Modicon

MCSESM, MCSESM-E, MCSESP Switch mit Management
Benutzer-Handbuch Konfiguration

QGH59058.02

www.schneider-electric.com

Schneider Electric

Die Informationen in der vorliegenden Dokumentation enthalten allgemeine Beschreibungen und/oder technische Leistungsmerkmale der hier erwähnten Produkte. Diese Dokumentation dient keinesfalls als Ersatz für die Ermittlung der Eignung oder Verlässlichkeit dieser Produkte für bestimmte Verwendungsbereiche des Benutzers und darf nicht zu diesem Zweck verwendet werden. Jeder Benutzer oder Integrator ist verpflichtet, angemessene und vollständige Risikoanalysen, Bewertungen und Tests der Produkte im Hinblick auf deren jeweils spezifischen Verwendungszweck vorzunehmen. Weder Schneider Electric noch deren Tochtergesellschaften oder verbundene Unternehmen sind für einen Missbrauch der Informationen in der vorliegenden Dokumentation verantwortlich oder können diesbezüglich haftbar gemacht werden. Verbesserungs- und Änderungsvorschläge sowie Hinweise auf angetroffene Fehler werden jederzeit gern entgegengenommen.

Sie erklären, dass Sie ohne schriftliche Genehmigung von Schneider Electric dieses Dokument weder ganz noch teilweise auf beliebigen Medien reproduzieren werden, ausgenommen zur Verwendung für persönliche nichtkommerzielle Zwecke. Darüber hinaus erklären Sie, dass Sie keine Hypertext-Links zu diesem Dokument oder seinem Inhalt einrichten werden. Schneider Electric gewährt keine Berechtigung oder Lizenz für die persönliche und nichtkommerzielle Verwendung dieses Dokument oder seines Inhalts, ausgenommen die nichtexklusive Lizenz zur Nutzung als Referenz. Das Handbuch wird hierfür "wie besehen" bereitgestellt, die Nutzung erfolgt auf eigene Gefahr. Alle weiteren Rechte sind vorbehalten.

Bei der Montage und Verwendung dieses Produkts sind alle zutreffenden staatlichen, landesspezifischen, regionalen und lokalen Sicherheitsbestimmungen zu beachten. Aus Sicherheitsgründen und um die Übereinstimmung mit dokumentierten Systemdaten besser zu gewährleisten, sollten Reparaturen an Komponenten nur vom Hersteller vorgenommen werden.

Beim Einsatz von Geräten für Anwendungen mit technischen Sicherheitsanforderungen sind die relevanten Anweisungen zu beachten.

Die Verwendung anderer Software als der Schneider Electric-eigenen bzw. einer von Schneider Electric genehmigten Software in Verbindung mit den Hardwareprodukten von Schneider Electric kann Körperverletzung, Schäden oder einen fehlerhaften Betrieb zur Folge haben.

Die Nichtbeachtung dieser Informationen kann Verletzungen oder Materialschäden zur Folge haben!

Als verantwortungsbewusstes Inklusionsunternehmen aktualisieren wir unsere Inhalte, die nicht-inklusive Terminologie enthalten. Bis dieser Vorgang abgeschlossen ist, können unsere Inhalte allerdings nach wie vor standardisierte Branchenbegriffe enthalten, die von unseren Kunden als unangemessen betrachtet werden.

Inhalt

Sicherheitshinweise

Beachten Sie: Lesen Sie diese Anweisungen gründlich durch und machen Sie sich mit dem Gerät vertraut, bevor Sie es installieren, in Betrieb nehmen oder warten. Die folgenden speziellen Hinweise werden in diesem Dokument oder auf den Geräten verwendet, um vor potenziellen Gefahren zu warnen oder um die Aufmerksamkeit auf erklärende Informationen zu lenken, welche die Nutzung der Geräte vereinfachen können.

Wird dieses Symbol zusätzlich zu einem Sicherheitshinweis des Typs "Gefahr" oder "Warnung" angezeigt, bedeutet das, dass die Gefahr eines elektrischen Schlags besteht und die Nichtbeachtung der Anweisungen unweigerlich Verletzung zur Folge hat.

Dies ist ein allgemeines Warnsymbol. Es macht Sie auf mögliche Verletzungsgefahren aufmerksam. Beachten Sie alle unter diesem Symbol aufgeführten Hinweise, um Verletzungen oder Unfälle mit Todesfolge zu vermeiden.

⚠ GEFAHR

GEFAHR macht auf eine unmittelbar gefährliche Situation aufmerksam, die bei Nichtbeachtung **unweigerlich** einen schweren oder tödlichen Unfall zur Folge hat.

⚠ WARNUNG

WARNUNG verweist auf eine mögliche Gefahr, die – wenn sie nicht vermieden wird – Tod oder schwere Verletzungen **zur Folge haben kann**.

⚠ VORSICHT

VORSICHT verweist auf eine mögliche Gefahr, die – wenn sie nicht vermieden wird – leichte Verletzungen **zur Folge haben kann**.

HINWEIS

HINWEIS gibt Auskunft über Vorgehensweisen, bei denen keine Verletzungen drohen.

Beachten Sie: Elektrische Geräte dürfen nur von Fachpersonal installiert, betrieben, gewartet und instand gesetzt werden. Schneider Electric haftet nicht für Schäden, die aufgrund der Verwendung dieses Materials entstehen.

Als qualifiziertes Fachpersonal gelten Mitarbeiter, die über Fähigkeiten und Kenntnisse hinsichtlich der Konstruktion und des Betriebs elektrischer Geräte und deren Installation verfügen und eine Schulung zur Erkennung und Vermeidung möglicher Gefahren absolviert haben.

Über dieses Handbuch

Gültigkeitsbereich

Die in diesem Buch enthaltenen Daten und Abbildungen sind nicht verbindlich. Wir behalten uns das Recht vor, unsere Erzeugnisse im Rahmen unserer Strategie der ständigen Produktentwicklung zu ändern. Die Informationen in dieser Unterlage können ohne Ankündigung geändert werden und dürfen nicht als für Schneider Electric verbindlich ausgelegt werden.

Benutzerkommentare

Ihre Anmerkungen und Hinweise sind uns jederzeit willkommen. Sie erreichen uns per E-Mail unter: techpub@schneider-electric.com

Weiterführende Dokumentation

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

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

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

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

Die Netzmanagement-Software ConneXium Network Manager bietet Ihnen weitere Möglichkeiten zur komfortablen Konfiguration und Überwachung:
- Autotopologie-Erkennung
- Browser-Interface
- Client/Server-Struktur
- Ereignisbehandlung
- Ereignisprotokoll
- Gleichzeitige Konfiguration mehrerer Geräte
- Grafische Benutzeroberfläche mit Netz-Layout
- SNMP/OPC-Gateway

Legende

Die in diesem Handbuch verwendeten Auszeichnungen haben folgende Bedeutungen:

▶	Aufzählung
☐	Arbeitsschritt
Verweis	Querverweis mit Verknüpfung
Anmerkung:	Eine Anmerkung betont eine wichtige Tatsache oder lenkt Ihre Aufmerksamkeit auf eine Abhängigkeit.
`Courier`	Darstellung eines CLI-Kommandos oder des Feldinhalts in der grafischen Benutzeroberfläche

Auszuführen in der grafische Benutzeroberfläche

Auszuführen im Command Line Interface

Ersetzen eines 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.
  Siehe „Konfigurationsprofil aus dem externen Speicher laden” auf Seite 106.
- Das neue Gerät erhält seine IP-Adresse mittels DHCP *Option 82*.
  Siehe „DHCP-L2-Relay” auf Seite 320.
  Siehe „DHCP-Server Option 82 einrichten” auf Seite 365.

Bei jeder Lösung erhält das neue Gerät beim Neustart die gleichen IP-Einstellungen, die das ersetzte Gerät zuvor hatte.

- Für Zugriffe auf das Management des Geräts über HTTPS verwendet das Gerät ein digitales Zertifikat. Sie haben die Möglichkeit, ein eigenes Zertifikat in das Gerät zu importieren.
  Siehe „HTTPS-Zertifikatsverwaltung” auf Seite 371.
- Für Zugriffe auf das Management des Geräts mittels SSH verwendet das Gerät einen RSA-Host-Key. Sie haben die Möglichkeit, einen eigenen Host-Key im PEM-Format in das Gerät zu importieren.
  Siehe „Eigenen Schlüssel in das Gerät laden” auf Seite 368.

1 Benutzeroberflächen

Das Gerät ermöglicht Ihnen, die Einstellungen des Geräts über folgende Benutzeroberflächen festzulegen.

Tab. 1: Benutzeroberflächen für Zugriff auf das Management des Geräts

Benutzeroberfläche	Erreichbar über …	Voraussetzung
Grafische Benutzeroberfläche	Ethernet (In-Band)	Web-Browser
Command Line Interface	Ethernet (In-Band) Serielle Schnittstelle (Out-of-Band)	Terminalemulations-Software
System-Monitor	Serielle Schnittstelle (Out-of-Band)	Terminalemulations-Software

1.1 Grafische Benutzeroberfläche

Systemanforderungen

Um die grafische Benutzeroberfläche zu öffnen, benötigen Sie die Desktop-Version eines Web-Browsers mit HTML5-Unterstützung.

Anmerkung: Software von Drittanbietern wie Web-Browser validieren Zertifikate anhand von Kriterien wie Verfallsdatum und aktuellen kryptografischen Parameter-Empfehlungen. Veraltete Zertifikate können aufgrund ungültiger oder veralteter Informationen Fehler verursachen. Beispiel: Ein abgelaufenes Zertifikat oder geänderte kryptografische Empfehlungen. Um Validierungskonflikte mit Software von Drittanbietern zu beheben, übertragen Sie Ihr eigenes, aktuelles Zertifikat auf das Gerät oder generieren Sie das Zertifikat mit der neuesten Firmware.

Grafische Benutzeroberfläche starten

Voraussetzung für das Starten der grafischen Benutzeroberfläche ist, dass die IP-Parameter im Gerät konfiguriert sind. Siehe „IP-Parameter festlegen” auf Seite 43.

Führen Sie die folgenden Schritte aus:
- ☐ Starten Sie Ihren Web-Browser.
- ☐ Fügen Sie die IP-Adresse des Geräts in das Adressfeld des Web-Browsers ein.
  Verwenden Sie die folgende Form: `https://xxx.xxx.xxx.xxx`
  Der Web-Browser stellt die Verbindung zum Gerät her und zeigt den Login-Dialog.
- ☐ Wenn Sie die Sprache der grafischen Benutzeroberfläche ändern möchten, klicken Sie im Login-Dialog auf den entsprechenden Link oben rechts.
- ☐ Fügen Sie den Benutzernamen ein.
- ☐ Fügen Sie das Passwort ein.
- ☐ Klicken Sie die Schaltfläche *Login*.
  Der Web-Browser zeigt die grafische Benutzeroberfläche.

1.2 Command Line Interface

Das Command Line Interface bietet Ihnen die Möglichkeit, die Funktionen des Gerätes über eine lokale oder eine Fernverbindung zu bedienen.

IT-Spezialisten finden im Command Line Interface die gewohnte Umgebung zum Konfigurieren von IT-Geräten. Als erfahrener Benutzer oder Administrator verfügen Sie über Wissen zu den Grundlagen und den Einsatz von Schneider Electric-Geräten.

1.2.1 Datenverbindung vorbereiten

Informationen zur Montage und Inbetriebnahme Ihres Geräts finden Sie im Anwender-Handbuch „Installation“.

- ☐ Verbinden Sie das Gerät mit dem Datennetz. Voraussetzung für die erfolgreiche Datenverbindung ist die korrekte Einstellung der Netzparameter.

Einen Zugang zur Benutzeroberfläche des Command Line Interfaces erhalten Sie zum Beispiel mit Hilfe des Freeware-Programms *PuTTY*.

- ☐ Installieren Sie auf Ihrem Rechner das Programm *PuTTY*.

1.2.2 Zugriff auf das Command Line Interface mit Telnet

Telnet-Verbindung über Windows

Telnet ist ausschließlich bei Windows-Versionen vor Windows Vista standardmäßig installiert.

Führen Sie die folgenden Schritte aus:

- ☐ Starten Sie auf Ihrem Rechner das Programm *Command Prompt*.
- ☐ Fügen Sie das Kommando `telnet <IP_address>` ein.

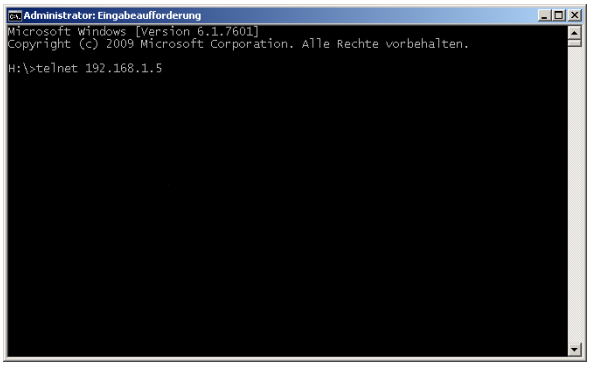


Abb. 1: Command Prompt: Telnet-Verbindung zum Gerät herstellen

Telnet-Verbindung über PuTTY

Führen Sie die folgenden Schritte aus:
- ☐ Starten Sie auf Ihrem Rechner das Programm *PuTTY*.

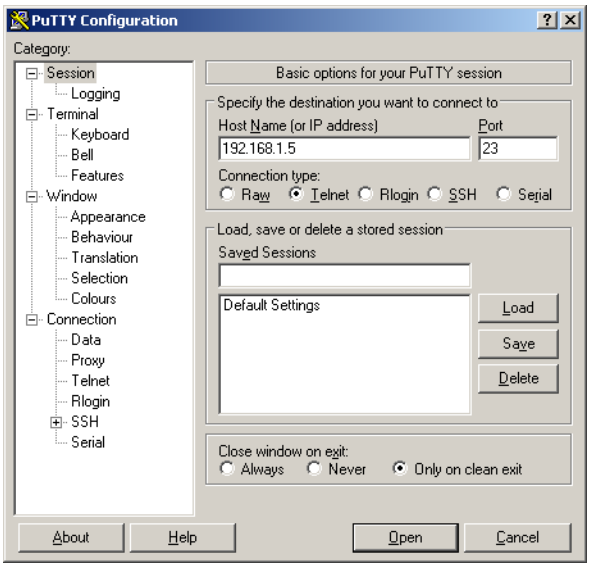


Abb. 2: PuTTY-Eingabemaske

- ☐ In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Geräts ein.
  Die IP-Adresse besteht aus 4 Dezimalzahlen im Wert von `0` bis `255`. Die 4 Dezimalzahlen sind durch einen Punkt getrennt.
- ☐ Um den Verbindungstyp auszuwählen, wählen Sie unter *Connection type* das Optionsfeld *Telnet*.
- ☐ Klicken Sie die Schaltfläche *Open*, um die Datenverbindung zu Ihrem Gerät aufzubauen.
  Das Command Line Interface meldet sich auf dem Bildschirm mit einem Fenster für die Eingabe des Benutzernamens. Das Gerät bietet bis zu 5 Benutzern gleichzeitig die Möglichkeit, auf das Command Line Interface zuzugreifen.

Anmerkung: Dieses Gerät ist ein sicherheitsrelevantes Produkt. Ändern Sie das Passwort gleich bei der ersten Inbetriebnahme.

Führen Sie die folgenden Schritte aus:
- ☐ Fügen Sie den Benutzernamen ein.
  Der voreingestellte Benutzername ist `admin`.
- ☐ Drücken Sie die <Enter>-Taste.

- ☐ Fügen Sie das Passwort ein.
  Das voreingestellte Passwort ist `private`.
- ☐ Drücken Sie die <Enter>-Taste.

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:24)


                    System Name   :  MCSESM-646038d5e846
                    Management IP :  192.168.1.5
                    Subnet Mask   :  255.255.255.0
                    Base MAC      :  64:60:38:01:02:03
                    USB IP        :  91.0.0.100
                    USB Mask      :  255.255.255.0
                    System Time   :  2022-07-13 19:35:56


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.

MCSESM-E>
```

Abb. 3: Start-Bildschirm des Command Line Interfaces

1.2.3 Zugriff auf das Command Line Interface mit SSH (Secure Shell)

Im folgenden Beispiel verwenden wir das Programm *PuTTY*. Eine weitere Möglichkeit, über SSH auf Ihr Gerät zuzugreifen, ist die OpenSSH Suite.

Führen Sie die folgenden Schritte aus:

- ☐ Starten Sie auf Ihrem Rechner das Programm *PuTTY*.

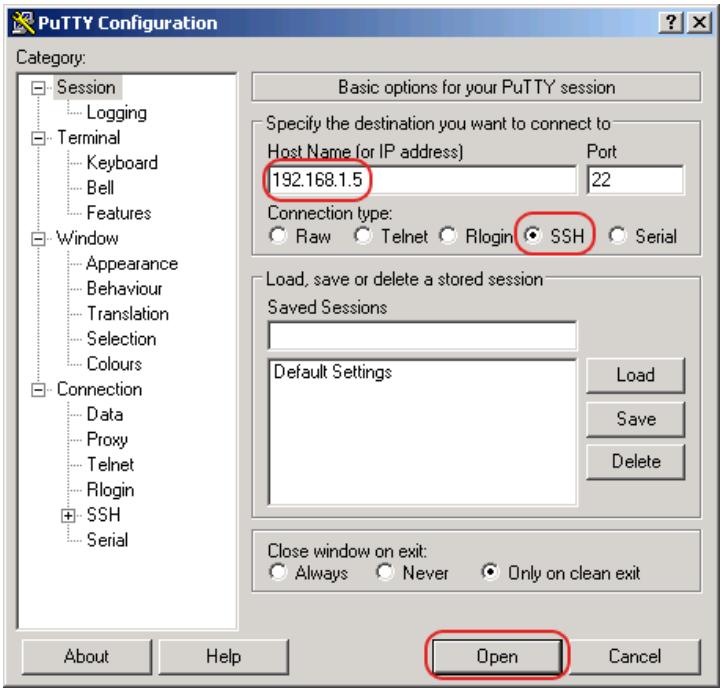


Abb. 4: PuTTY-Eingabemaske

- ☐ In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Geräts ein.
  Die IP-Adresse besteht aus 4 Dezimalzahlen im Wert von 0 bis 255. Die 4 Dezimalzahlen sind durch einen Punkt getrennt.
- ☐ Um den Verbindungstyp auszuwählen, wählen Sie in der Optionsliste *Connection type* das Optionsfeld *SSH*.
  Nach Auswahl und Einstellung der notwendigen Parameter bietet das Gerät Ihnen die Möglichkeit, die Datenverbindung über SSH herzustellen.

- ☐ Klicken Sie die Schaltfläche *Open*, um die Datenverbindung zu Ihrem Gerät aufzubauen.
  Abhängig vom Gerät und vom Zeitpunkt des Konfigurierens von SSH dauert der Verbindungsaufbau bis zu eine Minute.
  Bei der 1. Anmeldung zeigt das Programm *PuTTY* gegen Ende des Verbindungsaufbaus eine Sicherheitswarnmeldung und ermöglicht Ihnen, den Fingerabdruck des Schlüssels zu prüfen.

Abb. 5: Sicherheitsabfrage für den Fingerabdruck

- ☐ Prüfen Sie den Fingerabdruck.
  Das hilft Ihnen dabei, sich vor unliebsamen Gästen zu schützen.
- ☐ Stimmt der Fingerabdruck mit dem Fingerabdruck des Geräteschlüssels überein, klicken Sie die Schaltfläche *Yes*.
  Das Gerät ermöglicht Ihnen, die Fingerabdrücke der Geräteschlüssel mit dem Kommando `show ssh` oder in der grafischen Benutzeroberfläche im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH* auszulesen.
  Das Command Line Interface meldet sich auf dem Bildschirm mit einem Fenster für die Eingabe des Benutzernamens. Das Gerät bietet bis zu 5 Benutzern gleichzeitig die Möglichkeit, auf das Command Line Interface zuzugreifen.
- ☐ Fügen Sie den Benutzernamen ein.
  Der voreingestellte Benutzername ist `admin`.
- ☐ Drücken Sie die <Enter>-Taste.
- ☐ Fügen Sie das Passwort ein.
  Das voreingestellte Passwort ist `private`.
- ☐ Drücken Sie die <Enter>-Taste.

Anmerkung: Dieses Gerät ist ein sicherheitsrelevantes Produkt. Ändern Sie das Passwort gleich bei der ersten Inbetriebnahme.

