |
| 0814 | 2 | Port1 - Number of bad fragments rcvd(<64 bytes) | 0 | 4294967295 | 1 | - | F9 |
| 0816 | 2 | Port1 - Number of jabber frames received | 0 | 4294967295 | 1 | - | F9 |
| 0818 | 2 | Port1 - Number of collisions occurred | 0 | 4294967295 | 1 | - | F9 |
| 081A | 2 | Port1 - Number of late collisions occurred | 0 | 4294967295 | 1 | - | F9 |
| 081C | 2 | Port1 - Number of 64-byte frames rcvd/ sent | 0 | 4294967295 | 1 | - | F9 |
| 081E | 2 | Port1 - Number of 65-127 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 0820 | 2 | Port1 - Number of 128-255 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |

*Tab. 40: Port-Statistik (Forts.)*

| Address | Qty | Description | Min | Max | Step | Unit | Format |
|---|---|---|---|---|---|---|---|
| 0822 | 2 | Port1 - Number of 256-511 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 0824 | 2 | Port1 - Number of 512-1023 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 0826 | 2 | Port1 - Number of 1023-MAX byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 0828 | 2 | Port1 - Number of Mac Error Packets | 0 | 4294967295 | 1 | - | F9 |
| 082A | 2 | Port1 - Number of dropped received packets | 0 | 4294967295 | 1 | - | F9 |
| 082C | 2 | Port1 - Number of multicast frames sent | 0 | 4294967295 | 1 | - | F9 |
| 082E | 2 | Port1 - Number of broadcast frames sent | 0 | 4294967295 | 1 | - | F9 |
| 0830 | 2 | Port1 - Number of <64 byte fragments w/ good CRC | 0 | 4294967295 | 1 | - | F9 |
| 0832 | 2 | Port2 - Number of bytes received | 0 | 4294967295 | 1 | - | F9 |
| 0834 | 2 | Port2 - Number of bytes sent | 0 | 4294967295 | 1 | - | F9 |
| 0836 | 2 | Port2 - Number of frames received | 0 | 4294967295 | 1 | - | F9 |
| 0838 | 2 | Port2 - Number of frames sent | 0 | 4294967295 | 1 | - | F9 |
| 083A | 2 | Port2 - Total bytes received | 0 | 4294967295 | 1 | - | F9 |
| 083C | 2 | Port2 - Total frames received | 0 | 4294967295 | 1 | - | F9 |
| 083E | 2 | Port2 - Number of broadcast frames received | 0 | 4294967295 | 1 | - | F9 |
| 0840 | 2 | Port2 - Number of multicast frames received | 0 | 4294967295 | 1 | - | F9 |
| 0842 | 2 | Port2 - Number of frames with CRC error | 0 | 4294967295 | 1 | - | F9 |
| 0844 | 2 | Port2 - Number of oversized frames received | 0 | 4294967295 | 1 | - | F9 |
| 0846 | 2 | Port2 - Number of bad fragments rcvd(<64 bytes) | 0 | 4294967295 | 1 | - | F9 |
| 0848 | 2 | Port2 - Number of jabber frames received | 0 | 4294967295 | 1 | - | F9 |
| 084A | 2 | Port2 - Number of collisions occurred | 0 | 4294967295 | 1 | - | F9 |
| 084C | 2 | Port2 - Number of late collisions occurred | 0 | 4294967295 | 1 | - | F9 |
| 084E | 2 | Port2 - Number of 64-byte frames rcvd/ sent | 0 | 4294967295 | 1 | - | F9 |
| 0850 | 2 | Port2 - Number of 65-127 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 0852 | 2 | Port2 - Number of 128-255 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 0854 | 2 | Port2 - Number of 256-511 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 0856 | 2 | Port2 - Number of 512-1023 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 0858 | 2 | Port2 - Number of 1023-MAX byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 085A | 2 | Port2 - Number of Mac Error Packets | 0 | 4294967295 | 1 | - | F9 |
| 085C | 2 | Port2 - Number of dropped received packets | 0 | 4294967295 | 1 | - | F9 |
| 085E | 2 | Port2 - Number of multicast frames sent | 0 | 4294967295 | 1 | - | F9 |
| 0860 | 2 | Port2 - Number of broadcast frames sent | 0 | 4294967295 | 1 | - | F9 |
| 0862 | 2 | Port2 - Number of <64 byte fragments w/ good CRC | 0 | 4294967295 | 1 | - | F9 |
| | | ... | | | | | |
| 144E | 2 | Port64 - Number of bytes received | 0 | 4294967295 | 1 | - | F9 |

*Tab. 40: Port-Statistik (Forts.)*

| Address | Qty | Description | Min | Max | Step | Unit | Format |
|---|---|---|---|---|---|---|---|
| 1450 | 2 | Port64 - Number of bytes sent | 0 | 4294967295 | 1 | - | F9 |
| 1452 | 2 | Port64 - Number of frames received | 0 | 4294967295 | 1 | - | F9 |
| 1454 | 2 | Port64 - Number of frames sent | 0 | 4294967295 | 1 | - | F9 |
| 1456 | 2 | Port64 - Total bytes received | 0 | 4294967295 | 1 | - | F9 |
| 1458 | 2 | Port64 - Total frames received | 0 | 4294967295 | 1 | - | F9 |
| 145A | 2 | Port64 - Number of broadcast frames received | 0 | 4294967295 | 1 | - | F9 |
| 145C | 2 | Port64 - Number of multicast frames received | 0 | 4294967295 | 1 | - | F9 |
| 145E | 2 | Port64 - Number of frames with CRC error | 0 | 4294967295 | 1 | - | F9 |
| 1460 | 2 | Port64 - Number of oversized frames received | 0 | 4294967295 | 1 | - | F9 |
| 1462 | 2 | Port64 - Number of bad fragments rcvd(<64 bytes) | 0 | 4294967295 | 1 | - | F9 |
| 1464 | 2 | Port64 - Number of jabber frames received | 0 | 4294967295 | 1 | - | F9 |
| 1466 | 2 | Port64 - Number of collisions occurred | 0 | 4294967295 | 1 | - | F9 |
| 1468 | 2 | Port64 - Number of late collisions occurred | 0 | 4294967295 | 1 | - | F9 |
| 146A | 2 | Port64 - Number of 64-byte frames rcvd/ sent | 0 | 4294967295 | 1 | - | F9 |
| 146C | 2 | Port64 - Number of 65-127 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 146E | 2 | Port64 - Number of 128-255 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 1470 | 2 | Port64 - Number of 256-511 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 1472 | 2 | Port64 - Number of 512-1023 byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 1474 | 2 | Port64 - Number of 1023-MAX byte frames rcvd/sent | 0 | 4294967295 | 1 | - | F9 |
| 1476 | 2 | Port64 - Number of Mac Error Packets | 0 | 4294967295 | 1 | - | F9 |
| 1478 | 2 | Port64 - Number of dropped received packets | 0 | 4294967295 | 1 | - | F9 |
| 147A | 2 | Port64 - Number of multicast frames sent | 0 | 4294967295 | 1 | - | F9 |
| 147C | 2 | Port64 - Number of broadcast frames sent | 0 | 4294967295 | 1 | - | F9 |
| 147E | 2 | Port64 - Number of <64 byte fragments w/ good CRC | 0 | 4294967295 | 1 | - | F9 |

### 15.2.3 Anwendungsbeispiel für die Funktion Modbus TCP

Im folgenden Beispiel richten Sie das Gerät so ein, dass es auf Client-Anfragen antwortet. Voraussetzung für diese Konfiguration ist, dass das Client-Gerät mit einer IP-Adresse aus dem angegebenen Bereich eingerichtet 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 Voreinstellung sind die Funktionen *Modbus TCP* und *Schreibzugriff* inaktiv.

Die Funktion *Modbus TCP* 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 kann zu fehlerhaften Einstellungen im Gerät führen und möglicherweise Unterbrechungen im Netz zur Folge haben.

**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.

**Das Nicht-Beachten dieser Anweisungen kann zu Geräteschäden führen.**

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung*.
- ☐ Fügen Sie eine Tabellenzeile hinzu. Klicken Sie dazu die Schaltfläche .
- ☐ Legen Sie den IP-Adressbereich in der Tabellenzeile fest, in welcher die Spalte *Index* den Wert `2` hat. Geben 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*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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.
- ☐ Schalten Sie die Funktion *Modbus TCP* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Wenden Sie die Einstellungen vorläufig an. 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 hinzufügen. 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]
```

# 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*.

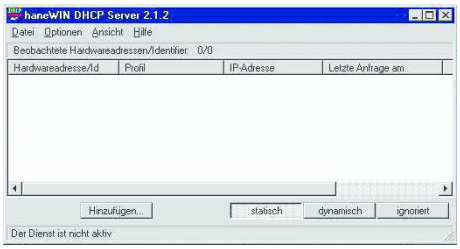



*Abb. 47: Startfenster des Programms haneWIN DHCP Server*

**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.

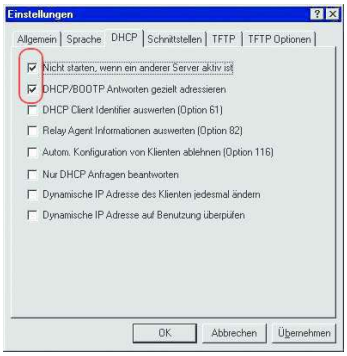



*Abb. 48:DHCP-Einstellung*

- ☐ 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.

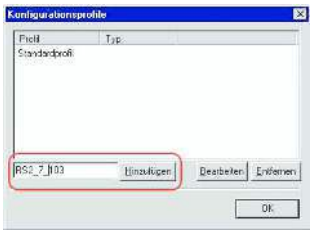



*Abb. 49:Konfigurationsprofile hinzufügen*

☐ Klicken Sie die Schaltfläche *Add*.
☐ Legen Sie die Netzmaske fest.

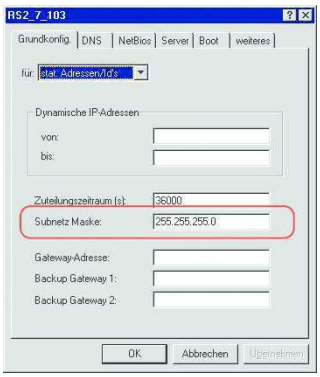



*Abb. 50:Netzmaske im Konfigurationsprofil*

☐ 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.

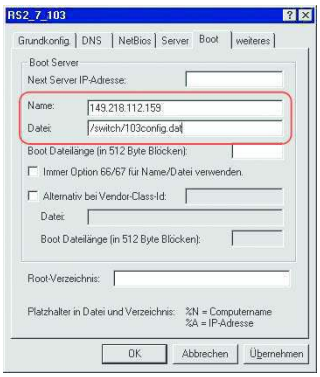



*Abb. 51:Konfigurationsdatei auf dem tftp-Server*

☐ Klicken Sie die Schaltfläche *Apply* und dann die Schaltfläche *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. 52: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*.

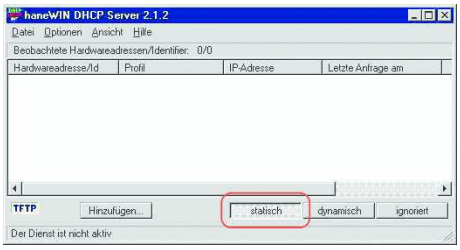



*Abb. 53:Statische Adresseingabe*

☐ Klicken Sie die Schaltfläche *Add*.

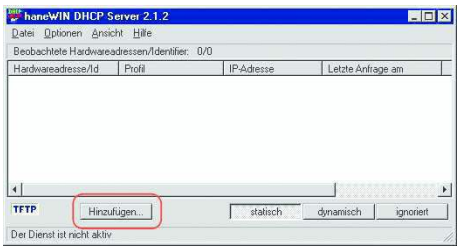



*Abb. 54:Statische Adressen hinzufügen*

☐ Geben Sie die MAC-Adresse des Geräts ein.
☐ Geben Sie die IP-Adresse des Geräts ein.

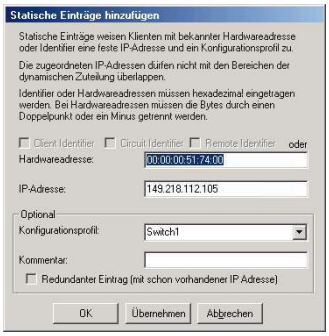



*Abb. 55:Einträge für statische Adressen*

☐ Wählen Sie das Konfigurationsprofil des Geräts.
☐ Klicken Sie die Schaltfläche *Apply* und dann die Schaltfläche *OK*.
☐ Fügen Sie für jedes Gerät, das vom DHCP-Server seine Parameter erhalten soll, einen Eintrag hinzu.

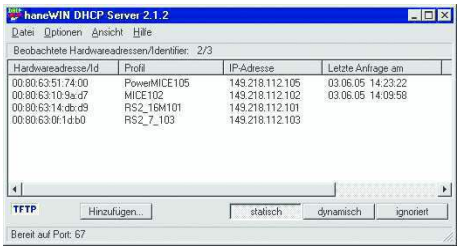



*Abb. 56:DHCP-Server mit Einträgen*

# 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*.

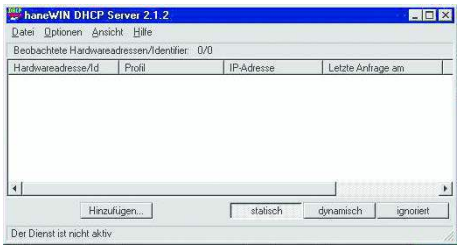



*Abb. 57: Startfenster des Programms haneWIN DHCP Server*

**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.

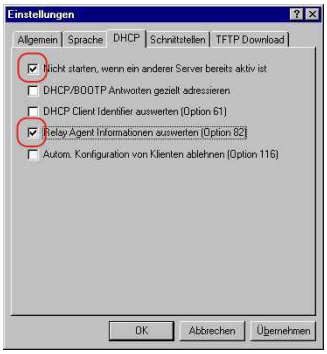



*Abb. 58: DHCP-Einstellung*

- ☐ Zur Eingabe der statischen Adressen klicken Sie die Schaltfläche *Add*.

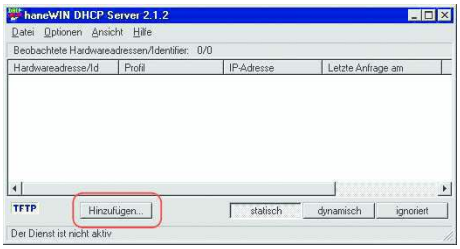



*Abb. 59: Statische Adressen hinzufügen*

- ☐ Markieren Sie das Kontrollkästchen *Circuit Identifier*.
- ☐ Markieren Sie das Kontrollkästchen *Remote Identifier*.

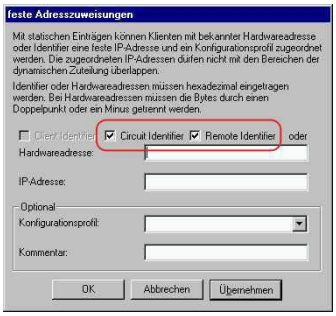



*Abb. 60: Voreinstellung für die feste Adresszuweisung*

- ☐ 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. 61: Festlegen der Adressen*

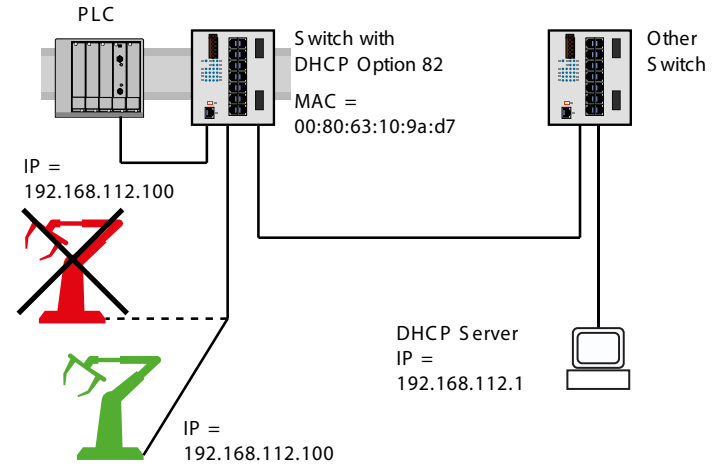



*Abb. 62: Anwendungsbeispiel für den Einsatz von Option 82*

# A.3 HTTPS-Zertifikat

Ihr Webbrowser stellt mittels Hypertext Transfer Protocol Secure (HTTPS) die Verbindung zum Gerät her. Voraussetzung ist, dass Sie die Funktion *HTTPS server* im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS* einschalten.

## A.3.1 Konflikte bei der Zertifikatsvalidierung

Webbrowser und andere Drittanbieter-Software validieren routinemäßig die Gültigkeit digitaler Zertifikate.

Wenn Ihr Webbrowser eine Meldung zeigt, die auf einen Konflikt bei der Validierung des digitalen Zertifikats des Geräts hinweist, führen Sie die folgenden Schritte aus:

- ☐ Prüfen Sie, ob das digitale Zertifikat noch gültig ist.
- ☐ Prüfen Sie, ob Ihr Webbrowser den Algorithmus, mit dem das digitale Zertifikat generiert wurde, nicht mehr als vertrauenswürdig einstuft.

Um den Konflikt bei der Zertifikatsvalidierung zu beheben, generieren Sie das digitale Zertifikat im Gerät mit der neuesten Gerätesoftware noch einmal. Siehe Abschnitt „HTTPS-Zertifikatsverwaltung”.

## A.3.2 HTTPS-Zertifikatsverwaltung

Um eine sichere Verbindung herzustellen, ist ein digitales Zertifikat im X.509-Format erforderlich. In der Voreinstellung verwendet das Gerät ein selbst signiertes digitales Zertifikat.

Sie können das selbst signierte digitale Zertifikat mit der neuesten Gerätesoftware noch einmal generieren. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS*.
- ☐ Um ein selbst signiertes digitales Zertifikat zu generieren, klicken Sie im Rahmen *Zertifikat* die Schaltfläche *Erstellen*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche  .
- ☐ Damit die Änderungen nach dem Übertragen eines digitalen Zertifikats auf das Gerät wirksam werden, schalten Sie den HTTPS-Server aus und wieder ein. Führen Sie den Neustart des HTTPS-Servers über das Command Line Interface durch.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `https certificate generate` | Ein digitales Zertifikat für den HTTPS-Server generieren. |
| `no https server` | Funktion *HTTPS* ausschalten. |
| `https server` | Funktion *HTTPS* einschalten. |

Alternativ dazu können Sie ein digitales Zertifikat extern mittels zeitgemäßer Signaturalgorithmen generieren. Übertragen Sie das neue digitale Zertifikat auf das Gerät. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS*.
- ☐ Befindet sich die Datei auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie diese in den ⬆-Bereich. Alternativ dazu klicken Sie in den Bereich, um die Datei auszuwählen.
- ☐ Um die Datei auf das Gerät zu übertragen, klicken Sie die Schaltfläche *Start*.
- ☐ Wenden Sie die Einstellungen vorläufig an. Klicken Sie dazu die Schaltfläche ✓.

| | |
|---|---|
| `enable` | In den Privileged-EXEC-Modus wechseln. |
| `copy httpscert envm <file name>` | Das digitale Zertifikat für den HTTPS-Server vom externen Speicher (*ENVM*) auf das Gerät übertragen. |
| `configure` | In den Konfigurationsmodus wechseln. |
| `no https server` | Funktion *HTTPS* ausschalten. |
| `https server` | Funktion *HTTPS* einschalten. |

**Anmerkung:**
Um das digitale Zertifikat zu aktivieren, nachdem das Gerät es generiert oder Sie es übertragen haben, 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.3.3 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*.
- ☐ Schalten Sie die Funktion *HTTPS* ein.
  Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Um über HTTPS auf das Gerät zuzugreifen, geben Sie in Ihrem Webbrowser 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 Hypertext Transfer Protocol Secure (HTTPS) 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, Axel Schneider
  Wiley, 2018
  ISBN 978-1-119-52791-6 (Print), ISBN 978-1-119-52799-2 (eBook)
- *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, 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 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`<br>(`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)<br>Zahlenwert = ganze Zahl im Bereich von $0..2^{32}-1$ |
| Timeout | Zeitwert in hundertstel Sekunden<br>Zeitwert = ganze Zahl im Bereich von $0..2^{32}-1$ |
| Typfeld | 4-stellige Hexadezimalzahl nach ISO/IEC 8802-3 |
| Zähler | Ganze Zahl ($0..2^{32}-1$), deren Wert beim Auftreten bestimmter Ereignisse um `1` erhöht wird. |

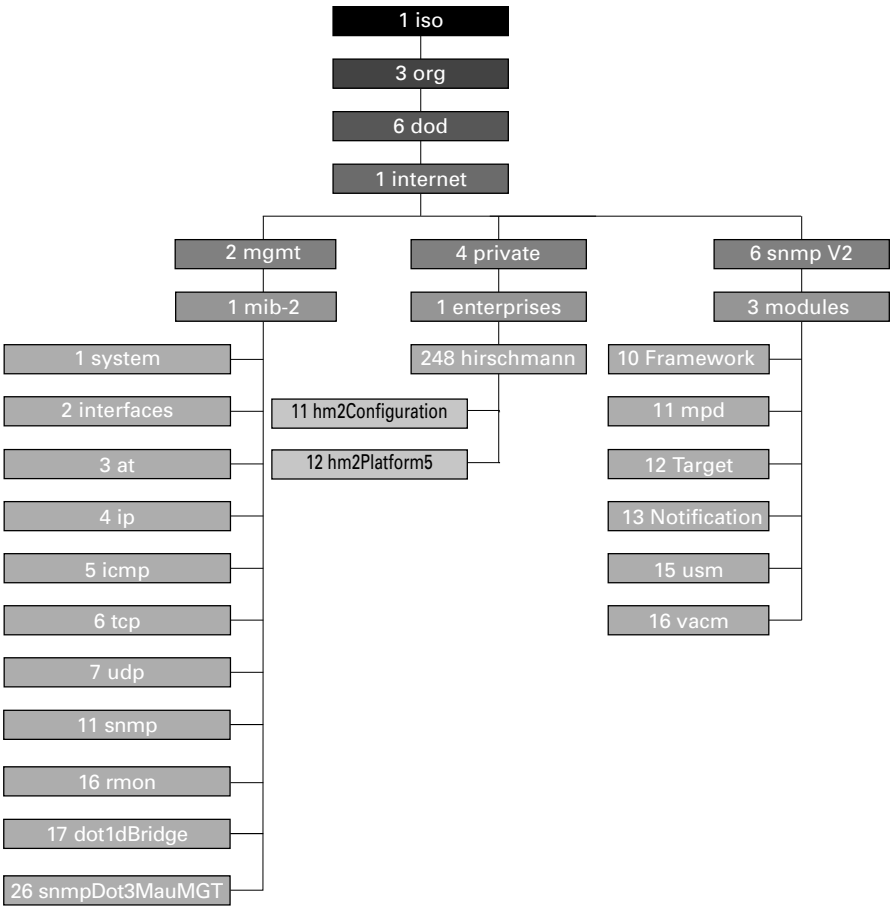



*Abb. 63: Baumstruktur der Hirschmann-MIB*

Wenn Sie von den Produktseiten im Internet eine aktualisierte Geräte-Software heruntergeladen haben, enthält das ZIP-Archiv außer der Geräte-Software auch die MIBs.

# B.3 Liste der RFCs

| | |
|---|---|
| RFC 768 | UDP |
| RFC 783 | TFTP |
| RFC 791 | IP |
| RFC 792 | ICMP |
| RFC 793 | TCP |
| RFC 826 | ARP |
| RFC 854 | Telnet |
| RFC 855 | Telnet Option |
| RFC 951 | BOOTP |
| RFC 1112 | IGMPv1 |
| RFC 1157 | SNMPv1 |
| RFC 1155 | SMIv1 |
| RFC 1212 | Concise MIB Definitions |
| RFC 1213 | MIB2 |
| RFC 1493 | Dot1d |
| RFC 1542 | BOOTP-Extensions |
| RFC 1643 | Ethernet-like -MIB |
| RFC 1757 | RMON |
| RFC 1867 | Form-Based File Upload in HTML |
| RFC 1901 | Community based SNMP v2 |
| RFC 1905 | Protocol Operations for SNMP v2 |
| RFC 1906 | Transport Mappings for SNMP v2 |
| RFC 1945 | HTTP/1.0 |
| RFC 2068 | HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03 |
| RFC 2131 | DHCP |
| RFC 2132 | DHCP-Options |
| RFC 2233 | The Interfaces Group MIB using SMI v2 |
| RFC 2236 | IGMPv2 |
| RFC 2246 | The TLS Protocol, Version 1.0 |
| RFC 2346 | AES Ciphersuites for Transport Layer Security |
| RFC 2365 | Administratively Scoped IP Multicast |
| RFC 2578 | SMIv2 |
| RFC 2579 | Textual Conventions for SMI v2 |
| RFC 2580 | Conformance statements for SMI v2 |
| RFC 2613 | SMON |
| RFC 2618 | RADIUS Authentication Client MIB |
| RFC 2620 | RADIUS Accounting MIB |
| RFC 2674 | Dot1p/Q |
| RFC 2818 | HTTP over TLS |
| RFC 2851 | Internet Addresses MIB |

| | |
|---|---|
| RFC 2863 | The Interfaces Group MIB |
| RFC 2865 | RADIUS Client |
| RFC 2866 | RADIUS Accounting |
| RFC 2868 | RADIUS Attributes for Tunnel Protocol Support |
| RFC 2869 | RADIUS Extensions |
| RFC 2869bis | RADIUS support for EAP |
| RFC 2933 | IGMP MIB |
| RFC 3164 | The BSD syslog protocol |
| RFC 3376 | IGMPv3 |
| RFC 3410 | Introduction and Applicability Statements for Internet Standard Management Framework |
| RFC 3411 | An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks |
| RFC 3412 | Message Processing and Dispatching for the Simple Network Management Protocol (SNMP) |
| RFC 3413 | Simple Network Management Protocol (SNMP) Applications |
| RFC 3414 | User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3) |
| RFC 3415 | View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP) |
| RFC 3418 | Management Information Base (MIB)<br>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 4291 | IPv6 Addressing 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 4861 | Neighbor Discovery for IPv6 |

| | |
|---|---|
| RFC 6221 | Leightweight DHCPv6 Relay Agent |
| RFC 8200 | IPv6 Specification |
| RFC 8415 | DHCPv6 |

# B.4 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.5 Zugrundeliegende IEC-Normen

| | |
|---|---|
| IEC 62439 | High availability automation networks<br>MRP – Media Redundancy Protocol based on a ring topology |

# B.6 Zugrundeliegende ANSI-Normen

| | |
|---|---|
| ANSI/TIA-1057 | Link Layer Discovery Protocol for Media Endpoint Devices, April 2006 |

# B.7 Technische Daten

## B.7.1 Switching

| | |
|---|---|
| Größe der MAC-Adresstabelle (Forwarding Database) (inkl. statische Filter) | 16384 |
| Max. Anzahl statisch eingerichteter MAC-Adressfilter | 100 |
| Max. Anzahl der mit IGMP-Snooping lernbaren MAC-Adressfilter | 512 |
| Max. Anzahl der MAC-Adresseinträge (MMRP) | 64 |
| Anzahl Warteschlangen | 8 Queues |
| Einstellbare Port-Prioritäten | 0..7 |
| MTU (max. erlaubte Länge der Pakete, die ein Port empfangen oder senden kann) | 1996 Bytes |

## B.7.2 VLAN

| | |
|---|---|
| VLAN-ID-Bereich | 1..4042 |
| Anzahl der VLANs | max. 128 gleichzeitig pro Gerät<br>max. 128 gleichzeitig pro Port |

## B.7.3 Access-Control-Listen (ACL)

| | |
|---|---|
| Max. Anzahl der ACLs | 50 |
| Max. Anzahl der Regeln pro ACL | 18 |
| Max. Anzahl der Regeln pro Port | 18 |
| Anzahl der insgesamt konfigurierbaren Regeln | 900 (50 × 18) |
| Max. Anzahl der VLAN-Zuweisungen | 12 |
| Max. Anzahl der Regeln, die ein Ereignis protokollieren | 128 |
| Max. Anzahl der Ingress-Regeln | 768 |

# B.8 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.9 Verwendete Abkürzungen

| | |
|---|---|
| ACA | Name des externen Speichers |
| ACL | Access Control List |
| BOOTP | Bootstrap Protocol |
| CLI | Command Line Interface |
| DHCP | Dynamic Host Configuration Protocol |
| DHCPv6 | Dynamic Host Configuration Protocol for IPv6 |
| DUID | DHCP Unique Identifier |
| 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 |
| IPv6 | Internet Protocol version 6 |
| LDRA | Lightweight DHCPv6 Relay Agent |
| LED | Light Emitting Diode |
| LLDP | Link Layer Discovery Protocol |
| MAC | Media Access Control |
| MIB | Management Information Base |
| MRP | Media Redundancy Protocol |
| NDP | Neighbor Discovery Protocol |
| NMS | Network Management System |
| PC | Personal Computer |
| 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**
802.1X . . . . . 66

**A**
Advanced-Modus . . . . . 193, 196
Aging-Time . . . . . 155
Alarm . . . . . 224
Alarmnachrichten . . . . . 223
Alternate-Port . . . . . 209, 215
APNIC . . . . . 44
ARIN . . . . . 44
ARP . . . . . 46
Arten von IPv6-Adressen . . . . . 49
Auslastung . . . . . 200, 201
Authentifizierungs-Liste . . . . . 66
Automatische Konfiguration . . . . . 118

**B**
Backup-Port . . . . . 210, 215
Bandbreite . . . . . 171
Baumstruktur (Spanning Tree) . . . . . 205, 208
Benutzernamen . . . . . 16, 18, 20
Berechtigungen . . . . . 69
Bericht . . . . . 246
BOOTP . . . . . 43
BPDU . . . . . 204
BPDU Guard . . . . . 214, 215
Bridge Protocol Data Unit . . . . . 204
Bridge-Identifikation . . . . . 201

**C**
CIDR . . . . . 46
Classless Inter Domain Routing . . . . . 46
Command Line Interface . . . . . 17

**D**
Datenstrom überwachen (Port-Mirroring) . . . . . 254
Datenverkehr . . . . . 137
Denial of Service . . . . . 137
Designated Bridge . . . . . 209
Designated Port . . . . . 209, 214
DHCP . . . . . 43
DHCP-L2-Relay . . . . . 265
DHCP-Server . . . . . 86, 90, 259, 291, 294
DHCPv6 . . . . . 62
Diameter (Spanning Tree) . . . . . 203
DiffServ . . . . . 161
Disabled-Port . . . . . 210
DoS . . . . . 137
DSCP . . . . . 161, 168

**E**
Echtzeit . . . 161
Edge-Port . . . 209, 214
Ereignisprotokoll . . . 249
Erstinstallation . . . 43
Erweiterte Informationen zu MRP . . . 194
Erweiterte Informationen, MRP . . . 194

**F**
FDB (MAC-Adresstabelle) . . . 151
Ferndiagnose . . . 233
Flüchtiger Speicher (RAM) . . . 93
Flusskontrolle . . . 171
Funktionsüberwachung . . . 233

**G**
GARP . . . 269
Gateway . . . 44, 53
Generische Objektklassen . . . 302
Gerät ersetzen . . . 13
Gerätestatus . . . 225
Global-Config-Modus . . . 23
GMRP . . . 269

**H**
HaneWin . . . 291, 294
Hardware-Reset . . . 223
HiDiscovery . . . 43
HiView . . . 65
Hostadresse . . . 44

**I**
IANA . . . 44
IAS . . . 66
IEC 61850 . . . 278
IEEE 802.1X . . . 66
IEEE-MAC-Adresse . . . 243
IGMP-Snooping . . . 155
Industrial HiVision . . . 11
Instanzierung . . . 302
Integrated Authentication Server . . . 66
IP-Adresse . . . 44, 53, 60
IP-Header . . . 161, 164
IPv6-Adresse . . . 48
ISO/OSI-Schichtenmodell . . . 46

**K**
Kommandobaum . . . 25
Konfigurationsänderungen . . . 223
Konfigurationsdatei . . . 60

**L**
LACNIC . . . 44
Leave-Nachricht . . . 155
Link-Aggregation . . . 190
Link-Überwachung . . . 225, 233
Login-Dialog . . . 16
Loop Guard . . . 215, 217

**M**
MAC-Adressen-Filter . . . 151
MAC-Adresstabelle (Forwarding Database) . . . 151
MAC-Zieladresse . . . 46
MaxAge . . . 204
MMS . . . 278
Modus . . . 118
MRP . . . 190, 192, 193
MRP-IEEE . . . 271
MRP-IEEE-Funktion . . . 271
MRP-IEEE-Timer . . . 272
MRP-Pakete . . . 194
MRP-Paket-Priorisierung . . . 195
Multicast . . . 155

**N**
Nachricht . . . 223
Netzlast . . . 200, 201
Netzmanagement . . . 61
Netzmaske . . . 44, 53
Netzstruktur . . . 192
Nichtflüchtiger Speicher (NVM) . . . 93
NVM (nichtflüchtiger Speicher) . . . 93

**O**
Object Description . . . 302
Object-ID . . . 302
Objektklassen . . . 302
OpenSSH . . . 19, 130
Option 82 . . . 294

**P**
Pfadkosten . . . 202, 205
Polling . . . 223
Port Mirroring . . . 254
Port-Identifikation . . . 201
Port-Priorität . . . 167
Port-Rollen (RSTP) . . . 209
Port-Status . . . 210
Präfixlänge . . . 49
Priorität . . . 163
Priority Tagged Frames . . . 163
Privileged-Exec-Modus . . . 22
PuTTY . . . 17, 19

**Q**
QoS . . . 162
Query . . . 155

**R**

RADIUS . . . . . 66
RAM (flüchtiger Speicher) . . . . . 93
Rapid Spanning Tree . . . . . 190, 209
Redundanz . . . . . 200
Referenzzeitquelle . . . . . 85, 90
Rekonfiguration . . . . . 201
Rekonfigurationszeit (MRP) . . . . . 193
Relaiskontakt . . . . . 233
Report-Nachricht . . . . . 155
RFC . . . . . 304
Ring . . . . . 192
Ring-Manager . . . . . 192
RIPE NCC . . . . . 44
RM (Ring-Manager) . . . . . 192
RMON-Probe . . . . . 254
Root Guard . . . . . 214, 217
Root-Bridge . . . . . 205
Root-Pfad . . . . . 206, 207
Root-Pfadkosten . . . . . 201
Root-Port . . . . . 209, 215
Router . . . . . 44
Router Advertisement Daemon . . . . . 58, 62
RST BPDU . . . . . 209, 211
RSTP . . . . . 212
Ruhestromschaltung . . . . . 233

**S**

Schulungsangebote . . . . . 321
Schutzfunktionen (Guards) . . . . . 214
Secure Shell (SSH) . . . . . 19
Segmentierung . . . . . 223
Serielle Verbindung . . . . . 17, 37
Service . . . . . 246
Service Shell deaktivieren . . . . . 35
Service-Shell . . . . . 22
SFP-Modul . . . . . 242
Signalkontakt . . . . . 233
SNMP . . . . . 223
SNMP-Trap . . . . . 223, 224
SNTP . . . . . 85
Software-Version . . . . . 107
SSH (Secure Shell) . . . . . 19
Store and Forward . . . . . 151
STP-BPDU . . . . . 204
Strict-Priority . . . . . 164
Subidentifier . . . . . 302
Subnetz . . . . . 53
System Monitor 1 . . . . . 37
Systemanforderungen (grafische Benutzeroberfläche) . . . . . 15
Systemzeit . . . . . 85

**T**
Tab-Completion . . . . . 32
TCN Guard . . . . . 215, 217
Technische Fragen . . . . . 321
Technische Unterlagen . . . . . 321
Technische Unterstützung . . . . . 321
Topology-Change-Flag . . . . . 215
ToS . . . . . 161, 164
Trap . . . . . 223, 224
Trap-Ziel-Tabelle . . . . . 223
Type of Service . . . . . 164

**U**
Übertragungssicherheit . . . . . 223
Uhrzeit einstellen . . . . . 85
User-Exec-Modus . . . . . 22

**V**
Verkehrsklasse . . . . . 164, 168
Verzögerungszeit (MRP) . . . . . 193
Video . . . . . 164
VLAN . . . . . 173
VLAN-Modus . . . . . 22
VLAN-Priorität . . . . . 167
VLAN-Tag . . . . . 163, 173
VoIP . . . . . 164
VT100 terminal emulation . . . . . 17, 37

**W**
Warteschlange . . . . . 164
Weighted Fair Queuing . . . . . 165
Weighted Round Robin . . . . . 165

**Z**
Ziel-Tabelle . . . . . 223
Zugangsschutz . . . . . 117

# D Technische 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.belden.com.

Technische Unterstützung erhalten Sie unter my.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/services/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 IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Deutschland

HIRSCHMANN

A BELDEN BRAND

HIRSCHMANN
A BELDEN BRAND

# User Manual

## Security
## GREYHOUND Switch GRS103
## HiOS-2S



Technical support
https://hirschmann-support.belden.com

The naming of copyrighted trademarks in this manual, even when not specially indicated, should not be taken to mean that these names may be considered as free in the sense of the trademark and tradename protection law and hence that they may be freely used by anyone.