```
login as: admin
admin@192.168.1.5's password:


                        Copyright (c) 2011-2022 Schneider Electric

                                  All rights reserved

                               MCSESM-E Release 08.7.00

                              (Build date 2022-07-11 16:24)


                     System Name    :  MCSESM-646038d5e846
                     Management IP  :  192.168.1.5
                     Subnet Mask    :  255.255.255.0
                     Base MAC       :  64:60:38:01:02:03
                     USB IP         :  91.0.0.100
                     USB Mask       :  255.255.255.0
                     System Time    :  2022-07-13 19:35:56


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.

MCSESM-E>
```

Abb. 6: Start-Bildschirm des Command Line Interfaces

1.2.4 Zugriff auf das Command Line Interface über die serielle Schnittstelle

Die serielle Schnittstelle dient zum lokalen Anschließen einer externen Netz-Management-Station (VT100-Terminal oder PC mit Terminal-Emulation). Die Schnittstelle ermöglicht Ihnen, eine Datenverbindung zum Command Line Interface und zum Systemmonitor herzustellen.

Führen Sie die folgenden Schritte aus:

- ☐ Verbinden Sie das Gerät über die serielle Schnittstelle mit einem Terminal. Alternativ verbinden Sie das Gerät mit einem COM-Port Ihres PCs mit Terminal-Emulation nach VT100 und drücken Sie eine beliebige Taste.
- ☐ Alternativ erstellen Sie die serielle Datenverbindung zum Gerät über die serielle Schnittstelle mit dem Programm *PuTTY*. Drücken Sie die <Enter>-Taste.

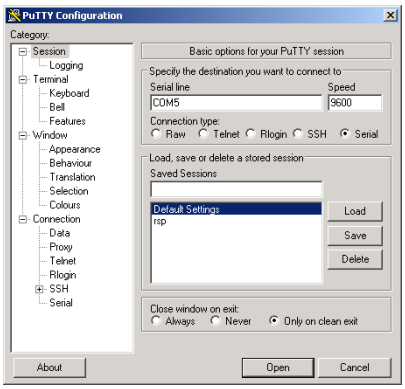


Abb. 7: Serielle Datenverbindung über die serielle Schnittstelle mit dem Programm PuTTY

- ☐ Drücken Sie mehrfach eine beliebige Taste Ihrer Terminal-Tastatur, bis Ihnen der Login-Bildschirm den CLI-Modus signalisiert.
- ☐ Fügen Sie den Benutzernamen ein.
  Der voreingestellte Benutzername ist `admin`.
- ☐ Drücken Sie die <Enter>-Taste.
- ☐ Fügen Sie das Passwort ein.
  Das voreingestellte Passwort ist `private`.
- ☐ Drücken Sie die <Enter>-Taste.

Anmerkung: Dieses Gerät ist ein sicherheitsrelevantes Produkt. Ändern Sie das Passwort gleich bei der ersten Inbetriebnahme.

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:24)


                  System Name   :  MCSESM-646038d5e846
                  Management IP :  192.168.1.5
                  Subnet Mask   :  255.255.255.0
                  Base MAC      :  64:60:38:01:02:03
                  USB IP        :  91.0.0.100
                  USB Mask      :  255.255.255.0
                  System Time   :  2022-07-13 19:35:56


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.

MCSESM-E>
```

Abb. 8: Start-Bildschirm des Command Line Interfaces

1.2.5 Modus-basierte Kommando-Hierarchie

Im Command Line Interface sind die Kommandos in zugehörige Modi gruppiert, entsprechend der Art des Kommandos. Jeder Kommando-Modus unterstützt bestimmte Schneider Electric Software-Kommandos.

Die Kommandos, die Ihnen als Benutzer zur Verfügung stehen, sind abhängig von Ihrer Berechtigungsstufe (administrator, operator, guest, auditor). Sie sind außerdem abhängig vom Modus, in dem Sie gerade arbeiten. Die Kommandos in einem bestimmten Modus sind für Sie verfügbar, wenn Sie zu diesem Modus umschalten.

Eine Ausnahme bilden die User Exec-Modus Kommandos. Das Command Line Interface bietet Ihnen die Möglichkeit, diese Kommandos auch im Privileged Exec Modus auszuführen.

Die folgende Abbildung zeigt die Modi des Command Line Interfaces.

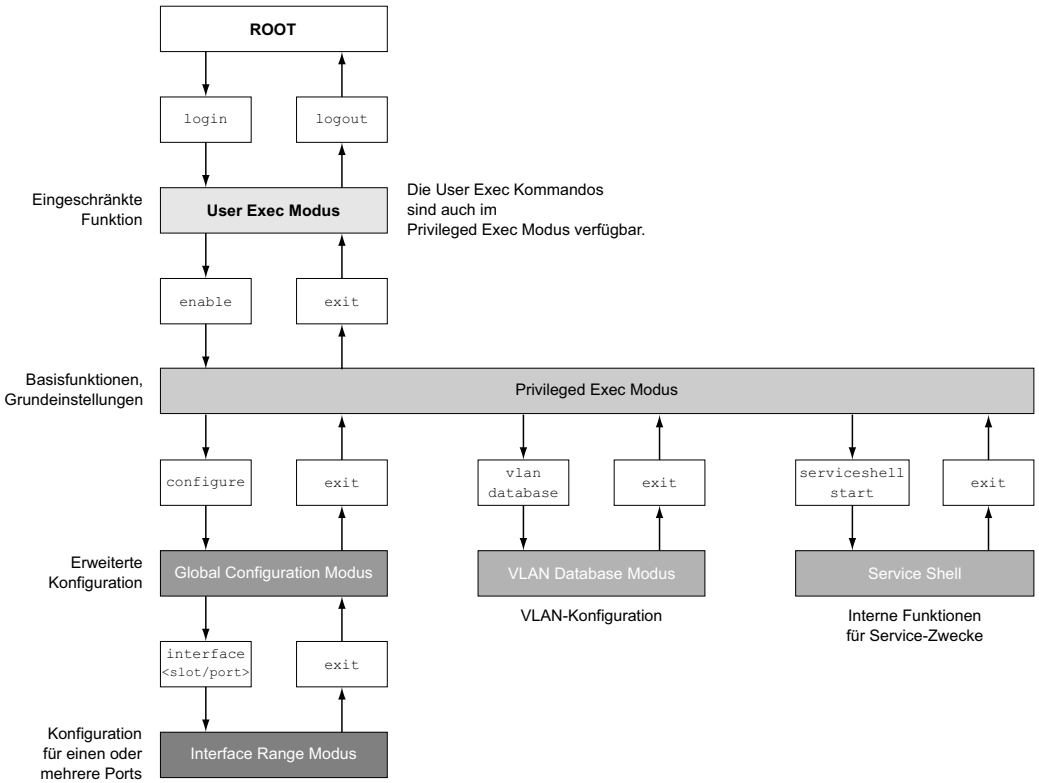


Abb. 9: Aufbau des Command Line Interfaces

Das Command Line Interface unterstützt, abhängig von der Berechtigungsstufe (User Level), die folgenden Modi:

- User Exec Modus
  Nach Anmelden mit dem Command Line Interface befinden Sie sich im User Exec Modus. Der User Exec Modus enthält einen begrenzten Umfang an Kommandos.
  Kommando-Prompt: `(MCSESM-E) >`
- Privileged Exec Modus
  Um Zugriff auf den gesamten Befehlsumfang zu haben, wechseln Sie in den Privileged Exec Modus. Voraussetzung für den Wechsel in den Privileged Exec Modus ist, dass Sie sich als privilegierter Benutzer anmelden. Vom Privileged Exec Modus aus sind auch die Kommandos des User Exec Modus ausführbar.
  Kommando-Prompt: `(MCSESM-E) #`
- VLAN-Modus
  Der VLAN-Modus enthält VLAN-bezogene Kommandos.
  Kommando-Prompt: `(MCSESM-E) (VLAN)#`
- Service Shell
  Die Service Shell dient ausschließlich zu Service-Zwecken.
  Kommando-Prompt: `/mnt/fastpath #`

- Global Config Modus
  Der Global Config Modus ermöglicht Ihnen, Modifikationen an der laufenden Konfiguration durchzuführen. In diesem Modus sind allgemeine Setup-Kommandos zusammengefasst.
  Kommando-Prompt: `(MCSESM-E) (config)#`
- Interface Range Modus
  Die Befehle Interface Range Modus wirken sich auf einen bestimmten Port, auf eine ausgewählte Gruppe von mehreren Ports oder auf alle Ports aus. Die Befehle modifizieren einen Wert oder schalten eine Funktion an einem oder an mehreren bestimmten Ports an/aus.
  - Alle physikalischen Ports des Gerätes
    Kommando-Prompt: `(MCSESM-E) ((interface) all)#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MCSESM-E) (config)#interface all
    (MCSESM-E) ((Interface)all)#
    ```
  - Einzelner Port an einem Interface
    Kommando-Prompt: `(MCSESM-E) (interface <slot/port>)#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MCSESM-E) (config)#interface 2/1
    (MCSESM-E) (interface 2/1)#
    ```
  - Eine Portreihe an einem Interface
    Kommando-Prompt: `(MCSESM-E) (interface <interface range> )#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MCSESM-E) (config)#interface 1/2-1/4
    (MCSESM-E) ((Interface)1/2-1/4)#
    ```
  - Eine Auflistung von einzelnen Ports
    Kommando-Prompt: `(MCSESM-E) (interface <interface list>)#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MCSESM-E) (config)#interface 1/2,1/4,1/5
    (MCSESM-E) ((Interface)1/2,1/4,1/5)#
    ```
  - Eine Auflistung von Portreihen und einzelnen Ports
    Kommando-Prompt: `(MCSESM-E) (interface <complex range>)#`
    Beispiel: Beim Wechsel vom Global Config Modus in den Interface Range Modus ändert sich das Kommando-Prompt wie folgt:
    ```
    (MCSESM-E) (config)#interface 1/2-1/4,1/6-1/9
    (MCSESM-E) ((Interface)1/2-1/4,1/6-1/9)
    ```

Die folgende Tabelle zeigt die Kommando Modi, die im jeweiligen Modus sichtbaren Kommando-Prompts (Eingabeaufforderungszeichen) und die Möglichkeit, mit der Sie den Modus beenden.

Tab. 2: Kommando-Modi

Kommando-modus	Zugriffsmethode	Beenden oder nächsten Modus starten

User Exec Modus	Erste Zugriffsebene. Basisaufgaben ausführen und Systeminformationen auflisten.	Zum Beenden geben Sie `logout` ein:
		`(MCSESM-E) >logout`
		`Are you sure (Y/N) ?y`

Privileged Exec Modus	Aus dem User Exec Modus geben Sie den Befehl `enable` ein.
	`(MCSESM-E) >enable`
	`(MCSESM-E) #`
		Um den Privileged Exec Modus zu beenden und in den User Exec Modus zurückzukehren, geben Sie `exit` ein:
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

VLAN-Modus	Aus dem Privileged Exec Modus geben Sie den Befehl `vlan database` ein.
	`(MCSESM-E) #vlan database`
	`(MCSESM-E) (Vlan)#`
		Um den VLAN-Modus zu beenden und in den Privileged Exec Modus zurückzukehren, geben Sie `exit` ein oder drücken Sie Ctrl-Z.
		`(MCSESM-E) (Vlan)#exit`
		`(MCSESM-E) #`

Global Config Modus	Aus dem Privileged Exec Modus geben Sie den Befehl `configure` ein.
	`(MCSESM-E) #configure`
	`(MCSESM-E) (config)#`
	Aus dem User Exec Modus geben Sie Befehl `enable` und dann im Privileged Exec Modus den Befehl `Configure` ein.
	`(MCSESM-E) >enable`
	`(MCSESM-E) #configure`
	`(MCSESM-E) (config)#`
		Um den Global Config Modus zu beenden und in den Privileged Exec Modus zurückzukehren, geben Sie `exit` ein:
		`(MCSESM-E) (config)#exit`
		`(MCSESM-E) #`
		Um anschließend den Privileged Exec Modus zu beenden und in den User Exec Modus zurückzukehren, geben Sie erneut `exit` ein:
		`(MCSESM-E) #exit`
		`(MCSESM-E) >`

Interface Range Modus	Aus dem Global Config Modus geben Sie den Befehl `interface {all|<slot/port>|<interface range> |<interface list>|<complex range>}` ein.
	`(MCSESM-E) (config)#interface <slot/port>`
	`(MCSESM-E) (interface slot/port)#`
		Um den Interface Range Modus zu beenden und in den Global Config Modus zurückzukehren, geben Sie `exit` ein. Um zum Privileged Exec Modus zurückzukehren, drücken Sie Ctrl-Z.
		`(MCSESM-E) (interface slot/port)#exit`
		`(MCSESM-E) #`

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.

```
(MCSESM-E)>
  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.

(MCSESM-E)>
```

Abb. 10: Kommandos im User Exec Modus

1.2.6 Ausführen von Kommandos

Syntaxanalyse

Nach Anmelden mit dem Command Line Interface befinden Sie sich im User Exec Modus. Das Command Line Interface gibt das `(MCSESM-E)>` Prompt auf dem Bildschirm aus.

Wenn Sie ein Kommando eingeben und die <Eingabetaste> drücken, startet das Command Line Interface die Syntax-Analyse. Das Command Line Interface durchsucht den Kommandobaum nach dem gewünschten Kommando.

Falls das Kommando außerhalb des Command Line Interface Kommandoumfangs liegt, zeigt Ihnen eine Meldung den erkannten Fehler.

Beispiel:

Sie beabsichtigen, den Befehl `show system info` auszuführen, geben jedoch `info` ohne `f` ein und drücken die <Enter>-Taste.

Das Command Line Interface gibt daraufhin eine Meldung aus:

```
(MCSESM-E)>show system ino

Error: Invalid command 'ino'
```

Kommandobaum

Die Kommandos im Command Line Interface sind in einer Baumstruktur organisiert. Die Kommandos und ggf. die zugehörigen Parameter verzweigen sich so lange weiter, bis das Kommando komplett definiert und damit ausführbar ist. Das Command Line Interface prüft die Eingaben. Wenn Sie den Befehl und die Parameter korrekt und vollständig eingegeben haben, führen Sie den Befehl durch Dücken der <Enter>-Taste aus.

Nachdem Sie den Befehl und die erforderlichen Parameter eingegeben haben, behandelt das CLI die weiteren eingegebenen Parameter wie optionale Parameter. Wenn einer der Parameter unbekannt ist, gibt das Command Line Interface eine Syntax-Meldung aus.

Der Kommandobaum verzweigt sich bei erforderlichen Parametern weiter, bis die erforderlichen Parameter die letzte Abzweigung der Struktur erreicht haben.

Bei optionalen Parametern verzweigt sich der Kommandobaum weiter, bis die erforderlichen und die optionalen Parameter die letzte Abzweigung der Struktur erreicht haben.

1.2.7 Aufbau eines Kommandos

Dieser Abschnitt beschreibt Syntax, Konventionen und Terminologie und stellt diese anhand von Beispielen dar.

Format der Kommandos

Ein Großteil der Kommandos enthält Parameter.

Fehlt der Kommando-Parameter, zeigt das Command Line Interface einen Hinweis auf eine erkannte fehlerhafte Syntax des Befehls.

Dieses Handbuch stellt die Befehle und Parameter in der Schriftart `Courier` dar.

Parameter

Die Reihenfolge der Parameter ist für die korrekte Syntax eines Kommandos relevant.

Parameter sind notwendige Werte, optionale Werte, Auswahlen oder eine Kombination davon. Die Darstellung zeigt die Art des Parameters.

Tab. 3: Parameter- und Kommando-Syntax

`<command>`	Kommandos in spitzen Klammern (<>) sind obligatorisch.
`[command]`	Kommandos in eckigen Klammern ([]) sind optional.
`<parameter>`	Parameter in spitzen Klammern (<>) sind obligatorisch.
`[parameter]`	Parameter in eckigen Klammern ([]) sind optional.
`...`	Auslassungspunkte (3 aufeinander folgende Punkte ohne Leerzeichen) nach einem Element zeigen an, dass Sie das Element wiederholen können.

Tab. 3: Parameter- und Kommando-Syntax

`[Choice1 | Choice2]`	Eine senkrechte Linie, eingeschlossen in Klammern, zeigt eine Auswahlmöglichkeit. Wählen Sie einen Wert. Durch eine senkrechte Linie getrennte Elemente, eingeschlossen in eckigen Klammern, zeigen eine optionale Auswahlmöglichkeit an (Auswahl1 oder Auswahl2 oder keine Auswahl).
`{list}`	Die geschweiften Klammern (`{}`) zeigen eine Auswahlmöglichkeit von Parametern aus einer Liste.
`{Choice1 | Choice2}`	Durch eine senkrechte Linie getrennte Elemente, eingeschlossen in geschweiften Klammern (`{}`), zeigen eine obligatorische Auswahlmöglichkeit an (Auswahl1 oder Auswahl2).
`[param1 {Choice1 | Choice2}]`	Zeigt einen optionalen Parameter, der eine obligatorische Auswahl beinhaltet.
`<a.b.c.d>`	Kleinbuchstaben sind Wildcards (Jokerzeichen). Parameter der Notation a.b.c.d geben Sie mit Punkten ein (zum Beispiel IP-Adressen).
`<cr>`	Erzeugen Sie durch Drücken der <Enter>-Taste einen Zeilenumbruch.

Die folgende Liste zeigt mögliche Parameterwerte innerhalb des Command Line Interface:

Tab. 4: Parameterwerte im Command Line Interface

Wert	Beschreibung
IP-Adresse	Dieser Parameter stellt eine gültige IPv4-Adresse dar. Die Adresse besteht aus 4 Hexadezimalzahlen vom Wert 0 bis 255. Die 4 Dezimalzahlen sind durch einen Dezimalpunkt getrennt. Die Eingabe der IP-Adresse `0.0.0.0` ist gültig.
MAC-Adresse	Dieser Parameter stellt eine gültige MAC-Adresse dar. Die Adresse besteht aus 6 Hexadezimalzahlen vom Wert 00 bis FF. Die Zahlen werden durch Doppelpunkte getrennt, zum Beispiel `00:F6:29:B2:81:40`.
string	Benutzerdefinierter Text mit einer Länge im angegebenen 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 angegebenen Bereich, zum Beispiel `0..999999`.
date	Datum im Format `YYYY-MM-DD`.
time	Zeit im Format `HH:MM:SS`.

Netzadressen

Netzadressen sind Voraussetzung beim Aufbau einer Datenverbindung zu einer entfernten Arbeitsstation, einem Server oder einem anderen Netz. Man unterscheidet zwischen IP-Adressen und MAC-Adressen.

Die IP-Adresse ist eine Adresse, die der Netzadministrator vergibt. Die IP-Adresse ist in einem Netz eindeutig.

Die MAC-Adressen vergibt der Hardware-Hersteller. MAC-Adressen sind weltweit eindeutig.

Die folgende Tabelle zeigt die Darstellung und den Bereich der Adresstypen:

Tab. 5: Format und Bereich von Netzadressen

Adresstyp	Format	Bereich	Beispiel
IP-Adresse	nnn.nnn.nnn.nnn	nnn: 0 bis 255 (dezimal)	192.168.11.110
MAC-Adresse	mm:mm:mm:mm:mm:mm	mm: 00 bis ff (hexadezimale Zahlenpaare)	A7:C9:89:DD:A9:B3

Zeichenfolgen (Strings)

Anführungszeichen markieren eine Zeichenfolge (String). Zum Beispiel: `"System name with space character"`. Leerzeichen sind keine gültigen benutzerdefinierten Strings. Ein Leerzeichen in einem Parameter geben Sie innerhalb von Anführungszeichen ein.