© 2026 Hirschmann Automation and Control GmbH

Manuals and software are protected by copyright. All rights reserved. The copying, reproduction, translation, conversion into any electronic medium or machine scannable form is not permitted, either in whole or in part. An exception is the preparation of a backup copy of the software for your own use.

The performance features described here are binding only if they have been expressly agreed when the contract was made. This document was produced by Hirschmann Automation and Control GmbH according to the best of the company's knowledge. Hirschmann reserves the right to change the contents of this document without prior notice. Hirschmann can give no guarantee in respect of the correctness or accuracy of the information in this document.

Hirschmann can accept no responsibility for damages, resulting from the use of the network components or the associated operating software. In addition, we refer to the conditions of use specified in the license contract.

You find the latest user documentation for your device at: doc.hirschmann.com

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

# Contents


**Safety instructions** . . . 9

**Safety information** . . . 10

**About this Manual** . . . 11

**Key** . . . 12

**Synopsis** . . . 13
Audience . . . 13

**1 Security planning** . . . 15
1.1 Basics . . . 15
1.1.1 Security terminology . . . 15
1.1.2 Convenience vs. security: Navigating the field of tension . . . 17
1.1.3 Skepticism vs. optimism: qualitative security philosophy . . . 18
1.1.4 Impartial assessment . . . 18
1.1.5 Threat analysis . . . 19
1.1.6 Mitigation: confidentiality example . . . 19
1.1.7 Theoretical and practical degrees of security . . . 20
1.1.8 Strategies to provide improved security: confidentiality example . . . 20
1.1.9 Skepticism: Approximations in this document . . . 20
1.2 Overview . . . 21
1.2.1 Subject . . . 21
1.2.2 Scope . . . 21
1.2.3 Capability security levels . . . 22
1.2.4 Required preparatory work . . . 22
1.2.5 Software setup scenarios and hardware scenarios . . . 24
1.2.6 Scenario development . . . 24
1.3 Compiling a threat profile . . . 25
1.3.1 Risk value and unit . . . 25
1.3.2 Assess the risk of an individual threat . . . 26
1.4 Defense in depth . . . 27
1.4.1 Introduction . . . 27
1.4.2 Purpose . . . 27
1.4.3 Defense in depth vs. hardening . . . 27
1.4.4 Responsibilities . . . 28
1.4.5 Defense in depth example . . . 28
1.5 Developing a mitigation strategy . . . 30
1.5.1 Assess the efficiency of an individual mitigation measure . . . 30
1.5.2 Mitigation efficiency value and unit . . . 31
1.5.3 Alternatives to mitigation . . . 31
1.6 Criticality assessment and mitigation strategies . . . 33
1.6.1 Mitigation calculation . . . 33
1.6.2 Combining threat risk and mitigation efficiency . . . 33
1.6.3 Recommended mitigation strategies . . . 34
1.6.4 Residual risk . . . 34
1.6.5 Security viewpoints: binary or continuous values . . . 34
1.7 Cryptographic key and password basics . . . 36
1.7.1 Cryptographic key policies . . . 36
1.7.2 Password and cryptographic key comparison . . . 37

1.8 Impact of the system life cycle on the device life cycle . . . 38
1.8.1 VLAN plan . . . 38
1.9 Impact of device requirements on system planning . . . 39
1.9.1 Planning a secure installation location . . . 39
1.9.2 Planning for device availability . . . 40
1.9.3 Planning for Software auto update from the external memory . . . 40
1.9.4 Planning for SSH key auto upload from the External Memory . . . 40
1.9.5 Planning the Configuration load priority for the external memory . . . 40
1.9.6 Planning for signal contact use . . . 41
1.9.7 Planning for device and port LED visibility . . . 41
1.9.8 Planning how to check the security seal . . . 41
1.9.9 Planning restrictions to the device hardware interfaces . . . 42
1.9.10 Planning a secure boot policy <SL-C2> . . . 42
1.9.11 Planning a dedicated user account login policy . . . 43
1.9.12 Planning a dedicated user account password policy . . . 44
1.9.13 Planning a dedicated user account name and access role policy for device management . . . 45
1.9.14 Planning configuration encryption and the associated password . . . 47
1.9.15 Planning session timeouts <SL-C2> . . . 47
1.9.16 Planning a dedicated logging policy . . . 47
1.9.17 Planning a dedicated LLDP policy <SL-C2> . . . 48
1.9.18 Advanced authentication measures <SL-C2> . . . 48
1.10 Impact of network aspects on system planning . . . 49
1.10.1 External server considerations . . . 49
1.10.2 Software update and configuration server considerations <SL-C2> . . . 49
1.10.3 External DHCP server considerations . . . 50
1.10.4 Authentication server considerations <SL-C2> . . . 51
1.10.5 Logging server considerations <SL-C2> . . . 51
1.11 Device-related policies . . . 53
1.11.1 Develop a backup policy for device-related data . . . 53
1.11.2 Develop a policy for replacing the device hardware . . . 53
1.11.3 Develop a policy for device hardware repair . . . 53
1.11.4 Develop a policy for device hardware decommissioning . . . 54
1.11.5 Develop a policy for device hardware disposal . . . 55
1.12 Operation and maintenance policy . . . 56
1.13 Document the planned policies . . . 57

**2 Device security in the life cycle phases** . . . 59
2.1 Develop the device configuration . . . 59
2.2 Software vs. hardware measures (logical vs. physical) . . . 60
2.3 Security-related vs. general device functions . . . 61
2.4 Prerequisites for installation and setup . . . 62
2.4.1 Possible further prerequisites . . . 62
2.5 Suggested installation step sequence . . . 63
2.5.1 Reasons for the suggested installation step sequence . . . 63
2.5.2 Suggested preparation for installation . . . 63
2.6 Choosing a secure installation location . . . 65
2.6.1 Considering the device availability requirements . . . 65
2.7 Considering the power supply redundancy requirements . . . 66
2.8 Considering the power budget requirements . . . 67
2.9 Considering the data link redundancy requirements . . . 68

2.10 Software update . . . 69
2.10.1 Initial access to the device management . . . 69
2.10.2 Initial password considerations . . . 69
2.10.3 Software update server considerations . . . 70
2.10.4 Secure boot considerations . . . 70
2.10.5 Best practices . . . 71
2.10.6 Detailed documentation . . . 71
2.11 Security setup overview . . . 72
2.11.1 Assign IP address parameters to the device management . . . 74
2.11.2 Disable HiDiscovery access . . . 74
2.11.3 Enable the secure boot mode <SL-C2> . . . 75
2.11.4 Enable configuration encryption <SL-C2> . . . 75
2.11.5 Set up a VLAN dedicated to device management access . . . 76
2.11.6 Disable logical access to the signal contact . . . 76
2.11.7 Disable logical access to unused ports and SFP slots . . . 76
2.11.8 Disable logical access for empty or unused media modules slots . . . 76
2.11.9 Set up Power over Ethernet (depends on hardware) . . . 77
2.11.10 Disable the automatic device software update from the external memory (ACA) . . . 77
2.11.11 Disable the SSH key auto upload from the external memory . . . 78
2.11.12 Disable the Configuration load priority for the external memory . . . 78
2.11.13 Disable copying a software file into the device that lacks a valid cryptographic signature . . . 78
2.11.14 Disable writing an unencrypted configuration profile to the external memory (ACA) . . . 79
2.11.15 Disable loading an unencrypted configuration profile from the external memory (ACA) <SL-C2> . 79
2.11.16 Disable insecure management protocols . . . 79
2.11.17 Set up management IP access restrictions . . . 80
2.11.18 Set up a dedicated HTTPS certificate for the device . . . 80
2.11.19 Set up a dedicated SSH host key for the device . . . 81
2.11.20 Set up the SSH Known Hosts fingerprints in the device . . . 82
2.11.21 Set up a dedicated user account login policy . . . 83
2.11.22 Set up a dedicated user account password policy . . . 83
2.11.23 Set up dedicated user account names and access roles for device management <SL-C2> . . . 84
2.11.24 Specify finite session timeouts <SL-C2> . . . 86
2.11.25 Set up certificates and possible revocation lists for authentication, logging and eMail servers . . . 86
2.11.26 Set up logging . . . 87
2.11.27 Disable SNMPv1 traps . . . 87
2.11.28 Enable SNMPv3 traps . . . 88
2.11.29 Set up dedicated login banners . . . 88
2.11.30 Advanced: Access to the system monitor through the serial port . . . 88
2.11.31 Advanced: disable access to the CLI service shell . . . 89
2.11.32 Set up advanced user authentication <SL-C2> . . . 89
2.11.33 Create a backup of the device-related data . . . 90
2.12 Possible restrictions to the device’s hardware interfaces . . . 91
2.12.1 Restrict physical access to the USB port . . . 91
2.12.2 Restrict physical access to network ports or SFP slots . . . 92
2.12.3 Restrict physical access to empty media module slots . . . 92
2.12.4 Restrict physical access to the signal contact . . . 92
2.12.5 Restrict physical (visual) access to the device LEDs and port LEDs . . . 92
2.13 Device installation . . . 93
2.13.1 Checking the security seal . . . 93
2.13.2 Data connections . . . 93
2.13.3 Signal contact considerations . . . 93
2.14 Operation . . . 94

2.15 Maintenance . . . 95
2.15.1 Check the security seal (regularly or triggered by an event) . . . 95
2.15.2 Software update . . . 95
2.15.3 Hardware changes . . . 95
2.15.4 Device hardware replacement . . . 96
2.15.5 Device hardware repair . . . 97
2.16 Device decommissioning . . . 99
2.16.1 Deletion of confidential data and secrets . . . 99
2.16.2 Reset to the delivery state . . . 99
2.16.3 Secure physical destruction of the device and its accessories . . . 100
2.16.4 Secure removal of device-related data from the administration environment . . . 100
2.16.5 Secure disposal of the device hardware . . . 100

**3 Network security support** . . . 101
3.1 Introduction . . . 101
3.1.1 Prerequisites for setting up network security . . . 101
3.1.2 Deploying defense in depth for your network . . . 102
3.1.3 Harden your network . . . 102
3.2 Measures to help secure the network . . . 103
3.3 Restrict logical access to your network . . . 104
3.3.1 Set up VLANs for traffic segregation . . . 104
3.3.2 Disable GVRP and MVRP . . . 104
3.3.3 Set up the Port Security . . . 104
3.4 Help secure the network protocols used . . . 106
3.4.1 Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) . . . 106
3.5 Help secure the redundancy protocols used . . . 107
3.5.1 Set up RSTP guards and helper protocols . . . 107
3.5.2 Set up the MRP (Media Redundancy Protocol) parameters. . . . 108
3.6 Set up the attack protection support functions . . . 109
3.6.1 Set up the Denial of Service (DoS) parameters . . . 109
3.6.2 Set up the rate limiter . . . 109
3.7 Set up Access Control Lists (ACLs) . . . 110
3.7.1 Introduction . . . 110
3.7.2 Resolving potential conflicts of aims for an ACL . . . 111
3.7.3 Creating ACLs and associations . . . 111
3.8 Set up the logging parameters . . . 114
3.8.1 Audit trail (created by persistent logging) . . . 114
3.9 Set up the LLDP parameters <SL-C2> . . . 115

**A Security seal** . . . 117
A.1 Overview . . . 117
A.2 Details . . . 118
A.2.1 Glued front label . . . 118
A.2.2 Potted device . . . 119
A.2.3 Security stickers . . . 119

**B Password strength and policy guide** . . . 121
B.1 Password classes . . . 121
B.2 Password policies . . . 123
B.3 Password schemes . . . 124
B.4 Password attack strategies . . . 125

B.5 Basic security assumptions . . . 126
B.5.1 Aggressive assumptions about attackers . . . 126
B.5.2 Conservative assumptions about users . . . 126
B.5.3 Conservative assumptions about the attack context . . . 127
B.6 Quantitative password strength . . . 128
B.6.1 High-complexity passwords . . . 128
B.6.2 Low-complexity passwords . . . 130
B.7 Attack resistance time (quantitative) . . . 133
B.7.1 Examples, unmitigated attack rate . . . 134
B.7.2 Attack rate mitigation . . . 134
B.7.3 Examples, mitigated attack rate . . . 135
B.8 Required attack resistance time (quantitative) . . . 136
B.9 Password entropy . . . 137
B.10 Calculating the required password entropy . . . 138
B.11 Password policy lookup tables (quantitative) . . . 140
B.11.1 Password entropy lookup tables . . . 140
B.11.2 Password policy lookup table, low-complexity passwords . . . 141
B.11.3 Password policy lookup table, high-complexity passwords . . . 142

**C Considerations for manually entered keys** . . . 145
C.1 Quantitative key strength . . . 145
C.1.1 Key entry as ASCII string . . . 146
C.1.2 Key entry as hexadecimal string . . . 147
C.1.3 Conclusion . . . 148
C.1.4 Example of random key value generation (tool use) . . . 150

**D Index** . . . 151

**E Technical support** . . . 163

**F Readers' Comments** . . . 164

# Safety instructions

**⚠ WARNING**

**UNCONTROLLED MACHINE ACTIONS**

To avoid uncontrolled machine actions caused by data loss, configure all the data transmission devices individually.

Before you start any machine which is controlled via data transmission, be sure to complete the configuration of all data transmission devices.

**Failure to follow these instructions can result in death, serious injury, or equipment damage.**

# Safety information

| ⚠ WARNING |
| --- |
| **WARNING** indicates a potentially hazardous situation which, if not avoided, **can result in** death or serious injury. |

| *NOTICE* |
| --- |
| **NOTICE** is used to address practices not related to physical injury. |

# About this Manual

The “Configuration” user manual contains the information you need to start operating the device. It takes you step by step from the first startup operation through to the basic settings for operation in your environment.

The “Installation” user manual contains a device description, safety instructions, a description of the display, and the other information that you need to install the device.

The “Graphical User Interface” reference manual contains detailed information on using the graphical user interface to operate the individual functions of the device.

The “Command Line Interface” reference manual contains detailed information on using the Command Line Interface to operate the individual functions of the device.

The “Device Security and Network Security Support” user manual contains an introduction, considerations for system security planning, and policy development, and an enumeration of device security measures. It also suggests how a secured device can assist in both securing and improving the availability of your network. Furthermore, password strength and specific mitigation measures are discussed, completed with a guide to password policy.

The Industrial HiVision Network Management software provides you with additional options for smooth configuration and monitoring:

- Auto-topology discovery
- Browser interface
- Client/server structure
- Event handling
- Event log
- Simultaneous configuration of multiple devices
- Graphical user interface with network layout
- SNMP/OPC gateway

# Key

The designations used in this manual have the following meanings:

| | |
|---|---|
| • Item<br>– Sub-item<br>▶ Item | General list item<br>Sublist item<br>Parameter value item |
| ☐ | Work or planning step |
|  | Marks a reference to an external user or reference manual. |
|  | The delivery state of the setting preceding the icon may be considered insecure. |
| Link | Cross-reference with link |
| **Note:** | A note emphasizes a significant fact or draws your attention to a dependency. |
| **Boldface** | Marks a key concept introduced for the first time. |
| "Chapter 1 > Chapter 1.1" | Practical reference to a chapter and sub-chapter in an external user manual or reference manual |
| [CR…][1] | Formal reference to an IEC 62443-4-2 Component Requirement |
| [CR… - informational][1] | Informational reference to an IEC 62443-4-2 Component Requirement |
| [CR…RE…][1] | Formal reference to the Requirement Enhancement of an IEC 62443-4-2 Component Requirement |
| [CR…RE…][1] | Formal reference to the Requirement Enhancement of an IEC 62443-4-2 Component Requirement |
| [NDR…][1] | Formal reference to an IEC 62443-4-2 Network Device Requirement |
| <SL-C…>[2] | Formally marks content that relates to IEC 62443 Security Capability Level 2 (SL-C2) or higher. For example, <SL-C2> marks content that conforms to SL-C2. |
| [SR…][1] | Reference to an IEC 62443-3-3 System Requirement |
| [SR… RE…][1] | Formal reference to the Requirement Enhancement of an IEC 62443-3-3 System Requirement |

1. If a formal reference to the standard appears at the beginning of a chapter, it applies to the whole chapter. If a reference appears at the beginning of a paragraph or list item, it applies only to the respective paragraph or list item. If a reference appears in a comma-separated list, it applies only to the item tagged with the reference.
2. If a formal reference to the SL-C level appears at the end of the of a chapter headline, it applies to the whole chapter. If a reference appears at the end of a sentence (before the period), it applies only to the respective sentence.

# Synopsis

This document deals with how to achieve and improve the security of an industrial communication network using the IEC 62443 "Security of Industrial Automation and Control Systems" series of standards as a framework.

The general security level addressed in this document is the IEC 62443 Capability Security Level 1 (SL-C1). SL-C1 means protection against casual or coincidental access by unauthenticated entities. Content conforming to SL-C1 is not marked up. However, content conforming to SL-C2 is marked up with <SL-C2>.

The chapter "Security Planning" (see on page 15 “Security planning”) introduces the subject, describes required preparatory work, explains some key concepts, and gives a hierarchy of hardware and software measures. It also describes the interdependence of device, network and system requirements, and details the required planning steps, resulting in a collection of policies.

The chapter "Device security in the life cycle phases" (see on page 59 “Device security in the life cycle phases”) details particular measures and steps to help secure a network device, based on the policies developed in the planning chapter.

The chapter "Network security support" (see on page 101 “Network security support”) describes particular measures to set up a network device to help support the security and availability of the network. The prerequisite is that the device itself has been secured. ACL setup is described extensively.

The appendix "Security seal" (see on page 117 “Security seal”) deals with the mechanical security methods of the device, their security properties, signs of tampering, the recommended procedures for checking the seals, and the recommended decommissioning procedure.

The appendix "Password strength and policy guide" (see on page 121 “Password strength and policy guide”) (informational only) deals with password strength, explains key concepts like password classes, password policies, password schemes, the strengths and weaknesses of password classes, shows how to calculate and improve the provided attack resistance time, shows how to calculate the required password entropy for an effective mitigation, and finally offers to look up a password policy that satisfies the desired level of attack resistance.

The appendix "Considerations for manually entered keys" (see on page 145 “Considerations for manually entered keys”) (informational only) deals with keys for symmetric cryptography, explains concepts like key classes, entry schemes, key strength, and the residual weaknesses of keys.

# Audience

This security user manual primarily addresses Ethernet network planners, commissioners, administrators, operators, maintainers, and decommissioners.

The contents may also be useful for solution providers, sales partners, and system integrators.

# 1 Security planning

## 1.1 Basics

If you are new to security for industrial networks, you may find this chapter a good start.

### 1.1.1 Security terminology

The term "Security" typically can be subdivided into the following aspects.

*Table 1: Aspects of security*

| Aspect | Description |
|---|---|
| **Confidentiality** | Only authorized entities have read access to specified information or devices. |
| **Integrity** | Only authorized entities have write or modify access to specified information. For devices, only authorized entities have the privileges to set up specified devices, and to install or update device software. |
| **Availability**[1] | Only authorized entities have the privileges to delete, modify, or deny access to specified information, or to remove or disable specified devices. |
| **Authenticity** | Specified information contains proof of which entity created or modified the specified information, or which entity installed, set up or a updated specified device. |
| **Nonrepudiability**[2] | Authenticated information or devices can be traced to the entity that created or modified the information, or updated or set up a device. This entity then cannot plausibly deny its creatorship. |

1. Availability can be regarded as a part of integrity.
2. Nonrepudiability can be regarded as a part of authenticity.

**Note:**
Depending on your actual situation, some or all of the above aspects must be satisfied to consider a situation secure.

### Example for confidentiality and integrity

For management of the device, the device offers different user account roles. These roles offer different degrees of access. This helps control confidentiality and integrity.

*Table 2: Example for confidentiality and integrity, based on user account roles*

| User account role | Description | Security consequences |
|---|---|---|
| `unauthorized` | A user with this account role cannot log into the device. | Device management data remains confidential and integer. |
| `guest` | A user with this account role can log into the device to read data, except the audit trail. The user does not have write access to any data. | This user account role can read confidential data. Integrity is provided by read-only access. |
| `auditor` | A user with this account role can log into the device to read data, including the audit trail. The user can write the audit trail to a log file. | This user role can read confidential data. Integrity is provided by the immutable audit trail in the device. |
| `operator` | A user with this account role can log into the device to read and write device management data. Access to security-relevant settings and the audit trail is read-only. | This user role can read and write confidential data. Integrity is provided by read-only access to security settings and the immutable audit trail. |
| `administrator` | A user with this account role can log into the device to read and write data, including security-relevant settings. This role can also read the audit trail. | This user role can read and write confidential data. Integrity is provided by the immutable audit trail in the device |

### More terms

Most of the terms in the following table are used and explained in more detail in the remainder of this main chapter.

*Table 3: Security terms*

| Aspect | Description |
|---|---|
| **Vulnerability** | A flaw or weakness of a system. Vulnerabilities can be unintentional (like an unintended software problem), or they can be unavoidable (like a system that offers a login). The union set of all vulnerabilities of a system is called an attack surface. |
| **Threat** | A potentially negative action, event, or circumstance that results in an unwanted impact to a system. A threat is related to a specific vulnerability of the system. A threat can be deliberate or accidental. |
| **Threat model** | A threat model is a model that defines the logical borders of a given asset, and the conditions under which threats are assumed. By defining these fundamental conditions, a threat model enables the reasonable, structured collection and description of perceivable threats. The outcome of a threat model is a threat collection. |
| **Threat collection** | A threat collection is the outcome when perceivable threats are applied to a threat model. It lists the perceivable threats that are deemed applicable to the threat model. It contains all collected threats, regardless of their exploitability, exploit severity, or their associated mitigation effort or effectiveness. |
| **Threat profile** | A threat profile is a threat collection ordered by threat risk, the combined treat/ mitigation criticality, or other, appropriate criteria. |

*Table 3: Security terms*

| Aspect | Description |
|---|---|
| **Threat risk** | The combination of both the degree of exploitability of a given threat and the severity of the results if the threat is applied to the system. The easier a threat can be exploited and the more severe its results, the higher the threat risk. |
| **Mitigation** | A process or action of countermeasure with the goal to thwart or attenuate a threat risk, either by lowering the exploitability of the threat or to diminish its results. Mitigation can be seen as part of vulnerability management. |
| **Mitigation efficiency** | The degree to which a given mitigation measure thwarts or attenuates a threat risk. It consists of the mitigation's effort and effectiveness. The lower the effort to implement a mitigation measure and the higher the effectiveness of the mitigation measure, the higher the mitigation effectiveness. |
| **Criticality** | The criticality applies to a specific threat risk in conjunction with a specific mitigation measure's efficiency. The higher the threat risk and the lower the associated mitigation's efficiency, the more critical this combination is. |

### 1.1.2 Convenience vs. security: Navigating the field of tension

On a qualitative level (that is, not using a structured approach), the concepts of security and convenience are often seen as contradicting each other. As an example, consider a database that stores personal data, for example, of customers.

**Convenience trumps security**: If access to the database requires only one user name for any database user and requires only a trivial password for login:
- Such a system is convenient for the database users.
- At the same time, it is highly insecure because the confidentiality of the personal data is insufficient.

**Security trumps convenience**: If access to the database requires individual, hard-to-remember user names and enforces the use of system-generated, long and truly random passwords for login:
- Such a system is considerably inconvenient for the database users.
- At the same time, it can be regarded as highly secure because the confidentiality of the personal data is well protected.

In practice, often none of the above given extreme examples are feasible.

As a consequence, security planning needs an impartial approach, and should be based on metrics. This approach enables you to weigh threats against mitigation measures, helps you attain a reasonably secure system and also provides you with detailed, comprehensible points for your chosen mitigation measures.

**Security is weighed against usability**: If access to the database requires individual but short user names and allows memorable and user-chosen passwords according to an enforced password policy for login:
- This system can be seen as acceptable (convenient enough) for the database users.
- At the same time, it can be regarded as reasonably secure because the confidentiality of the personal data is appropriately protected.

### Whitelist approach

In the context of network security, a whitelist approach is an implementation of the concept "Security trumps convenience", refined by the concept "Security is weighed against usability".

A whitelist approach means that only those network device functions shall be enabled that are clearly necessary for the network to function properly. All other device functions shall be disabled.

The functions that need to be disabled may include functions that are enabled in the factory setting, that is, in a device out-of-the-box. Therefore, plan a policy for the necessary functions.

## 1.1.3 Skepticism vs. optimism: qualitative security philosophy

When considering security aspects and the associated concepts of threat risks and mitigation efficiency, people can be associated with two groups:

- People with experience in security often tend to be conservative (skeptical), that is, they tend to give higher weight to security aspects and lower weight to convenience or usability aspects. The reason for that is that security considerations often involve examining seemingly uncritical details that can reveal unexpected threats, surprisingly high risks and unfortunately poor mitigation efficiency, possibly leading to the discovery of several critical, and as-yet, unmitigated vulnerabilities.
  - In a qualitative way, that is, not using a structured approach at all, this can be seen as leading to higher security but can sometimes also lead to poorer convenience or even usability.
- On the other hand, people mainly concerned with usability and convenience, tend to be optimistic, that is, they focus on convenience while at the same time tend to overlook the security aspects of a system. The reason for that is that convenience considerations aim at minimizing the effort (for example, cognitive load) for a user which in turn can unintentionally create or exacerbate vulnerabilities (exploitable threats) in a system.
  - In a qualitative way, that is, not using a structured approach at all, this can be seen as leading to good usability but can sometimes also lead to poor security.

As a consequence, a structured security approach that takes both aspects into account is indispensable.

## 1.1.4 Impartial assessment

**To get an impartial overview over the security of a given or a planned system, an analysis is mandatory.** This analysis typically consists of collecting the perceivable threats, based on a threat model, followed by an assessment of the individual threat risks.

This is typically followed by a collection and then an assessment of the available or perceivable mitigation measures.

The risk of a given threat can be combined with the efficiency of the respective mitigation. This combination can be regarded as a criticality value. This value can guide the priority with which a given threat/mitigation combination shall be pursued and also which mitigation strategy shall be employed.

### 1.1.5 Threat analysis

A thorough and reasonable security concept can only be developed when the threats to the asset under consideration are both known and assessed to a reasonable degree.

In practice, the threats are modeled and assessed in 2 steps:
- Develop a threat model that defines the conditions that in turn help collect and describe the conceivable threats to your system as completely as possible.
  The result is a threat collection.
- Develop a threat assessment concept that defines how to assess the collected threats individually and assign a risk to each threat.
  The result is a threat profile.

**Note:**
Without a threat model, the threat collection is prone to be incomplete, possibly leaving high-risk threats undiscovered.
Without a threat assessment, the threat profile, although possibly complete, is prone to assign unreasonable ad-hoc weight to individual threats. This may result in both high-risk threats going unmitigated as well as unreasonable effort going into the mitigation of minor threats. It also impairs the development of mitigation strategies.

### 1.1.6 Mitigation: confidentiality example

**Confidentiality is often one of the most important aspects of security**. It can be regarded as the property of a system or system component permitting or denying read access to an entity.

Confidentiality can be implemented by erecting one or more barriers for an unauthenticated entity. An unauthenticated entity must first identify and also authenticate itself toward a system that guards the confidential information. Only after the entity is regarded as authenticated, the system allows read access.

Typical mitigation measures (each implementing a barrier) can be:
- Compulsory identification (demanding a username).
- Compulsory authentication (demanding a password associated with the username).
- Measures that impede brute-force attacks, for example, by denying login access attempts for a given time after a number of successive failed login attempts.
- Possible additional measures to restrict login attempts to, for example, certain ports, VLANs, management protocols or IP source addresses.

As a consequence, develop an assessment for mitigation measures, and assign an efficiency to the individual mitigation measures in conjunction with the threat profile.

### 1.1.7 Theoretical and practical degrees of security

Even for barriers that provide a high degree of confidentiality, there are limitations:
- Theoretical confidentiality:
  - **Perfect confidentiality is unattainable.**
- Practical confidentiality:
  - **Near-perfect confidentiality can be uneconomical**, for example, if the cost for guarding the information is higher than the assigned price if the respective information is leaked.
  - **Near-perfect confidentiality can be impractical**, for example, if it requires device- and user-specific usernames and very long, truly random, device-specific passwords that users cannot reasonably memorize.

As a consequence, develop an assessment for the efficiency of an individual mitigation measure addressing a specific threat risk.

### 1.1.8 Strategies to provide improved security: confidentiality example

Regarding the above example, there are 2 aspects for achieving confidentiality:
- **Real-world barriers are imperfect**: No single real barrier offers perfect confidentiality.
- **Mitigation strategies may be required**:
  - **Defense in depth**: Single barriers can be combined (chained along the attacker's intended access path).
  - **Hardening**: Barriers (single or combined) can be implemented on several, parallel access paths, so a strong barrier cannot be circumvented by exploiting another, weaker, barrier.

As a consequence, develop an assessment for the criticality of a given threat risk in conjunction with the associated mitigation's efficiency. Also assess which critical thread risk/mitigation efficiency combinations need to be combined with other thread risk/mitigation combinations, for defense in depth. The resulting overview is also suitable for picking less critical thread risk/ mitigation efficiency combinations as possible targets for hardening.

### 1.1.9 Skepticism: Approximations in this document

In this document, approximations are sometimes used. The goal is to make the security considerations more practical and concise as opposed to a theoretical approach that may be more exact but impractical to implement.

When approximations are used, they typically tend to the skeptical side. That is, in case of doubt:
- Threat exploitability is considered easier (making the threat more likely).
- Threat exploit severity is considered higher (making a breach more dangerous).
- As a result, threat risks are considered higher.
- Mitigation effort is considered higher (making mitigation harder).
- Mitigation effectiveness is considered lower (making mitigation less worthwhile).
- As a result, mitigation efficiency is considered lower.
- The criticality (threat risk combined with mitigation efficiency) is considered more critical.

# 1.2 Overview

## 1.2.1 Subject

The "Security" user manual contains:

- Specific security considerations and actions to help secure your network device (see on page 59 “Device security in the life cycle phases”)
- Specific security considerations and actions which enable a secured network device to help support and enhance the security and availability of your network (see on page 101 “Network security support”)

It deals with the following life cycle phases of your network device:

- Secure installation (see on page 63 “Suggested installation step sequence”)
- Secure setup (see on page 72 “Security setup overview”)
- Secure operation (see on page 94 “Operation”)
- Secure maintenance (see on page 95 “Maintenance”)
- Secure replacement (see on page 96 “Device hardware replacement”)
- Secure repair (see on page 97 “Device hardware repair”)
- Secure decommissioning (see on page 99 “Device decommissioning”)

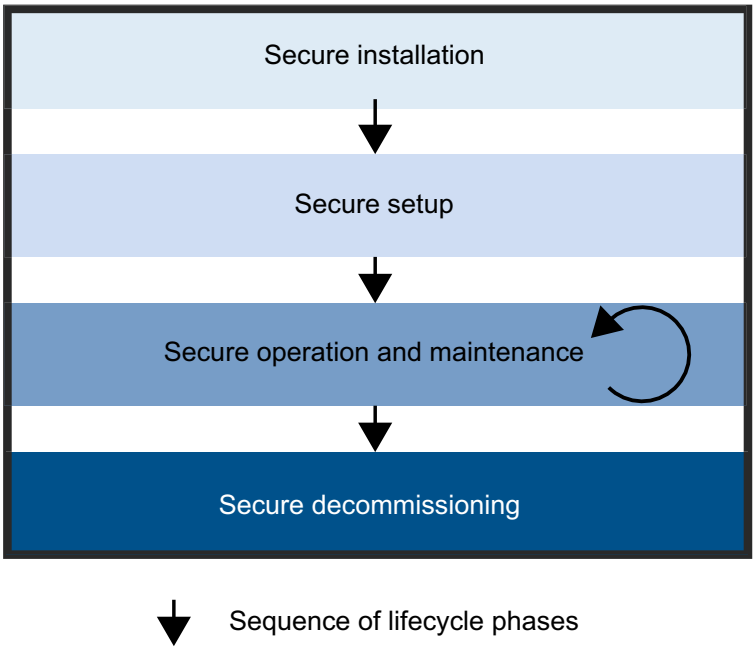



*Figure 1: Device life cycle overview*

## 1.2.2 Scope

This document deals with device security measures throughout the device life cycle. These measures build the base for the following overarching concepts:

- Security planning:
  - Assessing the threat risk, the mitigation efficiency, and the resulting criticality
  - Defense in depth for the device
  - Hardening the device

- Device security in the life cycle phases:
  - Specifically set up and deploy the device to help achieve defense in depth for your system
  - Specifically set up and deploy the device to help harden your system
- Network security support:
  - Specifically set up and deploy the device to support the security and availability of your network

A network device is part of a superordinate system. Therefore, the device and the system are interdependent. The system life cycle and the requirements of the system for defense in depth are outside the scope of this document. References to the system life cycle are made only if necessary, and only for information purposes.

**Note:**
For your network, additional planning and implementation steps may be required. For example, you may need a Layer 3 (L3) network plan in addition to the VLAN plan mentioned in this document. The L3 network plan and the VLAN plan are both outside the scope of this document.

### 1.2.3 Capability security levels

The general security level addressed in this document is the IEC 62443 Capability Security Level 1 (SL-C1). SL-C1 means protection against casual or coincidental access by unauthenticated entities. Content conforming to SL-C1 is not marked up.

Content conforming to SL-C2 or higher is marked up, for example, with <SL-C2>.

### 1.2.4 Required preparatory work

This manual focuses on the security measures for your network device and how a secured device can help maintain the security and availability of your system.

To be effective, these measures need a solid base. The prerequisite for working through this manual is that you have already performed the required high-level security planning steps.

These planning steps may include:
- ☐ Research standards that are applicable to your situation, for example, IEC 62443.
- ☐ Define your system scope.
- ☐ Define the security zones in your system.
- ☐ Define the required subsystem and device functions in each zone.
- ☐ Compile the threats to the individual system zones.
- ☐ Assess the threats' properties (yielding the threats' risks).
- ☐ Compile a threat profile per zone.
- ☐ Contextualize your threat profile with regard to applicable standards.
- ☐ Collect mitigation measures (create a pool).
- ☐ Assess the mitigation measures' properties (yielding the mitigation measures' efficiencies).
- ☐ Associate the mitigation measures with the threat profile.
- ☐ Develop a mitigation strategy.
- ☐ Develop an overarching system security concept.
- ☐ Develop a defense in depth concept.
- ☐ Develop a hardening concept.

**Note:**
Depending on your circumstances, additional or different steps may be required.