Beispiel:

```
*(MCSESM-E)#cli prompt Device name
Error: Invalid command 'name'

*(MCSESM-E)#cli prompt 'Device name'

*(Device name)#
```

1.2.8 Beispiele für Kommandos

Beispiel 1: clear arp-table-switch

Kommando zum Löschen der ARP-Tabelle des Management-Agenten (Cache).

`clear arp-table-switch` ist die Befehlsbezeichnung. Das Kommando ist ohne weitere Parameter durch Drücken der <Enter>-Taste ausführbar.

Beispiel 2: radius server timeout

Kommando, um die Zeitüberschreitung des RADIUS Servers zu konfigurieren.

```
(MCSESM-E) (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.

```
(MCSESM-E) (config)#radius server auth modify 1
 [name]               RADIUS authentication server name.
 [port]               RADIUS authentication server port.
```

```
                      (default: 1812).
 [msgauth]            Enable or disable the message authenticator
                      attribute for this server.
 [primary]            Configure the primary RADIUS server.
 [status]             Enable or disable a RADIUS authentication
                      server entry.
 [secret]             Configure the shared secret for the RADIUS
                      authentication server.
 [encrypted]          Configure the encrypted shared secret.
  <cr>                Press Enter to execute the command.
```

`radius server auth modify` ist die Befehlsbezeichnung.

Der Parameter `<1..8>` (RADIUS server index) ist notwendig. Der Wertebereich ist `1..8` (Integer).

Die Parameter `[name]`, `[port]`, `[msgauth]`, `[primary]`, `[status]`, `[secret]` und `[encrypted]` sind optional.

1.2.9 Eingabeprompt

Kommandomodus

Das Command Line Interface zeigt durch das Eingabeprompt, in welchem der Modi Sie sich befinden:

- `(MCSESM-E) >`
  User Exec Modus
- `(MCSESM-E) #`
  Privileged Exec Modus
- `(MCSESM-E) (config)#`
  Global Config Modus
- `(MCSESM-E) (Vlan)#`
  VLAN Database mode
- `(MCSESM-E) ((Interface)all)#`
  Interface Range Modus / Alle Ports des Geräts
- `(MCSESM-E) ((Interface)2/1)#`
  Interface Range Modus / Einzelner Port auf einem Interface
- `(MCSESM-E) ((Interface)1/2-1/4)#`
  Interface Range Modus / Eine Reihe von Ports auf einem Interface
- `(MCSESM-E) ((Interface)1/2,1/4,1/5)#`
  Interface Range Modus / Eine Auflistung von einzelnen Ports
- `(MCSESM-E) ((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.
  `*(MCSESM-E)>`

- Rautezeichen `#`
  Ein Rautezeichen `#` zu Beginn des Eingabeprompts zeigt, dass sich die Boot-Parameter von den Parametern während der Bootphase unterscheiden.
  `*#(MCSESM-E)>`
- Ausrufezeichen `!`
  Ein Ausrufezeichen `!` zu Beginn des Eingabeprompts zeigt: das Passwort für die Benutzerkonten `user` oder `admin` stimmt mit dem Lieferzustand überein.
  `!(MCSESM-E)>`

Wildcards

Das Gerät ermöglicht Ihnen, den Prompt der Befehlszeile zu ändern.

Das Command Line Interface unterstützt die folgenden Platzhalter:

Tab. 6: Verwendung von Wildcards am Eingabeprompt des Command Line Interfaces

Wildcard	Beschreibung
`%d`	Systemdatum
`%t`	Systemzeit
`%i`	IP-Adresse des Geräts
`%m`	MAC-Adresse des Gerätes
`%p`	Produktbezeichnung des Geräts

```
!(MCSESM-E)>enable

!(MCSESM-E)#cli prompt %i

!192.168.1.5#cli prompt (MCSESM-E)%d

!*(MCSESM-E)2022-07-13#cli prompt (MCSESM-E)%d%t

!*(MCSESM-E)2022-07-13 19:35:56#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.10 Tastaturkombinationen

Die folgenden Tastaturkombinationen erleichtern Ihnen die Arbeit mit dem Command Line Interface:

Tab. 7: Tastenkombinationen im Command Line Interface

Tastaturkombination	Beschreibung
<STRG> + <H>, <Zurück (Backspace)>	Letztes Zeichen löschen
<STRG> + <A>	Zum Zeilenanfang gehen
<STRG> + <E>	Zum Zeilenende gehen

Tab. 7: Tastenkombinationen im Command Line Interface

Tastaturkombination	Beschreibung
<STRG> + <F>	Ein Zeichen nach vorn gehen
<STRG> + <B>	Ein Zeichen zurück gehen
<STRG> + <D>	Nächstes Zeichen löschen
<STRG> + <U>, <X>	Zeichen bis zum Anfang der Zeile löschen
<STRG> + <K>	Zeichen bis zum Ende der Zeile löschen
<STRG> + <W>	Vorheriges Wort löschen
<STRG> + <P>	Zur vorherigen Zeile im Speicher wechseln
<STRG> + <R>	Zeile erneut schreiben oder Inhalte einfügen
<STRG> + <N>	Zur nächsten Zeile im Speicher wechseln
<STRG> + <Z>	Zum Ursprung wechseln
<STRG> + <G>	Laufende tcpdump-Ausgabe abbrechen
<Tabulator>, <LEER-TASTE>	Kommandozeilen Vervollständigung
`Exit`	Exit zur nächsten, niedrigen Kommandozeile wechseln
<?>	Auswahl anzeigen / Hilfe darstellen

Das Help-Kommando listet die möglichen Tastenkombinationen des Command Line Interface auf dem Bildschirm auf:

```
(MCSESM-E) #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

(MCSESM-E) #
```

Abb. 11: Auflisten der Tastenkombinationen mit dem Help-Kommando

1.2.11 Eingabehilfen

Befehlsergänzung

Das Command Line Interface ermöglicht Ihnen, die Befehlsvervollständigung (Tab-Completion) zu verwenden, um die Eingabe von Befehlen zu vereinfachen. Damit haben Sie die Möglichkeit, Schlüsselwörter abzukürzen.

- Tippen Sie den Beginn eines Schlüsselwortes ein. Wenn die eingegebenen Buchstaben ein Schlüsselwort (keyword) kennzeichnen und Sie die Tabulator- oder Leertaste betätigen, ergänzt das Command Line Interface das Schlüsselwort. Falls mehr als eine Schlüsselwort-Ergänzung möglich ist, geben Sie den oder die zur eindeutigen Identifizierung notwendigen Buchstaben ein. Betätigen Sie erneut die Tabulator- oder Leertaste. Das System ergänzt daraufhin den Befehl oder Parameter.
- Wenn Sie bei einer mehrdeutigen Eingabe 2 Mal die Taste <Tab>oder <Leerzeichen> drücken, gibt das Command Line Interface eine Auswahlliste aus.
- Bei einer mehrdeutigen Eingabe und Drücken der Taste <Tab> oder <Leerzeichen> ergänzt das Command Line Interface den Befehl bis zum Beginn der Mehrdeutigkeit. Wenn Sie anschließend erneut die Taste <Tab> oder <Leerzeichen> drücken, zeigt das Command Line Interface eine Auswahlliste.
  Beispiel:
  ```
  (MCSESM-E) (Config)#lo
  (MCSESM-E) (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 `(MCSESM-E) >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:

```
!*#(MCSESM-E)(Config)#show?

   show          Display device options and settings.
```

1.2.12 Anwendungsfälle

Konfiguration speichern

Damit Ihre Password-Einstellungen und Ihre sonstigen Konfigurationsänderungen nach einem Reset des Gerätes oder nach einer Unterbrechung der Spannungsversorgung erhalten bleiben, speichern Sie die Konfiguration. Führen Sie dazu die folgenden Schritte aus:

- ☐ Wechseln Sie mit `enable` in den Privileged Exec Modus.
- ☐ Geben Sie das folgende Kommando ein:
  `save [profile]`
- ☐ Führen Sie den Befehl aus durch Betätigen der <Enter>-Taste.

Syntax des Kommandos „radius server auth add“

Verwenden Sie dieses Kommando, um einen RADIUS-Authentication-Server hinzuzufügen.

- Kommandomodus: `Global Config` Modus
- Berechtigungsstufe: Administrator
- Format: `radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - `[name]`: Name des RADIUS Authentication Servers.
  - `[port]`: Port des RADIUS Authentication Servers (Voreinstellung: `1813`).

Parameter	Bedeutung	Wertebereich
`<1..8>`	Index des RADIUS Servers.	`1..8`
`<a.b.c.d>`	IP-Adresse des RADIUS Accounting Servers.	IP-Adresse
`<string>`	Geben Sie einen benutzerdefinierten Text ein, maximal 32 Zeichen lang.	
`<1..65535>`	Geben Sie eine Portnummer zwischen 1 und 65535 ein.	`1..65535`

Modus und Berechtigungsstufe:

- Voraussetzung für das Ausführen des Kommandos: Sie befinden sich im Global Config Modus. Siehe „Modus-basierte Kommando-Hierarchie” auf Seite 25.
- Voraussetzung für das Ausführen des Kommandos: Sie haben die Berechtigungsstufe Administrator.

Syntax der Kommandos und Parameter: Siehe „Aufbau eines Kommandos” auf Seite 30.

Beispiele für ausführbare Kommandos:

- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

1.2.13 Service Shell

Die Service Shell dient ausschließlich zu Service-Zwecken.

Die Service Shell ermöglicht Benutzern den Zugriff auf interne Funktionen des Geräts. Wenn Sie beim Zugriff auf Ihr Gerät Unterstützung benötigen, verwendet das Service-Personal die Service Shell, um interne Zustände wie Switch-Register und CPU-Register zu überwachen.

HINWEIS
GEFAHR EINER BEEINTRÄCHTIGUNG DER FUNKTIONSFÄHIGKEIT DES GERÄTS Führen Sie keine internen Funktionen ohne Anweisung eines Servicetechnikers aus, zum Beispiel Löschen des permanenten Speichers (*NVM*). **Das Nicht-Beachten dieser Anweisungen führt möglicherweise zu einem nicht mehr funktionierenden Gerät.**

Service Shell starten

Voraussetzung ist, dass Sie sich im User Exec-Modus befinden: `(MCSESM-E) >`

Führen Sie die folgenden Schritte aus:
- ☐ Fügen Sie `enable` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - Fügen Sie `e` ein und drücken die <Enter>-Taste.
- ☐ Fügen Sie `serviceshell start` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - Fügen Sie `ser` ein und drücken die <Enter>-Taste.
  - Fügen Sie `s` ein und drücken die <Enter>-Taste.

```
!MCSESM-E >enable

!*MCSESM-E #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 (2022-07-13 19:35:56 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

Arbeiten mit der Service Shell

Wenn die Service Shell aktiv ist, ist das Timeout des Command Line Interfaces inaktiv. Um Inkonsistenzen in der Gerätekonfiguration zu vermeiden, beenden Sie die Service Shell, bevor ein anderer Benutzer die Übertragung einer neuen Konfiguration auf das Gerät startet.

Service Shell-Kommandos anzeigen

Voraussetzung ist, dass Sie die Service Shell bereits gestartet haben.

Führen Sie die folgenden Schritte aus:
☐ Fügen Sie `help` ein und drücken die <Enter>-Taste.

```
/mnt/fastpath # help
Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let
        local pwd read readonly return set shift source test times trap
        true type ulimit umask unalias unset wait
/mnt/fastpath #
```

Service Shell beenden

Führen Sie die folgenden Schritte aus:
☐ Fügen Sie `exit` ein und drücken die <Enter>-Taste.

Service Shell permanent im Gerät deaktivieren

Wenn Sie die Service Shell deaktivieren, haben Sie weiterhin die Möglichkeit, das Gerät zu konfigurieren Sie schränken jedoch die Möglichkeiten des Service-Personals zur Durchführung von System-Diagnosen ein. Der Service-Techniker hat dann keine Möglichkeit mehr, auf interne Funktionen Ihres Geräts zuzugreifen.

Die Deaktivierung ist unumkehrbar. Die Service Shell bleibt dauerhaft deaktiviert. **Um die Service Shell zu reaktivieren ist das Öffnen des Geräts seitens des Herstellers erforderlich.**

Die Voraussetzungen sind:
- Die Service Shell ist nicht gestartet.
- Sie befinden sich im User Exec-Modus: `(MCSESM-E) >`

Führen Sie die folgenden Schritte aus:
☐ Fügen Sie `enable` ein und drücken die <Enter>-Taste.
Um den Aufwand beim Tippen zu reduzieren:
– Fügen Sie `e` ein und drücken die <Enter>-Taste.

- ☐ Fügen Sie `serviceshell deactivate` ein und drücken die <Enter>-Taste.
  Um den Aufwand beim Tippen zu reduzieren:
  - Fügen Sie `ser` ein und drücken die <Enter>-Taste.
  - Fügen Sie `dea` ein und drücken die <Enter>-Taste.
- ☐ **Dieser Schritt ist unumkehrbar!**
  Drücken Sie die <Y>-Taste.

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

1.3 System-Monitor

Der System-Monitor ermöglicht Ihnen, vor dem Starten des Betriebssystems grundlegende Betriebsparameter einzustellen.

1.3.1 Funktionsumfang

Im System-Monitor erledigen Sie beispielsweise folgende Aufgaben:
- Betriebssystem verwalten und Software-Image prüfen
- Betriebssystem aktualisieren
- Betriebssystem starten
- Konfigurationsprofile löschen, Gerät auf Lieferzustand zurücksetzen
- Bootcode-Information prüfen

1.3.2 System-Monitor starten

Sie stellen eine serielle Verbindung mit dem Gerät über die USB-C-Schnittstelle her. Während des Boot-Vorgangs ist die serielle Schnittstelle des Geräts nicht verfügbar. Deshalb funktioniert das Starten des System-Monitors anders als bei anderen Schneider Electric-Geräten. Um den System-Monitor zu starten, versetzen Sie das Gerät in den Recovery-Modus.

Das Gerät in den Recovery-Modus versetzen

Erforderliches Zubehör:
- Externer Speicher (empfohlen: ACA22-USB-C)
- USB-C-auf-USB-A-Adapter (ausschließlich wenn Sie einen anderen als den empfohlenen externen Speicher verwenden)
- USB-Kabel, um den USB-C-Anschluss des Geräts mit dem Computer zu verbinden
- Computer mit einer VT100-Terminalemulation (zum Beispiel PuTTY) oder serielles Terminal

Führen Sie die folgenden Schritte aus:
- ☐ Stecken Sie den externen Speicher in Ihren Computer.
- ☐ Erstellen Sie im Root-Verzeichnis des externen Speichers eine leere Datei mit dem Namen `recovery.txt`.
- ☐ Stecken Sie den externen Speicher in das Gerät.
- ☐ Starten Sie das Gerät neu.
- ☐ Beobachten Sie die LEDs, während das Gerät hochfährt. Wenn die LED *Status* abwechselnd rot und grün blinkt, ist das Gerät erfolgreich in den Recovery-Modus gestartet.

Anmerkung: Die Beschreibung der Anzeigeelemente finden Sie im Anwender-Handbuch Installation.

Zugang zum System-Monitor

Führen Sie die folgenden Schritte aus:
- ☐ Entfernen Sie den externen Speicher vom Gerät.
- ☐ Verbinden Sie Ihren Computer über das USB-Kabel mit dem Gerät.

- ☐ Öffnen Sie die VT100-Terminalemulation auf dem Computer, um den System-Monitor anzuzeigen.
- ☐ Wählen Sie den korrekten COM-Port.

Wenn der Computer und das Gerät erfolgreich verbunden sind, sehen Sie einen schwarzen Bildschirm.

Führen Sie die folgenden Schritte aus:

- ☐ Drücken Sie die <Enter>-Taste, um den System-Monitor anzuzeigen.
  Sie sehen die folgende Ansicht auf Ihrem Computer:

```
System Monitor 1
(Selected OS: ...-8.7 (2022-07-11 16:24))

1  Manage operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

Abb. 12: System Monitor Ansicht

- ☐ Um einen Menüpunkt auszuwählen, geben Sie die entsprechende Zahl ein.
- ☐ Um ein Untermenü zu verlassen und zum Hauptmenü zurückzukehren, drücken Sie die <ESC>-Taste.

Anmerkung: Um das Gerät beim nächsten Mal normal zu starten, stecken Sie den externen Speicher ohne die `recovery.txt`-Datei ins Gerät.

2 IP-Parameter festlegen

Bei der Erstinstallation des Geräts benötigen Sie die IP-Parameter.

Das Gerät bietet bei der Erstinstallation die folgenden Möglichkeiten zur Eingabe der IP-Parameter:

- Eingabe über das Command Line Interface.
  Wählen Sie diese „In-Band“-Methode, wenn Sie Ihr Gerät außerhalb seiner Betriebsumgebung vorkonfigurieren oder Sie den Netzzugang („Out-of-Band“) zu dem Gerät wiederherstellen.
- Eingabe über das Protokoll Ethernet Switch Configurator.
  Wählen Sie diese „In-Band“-Methode für ein bereits installiertes Gerät im Netz, oder wenn eine weitere Ethernet-Verbindung zwischen Ihrem PC und dem Gerät besteht.
- Konfiguration über den externen Speicher.
  Wählen Sie diese Methode, wenn Sie ein Gerät durch ein Gerät desselben Typs ersetzen und Sie die Konfiguration bereits im externen Speicher gespeichert haben.
- Verwendung von BOOTP.
  Wählen Sie diese „In-Band“-Methode, um die Konfiguration des installierten Geräts über BOOTP vorzunehmen. Hierzu benötigen Sie einen BOOTP-Server. Der BOOTP-Server weist dem Gerät anhand seiner MAC-Adresse die Konfigurationsdaten zu. Der DHCP-Modus ist der Standardmodus für den Bezug der Konfigurationsdaten.
- Konfiguration über DHCP.
  Wählen Sie diese „In-Band“-Methode, um die Konfiguration des installierten Geräts über DHCP vorzunehmen. Hierzu benötigen Sie einen DHCP-Server. Der DHCP-Server weist dem Gerät anhand seiner MAC-Adresse oder seines Systemnamens die Konfigurationsdaten zu.
- Konfiguration über die grafische Benutzeroberfläche.
  Verfügt das Gerät bereits über eine IP-Adresse und ist über das Netz erreichbar, dann bietet Ihnen die grafische Benutzeroberfläche eine weitere Möglichkeit, die IP-Parameter zu konfigurieren.

2.1 Grundlagen IP Parameter

2.1.1 IPv4

IP-Adresse

Die IP-Adressen bestehen aus 4 Bytes. Diese 4 Bytes werden durch einen Punkt getrennt, dezimal dargestellt.

Seit 1992 sind im RFC 1340 fünf Klassen von IP-Adressen definiert.

Tab. 8: IP-Adressklassen

Klasse	Netzadresse	Hostadresse	Adressbereich
A	1 Byte	3 Bytes	0.0.0.0 bis 127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 bis 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 bis 223.255.255.255
D			224.0.0.0 bis 239.255.255.255
E			240.0.0.0 bis 255.255.255.255

Der erste Byte einer IP-Adresse ist die Netzadresse. Der Regulierungsausschuss für die weltweite Zuweisung von Netzadressen ist IANA („Internet Assigned Numbers Authority“). Falls Sie einen IP-Adressenblock benötigen, wenden Sie sich an Ihren Internet Service Provider (ISP). Ihr ISP wendet sich an seine lokale übergeordnete Organisation, um einen IP-Adressenblock zu reservieren:

- APNIC (Asia Pacific Network Information Center)
  Asien/Pazifik
- ARIN (American Registry for Internet Numbers)
  Amerika und Subsahara-Afrika
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  Lateinamerika und weitere Karibik-Inseln
- RIPE NCC (Réseaux IP Européens)
  Europa und umliegende Regionen

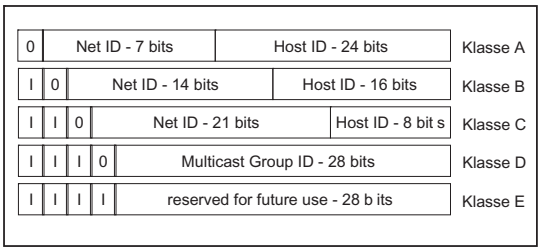


Abb. 13: Bitdarstellung der IP-Adresse

Ist das erste Oktett einer IP-Adresse eine Null, d. h. kleiner als 128, gehört sie der Klasse A an.

Ist das erste Bit einer IP-Adresse eine Eins und das zweite Bit eine Null, d. h. das erste Oktett liegt im Bereich von 128 bis 191, dann gehört die IP-Adresse der Klasse B an.

Sind die ersten beiden Bits einer IP-Adresse eine Eins, d. h. das erste Oktett ist größer als 191, dann handelt es sich um eine IP-Adresse der Klasse C.

Die Vergabe der Hostadresse (host ID) obliegt dem Netzbetreiber. Der Netzbetreiber allein ist für die Einmaligkeit der IP-Adressen, die er vergibt, verantwortlich.

Netzmaske

Router und Gateways unterteilen große Netze in Subnetze. Die Netzmaske ordnet die IP-Adressen der einzelnen Geräte einem bestimmten Subnetz zu.

Die Einteilung in Subnetze erfolgt über die Netzmaske analog zu der Einteilung der Netzadresse (net id) in die Klassen A bis C.

Setzen Sie die Bits der Hostadresse (host id), die die Maske darstellen, auf Eins. Setzen Sie die restlichen Bits der Hostadresse auf Null (vgl. folgende Beispiele).

Beispiel für eine Subnetzmaske:

Dezimale Darstellung
255.255.192.0

Binäre Darstellung
11111111.11111111.11000000.00000000

Subnetzmaskenbits
Klasse B

Beispiel für IP-Adressen mit Subnetzzuordnung gemäß der Netzmaske:

Dezimale Darstellung
129.218.65.17
└──── 128 < 129 191 › Klasse B

Binäre Darstellung
10000001.11011010.01000001.00010001
Subnetz 1
Netzadresse

Dezimale Darstellung
129.218.129.17
└──── 128 < 129 191 › Klasse B

Binäre Darstellung
10000001.11011010.10000001.00010001
Subnetz 2

Beispiel für die Anwendung der Netzmaske

In einem großen Netz ist es möglich, dass Gateways oder Router den Management-Agenten von ihrer Netz-Management-Station trennen. Wie erfolgt in einem solchen Fall die Adressierung?

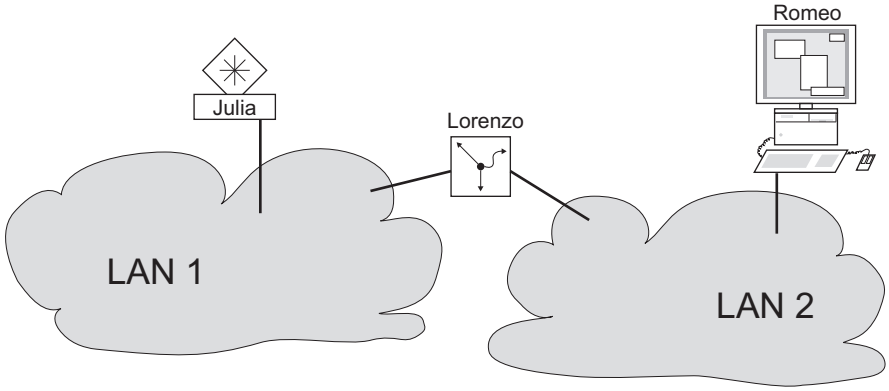


Abb. 14: Management-Agent durch Router von der Netz-Management-Station getrennt

Die Netz-Management-Station „Romeo” möchte Daten an den Management-Agenten „Julia” schicken. Romeo kennt die IP-Adresse von Julia und weiß, dass der Router „Lorenzo” den Weg zu Julia kennt.

Also packt Romeo seine Botschaft in einen Umschlag und schreibt als Zieladresse die IP-Adresse von Julia und als Quelladresse seine eigene IP-Adresse darauf.

Diesen Umschlag steckt Romeo in einen weiteren Umschlag mit der MAC-Adresse von Lorenzo als Zieladresse und seiner eigenen MAC-Adresse als Quelladresse. Dieser Vorgang ist vergleichbar mit dem Übergang von der Schicht 3 zur Schicht 2 des ISO/OSI-Basis-Referenzmodells.

Nun steckt Romeo das gesamte Datenpaket in den Briefkasten, vergleichbar mit dem Übergang von der Schicht 2 zur Schicht 1, das heißt dem Senden des Datenpaketes in das Ethernet.

Lorenzo erhält den Brief, entfernt den äußeren Umschlag und erkennt auf dem inneren Umschlag, dass der Brief für Julia bestimmt ist. Er steckt den inneren Umschlag in einen neuen äußeren Umschlag, schaut in seiner Adressliste, der ARP-Tabelle, nach der MAC-Adresse von Julia und schreibt diese auf den äußeren Umschlag als Zieladresse und seine eigene MAC-Adresse als Quelladresse. Das gesamte Datenpaket steckt er anschließend in den Briefkasten.

Julia empfängt den Brief, entfernt den äußeren Umschlag. Übrig bleibt der innere Umschlag mit Romeos IP-Adresse. Das Öffnen des inneren Umschlages und lesen der Botschaft entspricht einer Übergabe an höhere Protokollschichten des ISO/OSI-Schichtenmodells.

Julia möchte eine Antwort an Romeo zurücksenden. Sie steckt ihre Antwort in einen Umschlag mit der IP-Adresse von Romeo als Zieladresse und ihrer eigenen IP-Adresse als Quelladresse. Doch wohin soll Sie die Antwort schicken? Die MAC-Adresse von Romeo hat sie ja nicht erhalten. Die MAC-Adresse von Romeo blieb beim Wechseln des äußeren Umschlags bei Lorenzo zurück.

Julia findet in der MIB unter der Variablen `NetGatewayIPAddr` Lorenzo als Vermittler zu Romeo. So steckt sie den Umschlag mit den IP-Adressen in einen weiteren Umschlag mit der MAC-Zieladresse von Lorenzo.

Nun findet der Brief den gleichen Weg über Lorenzo zu Romeo, so wie der Brief von Romeo zu Julia fand.

Classless Inter-Domain Routing

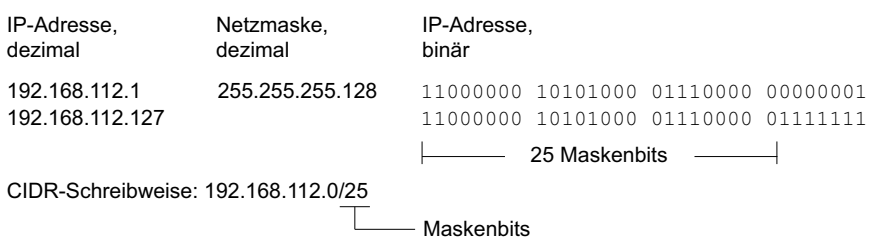
Die Klasse C mit maximal 254 Adressen war zu klein, und die Klasse B mit maximal 65534 Adressen war für die meisten Anwender zu groß. Hieraus resultierte eine nicht effektive Nutzung der zur Verfügung stehenden Klasse-B-Adressen.

Die Klasse D enthält reservierte Multicast-Adressen. Die Klasse E ist für experimentelle Zwecke vorgesehen. Ein Gateway, das nicht an diesen Experimenten teilnimmt, ignoriert experimentelle Datagramme mit diesen Zieladressen.

Seit 1993 verwendet RFC 1519 Classless Inter-Domain Routing (CIDR) zur Lösung dieses Problems. Das CIDR überwindet diese Klassenschranken und unterstützt klassenlose IP-Adressbereiche.

Mit CIDR legen Sie die Anzahl der Bits fest, die den IP-Adressbereich kennzeichnen. Hierzu stellen Sie den IP-Adressbereich in binärer Form dar und zählen die Maskenbits zur Bezeichnung der Netzmaske. Die Maskenbits entsprechen der Anzahl der Bits, die in einem bestimmten IP-Bereich für das Subnetz verwendet werden.

Beispiel:



Die Zusammenfassung mehrerer Adressbereiche der Klasse C wird als „Supernetting“ bezeichnet. Mit Supernetting lassen sich Adressbereiche der Klasse B sehr fein 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 IPv6können im Gerät parallel betrieben werden. Das wird durch die Verwendung vonDual 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.

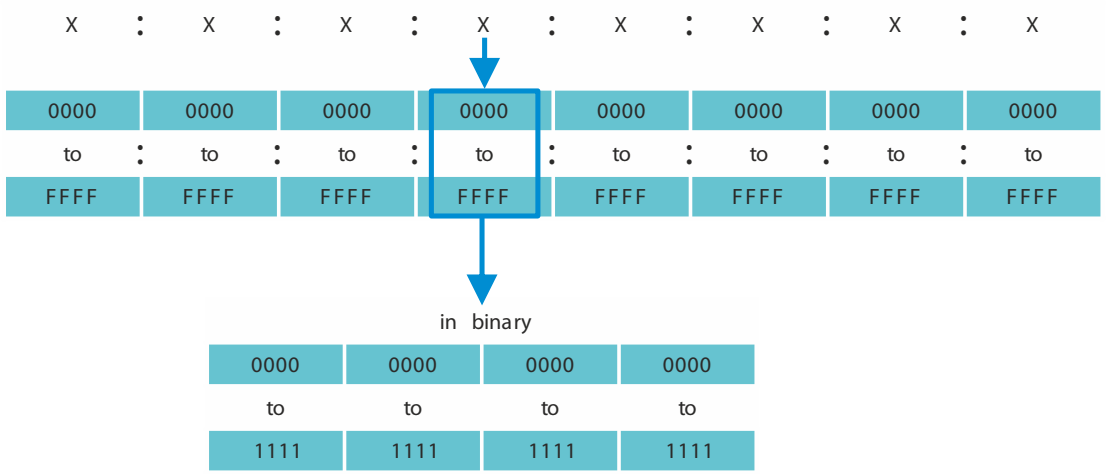


Abb. 15: Darstellung der IPv6-Adresse

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. 9: 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. 9: 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

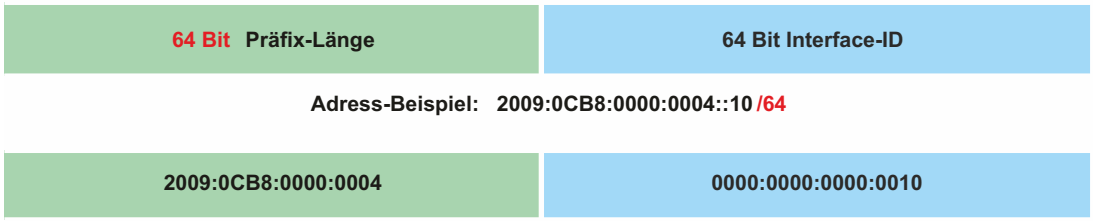
Im Gegensatz zu IPv4-Adressen verwenden IPv6-Adressen keine Subnetzmaske, um den Netzanteil einer Adresse zu bestimmen. Stattdessen nutzt das IPv6-Protokoll dafür die Präfixlänge.

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 der 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. 10: 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 nicht spezifizierte Adresse ist eine IPv6-Adresse, in der jedes Bit auf 0 gesetzt ist. Das entspricht 0.0.0.0 in IPv4. 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 wird Loopback-Adresse genannt. Sie kann von einem Gerät dazu verwendet werden, ein IPv6-Paket an sich selbst zu senden. Sie 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. 11: Format der Link-Local-Adresse

10 Bits	54 Bits	64 Bits
1111111010	0	Interface-ID

Die Link-Local-Adresse ist immer konfiguriert und nicht veränderbar.

Global-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.

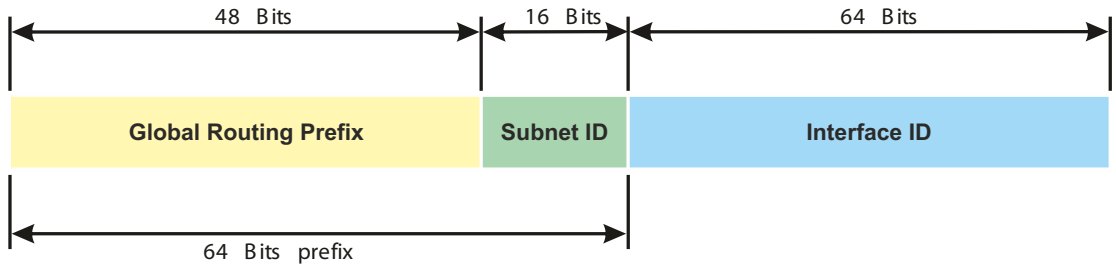


Abb. 16: Allgemeines Format der IPv6-Global-Unicast-Adresse

2.2 IP-Parameter mit dem Command Line Interface festlegen

2.2.1 IPv4

Es gibt folgende Möglichkeiten, die IP-Parameter einzugeben:
- BOOTP/DHCP
- Ethernet Switch Configurator-Protokoll
- Externer Speicher
- Command Line Interface über eine serielle Verbindung

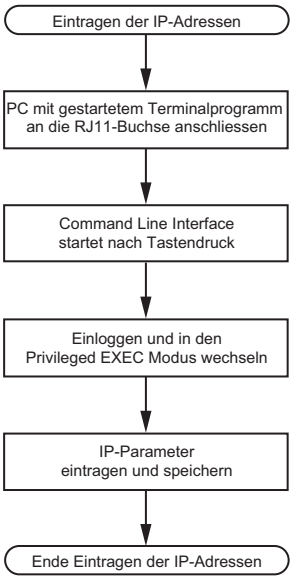


Abb. 17: Ablaufdiagramm Eintragen der IP-Adressen

Anmerkung: Sollten Sie in der Nähe des Installationsortes kein Terminal oder keinen PC mit Terminalemulation zur Verfügung haben, können Sie das Gerät an ihrem Arbeitsplatz konfigurieren und danach an seinen endgültigen Installationsort bringen.

Führen Sie die folgenden Schritte aus:
- ☐ Stellen Sie eine Verbindung zu dem Gerät her.
  Der Startbildschirm erscheint.

- ☐ Schalten Sie DHCP aus.

☐ Fügen Sie die IP-Parameter ein.
- Lokale IP-Adresse
  In der Voreinstellung ist die lokale IP-Adresse `0.0.0.0`.
- Netzmaske
  Wenn Sie Ihr Netz in Subnetze aufgeteilt haben und diese mit einer Netzmaske identifizieren, fügen Sie an dieser Stelle die Netzmaske ein. In der Voreinstellung ist die Netzmaske `0.0.0.0`.
- IP-Adresse des Gateways.
  Diese Eingabe ist ausschließlich dann notwendig, wenn sich das Gerät und die Netz-Management-Station bzw. der TFTP-Server in unterschiedlichen Subnetzen befinden (siehe auf Seite 45 „Beispiel für die Anwendung der Netzmaske”).
  Legen Sie die IP-Adresse des Gateways fest, welches das Subnetz mit dem Gerät vom Pfad zur Netz-Management-Station trennt.
  In der Voreinstellung ist die IP-Adresse `0.0.0.0`.

☐ Speichern Sie die festgelegte Konfiguration durch Verwendung von `copy config running-config nvm`.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network protocol none`	DHCP ausschalten.
`network parms 10.0.1.23 255.255.255.0`	Dem Gerät die IP-Adresse `10.0.1.23` und die Netzmaske `255.255.255.0` zuweisen. Optional können Sie zusätzlich eine Gateway-Adresse zuweisen.
`copy config running-config nvm`	Speichern der aktuellen Einstellungen im „ausgewählten” Konfigurationsprofil im permanenten Speicher (`nvm`).

Nach Eingabe der IP-Parameter können Sie das Gerät über die grafische Benutzeroberfläche komfortabel konfigurieren.

2.2.2 IPv6

Sie können die IPv6-Parameter mit dem Command Line Interface über die serielle Schnittstelle festlegen. 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.

- ☐ Aktivieren Sie das IPv6-Protokoll, falls es deaktiviert 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 IPv4-Adressen verwenden IPv6-Adressen keine Subnetzmaske, um den Netzanteil einer Adresse zu bestimmen. Diese Funktion übernimmt in IPv6 die Präfixlänge (siehe auf Seite 49 „Präfixlänge").
  - Funktion *EUI-Option*
    Mit der Funktion *EUI-Option* können Sie die Interface-ID der IPv6-Adresse automatisch konfigurieren. 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 erzeugen.
    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`	Wechsel in den Privileged-EXEC-Modus.
`network ipv6 operation`	Aktivieren Sie das IPv6-Protokoll, falls es deaktiviert ist. In der Voreinstellung ist das IPv6-Protokoll aktiviert.
`network ipv6 address add 2001::1 64 eui-64`	Zuweisen der IPv6-Adresse `2001::1` und der Präfixlänge `64`. Der Parameter `eui-64` ist optional. Optional können Sie zusätzlich eine Gateway-Adresse zuweisen.
`copy config running-config nvm`	Speichern der aktuellen Einstellungen im „ausgewählten" Konfigurationsprofil im permanenten Speicher (`nvm`).

Nach Eingabe der IPv6-Parameter können Sie das Gerät über die grafische Benutzeroberfläche komfortabel konfigurieren. Für die Verwendung einer IPv6-Adresse in einer URL gilt die folgende URL-Syntax: `https://[<IPv6_Adresse>]`.

2.3 IP-Parameter mit Ethernet Switch Configurator festlegen

Das Ethernet Switch Configurator-Protokoll ermöglicht Ihnen, dem Gerät über das Ethernet IP-Parameter zuzuweisen.

Die anderen Parameter konfigurieren Sie komfortabel über die grafische Benutzeroberfläche.

Installieren Sie die Ethernet Switch Configurator-Software auf Ihrem PC.

Führen Sie die folgenden Schritte aus:
- ☐ Starten Sie das Programm Ethernet Switch Configurator.

Beim Start von Ethernet Switch Configurator untersucht Ethernet Switch Configurator automatisch das Netz nach Geräten, die das Ethernet Switch Configurator-Protokoll unterstützen.

Ethernet Switch Configurator benutzt das erste gefundene Netz-Interface des PCs. Sollte Ihr Rechner über mehrere Netzwerkkarten verfügen, können Sie die gewünschte in der Werkzeugleiste von Ethernet Switch Configurator auswählen.

Ethernet Switch Configurator zeigt eine Zeile für jedes Gerät, das auf eine Ethernet Switch Configurator-Protokoll-Abfrage reagiert.

Ethernet Switch Configurator ermöglicht das Identifizieren der angezeigten Geräte.
- ☐ Wählen Sie eine Gerätezeile aus.
- ☐ Um für das ausgewählte Gerät das Blinken der LEDs einzuschalten, klicken Sie in der Werkzeugleiste die Schaltfläche *Signal*. Um das Blinken auszuschalten, klicken Sie noch einmal die Schaltfläche *Signal*.
- ☐ Mit Doppelklick in eine Zeile öffnen Sie ein Fenster, in welchem Sie den Gerätenamen und die IP-Parameter festlegen.

Anmerkung: Schalten Sie die Funktion Ethernet Switch Configurator im Geräts aus, nachdem Sie dem Gerät die IP-Parameter zugewiesen haben.

Anmerkung: Speichern Sie die Einstellungen, sodass die Eingaben nach einem Neustart wieder zur Verfügung stehen.

2.4 IP-Parameter mit grafischer Benutzeroberfläche festlegen

2.4.1 IPv4

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netz > Global*.

In diesem Dialog legen Sie das VLAN fest, in dem das Management des Geräts erreichbar ist, und konfigurieren den Ethernet Switch Configurator-Zugang.

- ☐ Legen Sie in Spalte *VLAN-ID* das VLAN fest, in welchem das Management des Geräts über das Netz erreichbar ist.

Beachten Sie hierbei, dass das Management des Geräts ausschließlich über Ports erreichbar ist, die Mitglied des betreffenden VLANS sind.

Das Feld *MAC-Adresse* zeigt die MAC-Adresse des Geräts, mit der Sie das Gerät über das Netz erreichen.

- ☐ Legen Sie im Rahmen *Ethernet Switch Configurator Protokoll v1/v2* die Einstellungen für den Zugriff auf das Gerät mit der Ethernet Switch Configurator-Software fest.
- ☐ Das Ethernet Switch Configurator-Protokoll ermöglicht Ihnen, dem Gerät anhand seiner MAC-Adresse eine IP-Adresse zuzuweisen. Aktivieren Sie das Ethernet Switch Configurator-Protokoll, wenn Sie von Ihrem PC aus mit der Ethernet Switch Configurator-Software dem Gerät eine IP-Adresse zuweisen wollen.
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netz > IPv4*.

In diesem Dialog legen Sie fest, aus welcher Quelle das Gerät seine IP-Parameter nach dem Start erhält.

- ☐ Legen Sie im Rahmen *Management-Schnittstelle* zunächst fest, woher das Gerät seine IP-Parameter bezieht:

- ▶ Im Modus `BOOTP` erfolgt die Konfiguration durch einen BOOTP- oder DHCP-Server auf Basis der MAC-Adresse des Geräts.
- ▶ Im Modus `DHCP` erfolgt die Konfiguration durch einen DHCP-Server auf der Basis der MAC-Adresse oder des Namens des Geräts.
- ▶ Im Modus `Lokal` verwendet das Gerät die Netzparameter aus dem internen Gerätespeicher.

Anmerkung: Wenn Sie den Modus für die IP-Adress-Zuweisung ändern, aktiviert das Gerät sofort den neuen Modus, wenn Sie die Schaltfläche ✓ klicken.

- ☐ Fügen Sie im Rahmen *IP-Parameter* die IP-Adresse, die Netzmaske und das Gateway bei Bedarf ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

2.4.2 IPv6

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netz > 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 63 „Erkennung doppelter Adressen").

Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Legen Sie manuell eine IPv6-Adresse fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netz > IPv6*.
- ☐ Klicken Sie die Schaltfläche ⊞.
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Fügen Sie die IPv6-Adresse in das Feld *IP-Adresse* ein.
- ☐ Fügen Sie die Präfixlänge der IPv6-Adresse in das Feld *Prefix-Länge* ein.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Gerät fügt einen neuen Tabelleneintrag 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 > Netz > IPv4* konfigurierte Client-ID. Der BOOTP-Server gibt die Client-ID in eine Datenbank ein und weist eine IP-Adresse zu. Der Server antwortet mit einer Boot-Antwort-Nachricht. Die Boot-Antwort-Nachricht enthält die zugewiesene IP-Adresse.

2.6 IP-Parameter mit DHCP festlegen

2.6.1 IPv4

Das DHCP (Dynamic Host Configuration Protocol) ist eine Weiterentwicklung von BOOTP und hat dieses abgelöst. DHCP ermöglicht zusätzlich die Konfiguration eines DHCP-Clients über einen Namen anstatt über die MAC-Adresse.

Dieser Name heißt bei DHCP nach RFC 2131 „Client Identifier".

Das Gerät verwendet den in der System-Gruppe der MIB II unter sysName festgelegten Namen als Client Identifier. Den Systemnamen können Sie in der grafischen Benutzeroberfläche (siehe Dialog *Grundeinstellungen > System*), im Command Line Interface oder mit SNMP ändern.

Das Gerät übermittelt dem DHCP-Server seinen Systemnamen. Der DHCP-Server verwendet anschließend den Systemnamen für die Zuweisung einer IP-Adresse als Alternative für die MAC-Adresse.

Neben der IP-Adresse überträgt der DHCP-Server
- die Netzmaske
- das Standard-Gateway (falls verfügbar)
- die TFTP-URL der Konfigurationsdatei (falls verfügbar).

Das Gerät wendet die Konfigurationsdaten auf die entsprechenden Parameter an. Wenn der DHCP-Server die IP-Adresse zuweist, speichert das Gerät die Konfigurationsdaten permanent im nichtflüchtigen Speicher.

Tab. 12: DHCP-Optionen, die das Gerät anfordert

Optionen	Bedeutung
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

Der Vorteil beim Einsatz von DHCP gegenüber BOOTP ist, dass der DHCP-Server die Gültigkeit der Konfigurationsparameter (“Lease”) auf eine bestimmte Zeitspanne einschränken kann (sogenannte dynamische Adress-Vergabe). Rechtzeitig vor Ablauf dieser Zeitspanne (“Lease Duration”), kann der DHCP-Client versuchen, dieses Lease zu erneuern. Alternativ kann er ein neues Lease aushandeln. Der DHCP-Server weist dann eine beliebige freie Adresse zu.

Um dies zu umgehen, bieten DHCP-Server die explizite Konfigurationsmöglichkeit, einem bestimmten Client anhand einer eindeutigen Hardware-ID dieselbe IP-Adresse zuzuweisen (sogenannte statische Adressvergabe).

In der Voreinstellung ist DHCP aktiviert. Solange DHCP aktiviert ist, versucht das Gerät, eine IP-Adresse zu bekommen. Findet das Gerät nach einem Neustart keinen DHCP-Server, hat es keine IP-Adresse. Im Dialog *Grundeinstellungen > Netz > IPv4* können Sie DHCP aktivieren oder deaktivieren.

Anmerkung: Vergewissern Sie sich bei Anwendung des Netzmanagements ConneXium Network Manager, 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 entnehmen Sie Ihrem 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 die IPv6-Entsprechung des DHCP-Protokolls für IPv4. Das DHCPv6 Protokoll wird 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 > Netz > 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 > Netz > 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 zur automatischen Konfiguration einer IPv6-Adresse.

In der Voreinstellung ist das Optionsfeld *Auto* ausgewählt. Sie können das Optionsfeld *Auto* im Dialog *Grundeinstellungen > Netz > 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 Starten sowie die Durchführung von regelmäßigen Prüfungen während des Betriebes. Diese Funktion wird im RFC 5227 beschrieben.

Ist die Funktion aktiviert, sendet das Gerät einen SNMP-Trap, der Sie darüber informiert, dass es einen IP-Adresskonflikt erkannt hat.

Die folgende Liste enthält die Voreinstellungen für diese Funktion:
- *Funktion*: `An`
- *Erkennungs-Modus*: `aktiv und passiv`
- *Periodische ARP-Überprüfung senden*: `markiert`
- *Erkennungs-Verzögerung [ms]*: `200`
- *Rückfallverzögerung [s]*: `15`
- *Address-Protections*: `3`
- *Protektions-Intervall [ms]*: `200`
- *Trap senden*: `markiert`

2.7.1 Aktive und passive Erkennung

Durch aktives Prüfen des Netzes wird verhindert, dass das Gerät mit einer doppelten IP-Adresse eine Verbindung mit dem Netz herstellt. Nachdem das Gerät mit dem Netz verbunden oder die IP-Adresse konfiguriert wurde, prüft das Gerät sofort, ob seine IP-Adresse innerhalb des Netzes bereits vorhanden ist. Um zu prüfen, ob Adresskonflikte im Netz vorhanden sind, sendet das Gerät 4 ARP-Probes mit einer Erkennungsverzögerung von 200 ms in das Netz. Wenn die IP-Adresse vorhanden ist, versucht das Gerät, die vorherige Konfiguration wiederherzustellen und nach Ablauf der konfigurierten Verzögerungszeit für die Freigabe eine weitere Prüfung durchzuführen.

Wenn Sie die aktive Erkennung deaktivieren, sendet das Gerät 2 unaufgeforderte ARP-Ankündigungen mit einem Intervall von 2 s. Ist bei der Verwendung von ARP-Ankündigungen die passive Erkennung aktiviert, fragt das Gerät das Netz ab, um zu ermitteln, ob ein Adresskonflikt vorliegt. Nach dem Lösen eines Adresskonfliktes oder nach dem Ablauf der Verzögerungszeit für die Freigabe stellt das Gerät erneut eine Verbindung mit dem Netz her. Nach 10 erkannten Konflikten setzt das Gerät das Verzögerungsintervall für die Freigabe auf 60 s, wenn das konfigurierte Verzögerungsintervall weniger als 60 s beträgt.

Nachdem das Gerät die aktive Erkennung durchgeführt hat oder Sie die Funktion für die aktive Erkennung deaktiviert haben, hört das Gerät mit aktivierter passiver Erkennung das Netzwerk auf Geräte ab, die dieselbe IP-Adresse verwenden. Erkennt das Gerät eine doppelte IP-Adresse, verteidigt es anfangs seine Adresse, indem es den ACD-Mechanismus im Modus für die passive Erkennung anwendet und unaufgeforderte ARP-Ankündigungen übermittelt. Die Anzahl der Schutzmaßnahmen, die das Gerät sendet, sowie das Schutzintervall sind konfigurierbar. Zur Lösung von Konflikten trennt die Netzschnittstelle des lokalen Geräts die Verbindung mit dem Netz, sofern weiterhin eine Verbindung des entfernten Geräts mit dem Netz besteht.

Wenn der DHCP-Server dem Gerät eine IP-Adresse zuweist und dabei ein Adressenkonflikt auftritt, gibt das Gerät eine DHCP-Decline-Nachricht zurück.

Das Gerät verwendet die ARP-Probe-Methode. Diese hat die folgenden Vorteile:
- ARP-Cache-Speicher auf anderen Geräten bleiben unverändert.
- Die Methode bleibt über mehrere ARP-Probe-Übertragungen stabil.

2.8 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 konfiguriert wird oder mit den Methoden *DHCPv6* oder *Auto*. 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 > Netz > 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`)
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network ipv6 dad-transmits <0..5>`	Einstellen der Anzahl von *Neighbor Solicitation*-Nachrichten, die das Gerät sendet. 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).

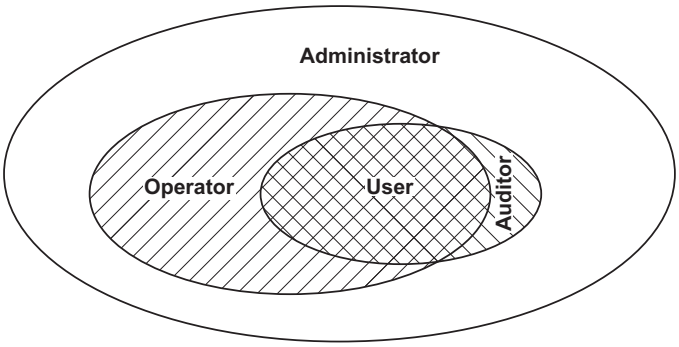
3 Zugriff auf das Gerät

3.1 Berechtigungen

Die Funktionen des Gerätes, die Ihnen als Benutzer zur Verfügung stehen, hängen von Ihrer Berechtigungsstufe ab. Der Funktionsumfang einer Berechtigungsstufe ist für Sie verfügbar, wenn Sie als Benutzer mit dieser Berechtigungsstufe angemeldet sind.

Die Kommandos, die Ihnen als Benutzer zur Verfügung stehen, sind außerdem abhängig vom Modus des Command Line Interface, in welchem Sie sich gerade befinden. Siehe „Modus-basierte Kommando-Hierarchie” auf Seite 25.

Das Gerät bietet Ihnen folgende Berechtigungsstufen:



Tab. 13: Berechtigungsstufen und Umfang der Benutzerrechte

Berechtigungs-stufe	Benutzerrechte
`User`	Mit der Berechtigungsstufe `User` angemeldete Benutzer sind berechtigt, das Gerät zu überwachen.
`Auditor`	Mit der Berechtigungsstufe `Auditor` angemeldete Benutzer sind berechtigt, das Gerät zu überwachen und das Protokoll im Dialog *Diagnose > Bericht > Audit-Trail* zu speichern.
`Operator`	Mit der Berechtigungsstufe `Operator` angemeldete Benutzer sind berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern – mit Ausnahme der Sicherheitseinstellungen für den Zugriff auf das Gerät.
`Administrator`	Mit der Berechtigungsstufe `Administrator` angemeldete Benutzer sind berechtigt, das Gerät zu überwachen und die Einstellungen zu ändern.
`Unauthorized`	Unauthorisierte Benutzer sind gesperrt, das Gerät verweigert die Anmeldung der Benutzer. Weisen Sie diesen Wert zu, um das Benutzerkonto vorübergehend zu sperren. Wenn beim Zuweisen eines anderen Berechtigungsprofils ein Fehler auftritt, weist das Gerät dem Benutzerkonto diese Berechtigung zu.

3.2 Erste Anmeldung (Passwortänderung)

Um unerwünschte Zugriffe auf das Gerät zu verhindern, ist es unerlässlich, dass Sie das voreingestellte Passwort bei der ersten Anmeldung ändern.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie die grafische Benutzeroberfläche, die Anwendung SE View oder das Command Line Interface, wenn Sie sich zum ersten Mal anmelden.
- ☐ Melden Sie sich mit dem voreingestellten Passwort an.
  Das Gerät fordert Sie auf, ein neues Passwort einzugeben.
- ☐ Geben Sie Ihr neues Passwort ein.
  Um die Sicherheit zu erhöhen, wählen Sie ein Passwort mit mindestens 8 Zeichen, das Großbuchstaben, Kleinbuchstaben, numerische Ziffern und Sonderzeichen enthält.
- ☐ Wenn Sie sich mit dem Command Line Interface anmelden, fordert Sie das Gerät auf, Ihr neues Passwort zu bestätigen.
- ☐ Melden Sie sich mit Ihrem neuen Passwort erneut an.

Anmerkung: Wenn Sie Ihr Passwort vergessen haben, dann wenden Sie sich an Ihren lokalen Support.

3.3 Authentifizierungs-Listen

Wenn ein Benutzer über eine bestimmte Verbindung auf das Gerät zugreift, verifiziert das Gerät die Anmeldedaten des Benutzers in einer Authentifizierungs-Liste, die die Richtlinien enthält, die das Gerät für die Authentifizierung anwendet.

Voraussetzung für den Zugriff eines Benutzers auf das Management des Geräts ist, dass der Authentifizierungs-Liste derjenigen Anwendung, über die der Zugriff erfolgt, mindestens eine Richtlinie zugeordnet ist.

3.3.1 Anwendungen

Das Gerät stellt für jede Art von Verbindung, über die jemand auf das Gerät zugreift, eine Anwendung zur Verfügung:
- Zugriff auf das Command Line Interface über eine serielle Verbindung: `Console(V.24)`
- Zugriff auf das Command Line Interface mit SSH: `SSH`
- Zugriff auf das Command Line Interface mit Telnet: `Telnet`
- Zugriff auf die grafische Benutzeroberfläche: `WebInterface`

Außerdem stellt das Gerät eine Anwendung zur Verfügung, um den Zugriff von angeschlossenen Endgeräten auf das Netz mit Port-basierter Zugriffskontrolle zu kontrollieren: `8021x`

3.3.2 Richtlinien

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

Mit der portbasierten Zugriffskontrolle gemäß IEEE 802.1X ermöglicht das Gerät angeschlossenen Endgeräten den Zugriff auf das Netz, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Endgeräte mit folgenden Richtlinien:
- RADIUS
- IAS (Integrated Authentication Server)

Das Gerät bietet Ihnen die Möglichkeit einer Fall-Back-Lösung. Legen Sie hierfür in der Authentifizierungs-Liste mehr als eine Richtlinie fest. Wenn die Authentifizierung mit der aktuellen Richtlinie erfolglos ist, wendet das Gerät die nächste festgelegte Richtlinie an.

3.3.3 Authentifizierungs-Listen verwalten

Die Authentifizierungs-Listen verwalten Sie in der grafischen Benutzeroberfläche oder im Command Line Interface. Führen Sie dazu die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

Der Dialog zeigt die eingerichteten Authentifizierungs-Listen.

`show authlists`	Zeigt die eingerichteten Authentifizierungs-Listen.

☐ Deaktivieren Sie die Authentifizierungs-Liste für diejenigen Anwendungen, über die kein Zugriff auf das Gerät erfolgt, zum Beispiel `8021x`.