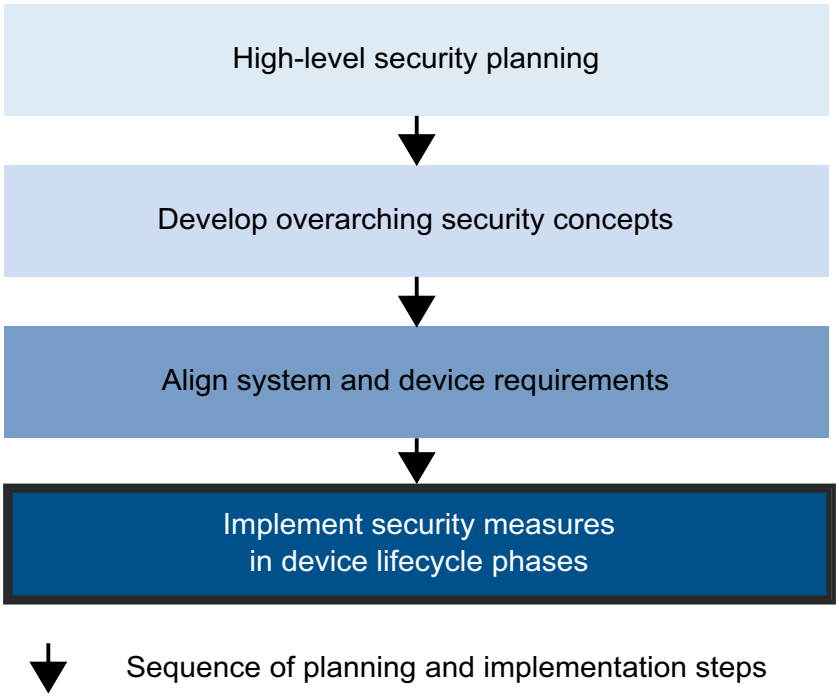



*Figure 2: Required preparatory work hierarchy before implementation*

The overarching system security concept may include:

Hardware-related concepts:
- [NDR3.13] Checking the security seal of a device
- A suitable physical location for the device
- Possible restrictions to the device's hardware interfaces
- A decommissioning policy [CR4.2]

Setup- (Software-) related concepts [CR7.6]:
- Concepts for helping secure the device itself:
  - A secure boot policy <SL-C2>
  - A user account login policy
  - A user account password policy
  - A user account and access role policy
  - A secure management protocol policy [CR7.7]
  - An SNMPv3 authentication and encryption types policy
  - An SNMPv3 trap password policy
  - A remote logging policy
  - A fall-back policy for protocols that offer fall-back
- Concepts for helping secure the network through device functions:
  - An LLDP policy <SL-C2>

Organizational concepts:
- Network time synchronization considerations <SL-C2>
- Software update and configuration server considerations <SL-C2>
- Authentication server considerations <SL-C2>
- Logging server considerations <SL-C2>
- A backup policy for device-related data [SR7.3] [SR7.3 RE1] [CR7.3]
- A policy for device hardware replacement and repair [CR7.4]

**Note:**
This manual refers to individual overarching security concepts when required. However, the details of developing the security concepts themselves are outside the scope of this document.

### 1.2.5 Software setup scenarios and hardware scenarios

The software setup scenario consists of the required software setup steps. A particular software scenario typically has a specific hardware scenario as its base.

The hardware scenario consists of a secure installation location, and of possible device hardware interface access restrictions.

**Note:**
A hardware scenario can by itself help mitigate a considerable part of the threats.
The hardware scenario planning is required as a base for the software setup planning. A specific hardware scenario base can make the planning and deployment of the software setup steps significantly easier.
When planning device security, the hardware scenario is typically planned first, followed by the software setup scenario. The practical implementation sequence may deviate from the planning sequence.

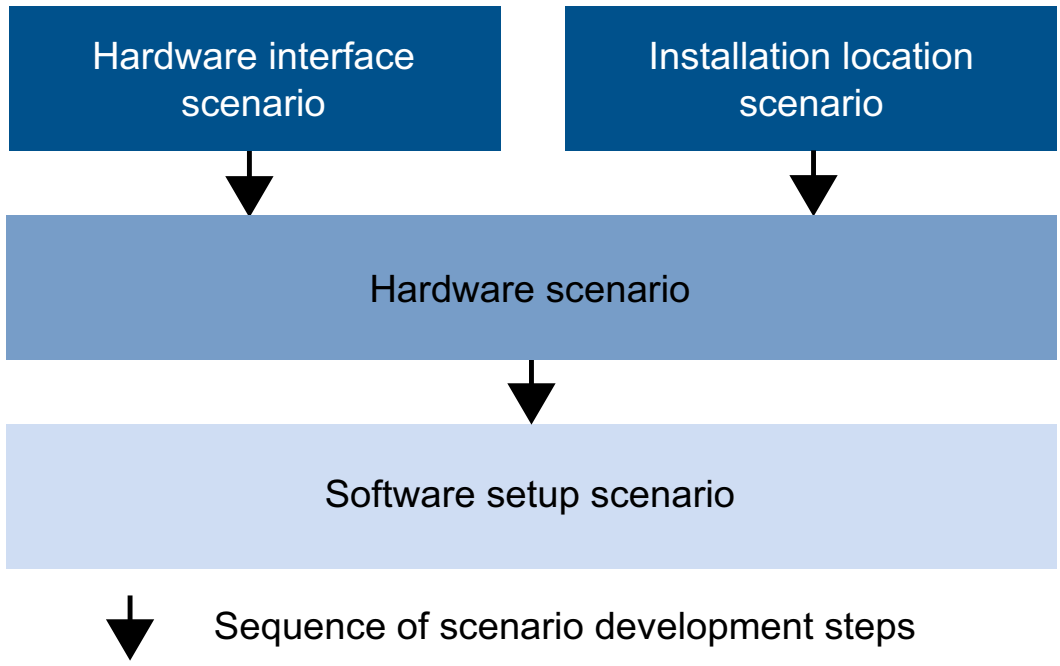



*Figure 3: Basic scenario development steps*

### 1.2.6 Scenario development

To develop a scenario (eventually represented by a set of hardware or software setup steps), typically a structured approach is taken. The steps of this approach are outlined in the following chapters:

- Gathering threats to compile a threat collection
- Assessing the threat risks to compile a threat profile
- Gathering mitigation measures to create a mitigation pool
- Assessing the mitigation measure efficiencies to develop a mitigation strategy
- Selecting mitigation measures for defense in depth
- Selecting mitigation measures for hardening

Consider using software tools that support you in these steps.

# 1.3 Compiling a threat profile

An individual threat profile for a device typically results from the specific user scenario (a collection of use cases) for the device.

The user scenario is defined by the following circumstances which are part of the threat model:
- the physical position of the device on the site
- the logical position of the device in the network
- the required functions of the device
- other functions of the device that are not required, but exist and may pose a vulnerability

When you compile the threat profile, determine the following aspects for each individual threat:
- Exploitability: How hard it is to exploit the individual threat
- Exploit severity: How significant the effects of an exploitation are

For gaining a better overview of the individual threats, you can assess the risk for an individual threat by combining exploitability and exploit severity.

## 1.3.1 Risk value and unit

A concrete, individual risk has a value and a unit:
- A risk can take on any positive, continuous, nonzero value.
- The unit of a risk depends on which risk you are considering. All risks include a probability (which has no unit) relating to a given time period (which has the unit of time). When combining these units, a risk has the unit of a rate, for example, a probability rate of 1% / year or 1 / 100 years.
  - Some risks can be reasonably associated with money, for example, the amount of money needed to restore lost data. Risks of this type, for example, can have the unit EUR / year, and an example value could be 10 EUR / year.
  - Other risks (for example, bodily injury or loss of reputation) cannot be assigned a straightforward amount of money. For risks of this type, it may be advisable to explicitly keep the unit of the individual risk together with the probability and the time period. For example, such a risk could have the unit "probability of light bodily injury per year" and an example value could be "probability of light bodily injury: 10 ppm / year".

**Note:**
The two types of risks (monetary and non-monetary) cannot be compared or combined directly because their units do not match. One possible approach to compare or combine them indirectly is to multiply the non-monetary residual risks by an explicit factor, resulting in a unit of money per time period. The factor should represent a very conservative approach to converting non-monetary risks (for example, personal injury) to monetary risks. This can be a demanding ethical assessment. There is no technical solution.

### 1.3.2 Assess the risk of an individual threat

The risk of a threat is determined both by its exploitability and by the severity of the effects of an exploit. These aspects can be summed up in a threat risk matrix. This matrix concentrates a 2-dimensional set of 9 possible combinations into a one-dimensional index of 5 values.

*Table 4: Threat risk matrix*

| | **Exploitability** | | |
|---|---|---|---|
| **Exploit severity** | Easy | Medium-hard | Hard |
| High | **5**: Very high risk | 4: High risk | **3**: Medium risk |
| Medium | **4**: High risk | **3**: Medium risk | 2: Low risk |
| Low | **3**: Medium risk | **2**: Low risk | **1**: Very low risk |

**Note:**
This matrix is intended to provide basic guidance on how to assess a threat's risk. Your actual situation may require a different assessment approach.

*Table 5: Examples for threat exploitability*

| **Threat** | **Exploitability** | **Remarks** |
|---|---|---|
| Telnet access to the device management is possible. | Easy | Telnet offers no confidentiality, no integrity, and no authenticity. |
| SSH access to the device management has weak password. | Medium-hard | Dictionary or brute-force attack needed for exploit. |
| The device LEDS on front panel are visible. | Hard | An observer can infer a small part of the device and port status. |

**Note:**
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of threat exploitability.

*Table 6: Examples for threat exploit severity*

| **Threat** | **Exploit severity** | **Remarks** |
|---|---|---|
| Attacker has access to the device management | High | Attacker can circumvent confidentiality, integrity and authenticity of sensitive information. |
| Attacker abuses a loop guard on a specific segment | Medium | Attacker can execute a Denial of Service (DoS) attack on this segment. |
| Attacker can create arbitrary Syslog messages | Low | Attacker can create false Syslog entries. |

**Note:**
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of exploit severity.

# 1.4 Defense in depth

## 1.4.1 Introduction

The concept of defense in depth is presented here because it is useful and even necessary for planning the mitigation strategies that are introduced later.

The same applies to the complementary concept of hardening.

## 1.4.2 Purpose

Defense in depth is a strategic concept that employs various independent security (that is, mitigation) measures to guard an asset under consideration against specific threats, as summed up in a threat profile.

A system that employs defense in depth first confronts an attacker with a particular barrier. If an attacker overcomes this barrier, the system presents another barrier of a different type. This layered security approach is considered best practice. It potentially demoralizes an attacker while taking the imperfection of real-world security barriers into account.

**Note:**
Implementing at least 2 barriers may require additional mitigation steps than those resulting from the particular user scenario part that the threat profile is based on. These additional mitigation steps could be taken from another part of the user scenario.
If no additional mitigation measures readily exist, this may be a sign that your user scenario or your mitigation strategy needs enhancement. You may then be required to plan for additional mitigation measures.

## 1.4.3 Defense in depth vs. hardening

In comparison to hardening, defense in depth is a more selective and structured approach. Defense in depth employs a specific subset of all conceivable security measures.

Hardening can be characterized as defense in broad. It aims at closing as many weaknesses in any barriers as possible and reasonable. When you are planning a mitigation strategy, use the concept of defense in depth first and deduce a plan with particular mitigation measures. Then consider complementing the plan by using additional hardening measures.

Implementing hardening measures may also help to establish additional barriers in the context of defense in depth. This way, implementing hardening measures steps can also enhance the defense in depth measures. Therefore, hardening measures, although more general in nature, can be efficient.

A strategic approach to hardening may include the concepts:
- Least required privileges – for the device user accounts
- Least required device functions – for the device security
- Least required device functions – for the network security support

### 1.4.4 Responsibilities

Defense in depth and hardening both require planning, implementation, and maintenance. The system operator is responsible for performing these steps.

To help secure your system, consider the security measures provided in this manual. Select those that are most relevant for your specific situation.

### 1.4.5 Defense in depth example

An attacker is supposed to be connected to a company's industrial network. The asset under consideration is an industrial Ethernet switch in a production cell. The goal of the attacker is to gain access to the device management. The following graphic shows a possible arrangement of device-level barriers in a simplified way.

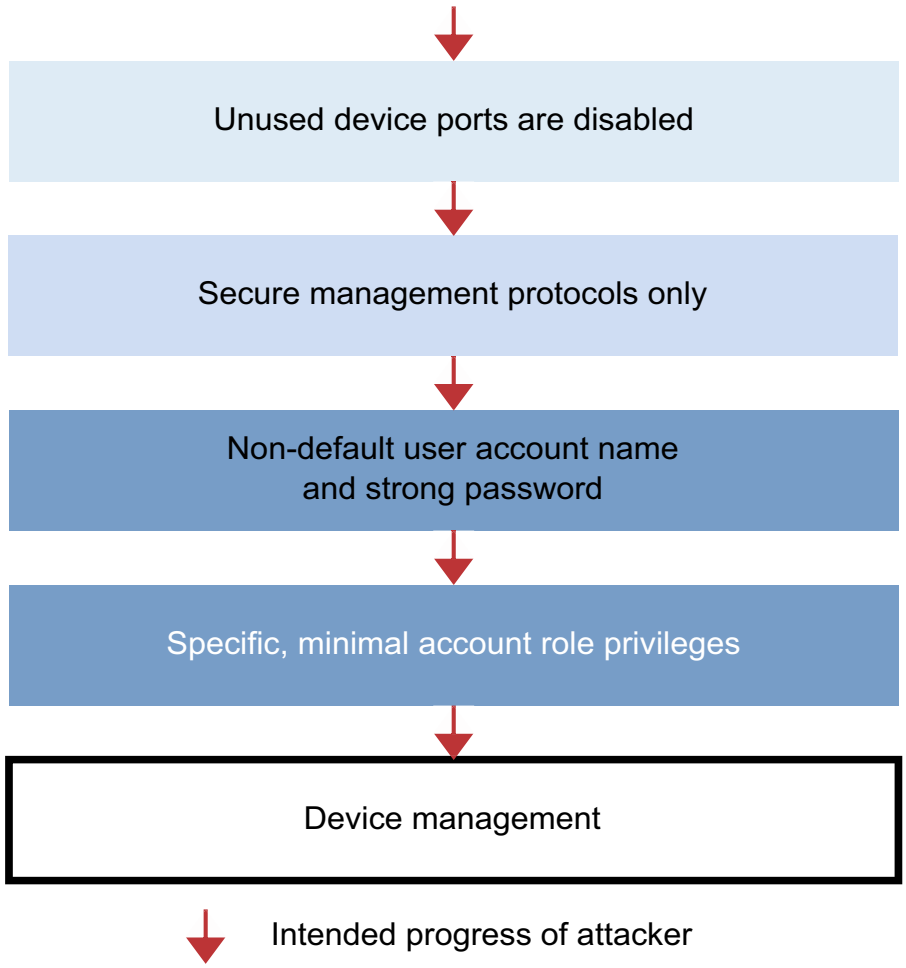



*Figure 4: Barrier arrangement example for defense in depth*

### A more detailed example

The attacker is supposed to be connected to the company's industrial network (1). In more general cases, the attacker may instead be connected to the company Intranet (b) to the Internet (a).

*Table 7: Defense in depth barriers example*

| ID | Barrier | Description |
|---|---|---|
| | **System level** | |
| a | Internet Firewall | The attacker must overcome the firewall between the Internet and the company Intranet to get access to the company Intranet. |
| b | Industrial Firewall | The attacker must overcome the industrial firewall to get access to the industrial network. The industrial firewall separates the industrial network from the company Intranet. |
| 1 | Dedicated device management VLAN | The attacker must overcome VLAN restrictions to snoop or inject packets. |
| | **Device level** | |
| 2 | Secure management protocols only | The attacker must overcome encryption to snoop or create packet contents. |
| 2a | Non-default user account name[1] | The attacker must perform a brute-force attack to find the real user account name. |
| 2b | Strong password[2] | The attacker must perform a brute-force attack to find the real password. |
| 3 | Specific, restricted account privileges | To read privileged data or manipulate device settings, the attacker must perform a dictionary or brute-force attack to find the real administrator account credentials. |

1. A dedicated user account name can be device-specific and could be intentionally chosen to be non-descriptive.
2. A password can be specific to a certain access protocol (for example HTTPS) and can also be device-specific.

# 1.5 Developing a mitigation strategy

To build a mitigation strategy, first develop a pool of conceivable mitigation measures. Then assess the mitigation measures' efficiencies to develop a mitigation strategy.

When you develop a mitigation strategy, determine the following aspects for each individual mitigation measure:

- Effort: How much effort it takes to implement an individual mitigation measure
- Effectiveness: How effective the individual mitigation measure is in reducing or eliminating the threat

To gain a better overview on the individual mitigation measures, you can determine the efficiency for an individual mitigation measure by combining effort and effectiveness.

## 1.5.1 Assess the efficiency of an individual mitigation measure

The efficiency of a mitigation measure is determined both by the required mitigation effort and by the mitigation's effectiveness. These aspects can be summed up in a mitigation efficiency matrix. This matrix concentrates a 2-dimensional set of 9 possible combinations into a one-dimensional index of 5 values.

*Table 8: Mitigation efficiency matrix*

| | **Effort** | | |
|---|---|---|---|
| **Effectiveness** | Small | Moderate | Big |
| High | **A**: Very high efficiency | **B**: High efficiency | **C**: High efficiency |
| Medium | **B**: High efficiency | **C**: Medium efficiency | **D**: Low efficiency |
| Low | **C**: Medium efficiency | **D**: Low efficiency | **E**: Very low efficiency |

**Note:**
This matrix is intended to provide basic guidance on how to assess a mitigation measure's efficiency. Your actual situation may require a different assessment approach.

*Table 9: Examples for mitigation efforts*

| Mitigation measure | Effort | Remarks |
|---|---|---|
| Disable Telnet access. | Small | Telnet access has a simple, binary, setting. |
| Set up restrictions to device management, by protocol and IP address range. | Moderate | The restrictions consist of a number of tabular settings and require an L3 network plan. |
| Create individual and CA-signed HTTPS certificates for each device. | Big | Generating private/public key pairs requires high-quality entropy and possibly dedicated hardware. Signing the individual keys by a certificate authority (CA) additionally requires a public key infrastructure (PKI). |

**Note:**
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of mitigation effort.

*Table 10: Examples for mitigation effectiveness*

| Mitigation measure | Effectiveness | Remarks |
|---|---|---|
| Set the waiting period after a number of successive failed device management logins to >0. | High | The mitigated attack rate of a dictionary or a brute-force attack is significantly lowered. |
| Define a VLAN dedicated to device management access. | Medium | Flooded unknown unicast frames of the device management traffic are confined to the respective VLAN and cannot be intercepted from other VLANs. |
| Set up the CLI post-login banner with only the minimal information required. | Low | The restricted information applies to a situation when an attacker has already succeeded in logging in. |

**Note:**
These examples are intended to provide basic guidance and are non-exhaustive. Your actual situation may require a different classification of mitigation effectiveness.

### 1.5.2 Mitigation efficiency value and unit

The efficiency of a concrete, individual mitigation measure can take on a value in the range $0 \leq x \leq 1$. It has no unit, so it can be regarded as a factor.

A very high mitigation efficiency means a value close to 1, and a very low mitigation efficiency means a value close to 0. In theory, a mitigation efficiency of 1 means that the individual mitigation measure completely eliminates the associated risk, and 0 means that the individual mitigation measure has no effect at all.

If we define the risk reduction factor as (1 - mitigation efficiency), we see that the greater the mitigation effectiveness, the smaller the risk mitigation factor.

### 1.5.3 Alternatives to mitigation

From a business-global view, there are alternatives to threat mitigation:

- **Risk acceptance:**
  - If the risk of a threat seems acceptable, a business may choose not to deploy any mitigation measures.
  - An example may be the leaking of unimportant data from a public system. The monetary risk of such a leak may be considered much lower than the monetary effort to secure the public system. As a consequence, a business may chose to accept the risk.
  - In this document, the acceptance of a risk is implicitly dealt with when considering the residual risk. If the risk of an unmitigated threat is lower than the accepted risk, the threat may be considered as acceptable.

- **Risk avoidance:**
  - If a business process that has a risk associated can be avoided, the risk is also avoided. In terms of technical systems, this translates into not setting up certain network or device functions.
  - An example may be that an internal system with business-critical data will not be connected to a public network but the subset of data intended to be publicly accessible is placed on another, dedicated system. The transfer of the publicly accessible data subset is then performed by a system that is only active while the transfer is performed. This avoids the permanent risk of leaking business-critical data from the internal system.
  - In this document, the avoidance of a risk is implicitly dealt with when excluding a device or network function from implementation because the risk cannot reasonably be mitigated.
- **Risk transference:**
  - In broad business terms, a certain business risk can be transferred to a third party.
  - An example can be buying insurance against the risk of fire in a data center. The risk of fire can never be completely ruled out, so it may reasonably to buy insurance.
  - Risk transference is outside the scope of this document.

**Note:**
This document focuses on technical mitigation measures, and does not detail the above alternatives to mitigation.

# 1.6 Criticality assessment and mitigation strategies

## 1.6.1 Mitigation calculation

Applying a concrete mitigation measure to counter an individual risk can be modeled by multiplying the risk value by the risk reduction factor (1 - mitigation efficiency), resulting in a smaller, residual risk.

If 2 or more mitigation measures to address the same risk are independent of each other (that is, they do not influence each other), the combined risk reduction factor can be calculated by multiplying the individual risk reduction factors. This is the numeric background of the general recommendation to combine mitigation measures if required or possible.

**Note:**
When you combine 2 or more mitigation measures to address the same risk, the mitigations may influence each other. That is, the risk reduction factor may be higher or lower than the calculation of the combined mitigation efficiency (1 - mitigation efficiency$_1$) × (1 - mitigation efficiency$_2$) would give.
Therefore, when you combine mitigation measures, check if you have to consider the combined mitigation efficiencies individually.

## 1.6.2 Combining threat risk and mitigation efficiency

The risk of an individual threat, combined with the efficiency of a specific mitigation measure, can be summed up in a criticality matrix. This matrix concentrates a 2-dimensional set of 25 possible combinations into a one-dimensional index of 9 values.

*Table 11: Criticality matrix matrix (threat risk and mitigation efficiency combined)*

| | **Threat risk** | | | | |
|---|---|---|---|---|---|
| **Mitigation efficiency** | **5**: Very high | **4**: High | **3**: Medium | **2**: Low | **1**: Very low |
| **E**: Very low efficiency | (1) | (2) | (3) | (4) | (5) |
| **D**: Low efficiency | (2) | (3) | (4) | (5) | (6) |
| **C**: Medium efficiency | (3) | (4) | (5) | (6) | (7) |
| **B**: High efficiency | (4) | (5) | (6) | (7) | (8) |
| **A**: Very high efficiency | (5) | (6) | (7) | (8) | (9) |

**Note:**
This matrix is intended to provide basic guidance on how to assess the combination of a particular threat's risk with respect to a particular mitigation measure's efficiency. Your actual situation may require a different criticality assessment.

The criticality value is an index of the urgency of a given threat/mitigation combination. It can also be used to evaluate:
- The possible necessity for defense in depth
- Hints for possible hardening measures

### 1.6.3 Recommended mitigation strategies

**Note:**
The following table is intended to provide basic guidance on how to mitigate a given criticality (the combination of the threat risk and the mitigation efficiency).
You actual situation may require a different mitigation classification for any given criticality.
In fact, when assigning a mitigation strategy to a given criticality, you have considerable leeway to create a solution tailored to your situation.

*Table 12: Criticality and recommended associated mitigation strategies*

| Criticality | Combination with another mitigation for the same threat |
|---|---|
| (1) | **Defense in depth required**: ≥2 other mitigation measures of same or higher efficiency |
| (2) | **Defense in depth required**: ≥1 other mitigation measure of same or higher efficiency |
| (3) | **Defense in depth required**: 1 other mitigation measure of same or higher efficiency |
| (4) | **Defense in depth recommended**: 1 other mitigation measure of same or higher efficiency |
| (5) | **Defense in depth recommended**: 1 other mitigation measure of same or higher efficiency |
| (6) | **Hardening recommended**: 1 other mitigation measure of same or higher efficiency |
| (7) | **Hardening recommended**: 1 other mitigation measure of same or higher efficiency |
| (8) | **Hardening optional**: 1 other mitigation measure |
| (9) | **Hardening optional**: 1 other mitigation measure |

### 1.6.4 Residual risk

This residual risk per threat is the main outcome of the threat analysis and the applied mitigation strategy. The residual risk can take on any positive, nonzero value, that is, it is a continuous value.

**Note:**
For the unit of the residual risk, as well as how to combine different residual risk values (see on page 25 “Risk value and unit”)

### 1.6.5 Security viewpoints: binary or continuous values

The security of a system under consideration, with respect to a defined threat and defined circumstances (like operation and maintenance), can be viewed in two different ways:
- Security can be regarded as a continuous value (the residual risk can take on any value).
- Security can be regarded as a binary value (security is either given or not).

When viewed as a continuous value (derived from or identical to the residual risk), security can be improved gradually if the residual risk can be lowered.

When viewed as a binary value (security is either given or not), security is the result of comparing the residual risk to the maximum accepted risk for that given residual risk:
- Security is given if the residual risk is below or equal to the maximum accepted risk.
- Security is not given if the residual risk is higher than the maximum accepted risk.
- From this viewpoint, and strictly speaking, security, once given, cannot be improved.

### Meaning of "improving the security"

When documents use phrases like "improving the security", this can have two meanings:
- For security as a continuous value, it means lowering the residual risk.
- For security as a binary value, it means having a secure system even after lowering the maximum accepted risk. This is typically achieved by lowering the residual risk.

In practice, a phrase like "improving the security" often has the meaning "lowering the residual risk".

# 1.7 Cryptographic key and password basics

The setup and operation of a network device typically involves the use of cryptographic keys and passwords.

An example of an asymmetric cryptographic key is:
- SSH server keys

Examples of passwords are:
- User account passwords
- SNMPv3 passwords
- The configuration encryption password
- User passwords for the Integrated Authentication Server (IAS)
- SNMPv3 trap passwords

## 1.7.1 Cryptographic key policies

Cryptographic keys are used for two different types of cryptographic algorithms:
- Symmetric cryptographic algorithms
- Asymmetric cryptographic algorithms (also called public key algorithms)

The properties of symmetric and asymmetric algorithms are very different, and therefore, the properties of the respective keys are also different. This is why the recommended policies for generating the keys applies to different aspects:

*Table 13: Comparison between symmetric and asymmetric cryptographic keys*

| Aspect | Symmetric cryptographic keys | Asymmetric cryptographic keys |
|---|---|---|
| Key properties | 1 key (used for encryption as well as decryption) | 2 keys (key pair):<br>• Private key:<br>– Must be kept secret<br>– For decryption or signing<br>• Public key:<br>– Publicly available<br>– For encryption or signature check |
| Key content | Essentially a large random number, need not be prime. | • Private key: 2 separate large prime numbers<br>• Public key: Product of the private key's prime numbers |
| Typical key generation | Manually or automated (recommended) | Automated (compulsory) |
| Different key policy subjects | Key generation | Key signing |
| Common key policy subjects | Distribution, and rotation | Distribution, and rotation |

For both cryptography types, this document gives general policy recommendations for key distribution and rotation.

For symmetric cryptography keys, this document also gives detailed policy recommendations for key generation (see the following chapter).

For asymmetric cryptography, the policy details for key generation and signing are outside the scope of this document.

### 1.7.2 Password and cryptographic key comparison

From a cryptographic viewpoint, symmetric cryptography keys can be considered a subset (special case) of passwords.

**Note:**
For asymmetric cryptography, the comparison between passwords and keys does not apply.

*Table 14: Comparison between passwords and symmetric cryptographic keys*

| Property | Passwords | Symmetric cryptographic keys |
|---|---|---|
| Representation | ASCII string (in most cases) | • Hexadecimal<br>• Base64-encoded<br>• ASCII string |
| Length (representation) | Variable (allowed length range) | • Variable (allowed length range)<br>• Fixed |
| Length (internal) | • Variable (when stored as value)<br>• Fixed (when stored as hash) | Fixed |
| Creation | Manually by human users (in most cases) | • Automated, by dedicated software tools or systems<br>• Manually by human users |
| Strength | Strength depends strongly on the enforced password policy. Without an enforced password policy, strength may be poor. | • Automated creation: High strength<br>• Manual creation: Strength depends strongly on the enforced policy. Without a policy, strength may be poor. |

For both passwords and symmetric cryptographic keys entered manually, their the strength depends strongly on the enforced policy. This is why a planning, setting up and enforcing a policy for manually generated passwords and keys is recommended. A policy may include the requirement that passwords or keys be generated by a specialized application.

For details on the strength of manually generated passwords (see on page 121 “Password strength and policy guide”).

For symmetric cryptographic keys, an automated generation is recommended. In cases where a key is entered manually, following a policy is highly recommended (see on page 145 “Considerations for manually entered keys”).

# 1.8 Impact of the system life cycle on the device life cycle

A network device is a component of the superordinate system. Therefore, the system life cycle determines parts of the device life cycle. A system life cycle involves a planning phase. The decisions taken in the planning phase affect the device life cycle directly or indirectly.

Typical decisions during system planning include:
- The physical location of the device, for example, its installation location and the location's environmental conditions
- The logical position of the device, for example, the security zone
- The requirements of the system for defense in depth

## 1.8.1 VLAN plan

[SR5.1] [CR5.1]

VLANs are a software-configurable concept to segregate a LAN (Layer 1) into separate Virtual LANs (VLANs) on Layer 2. Advantages include the separation of data packets belonging to different VLANs. The separation also applies to flooded multicast, broadcast, and unknown unicast frames. This helps confidentiality and also helps reduce the network load on Layer 1.

A VLAN plan, including a dedicated device management VLAN, is considered a prerequisite for a secure setup of the device itself, and in turn for the security and availability of your system. Create a VLAN plan that segregates your network on Layer 2. A dedicated management VLAN can be a barrier component in the strategy "Defense in depth".

For small networks with few communication relations, a VLAN plan and the setup of VLANs may be considered unnecessary from a functional perspective. However, from a security perspective, VLANs can be useful or even required.

**Note:**
For your network, additional planning and implementation steps may be required. For example, you may need an L3 network plan in addition to the VLAN plan. Both the L3 network plan and the VLAN plan are outside the scope of this manual.

# 1.9 Impact of device requirements on system planning

Some requirements of the device have an impact on the system life cycle phases, in particular on system planning.

Topics of this interdependence include:
- A secure installation location, including the aspects:
  - Device availability: Power supply [SR7.5], PoE power budget, and data link redundancy
  - Properties of the USB port
  - Properties of the media module slots
  - Properties of the signal contact
  - Device and port LEDs
- The detailed physical device security requirements, in particular of its hardware interfaces
- The user account policy parameters the device offers:
  - For the login policy
  - For the password policy
  - For the username and access role policy
  - For the SNMPv3 authentication and encryption type, and password policy
- Configuration encryption and the associated password
- Advanced user authentication measures like 802.1X, a dedicated authentication policy list or RADIUS: These measures require planning for the client in the device and may also require planning for external servers:
  - Plan the 802.1X setup [SR2.3] [SR2.3 RE1].
  - Plan the dedicated authentication policy list.
  - Plan the RADIUS server setup.

**Note:**
These topics are covered in more detail in the following main chapter (see on page 65 “Considering the device availability requirements”).

## 1.9.1 Planning a secure installation location

Select a location that in addition to its physical properties offers appropriate device security by restricting physical access to the device. For example:
- Install the device in a lockable room to which only authorized personnel have access.
- Install the device in a lockable cabinet to which only authorized personnel have access.
- Install the device in a lockable cabinet with a nontransparent door.

Refer to the "Installation" user manual for a suitable physical installation location:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

### 1.9.2 Planning for device availability

Device availability can be an important base for the security of the superordinate system. Check that the following device availability requirements are met as required in your situation:

- [SR7.5] Provide a redundant power supply
- Provide an adequate power budget for the device and for PoE
- Provide data link redundancy

### 1.9.3 Planning for Software auto update from the external memory

The device offers to automatically update the device software during system startup. The prerequisites are:

- The external memory function is enabled.
- On the external memory, there is a valid software image in the root directory

Disabling the Software auto update from the external memory can be a reasonable alternative to disabling the external memory function entirely.

For the setup of the Software auto update from the external memory (see on page 77 “Disable the automatic device software update from the external memory (ACA)”).

Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to enable/disable the Software auto update.

### 1.9.4 Planning for SSH key auto upload from the External Memory

The device offers to automatically upload an SSH key during system startup. The prerequisites are:

- The external memory function is enabled.
- On the external memory, there is a valid SSH key in the root directory

Disabling the SSH key auto upload from the external memory can be a reasonable alternative to disabling the external memory function entirely.

For the setup of the SSH key auto upload from the external memory (see on page 78 “Disable the SSH key auto upload from the external memory”).

Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to enable/disable the SSH key auto upload.

### 1.9.5 Planning the Configuration load priority for the external memory

The device offers to assign a priority for the loading of a configuration profile from the external memory.

Setting the Configuration load priority to *disable* for the external memory can be a reasonable alternative to disabling the external memory function entirely.

For the setup of the Configuration load priority for the external memory (see on page 78 “Disable the Configuration load priority for the external memory”).

Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to set the Configuration load priority for the external memory.

### 1.9.6 Planning for signal contact use

If you intend to use the signal contact, consider the following security aspects:
- To help protect the device, connect the signal contact only to a circuit that meets the device requirements.
- To help protect your system, connect the signal contact only to a circuit that does not have explicit security or safety requirements.

For details (see on page 76 “Disable logical access to the signal contact”).

Refer to the "Installation" user manual:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data > Signal contact" for allowed signal contact operating conditions
- Chapter "Installation > Connecting the terminal blocks > Signal contact" for the electrical signal contact connection

### 1.9.7 Planning for device and port LED visibility

The device and port LEDs show important information about the device state and the port states.

If you have high security requirements, consider the following security measures as required to help prevent information leakage:
- Install the device in a cabinet with a nontransparent door.
- Cover or obstruct the LEDs with a removable cover.

Refer to the "Installation" user manual, chapter "Description > Display elements" for the device and port LEDs.

### 1.9.8 Planning how to check the security seal

[NDR3.13]

<SL-C2> [NDR 3.11] [NDR 2.13]

Plan on how the security seal on a new device shall be checked (see on page 117 “Security seal”).

### 1.9.9 Planning restrictions to the device hardware interfaces

The possible modifications discussed here apply exclusively to the external hardware interfaces at the device surface. The intent of these measures is to restrict physical access to particular device hardware interfaces while keeping the device closed.

Plan the restrictions, like covering or obstructing a slot or a port, according to your requirements:
- Restrict physical access to the USB port.
- Restrict physical access to network ports or SFP slots.
- Restrict physical access to empty media module slots.
- Restrict physical access to the signal contact.
- Restrict physical (visual) access to the device LEDs and port LEDs.

Refer to the "Installation" user manual, chapter "Description > Management interfaces" for the hardware interfaces.

### 1.9.10 Planning a secure boot policy <SL-C2>

<SL-C2> [NDR 3.10 RE1] [NDR 3.12] [NDR 3.14 RE1]

The device offers booting only from trustworthy, that is, cryptographically signed software images that have not been tampered with.

**Note:**
The secure boot mode is required for a device setup compliant with SL-C2 and is the recommended boot mode.

The default setting of the secure boot mode is disabled . If the secure boot mode is disabled, the *Security Status* function in the Web-based interface notifies the user.

After the first successful boot from a proper, signed software image, you have the option to enable the secure boot mode. This initial boot process may have been taken place during manufacturing, or it may take place on the customer premises during a device software update.

Before you enable the secure boot mode:
- Check if the device is trustworthy, that is, that it has not been tampered with.
  For details on this check (see on page 117 “Security seal”) and the hardware installation manual.
- Make sure you are OK with using only secure boot-enabled software images in the future, that is, you will not need to downgrade to a non-secure boot-enabled software image.

**Note:**
Once you enable secure boot mode, you cannot disable it again. This means that the device will subsequently only boot from secure boot-enabled software images. Consequently the device will refuse booting from any other software images, including images of older device software releases even if these are perfectly intact and trustworthy but are not secure boot-enabled.

#### Upload of unsigned device software

When the secure boot mode is off, the device offers the possibility to upload an unsigned software image into the device. The default setting *Allow upload of unsigned device software* is enabled ⚠.

**Note:**
If you activate the secure boot mode, the device only accepts signed software images. The device no longer offers the possibility to upload an unsigned software image.

### 1.9.11 Planning a dedicated user account login policy

[SR3.8] [SR3.8 RE1] [SR3.8 RE2] [SR3.8 RE3] [CR1.11] [CR2.5] [CR3.8]

The device lets you set up a login policy for the user accounts.

The login policy applies consists of:
- Login attempts:
  The maximum number of failed user login attempts in a row until the device locks the respective user account
- Minimum password length:
  The minimum password length that the device enforces when changing a password or specifying a new password
- Login attempts period:
  The waiting time before the device auto-unlocks a locked user account

The login policy applies to every user account.

The login policy applies to the following user interfaces and access protocols:
- The Command Line Interface (CLI) using SSH or Telnet
- The Graphical User Interface (GUI) using HTTPS or HTTP

**Note:**
For quantitative information on how to help ensure a secure login policy (see on page 134 “Attack rate mitigation”). For quantitative information on how to provide for hard-to-break passwords (see on page 121 “Password strength and policy guide”).