☐ Heben Sie in Spalte *Aktiv* der Authentifizierungs-Liste `defaultDot1x8021AuthList` die Markierung des Kontrollkästchens auf.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`authlists disable defaultDot1x8021AuthList`	Deaktiviert die Authentifizierungs-Liste `defaultDot1x8021AuthList`.

3.3.4 Einstellungen anpassen

Beispiel: Richten Sie eine eigenständige Authentifizierungs-Liste für die Anwendung `WebInterface` ein, die per Voreinstellung in der Authentifizierungs-Liste `defaultLoginAuthList` enthalten ist.

Das Gerät leitet Authentifizierungsanfragen an einen RADIUS-Server im Netz weiter. Als Fallback-Lösung authentifiziert das Gerät die Benutzer über die lokale Benutzerverwaltung. Führen Sie dazu die folgenden Schritte aus:

☐ Erzeugen Sie eine Authentifizierungs-Liste `loginGUI`.

☐ Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

☐ Klicken Sie die Schaltfläche .
Der Dialog zeigt das Fenster *Erzeugen*.

☐ Fügen Sie in das Feld *Name* eine aussagekräftige Bezeichnung ein.
Fügen Sie in diesem Beispiel den Namen `loginGUI` ein.

☐ Klicken Sie die Schaltfläche *Ok*.
Das Gerät fügt einen neuen Tabelleneintrag hinzu.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`authlists add loginGUI`	Erzeugt die Authentifizierungs-Liste `loginGUI`.

☐ Wählen Sie die Richtlinien für die Authentifizierungs-Liste `loginGUI`.

☐ Markieren Sie in Spalte *Richtlinie 1* den Wert *radius*.

☐ Markieren Sie in Spalte *Richtlinie 2* den Wert *lokal*.

☐ Wählen Sie in den Spalten *Richtlinie 3* bis *Richtlinie 5* den Wert *reject*, um weiteres Fall-Back zu vermeiden.

☐ Markieren Sie in Spalte *Aktiv* das Kontrollkästchen.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`authlists set-policy loginGUI radius local reject reject reject`	Weist die Richtlinien `radius`, `local` und `reject` der Authentifizierungs-Liste `loginGUI` zu.
`show authlists`	Zeigt die eingerichteten Authentifizierungs-Listen.
`authlists enable loginGUI`	Aktiviert die Authentifizierungs-Liste `loginGUI`.

☐ Weist der Authentifizierungs-Liste `loginGUI` eine Anwendung zu.

- ☐ Markieren Sie im Dialog *Gerätesicherheit > Authentifizierungs-Liste* die Authentifizierungsliste `loginGUI`.
- ☐ Klicken Sie die Schaltfläche und dann den Eintrag *Anwendungen zuordnen*.
  Der Dialog zeigt das Fenster *Anwendungen zuordnen*.
- ☐ Markieren Sie in der linken Spalte die Anwendung `WebInterface`.
- ☐ Klicken Sie die Schaltfläche .
  Die rechte Spalte zeigt jetzt die Anwendung `WebInterface`.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Der Dialog zeigt die aktualisierten Einstellungen:
  - Die Spalte *Zugeordnete Anwendungen* der Authentifizierungs-Liste `loginGUI` zeigt die Anwendung `WebInterface`.
  - Die Spalte *Zugeordnete Anwendungen* der Authentifizierungs-Liste `defaultLoginAuthList` zeigt die Anwendung `WebInterface` nicht mehr.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`show applists`	Zeigt die Anwendungen und die zugewiesenen Listen.
`applists set-authlist WebInterface loginGUI`	Weist die Anwendung `loginGUI` der Authentifizierungs-Liste `WebInterface` zu.

3.4 Benutzerverwaltung

Das Gerät ermöglicht Benutzern den Zugriff auf das Management des Geräts, wenn diese sich mit gültigen Zugangsdaten anmelden. Das Gerät authentifiziert die Benutzer entweder anhand der lokalen Benutzerverwaltung oder mit einem RADIUS-Server im Netz. Damit das Gerät auf die Benutzerverwaltung zurückgreift, weisen Sie einer Authentifizierungsliste die Richtlinie `local` zu, siehe Dialog *Gerätesicherheit > Authentifizierungs-Liste*.

In der lokalen Benutzerverwaltung verwalten Sie die Benutzerkonten. Jedem Benutzer ist in aller Regel jeweils ein Benutzerkonto zugeordnet.

3.4.1 Berechtigungen

Das Gerät ermöglicht Ihnen, durch ein rollenbasiertes Berechtigungsmodell die Zugriffe auf das Management des Geräts differenziert zu steuern. Benutzer, denen ein bestimmtes Berechtigungsprofil zugeordnet ist, sind befugt, Kommandos und Funktionen aus demselben oder einem niedrigeren Berechtigungsprofil anzuwenden.

Das Gerät wendet die Berechtigungsprofile auf jede Anwendung an, mit welcher Zugriffe auf das Management des Geräts möglich sind.

Jedes Benutzerkonto ist mit einer Berechtigung verknüpft, das den Zugriff auf die einzelnen Funktionen des Geräts reguliert. Abhängig von der vorgesehenen Tätigkeit des jeweiligen Benutzers weisen Sie ihm eine vordefinierte Berechtigung zu. Das Gerät unterscheidet die folgenden Berechtigungen.

Tab. 14: Berechtigungen für Benutzerkonten

Rolle	Beschreibung	Autorisiert für folgende Tätigkeiten
Administrator	Der Benutzer ist berechtigt, das Gerät zu überwachen und zu administrieren.	Sämtliche Tätigkeiten mit Lese-/Schreibzugriff einschließlich der folgenden, einem Administrator vorbehaltenen Tätigkeiten: ▶ Benutzerkonten hinzufügen, ändern und löschen ▶ Benutzerkonten aktivieren, deaktivieren und entsperren ▶ Jedes Passwort ändern ▶ Passwort-Management konfigurieren ▶ Systemzeit einstellen und ändern ▶ Dateien auf das Gerät laden, zum Beispiel Gerätekonfigurationen, Zertifikate oder Software-Images ▶ Einstellungen und sicherheitsbezogene Einstellungen auf den Lieferzustand zurücksetzen ▶ RADIUS-Server und Authentifizierungslisten konfigurieren ▶ Skripte anwenden mit dem Command Line Interface ▶ CLI-Logging und SNMP-Logging ein- und ausschalten ▶ Externen Speicher aktivieren und deaktivieren ▶ System-Monitor aktivieren und deaktivieren ▶ Dienste für den Zugriff auf das Management des Geräts (zum Beispiel SNMP) ein- und ausschalten. ▶ Zugriffsbeschränkungen auf die grafische Benutzeroberfläche oder das Command Line Interface auf Basis der IP-Adresse konfigurieren
Operator	Der Benutzer ist berechtigt, das Gerät zu überwachen und zu konfigurieren – mit Ausnahme sicherheitsbezogener Einstellungen.	Sämtliche Tätigkeiten mit Lese-/Schreibzugriff mit Ausnahme der o.g. Tätigkeiten, die ausschließlich einem Administrator vorbehalten sind.

Tab. 14: Berechtigungen für Benutzerkonten (Forts

Rolle	Beschreibung	Autorisiert für folgende Tätigkeiten
Auditor	Der Benutzer ist berechtigt, das Gerät zu überwachen und das Protokoll im Dialog *Diagnose > Bericht > Audit-Trail* zu speichern.	Überwachende Tätigkeiten mit Lesezugriff.
Guest	Der Benutzer ist berechtigt, das Gerät zu überwachen – mit Ausnahme sicherheitsbezogener Einstellungen.	Überwachende Tätigkeiten mit Lesezugriff.
Unauthorized	Kein Zugriff auf das Gerät möglich. ▶ Als Administrator weisen Sie diese Berechtigung zu, um ein Benutzerkonto vorübergehend zu sperren. ▶ Wenn beim Zuweisen einer anderen Berechtigung ein Fehler erkannt wird, dann weist das Gerät dem Benutzerkonto diese Berechtigung zu.	Keine erlaubten Tätigkeiten.

3.4.2 Benutzerkonten verwalten

Die Benutzerkonten verwalten Sie in der grafischen Benutzeroberfläche oder im Command Line Interface. Führen Sie dazu die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.

Der Dialog zeigt die eingerichteten Benutzerkonten.

`show users`	Zeigt die eingerichteten Benutzerkonten.

3.4.3 Voreinstellung

Im Lieferzustand sind die Benutzerkonten `admin` und `user` im Gerät eingerichtet.

Tab. 15: Voreinstellungen der werkseitig eingerichteten Benutzerkonten

Parameter	Voreinstellung	
Benutzername	`admin`	`user`
Passwort	`private`	`public`
Rolle	`administrator`	`guest`
Benutzer gesperrt	`unmarkiert`	`unmarkiert`
Richtlinien überprüfen	`unmarkiert`	`unmarkiert`
SNMP-Authentifizierung	`hmacmd5`	`hmacmd5`
SNMP-Verschlüsselung	`des`	`des`

Ändern Sie das Passwort des Benutzerkontos `admin`, bevor Sie das Gerät im Netz zugänglich machen.

3.4.4 Voreingestellte Passwörter ändern

Um ungewünschte Eingriffe zu vermeiden, ändern Sie das Passwort der voreingestellten Benutzerkonten. Führen Sie dazu die folgenden Schritte aus:

☐ Ändern Sie das Passwort für die Benutzerkonten `admin` und `user`.

☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.

Der Dialog zeigt die eingerichteten Benutzerkonten.

☐ Um eine höhere Komplexität des Passwortes zu erzielen, markieren Sie das Kontrollkästchen in Spalte *Richtlinien überprüfen*.
Das Gerät prüft das Passwort vor dem Speichern anhand der im Rahmen *Passwort-Richtlinien* festgelegten Richtlinien.

Anmerkung: Das Prüfen des Passworts führt möglicherweise zu einer Meldung im Dialog *Grundeinstellungen > System*, Rahmen *Sicherheits-Status*. Die Einstellungen, die zu dieser Meldung führen, legen Sie fest im Dialog *Grundeinstellungen > System*.

☐ Klicken Sie in der Zeile des betreffenden Benutzerkontos in das Feld *Passwort*. Fügen Sie das Passwort mit mindestens 6 Zeichen ein.
Erlaubt sind bis zu 64 alphanumerische Zeichen.
- Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
- Die Mindestlänge des Passworts ist im Rahmen *Konfiguration* festgelegt. Das Gerät prüft stets die Mindestlänge des Passworts.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`users password-policy-check <user> enable`	Aktiviert für das Benutzerkonto `<user>` das Prüfen des Passwortes anhand der festgelegten Richtlinien. Damit erzielen Sie eine höhere Komplexität des Passwortes.

Anmerkung: Das Prüfen des Passworts führt möglicherweise zu einer Meldung, wenn Sie den Sicherheitsstatus anzeigen (`show security-status all`). Die Einstellungen, die zu dieser Meldung führen, legen Sie fest mit dem Kommando `security-status monitor pwd-policy-inactive`.

`users password <user> SECRET`	Legt für das Benutzerkonto `<user>` das Passwort `SECRET` fest. Fügen Sie mindestens 6 Zeichen ein.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

3.4.5 Neues Benutzerkonto einrichten

Weisen Sie Benutzern, die auf das Management des Geräts zugreifen, jeweils ein eigenes Benutzerkonto zu. Auf diese Weise haben Sie die Möglichkeit, die Berechtigungen für die Zugriffe differenziert zu steuern.

Im folgenden Beispiel werden wir das Benutzerkonto für einen Benutzer `USER` mit der Rolle `operator` einrichten. Benutzer mit der Rolle `operator` sind berechtigt, das Gerät zu überwachen und zu konfigurieren – mit Ausnahme sicherheitsbezogener Einstellungen. Führen Sie dazu die folgenden Schritte aus:

☐ Erzeugen Sie ein neues Benutzerkonto.

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Fügen Sie in das Feld *Benutzername* die Bezeichnung ein.
  In diesem Beispiel geben wir dem Benutzerkonto die Bezeichnung `USER`.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Um eine höhere Komplexität des Passwortes zu erzielen, markieren Sie das Kontrollkästchen in Spalte *Richtlinien überprüfen*.
  Das Gerät prüft das Passwort vor dem Speichern anhand der im Rahmen *Passwort-Richtlinien* festgelegten Richtlinien.
- ☐ Fügen Sie in das Feld *Passwort* das Passwort mit mindestens 6 Zeichen ein.
  Erlaubt sind bis zu 64 alphanumerische Zeichen.
  - ▶ Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
  - ▶ Die Mindestlänge des Passworts ist im Rahmen *Konfiguration* festgelegt. Das Gerät prüft stets die Mindestlänge des Passworts.
- ☐ Wählen Sie in Spalte *Rolle* die Benutzer-Rolle.
  In diesem Beispiel wählen wir den Wert `operator`.
- ☐ Um das Benutzerkonto zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .
  Der Dialog zeigt die eingerichteten Benutzerkonten.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`users add USER`	Erzeugt das Benutzerkonto `USER`.
`users password-policy-check USER enable`	Aktiviert für das Benutzerkonto `USER` das Prüfen des Passwortes anhand der festgelegten Richtlinien. Damit erzielen Sie eine höhere Komplexität des Passwortes.

`users password USER SECRET`	Legt für das Benutzerkonto `USER` das Passwort `SECRET` fest. Fügen Sie mindestens 6 Zeichen ein.
`users access-role USER  operator`	Weist die Rolle `operator` dem Benutzerkonto `USER` zu.
`users enable USER`	Aktiviert das Benutzerkonto `USER`.
`show users`	Zeigt die eingerichteten Benutzerkonten.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

Anmerkung: Denken Sie daran, das Passwort zuzuweisen, wenn Sie ein neues Benutzerkonto im Command Line Interface einrichten.

3.4.6 Benutzerkonto deaktivieren

Nach Deaktivieren eines Benutzerkontos verweigert das Gerät Zugriffe des zugehörigen Benutzers auf das Management des Geräts. Im Gegensatz zum vollständigen Löschen ermöglicht Ihnen das Deaktivieren, die Einstellungen des Benutzerkontos für eine künftige Wiederverwendung beizubehalten. Führen Sie dazu die folgenden Schritte aus:

☐ Um die Einstellungen des Benutzerkontos für eine künftige Wiederverwendung beizubehalten, deaktivieren Sie das Benutzerkonto temporär.

☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.
Der Dialog zeigt die eingerichteten Benutzerkonten.

☐ Heben Sie in der Zeile des betreffenden Benutzerkontos die Markierung des Kontrollkästchens *Aktiv* auf.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`users disable <user>`	Deaktivieren eines Benutzerkontos.
`show users`	Zeigt die eingerichteten Benutzerkonten.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

☐ Um die Einstellungen des Benutzerkontos dauerhaft zu deaktivieren, löschen Sie das Benutzerkonto.

☐ Markieren Sie die Zeile des betreffenden Benutzerkontos.

☐ Klicken Sie die Schaltfläche  .

`users delete <user>`	Löscht das Benutzerkonto `<user>`.
`show users`	Zeigt die eingerichteten Benutzerkonten.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

3.4.7 Richtlinien für Passwörter anpassen

Das Gerät ermöglicht Ihnen, die Passwörter der Benutzerkonten auf Einhaltung vorgegebener Richtlinien zu prüfen. Durch Einhaltung der Richtlinien erzielen Sie Passwörter mit höherer Komplexität.

Die Benutzerverwaltung des Geräts ermöglicht Ihnen, die Prüfung in jedem Benutzerkonto individuell ein- oder auszuschalten. Bei eingeschalteter Prüfung akzeptiert das Gerät ein geändertes Passwort, wenn es die Anforderungen der Richtlinien erfüllt.

Im Lieferzustand sind praxistaugliche Werte für die Richtlinien im Gerät eingerichtet. Sie haben die Möglichkeit, die Richtlinien an Ihre Erfordernisse anzupassen. Führen Sie dazu die folgenden Schritte aus:

☐ Passen Sie die Richtlinien für Passwörter an Ihre Erfordernisse an.

☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.

Im Rahmen *Konfiguration* legen Sie fest, wie viele Login-Versuche das Gerät zulässt, bevor es den Benutzer sperrt. Sie legen ebenfalls die Mindestanzahl von Zeichen fest, aus denen ein Passwort besteht.

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

Die Anzahl der Login-Versuche sowie die mögliche Sperre des Benutzers beziehen sich ausschließlich auf den Zugriff auf das Management des Geräts über:

- die grafische Benutzeroberfläche
- das SSH-Protokoll
- das Telnet-Protokoll

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

☐ Legen Sie die Werte entsprechend Ihren Anforderungen fest.

- Die Anzahl der Login-Versuche eines Benutzers legen Sie fest im Feld *Login-Versuche* fest. Das Feld ermöglicht Ihnen, diesen Wert im Bereich `0..5` festzulegen.
  Im obigen Beispiel deaktiviert der Wert `0` die Funktion.
- Das Feld *Min. Passwort-Länge* ermöglicht Ihnen, Werte im Bereich `1..64` einzufügen.

Der Dialog zeigt im Rahmen *Passwort-Richtlinien* die eingerichteten Richtlinien.

☐ Passen Sie die Werte an Ihre Erfordernisse an.

- Erlaubt sind Werte im Bereich `1` bis `16`.