You can plan the following requirements for the user login:
- Login attempts:
  - For security reasons, plan the value as low as possible but >0.
  - For availability reasons, plan it as high as practical. Chose a value that fits your requirements.
- Minimum password length:
  - For security reasons, plan a value as high as reasonable.
  - Consider the type of password you want to use: High-complexity passwords contain a higher level of entropy than low-complexity passwords of the same length. To achieve a given entropy, low-complexity passwords therefore should be considerably longer than high-complexity passwords.

  - Chose a minimum password length that fits your requirements.
  - For quantitative information on how to ensure hard-to-break passwords (see on page 121 “Password strength and policy guide”).
- Login attempts period:
  - For security reasons, plan the value >0 and as high as reasonable.
  - For availability reasons, plan it as low as practical but >0. Chose a value that fits your requirements.

**Note:**
Access to the CLI using the serial port is exempt from the login policy. Users accessing the CLI through the serial port have an unlimited number of login attempts. These users are also not required to wait for the next login attempt, that is, the Login attempts period does not apply. This helps ensure access to the device management in situations where availability may be critical, and for users who already have physical access to the device.
To help secure your system, develop an overarching user account login policy.

Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device login functions.

### 1.9.12 Planning a dedicated user account password policy

[CR1.7]

The device lets you set up a password policy for the user accounts.

For detailed information on how to ensure hard-to-break passwords (see on page 121 “Password strength and policy guide”).

Consider the type of password you want to use (see on page 128 “Quantitative password strength”):
- High-complexity passwords have the following properties (see on page 128 “High-complexity passwords”):
  - No part of the password can be found in a dictionary
  - Contains ≥1 lowercase characters, ≥1 uppercase characters, ≥1 digits, and ≥1 special characters
- Low-complexity passwords have the following properties (see on page 130 “Low-complexity passwords”):
  - Consist of several words, each of which can be found in a dictionary
  - A punctuation character typically separates the words
  - Allow but do not require uppercase characters, digits, or special characters

High-complexity passwords of a given length contain a higher level of entropy than low-complexity passwords of the same length. To achieve a given entropy, low-complexity passwords should be considerably longer than high-complexity passwords.

**Note:**
High-complexity passwords are more commonly used.

You can set up the following requirements for the password:
- The minimum number of uppercase characters
- The minimum number of lowercase characters

- The minimum number of digits
- The minimum number of special characters

**Note:**
The minimum password length belongs to the user account login policy (see on page 43 “Planning a dedicated user account login policy”).

To help secure your system, develop an overarching user account password policy. When you do, consider the following aspects to deter attackers:
- Consider using account names that are non-standard, and are non-descriptive to unauthorized entities.
- Consider using different user account names on different devices.
- Consider using different passwords on different devices, even for user accounts with the same name.
- Consider using different SNMPv3 passwords on different devices.

For the user credentials in the delivery state (see on page 83 “Set up a dedicated user account login policy”).

Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device password policy functions.

### 1.9.13 Planning a dedicated user account name and access role policy for device management

[SR2.1] [SR2.1 RE1] [SR2.1 RE2] [CR1.1 RE1] [CR1.3] [CR1.4] [CR1.5] [CR2.1 RE1] [CR2.1 RE2]

The device requires each user to identify themselves (by the user account name) and to authenticate themselves (by the associated password). The device associates a specific access role to each user account <SL-C2>.

**Note:**
User account names are case-sensitive.

*Table 15: User account roles and privileges*

| User account role | Privileges |
|---|---|
| `unauthorized` | None: The device refuses login. |
| `guest` | The device permits reading of device management data, except the audit trail. The device refuses any write access to data. |
| `auditor` | The device permits reading of device management data, including the audit trail. The device permits writing the audit trail to a log file, but refuses any other write access. |
| `operator` | The device permits reading and writing of device management data. The device refuses write access to security-relevant settings and the audit trail. |
| `administrator` | The device permits reading and writing of device management data, including security-relevant settings. This device also permits the reading of the audit trail. |

In the delivery state, the device has the following user account preconfigured:

*Table 16: User credentials for the administrator account in the delivery state*

| Username | Password | User account role |
|---|---|---|
| admin | private (May have been changed at first login.) | administrator |

**Note:**
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name user and the associated password public. If you need a user account that has only read access, you can create a user account with the access role guest and assign it the username user, for example.

Set up dedicated user accounts as required:

- Create user accounts with:
  - Dedicated names <SL-C2>
  - Chosen access roles that offer only the least required privileges
  - The password policy check enabled
- Assign the new user accounts strong, individual passwords.
  - Plan strong SNMPv3 authentication and encryption types and strong related passwords for the new user accounts.
- <SL-C2> Remove user accounts with standard names.

**Note:**
To help secure your system, develop an overarching user account and access role policy.
If you have high security requirements, consider planning different user account names and different passwords on different devices. Also consider user account names that are intentionally non-descriptive to unauthorized entities.
If you intend to use SNMPv3, also consider developing an overarching policy for SNMPv3 authentication and encryption types, and the related passwords. If you have high security requirements, consider planning different SNMPv3 passwords on different devices.

Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device user account name and access role functions.

### 1.9.14 Planning configuration encryption and the associated password

Plan a configuration encryption policy:
- Plan if you want to enable the configuration encryption.
- Plan a specific password policy for the configuration encryption password.

**Note:**
Configuration encryption with a password is required for a device setup compliant with SL-C2.

The default setting of the configuration encryption is disabled ⚠. If the configuration encryption is disabled, the *Security Status* function in the Web-based interface notifies the user.

**Note:**
The configuration encryption password can and likely should be different from the user account passwords.
The configuration encryption password is not checked against the user account password policy.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/ Save" for the configuration encryption and the associated password.

### 1.9.15 Planning session timeouts <SL-C2>

Plan finite session timeouts for:
- The Graphical User Interface using HTTPS or HTTP
- The Command Line Interface through the serial port, SSH, or Telnet

ⓘ Refer to the "Graphical User Interface" reference manual:
- Chapter "Device Security > Management access > Web" for the Graphical User Interface timeout function
- Chapter "Device Security > Management access > CLI" for the SSH and serial port timeout function

### 1.9.16 Planning a dedicated logging policy

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR2.8] [CR2.9] [CR2.10] [CR2.12] [CR3.9] [CR6.1] [CR6.2]

Set up the device logging settings:
- Specify the severity levels of events you require to be logged.
- Specify the logging destinations you require, including possible remote logging.

To help secure your system, develop an overarching remote logging policy (see on page 51 “Logging server considerations <SL-C2>”).

**Note:**
The Syslog (system message logging) client in the device offers unencrypted communication only. The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Syslog" for the device Syslog function.

### 1.9.17 Planning a dedicated LLDP policy <SL-C2>

When LLDP is enabled on your device:
- When the LLDP receive function is enabled, the device collects information about its neighbors and provides this information to a management station.
  - The prerequisite is that the other devices in the same network have their individual LLDP send function enabled.
- When the LLDP send function is enabled, the device sends information about itself and its respective port to its neighbors. The neighbors can collect that information and provide it to a management station.
  - The prerequisite is that the other devices in the same network have their individual LLDP receive function enabled.

LLDP can help automate a system inventory. LLDP may also help discover mismatches in port settings, like half-duplex and full-duplex settings, or VLAN settings, of ports connected to each other.

Depending on your security requirements, LLDP may need to be disabled on the device as well as on other network devices. You may also elect to enable only the receive function. The delivery state for LLDP is globally disabled.

For details (see on page 115 “Set up the LLDP parameters <SL-C2>”).

### 1.9.18 Advanced authentication measures <SL-C2>

If you intend to use advanced user authentication measures like 802.1X or a dedicated authentication policy list:
- Plan the 802.1X setup [SR2.3] [SR2.3 RE1].
- Plan the dedicated authentication policy list.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Network security > 802.1X" for the 802.1X function
- Chapter "Device security > Authentication lists" for the dedicated authentication policy list

# 1.10 Impact of network aspects on system planning

## 1.10.1 External server considerations

<SL-C2> [CR 1.9]

To perform its functions, the device may rely on other system components. These system components are internal to the network but external to the device.

Typical examples are:
- Software update and configuration servers
- DHCP servers
- Authentication servers
- Syslog servers

Using these servers can provide extended functionality that is not available in a purely local system concept. Examples for extended functionality are:
- Authentication servers offer various optional parameters, like assigning a VLAN ID to a user.
- Syslog servers offer log entry redundancy and virtually unlimited storage capacity.

For some protocols, like system message logging (Syslog), you can use the remote server in the normal state of operation, and have a fall-back to the local operation should the respective server become unreachable.

**Note:**
If your planned device configuration uses such external system components, consider developing an overarching policy for the external system components.
If you intend to use a fall-back operation for a certain protocol, check if the protocol offers this possibility, and if it is appropriate for your situation. Then develop an overarching policy for the fall-back.

## 1.10.2 Software update and configuration server considerations <SL-C2>

If you intend to use servers for the update of the device software and to distribute device configuration files, plan a host key policy for these servers, possibly including server key rotation.

**Note:**
**These keys typically are asymmetric cryptography keys.**
As such, these keys need a specific key policy.
This policy is different than the policy for keys for symmetric cryptography that is discussed in other locations of this document.

Asymmetric key policy items may include:
- Plan a secure transfer protocol, for example, SFTP or SCP
- Plan the distribution of the server public key fingerprints
- Plan for a rotation of the server keys and the associated fingerprints

### Server key rotation

Server key rotation on a regular basis limits the amount of data encrypted or signed by a specific key. This key can be:

- For asymmetric cryptography (used for example by TLS): The private key of a specific key pair
- For symmetric cryptography (used for example by encrypted SNMPv3 traps): The key that both communications partners share

Given that the key has a non-zero probability of being leaked, key rotation limits the amount of data encrypted or signed by that key:

- Data encrypted by that key may have also been leaked and might subsequently be exposed to decryption by the leaked key. Therefore, key rotation limits the extend of possible decryption exposure.
- For data signed by that key, it limits the amount of data that could have signed by an attacker, thus pretending a trustworthy signature.

Server key rotation means that a specific key will only be user for a limited period and will normally replaced by another key shortly before the period of the given key runs out.

A server key rotation scheme may include the setting up of 2 or more keys per server whose validity periods are adjacent or overlap.

## 1.10.3 External DHCP server considerations

If you intend to use DHCP to obtain the device management IP address or other parameters, plan the DHCP server setup. If you intend to use external DHCP servers, consider developing an overarching DHCP server policy.

**Note:**
The DHCP client implicitly trusts the DHCP server. Depending on your actual situation, assigning a static (that is, locally specified) IP address to the device may be considered more secure than using the DHCP client.

Refer to the "Graphical User Interface" reference manual:

- Chapter "Basic settings > IPv4 > BOOT/DHCP" for the device IPv4 DHCP client function
- Chapter "Basic settings > IPv6 > DHCP" for the device IPv6 DHCP client function

### 1.10.4 Authentication server considerations <SL-C2>

<SL-C2> [CR 1.9]

If you intend to use authentication servers to help the device authenticate users or other system entities, plan the setup of the appropriate authentication servers:
- Plan for the dedicated local authentication policy list to use an external authentication server.
- Plan the external RADIUS server setup.

**Note:**
Depending on your actual situation, setting up only a static, local Integrated Authentication Server (IAS) in the device may be considered more secure than using external authentication servers.
The RADIUS client in the device exclusively offers obfuscated communication. The secure RADIUS protocol establishes mutual trust between the device (the RADIUS client) and the RADIUS server by means of a shared secret.
The unobfuscated protocol version of RADIUS implicitly trusts its servers. If you intend to use remote authentication, consider developing an overarching remote authentication policy and using only the obfuscated RADIUS protocol version.

**Note:**
Encrypted LDAP can be considered preferable over obfuscated RADIUS because encrypted LDAP employ newer and more sophisticated concepts for both establishing trust towards its authentication server and the encryption of the communication.
RADIUS and TACACS+ use obfuscated communication which offers weaker security than encrypted LDAP.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Device security > Authentication lists" for the dedicated authentication policy list
- Chapter "Network security > RADIUS" for the device RADIUS client function

### 1.10.5 Logging server considerations <SL-C2>

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR2.8] [CR2.9] [CR2.10] [CR2.12] [CR3.9] [CR6.1] [CR6.2]

If you intend to use Syslog (system message logging) servers to help keep a complete and persistent log of the events reported by the device, plan the setup of the appropriate external Syslog servers.

<SL-C2> [CR 1.9]

**Note:**
The Syslog client in the device offers unencrypted communication only.
Using Syslog servers offers the advantage of sending the log entries to a remote location different from the device. This helps provide redundancy. It also helps overcome local log capacity constraints on the device.
If you intend to use remote logging, consider developing an overarching remote logging policy.
The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

Refer to the "Graphical User Interface" reference manual:

- Chapter "Diagnostics > Syslog" for the device Syslog function
- Chapter "Diagnostics > Report > Audit trail" for the device Audit trail

# 1.11 Device-related policies

## 1.11.1 Develop a backup policy for device-related data

[SR7.3] [SR7.3 RE1]

Consider developing a backup policy for device-related data. This minimizes your effort for replacing a device if the device becomes inoperable.

This policy may include:
- [SR7.3] [SR7.3 RE1] [CR7.3] [CR7.3 RE1] Creating a backup copy of the device configuration profiles <SL-C2>.
- Keeping the backup files separate from the device in a secure location.
  For example, placing the backup files on a file server in a device-specific folder.
- Including other device-specific data in the same device-specific folder.
  For example, including device-specific private keys or certificates.
- Using a file or folder numbering scheme or even a version control tool to track the device configuration history.

## 1.11.2 Develop a policy for replacing the device hardware

[CR7.4]

<SL-C2> [CR 1.9] [NDR 3.11] [NDR 2.13]

Consider developing a policy for replacing the device hardware.

Topics of this policy may include:
- Which data of the former device shall be backed up to a remote location
- [NDR3.13] How the security seal of the new device shall be checked (see on page 117 “Security seal”)
- Which data of the former device shall be restored to the new device. For example, the following data for the new device may or may not be identical to the former device’s data:
  - User account names and passwords
  - Host keys (public and private) or certificates
- Which software shall be loaded onto the new device. For example, the software on the new device may or may not be identical to the former device’s software:
  - The new device may be of a different device family.
  - The new device may be of a different device generation.
- If the hardware interfaces of the new device shall be restricted

Align the device hardware replacement policy with:
- The hardware repair policy
- The hardware decommissioning policy

## 1.11.3 Develop a policy for device hardware repair

<SL-C2> [CR 1.9]

Consider developing a policy for device hardware repair.

If a device needs repair, consider your actual confidentiality needs regarding the data present on the device:

- The configuration profiles and configuration scripts
- The boot parameters
- The current HTTPS certificate
- The current SSH host key or host key pair
- The current software files
- The configuration profiles on the external memory

Furthermore, consider the following organizational steps:

- For the device hardware, specify:
  - If you expect to get the same device back (identified by the same base MAC address)
  - If you agree to receive another device of identical type (will have a different base MAC address)
  - If you agree to receive a device of another, superior type or generation (will have a different base MAC address and possibly also other properties)
- For the security seal on the device (see on page 117 “Security seal”), specify
  - How you check the security seal’s condition before sending the device to the manufacturer
  - How you check the security seal’s condition after receiving the device back from the manufacturer

### 1.11.4 Develop a policy for device hardware decommissioning

Consider developing a policy for device hardware decommissioning.

Specify which of the following steps to carry out, and how.

**Note:**
Depending on your actual environment, fewer, more or other steps than those listed below may be necessary.

Deletion of confidential data and secrets:

- Reset to the delivery state:
  - Deletes the configuration profiles and configuration scripts in the device
  - Resets the boot parameters
  - Deletes the current HTTPS certificate in the device and creates a new, self-signed HTTPS certificate
  - Deletes the current SSH host key pair in the device and creates a new, self-signed SSH host key pair
  - If the external memory is plugged in, the device also deletes the configuration profiles on the external memory.
- Possible secure wipe (instead or in addition to the reset to the delivery state):
  - Securely overwrite the data and secrets listed in the previous list item, "Reset to the delivery state".
  - If required, securely overwrite the software files in the device.
  - Securely overwrite every configuration profile on a connected external memory.

Secure physical destruction of the device and its accessories:
- Destroy the security seal on the device (see on page 117 “Security seal”).
- Physically destroy the device, including the flash memory chips. This destroys the data and secrets listed in the above list item "Reset to the delivery state".
- If required, physically destroy the external memory.

**Note:**
The reset to the delivery state leaves the audit trail intact.
The reset to the delivery state leaves the secure boot setting intact. <SL-C2>
If you intend to continue using the device, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

For the secure removal of device-related data from the administration environment, perform the following steps. This may include:
- The removal of:
  - Configuration data and its backups
  - Private cryptographic keys
  - Self-signed certificates
- The removal of references to:
  - The device MAC base address
  - The device serial number
  - The device product code

### 1.11.5 Develop a policy for device hardware disposal

Consider developing a policy for device hardware disposal.

If you have high security requirements, consider disposing of the device by shredding it.

# 1.12 Operation and maintenance policy

Develop a policy for operation and maintenance. Such a policy may include:

- Which administrative roles for operating or maintaining the device hardware are required
- Which administrative roles for operating or maintaining the device settings are required, along with specific privileges and responsibilities for each role (see on page 45 “Planning a dedicated user account name and access role policy for device management”).
- A schedule for routine operation and maintenance tasks
- A synchronization with operation or maintenance tasks for superordinate system components
- The extent of the scheduled tasks, for example:
  - Looking for a available software update and evaluating or applying it
  - Performing a check on a set of security-related settings and statuses
  - <SL-C2> [CR 1.9] Performing a server key or certificate rotation and applying the resulting changes to the associated device settings, possibly both before and after the server key or certificate rotation
- The extent of active measures that determine the device security status, like:
  - Checking the security status variable of the device
  - Checking other, selected security-related settings in the device
  - Regular penetration tests
- Manual triggers of an out-of-schedule operation or maintenance task, for example:
  - Because of a change in the device setup
  - Because of an audit
  - Because of the results of a penetration test
  - Because of the manual evaluation of log files
- Automatic triggers of an out-of-schedule operation or maintenance task, for example:
  - Caused by the detected change of the security status variable of the device
  - Caused by the detected change in selected security-related settings and statuses
  - Caused by the automatic evaluation of log files

# 1.13 Document the planned policies

Document the overarching policies. These policies serve as an essential base for planning the individual device configuration and setting up the device.

Depending on your requirements and circumstances, you can plan and maintain the policies with a general software tool (for example, an office spreadsheet or a database application), or use a dedicated software tool.

# 2 Device security in the life cycle phases

## 2.1 Develop the device configuration

Based on your documented overarching policies, plan (develop) the configuration for each considered device. If you follow a whitelist approach, include the necessary function policy from your whitelist policy.

Document the planned configuration for each considered device. This helps to keep track of the system.

This planned configuration per device can be, for example:
- On a generalized level:
  The device needs to have 2 ring ports and 1 uplink port.
- On a concrete level:
  The device needs ports 3 and 4 as MRP ring ports with a data rate of at least 1 Gbit/s, and ports 1 and 2 for the redundant uplink with at least 100 Mbit/s.

Depending on your actual situation, you can either directly deduct the detailed device configuration from the policies, or allocate 2 steps by planning the device configuration on a generalized level first and then detailing it.
- For a small system or system zone, and if you have already decided which device types you will use, it may be appropriate to plan the concrete device configuration directly (deduct it directly from the policies).
- For a large or complex system or system zone, it may be necessary to split the steps:
  - Plan a generalized device configuration first.
  - Decide which concrete device type and variant you want to deploy.
  - Detail the device configuration.

Depending on your requirements and circumstances, you can plan and maintain the device configuration with a general software tool (for example, an office spreadsheet or a database application), or use a dedicated network planning/management tool.

## 2.2 Software vs. hardware measures (logical vs. physical)

This main chapter deals with software setup measures as well as hardware measures.

- The software setup measures are also referred to as logical measures.
  - For example: Disable logical access to unused ports and SFP slots.
  - For example: Disable logical access to the digital input.
- The hardware measures are also referred to as physical measures.
  - For example: Restrict or disable physical access to the USB port.

## 2.3 Security-related vs. general device functions

The software setup measures in this main chapter deal with the security-related setup of device functions throughout the life cycle phases of the device.

The device functions can be divided into three groups:

- Security-related device functions that help secure the device itself:
  The setup of these functions is described in this main chapter (see on page 72 “Security setup overview”).
- Security-related device functions that help secure your system and improve its availability:
  The setup of these functions is described in the following main chapter "Network security support" (see on page 101 “Network security support”).
- General device functions: The setup of the general device functions is outside the scope of this document. If you follow a whitelist approach, include the necessary function policy from your whitelist policy. The necessary function policy may stipulate which general device functions need to be disabled although they are not directly security-related.

  For the general device functions, refer to the detailed manuals:
  - The "Configuration" user manual
  - The "Graphical User Intere" user manual
  - The "Command Line Interface" reference manual
  - The "Installation" user manual (for hardware-related setup steps)

## 2.4 Prerequisites for installation and setup

The prerequisite for working through this section is that you have already performed the system planning steps, including:

- ☐ Planning a suitable physical location for the device (see on page 65 “Choosing a secure installation location”)
- ☐ Planning restrictions to the device hardware interfaces (see on page 42 “Planning restrictions to the device hardware interfaces”)
- ☐ If you follow a whitelist approach, develop a necessary function policy from your whitelist policy. The necessary function policy may stipulate which general device functions need to be disabled although they are not directly security-related.
- ☐ Developing a dedicated user account **login** policy (see on page 43 “Planning a dedicated user account login policy”)
- ☐ Developing a dedicated user account **password** policy (see on page 44 “Planning a dedicated user account password policy”)
- ☐ Developing a dedicated user account and access role policy for device management (see on page 45 “Planning a dedicated user account name and access role policy for device management”)
  - – Developing a dedicated policy for SNMPv3 authentication and encryption types, and for the related passwords
- ☐ Planning configuration encryption <SL-C2> (see on page 47 “Planning configuration encryption and the associated password”)
- ☐ Planning session timeouts <SL-C2> (see on page 47 “Planning session timeouts <SL-C2>”)
- ☐ Developing a dedicated logging policy, possibly including remote logging (see on page 47 “Planning a dedicated logging policy”)
- ☐ Developing a policy for the servers that hold device software updates and configuration files <SL-C2> (see on page 49 “Software update and configuration server considerations <SL-C2>”)
- ☐ Planning a dedicated LLDP policy <SL-C2> (see on page 48 “Planning a dedicated LLDP policy <SL-C2>”)

If required, the following organizational concepts are also part of the above planning work:

- ☐ Network time synchronization considerations <SL-C2>
- ☐ Authentication server considerations <SL-C2>
- ☐ Logging server considerations <SL-C2>
- ☐ A backup policy for device-related data [SR7.3] [SR7.3 RE1]
- ☐ A policy for device hardware replacement

### 2.4.1 Possible further prerequisites

Your network may require further system planning steps, including:

- ☐ Traffic segregation on Layer 2 by a VLAN plan
- ☐ Use of a network management system like Industrial HiVision (optional)

**Note:**
The details of these steps are outside the scope of this document.

# 2.5 Suggested installation step sequence

The steps in the device security life cycle phases in a practical order are:

- ☐ Choose a secure installation location (see on page 65 “Choosing a secure installation location”)
- ☐ Perform the initial software update (see on page 69 “Software update”)
- ☐ Perform the initial security setup (see on page 72 “Security setup overview”)
- ☐ If required, modify the hardware interfaces for security (see on page 91 “Possible restrictions to the device’s hardware interfaces”)
- ☐ Perform the initial device installation (see on page 93 “Device installation”)
- ☐ Operation measures (see on page 94 “Operation”)
- ☐ Maintenance measures (see on page 95 “Maintenance”)
- ☐ Decommissioning measures (see on page 99 “Device decommissioning”)

**Note:**
Depending on your requirements, you may want to perform the steps in a different sequence.

## 2.5.1 Reasons for the suggested installation step sequence

Performing the initial setup and the initial software update before the initial device installation can have the following benefits:

- The required resources, for example, SSH known host fingerprints, prepared device configuration files and device labels, may be more conveniently available in an office location.
- Time-consuming steps like software updates can be performed in parallel.
- Associated devices, for example, devices participating in a ring redundancy, can be set up contiguously.
- For certain hardware measures like physically blocking a USB port, you may need the USB port for the software update and initial setup before you can block the USB port.
- The remaining work steps in the field require less time.

## 2.5.2 Suggested preparation for installation

The following suggested steps and their sequence can help reduce the initial effort and save time:

- ☐ Check the security seal of the device, (see on page 117 “Security seal”).
- ☐ Check the available device software release on the Hirschmann product pages on the Internet at catalog.belden.com.
- ☐ Decide which device software release you want to run on your devices.
- ☐ Download the respective software files.
- ☐ If you want to load the device configuration or update the device software from an SFTP or SCP server, determine the fingerprints of the respective configuration profile or software update servers. Verify that the fingerprints are from a trustworthy source, like the server administrator.

☐ If desired, prepare the individual device configuration files based on the respective planned device configuration. If you want to enable the configuration encryption, (see on page 75 “Options to enable configuration encryption”).
☐ Prepare the device labels.

**Note:**
To help keep your system secure, consider using the latest available release of the device software. If you want to load the device configuration or update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the files (software or configuration files) are cryptographically signed.

**Note:**
Configuration encryption with a password is required for a device setup compliant with SL-C2.

Refer to the "Configuration" user manual:
- Chapter "Loading software updates" for details on how to:
  - Determine the currently running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Check for a newer available software release
  - Update the device software
- Chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts’ public key fingerprints.

# 2.6 Choosing a secure installation location

**Note:**
The prerequisite for working through this section is that you have already performed the planning for a secure installation location (see on page 39 “Planning a secure installation location”).

Select an installation location that in addition to its physical ambient conditions offers appropriate device security by restricting physical access to the device or its hardware interfaces.

Check that the following device security requirements are fulfilled as required:
- Install the device in a room that can be locked and to which only authorized personnel have access.
- Install the device in a lockable cabinet to which only authorized personnel have access.
- Install the device in a lockable cabinet with a nontransparent door (see on page 92 “Restrict physical (visual) access to the device LEDs and port LEDs”).

Refer to the "Installation" user manual for a suitable physical installation location:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

## 2.6.1 Considering the device availability requirements

Device availability can be an important base for the security of the superordinate system. Therefore, also consider implementing measures that increase device availability.

Check that the following device availability requirements are fulfilled, if required:
- [SR7.5] Consider the power supply requirements (see on page 66 “Considering the power supply redundancy requirements”).
- Consider the power budget requirements (see on page 67 “Considering the power budget requirements”).
- Consider the data link redundancy requirements (see on page 68 “Considering the data link redundancy requirements”).

Refer to the "Installation" user manual, chapters "Technical data > Supply voltage" and "Technical data > Power consumption/power output" for the power requirements of the device.

# 2.7 Considering the power supply redundancy requirements

[SR7.5]

Check that the power supply redundancy requirements are fulfilled, if required:
- The device is powered by 2 redundant power sources.
- The power supply cables to the device run along different paths as far as possible.
- The power supplies themselves are powered in a redundant way, for example, by 2 separate mains cables.
- The mains cables to the redundant power supplies run along different paths as far as possible.

Refer to the "Installation" user manual, chapters "Safety instructions > Requirements for connecting the supply voltage" and "Description > Device views > …" for the power supply redundancy aspects of the device.

# 2.8 Considering the power budget requirements

Check that the power requirements are fulfilled as required:

- One single power supply can deliver power for every connected device.
  - Also consider the worst-case power requirements of the inserted SFPs.
  - Also consider the inserted media module worst-case power requirements.
- One single power supply can also deliver the worst-case set-up PoE or PoE+ power. **(depends on hardware)**

**Note:**
The condition "one single power supply" takes the possible failure of one power supply in a dual power supply configuration into account.

Refer to the "Installation" user manual, chapters "Technical data > Supply voltage" and "Technical data > Power consumption/power output" for the power requirements of the device.

## 2.9 Considering the data link redundancy requirements

Check that the data link redundancy requirements are fulfilled as required:

- The device has redundant data links (typically for an upstream connection).
- The cabinet or room has redundant data links.
- The redundant data links of the cabinet or the room run along different paths as far as possible.

# 2.10 Software update

[CR4.3] [NDR3.10] [NDR3.14]

<SL-C2> [NDR 3.10 RE1] [NDR 3.12] [NDR 3.14 RE1]

The following description applies to:
- The initial software update for a device out-of-the-box
- A software update as part of operation or maintenance

Check if an updated release of the device software is available. You find information and software downloads on the Hirschmann product pages on the Internet at catalog.belden.com. Then decide which software release you want to run on your device [NDR 3.10 RE1] <SL-C2>.

## 2.10.1 Initial access to the device management

To update the software on the device, you need management access to the device.

A device out-of-the-box requires at least a preliminary IP address setup. Hirschmann recommends using HiView to assign an IP address setup to the device. After that, HiView allows you to open the Graphical User Interface or the Command Line Interface of the device.

## 2.10.2 Initial password considerations

In the delivery state, the device has the following user account preconfigured:

*Table 17: User credentials for the administrator account in the delivery state*

| Username | Password | User account role | Privileges |
|---|---|---|---|
| `admin` | `private` (May have been changed at first login.) | `administrator` | The device permits the reading and writing of device management data, including security-relevant settings. The device also permits the reading of the audit trail. |

**Note:**
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name `user` and the associated password `public`.
If you need a user account that has only read access, you can create a user account with the access role `guest` and assign it the username `user`, for example.

[CR1.10] At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 44 “Planning a dedicated user account password policy”).

### 2.10.3 Software update server considerations

If you want to update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the software files are cryptographically signed.

If you want to perform the initial software update for a device out-of-the-box and you have the new software image on an SFTP or SCP server, first set up the SSH known host fingerprints in the device (see on page 82 “Set up the SSH Known Hosts fingerprints in the device”). Use the fingerprint of the software update server. This enables the device to decide whether the software update server it contacts is trustworthy or not.

**Note:**
Verify that the server fingerprints are from a trustworthy source, like the server administrator, and that hey have been transferred either in protected form or over a trustworthy network.

### 2.10.4 Secure boot considerations

Before a possible device software update, determine if you need to apply your secure boot policy, if you have one:

- ☐ Check if the current software and its settings belong to one of the following categories:
  - The image has not been cryptographically signed. Such a software image does not offer the secure boot setting.
  - The image has been cryptographically signed but the secure boot mode is disabled.
- ☐ Check if the new software is cryptographically signed.

If **both** of the above statements are true, apply your secure boot policy (see on page 42 “Planning a secure boot policy <SL-C2>”).

**Note:**
If you do not have a secure boot policy, to help you decide whether to enable secure boot on that specific device or not, (see on page 47 “Planning configuration encryption and the associated password”)
The secure boot mode is required for a device setup compliant with SL-C2.

If you decide to upload an unsigned software image to the device, verify that the secure boot mode is disabled and that the setting *Allow upload of unsigned device software* is enabled. In the factory setting, the device allows the upload of an unsigned software image ⚠.

**Note:**
If you enable the secure boot mode, the device no longer offers the setting *Allow upload of unsigned device software*. The device then refuses the upload of an unsigned software image.

If you decide to update the device software:

- ☐ Save the configuration profile in the volatile memory (*RAM*) to the non-volatile memory (*NVM*).
- ☐ Back up the device configuration.
  - If required by your backup policy, save the backup configuration (see on page 53 “Develop a backup policy for device-related data”).
- ☐ Update the device software.
- ☐ Reboot the device for the new software to take effect.

### 2.10.5 Best practices

To help keep your system secure, consider checking for device software updates regularly and using the latest available release. A newer release of the device software may provide you with security improvements or benefits like new functions, including new device functions that can assist in securing your network.

### 2.10.6 Detailed documentation

Refer to the "Configuration" user manual,

- Chapter "Managing configuration profiles" for the device configuration profiles
- Chapter "Loading software updates" for details on how to:
  - Determine the currently running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Check for a newer available software release
  - Update the device software
- Chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts' public key fingerprints.

# 2.11 Security setup overview

[CR7.1] [CR7.6] [NDR 3.2] [NDR 3.10] [NDR3.14]

The following descriptions apply to:
- The initial device security setup for a device out-of-the-box
- Changes in the device security setup as part of operation or maintenance

**Note:**
To update the software on the device, you need management access to the device, which requires at least a preliminary IP address setup. Hirschmann recommends using HiView to assign an IP address setup to the device.
[CR7.1 RE1] After the IP address setup, HiView offers you to open the device management. For the software update (see on page 69 “Software update”).
[CR3.3] The *Security Status* function in the device GUI can help you gain a first overview of the device security status. The *Security Status* function monitors some security configuration settings that are considered basic. Depending on your requirements, additional security setup steps may be required even if the *Security Status* function reports *ok*.

Refer to:
- The "Graphical User Interface" user manual, chapter "Diagnostics > Status Configuration > Security Status" for the *Security Status* function
- The "Configuration" user manual, chapter "Assistance in the protection from unauthorized access" for a basic device security setup

You will find more details for the security setup in the remainder of this chapter.

**Note:**
To conserve time and effort, you can perform the following security setup steps by loading a prepared configuration profile into the device.
[CR1.10] At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 44 “Planning a dedicated user account password policy”).

**Note:**
If you want to perform the initial security setup for a device out-of-the-box over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the configuration files are encrypted.
If you want to perform the initial security setup for a device out-of-the-box and you have the configuration profile on an SFTP or SCP server, first set up the SSH known host fingerprints in the device (see on page 82 “Set up the SSH Known Hosts fingerprints in the device”). Use the fingerprint of the configuration profile server. This enables the device to decide whether the configuration profile server it contacts is trustworthy or not.
Verify that the fingerprints are from a trustworthy source, like the server administrator.

In the following list and the related chapters, "disable logical access" means disabling a feature by a logical measure (a setup in the software). In contrast, "restrict physical access" means disabling a feature or an interface by a physical measure (a hardware modification) (see on page 91 “Possible restrictions to the device’s hardware interfaces”).

**Note:**
For a device setup compliant with SL-C2, the secure boot mode must be enabled.

The default setting of the secure boot mode is disabled ⚠. If the secure boot mode is disabled, the *Security Status* function in the Web-based interface notifies the user.

If the secure boot mode is enabled but the support mode is also enabled ⚠ (default setting: disabled), the *Security Status* function in the Web-based interface notifies the user.

**Note:**
If you follow a whitelist approach, consult your necessary function policy. The necessary function policy may stipulate which device functions need to be disabled. This may include functions that are not directly security-related.

Overview of possible security setup steps, in suggested sequence:
- Assign an IP address to the device management:
  - Assign a static IP address (may be considered more secure)
  - Or set up DHCP (depending on your DHCP server policy)
- Disable HiDiscovery access.
- Enable the secure boot mode <SL-C2>.
- Enable configuration encryption <SL-C2>.
- Set up a VLAN dedicated to management access.
- Disable logical access to unused ports and SFP slots.
- Disable logical access for empty media module slots.
- Disable logical access to the signal contact.
- Set up Power over Ethernet. **(depends on hardware)**
- Disable the automatic device software update from the external memory (ACA).
- Disable the SSH key auto upload from the external memory.
- Disable the Configuration load priority for the external memory.
- Disable copying a software file into the device that lacks a valid cryptographic signature.
- Disable writing an unencrypted configuration profile to the external memory (ACA) <SL-C2>.
- Disable loading an unencrypted configuration profile from the external memory (ACA) <SL-C2>.
- Disable insecure management protocols.
- Enable IP access restrictions.
- Set up a dedicated HTTPS certificate for the device.
- Set up a dedicated SSH host key for the device.
- Set up the SSH Known Hosts fingerprints in the device.
- Set up a dedicated, planned user account login policy.
- Set up a dedicated, planned user account password policy.
- Set up dedicated, planned user account names and roles <SL-C2>.
- Remove user accounts that have standard names <SL-C2>.
- Specify session timeouts <SL-C2>.
- Set up logging.
- Disable SNMPv1 traps.
- Enable SNMPv3 traps.
- Set up dedicated login banners.

You can choose to set up the following advanced device security features as required:
- Access to the system monitor through the serial port
- Disable access to the CLI service shell.

You can also choose to set up the following advanced user authentication measures as required (see on page 89 “Set up advanced user authentication <SL-C2>”):
- Use 802.1X for user authentication.
- Use a dedicated authentication policy list.
- Set up the following remote authentication protocol clients as needed, instead of or in addition to the local Integrated Authentication Server (IAS):
  - RADIUS

When the device configuration is complete:
- Create a backup of the configuration according to your backup policy for device-related data.
- If required, include other device-related data like private keys.
- If you plan on accessing the device through a web browser and use a self-signed HTTPS certificate generated on the device, look up and document the HTTPS certificate fingerprint.
- If you plan for accessing the device through SSH and use the self-signed SSH key generated on the device, look up and document the SSH host key fingerprint for use as an SSH Known Hosts entry on the clients.

### 2.11.1 Assign IP address parameters to the device management

**Note:**
At the first login with the delivery state password, the device asks you to change the password. Use a dedicated password according to your password policy (see on page 44 “Planning a dedicated user account password policy”).

The device offers you the following options for assigning a device management IP address: Local, DHCP (delivery state) ⚠, and BOOTP.

**Note:**
The setting "Local" (static) is generally considered more secure than using DHCP or BOOTP.
If you use use DHCP or BOOTP, consider loading the configuration or the operating system for the device from the local device memory. This is considered more secure than loading through TFTP. Load from a TFTP server only if you trust the transfer network or if the configuration files are encrypted.

ⓘ Refer to the "Configuration" user manual, chapter "Specifying the IP parameters" on how to specify an IP address for the device management

### 2.11.2 Disable HiDiscovery access

[CR4.3]

The delivery state of HiDiscovery is enabled ⚠.

Set the HiDiscovery protocol to `Off` after its initial use. This helps make the device more immune against unauthorized discovery and manipulation.

ⓘ Refer to the "Configuration" user manual, chapter "Specifying the IP parameters using HiDiscovery" on how to:
- Specify the IP address parameters for the device management
- Disable HiDiscovery

### 2.11.3 Enable the secure boot mode <SL-C2>

<SL-C2> [NDR 3.10 RE1] [NDR 3.12] [NDR 3.14 RE1]

The setting *Secure Boot enabled* disables the booting from a an unsigned software image. This helps secure the device against rogue device software without a valid cryptographic signature.

If you have a secure boot policy, apply your secure boot policy (see on page 42 “Planning a secure boot policy <SL-C2>”) for enabling the secure boot mode on that specific device.

If you do not have a secure boot policy, to help you decide (see on page 42 “Planning a secure boot policy <SL-C2>”).

**Note:**
The secure boot mode is required for a device setup compliant with SL-C2.

Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Software > Software update" on how to enable the secure boot mode.

### 2.11.4 Enable configuration encryption <SL-C2>

Enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 47 “Planning configuration encryption and the associated password”).

**Note:**
Configuration encryption with a password is required for a device setup compliant with SL-C2.

The default setting of the configuration encryption is disabled . If the configuration encryption is disabled, the *Security Status* function in the Web-based interface notifies the user.
The configuration encryption password is essentially a symmetric cryptography key, so if you have already planned a policy for symmetric cryptography keys (see on page 36 “Cryptographic key and password basics”), apply it to this key.

Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/ Save" for the configuration encryption and the associated password.

#### Options to enable configuration encryption

You have several options to enable configuration encryption:

- If you have a precompiled, unencrypted configuration file:
  - Load the precompiled, unencrypted configuration file.
  - Enable the configuration encryption and set the associated password manually.
  - Save the configuration.
- If you have a precompiled, encrypted configuration file:
  - Enable the configuration encryption and set the associated password manually.
  - Load the precompiled, encrypted configuration file.
- If you do not have a precompiled configuration file:
  - Configure the device manually.
  - Enable the configuration encryption and set the associated password manually.
  - Save the configuration.

### 2.11.5 Set up a VLAN dedicated to device management access

[SR5.1] [CR5.1] [NDR1.13]

The delivery state VLAN ID for device management access is 1.

Set up a VLAN dedicated exclusively to device management access. This helps make the device more immune to potential attacks via the network. It may also help improve the reachability of the device management when there is heavy general network traffic.

Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Global > Management interface" on how to specify a VLAN for device management access.

### 2.11.6 Disable logical access to the signal contact

If you do not need the signal contact, disable the signal contact in the device setup. In the delivery state, the signal contact is enabled in the mode "Monitoring correct operation".

If you do need the signal contact (see on page 93 “Signal contact considerations”).

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status configuration > Signal contact" for the signal contact.

### 2.11.7 Disable logical access to unused ports and SFP slots

In the delivery state, every port and SFP slot is enabled .

Disable network access for unused ports and empty SFP slots. Treat inserted SFPs without a data cable connected the same way as an unused port. This helps prevent potential attacks that connect a rogue network device to an unused port.

Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Port" for disabling ports.

### 2.11.8 Disable logical access for empty or unused media modules slots

In the delivery state, every media module slot allows access to the network . With this setting, if a media module is inserted into an empty media module slot, or if ports on an unused media module are physically accessed, the ports of the media module will establish network connections.

Disable empty and unused media module slots in the device setup. This helps prevent potential attacks that connect a rogue network device to a port on a newly inserted or unused media module.

Refer to the "Configuration" user manual, chapter "Deactivating the unused modules" for disabling unused media module slots.

### 2.11.9 Set up Power over Ethernet (depends on hardware)

Delivery state:
- The device-global setting `PoE Global Operation` is *`On`*.
- Port-related settings:
  - The setting `PoE Port Enable` is *`PoE enable`*.
  - The allowed classes, *`Class 0`*..*`Class 4`*, are enabled.
  - The `Power limit [W]` is `0.0` — the device will not enforce a specific power limit.
  - The power PoE `Priority` is *`low`*.

Device security aspects:
- If you do not need PoE or PoE+, disable PoE and PoE+ globally in the device.
- If you need PoE or PoE+:
  - Disable PoE or PoE+ on those ports that shall not deliver power.
  - For each port with PoE or PoE+ enabled, set up the minimal required reserved power according to the class (*`Class 0`*..*`Class 4`*) of the powered device (PD).
  - If you know the exact maximum power consumption of a PD, you can additionally set the power limit for the given port to this known value.

Network availability aspects: Assign a PoE priority (*`critical`*, *`high`*, or *`low`*) to each PoE port. This helps deliver power to the most important PDs when the device is unable to deliver nominal power to all the connected PDs.

Energy conservation aspects:
- If you set the power limit for a given port to the known power consumption of the PD, this may help in powering more PDs simultaneously in certain cases.
- If you know the power consumption requirements of a PD on a time-of-day or day-of-week basis, you can activate the *Auto-shutdown power* function and set up the associated values *Disable power at [hh:mm]* and *Re-enable power at [hh:mm]*. The prerequisite for this is that the device system clock is synchronized to a reliable, trustworthy source.

Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Power over Ethernet" for setting up Power over Ethernet.

### 2.11.10 Disable the automatic device software update from the external memory (ACA)

The device offers to automatically update the device software during system startup. The prerequisites are:
- The external memory function is enabled.
- On the external memory is a valid software image that is referred to in the file `startup.txt`.

Disable the automatic device software update from the external memory. This helps secure the device against a rogue device software image on an external memory being copied to the device and take effect after a reboot.

In the delivery state setting, the automatic device software update from the external memory is enabled ⚠.

Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > External Memory" on how to disable the automatic software update from the external memory.

### 2.11.11 Disable the SSH key auto upload from the external memory

The device offers to automatically upload an SSH key during system startup. The prerequisites are:
- The external memory function is enabled.
- On the external memory is a valid SSH key that is referred to in the file `startup.txt`.

Disabling the SSH key auto upload from the external memory can be a reasonable alternative to disabling the external memory function entirely.

Disable the SSH key auto upload from the external memory. This helps secure the device against a rogue SSH key on an external memory being copied to the device and take effect after a reboot.

In the delivery state setting, the SSH key auto upload from the external memory is enabled ⚠.

ⓘ Refer to the "Configuration" user manual:
- Chapter "Basic Settings > External Memory" on how to enable/disable the SSH key auto upload

### 2.11.12 Disable the Configuration load priority for the external memory

The device offers to assign a priority for the loading of a configuration profile from the external memory:
- *disable*
  The device loads the configuration profile only from the internal non-volatile memory (*NVM*).
- *first*
  The device loads the configuration profile from the external memory first.
  When the device does not find a configuration profile in the external memory, it loads the configuration profile from the internal non-volatile memory (*NVM*).

In the delivery state setting, the Configuration load priority for the external memory is *first* ⚠.

ⓘ Refer to the "Configuration" user manual, chapter "Basic Settings > External Memory" on how to set the Configuration load priority for the external memory.

### 2.11.13 Disable copying a software file into the device that lacks a valid cryptographic signature

[NDR 3.2]

<SL-C2> [NDR 3.10 RE1] [NDR 3.12] [NDR 3.14 RE1]

Disable copying a software file into the device that lacks a valid cryptographic signature: This helps secure the device against rogue device software without a valid cryptographic signature.

If the secure boot mode setting *Secure Boot enabled* is disabled, the device offers you the setting *Allow upload of unsigned device software*. This setting controls whether the device allows the upload of an unsigned software image into the device. If you activate *Secure Boot enabled*, the devide no longer offers the setting *Allow upload of unsigned device software*. The device then refuses the upload of an unsigned software image.

The default setting *Allow upload of unsigned device software* is enabled ⚠. The device will allow the upload a software file into the device that lacks a valid cryptographic signature.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Software > Allow upload of unsigned device software" on how to allow the upload of unsigned device software.

### 2.11.14 Disable writing an unencrypted configuration profile to the external memory (ACA)

To disable writing an unencrypted configuration file to any medium, enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 75 “Enable configuration encryption <SL-C2>”).

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Load/ Save > Configuration encryption" on how to disable writing an unencrypted configuration profile to the external memory.

### 2.11.15 Disable loading an unencrypted configuration profile from the external memory (ACA) <SL-C2>

[CR3.4 RE1]

To disable loading an unencrypted configuration file from any medium, enable the configuration encryption and set the associated password according to your configuration encryption policy (see on page 75 “Enable configuration encryption <SL-C2>”).

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic settings > Load/ Save > Configuration encryption" on how to disable loading an unencrypted configuration profile from the external memory.

### 2.11.16 Disable insecure management protocols

[CR4.3] [NDR1.13]

Disable insecure management protocols:
- ☐ Disable SNMPv1/v2 (delivery state: disabled).
- ☐ Disable Telnet (delivery state: disabled).
- ☐ Disable HTTP (delivery state: enabled ⚠ – redirects to HTTPS).

ⓘ Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access" for disabling insecure management protocols.

### 2.11.17 Set up management IP access restrictions

[CR3.1] [CR7.7] [CR4.3] [NDR1.13]

The device allows restricting the management access to the device to a source IP address range. You specify the address range by giving an IP address and a netmask.

You can set up the management access IP restrictions individually for each protocol or for a group of protocols.

*Table 18: Management access protocol overview*

| Protocol | Recommended setting for operation | Delivery state |
|---|---|---|
| HTTP | Disabled | Enabled ⚠ – redirects to HTTPS |
| HTTPS | Enabled | Enabled |
| SNMPv1/v2 | Disabled | Disabled |
| SNMPv3 | Enabled | Enabled |
| Telnet | Disabled | Disabled |
| SSHv2 | Enabled | Enabled |
| IEC 61850-MMS | Disabled | Disabled |
| Modbus TCP | Disabled | Disabled |

**Note:**

HTTP (delivery state enabled ⚠) may be useful for the initial setup of the device. However, it is considered insecure for operation. To help secure your system, disable HTTP as soon as you no longer need it, at the latest before your system goes live.

**Note:**
Confirm that at least one of the set-up management access IP restrictions is active. If no restriction is active, this results in unrestricted management access for every enabled protocol.
Also confirm that for every enabled protocol, at least one of the set-up management access IP restrictions is active. Excluding a protocol from every management access IP restrictions while the protocol itself is enabled, results in unrestricted management access for the respective protocol.

ⓘ Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access > Activating the IP access restriction" for setting up IP access restrictions.

### 2.11.18 Set up a dedicated HTTPS certificate for the device

[SR3.1] [SR4.1] [SR4.1 RE1] [CR1.8] [CR4.1] [CR4.3]

<SL-C2> [CR 1.9]

In the delivery state, the device contains a self-signed HTTPS certificate ⚠.

You have the option to:
- Replace the existing HTTPS certificate with a new, self-signed HTTPS certificate on the device
  - To help increase security, use the fingerprint algorithm *sha256* (delivery state: *sha256*) for the self-signed HTTPS certificate fingerprint.
  - After generating a new, self-signed HTTPS certificate on the device, write down its fingerprint for later use when you connect with web browser to the device for the first time.
- Load a dedicated, self-signed HTTPS certificate into the device.
  - If you have control over the entropy used for certificate generation, this way of certificate generation is considered more secure.
  - This alternative is also considered more secure because after generating the HTTPS certificate, you have the certificate and its fingerprint available on your external system. This can help you verify the device HTTPS certificate fingerprint when you connect with a web browser to the device for the first time.
- Load a dedicated, CA-signed HTTPS certificate into the device <SL-C2>
  - If you have an established Public Key Infrastructure (PKI), this option is considered more secure and also more convenient: A CA-signed HTTPS certificate on the device helps you solve the problem "Trust On First Use" when you connect a web browser to the device for the first time. <SL-C2>

Choose the option that best suits your requirements.

**Note:**
If you have an established Public Key Infrastructure (PKI), then loading a dedicated HTTPS certificate onto the device is generally considered more secure and also more convenient. <SL-C2>
You can find possible popular certificate generation tools on the Internet, for example, by searching for the keywords "HTTPS certificate generation".
To help increase security when you create a new, self-signed HTTPS certificate on the device, use the HTTPS certificate fingerprint algorithm *sha256* (delivery state: *sha256*).

Refer to the "Configuration" user manual, appendix "Setting up the configuration environment > HTTPS certificate" for an example of setting up your own HTTPS certificate.

### 2.11.19 Set up a dedicated SSH host key for the device

[CR1.8] [SR3.1] [SR4.1] [SR4.1 RE1] [CR4.1] [CR4.3]

<SL-C2> [CR 1.9]

In the delivery state, the device contains a self-signed SSH host key .

You have the following options:
- Replace the existing SSH host key with a new, self-signed SSH host key by generating a new SSH host key on the device.
  - To help increase security, use the fingerprint algorithm *sha256* (delivery state: *sha256*) for the SSH host key fingerprint.
  - After generating a new SSH host key on the device, write down its fingerprint for later use when you connect an SSH client to the device for the first time.

- Generate a dedicated SSH host key pair on an external system, self-sign the public key and load the key onto the device.
  - If you have control over the entropy used for key generation, this way of key generation is considered more secure.
  - This alternative is also considered more secure because after generating the SSH host keys, you have the keys and their fingerprints available on your external system. This can help you verify the device SSH host key fingerprint when you connect an SSH client to the device for the first time. <SL-C2>
- Generate a dedicated SSH host key pair, sign the public host key with your Certificate Authority (CA) key and load the CA-signed public host key onto the device.
  - If you have an established public key Infrastructure (PKI), this option is considered more secure and also more convenient: A CA-signed SSH host key on the device helps you solve the problem "Trust On First Use" when you connect an SSH client to the device for the first time. <SL-C2>

Choose the option that best suits your requirements.

**Note:**
You can find possible popular key generation and signing tools on the Internet, for example, by searching for the keywords "SSH key generation tool".

Refer to the "Configuration" user manual, appendix "Setting up the configuration environment > Preparing access using SSH > Loading your own key onto the device" for an example of setting up your own SSH key pair.

### 2.11.20 Set up the SSH Known Hosts fingerprints in the device

If you want to load the device configuration or update the device software from an SFTP or SCP server, set up the SSH known host fingerprints for these servers in the device. Use the fingerprints of the respective configuration profile or software update servers. This enables the device to decide whether the SFTP or SCP server it contacts is trustworthy or not.

**Note:**
Verify that the fingerprints are from a trustworthy source, like the server administrator.
If you want to load the device configuration or update the device software over a network, verify that you are using a secure transfer protocol, like HTTPS, SFTP or SCP. Use the insecure protocols FTP or TFTP only if you trust the servers and the transfer network or if the configuration files are encrypted.

Refer to the "Configuration" user manual, chapter "Assistance in the protection from unauthorized access > Making SSH hosts known to the device" for details on how to set up the known hosts' public key fingerprints.

### 2.11.21 Set up a dedicated user account login policy

[SR3.8] [SR3.8 RE1] [SR3.8 RE2] [SR3.8 RE3] [CR1.11] [CR2.5] [CR3.8]

**Note:**
The prerequisite for working through this section is that you have already planned a dedicated user account login policy (see on page 43 “Planning a dedicated user account login policy”).
For quantitative information on how to ensure a secure login policy (see on page 134 “Attack rate mitigation”). For quantitative information on how to help ensure hard-to-break passwords (see on page 121 “Password strength and policy guide”).

The login policy applies to the following user interfaces and access protocols:
- The Command Line Interface (CLI) using SSH or Telnet
- The Graphical User Interface (GUI) using HTTPS or HTTP

Apply your planned user account login policy. This helps ensure that the device locks out a user after the specified maximum number of failed user logins in a row, requires a password with minimum length, and enforces the specified waiting period after a failed login.

Set up a dedicated user account login policy as required:
- ☐ Login attempts:
  - Specify the maximum number of failed user logins in a row until the device locks the respective user account (delivery state: 0 – no limit ⚠).
- ☐ Minimum password length:
  - Specify the minimum password length (delivery state: 6 ⚠).
- ☐ Login attempts period:
  - Specify the waiting time (Login attempts period in minutes) before the device auto-unlocks a locked user account (delivery state: 0 – no waiting time ⚠).

**Note:**
Access to the CLI using the serial port is exempt from the login policy. Users accessing the CLI through the serial port have an unlimited number of login attempts. They are also not required to wait for the next login attempt, that is, the Login attempts period does not apply. This helps ensure access to the device management in situations where availability may be critical, and for users who already have physical access to the device.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device login functions.

### 2.11.22 Set up a dedicated user account password policy

[CR1.7]

**Note:**
The prerequisite for working through this section is that you have already planned a dedicated user account password policy (see on page 44 “Planning a dedicated user account password policy”).
For quantitative information on how to help ensure hard-to-break passwords (see on page 121 “Password strength and policy guide”).

Set up a dedicated user account password policy as required:

- ☐ Minimum required number of uppercase characters (delivery state: 1 ⚠)
- ☐ Minimum required number of lowercase characters (delivery state: 1 ⚠)
- ☐ Minimum required number of digits in a password (delivery state: 1 ⚠)
- ☐ Minimum required number of special characters (delivery state: 1 ⚠)

**Note:**
The minimum password length belongs to the user account login policy (see on page 83 “Set up a dedicated user account login policy”).
The enforcement of the password policy belongs to the account names and access roles for device management (see on page 84 “Set up dedicated user account names and access roles for device management <SL-C2>”).

In the delivery state, the device has the following user account preconfigured:

*Table 19: User credentials for the administrator account in the delivery state*

| Username | Password | User account role | Privileges |
|---|---|---|---|
| admin | private (May have been changed at first login.) | administrator | The device permits the reading and writing of device management data, including security-relevant settings. The device also permits the reading of the audit trail. |

**Note:**
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name user and the associated password public. If you need a user account that has only read access, you can create a user account with the access role guest and assign it the username user, for example.

**Note:**
The device asks you to change the delivery state password on the first login. Use a password different from the delivery state password.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device password policy functions.

### 2.11.23 Set up dedicated user account names and access roles for device management <SL-C2>

[SR2.1] [SR2.1 RE1] [SR2.1 RE2] [CR1.1 RE1] [CR1.3] [CR1.4] [CR1.5] [CR2.1 RE1] [CR2.1 RE2]

**Note:**
The prerequisite for working through this section is that you have already planned a dedicated user account name and access role policy (see on page 45 “Planning a dedicated user account name and access role policy for device management”), and that you have planned a dedicated policy for SNMPv3 authentication and encryption types, and for the related SNMPv3 passwords.
The SNMPv3 passwords are essentially symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys (see on page 36 “Cryptographic key and password basics”), apply it to these keys.

In the delivery state, the device has the following user account preconfigured:

*Table 20: User credentials for the administrator account in the delivery state*

| Username | Password | User account role | Privileges |
|---|---|---|---|
| `admin` | `private` (May have been changed at first login.) | `administrator` | Permits reading and writing of device management data, including security-relevant settings. Also permits the reading of the audit trail. |

**Note:**
Software releases 08.1.00 and higher in the delivery state no longer offer a user account with the name `user` and the associated password `public`. If you need a user account that has only read access, you can create a user account with the access role `guest` and assign it the username `user`, for example.

**Note:**
SNMPv3 passwords are essentially symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys (see on page 36 “Cryptographic key and password basics”), apply it to these keys.

Set up dedicated user accounts as required:

- ☐ <SL-C2> Create user accounts. For each new user account, perform the following steps:
  - Create a user account with a dedicated name.
    Note that user account names are case-sensitive.
  - Assign the new user account a strong password.
    Avoid standard passwords like "private" or "public", even for accounts with non-descriptive names.
  - Assign the new user account an access role that offers only the least required privileges.
  - Enforce the password policy check for the new user account (in the delivery state, the password policy check is not enforced ⚠).
  - Save the settings temporarily to let the device check the password of the new account against the enforced password policy.
- ☐ For each new user account, set up an SNMPv3 policy if required:
  - To help increase security, set the SNMPv3 authentication type to *`hmacsha`* (considered more secure than the delivery state *`hmacmd5`* ⚠).
  - Set an SNMPv3 authentication password according to your policy.
  - To help increase security, set the SNMPv3 encryption type to *`aesCfb128`* (considered more secure than the delivery state *`des`* ⚠).
  - Set an SNMPv3 encryption password according to your policy.
- ☐ Help secure existing user accounts:
  - Enforce the password policy check for the existing user accounts (in the delivery state, the password policy check is not enforced ⚠).
  - Set up the SNMPv3 settings as described above for a new user account.

- If you enforce the password policy subsequently for an existing user account, re-enter the password and save the changed settings temporarily to let the device check the password against the policy.
- If you change user account data for the currently logged-in user, the device will warn you that you will be logged out.
  To avoid this, consider changing user account data only for user accounts other than the currently logged-in one.
  This may need an additional user account with administrator privileges.

☐ <SL-C2> Remove user accounts that have standard names:
- To remove a user account, first log out of the respective user account and log in with an administrator-role account. Then remove the respective user account.
- The device requires you to have at least 1 administrator-role account.
  To remove the standard administrator-role account "admin", you need another account with the administrator role. If you haven't, create a new administrator-role account first.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Device Security > User Management" for the device user account name and access role functions.

### 2.11.24 Specify finite session timeouts <SL-C2>

[CR2.6]

Apply your planned sessions timeout policy. This helps ensure that the device terminates the respective session automatically when idle.

Specify finite session timeouts:

☐ Graphical User Interface using HTTPS or HTTP ⚠ (delivery state: 160 min. ⚠)

☐ For the Command Line Interface through the serial port, SSH, or Telnet ⚠ (delivery state: 160 min. ⚠)

ⓘ Refer to the "Graphical User Interface" reference manual:
- Chapter "Device Security > Management access > Web" for the Graphical User Interface timeout function
- Chapter "Device Security > Management access > CLI" for the SSH and serial port timeout function

### 2.11.25 Set up certificates and possible revocation lists for authentication, logging and eMail servers

<SL-C2> [CR 1.9]

If you intend to use TLS-based servers for one of the following functions, set up the server certificates and possible revocation lists in the device:
- Authentication servers
- Logging servers

This enables the device to decide whether a TLS-based server it contacts is trustworthy or not.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Diagnostics > LDAP > Configuration" for managing the certificates for the LDAP client function.
- Chapter "Diagnostics > eMail Notification > Global" for managing the certificates for the email submission function.
- Chapter "Diagnostics > Syslog" for managing the certificates for the Syslog over TLS function.

### 2.11.26 Set up logging

[SR2.8] [SR2.8 RE1] [SR2.11] [SR2.11 RE1] [SR2.12] [SR2.12 RE1] [SR6.1] [CR1.2] [CR1.8] [CR2.8] [CR2.9] [CR2.10] [CR2.11] [CR2.12] [CR3.1] [CR3.9] [CR6.1] [CR6.2]

Set up logging:
- ☐ Set up the minimum severity level to be logged.
  The setting depends on our functional and security requirements.
- ☐ Set up logging destinations:
  - The required settings depend on our security requirements.
  - For log availability reasons, a remote destination, different from the location of the device, may be preferable. This is typically a Syslog server.
  - For log confidentiality reasons (logs as data at rest), an appropriately secured remote destination may be preferable.

**Note:**
The Syslog client in the device offers unencrypted communication only.

**Note:**
The persistent logging function can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Diagnostics > Syslog" for the device Syslog function
- Chapter "Time > SNTP > SNTP Client" on how to synchronize the device clock through SNTP

### 2.11.27 Disable SNMPv1 traps

[CR6.2]

The device can send SNMPv1 traps. SNMPv1 traps are unencrypted. From a security perspective, this may be considered insecure.

Disable SNMPv1 traps if you do not need them (delivery state: disabled).

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status Configuration > Alarms (Traps)" for the device SNMPv1 trap send function.

### 2.11.28 Enable SNMPv3 traps

[CR6.2]

The device can send SNMPv3 traps. SNMPv3 traps can be signed (authenticated) and additionally encrypted. From a security perspective, authenticated and encrypted SNMPv3 traps are preferable over SNMPv1 traps.

Set up authenticated (and possibly also encrypted) SNMPv3 traps if you require them (delivery state: no SNMPv3 traps configured).

**Note:**
The SNMPv3 trap passwords are essentially symmetric cryptography keys, so if you have already planned a policy for symmetric cryptography keys (see on page 36 “Cryptographic key and password basics”), apply it to these keys.

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Status Configuration > Alarms (Traps)" for the device SNMPv3 trap send function.

### 2.11.29 Set up dedicated login banners

[CR1.12]

Set up dedicated login banners:
- ☐ Set up the GUI pre-login banner with only the minimal information required. Avoid any additional information that may help an attacker.
- ☐ Set up the CLI pre-login banner with only the minimal information required. Avoid any additional information that may help an attacker.
- ☐ Set up the CLI (post-) login banner with only the minimal information required.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Device Security > Pre-login Banner" for setting up the GUI and CLI pre-login banner
- Chapter "Device Security > Management Access > Command Line Interface" for setting up the CLI post-login banner

### 2.11.30 Advanced: Access to the system monitor through the serial port

You can enable the access to the system monitor via the serial port (V.24/RS-232).

*Table 21: Serial port by device type*

| Device type | Connector type | Connector labeling | Function |
|---|---|---|---|
| EAGLE40-03 | RJ45 socket | - | Console access to the device management |
| EAGLE40-07 | DB9 socket | CONSOLE | Console access to the device management |
| | DB9 socket | COM | None (reserved for future use) |

Refer to the "Graphical User Interface" reference manual, chapter "Operation diagnosis > Self-test" on how to enable access to the system monitor via V.24/RS-232.

### 2.11.31 Advanced: disable access to the CLI service shell

You can disable access to the CLI service shell (delivery state: enabled).

**Note:**
The CLI service shell can be accessed only by users with the administrator access role.

**NOTICE**

**INOPERABLE DEVICE**

Disabling the CLI service shell may impair service access. A possible use case when the CLI service shell is needed, is on-site staff needing to issue service shell commands as instructed by the manufacturer support.

**Disabling the CLI service shell can result in an inadvertently inoperable device. Disabling the CLI service shell is permanent. To re-enable the CLI service shell, you have to send the device to the manufacturer.**

Refer to the "Configuration" user manual, chapter "User Interfaces > Command Line Interface > Service Shell > Deactivate the Service Shell permanently in the device" on how to disable access to the CLI service shell.

### 2.11.32 Set up advanced user authentication <SL-C2>

[CR1.2]

Set up the following advanced user authentication measures as required:
- Use 802.1X for user authentication [SR2.3] [SR2.3 RE1] [NDR1.13].
- Use a dedicated authentication policy list.
- Set up the following remote authentication protocol clients as needed, instead of or in addition to the local Integrated Authentication Server (IAS):
  - RADIUS (offers obfuscated communication)

**Note:**
The RADIUS client in the device exclusively offers obfuscated communication which is considered weaker than encrypted LDAP.

**Note:**
If you use authentication servers, this requires setup and maintenance of these external servers. The system operator is responsible to plan and implement these steps.

Refer to:
- The "Graphical User Interface" reference manual:
  - Chapter "Network Security > 802.1X" on how to set up 802.1X port security
  - Chapter "Device Security > Authentication List" on how to set up the authentication policy list of the device’s local IAS
- The "Graphical User Interface" reference manual:
  - Chapter "Network Security > RADIUS" on how to set up the RADIUS client in the device

### 2.11.33 Create a backup of the device-related data

[SR7.3] [SR7.3 RE1]

Create a backup of the device-related data according to your backup policy. This minimizes the effort to replace the device if the device becomes inoperable.

- ☐ [SR7.3] [SR7.3 RE1] [CR7.3] [CR7.3 RE1] Consider creating a backup copy of the device configuration profile <SL-C2>.
- ☐ Keep the backup files separate from the device in a secure location.
  - For example, place the backup files on a file server in a device-specific folder.
- ☐ If required and useful, include other device-specific data in the same device-specific folder.
  - For example, include device-specific private keys or certificates.
  - If you plan on accessing the device through a web browser and use a self-signed HTTPS certificate generated on the device, look up and document the HTTPS certificate fingerprint.
  - If you plan for accessing the device through SSH and use a self-signed SSH key generated on the device, look up and document the SSH host key fingerprint for use as an SSH Known Hosts entry on the clients.

ⓘ Refer to the "Graphical User Interface" reference manual, chapter "Basic Settings > Load/Save" on how to save the device configuration.

# 2.12 Possible restrictions to the device’s hardware interfaces

**Note:**
The prerequisite for working through this section is that you have already performed planning possible restrictions to the device’s hardware interfaces (see on page 42 “Planning restrictions to the device hardware interfaces”).

The following possible modifications to the device hardware apply exclusively to the device hardware interfaces that are reachable from the device surface. The purpose of these measures is to restrict physical access to particular device interfaces while keeping the device closed.

**⚠ WARNING**

**ELECTRIC SHOCK**

To avoid electric shock, do not open the device.

**Failure to follow these instructions can result in death or serious injury.**

**Note:**
In the following list and the related chapters, "restrict physical access" means disabling a feature or an interface by a physical measure (a hardware modification). In contrast, "disable logical access" a feature by a logical measure (a software setup) (see on page 72 “Security setup overview”).

The following descriptions apply to possible hardware modifications in the following cases:
- For a device out-of-the-box before installation
- After initial installation
- As part of operation or maintenance

Perform the following modification steps to restrict access to the device hardware interfaces, like covering or obstructing a slot or a port, as required. Restrict physical access:
- To the USB port
- To network ports or SFP slots
- To empty media module slots
- To the signal contact
- Restrict physical (visual) access to the device LEDs and port LEDs.

## 2.12.1 Restrict physical access to the USB port

If you have high security requirements, and you are sure you will not need the USB port after commissioning, consider covering or obstructing the USB port.

ⓘ Refer to the "Installation" user manual, chapter "Description > Management interfaces" for the USB port.

### 2.12.2 Restrict physical access to network ports or SFP slots

If you have high security requirements, and you are sure you will not need certain network ports or SFP slots after commissioning, consider covering or obstructing these network ports and SFP slots.

Refer to the "Installation" user manual, chapter "Description > Ethernet ports" for the network ports and SFP slots.

### 2.12.3 Restrict physical access to empty media module slots

If you have high security requirements, and you are sure you will not need certain empty media module slots after commissioning, consider covering or obstructing the empty media module slots.

Refer to the "Installation" user manual:
- Chapter "Installation > Installing media modules" for installing a media module into a slot
- Chapter "Disassembly > Removing a media module" for removing a media module from a slot

### 2.12.4 Restrict physical access to the signal contact

If you do not need the signal contact and have high security requirements, consider covering or obstructing the signal contact terminals.

If you use the signal contact (see on page 93 “Signal contact considerations”).

Refer to the "Installation" user manual:
- Chapter "Description > Management interfaces > Signal contact" for the signal contact location
- Chapter "Technical data > Signal contact" for the allowed signal contact operating conditions

### 2.12.5 Restrict physical (visual) access to the device LEDs and port LEDs

If you have high security requirements, consider performing the following steps:
- Install the device in a cabinet with a nontransparent door.
- Cover or obstruct the device LEDs and the port LEDs with a removable cover.

Refer to the "Installation" user manual, chapter "Description > Display elements" for the device and port LEDs.

# 2.13 Device installation

The following description applies to:
- The installation of a device in a new system or system zone
- Changes to the device as part of operation or maintenance

Refer to the "Installation" user manual for a suitable physical installation location:
- Chapter "Safety instructions" for safety and regulatory topics
- Chapter "Technical data" for the allowed device temperature ranges and climatic conditions
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical device installation

## 2.13.1 Checking the security seal

[NDR 3.13]

On the new device, check the security seal, (see on page 117 “Security seal”).

## 2.13.2 Data connections

If you have high device availability requirements, use redundant data connections, for example, for an upstream connection.

Refer to the "Installation" user manual:
- Chapter "Installation > Installing an SFP transceiver" for the SFP slots
- Chapter "Description > Ethernet ports" for the network ports
- Chapter "Installation > Connecting data cables" on details how to make data connections

## 2.13.3 Signal contact considerations

If you use the signal contact, consider the following security and safety aspects:
- **To help protect the device**, connect the signal contact only to a circuit that meets the electrical and safety device requirements.
- **To help protect your system**, connect the signal contact only to circuits that do not have explicit security or safety requirements. This means:
  - The circuit controlled by the signal contact does not have any security or safety function.
  - The controlled circuit does not rely on the secure or safe operation of the signal contact.

Refer to the "Installation" user manual for the signal contact:
- Chapter "Technical data > Signal contact" for the allowed signal contact operating conditions
- Chapter "Installation > Connecting the terminal blocks > Signal contact" for the electrical signal contact connection

## 2.14 Operation

The prerequisite for the operation life cycle phase is that you have taken the appropriate physical and logical steps to set up the device, both regarding functionality and security. This essentially reduces the required security steps during the operation phase to the considerations already described in this security manual, the "Installation" and "Configuration" user manuals, and the "Graphical User Interface" and "Command Line Interface" reference manuals.

As a minimal overview, the essential parts of how to operate the device properly are:

- Environmental conditions (see on page 93 “Device installation”)
- Device availability requirements (see on page 65 “Considering the device availability requirements”)
- Data connections (see on page 93 “Data connections”)

For the privileges and responsibilities of the administrative user roles for both the device hardware and software settings, as well as for the scheduled or event-driven operation and maintenance parts, follow your policy, (see on page 56 “Operation and maintenance policy”).

# 2.15 Maintenance

For the privileges and responsibilities of the administrative device user roles as well as for the scheduled or event-driven operation and maintenance parts, follow your policy, (see on page 56 “Operation and maintenance policy”).

## 2.15.1 Check the security seal (regularly or triggered by an event)

[NDR 3.11]

On the device, check the security seal, (see on page 117 “Security seal”).

## 2.15.2 Software update

[NDR 3.10]

If required, perform a device software update.

For the security aspects of the software update (see on page 69 “Software update”).

Refer to the "Configuration" user manual, chapter "Loading software updates" for details on how to:

- Determine the currently running software release
- Determine the stored software release
- Load a previous software version, if required
- Check for a newer available software release
- Update the device software

## 2.15.3 Hardware changes

**⚠ WARNING**

**ELECTRIC SHOCK**

To avoid electric shock, do not open the device.

**Failure to follow these instructions can result in death or serious injury.**

Typical application cases include:

- Connecting or removing an external device on an Ethernet port
- Inserting or removing an SFP
- Inserting or removing a media module on a media module slot

- Connecting or removing a power supply
- Connecting or removing a PoE-/PoE+-powered device (PD) on a port **(depends on hardware)**

**Note:**
Depending on your system availability requirements, provide a redundant data upstream connection.
Consider the worst-case power requirements of the inserted SFPs.