  Der Wert `0` deaktiviert die betreffende Richtlinie.

Um die in den Rahmen *Konfiguration* und *Passwort-Richtlinien* festgelegten Einträge anzuwenden, markieren Sie das Kontrollkästchen in Spalte *Richtlinien überprüfen* für einen bestimmten Benutzer.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`passwords min-length 6`	Legt die Richtlinie für die Mindestlänge des Passworts fest.
`passwords min-lowercase-chars 1`	Legt die Richtlinie für die Mindestanzahl von Kleinbuchstaben im Passwort fest.
`passwords min-numeric-chars 1`	Legt die Richtlinie für die Mindestanzahl von Ziffern im Passwort fest.

`passwords min-special-chars 1`	Legt die Richtlinie für die Mindestanzahl von Sonderzeichen im Passwort fest.
`passwords min-uppercase-chars 1`	Legt die Richtlinie für die Mindestanzahl von Großbuchstaben im Passwort fest.
`show passwords`	Zeigt die eingerichteten Richtlinien.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

3.5 LDAP

Server-Administratoren verwalten Active Directorys, die Benutzeranmelde-Informationen für in Büroumgebungen eingesetzte Anwendungen enthalten. Ein Active Directory weist eine hierarchische Struktur auf und enthält Benutzernamen, Passwörter und die autorisierten Berechtigungsstufen mit Lese-/Schreibrechten für die einzelnen Benutzer.

Um Benutzeranmeldeinformationen und Berechtigungsstufen aus einem Active Directory abzurufen, verwendet das Gerät das Lightweight Directory Access Protocol (LDAP). Dies ermöglicht das „Single Sign-On“ (einmalige Anmeldung) für Geräte im Netz. Das Abrufen der Anmeldedaten aus einem Active Directory ermöglicht dem Benutzer, sich mit denselben Anmeldedaten anzumelden, die in der Büroumgebung verwendet werden.

Eine LDAP-Sitzung beginnt damit, dass das Gerät den Directory System Agent (DSA) kontaktiert, um das Active Directory eines LDAP-Servers zu durchsuchen. Findet der Server für einen Benutzer mehrere Einträge im Active Directory, sendet der Server die höhere ermittelte Berechtigungsstufe. Der DSA lauscht nach Informationsanforderungen und sendet Antworten für LDAP über TCP-Port `389` oder für LDAP über SSL (LDAPS) über TCP-Port `636`. Clients und Server kodieren LDAPS-Anfragen und -Antworten mittels der Basic Encoding Rules (BER). Das Gerät öffnet für jede Anfrage eine neue Verbindung und schließt die Verbindung, nachdem das Gerät eine Antwort vom Server empfangen hat.

Das Gerät ermöglicht Ihnen, ein CA-Zertifikat zur Validierung des Servers für SSL- (Secure Socket Layer) und TLS-Sitzungen (Transport Layer Security) hochzuladen. Hierbei ist das Zertifikat für TLS-Sitzungen optional.

Das Gerät ist in der Lage, Anmeldedaten für bis zu 1024 Benutzer im Speicher zwischenzuspeichern. Sind die Active-Directory-Server nicht erreichbar, können sich die Benutzer weiterhin über ihre Büro-Anmeldedaten anmelden.

3.5.1 Abstimmung mit dem Server-Administrator

Die Konfiguration der Funktion *LDAP* erfordert, dass der Netzadministrator die folgenden Informationen vom Server-Administrator anfordert:

- Server-Name oder IP-Adresse
- Ort, an dem sich das Active Directory auf dem Server befindet
- Verwendeter Verbindungstyp
- TCP-Überwachungs-Port
- Falls erforderlich, Speicherort des Zertifikats
- Name des Attributs, das den Benutzeranmeldenamen enthält
- Namen der Attribute, welche die Benutzerberechtigungsstufen enthalten

Der Server-Administrator kann Berechtigungsstufen individuell mit einem Attribut wie `description` oder einer Gruppe mit dem Attribut `memberOf` zuweisen. Im Dialog *Gerätesicherheit > LDAP > Rollen-Zuweisung* legen Sie fest, welche Attribute die verschiedenen Berechtigungsstufen erhalten.

Sie haben außerdem die Möglichkeit, über einen LDAP-Browser wie JXplorer oder Softerra die Namen der Attribute abzurufen, die den Benutzeranmeldenamen und die Berechtigungsstufen enthalten.

3.5.2 Beispiel-Konfiguration

Das Gerät ist in der Lage, eine verschlüsselte Verbindung zu einem lokalen Server ausschließlich über den Server-Namen oder zu einem Server in einem anderen Netz über eine IP-Adresse herzustellen. Der Server-Administrator verwendet Attribute zur Identifizierung der Anmeldedaten eines Benutzers und für die Zuordnung von individuellen Berechtigungsstufen und Gruppenberechtigungsstufen.

Legen Sie anhand der vom Server-Administrator erhaltenen Informationen fest, welche Attribute im Active Directory die Benutzer-Anmeldedaten und die Berechtigungsstufe enthalten. Das Gerät vergleicht anschließend die Benutzer-Anmeldedaten mit den auf dem Gerät festgelegten Berechtigungsstufen und ermöglicht dem Benutzer die Anmeldung mit der zugewiesenen Berechtigungsstufe.

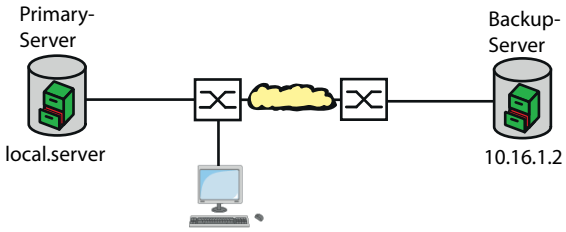


Abb. 18: Beispiel für eine LDAP-Konfiguration

In diesem Beispiel hat der Server-Administrator die folgenden Informationen gesendet:

Information	Primary Server	Backup Server
Server-Name oder IP-Adresse	`local.server`	`10.16.1.2`
Ort, an dem sich das Active Directory auf dem Server befindet	`Land/Stadt/Benutzer`	`Land/Unternehmen/Benutzer`
Verwendeter Verbindungstyp	`TLS` (mit Zertifikat)	`SSL`
Der Server-Administrator hat das CA-Zertifikat in einer E-Mail gesendet.	Lokal gespeichertes CA-Zertifikat für den primären Server	Lokal gespeichertes CA-Zertifikat für den Backup-Server
TCP-Überwachungs-Port	`389 (tls)`	`636 (ssl)`
Name des Attributs, das den Benutzernamen enthält	`userPrincipalName`	`userPrincipalName`
Namen der Attribute, welche die Benutzerberechtigungsstufen enthalten	`OPERATOR` `ADMINISTRATOR`	`OPERATOR` `ADMINISTRATOR`

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Authentifizierungs-Liste*.
- ☐ Um das Gerät so zu konfigurieren, dass es bei der Anmeldung über die grafische Benutzeroberfläche die Benutzer-Anmeldedaten zuerst aus dem Active Directory abruft, legen Sie für die Liste `defaultLoginAuthList` in Spalte *Richtlinie 1* den Wert `ldap` fest.
- ☐ Öffnen Sie den Dialog *Gerätesicherheit > LDAP > Konfiguration*.

- ☐ Das Gerät ermöglicht Ihnen festzulegen, über welchen Zeitraum das Gerät die Benutzer-Anmeldedaten im Cache speichert. Um Benutzer-Anmeldedaten für einen Tag im Cache zu speichern, legen Sie im Rahmen *Konfiguration*, Feld *Client-Cache-Timeout [min]* den Wert `1440` fest.
- ☐ Der Eintrag *Bind-Benutzer* ist optional. Wenn festgelegt, fügen Benutzer ihren Benutzernamen ein, um sich anzumelden. Der Dienstbenutzer kann jede Person mit Anmeldedaten sein, die im Active Directory unter dem in Spalte *Benutzername-Attribut* festgelegten Attribut aufgeführt sind. Legen Sie in Spalte *Bind-Benutzer* den Benutzernamen und die Domäne fest.
- ☐ Der *Base DN* ist eine Kombination der Domänenkomponente (DC) und der Organisationseinheit (OU). Der *Base DN* ermöglicht dem Gerät, einen Server in einer Domäne (DC) zu orten und das Active Directory (OU) ausfindig zu machen. Legen Sie den Speicherort des Active Directory fest. Legen Sie in Spalte *Base DN* den Wert `ou=Users,ou=City,ou=Country,dc=server,dc=local` fest.
- ☐ Um das Attribut festzulegen, unter dem der Server-Administrator die Benutzer aufführt, legen Sie in Spalte *Benutzername-Attribut* den Wert `userPrincipalName` fest.

Das Gerät verwendet zur Verifizierung des Servers ein CA-Zertifikat.

- ☐ Befindet sich das Zertifikat auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie das Zertifikat in den -Bereich. Alternativ klicken Sie in den Bereich, um das Zertifikat auszuwählen.
- ☐ Um das CA-Zertifikat auf das Gerät zu übertragen, klicken Sie die Schaltfläche *Start*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Um eine Beschreibung festzulegen, fügen Sie in Spalte *Beschreibung* den Wert `Primary AD Server` ein.
- ☐ Um den Server-Namen und die Domäne des primären Servers festzulegen, fügen Sie in Spalte *Adresse* den Wert `local.server` ein.
- ☐ Der primäre Server verwendet für die Kommunikation den TCP-Port `389`, welches der voreingestellte Wert für *Ziel-TCP-Port* ist.
- ☐ Der primäre Server verwendet TLS für die Verschlüsselung der Kommunikation und ein CA-Zertifikat für die Server-Validierung. Legen Sie in Spalte *Verbindungssicherheit* den Wert `startTLS` fest.
- ☐ Um den Eintrag zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Fügen Sie eine weitere Zeile hinzu, die Sie mit den vom Server-Administrator für den Backup-Server empfangenen Dateien konfigurieren und aktivieren.

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > LDAP > Rollen-Zuweisung*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .

Wenn ein Benutzer sich mit konfiguriertem und aktiviertem LDAP anmeldet, sucht das Gerät im Active Directory nach den Anmeldedaten des Benutzers. Wenn das Gerät feststellt, dass Benutzername und Passwort korrekt sind, sucht das Gerät nach dem Wert, den Sie in die Spalte *Typ* festgelegt haben. Wenn das Gerät das Attribut findet und der Text in Spalte *Parameter* mit dem Text im Active Directory übereinstimmt, ermöglicht das Gerät dem Benutzer die Anmeldung mit der zugewiesenen Berechtigungsstufe. Wenn der Wert `attribute` in Spalte *Typ* festgelegt ist, legen Sie den Wert in Spalte *Parameter* in der folgenden Form fest: `attributeName=attributeValue`.

- ☐ Um die Benutzer-Rolle festzulegen, legen Sie in Spalte *Rolle* den Wert `operator` fest.
- ☐ Um den Eintrag zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.

- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
  Fügen Sie die vom Server-Administrator erhaltenen Werte für die Rolle `administrator` ein.
  Um den Eintrag zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Öffnen Sie den Dialog *Gerätesicherheit > LDAP > Konfiguration*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.

Die folgende Tabelle beschreibt die Vorgehensweise zum Konfigurieren der Funktion *LDAP* auf dem Gerät mit dem Command Line Interface. Die Tabelle zeigt die Kommandos für `Index 1`. Um `Index 2` zu konfigurieren, verwenden Sie dieselben Kommandos und ersetzen die entsprechenden Informationen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ldap cache-timeout 1440`	Legen Sie fest, dass das Gerät den permanenten Speicher nach einem Tag leert.
`ldap client server add 1 local.server port 389`	Fügen Sie eine Verbindung zum Remote-Authentifizierungs-Client-Server mit dem Host-Namen `local.server` und UDP-Port `389` hinzu.
`ldap client server modify 1 security startTLS`	Legen Sie den Sicherheitstyp für die Verbindung fest.
`ldap client server modify 1 description Primary_AD_Server`	Legen Sie den Konfigurationsnamen für den Eintrag fest.
`ldap basedn ou=Users,ou=City,ou=Country,dc=server,dc=local`	Legen Sie den Basisdomänennamen fest, der zur Ermittlung des Active Directory auf dem Server verwendet wird.
`ldap search-attr userPrincipalName`	Legen Sie das Attribut fest, nach dem in dem Active Directory, das die Anmeldedaten der Benutzer enthält, gesucht wird.
`ldap bind-user user@company.com`	Legen Sie den Namen und die Domäne des Bind-Account-Benutzers fest.
`ldap bind-passwd Ur-123456`	Legen Sie das Password des Bind-Account-Benutzers fest..
`ldap client server enable 1`	Aktivieren Sie die Remote-Authentifizierungs-Client-Server-Verbindung.
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	Fügen Sie für die Rolle `Operator` einen Eintrag zur Zuordnung der Remote-Authentifizierungsrolle hinzu. Ordnen Sie die Rolle`operator` dem Attribut zu, welches das Wort `OPERATOR` enthält.
`ldap mapping enable 1`	Aktivieren Sie den Eintrag für die Remote-Zuordnung von Authentifizierungsrollen.
`ldap operation`	Aktivieren Sie die Funktion für die Remote-Authentifizierung.

3.6 SNMP-Zugriff

Das Protokoll SNMP ermöglicht Ihnen, mit einem Netzmanagementsystem das Gerät über das Netz zu überwachen und seine Einstellungen zu ändern.

3.6.1 SNMPv1/v2-Zugriff

Mit SNMPv1 oder SNMPv2 kommunizieren das Netzmanagementsystem und das Gerät unverschlüsselt. Jedes SNMP-Paket enthält den Community-Namen im Klartext und die IP-Adresse des Absenders.

Im Gerät voreingestellt sind die Community-Namen `user` für Lese-Zugriffe und `admin` für Schreib-Zugriffe. Wenn SNMPv1/v2 eingeschaltet ist, erlaubt das Gerät jedem, der den Community-Namen kennt, den Zugriff auf das Gerät.

Erschweren Sie unerwünschten Zugriff auf das Gerät. Führen Sie dazu die folgenden Schritte aus:

- ☐ Ändern Sie im Gerät die voreingestellten Community-Namen.
  Behandeln Sie die Community-Namen vertraulich.
  Jeder, der den Community-Namen für Schreibzugriffe kennt, hat die Möglichkeit, die Einstellungen des Geräts zu ändern.
- ☐ Legen Sie für Lese-/Schreibzugriffe einen anderen Community-Namen fest als für Lesezugriffe.
- ☐ Verwenden Sie SNMPv1 oder SNMPv2 ausschließlich in abhörsicheren Umgebungen. Die Protokolle verwenden keine Verschlüsselung.
- ☐ Wir empfehlen, SNMPv3 zu nutzen und im Gerät den Zugriff über SNMPv1 und SNMPv2 auszuschalten.

3.6.2 SNMPv3-Zugriff

Mit SNMPv3 kommunizieren das Netzmanagementsystem und das Gerät verschlüsselt. Das Netzmanagementsystem authentifiziert sich gegenüber dem Gerät mit den Anmeldedaten eines Benutzers. Voraussetzung für den SNMPv3-Zugriff ist, dass im Netzmanagementsystem dieselben Einstellungen wie im Gerät festgelegt sind.

Das Gerät ermöglicht Ihnen, für jedes Benutzerkonto die Parameter *SNMP-Authentifizierung* und *SNMP-Verschlüsselung* individuell festzulegen.

Wenn Sie im Gerät ein neues Benutzerkonto einrichten, sind die Parameter so voreingestellt, dass das Netzmanagementsystem ConneXium Network Manager das Gerät damit sofort erreicht.

Die im Gerät eingerichteten Benutzerkonten verwenden in der grafischen Benutzeroberfläche, im Command Line Interface (CLI) und für SNMPv3 dieselben Passwörter.

Um die SNMPv3-Parameter des Benutzerkontos an die Einstellungen in Ihrem Netzmanagementsystem anzupassen, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Benutzerverwaltung*.

Der Dialog zeigt die eingerichteten Benutzerkonten.

- ☐ Klicken Sie in der Zeile des betreffenden Benutzerkontos in das Feld *SNMP-Authentifizierung*. Wählen Sie die gewünschte Einstellung.
- ☐ Klicken Sie in der Zeile des betreffenden Benutzerkontos in das Feld *SNMP-Verschlüsselung*. Wählen Sie die gewünschte Einstellung.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`users snmpv3 authentication <user> md5 | sha1`	Protokoll HMAC-MD5 oder HMAC-SHA dem Benutzerkonto `<user>` für Authentifizierungsanfragen zuweisen.
`users snmpv3 encryption <user> des | aescfb128 | none`	Algorithmus DES oder AES-128 dem Benutzerkonto `<user>` zuweisen. Mit dem Algorithmus verschlüsselt das Gerät Authentifizierungsanfragen. Der Wert `none` hebt die Verschlüsselung auf.
`show users`	Eingerichtete Benutzerkonten anzeigen.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

3.7 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* `91.0.0.100`
- *Netzmaske* `255.255.255.0`

Das Gerät ermöglicht Ihnen mit den folgenden Protokollen den Zugriff auf das Management des Geräts:

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

3.7.1 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 `91.0.0.101`). 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*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