Consider the worst-case power requirements of the inserted media modules.
[SR7.5] Connecting an additional power supply to a device with an existing power supply forms a redundant power supply that helps the device availability. Consider the worst-case device power budget for every power supply, in case one of the redundant power supplies becomes inoperable. Consider the new PoE/PoE+ power budget. Take the worst-case PoE/PoE+ power budget into account. If required, adapt the PoE/PoE+ parameters.

Refer to:
- The "Installation" user manual:
  - Chapter "Description > Ethernet ports" for the network ports and SFP slots
  - Chapter "Connecting data cables" on details how to make data connections
  - Chapter "Installation > Installing an SFP transceiver" for installing an SFP
  - Chapter "Disassembly > Removing an SFP transceiver" for removing an SFP
  - Chapter "Installation > Installing media modules" for inserting a media module into an empty media module slot
  - Chapter "Disassembly > Removing a media module" for removing a media module
- The "Configuration" user manual:
  - Chapter "Configuring the ports > Enabling/disabling the port" for enabling or disabling a port
  - Chapter "Assistance in the protection from unauthorized access > Deactivating the unused modules" for enabling or disabling a media module slot
  - Chapter "Basic Settings > Power over Ethernet" for setting up PoE/PoE+ **(depends on hardware)**

### 2.15.4 Device hardware replacement

**⚠ WARNING**

**ELECTRIC SHOCK**

To avoid electric shock, do not open the device.

**Failure to follow these instructions can result in death or serious injury.**

[CR7.4]

Perform the following steps:
- According to your backup policy (see on page 53 “Develop a backup policy for device-related data”)
- According to your hardware replacement policy (see on page 53 “Develop a policy for replacing the device hardware”)

Device hardware replacement steps:
- ☐ On the former device, back up the configuration if required and possible.
  - If you have enabled configuration encryption, document the encryption password.
- ☐ Remove the former device from its environment.
- ☐ [NDR 3.11] On the new device, check the security seal, (see on page 117 “Security seal”).

- ☐ On the new device, perform an initial software update (see on page 69 “Software update”).
- ☐ On the new device, set up the device software, for example, by transferring the existing configuration profiles of the former device to the new device (see on page 72 “Security setup overview”).
  - If you have enabled configuration encryption (see on page 75 “Options to enable configuration encryption”).
- ☐ On the new device, restrict the hardware interfaces if required (see on page 91 “Possible restrictions to the device’s hardware interfaces”).
- ☐ Install and connect the new device in its environment.
- ☐ For the former device:
  - If you want the device repaired, follow your hardware repair policy (see on page 97 “Device hardware repair”).
  - If you want to decommission the device, follow your hardware decommissioning policy (see on page 99 “Device decommissioning”).

ⓘ Refer to:

- The "Graphical User Interface" reference manual, chapter "Basic Settings > Load/Save" on:
  - How to save the former device’s configuration
  - How to load the configuration into the new device
- The "Configuration" user manual, chapter "Loading software updates" for the new device on how to:
  - Determine the currently running software release
  - Determine the stored software release
  - Load a previous software version, if required
  - Check for a newer available software release
  - Update the device software
- The "Installation" user manual:
  - Chapter "Disassembly > Removing the device" for mechanically removing the former device from its environment
  - Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical installation of the new device

### 2.15.5 Device hardware repair

**⚠ WARNING**

**ELECTRIC SHOCK**

To avoid electric shock, do not open the device.

**Failure to follow these instructions can result in death or serious injury.**

Should your device need repair, follow your device hardware repair policy (see on page 53 “Develop a policy for device hardware repair”).

Consider the following steps:

- ☐ Keep a backup copy of the device configuration (see on page 90 “Create a backup of the device-related data”).
  - If you have enabled configuration encryption, document the encryption password.
- ☐ Make a note of the device base MAC address (read it from the label on the front panel or look it up in the device management).
- ☐ If required and possible, wipe or delete the configuration and other data you consider confidential (see on page 99 “Deletion of confidential data and secrets”).
- ☐ Record the condition of the security seal on the device (see on page 117 “Security seal”).

☐ Send the device to the manufacturer for repair.
☐ When the device is back from repair:
  – Check according to your device hardware repair policy if the device you received back is acceptable (is either identical to the device you sent in, is a different device of the same type, or is a different device of a superior type).
  – Check the security seal of the repaired device, (see on page 117 “Security seal”). The security seal on the identical device received back should either be a new security seal or the old security seal shall be approximately in the same condition as when you sent the device in. If the device you received back is a different device of the same type or a different device of a superior type, it should have a new security seal.
  – If you have enabled configuration encryption (see on page 75 “Options to enable configuration encryption”).
  – Restore the files on the repaired device from the backup.
  – If required by your policy, compare the repaired device’s actual base MAC address with the address you noted earlier. This helps ensure you have the same device back that you sent in.
  – If required, update the software on the repaired device.

ⓘ Refer to the "Installation" user manual:
- Chapter "Disassembly > Removing the device" for mechanically removing the device from its environment
- Chapters "Installation > Installing and grounding the device" and "Installation > Connecting the terminal blocks" for the mechanical and electrical installation of the repaired device

# 2.16 Device decommissioning

When decommissioning a device, follow your device hardware decommissioning policy (see on page 54 “Develop a policy for device hardware decommissioning”).

**⚠ WARNING**

**ELECTRIC SHOCK**

To avoid electric shock, do not open the device.

**Failure to follow these instructions can result in death or serious injury.**

**Note:**
If you have high security requirements, consider physical destruction of the device and the external memory (ACA)(see on page 100 “Secure physical destruction of the device and its accessories”). Secure physical destruction addresses the possible reading-out of memory blocks from the flash memory and makes deletion and wiping unnecessary (see on page 99 “Deletion of confidential data and secrets”).
If you plan to continue using the device, consider leaving the device and its software intact and deleting or wiping only the data on the device and on the external memory.

ⓘ Refer to the "Installation" user manual, Chapter "Disassembly > Removing the device" for mechanically removing the device from its environment.

## 2.16.1 Deletion of confidential data and secrets

**Note:**
Resetting the device to the delivery state performs normal file deletion operations on the device, and on the external memory (ACA), which may leave parts of the file contents or memory blocks in the flash memory intact [CR4.2]. Furthermore, the audit trail persists after a reset to the delivery state.
If you have high security requirements, consider the physical destruction of the device and the external memory.

## 2.16.2 Reset to the delivery state

For the deletion of data, perform the following steps as required:

- Reset the device to the delivery state. This performs the following operations:
  - Deletes the configuration profiles and configuration scripts in the device.
  - If an external memory is connected, then the device also deletes the configuration profiles saved in the external memory.
  - Resets the boot parameters.
  - Deletes the current HTTPS certificate in the device and creates a new, self-signed HTTPS certificate.

  - Deletes the current SSH host key pair in the device and creates a new, self-signed SSH host key pair.
  - If the external memory (ACA) is plugged in, the device also deletes the configuration profiles on the external memory.
- If required, manually delete other files on the external memory.

**Note:**
The audit trail persists in the device even after a reset to the delivery state.

Refer to the "Configuration" user manual, chapter "Managing configuration profiles > Reset the device to the factory defaults" on how to reset the device to the delivery state.

### 2.16.3 Secure physical destruction of the device and its accessories

For the secure physical destruction of physical components, perform the following steps as required by your decommissioning policy:

- ☐ Destroy the security seal on the device, (see on page 117 “Security seal”).
- ☐ Physically destroy the device, including the flash memory chips. This addresses:
  - The HTTPS certificate in the device
  - The SSH host key pair in the device
  - The configuration profiles in the device
  - Any other files in the device
- ☐ If required, physically destroy the external memory (ACA). This addresses:
  - The configuration profiles on the external memory
  - The software files on the external memory
  - Any other files on the external memory

### 2.16.4 Secure removal of device-related data from the administration environment

<SL-C2> [CR 1.9]

For the secure removal of device-related data from the administration environment, perform the following steps as required by your decommissioning policy.This may include:

- ☐ The removal of configuration data and its backups
- ☐ The removal of private cryptographic keys
- ☐ The removal of self-signed certificates
- ☐ The removal of references to:
  - The device MAC base address
  - The device serial number
  - The device product code

### 2.16.5 Secure disposal of the device hardware

For the secure disposal of the device hardware, follow your disposal policy.

**Note:**
If you have high security requirements, consider disposing of the device by shredding it.

# 3 Network security support

This main chapter describes how the device can assist in:
- Securing your system
- Improving the availability of your system

This chapter deals with specific device functionality in the operation and maintenance life cycle phases that can help improve the security or availability of your network.

## 3.1 Introduction

Aside from the basic task of forwarding and processing data packets in your network, the device can also help:
- Deploy defense in depth for your network
- Harden your network
- Enhance and maintain the availability of your network

### 3.1.1 Prerequisites for setting up network security

Only a device that is itself already secured can help reasonably improve the security and availability of your network. The prerequisite for working through this section is that you have taken the required steps to securing the device itself (see on page 59 “Device security in the life cycle phases”).

To determine which device functions are suitable for providing or enhancing the security of your network, apply the process of assessing threat risks, mitigation efficiency and the criticality of the individual threat risk/mitigation efficiency combinations analogous to the device-centered process:
- Compile a network threat profile (see on page 25 “Compiling a threat profile”):
  - Develop a network threat model.
  - Collect the perceivable threats to the network.
  - Assess the network threat risks.
- Develop a general network defense strategy (see on page 27 “Defense in depth vs. hardening”).
- Develop a general network mitigation strategy (see on page 30 “Developing a mitigation strategy”):
  - Collect the perceivable network mitigations.
  - Assess the network mitigation efficiency.
- Develop an individual mitigation strategy (see on page 33 “Criticality assessment and mitigation strategies”):
  - Assess the criticality of the individual network threat/mitigation combinations.
  - Develop a mitigation strategy based on the individual criticality values.

### 3.1.2 Deploying defense in depth for your network

Defense in depth creates several barriers that a potential attacker must overcome one after the other. The prerequisite for working through this section is that you have already set up a dedicated plan for defending your network in depth (see on page 27 “Defense in depth”).

From a system view, there are 2 complementary ways to implement defense in depth for a network:

- The device-related way:
  The device-related way deploys measures to help secure the device itself. This in turn helps secure the network. These measures are described in the preceding main chapter (see on page 72 “Security setup overview”).
- The network-related way:
  The network-related way deploys specific device functions as measures to help secure the network. These measures are described in the remainder of this main chapter.

The suggested network-related mitigation measures are collected in the following chapter (see on page 103 “Measures to help secure the network”).

**Note:**
First pick the mitigation measures suitable for defense in depth. Then consider hardening by selecting additional measures from the remaining options.

### 3.1.3 Harden your network

The suggested network-related mitigation measures are collected in the following chapter (see on page 103 “Measures to help secure the network”).

**Note:**
Pick the mitigation measures suitable for defense in depth first. Then pick hardening measures from the remaining options.

## 3.2 Measures to help secure the network

The below collection of network-related mitigation measures can be used for defense in depth as well as for hardening. First pick the measures suitable for defense in depth. Then consider hardening by selecting additional measures from the remaining options.

To help you secure your network, perform the following steps on the device according to your requirements, threat and mitigation assessment results, and policies:

- Restrict logical access to your network:
  - Set up VLANs for traffic segregation.
  - Disable GVRP and MVRP.
  - Set up Port Security.
- Help secure the network protocols used.
  - Disable GMRP and MMRP.
- Help secure the redundancy protocols used:
  - Set up RSTP guards and helper protocols.
  - Set up the *MRP* (MRP VLAN ID ≥2, tagged packets) parameters.
- Set up the attack protection support functions:
  - Set up the Denial of Service (DoS) parameters.
  - Set up the Access Control Lists (ACLs).
  - Set up the rate limiter.
- Set up the network time synchronization parameters.
- Set up the logging parameters.
- Set up the LLDP parameters.

**Note:**
Securing the redundancy protocols used can also help enhance and maintain the availability of your network.
Routing protocols like HiVRRP, VRRP, OSPF or RIP are outside the scope of this document.

# 3.3 Restrict logical access to your network

## 3.3.1 Set up VLANs for traffic segregation

[SR5.1] [CR5.1]

The essential prerequisite for setting up VLANs in the device is that you have created a VLAN plan for your network (see on page 38 “VLAN plan”).

Set up the VLANs, the port memberships and the properties of the port memberships according to your VLAN plan.

Refer to the "Graphical User Interface" reference manual, chapter "Switching > VLAN" on how to set up VLANs for traffic segregation.

## 3.3.2 Disable GVRP and MVRP

The GARP VLAN Registration Protocol (GVRP) and its successor, the Multiple VLAN Registration Protocol (MVRP or MRP-IEEE Multiple VLAN Registration Protocol) can be used to dynamically set up VLANs in a device. However, using these protocols can also pose a vulnerability if an attacker can snoop GVRP or MVRP frames or inject deliberately crafted GVRP or MVRP frames.

It is generally considered more secure to disable GVRP and MVRP.

**Note:**
The delivery state for both GVRP and MVRP is globally disabled.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Switching > GARP > GVRP" on how to set up GVRP
- Chapter "Switching > MRP-IEEE > MRP-IEEE Multiple VLAN Registration Protocol" on how to set up MVRP

## 3.3.3 Set up the Port Security

[NDR 1.13]

Port Security is a concept to restrict which frames the network device accepts that have been received on a specific port or VLAN. This can help secure your network.

Port Security distinguishes frames by their MAC source address and their VLAN tag. These values identify frames sent by another device in the L2 network. The device drops frames with a disallowed MAC source address or VLAN ID.

To set up Port Security, create a list of allowed MAC source addresses and VLAN IDs. If the device receives a frame with a MAC source address that is not on the allow list, the device can take a configurable action like sending an SNMP trap to the network management station or disabling the port.

**Note:**
The delivery state for the Port Security operation is globally disabled. The sub-function "Auto-disable" is also disabled.
Activating Port Security can help protect your network against injection of frames from unknown network nodes. However, if the Port security function is configured to auto-disable a given port when the function detects undesired frames, this can lead to a Denial of Service (DoS) situation. An attacker may even deliberately send deliberately crafted frames to cause a DoS.
Configure the Port Security function according to what best matches your situation.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > Port Security" on how to set up Port Security.

# 3.4 Help secure the network protocols used

## 3.4.1 Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol)

The GARP Multicast Registration Protocol (GMRP) and its successor, the Multiple MAC Registration Protocol (MMRP or MRP-IEEE Multiple MAC Registration Protocol), can be used to register group (that is, Multicast) MAC addresses dynamically and to automatically setup Multicast forwarding in a device. However, using these protocols can also pose a vulnerability if an attacker can snoop GMRP or MMRP frames or inject deliberately crafted GMRP or MMRP frames.

It is generally considered more secure to disable GMRP and MMRP.

**Note:**
The delivery state for both GMRP and MMRP is globally disabled.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Switching > GARP > GMRP" on how to set up GMRP
- Chapter "Switching > MRP-IEEE > MRP-IEEE Multiple MAC Registration Protocol" on how to set up MMRP

# 3.5 Help secure the redundancy protocols used

**Note:**
Securing the redundancy protocols used can also help enhance and maintain the availability of your network.

## 3.5.1 Set up RSTP guards and helper protocols

[CR3.1]

If you use RSTP, consider securing the RSTP guards:
- Consider enabling the BPDU guard function on Edge ports (delivery state: disabled).
- Consider enabling the BPDU filter function on Admin Edge ports (delivery state: disabled).
- Consider disabling the BPDU flood function on ports that have RSTP disabled (delivery state: disabled).

Help secure RSTP helper protocols:
- Consider disabling the L2 loop protection (delivery state: disabled). This helps protecting against a possible DoS attack, where an attacker sends malicious loop protection frames to the device, intending to trick it into disabling its respective port.

**Note:**
Enabling RSTP guards and helper protocols can help protect your network against rogue network nodes trying to diverting, snoop or manipulate legitimate traffic. However, if a function is configured to auto-disable a given port when the respective function is triggered, this can lead to a Denial of Service (DoS) situation. An attacker may even send deliberately crafted frames to cause a DoS. Configure the RSTP guards and helper protocols according to what best matches your situation.

Refer to the "Graphical User Interface" reference manual:
- Chapter "Switching > L2-Redundancy > Spanning Tree > Spanning Tree Global" on how to set up the BPDU guard and BPDU filter in the device
- Chapter "Switching > L2-Redundancy > Spanning Tree > Spanning Tree Port" on how to set up the Root guard, TCN guard, the port-related BPDU filter and the BPDU flood functions
- Chapter "Diagnostics > Loop Protection" on the device L2 loop protection function.

### 3.5.2 Set up the MRP (Media Redundancy Protocol) parameters.

[SR5.1] [CR5.1] [CR3.1]

If you use MRP, consider:
- Using tagged packets for the MRP VLAN
  This helps MRP availability by prioritizing MRP control packets.
- Specifying a MRP VLAN ID ≥1
  This causes MRP to use a standard VLAN tag in MRP control packets. This may require an existing VLAN plan.

**Note:**
The delivery state for MRP is disabled in the device, the MRP VLAN ID is 0.

Refer to the "Graphical User Interface" reference manual, chapter "Switching > L2 Redundancy > MRP" on how to set up MRP.

# 3.6 Set up the attack protection support functions

## 3.6.1 Set up the Denial of Service (DoS) parameters

[CR7.2]

Consider setting up DoS filters.

**Note:**
The delivery state for the DoS filters is globally disabled.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > DoS > DoS Global" on the device DoS filter functions.

## 3.6.2 Set up the rate limiter

[CR7.2]

Consider setting up the rate limiter for broadcast, Multicast or Unknown Unicast frames.

**Note:**
The delivery state for the broadcast, Multicast or Unknown Unicast rate limiters is disabled.

Refer to the "Graphical User Interface" reference manual, chapter "Switching > Rate Limiter" on the device Rate Limiter functions.

# 3.7 Set up Access Control Lists (ACLs)

[CR7.2] [NDR 1.13] [NDR5.2] [NDR5.2 RE1] [NDR5.3]

This chapter deals with ACLs, their function and the suggested setup steps. It describes the basic ACL functions. Extended ACL functions are outside the scope of this chapter.

Refer to the "Graphical User Interface" reference manual, chapter "Network Security > ACL" for the device ACL function.

## 3.7.1 Introduction

Access Control lists (ACLs) offer extensive and fine-grained control over the forwarding or dropping of data packets received or transmitted by the device. ACLs can therefore be useful to mitigate security threats in a straightforward yet detailed way.

**Note:**
In the GUI, an ACL is referred to as a "Group" (a rule group) that has a name and contains one or more rules.

A rule consists of:
- One or more criteria that have to match simultaneously (like a device port number, or an L3 protocol field) and
- One or more actions (mainly `permit` or `deny`) that the device takes when a data packet matches the rule's criterion

The following rule features are outside the scope of this chapter:
- A rule can have the following action:
  - Creating a log entry (only if assigned to an ingress port or a VLAN)

Each rule belongs to an ACL with a specific name and has the same type (IPv4-based) as the ACL and its sibling rules. Rules belonging to the same ACL are processed in ascending order of the individual rule index.

Every ACL has an implicit, invisible `deny` rule as the last rule <SL-C2>. As a result, if no explicit rule of an ACL matches a data packet, the device drops the data packet.

**Note:**
The IPv4-based numerical range starts with 1000.

For an ACL to take effect, assign the ACL: Choose a device port (source or destination port) or a VLAN. Assign a priority to this association, choose the desired direction of the data flow the ACL association shall apply to, and finally select an existing ACL name (followed by the ACL's internal number).

Properties of ACL assignments:
- On a device, 2 or more ACLs can be active simultaneously.
- Each assignment has a priority.
- If there are 2 or more ACLs of the same type assigned to the same device port or VLAN, the device processes the ACL with the higher priority first.

- If the same ACL is assigned to both a port and a VLAN, the device processes the port-related assignment first.
- A particular ACL can be assigned to more than one device port or VLAN, for example, to allow for bidirectional packet flow.

**Note:**
The device can apply ACLs only to received data packets.

**Note:**
To help ensure a defined processing order, specify for each assignment a priority that is unique in the scope of the device.

Because ACLs have a potentially heavy impact on the forwarding of data packets, ACLs should be planned accurately and generally need to be tested. If possible, test your planned and set-up ACLs in a test environment before applying the ACLs in a production environment. This allows for the modification, addition, or deletion of rules, ACLs, or ACL assignments that may have been overlooked during planning.

### 3.7.2 Resolving potential conflicts of aims for an ACL

When creating or modifying an ACL, there can be a conflict of aims between the security aspects of the network and the desire for the smooth functioning of the network:

- Security aspects of the network require the ACLs to be as restrictive as possible and to set up only the smallest possible set of `permit` rules. These ACLs are preferably applied to incoming data packets to drop unwanted data packets at the earliest possibility, and also to minimize the traffic within the device.
- Smooth functioning of the network desires the ACLs to be as permissive as possible and to set up only the smallest possible set of `deny` rules. The ACLs can be applied to outgoing data packets to maximize possible data packet processing in the device and to drop only the explicitly undesired data packets.

One possible way to address this conflict of aims is to put security first. That is, you plan and set up only the explicitly required `permit` rules. If the test results indicate that ACLs or their assignments are too restrictive, you can modify the ACLs (for example, add new `permit` rules) or their assignments appropriately.

### 3.7.3 Creating ACLs and associations

The following section describes one possible way of planning, setting up, testing, and administering ACLs for a device. Adapt these steps to suit your specific situation. Some steps may need to be applied iteratively.

**Note:**
You can plan the ACLs by setting up the ACLs directly on the device, or by using an off-line process and uploading the resulting ACLs to the device later.

**Planning**

- ☐ Make a list of packet types that explicitly need to be forwarded by the device.
- ☐ Common criteria for packets are (not exhaustive):
  - For an IPv4-based ACL: Source IP address, destination IP address, protocol, source TCP/UDP port, and destination TCP/UDP port
- ☐ As data traffic is typically bidirectional, plan 2 ACLs to consider the data packets for both directions. If the ACLs for different data directions are identical, consider creating only one ACL and assign it separately to each data direction, if possible.
- ☐ Determine to which device port or VLAN you assign the planned ACLs.
- ☐ Consider if it is advantageous to split up the set of packet types into subsets, so each subset can be processed by a particular ACL of a given type, assignment, and data packet direction. Name the individual ACLs (groups) to reflect the ACL's purpose, and, for example, by using a common name prefix for related ACLs.
- ☐ For each ACL, order its rules, using the following criteria:
  - Put the `permit` rule with the most general criteria first (for example, every packet with a certain VLAN tag). Give this rule the lowest index within the ACL. This takes care of the ACL function aspect.
    In the simplest case, this rule is general and has no exceptions. If exceptions are required, deal with them in the next planning step, "Refine the rule list…".
  - Put the `permit` rule with the second-most general criteria next (after the previous rule) by giving it a higher index than the first rule.
  - Proceed with the remaining `permit` rules in this order.
- ☐ Refine the ACL by planning exceptions:
  - For required exceptions to an `permit` rule, put a specific `deny` rule before the respective `permit` rule by giving it a lower index than the existing `permit` rule. This takes care of the ACL security aspect.
  - If further exceptions are required, insert the respective new `deny` rules before the respective existing `permit` rule (give it a lower index). This takes care of the ACL security aspect.
  - Put the rule with the most general exception first (give it the lowest index), followed by the rule with the second-most general exception (give it the second-lowest index), and so on.
  - Repeat these steps for every required exception in the given ACL.
  - A new `deny` rule may turn out to be too general and may therefore require further exceptions in the form of one or more additional preceding `permit` rules. This takes care of the ACL function aspect.

**Note:**
ACLs and their assignments can become complex. Consider testing the ACLs before you deploy them.

**Setup**

- ☐ Use the GUI, CLI, or network management software to set up the planned ACLs on the device, or
- ☐ Upload a configuration script (for example, generated by an offline configuration tool) to the device.

**Test**

- ☐ Activate and assign the ACLs on the device in a test setup.
- ☐ Generate test traffic that represents the expected traffic, that is, consisting of desired as well as of undesired data packets.

- ☐ Evaluate the packets received on the test end devices:
  - Look for unexpected packets. If unexpected undesired packets are transmitted by the test device, add a matching `deny` rule to the ACL plan and subsequently to the respective ACL.
    Note that the unexpected, undesired packets may include packets targeted at the device-under-test's management.
  - Look for missing packets. If expected desired packets are not received on the test end devices, consider adding a matching `permit` rule to the ACL plan and subsequently to the respective ACL.
    Note that the expected desired packets may include packets sent by the device-under-test's management.
- ☐ Evaluate the log entries created by the device:
  If you have configured your ACL rules to create log entries, inspect the log entries. This can be useful to determine, for example, why the device has dropped a packet.

**Administration**

- Give the ACLs descriptive names, for example, showing their purpose, possibly including the assignment to a port or VLAN, and the data direction.
- Consider:
  - Saving the ACLs separately from the device configuration or in addition to the device configuration, for example, as script files
  - Assigning the ACL a version number, if you have separate script files for each ACL
  - Using version control to track the ACL history

# 3.8 Set up the logging parameters

[CR1.2] [CR1.8] [CR2.11] [CR3.1]

Set up logging severity levels and destinations. The required settings depend:
- on your device logging policy
- on your remote logging policy

**Note:**
In the delivery state, the Syslog function is globally disabled.
The Syslog client in the device offers unencrypted communication only.
The persistent logging function, which writes logged events to a device-internal log, can be enabled or disabled. However, the audit trail created by the persistent logging function cannot be deleted once created and written to. Neither can the audit trail be deleted by resetting the device to the delivery state.

Refer to the "Graphical User Interface" reference manual, chapter "Diagnostics > Syslog" for the device Syslog function.

## 3.8.1 Audit trail (created by persistent logging)

[CR2.11]

The persistent logging function itself can be enabled or disabled. However, existing audit trail entries persist even after the persistent logging function has been disabled.

**Note:**
The audit trail cannot be deleted by resetting the device to the delivery state.

# 3.9 Set up the LLDP parameters <SL-C2>

The LLDP global operation setting can be *On* or *Off*. The delivery state is *Off* (disabled).

The device also offers the following basic port-related LLDP operating modes:

- *transmit*
  - The port transmits information about the device and the port itself to its neighbors.
  - The neighbors can collect that information, provide it to a management station, or process it themselves. The prerequisite is that the other devices in the same network have their individual *receive* function enabled.
- *receive*
  - The device collects information about its neighbors that it receives at the given port.
  - The device can provide this information to a management station or process the information itself. The prerequisite is that the other devices in the same network have their individual *transmit* function enabled.
- *receive and transmit* (delivery state ⚠)
  - The port transmits information about the device and the port itself to its neighbors.
  - The device also collects information about its neighbors that it receives at the given port.
- *disabled*
  - The port neither transmits any information about the device or the port itself, nor does it collect information received from other devices.

Enabling LLDP on the device has the following possible advantages and drawbacks:

- Security aspects:
  - Drawback: The device sends information about itself to its immediate neighbors. This might pose an attack surface.
  - Drawback: LLDP-unaware neighbors (for example, a hub) may distribute the device information beyond the immediate neighbors, possibly to the entire L2 network, which might pose an additional attack surface.
  - Advantage: The device can indirectly detect the addition, removal, or reconfiguration of an LLDP-enabled neighbor and report that event to a management station.
- Functional aspects:
  - Advantage: Topology discovery: The device can help perform a system inventory by collecting information about its neighbors and providing this information to a management station.
  - Advantage: The device can use the received information, for example, to automatically detect a duplex mismatch between one of its ports and the given port's immediate neighbor without the need to set up the Port Monitor function.

Disabling LLDP on the device has the following possible advantages and drawbacks:

- Security aspects:
  - Advantage: The device does not send out any explicit information about itself. This reduces the attack surface.
  - Drawback: The device cannot detect the addition, removal, or reconfiguration of an LLDP-enabled neighbor.
- Functional aspects:
  - Drawback: No Topology discovery: The device cannot help perform a system inventory.
  - Drawback: The device cannot automatically detect, for example, a duplex mismatch. For that, the Port Monitor function needs to be set up.

The above lists are not exhaustive. Evaluate the possible LLDP settings on the device according to your planned LLDP policy.

Enable or disable LLDP globally and choose the port-related operation modes according to your planned LLDP policy. You may elect to enable only the receive function. Setting up LLDP on the device may require that other network devices have their own LLDP function appropriately enabled.

Refer to:

- The "Graphical User Interface" reference manual, chapter "Diagnostics > LLDP > LLDP Configuration" for the device LLDP function
- The "Configuration" user manual, chapter "Operation diagnosis > Topology discovery" for an explanation of LLDP use cases

# A Security seal

## A.1 Overview

<SL-C2> [NDR 3.11]

The devices are equipped with mechanical components that have the function of a security seal. The type and location of the security seal depends on the device hardware family.

The purpose of the security seal is:
- To either thwart attempts to manipulate the internal hardware of the device
- Or to uncover manipulations through visible traces

A security seal can be of the following type:
- Glued front label (see on page 118 “Glued front label”)
- Potted device (see on page 119 “Potted device”)
- Security stickers (see on page 119 “Security stickers”)

# A.2 Details

The following chapters describe the properties and procedures for the mechanical security components, also called security seals.

**Note:**
The decommissioning procedures describe only the minimum steps to mark the security seals as decommissioned. Depending on your situation, additional decommissioning steps may be required.

## A.2.1 Glued front label

Security properties:
- The front label is glued to the front panel and completely covers the screws that are needed to open the device.
- There are no other screws that permit opening the device.

Tampering evidence:
- The front panel has exposed screws.
- The front label has cutaways, cuts, scratches, wrinkles or folds, especially in the corners where the screws are located.

Check procedures:
- New device:
  - Check that the front label is new and has no exposed screws, cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
- Device before sending it to the manufacturer for repair or replacement:
  - Check and record the condition of the front label.
    The front label shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
- Repaired device back from manufacturer:
  - If the device and the front label are both the same:
    Check the condition of the front panel against the recorded condition. The front label shall be approximately in the same condition as before.
    The front label shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device is the same but the front label is new:
    The front label is new and shall have no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device has been replaced (same device type):
    Check that the front label is new and has no exposed screws, and no cutaways, cuts, scratches, wrinkles, or folds, especially in the corners where the screws are located.
  - If the device has been replaced (other device type):
    Check according to the new device type’s security seal.

Mechanical decommissioning procedure:
- Cut off the front label corners to expose the screws.
- Scratch the front label, for example, with a flat screwdriver.

### A.2.2 Potted device

Security properties:
- The device hardware except the connectors and LEDs is potted with a hard casting compound.
- Trying to open the device leaves signs of mechanical processing.

Tampering evidence:
- The casting compound, the connectors, or the LEDs show signs of mechanical processing, like scratches, boreholes or partial application of new casting compound.

Check procedures:
- New device:
  - Check the condition of the casting compound, the connectors, and the LEDs.
    These components shall show no signs of mechanical processing.
- Device before sending it to the manufacturer for repair or replacement:
  - Check and record the condition of the casting compound, the connectors, and the LEDs.
    These components shall show no signs of mechanical processing.
- Repaired device back from manufacturer:
  - If the device is the same:
    Check the condition of the casting compound, the connectors, and the LEDs against the recorded condition.
    The condition of these components shall only deviate minimally from the recorded condition and show no signs of mechanical processing.
  - If the device has been replaced (same device type):
    Check the condition of the casting compound, the connectors, and the LEDs.
    These components shall be new and show no signs of mechanical processing.
  - If the device has been replaced (other device type):
    Check according to the new device type's security seal.

Mechanical decommissioning procedure:
- Deform the connectors and LEDs with a heavy tool, for example, with a hammer.

### A.2.3 Security stickers

Security properties:
- The security stickers used by the device manufacturer have the following properties:
  - Incisions that impede the unnoticed removal of a sticker
  - Self-delaminating layers that impede the unnoticed removal and re-application of a sticker
  - A hologram (optional) that impedes copying or counterfeiting a sticker
  - The stickers are non-standard, unique stickers that cannot be acquired on the open market.
- The security stickers can be in the following locations on the device:
  - The stickers cover screws necessary to open the device.
  - The stickers overlap (that is, mechanically connect) removable device parts.

**Note:**
For devices that offer customer-side modularity, the operator is responsible for applying their own, customer-specific, security stickers once the hardware configuration is complete.
The customer-specific security stickers shall offer appropriate security, for example, by having the properties of the manufacturer's stickers given above.
The customer-specific security stickers shall be applied in appropriate locations, for example, in the locations given above.

Tampering evidence:
- The security stickers show cutaways, cuts, scratches, wrinkles, folds, delamination, or (if applicable) a missing, changed or incomplete hologram.

Check procedures:
- New device:
  - Check the front panel and the stickers:
    The stickers shall be new and show no cutaways, cuts, scratches, wrinkles, folds, or delamination, but an intact hologram (if applicable).
  - For devices that offer customer-side modularity:
    Once the hardware configuration is complete, apply your own, customer-specific stickers.
- Device before sending it to the manufacturer for repair or replacement:
  - Check and record the condition of the stickers.
    The stickers shall show no cutaways, cuts, scratches, wrinkles, folds, delamination, but an intact hologram (if applicable).
- Repaired device back from manufacturer:
  - If the device is the same:
    Check the condition of the stickers against the recorded condition.
    Both should only deviate minimally.
  - If the device has been replaced (same device type):
    Check the condition of the stickers against the recorded condition.
    The stickers shall be new and show no cutaways, cuts, scratches, wrinkles, folds, or delamination, but an intact hologram (if applicable).
  - If the device has been replaced (other device type):
    Check according to the new device type’s security seal.

Mechanical decommissioning procedure:
- Destroy the security stickers:
  - Cut the stickers along the edge where the front and side panels of the device meet, for example with a screwdriver.
  - Pull off the loose parts of the stickers.
- Mark the front panel as decommissioned:
  - Scratch the front panel, for example with a flat screwdriver.

# B Password strength and policy guide

**Note:**
This chapter is informational only.

A strong password is hard to break by both a brute-force attack and a dictionary attack. "Hard to break" means that the mean time an attack needs to succeed is higher than a specified time.

A strong password is at the same time reasonably convenient to memorize without the need to write it down or use a password management application.

To make a quantitative statement about which password policy satisfies your specific situation, the following values have to be at hand:
- The required mean attack resistance time
- The maximum accepted breach probability after the mean attack resistance time (if < 50%)
- The maximum assumed attack rate (mitigated or unmitigated)
- The desired password class (high- or low-complexity, see below)

When these values are given, you can look up a password policy that satisfies your requirements (see on page 140 “Password policy lookup tables (quantitative)”).

For a more in-depth approach, the following chapters provide a short introduction to the key concepts of password strength.

The following topics are covered in this chapter:
- A detailed discussion of password classes and password strength
- The suggestion to prefer low-complexity passwords over high-complexity passwords and the reasons for the suggestion
- A general discussion of password policies and the resulting password schemes
- A detailed discussion of password schemes and the resulting password strength
- A precise guide to a recommended password policy, based on quantitative considerations

The following topics are outside the scope of this document:
- The automated generation of strong passwords
- The secure administration and distribution of passwords
- A possible password change policy
- The handling of password breaches or leaks
- The human aspects for passwords, like social engineering

## B.1 Password classes

**Note:**
The terms used in this chapter, like "password complexity", will be explained in the course of the sub-chapters.

Passwords can be grouped into 2 classes:
- High-complexity passwords:
  - High-complexity passwords have a minimum length.
  - They must consist of characters of the following character types: lowercase characters, upper case characters, digits and special characters.
  - Often, at least one character of each type is required.

  - The resulting password must not contain any word that can be found in a dictionary.
  - The minimum length required by the respective password policy is relatively low.
  - High-complexity passwords are relatively hard to memorize, especially if they are long.
  - Examples are "bZ1/Yc0$", "L{3}qz9M_k", or "*%Gr.43FD7xw".
- Low-complexity passwords:
  - Low-complexity passwords consist only of lowercase characters, for example, as a group of words.
  - Other character types are possible but not required.
  - The resulting password typically contains words that can be found in a dictionary.
  - The words in the password may be separated by a special character like "-".
  - The minimum length required by a specific password policy is higher than for high-complexity passwords of comparable strength.
  - Despite their greater length, low-complexity passwords are relatively easy to memorize.
  - Therefore, and counter-intuitively, low-complexity passwords may offer higher practical strength than high-complexity passwords.
  - Examples are "barrel-hamlet-famous", "imagine.lioness.knuckle.manager", or "natality painless yeomanry obligate quenched".

**Note:**
At the time of writing, high-complexity passwords are in more common use than low-complexity passwords. The reason is that users tend to create short passwords and common password policies favor high-complexity passwords.

# B.2 Password policies

A password policy typically has the following properties:
- It stipulates quantitative requirements:
  - The minimum password length
  - The allowed character types from which the password characters shall be taken (typically, the types are: lowercase characters, uppercase characters, digits, and special characters)
  - The minimum number of characters of each type
- It stipulates qualitative requirements:
  - The password must not contain any words from a given dictionary
- It stipulates time requirements:
  - The chosen password must be changed after a specified max. time period.

In essence, a password policy indirectly stipulates:
- The minimum password strength
- The password class (high- or low-complexity)

**Notes**:
- A password policy is a template for developing password schemes that satisfy given minimum requirements.
- The maximum time after which a password shall be changed has no effect on the password strength.
  - A required interval for changing a given password is reasonable if you assume that your password will be or has already been breached during the interval and you have not noticed.
  - This requirement also takes care of the possibility that a password may have leaked to an attacker.
  - While requiring a maximum interval for changing a password is common for many office and Internet IT systems, embedded systems typically do not enforce a regular password change by themselves.
  - For a system not enforcing regular password change, you can still minimize the probability of an unnoticed, successful password attack by specifying the required attack resistance time much higher than the expected lifetime of the system. This can be accomplished by setting up a strong password policy.

In the following table, the minimum values stipulated by some example password policies are given, along with an exemplary description of the policy results.

*Table 22: Password policy examples and qualitative password strength*

| Min, password length | Min no. of lowercase chars | Min no. of uppercase chars | Min no. of digits | Min no. of special chars | Password type and qualitative strength |
|---|---|---|---|---|---|
| 6 | 1 | 1 | 1 | 1 | High-complexity password, low strength ⚠ |
| 8 | 1 | 1 | 1 | 1 | High-complexity password, medium strength |
| 10 | 1 | 1 | 1 | 1 | High-complexity password, higher strength |
| 24 | 0 | 0 | 0 | 0 | Low-complexity password, high strength |

**Note:**
The qualitative password strength description in the above table assumes low security requirements. Your assessment may associate lower password strengths with the password policy examples given above. The password strength is considered in quantitative detail in the following chapters.

# B.3 Password schemes

A password scheme results from a given password policy and has the following properties.

- A password scheme uses a specific password policy as a template.
- A specific scheme is one of several possible schemes that satisfy a specific policy.
- Different schemes can generate passwords of different strength.
- A minimum scheme barely satisfies the policy requirements, but no more.
  Consequently, a password following a minimum scheme has a minimum strength.
- An extended scheme exceeds the policy's minimum requirements.
  A password following an extended scheme typically has larger strength than a password following a minimum scheme but in practice, extended schemes are rarely chosen by users.

**Note:**
In keeping with a conservative (skeptical) security approach, all password schemes discussed in this chapter are minimum schemes (see on page 126 "Conservative assumptions about users"). This helps ensure that the strength of an actual password meets or exceeds the required strength despite the minimum scheme it is based on.

# B.4 Password attack strategies

For an attacker who aims to gain login access by breaking the account password, there are 2 basic attack strategies:

- Dictionary attack:
  - A dictionary attack is highly efficient if a password is in the dictionary (list) of passwords the attacker knows.
  - This applies in particular to frequently used passwords on lists that are available on the Internet.
  - For maximum efficiency, these lists are ordered with the most frequently used passwords first, for example "123456", "secret", "password1", or "Password.1".
  - If the real password is not in the attacker's dictionary, the dictionary attack will fail.
- Brute-force attack:
  - A brute-force attack is necessary for highly random passwords that do not contain any word from a dictionary.
  - This attack basically tries all possible passwords for a given password scheme.
  - The number of possible passwords roughly grows exponentially with the password length.
  - A brute-force attack takes much longer than a dictionary attack but will eventually succeed, given enough time and a lack of mitigating factors.

**Note:**
An attacker can also try to steal a password or provoke a password leak, for example, by social engineering. Thus, for mitigation, passwords must be guarded well. These aspects are outside the scope of this document.

# B.5 Basic security assumptions

In keeping with the conservative security approach, this main chapter makes qualitative assumptions about:

- Attackers
- Users
- The attack context

## B.5.1 Aggressive assumptions about attackers

- An attacker looks for the most efficient way to gain access.
- To accomplish this, they will first look for the weakest aspects (most frequent existing vulnerabilities) of the target. This may make login attempts entirely redundant from the viewpoint of the attacker.
- If a login attack is necessary, they may use the following strategy:
  - They try to find an interface or a protocol that does not explicitly rate-limit attacks.
  - They try the most frequently used passwords first, so they will start with a dedicated dictionary attack. That is, they try a list of known frequent passwords.
  - If the dictionary attack does not succeed, they may either give up or switch to a brute-force attack.
  - They may either know the username of the account, or assume a low number of frequent usernames and perform a dictionary attack against the username. That is, they may use a list of frequent usernames. They may also try those usernames first that are typically associated with administrator privileges.
- If they do not succeed with the given target, interface, and protocol, they will switch to another target, interface, or protocol.

Conclusion: From a system view, closing or mitigating the weakest vulnerabilities first is necessary.

## B.5.2 Conservative assumptions about users

- When users have the choice of either creating their own password or accept a password suggestion randomly generated by a system, users will tend to create their own password. The consequences may be:
  - Given a liberal high-complexity password policy, a user-chosen password will in practice almost always be weaker than a randomly suggested password (see details below).
  - When forced to follow a strict high-complexity password policy, users may experience problems in memorizing the password and thus may tend to either write it down or use an unapproved password management application.
- When choosing a password, users will create the easiest possible password, for example, using only lowercase characters.
- When a password policy enforces a minimum length, users will tend to use an as short as possible password of lowercase characters that just satisfies the minimum length.
- When a password policy also enforces a minimum number of other character types, users will create the easiest possible password that barely satisfies the password policy. That is, they tend to use a minimum scheme (see on page 124 “Password schemes”):
  - When at least one uppercase characters is required, users will tend to use only one uppercase character, and may put it at the start.
  - When at least one digit is required, users will tend to use only one digit. They may put it at the end or replace a single letter with a digit (for example "A" -> "4").

  - When at least one special character is required, users will choose from a limited pool of special characters, and will not exhaust the possible pool of special characters.
  - The properties of user-chosen passwords may make these passwords more vulnerable to a dictionary attack, and possibly even to a brute-force attack.
- When given the choice of either creating a short, complex password or a longer, less complex password, users will tend to choose a short, complex password that barely satisfies the required password policy, although a longer, even less-complex password may be stronger.
- When asked to create a long password, users will also create a password that barely satisfies the required password policy.

Conclusion: From a system view, a password policy needs to be strong enough so passwords created according to the resulting minimum scheme have sufficient strength.

### B.5.3 Conservative assumptions about the attack context

- The username of an account under attack is assumed to be already known to the attacker. Username examples are "user", "admin", or "administrator".
  This essentially eliminates the effort and time for guessing the username and is a typical skeptical security assumption.
- The attack rate may or may not be limited by system settings. In the worst case, it is unlimited. In the absence of any network concept that detects anomalies or intrusions, this in essence means that the attacker is able to sustain a high attack rate for a long time.
- When performing a dictionary attack, the attacker has insider knowledge, that is, they already know the dictionary the password generation system uses to suggest long, low-complexity passwords.

**Note:**
We will shortly see that the seemingly paranoid assumption of an attacker knowing the complete password dictionary is not really a security problem. That is, a system-suggested, sufficiently long, low-complexity password can be both stronger and also easier to memorize than a typical high-complexity password of similar strength. This may seem counterintuitive but can be proven quantitatively, while assuming reasonable and even skeptical conditions.

# B.6 Quantitative password strength

## B.6.1 High-complexity passwords

The strength of a high-complexity password can be quantified as the number of possible passwords for a given scheme.

**Note:**
The preferred attack method to crack a high-complexity password is a brute-force attack. A good, high-complexity password will not give in to a dictionary attack.

For a high-complexity password of a given scheme, the number of possible passwords depends on the character type (more precisely: on the size of the pool from which the respective character is taken) and on how many characters of the given type appear.

The expected password strength depends on the assumptions how a password is created:
- Optimistic password strength:
  - Only truly random passwords have the highest possible expected information content.
  - Reasonable passwords of this type typically must be generated by an application.
  - Caveat: User-chosen high-complexity passwords typically have significantly less "randomness" (that is, entropy) and therefore tend to be weaker.
- Skeptic password strength:
  - When users are faced with a password policy, users will tend to make up a password scheme that barely satisfies the policy, that is, they will choose a minimum scheme.
  - User-chosen passwords therefore tend to have lower-than-possible strength.
  - The reason is that people tend to use certain characters more often than others.
  - For example, the character "e" appears in an general, English-language text with a probability of approx. 12.5% (1/8) and not with the probability of 3.8% (1/26).
  - To account for the unevenly distributed character frequencies to and pursue a skeptic approach, we can calculate with a smaller pool size than 26, for example, by assuming 8 (this approximates the frequency of the most frequent character, here, "e").
  - Similarly, to account for the unevenly distributed digit and special character frequencies, we can also calculate with a smaller pool size, for example, by also assuming 8.

The number of possible different high-complexity passwords of a given scheme is therefore:

$$N_{ph} = L^l \times U^u \times D^d \times S^s$$

Where:
- $N_{ph}$: Number of possible high-complexity passwords
- L: Pool size of lowercase characters (constant)
- l: Number of lowercase characters in the password (variable)
- U: Pool size of uppercase character (constant)
- u: Number of uppercase characters in the password (variable)
- D: Pool size of digits (constant)
- d: Number of digits in the password (variable)
- S: Pool size of special characters (constant)
- s: Number of special characters in the password (variable)

We see that the password strength grows with the length of the password. Unsurprisingly, we see that adding more characters, digits or special characters to an existing password makes the resulting password stronger.

**Note:**
A simple generator for high-complexity passwords, following a minimum password scheme, might in fact sometimes suggest passwords like "123456", "abcdef" or "secret". These passwords are weak because they most likely are in an attacker's dictionary. The skeptic probability for a randomly generated password to be like one of the given examples is $8^{-6} \approx 3.81 \times 10^{-6}$. Because there are many known weak passwords, the probability of a randomly generated password matching one of the known weak passwords is considerable – possibly too high to be accepted. Therefore, **checking a system-suggested or user-chosen high-complexity password against a list of known weak passwords can be regarded as mandatory.**

### Example (optimistic password strength)

An example password policy requires a length of 8 characters, with at least one lowercase character, one uppercase character, one digit, and one special character.

In keeping with the conservative security approach given, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the password policy: The user chooses to use 5 lowercase characters, one uppercase character, one digit, and one special character.

*Table 23: High-complexity password components, optimistic strength*

| Character class ID | Class description | Pool characters | Assumed pool size |
|---|---|---|---|
| L | Lowercase characters | a-z | 26 |
| U | Uppercase characters | A-Z | 26 |
| D | Digits | 0-9 | 10 |
| S | Special characters | !"#$%&()*+'.-/:; | 16[1] |

1. The special character pool size is given as 16 although the ASCII codes provides for 32 special characters. The reason for the smaller assumed pool size is that some characters may be impossible or hard to type on a given keyboard and may therefore not be chosen by a user.

The optimistic number of possible passwords of this scheme is therefore:

$$N_{pho} = 26^5 \times 26^1 \times 10^1 \times 16^1 = 49{,}426{,}524{,}160 \approx 4.94 \times 10^{10}$$

Where:
- $N_{pho}$: Number of possible high-complexity passwords, optimistic approach

**Note:**
Modifying an existing password by replacing lowercase characters by digits or special characters can actually make the password weaker. This seems to contradict the recommendation to include digits and special characters in a password. The explanation is that replacing lowercase characters by digits or special characters only helps against dictionary attacks, not against brute-force attacks. The recommendation to include digits and special characters is based on the assumption that the password prior to the modification is vulnerable to a dictionary attack. That again means that the original password wasn't a high-complexity password to begin with.

### Example (skeptic password strength)

*Table 24: High-complexity password components, skeptic strength*

| Character class ID | Class description | Pool characters | Assumed, reduced pool size |
|---|---|---|---|
| L | Lowercase characters | a-z | 8 |
| U | Uppercase characters | A-Z | 8 |
| D | Digits | 0-9 | 8 |
| S | Special characters | !#$&+.-/ (example) | 8 |

Assuming the same password scheme as above, but with a reduced pool size of 8 for each character type to account for frequent characters or digits like "e", "1", or ",", the skeptic number of possible passwords of this scheme is therefore:

$N_{phs} = 8^5 \times 8^1 \times 8^1 \times 8^1 = 8^8 = 2^{24} = 16{,}777{,}216 \approx 1.67 \times 10^7$

Where:
- $N_{phs}$: Number of possible high-complexity passwords, skeptic approach

We see that the skeptic password strength is much smaller than the optimistic strength.

## B.6.2 Low-complexity passwords

The strength of a low-complexity password can also be quantified as the number of possible passwords for a given scheme.

**Note:**
The preferred attack method to crack a low-complexity password is a dictionary attack. A brute-force attack is possible but practically futile. Given the bigger length of a low-complexity password (for example, 24 lowercase characters), the skeptic number of possible passwords is on the order of $10^{21}$. The optimistic number of possible passwords is even on the order of $10^{33}$.

A low-complexity password contains words from a dictionary (word list). The strength of a low-complexity password depends on the following aspects:
- It strongly depends on the number of words in the password.
- It moderately depends on the size of the dictionary.
- It marginally depends on the detailed rules how passwords are chosen from the dictionary.
- It is virtually independent of the word length as long as a minimum length is maintained.

For the sake of security skepticism, let's make 4 conservative assumptions:
- The dictionary from which the words are taken (for example, by a password-generating application) has only straightforward size (for example, only 2,048 entries).
- The entire dictionary is already known to the attacker. This is a very conservative assumption.
- Words from the dictionary shall be selected only once.
  - This excludes the equivalent of weak passwords like "111111" or "aaaaaa".
- Words selected from the dictionary shall not be adjacent to any of the words already selected.
  - This excludes the equivalent of weak of passwords like "123456", "654321, "abcdef" or "fedcba".

We will shortly see that a low-complexity password scheme following these assumptions still results in passwords of high skeptic strength. The optimistic strength for a low-complexity password does not need to be examined in detail because such a password would in essence describe a long, high-complexity password, against which a dictionary attack is practically futile.

There is one additional condition that needs to be satisfied:

- The minimum word length shall be high enough to contain much more possible words than there are words in the dictionary.
  - This ensures that the list entropy is not undermined by a low word entropy (we will discuss entropy shortly, (see on page 137 “Password entropy”)). This condition is easily satisfied by a password policy requiring a minimum number of characters.

*Table 25: Low-complexity password properties*

| Parameter ID | Parameter | Description |
|---|---|---|
| S | Dictionary size | Number of words in the dictionary |
| w | Number of words | Number of such words in the password. |

The approximate number of possible different low-complexity passwords of a given scheme is therefore:

$N_{plo} \approx S^w$

Where:

- $N_{plo}$: Number of possible low-complexity passwords, optimistic approach
- S: Dictionary size
- w: Number of words used in the password

**Note:**
For w ≥ 2, the above equation gives a slightly optimistic strength. Compared to the exact value, assuming a dictionary size of 2,048 and 6 words, it is off by +2.3%. For fewer words, the deviation is lower. For w = 1, the equation gives the correct strength.

The exact equation is:

$N_{ple} = S \times (S - 3) \times (S - 6) \times \ldots \times (S - 3 \times (w-1))$

Where:

- $N_{ple}$: Number of possible low-complexity passwords, exact approach

**Note:**
The multipliers S - 3, S - 6 etc. stem from the fact that the choice of the first word has S possibilities but the choice of the 2nd word has only (S - 3) possibilities. This is because the first word chosen, its immediate predecessor as well as its immediate successor shall not be chosen again, according to the last of the above given skeptic assumptions.

This unwieldy formula can safely be approximated by a skeptic approximation, that is, by dividing the result of the approximate, optimistic equation by 2:

$N_{pls} = S^w / 2$ (for w ≥ 2)

Where:

- $N_{pls}$: Number of possible low-complexity passwords, skeptic approach

### Example

**Note:**
In keeping with the conservative security approach, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the password policy. The word list is assumed to contain only 2,048 words. The minimum word length is 6.

An example password policy requires a length of 24 characters (therefore 4 words with 6 characters minimum length each), with at least 1 lowercase character. Uppercase characters, digits, and special characters are possible but not required. Given the choice of making up their own password, a user chooses the password "barrel-hamlet-famous-staple", possibly with the help of an application.

The number of possible passwords of this scheme is therefore:

$N_{pl} = 2{,}048^4 / 2 = 2^{43} = 8{,}796{,}093{,}022{,}208 \approx 8.79 \times 10^{12}$

**Note:**
Despite the above, conservative assumptions, the low-complexity password strength in this example is much higher than for the aforementioned high-complexity password examples. This holds even if we compare the conservative strength of the low-complexity password to the optimistic strength of the high-complexity password.

# B.7 Attack resistance time (quantitative)

**The theoretical (but impractical) resistance to an attack** can be calculated as the maximum time the password withstands an attack until it is broken with 100% probability.

This time can be calculated as the number of necessary attacks, divided by the attack rate:

$T_{sb} = N_a / r_a$

Where:
- $T_{tb}$: Theoretical max. time to 100% probable password breach, in seconds
- $N_a$: Number of necessary attacks
- $r_a$: Attack rate (in attacks per second)

Of course, accepting a 100% probability for a password breach is a weak concept. In practice, a 50% probability is often assumed instead because the assumption of 50% makes the equations a bit easier.

**The practical resistance to an attack** is typically calculated as the mean time the password withstands the attack until it is broken with 50% probability. This is half the time for a 100% probability breach:

$T_{sp} = N_a / r_a / 2$

Where:
- $T_{pb}$: Mean time to practical (50% probable) password breach

The (unsurprising) result is that the attack resistance time increases with a higher number of possible different passwords and decreases with higher attack rate.

The (unsurprising) conclusion is: To make a login password as strong as possible, you have 2 possibilities, and you can combine these:
- Specify a strong password policy by setting up an appropriate password policy, either for high-complexity or for low-complexity passwords, thus enabling strong-enough resulting minimum schemes.
- Wherever possible, set up a login policy to lower the effective attack rate for a given interface and protocol.

### B.7.1 Examples, unmitigated attack rate

In keeping with the conservative security approach, the assumed attack rate is high and unmitigated, so we assume 1,000 attacks per second. An example for such a possible high rate is an attack using SNMPv3 get requests. SNMP has no obvious means of attack rate mitigation. We accept a 50% probability of a breach.

For the password example strengths in the previous chapters, the mean attack resistance time is:

*Table 26: Attack resistance time for different password scheme examples, for an unmitigated attack rate*

| Password class | Approach | Password strength | Unmitigated attack rate per second | Attack resistance time | |
|---|---|---|---|---|---|
| | | | | in seconds | in usual units |
| High complexity | Optimistic | $4.94 \times 10^{10}$ | 1,000 | $2.47 \times 10^{7}$ | 9.53 months |
| | Skeptic | $1.67 \times 10^{7}$ | 1,000 | $8.38 \times 10^{3}$ | 2.33 hours |
| Low complexity | Skeptic | $8.79 \times 10^{12}$ | 1,000 | $4.39 \times 10^{9}$ | 139 years |

We see that despite the very conservative assumptions for the low-complexity password, the low-complexity password results in a much attack higher attack resistance time than a high-complexity passwords. This holds even if we compare to the optimistic case of the high-complexity password.

### B.7.2 Attack rate mitigation

The rate (strength) of a dictionary or brute-force attack can be given as the number of login attempts per second.

The lower the attack rate, the longer it takes to reach the mean number of attempts until the password is accepted.

Let's assume that an attacker is capable of delivering many attacks per second to a certain interface and protocol (an attack rate ≥ 1 / sec = 3,600 / hour). How this affects the system under attack depends on if the system has mitigating parameters set up. Examples for protocols offering such mitigation parameters are HTTPS and SSH.

There are 2 settings that provide mitigation:
- The maximum number of successive failed login attempts until the system enforces a waiting time
- The enforced waiting time the system has set up.

The assumed high attack rate is thus effectively reduced to:

$r_{am} = n_{sf} / t_w$

Where:
- $r_{am}$: Mitigated attack rate
- $n_{sf}$: Number of successive failed login attempts
- $t_w$: The enforced waiting time

We see that the mitigated attack rate only depends of the mitigating parameters' values, not on the high attack rate originally assumed. This makes these mitigations parameters particularly effective.

**Note:**
This approximate equation is slightly skeptic. The real mitigated attack rate is slightly lower.

### Mitigation examples

Skeptic example: An example system is set up to ignore logins after 10 successive failed login attempts. This is a fairly high value, assuming users tend to value convenience. After the condition triggers, the target system enforces a one-minute wait time (a fairly low value, also convenient) and ignores any login attempts during that time. What is convenient for the users, is regarded skeptically from a security perspective.

$r_{am}$ = 10 / 1 min = 10 / min = 600 / hour.

Optimistic example: A system ignore logins after already 5 successive failed login attempts (a smaller value) and then enforces a 2-minute wait time (a larger value). These values may be more inconvenient for the users, but are regarded as more desirable from a security perspective.

$r_{am}$ = 5 / 2 min = 2.5 / min = 150 / hour.

We see that setting up reasonable attack mitigation parameters can significantly lower the effective attack rate, often by an order of magnitude or more.

## B.7.3 Examples, mitigated attack rate

The login with the protocols HTTPS and SSH provides mitigating parameters. In keeping with the conservative security approach, the assumed mitigated attack rate is relatively high because the mitigation parameters were chosen to be convenient for the users. So we assume 600 attacks per hour (that is, 10 per minute or 1/6 per second).

For the password example strengths in the previous chapters, the mean attack resistance time is:

*Table 27: Attack resistance time for different password scheme examples, for a mitigated attack rate*

| Password class | Approach | Password strength | Mitigated attack rate per second | Attack resistance time | |
|---|---|---|---|---|---|
| | | | | in seconds | in usual units |
| High complexity | Optimistic | $4.94 \times 10^{10}$ | 1/6 | $1.48 \times 10^{11}$ | 4,698 years |
| | Skeptic | $1.67 \times 10^{7}$ | 1/6 | $5.03 \times 10^{7}$ | 1.59 years |
| Low complexity | Skeptic | $8.79 \times 10^{12}$ | 1/6 | $2.63 \times 10^{13}$ | 836,194 years |

**Note:**
We see that attack rate mitigation can be very effective in raising the provided attack resistance time. However, this only applies to protocols that offer the said mitigation parameters. In the worst case (that is, with a skeptic approach), we still have to assume the unmitigated attack rate, as may be the case for the SNMPv3 protocol.

# B.8 Required attack resistance time (quantitative)

For a required mean attack resistance time, an assumed attack rate, and a specific, accepted breach probability, we can calculate the required password strength:

$N_{pr} = T_{ar} \times r_a \times (1 / P_b)$

Where:
- $N_{pr}$: Required password strength
- $T_{ar}$: Required attack resistance time
- $r_a$: Assumed tack rate (in attacks per second), either mitigated or unmitigated
- $P_b$: Accepted breach probability when the required mean attack resistance time has elapsed

The (unsurprising) result is that the required password strength increases with a higher required attack resistance time, with a higher assumed attack rate and with a lower accepted breach probability.

The commonly accepted breach probability is 50%. This gives the simplified equation:

$N_{pr} = T_{ar} \times r_a \times 2$

**Note:**
Your situation may require a lower breach probability than 50%. In this case, use the former equation.

# B.9 Password entropy

The strength of a given password scheme can be expressed as:
- Possibilities (symbol N): The number of possible different passwords
- Entropy (symbol H): The expected information content for a random number in the range 1…N. (The symbol H is the uppercase Greek letter Eta.)

Entropy in the context of information theory has the following properties:
- It has the unit "shannon" (short: "Sh"). It can be non-integer.
- Its value can be interpreted as the minimum number of bits required to hold a number in the range 1…N. If the entropy value is non-integer, it has to be rounded up to the nearest integer to give the minimum number of bits.

The password entropy is a more convenient way of representing the password strength than the number of possible passwords. Whereas the typical number of possible passwords for a given scheme is > $10^6$, the entropy of a reasonable strong password typically is in the range 20…45. The reason is that there is a logarithm involved.

The entropy can be calculated from the password strength:

$H_p = \log_2 (N_p)$

Where:
- $H_p$: The password entropy (min. number of bits required to represent $N_p$)
- $\log_2$: The Logarithm function to the base of 2
- $N_p$: The password strength (as the number of possibilities)

The calculated entropy of a given password strength can be non-integer number. In keeping with security skepticism, the number of bits associated with the entropy is rounded to the nearest integer in the following way:
- For the entropy required for a certain password scheme, the number of bits is rounded up.
- For the entropy provided by a certain password scheme, the number of bits is rounded down.

Generally, there are 3 basic types of entropy in relation to password strength:
- The **Shannon entropy** $H_1$ represents the **detailed** approach.
- The **max. entropy** $H_{max}$ represents the **optimistic** approach.
- The **min. entropy** $H_{min}$ represents the **skeptic** approach.

As we follow the skeptic approach, we only deal with the min. entropy $H_{min}$.

In this main chapter, using only the min. entropy is incorporated by the following approach:
- For high-complexity passwords, the applied skeptic pool size for any character type is chosen to be only 8, instead of 26, 10, or 16 (or even 32). This results in 3 sh per character.
- For low-complexity passwords:
  - Only the size of a known dictionary (for example, 2,048) is taken into account. This results in a dictionary entropy of 11 sh.
  - The length of individual words is ignored, only a minimum length is required (for example, 6).
  - The strength of a given password scheme is calculated conservatively, by dividing the approximate formula's value by 2, if the number of words in the password is ≥ 2.

# B.10 Calculating the required password entropy

For a required mean attack resistance time, a specified attack rate, and a specified, accepted breach probability, we can calculate the required password strength as the required password entropy.

Given the above equation $N_{pr} = T_{ar} \times r_a \times (1 / P_b)$ (see on page 136 “Required attack resistance time (quantitative)”), the entropy is:

$H_{prb} = \log_2 (N_{pr}) = \log_2 (T_{ar} \times r_a \times (1 / P_b))$

$H_{prb} = \log_2 (T_{ar} \times r_a) - \log_2 (P_b)$

Where:
- $H_{prb}$: Required password entropy for the required breach probability $P_b$
- $N_{pr}$: The required password strength (as the number of possibilities)
- $T_{ar}$: Required attack resistance time
- $r_a$: Assumed attack rate (in attacks per second), either mitigated or unmitigated
- $P_b$: Accepted mean breach probability when the required mean attack resistance time has elapsed

In theory, a breach probability of 100% is possible (although mostly not accepted). This leads to:

$H_{pr100} = \log_2 (T_{ar} \times r_a / 1) = \log_2 (T_{ar} \times r_a)$

Where:
- $H_{pr100}$: The theoretically required password entropy for a breach probability of 100%

In literature, a breach probability of 50% is often accepted. This leads to:

$H_{pr50} = \log_2 (T_{ar} \times r_a / 0.5) = \log_2 (T_{ar} \times r_a) + \log_2 (2) = \log_2 (T_{ar} \times r_a) + 1$

$H_{pr50} = H_{p100} + 1$

Where:
- $H_{pr50}$: The required password entropy for a breach probability of 50%

We see that an accepted breach probability of 50% raises the required password entropy by 1 sh, in comparison to the theoretical (and practically unacceptable) breach probability of 100%.

The generalized formula for a required password entropy, assuming a specified breach probability is:

$H_{prb} = H_{p100} - \log_2 (P_{br}) = H_{p100} + | \log_2 (P_{br}) |$

Where:
- $H_{prb}$: The required password entropy for an arbitrary breach probability
- $P_{br}$: The required breach probability (< 1) within the attack time.
- $| x |$: the absolute value of x (always >0 even if x <0)

We see that an arbitrarily required breach probability < 100% simply adds more required entropy to the theoretical (and undesirably low) password entropy $H_{pr100}$.

**Note:**
Because $P_{br} < 1$, $\log_2 (P_{br}) < 0$ and therefore $-\log_2 (P_{br}) > 0$.

# B.11 Password policy lookup tables (quantitative)

To find a password policy that quantitatively meets the specified requirements, we need the following values at hand:

- The required mean attack resistance time
- The maximum accepted breach probability after the mean attack resistance time (if < 50%)
- The maximum assumed attack rate (mitigated or unmitigated)
- The desired password class (high- or low-complexity)

We can then look up the required password policy, using a series of tables:

## B.11.1 Password entropy lookup tables

Table input:

- $T_{ar}$: Required attack resistance time
- $r_a$: Assumed attack rate

Table output:

- $H_{pr50}$: Required password entropy for an accepted breach probability of 50%

*Table 28: Lookup table for required password entropy (in Sh, rounded up)*

| Required attack resistance time $T_{ar}$ | Assumed attack rate $r_a$ | | | | | |
|---|---|---|---|---|---|---|
| | 1 / min | 10 / min | 1 / sec | 10 / sec | 100 / sec | 1,000 / sec |
| 1 day | 12 | 15 | 18 | 21 | 25 | 28 |
| 1 week | 15 | 18 | 21 | 24 | 27 | 31 |
| 1 month | 17 | 20 | 23 | 26 | 29 | 33 |
| 1 year | 21 | 24 | 26 | 30 | 33 | 36 |
| 10 years | 24 | 27 | 30 | 33 | 36 | 40 |
| 100 years | 27 | 30 | 33 | 36 | 40 | 43 |
| 1,000 years | 30 | 34 | 36 | 40 | 43 | 46 |

### Password entropy lookup table for < 50% breach probability

Table input:
- $P_{br}$: Required max. breach probability after the acceptable mean attack time has elapsed

Table output:
- $H_{ab}$: Required additional password entropy for breach probability $P_{br}$

*Table 29: Lookup table for additional required password entropy (in Sh, rounded up)*

| Accepted max. breach probability $P_{br}$ | Required additional password entropy $H_{ab}$ |
|---|---|
| 50% | 0 |
| 10% | 3 |
| 1% | 6 |
| 1‰ ($10^{-3}$) | 9 |
| 100 ppm ($10^{-4}$) | 13 |
| 10 ppm ($10^{-5}$) | 16 |
| 1 ppm ($10^{-6}$) | 19 |
| 100 ppb ($10^{-7}$) | 23 |
| 10 ppb ($10^{-8}$) | 26 |
| 1 ppb ($10^{-9}$) | 29 |

For < 50% breach probability, add the required password entropies from the 2 tables:

$H_{prb} = H_{pr50} + H_{ab}$

Where:
- $H_{prb}$: Required password entropy for a breach probability $P_{br}$ < 50%
- $H_{pr50}$: Required password entropy for standard breach probability of 50%
- $H_{ab}$: Additional required entropy for an accepted breach probability < 50%

## B.11.2 Password policy lookup table, low-complexity passwords

Table input:
- $H_{prb}$: Required password entropy for the required breach probability

Constants:
- S: Dictionary size, assumed to be 2,048
- $L_w$: Minimum length of any word in dictionary: assumed to be 6

Table output:
- $n_w$: Minimum number of words required by the password policy
- $n_c$: Minimum overall number of characters required by the password policy

*Table 30: Lookup table for password policy (for low-complexity passwords)*

| Required password entropy ($H_{prb}$) | Required no. of words $n_w$ | Required no. of characters $n_c$ | Required no. of any character type | Provided entropy (skeptical) |
|---|---|---|---|---|
| 12…21 | 2 | **12** | 0 | 21 |
| 22…32 | 3 | **18** | 0 | 32 |
| 33…43 | 4 | **24** | 0 | 43 |
| 44…54 | 5 | **30** | 0 | 54 |
| 55…65 | 6 | **36** | 0 | 65 |
| 66…75 | 7 | **42** | 0 | 76 |

Notes on low-complexity passwords (see on page 130 “Low-complexity passwords”):

- **The use of only lowercase characters permitted.** This is a conservative approach. Other character types are possible but will not increase the provided password entropy.
  - Reason: The entropy of a low-complexity password is already calculated in a very conservative way by the dictionary entropy.
- **The password policy need not require a minimum number of other character types.**
  - This is why 0 is given as the requirement in the table above.
- The number of words in the password is a required minimum.
  - A higher word count will **significantly** increase the password entropy.
- The dictionary size is assumed to be 2,048 (11 sh of entropy). This is a conservative approach.
  - Higher dictionary sizes will result in **moderately** higher password entropy. For example, a dictionary size of 4,096 represents 12 sh of entropy.
- The detailed rules how passwords are chosen from the dictionary, have a **marginal** effect on the entropy: The stricter the rules, the lower the skeptic entropy.
- The minimum word length is assumed to be 6. This is a conservative approach. Higher minimum word lengths will **not** increase the password entropy.
  - Reason: An individual word’s entropy must be much higher than the dictionary entropy, the key parameter for a low-complexity password. Only then, the dictionary entropy is unimpaired by the word entropy.
  - Calculation: For 11 sh of dictionary entropy and 3 sh skeptic entropy for a lowercase character, we need words with at least 4 characters. To make a conservative approximation, we chose a word length of 6 which represents 18 sh of skeptic entropy.

### B.11.3 Password policy lookup table, high-complexity passwords

Table input:

- $H_{prb}$: Required password entropy for the accepted breach probability

Constants:

- L: Pool size of lowercase characters (assumed to be 8)
- U: Pool size of uppercase character (assumed to be 8)
- D: Pool size of digits (assumed to be 8)
- S: Pool size of special characters (assumed to be 8)

Table output:
- $n_c$: Required total number of characters in the password

*Table 31: Lookup table for password policy (for low-complexity passwords)*

| Required password entropy ($H_{prb}$) | Req. total chars ($n_c$) | Req. lowercase chars (l) | Req. uppercase chars (u) | Required digits (d) | Req. special chars (s) |
|---|---|---|---|---|---|
| 12…24 | **8** | **1** | **1** | **1** | **1** |
| 25…27 | **9** | **1** | **1** | **1** | **1** |
| 28…30 | **10** | **1** | **1** | **1** | **1** |
| 31…33 | **11** | **1** | **1** | **1** | **1** |
| 34…36 | **12** | **1** | **1** | **1** | **1** |
| 37…39 | **13** | **1** | **1** | **1** | **1** |
| 40…42 | **14** | **1** | **1** | **1** | **1** |
| 43…45 | **15** | **1** | **1** | **1** | **1** |
| 46…48 | **16** | **1** | **1** | **1** | **1** |
| 49…51 | **17** | **1** | **1** | **1** | **1** |
| 52…54 | **18** | **1** | **1** | **1** | **1** |
| 55…57 | **19** | **1** | **1** | **1** | **1** |
| 58…60 | **20** | **1** | **1** | **1** | **1** |
| 61…63 | **21** | **1** | **1** | **1** | **1** |
| 64…66 | **22** | **1** | **1** | **1** | **1** |
| 67…69 | **23** | **1** | **1** | **1** | **1** |
| 70…72 | **24** | **1** | **1** | **1** | **1** |
| 73…75 | **25** | **1** | **1** | **1** | **1** |

**Note:**
The suggested password length starts with 8. The required password entropies in the range 12…21 sh could theoretically be satisfied with a shorter password length 4…7. These short password policies are not suggested because, from a skeptic security perspective, the resulting passwords are highly susceptible to dictionary attacks as well as brute-force attacks.

Note on the required numbers of lowercase characters (l), uppercase characters (u), digits (d), and special characters (s):
- All characters types are required to appear a minimum number of times in the password policy, for example, 1 per type.
- Requiring a higher minimum number for the digits or special characters will **not** yield higher password entropy because the skeptic assumptions about the pool sizes for the character types are the same.
- A password policy should therefore allow for the other characters but only require a minimum number of 1.
- Theoretically, a minimum number of 0 would also suffice if the password were strictly random, for example, created by an application.
- In practice, with user-chosen passwords, this is not viable: Users may understand such a policy as an invitation to create weak passwords, for example, consisting only of lowercase characters or digits, like "abcdefgh" or "12345678".

# C Considerations for manually entered keys

**Note:**
This chapter is informational only.

Symmetric cryptography keys can be considered special cases of high-complexity passwords. Therefore, some aspects for passwords also apply to symmetric cryptographic keys.

**Note:**
This chapter deals exclusively with keys for symmetric cryptography. A key usually is for symmetric cryptography if the same key is used for encryption as well as for decryption.
For asymmetric cryptography, the comparison of keys to passwords does not apply. A key usually is for asymmetric cryptography when the key is part of a key pair (public and private key).

If you need to enter keys for symmetric cryptography manually, consider the following recommendations:

- General recommendation:
  Include as much entropy ("randomness") in the key string as possible. A key with a higher entropy is stronger because it is harder to guess by a brute-force attack.
- Detailed recommendations:
  - If possible, let a software tool generate a random value of the required length and in the required format (for example, hexadecimal- or Base64-encoded).
  - If you have to enter a key value manually, avoid including character sequences that repeat, increase or decrease. This lowers the key strength.
    If possible, set up and follow (better: enforce) a policy for manually generated keys.

To help ensure reasonable key strength (see on page 149 “Residual weaknesses of user-generated keys”).

## C.1 Quantitative key strength

The strength of a key can be quantified as the number of possible keys for a given key entry scheme. The key entry scheme depends on the key entry policy.

Depending on the actual policy:

- The scheme can be derived from the policy in an optimistic or a skeptic way (see on page 146 “Key entry as ASCII string”).
- The policy strictly specifies a scheme (see on page 147 “Key entry as hexadecimal string”).

### C.1.1 Key entry as ASCII string

Let us assume that an example key policy for the entry of a 128-bit key requires an ASCII string of variable length with at least 12 characters, including at least 2 uppercase characters, 2 digits, and 2 special characters.

This is a considerably stronger policy than the password policy assumed in the chapter about high-complexity passwords (see on page 129 “Example (optimistic password strength)”). The reason is that when a manually entered key serves as a master key, its minimum strength should be higher than that of a password.

**Note:**
To account for the fixed key length, the key value is derived from the variable length ASCII string by a cryptographic hash function, for example, SHA-1. The resulting key has a different value and representation. It may look more random than the original ASCII string, but the derived key has the same strength as the ASCII string.

#### Example (optimistic key strength)

In keeping with the conservative security approach given, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the key entry policy: The user chooses to use 6 lowercase characters, 2 uppercase characters, 2 digits, and 2 special characters.

*Table 32: Key of length 12 ASCII characters, skeptic strength*

| Character class ID | Class description | Pool characters | Assumed pool size |
|---|---|---|---|
| L | Lowercase characters | a-z | 26 |
| U | Uppercase characters | A-Z | 26 |
| D | Digits | 0-9 | 10 |
| S | Special characters | !"#$%&()*+’.-/:; | 16[1] |

1. The special character pool size is given as 16 although the ASCII codes provides for 32 special characters. The reason for the smaller assumed pool size is that some characters may be impossible or hard to type on a given keyboard and may therefore not be chosen by a user.

The optimistic number of possible keys of this scheme is therefore:

$$N_{pkao} = 26^6 \times 26^2 \times 10^2 \times 16^2 \approx 5.34 \times 10^{15}$$

Where:
- $N_{pkao}$: Number of possible keys, ASCII entry, optimistic approach

We see that the optimistic number of possible keys enforced by the key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy enforces only a tiny fraction of about $10^{-23}$ of the possible keys even in the optimistic view.

#### Example (skeptic key strength)

We assume a reduced pool size of 8 for each character type to account for frequent characters or digits like "e", "1", or ",".

*Table 33: Key of length 12 ASCII characters, skeptic strength*

| Character class ID | Class description | Pool characters | Assumed, reduced pool size |
|---|---|---|---|
| L | Lowercase characters | a-z | 8 |
| U | Uppercase characters | A-Z | 8 |
| D | Digits | 0-9 | 8 |
| S | Special characters | !#$&+.-/ (example) | 8[1] |

1. The special character pool size is given as 8 although the ASCII codes provides for 32 special characters. The reason for the smaller assumed pool size is that some characters may be impossible or hard to type on a given keyboard and may therefore not be chosen by a user.

The skeptic number of possible keys is therefore:

$$N_{pkas} = 8^6 \times 8^2 \times 8^2 \times 8^2 = 8^{12} = 2^{36} \approx 6.87 \times 10^{10}$$

Where:
- $N_{pkas}$: Number of possible keys, ASCII entry, skeptic approach

We see that the skeptic number of possible keys enforced by the above key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy enforces only a minute fraction of about $10^{-28}$ of the possible keys.

### C.1.2 Key entry as hexadecimal string

#### Example (optimistic policy)

Let us assume that an example key policy for the entry of a 128-bit key requires a hexadecimal string with a length between 16 and 32 characters.

In keeping with the conservative security approach given, the assumed password scheme chosen by the user is a minimum scheme that barely satisfies the key entry policy: The user chooses to use just 16 hexadecimal characters.

*Table 34: Key of length 16 hex characters, optimistic policy*

| Character class ID | Class description | Pool characters | Pool size |
|---|---|---|---|
| H | Hexadecimal characters | 0-9, a-f | 16 |

The number of possible keys of this scheme is therefore:

$$N_{pkho} = 16^{16} = 2^{64} \approx 1.84 \times 10^{19}$$

Where:
- $N_{pkho}$: Number of possible keys, hexadecimal characters, optimistic policy

We see that the number of possible keys enforced by the optimistic key policy is much lower than the theoretically possible different keys ($2^{128} \approx 3.40 \times 10^{38}$). That is, the example policy enforces only a small fraction of about $10^{-11}$ of the possible keys even in the optimistic view.

#### Example (skeptic policy)

The key policy for the entry of a 128-bit key requires a hexadecimal string of fixed length with 32 characters. This is a common situation.

*Table 35: Key of length 16 hex characters, skeptic policy*

| Character class ID | Class description | Pool characters | Pool size |
|---|---|---|---|
| H | Hexadecimal characters | 0-9, a-f | 16 |

The number of possible keys of this scheme is therefore:

$N_{pkhs} = 16^{32} = 2^{128} \approx 3.40 \times 10^{38}$

Where:
- $N_{pkhs}$: Number of possible keys, hexadecimal characters, skeptic policy

We see that the number of possible keys enforced by the skeptic key policy matches the number of theoretically possible different keys. That is, the example key entry policy theoretically enforces a strong key.

**Note:**
For the entry of a 256-bit key, the policy should require 64 hexadecimal characters. This helps ensure that the number of possible keys for a 256-bit key matches the number of theoretically possible different keys ($2^{256} \approx 1.16 \times 10^{77}$).

### C.1.3 Conclusion

As the above examples show, a policy for manual key entry that enforces strong key values shall require a fixed number of hexadecimal characters. The result is a key with a high theoretical strength.

However, the real key strength resulting from a strong policy can still be lower:
- Only truly random key values have the highest possible expected information content.
- Therefore, reasonably strong keys typically shall be generated by an application.
- User-chosen keys typically have significantly less "randomness" (that is, entropy) than application-generated keys and therefore tend to be considerably weaker than application-generated keys, despite matching a strong scheme.

There are two aspects that can impair a key's strength even if it was generated according to a strong scheme:
- Residual weaknesses of user-generated keys
- Residual weaknesses of application-generated keys

### Residual weaknesses of user-generated keys

Users, even if following a strong key scheme, might chose hexadecimal keys that include sequences like "1111" or "1234". Even if such a sequence makes up only a part of the key, it impairs the key strength. Reason: Such sequences have a high probability of occurring, which means that their entropy ("randomness") is low. Therefore, such keys are considered weak because these sequences most likely are in an attacker's dictionary. This makes such keys more vulnerable to a dictionary attack, which requires less effort than a brute-force attack.

Even under optimistic assumptions, the probability for a user-generated password to contain an above given example sequence is $16^{-4} \approx 1.52 \times 10^{-5}$ per sequence. In reality, the probability is much higher (rough guess: $10^{-3}$) because users tend to follow patterns instead of choosing real random sequences. Furthermore, a user-generated key may contain multiple weak sequences which weakens the key further.

Because there are many known weak key sequences, the probability of a user-generated key containing a known weak sequences is rather high – probably too high to be accepted. Therefore, **consider checking a user-chosen key value against a list of known weak sequences.**

### Residual weaknesses of application-generated keys

An application-generated key typically is stronger than a user-generated key. Nevertheless, a simple generator for hexadecimal keys might in fact also sometimes suggest keys that include sequences like "1111" or "1234". Such keys may be considered weak because the sequences may be in an attacker's dictionary.

The probability for an application-generated password to contain an above given example sequence is $16^{-4} \approx 1.52 \times 10^{-5}$ per sequence. In contrast to user-generated keys, this is a real (skeptic) probability. It is also less likely than for user-generated keys that an application-generated key contains multiple weak sequences.

Because there are many known weak key sequences, the probability of an application-generated key containing one of the known weak sequences may be unacceptable. In this case, **consider checking a system-suggested key value against a list of known weak sequences.**

### C.1.4 Example of random key value generation (tool use)

If you have access to a Linux command shell (for example, bash) and have the hexadecimal dump utility `xxd` installed, you can generate a key of reasonable entropy as a hexadecimal string with the following command line:

- For a 256-bit key value (32 bytes):
  $ `xxd -l 32 -c 32 -p /dev/random`
  Example output:
  `26744caec971fc17300df577c8f7e7fda1297aa51881af5be7e58d0de3f55a68`

- For a 128-bit key value (16 bytes):
  $ `xxd -l 16 -c 16 -p /dev/random`
  Example output:
  `d773b4352a6de7c043477b4b55d106ff`

**Note:**
The random number device `/dev/random` delivers a virtually unlimited sequence of random bytes, with reasonable entropy, in binary format (the byte values are `0x00` .. `0xff`).
You can use other tools than `xxd` to read the desired number of bytes from the random number device and to convert the bytes to the required format.

# D Index

**A**

Abstract of this document . . . 13
Access through IEC 61850-MMS (setup) . . . 80
Access through Modbus TCP (setup) . . . 80
Access to the system monitor through the serial port (setup) . . . 88
Acess Control Lists, setup details (network) . . . 110
ACL administration (network) . . . 113
ACL introduction (network) . . . 110
ACL planning (network) . . . 112
ACL setup (network) . . . 112
ACL setup details (network) . . . 110
ACL test (network) . . . 112
ACLs and their associations (network) . . . 111
Advanced user authentication (setup) . . . 89
Advanced user authentication measures (planning) . . . 48
Aggressive assumptions about attackers . . . 126
Alternatives to mitigation (planning) . . . 31
Approximations in this document (Planning) . . . 20
Assess mitigation measure efficiency (planning) . . . 30
Assess the individual threat risks (Planning) . . . 26
Assign IP address parameters to the device management (setup) . . . 74
Assumptions (aggressive) about attackers . . . 126
Assumptions (conservative) about the attack context . . . 127
Assumptions (conservative) about users . . . 126
Attack protection support functions (network) . . . 109
Attack rate mitigation . . . 134
Attack rate mitigation examples . . . 135
Attack resistance time (quantitative) . . . 133
Attack resistance time examples (mitigated attack rate) . . . 135
Attack resistance time examples (unmitigated attack rate) . . . 134
Attack strategies on passwords . . . 125
Audience of this document . . . 13
Audit trail (created by persistent logging) . . . 114
Authentication server considerations (planning) . . . 51

**B**

Backup of device-specific data (setup) . . . 90
Backup policy for device-related data (planning) . . . 53
Basic security - confidentiality example (Planning) . . . 19
Basic security assumptions for passwords . . . 126
Basics (Planning) . . . 15
Binary or continuous security viewpoints (planning) . . . 34

**C**

Calculating the required password entropy . . . . . 138
Capability security levels (introduction) . . . . . 22
Certificates and revocation lists (setup) . . . . . 86
Checking the security seal (Maintenance) . . . . . 95
Checking the security seal (Planning) . . . . . 41
Checking the security seal (setup) . . . . . 93
Choosing a secure installation location (setup) . . . . . 65
CLI service shell, disable access (setup) . . . . . 89
Combining threat risk and mitigation efficiency - criticality (planning) . . . . . 33, 34
Compilininge a threat profile (Planning) . . . . . 25
Configuration load priority (Planning) . . . . . 40
Configuration load priority (Setup) . . . . . 78
Conservative assumptions about the attack context . . . . . 127
Conservative assumptions about users . . . . . 126
Consider data link redundancy requirements (setup) . . . . . 68
Consider device availability requirements (setup) . . . . . 65
Consider power budget requirements (setup) . . . . . 67
Consider power supply redundancy requirements (setup) . . . . . 66
Considerations for manually generated keys . . . . . 145
Create backup of device-specific data (setup) . . . . . 90
Creating ACLs and associations (network) . . . . . 111
Criticality - Combining threat risk and mitigation efficiency (planning) . . . . . 33, 34
Criticality assessment and mitigation (Planning) . . . . . 33

**D**

Data connections (installation) . . . 93
Data link redundancy requirements (considerations for setup) . . . 68
Decommissioning
Deletion of confidential data and secrets . . . 99
Delivery state, reset to . . . 99
Reset to the delivery state . . . 99
Secure physical destruction of device and possible accessories . . . 100
Decommissioning policy, device hardware (planning) . . . 54
Dedicated HTTPS certificate (setup) . . . 80
Dedicated login banners (setup) . . . 88
Dedicated SNMPv3 authentication and encryption password policy (setup) . . . 85
Dedicated SSH host key pair (setup) . . . 81
Dedicated user account login policy (setup) . . . 83
Dedicated user account password policy (setup) . . . 83
Dedicated user accounts and roles for device management (setup) . . . 84
Defense in depth (network) . . . 102
Defense in depth (system planning) . . . 27
Defense in depth (system planning), responsibilities . . . 28
Defense in depth example (planning) . . . 28
Defense in depth vs. hardening (planning) . . . 27
Defense in depth, detailed example (planning) . . . 29
Deletion of confidential data and secrets (decommissioning) . . . 99
Delivery state (Reset to, decommissioning) . . . 99
Detailed example of defense in depth (planning) . . . 29
Develop the device configuration (setup) . . . 59
Developing a mitigation strategy (planning) . . . 30
Developing a secure boot policy (Planning) . . . 42
Device and port LED visibility (planning) . . . 41
Device and port LEDs (restrict physical (visual) access, Security setup) . . . 92
Device availability (planning) . . . 40
Device decommissioning (overview) . . . 99
Device hardware decommissioning policy (planning) . . . 54
Device hardware interfaces (restrictions to, Security setup) . . . 91
Device hardware repair (maintenance) . . . 97
Device hardware repair policy (planning) . . . 53
Device hardware replacement (maintenance) . . . 96
Device hardware setup (installation) . . . 93
Device hardware, replacement policy (planning) . . . 53
Device installation . . . 93
Device security in the lifecycle phases (main chapter) . . . 59
Device-related data, backup policy (planning) . . . 53
Device-related policies (planning) . . . 53
DHCP server considerations (planning) . . . 50
Disable access (logical) for empty or unused modules (setup) . . . 76
Disable access (logical) to Signal Contact (setup) . . . 76
Disable access (logical) to unused ports and SFP slots (setup) . . . 76
Disable access to the CLI service shell (setup) . . . 89
Disable automatic device software update from external memory (setup) . . . 77
Disable copying a file into the device without valid cryptographic signature (setup) . . . 78
Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) (network) . . . 106
Disable GVRP and MVRP (MRP-IEEE Multiple VLAN Registration Protocol) (network) . . . 104
Disable insecure management protocols (setup) . . . 79
Disable loading configuration profile without valid fingerprint (setup) . . . 79
Disable logical access for empty or unused modules (setup) . . . 76
Disable logical access to Signal Contact (setup) . . . 76
Disable logical access to unused ports and SFP slots (setup) . . . 76
Disable MMRP (MRP-IEEE Multiple MAC Registration Protocol) and GMRP (network) . . . 106
Disable MVRP (MRP-IEEE Multiple VLAN Registration Protocol) and GVRP (network) . . . 104

Disable SNMPv1 traps (setup) . . . 87
Disable writing unencrypted configuration profile to external memory (setup) . . . 79
Document the planned policies . . . 57

**E**
Empty media module slots (restrict physical access) . . . 92
Enable SNMPv3 traps (setup) . . . 88
Entropy (password) . . . 137
Example (Planning) . . . 16
Example of defense in depth (planning) . . . 28
External authentication server considerations (planning) . . . 51
External DHCP server considerations (planning) . . . 50
External log server considerations (planning) . . . 51
External server considerations (planning) . . . 49

**G**
General vs. security-related device functions (setup) . . . 61

**H**
Harden your network (network) . . . 102
Hardening vs. defense in depth (planning) . . . 27
Hardware and setup scenarios, relationship . . . 24
Hardware changes (maintenance) . . . 95
Hardware vs. software measures (setup) . . . 60
Help secure the network protocols used (network) . . . 106
Help secure the redundancy protocols used (network) . . . 107
Helping secure the network infrastructure (network) . . . 103
HiDiscovery . . . 73
HiDiscovery (Setup) . . . 74
High-complexity passwords . . . 128
HiView . . . 69
HTTPS certificate (setup) . . . 80

**I**
Impact of device requirements on system planning . . . 39
Impact of external servers on system planning . . . 49
Impact of network aspects on system planning . . . 49
Impact of system lifecycle on the device lifecycle (planning) . . . 38
Impartial assessment (Planning) . . . 18
Industrial HiVision . . . 11
Installation
  Data connections . . . 93
  Device . . . 93
  Device hardware setup . . . 93
  Signal Contact considerations . . . 93
Intended audience of this document . . . 13
Introduction
  Capability security levels (SL-C) . . . 22
Introduction (network) . . . 101
Introduction (required preparatory work) . . . 22
Introduction to defense in depth (planning) . . . 27
IP access restrictions (setup) . . . 80
IP address parameters for the device management (setup) . . . 74

**K**
Key rotation . . . 50
Key strength (quantitative) . . . 145
Key strength example (optimistic) . . . 146, 147
Key strength example (skeptic) . . . 147, 148

**L**

LED visibility (device and port LEDs, planning) . . . 41
LEDs (restrict physical (visual) access, Security setup) . . . 92
Lifecycle phases for device security (main chapter) . . . 59
LLDP parameter planning (network) . . . 48
LLDP parameter setup (network) . . . 115
Log server considerations (planning) . . . 51
Logging (setup) . . . 87
Logging parameters (network) . . . 114
Logging policy (planning) . . . 47
Logical vs. physical measures (setup) . . . 60
Login banners (setup) . . . 88
Lookup tables for password policies (quantitative) . . . 140
Low-complexity passwords . . . 130

**M**

Maintenance
  Checking the security seal . . . 95
  Device hardware replacement . . . 96
  Hardware changes . . . 95
  Hardware repair . . . 97
  Software update . . . 95
Maintenance and operation policy (planning) . . . 56
Maintenance overview (setup) . . . 95
Management IP access restrictions (setup) . . . 80
Management VLAN (setup) . . . 76
Manually generated keys, considerations . . . 145
Measures to help secure the network infrastructure (network) . . . 103
Media module slots (empty, restrict physical access) . . . 92
Mitigation (attack rate) . . . 134
Mitigation efficiency value and unit (planning) . . . 31
Mitigation examples (attack rate) . . . 135
Mitigation strategy development (planning) . . . 30
Mitigation, alternatives (planning) . . . 31

**N**

Network
Acess Control Lists details (setup) . . . 110
ACL administration . . . 113
ACL introduction . . . 110
ACL planning . . . 112
ACL setup . . . 112
ACL setup details . . . 110
ACL test . . . 112
ACLs and their associations . . . 111
Attack protection support functions . . . 109
Audit trail (created by persistent logging) . . . 114
Creating ACLs and associations . . . 111
Defense in depth . . . 102
Disable GMRP and MMRP (MRP-IEEE Multiple MAC Registration Protocol) . . . 106
Disable GVRP and MVRP (MRP-IEEE Multiple VLAN Registration Protocol) . . . 104
Disable MMRP (MRP-IEEE Multiple MAC Registration Protocol) and GMRP . . . 106
Disable MVRP (MRP-IEEE Multiple VLAN Registration Protocol) and GVRP . . . 104
Harden your network . . . 102
Help secure the network protocols used . . . 106
Help secure the redundancy protocols used . . . 107
Helping secure the infrastructure . . . 103
Introduction . . . 101
LLDP parameter planning . . . 48
LLDP parameter setup . . . 115
Logging parameters . . . 114
Measures to help secure the infrastructure . . . 103
Planning the LLDP parameters . . . 48
Port Security . . . 104
Potential conflicts of aims for an ACL . . . 111
Prerequisites . . . 101
Rate limiter . . . 109
Restrict logical access . . . 104
RSTP guards and helper protocols, set up . . . 107
Security support (by the device) . . . 101
Set up RSTP guards and helper protocols . . . 107
Set up the Denial of Service (DoS) parameters . . . 109
Set up the LLDP parameters . . . 115
Set up the logging parameters . . . 114
Set up the Media Redundancy Protocol (MRP) parameters . . . 108
Set up the MRP (Media Redundancy Protocol) parameters . . . 108
VLAN segregation . . . 104
Network ports or SFP slots (restrict physical access) . . . 92
Network security support (by the device) . . . 101

**O**

Operation and maintenance policy (planning) . . . 56
Operation overview (setup) . . . 94
Overview (Planning) . . . 21
Overview (setup) . . . 72

**P**

Password and cryptographic key basics (planning) . . . 36
Password attack strategies . . . 125
Password classes . . . 121
Password entropy . . . 137
Password policies . . . 123
Password policy guide . . . 121
Password policy lookup tables (quantitative) . . . 140
Password schemes . . . 124
Password security assumptions . . . 126
Password strength . . . 121
Password strength (quantitative) . . . 128
Password strength example (high-complexity, optimistic) . . . 129
Password strength example (high-complexity, skeptic) . . . 130
Password strength example (low-complexity) . . . 132
Passwords (high-complexity) . . . 128
Passwords (low-complexity) . . . 130
Physical
  Restrict access to empty media module slots (setup) . . . 92
  Restrict access to network ports or SFP slots (setup) . . . 92
  Restrict access to the device and port LEDs (setup) . . . 92
  Restrict access to the Signal Contact (setup) . . . 92
Physical vs. logical measures (setup) . . . 60
Planning
  Advanced user authentication measures . . . 48
  Alternatives to mitigation . . . 31
  Assess mitigation measure efficiency . . . 30
  Assess the individual threat risks . . . 26
  Authentication server considerations . . . 51
  Backup policy for device-related data . . . 53
  Basic mitigation - confidentiality example . . . 19
  Basics . . . 15
  Binary or continuous security viewpoints . . . 34
  Checking the security seal . . . 41
  Combining threat risk and mitigation efficiency - criticality . . . 33, 34
  Compiling a threat profile . . . 25
  Configuration load priority . . . 40
  Criticality - Combining threat risk and mitigation efficiency . . . 33, 34
  Criticality assessment and mitigation . . . 33
  Decommissioning policy, device hardware . . . 54
  Defense in depth . . . 27
  Defense in depth example . . . 28
  Defense in depth vs. hardening . . . 27
  Defense in depth, detailed example . . . 29
  Defense in depth, introduction . . . 27
  Defense in depth, purpose . . . 27
  Defense in depth, responsibilities . . . 28
  Detailed example of defense in depth . . . 29
  Developing a mitigation strategy . . . 30
  Developing a secure boot policy . . . 42
  Device and port LED visibility . . . 41
  Device availability . . . 40
  Device hardware decommissioning policy . . . 54
  Device hardware repair policy . . . 53
  Device hardware, replacement policy . . . 53
  Device-related data, backup policy . . . 53
  Device-related policies . . . 53
  DHCP server considerations . . . 50
  Document the planned policies . . . 57

Example . . . 16
Example of defense in depth . . . 28
External authentication server considerations . . . 51
External DHCP server considerations . . . 50
External log server considerations . . . 51
External server considerations . . . 49
Hardening vs. defense in depth . . . 27
Impact of device requirements on system . . . 39
Impact of external servers on the system . . . 49
Impact of network aspects on the system . . . 49
Impact of system lifecycle on device lifecycle . . . 38
Impartial assessment . . . 18
LED visibility (device and port LEDs) . . . 41
Log server considerations . . . 51
Logging policy . . . 47
Maintenance and operation policy . . . 56
Mitigation efficiency value and unit . . . 31
Mitigation strategy development . . . 30
Mitigation, alternatives . . . 31
Operation and Maintenance policy . . . 56
Overview . . . 21
Password and cryptographic key basics . . . 36
Port and device LED visibility . . . 41
Purpose of . . . 27
RADIUS server . . . 51
Repair policy, device hardware . . . 53
Replacement policy for device hardware . . . 53
Residual risk . . . 34
Responsibilities for defense in depth . . . 28
Restrictions to the device hardware interfaces . . . 42
Risk value and unit . . . 25
Scenario development . . . 24
Secure installation location . . . 39
Security terminology . . . 15
Security terminology, more . . . 16
Security viewpoints (binary or continuous) . . . 34
Session timeouts . . . 47
Signal contact use . . . 41
Skepticism vs. optimism . . . 18
SNMPv3 authentication and encryption password . . . 46
Software auto update . . . 40
Software update and configuration server considerations . . . 49
SSH key auto upload . . . 40
Strategies to improve security . . . 20
Tension of convenience vs. security . . . 17
Theoretical and practical degrees of security . . . 20
Threat analysis . . . 19
Unsigned device software, upload . . . 43
Upload of unsigned device software . . . 43
User account and role policy for device management . . . 45
User account login policy . . . 43
User account password policy . . . 44
VLAN . . . 38
Planning for security . . . 15
Planning the LLDP parameters (network) . . . 48
PoE (setup) (depends on hardware) . . . 77
Port and device LED visibility (planning) . . . 41
Port and device LEDs (restrict physical (visual) access, Security setup) . . . 92
Port Security (network) . . . 104

Possible further prerequisites (setup overview) . . . 62
Potential conflicts of aims for an ACL (network) . . . 111
Power over Ethernet (setup) (depends on hardware) . . . 77
Preparation for installation, suggested (Setup) . . . 63
Preparatory work (introduction) . . . 22
Prerequisites (network) . . . 101
Prerequisites for installation and setup (setup overview) . . . 62
Purpose of defense in depth (planning) . . . 27

**Q**

Quantitative key strength . . . 145
Quantitative password strength . . . 128

**R**

RADIUS client (Setup) . . . 89
RADIUS server (Planning) . . . 51
Rate limiter (network) . . . 109
Reasons for suggested installation step sequence (setup) . . . 63
Recommended work step sequence (Setup overview) . . . 63
Relationship of hardware and setup scenarios . . . 24
Repair policy, device hardware (planning) . . . 53
Replacement policy for device hardware (planning) . . . 53
Required attack resistance time (quantitative) . . . 136
Required password entropy (calculation) . . . 138
Required preparatory work (introduction) . . . 22
Reset to the delivery state (decommissioning) . . . 99
Residual risk (planning) . . . 34
Responsibilities for defense in depth (system planning) . . . 28
Restrict access to empty media module slots (physical, Security setup) . . . 92
Restrict access to network ports or SFP slots (physical, Security setup) . . . 92
Restrict access to the device and port LEDs (physical, Security setup) . . . 92
Restrict access to the Signal Contact (physical, Security setup) . . . 92
Restrict access to USB port (physical, security setup) . . . 91
Restrict logical access (network) . . . 104
Restrictions to device hardware interfaces (setup) . . . 91
Restrictions to the device hardware interfaces (planning) . . . 42
Risk value and unit (planning) . . . 25
RSTP guards and helper protocols (network, set up) . . . 107

**S**

Scenario development (planning) . . . 24
Scenarios (Relationship of hardware and setup scenarios) . . . 24
Scope of this document . . . 21
Secure installation location (planning) . . . 39
Secure physical destruction of device and possible accessories (decommissioning) . . . 100
Security assumptions for passwords . . . 126
Security levels (SL-C, introduction) . . . 22
Security planning . . . 15
Security seal . . . 117
Security seal details . . . 117, 118
Security seal overview . . . 117
Security setup overview . . . 72
Security terminology (Planning) . . . 15
Security terminology, more (Planning) . . . 16
Security viewpoints (binary or continuous, planning) . . . 34
Security-related vs. general device functions (setup) . . . 61
Server key rotation . . . 50
Session timeouts (planning) . . . 47
Set up RSTP guards and helper protocols (network) . . . 107
Set up the Denial of Service (DoS) parameters (network) . . . 109
Set up the LLDP parameters (network) . . . 115
Set up the logging parameters (network) . . . 114
Set up the MRP (Media Redundancy Protocol) parameters (network) . . . 108
Set up the SSH Known Hosts fingerprints (setup) . . . 82
Set up the the Media Redundancy Protocol (MRP) parameters (network) . . . 108
Setting of secure boot mode (setup) . . . 75
Setup
- Access through IEC 61850-MMS . . . 80
- Access through Modbus TCP . . . 80
- Access to the system monitor through the serial port . . . 88
- Advanced user authentication . . . 89
- Assign IP address parameters for the device management . . . 74
- Backup of device-specific data . . . 90
- Certificates and revocation lists . . . 86
- Checking the security seal . . . 93
- Choosing a secure installation location . . . 65
- CLI service shell, disable access . . . 89
- Configuration load priority . . . 78
- Consider data link redundancy requirements . . . 68
- Consider device availability requirements . . . 65
- Consider power budget requirements . . . 67
- Consider power supply redundancy requirements . . . 66
- Create backup of device-specific data . . . 90
- Data link redundancy requirements . . . 68
- Dedicated HTTPS certificate . . . 80
- Dedicated login banners . . . 88
- Dedicated SNMPv3 authentication and encryption password policy . . . 85
- Dedicated SSH host key pair . . . 81
- Dedicated user account login policy . . . 83
- Dedicated user account password policy . . . 83
- Dedicated user accounts and roles for device management . . . 84
- Develop the device configuration . . . 59
- Device hardware . . . 93
- Device hardware interfaces (restrictions to) . . . 91
- Disable access (logical) for empty or unused modules . . . 76
- Disable access (logical) to Signal Contact . . . 76
- Disable access (logical) to unused ports and SFP slots . . . 76
- Disable access to the CLI service shell . . . 89

Disable automatic device software update from external memory . . . 77
Disable copying a file into the device without valid cryptographic signature . . . 78
Disable insecure management protocols . . . 79
Disable loading configuration profile without valid fingerprint . . . 79
Disable logical access for empty or unused modules . . . 76
Disable logical access to Signal Contact . . . 76
Disable logical access to unused ports and SFP slots . . . 76
Disable SNMPv1 traps . . . 87
Disable writing unencrypted configuration profile to external memory . . . 79
Enable SNMPv3 traps . . . 88
General vs. security-related device functions . . . 61
Hardware vs. software measures . . . 60
HiDiscovery . . . 74
HTTPS certificate . . . 80
IP access restrictions . . . 80
IP address parameters for the device management . . . 74
Logging . . . 87
Logical vs. physical measures . . . 60
Login banners . . . 88
Maintenance overview . . . 95
Management IP access restrictions . . . 80
Management VLAN . . . 76
Operation overview . . . 94
Physical vs. logical measures . . . 60
PoE (depends on hardware) . . . 77
Power over Ethernet (depends on hardware) . . . 77
Preparation for installation, suggested . . . 63
Prerequisites for installation and setup . . . 62
RADIUS client . . . 89
Reasons for suggested installation step sequence . . . 63
Restrict physical access to USB port . . . 91
Restrictions to device hardware interfaces . . . 91
Security-related vs. general device functions . . . 61
Set up the SSH Known Hosts fingerprints . . . 82
Setting of secure boot mode . . . 75
SNMPv1 traps . . . 87
SNMPv3 authentication and encryption password policy . . . 85
SNMPv3 traps . . . 88
Software update . . . 69
Software vs. hardware measures . . . 60
Specify finite session timeouts . . . 86
SSH host key pair . . . 81
SSH key auto upload . . . 78
Suggested installation step sequence (reasons for) . . . 63
Suggested preparation for installation . . . 63
System monitor, Access through the serial port . . . 88
USB port (restrict physical access) . . . 91
User account login policy . . . 83
User account password policy . . . 83
User accounts and roles for device management . . . 84
VLAN dedicated to management access . . . 76
Setup overview . . . 72
Setup overview (Possible further prerequisites) . . . 62
SFP slots or network ports (restrict physical access) . . . 92
Signal Contact (restrict physical access, Security setup) . . . 92
Signal Contact considerations (installation) . . . 93
Signal contact use (planning) . . . 41
Skepticism (Basic approximations) . . . 20
Skepticism (Planning) . . . 20

Skepticism vs. optimism (Planning) . . . 18
SL-C (introduction) . . . 22
SNMPv1 traps (setup) . . . 87
SNMPv3 authentication and encryption password (planning) . . . 46
SNMPv3 authentication and encryption password policy (setup) . . . 85
SNMPv3 traps (setup) . . . 88
Software auto update (Planning) . . . 40
Software update (maintenance) . . . 95
Software update (setup) . . . 69
Software update and configuration server considerations (Planning) . . . 49
Software vs. hardware measures (setup) . . . 60
Specify finite session timeouts (setup) . . . 86
SSH host key pair (setup) . . . 81
SSH key auto upload (Planning) . . . 40
SSH key auto upload (Setup) . . . 78
SSH server key rotation . . . 50
Strategies to improve security (Planning) . . . 20
Subject of this document . . . 21
Suggested installation step sequence (reasons for, setup) . . . 63
Suggested preparation for installation (Setup) . . . 63
Summary of this document . . . 13
Synopsis of this document . . . 13
System monitor, Access through the serial port (setup) . . . 88

**T**

Technical Documents . . . 163
Technical questions . . . 163
Technical Support . . . 163
Tension of convenience vs. security (Planning) . . . 17
Theoretical and practical degrees of security (Planning) . . . 20
Threat analysis (Planning) . . . 19
Training courses . . . 163

**U**

Unsigned device software, upload (Planning) . . . 43
Upload of unsigned device software (Planning) . . . 43
USB port (restrict physical access, security setup) . . . 91
User account and role policy for device management (planning) . . . 45
User account login policy (planning) . . . 43
User account login policy (setup) . . . 83
User account password policy (planning) . . . 44
User account password policy (setup) . . . 83
User accounts and roles for device management (setup) . . . 84

**V**

VLAN (planning) . . . 38
VLAN dedicated to management access (setup) . . . 76
VLAN segregation (network) . . . 104

**W**

Work step sequence (recommended, Setup overview) . . . 63

# E Technical support

### Technical questions

For technical questions, please contact any Hirschmann dealer in your area or Hirschmann directly. You find the addresses of our partners on the Internet at www.belden.com.

For technical support, visit my.belden.com. This site also includes a free of charge knowledge base and a software download section.

### Technical Documents

The current manuals and operating instructions for Hirschmann products are available at doc.hirschmann.com.

### Customer Innovation Center

The Customer Innovation Center is ahead of its competitors on three counts with its complete range of innovative services:

- Consulting incorporates comprehensive technical advice, from system evaluation through network planning to project planning.
- Training offers you an introduction to the basics, product briefing and user training with certification. You find the training courses on technology and products currently available at www.belden.com/services/customer-innovation-center.
- Support ranges from the first installation through the standby service to maintenance concepts.

With the Customer Innovation Center, you decide against any compromise in any case. Our client-customized package leaves you free to choose the service components you want to use.

# F Readers' Comments

What is your opinion of this manual? We are constantly striving to provide as comprehensive a description of our product as possible, as well as important information to assist you in the operation of this product. Your comments and suggestions help us to further improve the quality of our documentation.

Your assessment of this manual:

| | Very Good | Good | Satisfactory | Mediocre | Poor |
|---|---|---|---|---|---|
| Precise description | O | O | O | O | O |
| Readability | O | O | O | O | O |
| Understandability | O | O | O | O | O |
| Examples | O | O | O | O | O |
| Structure | O | O | O | O | O |
| Comprehensive | O | O | O | O | O |
| Graphics | O | O | O | O | O |
| Drawings | O | O | O | O | O |
| Tables | O | O | O | O | O |

Did you discover any errors in this manual?
If so, on what page?

Suggestions for improvement and additional information:

General comments:

Sender:

Company / Department:

Name / Telephone number:

Street:

Zip code / City:

E-mail:

Date / Signature:

Dear User,

Please fill out and return this page
- as a fax to the number +49 (0)7127/14-1600 or
- per mail to
  Hirschmann Automation and Control GmbH
  Department IRD-NT
  Stuttgarter Str. 45-51
  72654 Neckartenzlingen
  Germany

HIRSCHMANN

A BELDEN BRAND