```
enable
```
Wechsel in den Privileged-EXEC-Modus.

```
network usb parms 192.168.1.1
255.255.255.0
```
Festlegen der IP-Adresse `192.168.1.1` und der Netzmaske `255.255.255.0` für die USB-Netzschnittstelle.

```
show network usb
```
Anzeigen der Einstellungen der USB-Netzschnittstelle.

```
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
```
Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

3.7.2 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*.
- ☐ Um die USB-Netzschnittstelle auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

```
enable
```
Wechsel in den Privileged-EXEC-Modus.

```
no network usb operation
```
Ausschalten der USB-Netzschnittstelle

```
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
```
Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

4 Die Systemzeit im Netz synchronisieren

Viele Anwendungen sind auf eine möglichst korrekte Zeit angewiesen. Die notwendige Genauigkeit, also die zulässige Abweichung zur Echtzeit, ist abhängig vom Anwendungsgebiet.

Anwendungsgebiete sind beispielsweise:
- Logbucheinträge
- Produktionsdaten mit Zeitstempel versehen
- Prozesssteuerung

Das Gerät ermöglicht Ihnen, die Zeit im Netz mit den folgenden Optionen zu synchronisieren:
- Das Simple Network Time Protocol (SNTP) ist eine einfache Lösung für geringere Genauigkeitsanforderungen. Unter idealen Bedingungen erzielt SNTP eine Genauigkeit im Millisekunden-Bereich. Die Genauigkeit ist abhängig von der Signallaufzeit.
- IEEE 1588 mit dem Precision Time Protocol (PTP) erreicht eine Genauigkeit im Submikrosekunden-Bereich. Diese Methode eignet sich auch für anspruchsvolle Anwendungen bis hin zur Prozesssteuerung.

PTP ist die bessere Wahl, wenn die beteiligten Geräte dieses Protokoll unterstützen. PTP ist exakter, verfügt über fortgeschrittene Methoden zur Fehlerkorrektur und verursacht eine geringe Netzlast. Die Implementation von PTP ist vergleichsweise einfach.

Anmerkung: Laut PTP- und SNTP-Standard funktionieren beide Protokolle parallel in einem Netz. Da beide Protokolle die Systemzeit des Geräts beeinflussen, sind Situationen denkbar, in denen beide Protokolle konkurrieren.

4.1 Grundeinstellungen

Im Dialog *Zeit > Grundeinstellungen* legen Sie allgemeine Einstellungen für die Zeit fest.

4.1.1 Uhrzeit einstellen

Steht Ihnen keine Referenzzeitquelle zur Verfügung, haben Sie die Möglichkeit, im Gerät die Uhrzeit einzustellen.

Sofern keine Echtzeituhr vorhanden ist oder diese eine ungültige Zeit übermittelt, initialisiert das Gerät nach einem Kalt- oder Neustart seine Uhr auf den 1. Januar, 00:00 Uhr. Nach Ausschalten des Netzteils puffert das Gerät die Einstellungen der Echtzeituhr bis zu 24 Stunden lang.

Alternativ legen Sie die Einstellungen im Gerät so fest, dass es die aktuelle Uhrzeit automatisch von einer PTP-Uhr oder von einem SNTP-Server bezieht.

Alternativ legen Sie die Einstellungen im Gerät so fest, dass es die aktuelle Uhrzeit automatisch von einem SNTP-Server bezieht.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Zeit > Grundeinstellungen*.
- ▶ Das Feld *Systemzeit (UTC)* zeigt die aktuelle UTC (Universal Time Coordinated) des Geräts. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die UTC ist weltweit gleich und berücksichtigt keine lokalen Zeitverschiebungen.
- ▶ Die Zeit im Feld *Systemzeit* ergibt sich aus der *Systemzeit (UTC)* zuzüglich dem Wert *Lokaler Offset [min]* sowie einer möglichen Verschiebung durch die Sommerzeit.

Anmerkung: PTP sendet die Internationale Atomzeit (TAI). Mit Stand vom 1. Juli 2020 geht die TAI-Zeit 37 s gegenüber der UTC-Zeit vor. Wenn auf der PTP-Referenzzeitquelle der UTC-Offset korrekt festgelegt ist, korrigiert das Gerät diesen Unterschied bei der Anzeige im Feld *Systemzeit (UTC)* automatisch.

- ☐ Damit das Gerät die Zeit Ihres PCs in das Feld *Systemzeit* übernimmt, klicken Sie die Schaltfläche *Setze Zeit vom PC*.
  Anhand des Werts im Feld *Lokaler Offset [min]* berechnet das Gerät die Zeit im Feld *Systemzeit (UTC)*: Die Zeit im Feld *Systemzeit (UTC)* ergibt sich aus der *Systemzeit* abzüglich dem Wert *Lokaler Offset [min]* sowie einer möglichen Verschiebung durch die Sommerzeit.
- ▶ Das Feld *Quelle der Zeit* zeigt den Ursprung der Zeitangabe. Das Gerät wählt automatisch die Quelle mit der höchsten Genauigkeit.
  Die Quelle ist zunächst `local`.
  Ist SNTP aktiviert und empfängt das Gerät ein gültiges SNTP-Paket, setzt es seine Zeitquelle auf `sntp`.
  Ist PTP aktiviert und empfängt das Gerät eine gültige PTP-Nachricht, setzt es seine Zeitquelle auf `ptp`. Das Gerät gibt der Zeitquelle PTP den Vorrang vor SNTP.
- ▶ Der Wert *Lokaler Offset [min]* legt die Zeitdifferenz fest zwischen der lokalen Zeit und der *Systemzeit (UTC)*.
- ☐ Damit das Gerät die Zeitzone Ihres PCs ermittelt, klicken Sie die Schaltfläche *Setze Zeit vom PC*. Das Gerät berechnet daraus die lokale Zeitdifferenz zur UTC-Zeit und trägt die Differenz in das Feld *Lokaler Offset [min]* ein.

Anmerkung: Das Gerät bietet die Möglichkeit, den lokalen Offset von einem DHCP-Server beziehen.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`clock set <YYYY-MM-DD> <HH:MM:SS>`	Einstellen der Systemzeit des Geräts.
`clock timezone offset <-780..840>`	Eingabe der Zeitdifferenz zwischen der lokalen Zeit und der empfangenen UTC-Zeit in Minuten.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

4.1.2 Automatische Sommerzeitumschaltung

Wenn Sie das Gerät in einer Zeitzone betreiben, in der es die Sommerzeitumstellung gibt, richten Sie auf der Registerkarte *Sommerzeit* die automatische Zeitumstellung ein.

Wenn die Sommerzeitumschaltung aktiviert ist, erhöht das Gerät zu Beginn der Sommerzeit die lokale Systemzeit um 1 Stunde. Zum Ende der Sommerzeit reduziert das Gerät die lokale Systemzeit wieder um 1 Stunde. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Zeit > Grundeinstellungen*, Registerkarte *Sommerzeit*.
- ☐ Um ein eine vordefiniertes Profil für Beginn und Ende der Sommerzeit auszuwählen, klicken Sie im Rahmen *Funktion* die Schaltfläche *Profil...*.
- ☐ Wenn kein passendes Sommerzeitprofil verfügbar ist, dann legen Sie in den Feldern *Sommerzeit Beginn* und *Sommerzeit Ende* die Zeitpunkte der Zeitumstellung fest.
  Für beide Zeitpunkte legen Sie den Monat, die Woche innerhalb dieses Monats, den Wochentag sowie die Uhrzeit fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`clock summer-time mode <disable|recurring|eu|usa>`	Konfigurieren der automatischen Sommerzeitumstellung: einschalten, ausschalten oder mit Profil aktivieren.
`clock summer-time recurring start`	Eingabe des Startzeitpunkts für die Umschaltung.
`clock summer-time recurring end`	Eingabe des Endzeitpunkts für die Umschaltung.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

4.2 SNTP

Das Simple Network Time Protocol (SNTP) ermöglicht Ihnen, die Systemzeit in Ihrem Netz zu synchronisieren. Das Gerät unterstützt die SNTP-Client- und die SNTP-Server-Funktion.

Der SNTP-Server stellt die UTC (Universal Time Coordinated) zur Verfügung. Die UTC ist die auf die koordinierte Weltzeitmessung bezogene Uhrzeit. Die UTC ist weltweit gleich und ignoriert lokale Zeitverschiebungen.

SNTP ist eine vereinfachte Version des NTP (Network Time Protocol). Die Datenpakete sind bei SNTP und NTP identisch aufgebaut. Demzufolge dienen sowohl NTP- als auch SNTP-Server als Zeitquelle für SNTP-Clients.

Anmerkung: Aussagen in diesem Kapitel, die sich auf externe SNTP-Server beziehen, gelten ebenso für NTP-Server.

SNTP kennt die folgenden Betriebsmodi zur Übertragung der Zeit:

- *Unicast*
  Im *Unicast*-Betriebsmodus sendet ein SNTP-Client Anfragen an einen SNTP-Server und erwartet eine Antwort von diesem Server.
- *Broadcast*
  Im *Broadcast*-Betriebsmodus sendet ein SNTP-Server in definierten Abständen SNTP-Nachrichten in das Netz aus. SNTP-Clients empfangen diese SNTP-Nachrichten und werten sie aus.

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. 16: IPv4-Zieladressklassen für Broadcast-Betriebsmodus

IPv4-Zieladresse	SNTP-Pakete senden an
`0.0.0.0`	Niemand
`224.0.1.1`	*Multicast*-Adresse für SNTP-Nachrichten
`255.255.255.255`	*Broadcast*-Adresse

Anmerkung: Ein SNTP-Server im *Broadcast*-Betriebsmodus beantwortet auch direkte Anfragen per *Unicast* von SNTP-Clients. SNTP-Clients arbeiten hingegen entweder im *Unicast*- oder im *Broadcast*-Betriebsmodus.

4.2.1 Vorbereitung

Führen Sie die folgenden Schritte aus:

- ☐ Zeichnen Sie einen Netzplan mit den am SNTP beteiligten Geräten, um einen Überblick über die Weitergabe der Uhrzeit zu erhalten.
  Beachten Sie bei der Planung, dass die Genauigkeit der Uhrzeit von den Laufzeiten der SNTP-Nachrichten abhängig ist. Um die Laufzeiten und deren Varianz zu minimieren, platzieren Sie in jedem Netzsegment einen SNTP-Server. Jeder dieser SNTP-Server synchronisiert seine eigene Systemzeit als SNTP-Client am jeweils übergeordneten SNTP-Server (SNTP-Kaskade). Der oberste SNTP-Server in der SNTP-Kaskade hat möglichst direkten Zugriff auf eine Referenzzeitquelle.

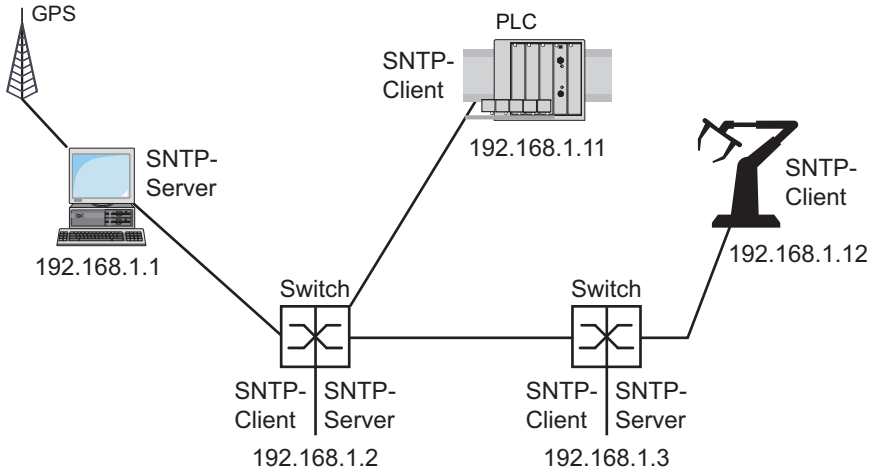


Abb. 19: Beispiel SNTP-Kaskade

Anmerkung: Für eine genaue Zeitverteilung verwenden Sie zwischen SNTP-Servern und SNTP-Clients bevorzugt Netzkomponenten (Router und Switches), die SNTP-Pakete mit möglichst geringer und gleichmäßiger Durchlaufzeit (Latenz) weiterleiten.

- Ein SNTP-Client sendet seine Anfragen an bis zu 4 konfigurierte SNTP-Server. Bleibt die Antwort des 1. SNTP-Servers aus, sendet der SNTP-Client seine Anfragen an den 2. SNTP-Server. Ist auch diese Anfrage erfolglos, sendet er die Anfrage an den 3. und schließlich an den 4. SNTP-Server. Antwortet keiner dieser SNTP-Server, verliert der SNTP-Client seine Synchronisation. Der SNTP-Client fragt solange zyklisch nacheinander bei den SNTP-Servern an, bis ein Server eine gültige Zeit liefert.

Anmerkung: Das Gerät bietet die Möglichkeit, eine Liste von SNTP-Server-IP-Adressen von einem DHCP-Server beziehen.

- ☐ Wenn Sie keine Referenzzeitquelle zur Verfügung haben, bestimmen Sie ein Gerät mit SNTP-Server zur Referenzzeitquelle. Justieren Sie dessen Systemzeit turnusmäßig.

4.2.2 Einstellungen des SNTP-Clients festlegen

Als SNTP-Client bezieht das Gerät die Zeitinformationen von SNTP- oder NTP-Servern und synchronisiert seine Systemuhr dementsprechend. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Zeit > SNTP > Client*.
- ☐ Legen Sie den SNTP-Betriebsmodus fest.
  Markieren Sie im Rahmen *Konfiguration*, Feld *Modus* einen der folgenden Werte:
  - `unicast`
    Das Gerät sendet Anfragen an einen SNTP-Server und erwartet von diesem Server eine Antwort.
  - `broadcast`
    Das Gerät wartet auf *Broadcast*- oder *Multicast*-Nachrichten von SNTP-Servern im Netz.
- ☐ Um die Zeit ausschließlich ein einziges Mal zu synchronisieren, markieren Sie das Kontrollkästchen *Deaktiviere Client nach erfolgreicher Synchronisierung*.
  Nach erfolgreicher Synchronisation schaltet das Gerät die Funktion *SNTP Client* aus.
- Die Tabelle zeigt die SNTP-Server, die der SNTP-Client im *Unicast*-Betriebsmodus anfragt. Die Tabelle enthält bis zu 4 SNTP-Server-Definitionen.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Legen Sie die Verbindungsdaten des SNTP-Servers fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .
- Das Feld *Zustand* zeigt den aktuellen Status der Funktion *SNTP Client*.

Tab. 17: Einstellungen der SNTP-Clients für das Beispiel

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Funktion *SNTP Client*	`Aus`	`An`	`An`	`An`	`An`

Tab. 17: Einstellungen der SNTP-Clients für das Beispiel (Forts

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Konfiguration: *Modus*	unicast	unicast	unicast	unicast	unicast
Request-Intervall [s]	30	30	30	30	30
SNTP Server-Adresse(n)	–	192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.2 192.168.1.1	192.168.1.3 192.168.1.2 192.168.1.1

4.2.3 Einstellungen des SNTP-Servers festlegen

Wenn das Gerät als SNTP-Server arbeitet, stellt es seine Systemzeit als koordinierte Weltzeit (UTC) im Netz zur Verfügung. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Zeit > SNTP > Server*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Um den *Broadcast*-Betriebsmodus einzuschalten, markieren Sie im Rahmen *Konfiguration* das Kontrollkästchen *Broadcast-Admin-Modus*.
  Im *Broadcast*-Betriebsmodus sendet der SNTP-Server in definierten Abständen SNTP-Nachrichten in das Netz aus. Außerdem beantwortet der SNTP-Server Anfragen von SNTP-Clients im *Unicast*-Betriebsmodus.
  - ☐ Im Feld *Broadcast-Ziel-Adresse* legen Sie die IPv4-Adresse fest, an die der SNTP-Server die SNTP-Pakete sendet. Legen Sie eine *Broadcast*-Adresse oder eine *Multicast*-Adresse fest.
    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 die ID des VLANs fest, in welches der SNTP-Server die SNTP-Pakete im *Broadcast*-Betriebsmodus sendet.
  - ☐ Im Feld *Broadcast-Sende-Intervall [s]* legen Sie den Zeitabstand fest, in dem der SNTP-Server die SNTP-Pakete im *Broadcast*-Betriebsmodus sendet.

Anmerkung: Mit Ausnahme des Felds *Broadcast-Ziel-Adresse* sind die übrigen Einstellungen auf IPv4- und IPv6-SNTP-Server anwendbar.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.
- ▶ Das Feld *Zustand* zeigt den aktuellen Status der Funktion *SNTP Server*.

Tab. 18: Einstellungen für das Beispiel

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Funktion *SNTP Server*	*An*	*An*	*An*	*Aus*	*Aus*
UDP-Port	123	123	123	123	123
Broadcast-Admin-Modus	unmarkiert	unmarkiert	unmarkiert	unmarkiert	unmarkiert
Broadcast-Ziel-Adresse	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast-UDP-Port	123	123	123	123	123

Tab. 18: Einstellungen für das Beispiel (Forts

Gerät	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
Broadcast VLAN-ID	1	1	1	1	1
Broadcast-Sende-Intervall [s]	128	128	128	128	128
Server deaktivieren bei lokaler Zeitquelle	unmarkiert	unmarkiert	unmarkiert	unmarkiert	unmarkiert

4.3 PTP

Damit über ein LAN gesteuerte Anwendungen ohne Latenz arbeiten, ist ein präzises Zeitmanagement erforderlich. IEEE 1588 beschreibt mit PTP (Precision Time Protocol) ein Verfahren, das die präzise Synchronisation der Uhren im Netz ermöglicht.

Das PTP erlaubt die Synchronisation mit einer Genauigkeit bis zu wenigen 100 ns. PTP verwendet Multicasts für die Synchronisationsnachrichten, dadurch ist die Netzlast gering.

4.3.1 Typen von Uhren

Das PTP definiert für die Uhren im Netz die Rollen „Master“ und „Slave“:
- Eine Master-Uhr (Referenzzeitquelle) verteilt ihre Zeit.
- Eine Slave-Uhr synchronisiert sich auf das von der Master-Uhr empfangene Zeitsignal.

Boundary Clock

Die Durchlaufzeit (Latenz) in Routern und Switches wirkt sich messbar auf die Präzision der Zeitübertragung aus. Um solche Ungenauigkeiten zu korrigieren, definiert PTP sogenannte Boundary-Clocks.

Eine Boundary-Clock ist die Referenzzeitquelle (Master-Uhr) in einem Netzsegment, auf die sich die untergeordneten Slave-Uhren synchronisieren. Typischerweise übernehmen Router und Switches die Rolle der Boundary-Clock.

Die Boundary-Clock bezieht ihrerseits die Uhrzeit von einer übergeordneten Referenzzeitquelle (Grandmaster).

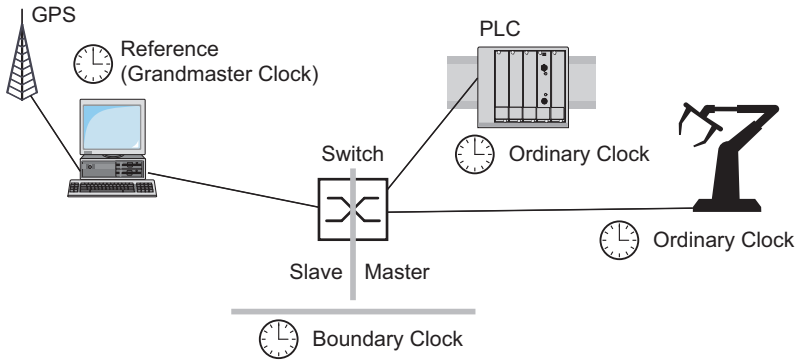


Abb. 20: Position der Boundary-Clock in einem Netz

Transparent Clock

Typischerweise übernehmen Switches die Rolle der Transparent Clock, um über Kaskaden hinweg eine hohe Genauigkeit zu ermöglichen. Die Transparent Clock ist eine Slave-Uhr, die beim Weiterleiten empfangener Synchronisationsnachrichten die eigene Durchlaufzeit korrigiert.

Ordinary Clock

Die Uhr in einem Endgerät bezeichnet PTP als „Ordinary Clock“. Eine Ordinary Clock funktioniert entweder als Master-Uhr oder als Slave-Uhr.

4.3.2 Best-Master-Clock-Algorithmus

Die an PTP beteiligten Geräte bestimmen ein Gerät im Netz zur Referenzzeitquelle (Grandmaster). Dabei kommt der „Best Master Clock“-Algorithmus zum Einsatz, der die Genauigkeit der verfügbaren Uhren im Netz ermittelt.

Der „Best Master Clock“-Algorithmus bewertet dabei folgende Kriterien:
- *Priorität 1*
- *Uhr-Klasse*
- *Präzision*
- *Uhr-Varianz*
- *Priorität 2*

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

Das Gerät ermöglicht Ihnen, in den Einstellungen der Boundary-Clock den Wert für *Priorität 1* und *Priorität 2* individuell festzulegen. Dies ermöglicht Ihnen, Einfluss darauf zu nehmen, welches Gerät die Referenzzeitquelle (Grandmaster) im Netz wird.

4.3.3 Laufzeitmessung

Die Laufzeit der Synchronisationsnachrichten zwischen den beteiligten Geräten hat Einfluss auf die Genauigkeit. Durch die Laufzeitmessung berücksichtigen die Geräte die mittlere Laufzeit.

PTP Version 2 bietet folgende Verfahren für die Laufzeitmessung:
- `e2e` (End to End)
  Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
- `e2e-optimized`
  Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
  Dieses Verfahren ist ausschließlich für Transparent-Clocks verfügbar. Das Gerät vermittelt die per Multicast gesendeten Synchronisationsnachrichten ausschließlich an die Master-Uhr und hält dadurch die Netzlast gering. Wenn das Gerät eine Synchronisationsnachricht von einer anderen Master-Uhr empfängt, vermittelt es die Synchronisationsnachrichten ausschließlich an diesen neuen Port.
  Kennt das Gerät keine Master-Uhr, vermittelt es Synchronisationsnachrichten an jeden Port.
- `p2p` (Peer to Peer)
  Die Slave-Uhr misst die Laufzeit der Synchronisationsnachrichten zur Master-Uhr.
  Zusätzlich misst die Master-Uhr die Laufzeit zu jeder Slave-Uhr, auch über blockierte Ports hinweg. Voraussetzung ist, dass Master- und Slave-Uhr Peer-to-Peer (`p2p`) unterstützen.
  Bei Unterbrechung eines redundanten Rings beispielsweise wird eine Slave-Uhr zur Master-Uhr und die Master-Uhr zur Slave-Uhr. Dieser Wechsel findet ohne Präzisionsverlust statt, weil die Uhren die Laufzeit in die andere Richtung bereits kennen.

4.3.4 PTP-Domänen

Synchronisationsnachrichten überträgt das Gerät ausschließlich von und zu Geräten in derselben PTP-Domäne. Das Gerät ermöglicht Ihnen, die Domäne für die Boundary-Clock und für die Transparent-Clock individuell festzulegen.

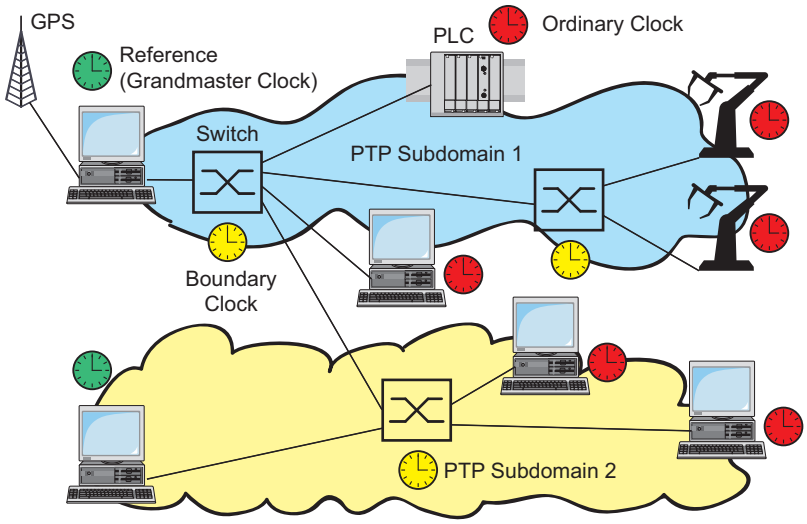


Abb. 21: Beispiel für PTP-Domänen

4.3.5 PTP verwenden

Um die Uhren präzise mit PTP zu synchronisieren, verwenden Sie als Netzknoten ausschließlich Switches mit Boundary-Clock oder Transparent-Clock.

Führen Sie die folgenden Schritte aus:

- ☐ Um sich einen Überblick über die Uhrenverteilung zu verschaffen, zeichnen Sie einen Netzplan mit den am PTP beteiligten Geräten.
- ☐ Legen Sie für jeden beteiligten Switch die Rolle fest (Boundary-Clock oder Transparent-Clock). Im Gerät heißt diese Einstellung *PTP-Modus*.

Tab. 19: Mögliche Einstellwerte für den PTP-Modus

PTP-Modus	Anwendung
`v2-boundary-clock`	Als Boundary-Clock verteilt das Gerät die Synchronisationsnachrichten an die Slave-Uhren im untergeordneten Netzsegment. Die Boundary-Clock bezieht ihrerseits die Uhrzeit von einer übergeordneten Referenzzeitquelle (Grandmaster).
`v2-transparent-clock`	Als Transparent-Clock leitet das Gerät empfangene Synchronisationsnachrichten korrigiert um die eigene Durchlaufzeit weiter.

- ☐ Schalten Sie PTP auf jedem beteiligten Switch ein.
  PTP konfiguriert sich anschließend weitestgehend automatisch.
- ☐ Schalten Sie PTP auf den Endgeräten ein.
- ☐ Das Gerät ermöglicht Ihnen, Einfluss darauf zu nehmen, welches Gerät im Netz Referenzzeitquelle (Grandmaster) wird. Ändern Sie dazu für die *Boundary Clock* den voreingestellten Wert in den Feldern *Priorität 1* und *Priorität 2*.

5 Konfigurationsprofile verwalten

Wenn Sie die Einstellungen des Geräts im laufenden Betrieb ändern, dann speichert das Gerät diese Änderungen im flüchtigen Speicher (*RAM*). Nach einem Neustart sind diese Einstellungen verloren.

Damit die Änderungen einen Neustart überdauern, ermöglicht Ihnen das Gerät, die Einstellungen in einem Konfigurationsprofil im permanenten Speicher (*NVM*) zu speichern. Um gegebenenfalls schnell auf andere Einstellungen umzuschalten, bietet der permanente Speicher Platz für mehrere Konfigurationsprofile.

Wenn ein externer Speicher angeschlossen ist, dann speichert das Gerät automatisch eine Kopie des Konfigurationsprofils im externen Speicher (*ENVM*). Sie können diese Funktion ausschalten.

5.1 Geänderte Einstellungen erkennen

Das Gerät speichert die während des Betriebs geänderten Einstellungen im flüchtigen Speicher (*RAM*). Das Konfigurationsprofil im permanenten Speicher (*NVM*) bleibt dabei so lange unverändert, bis Sie die geänderten Einstellungen explizit speichern. Bis dahin unterscheiden sich die Konfigurationsprofile im flüchtigen und im permanenten Speicher. Das Gerät unterstützt Sie dabei, geänderte Einstellungen zu erkennen.

5.1.1 Flüchtiger Speicher (RAM) und nichtflüchtiger Speicher (NVM)

Sie können erkennen, wenn das Konfigurationsprofil im flüchtigen Speicher (*RAM*) vom "ausgewählten" Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) abweicht. Führen Sie dazu die folgenden Schritte aus:

- ☐ Prüfen Sie die Statusleiste im oberen Bereich des Menüteils:
  - Wenn ein blinkendes Symbol sichtbar ist, weichen die Konfigurationsprofile voneinander ab.
  - Wenn kein Symbol sichtbar ist, stimmen die Konfigurationsprofile überein.

oder:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Prüfen Sie den Zustand des Kontrollkästchens im Rahmen *Information*:
  - Wenn das Kontrollkästchen nicht markiert ist, weichen die Konfigurationsprofile voneinander ab.
  - Wenn das Kontrollkästchen markiert ist, stimmen die Konfigurationsprofile überein.

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.......................out of sync
...
```

5.1.2 Externer Speicher (EAM) und nichtflüchtiger Speicher (NVM)

Sie können auch erkennen, wenn die Kopie im externen Speicher (EAM) vom Konfigurationsprofil im nichtflüchtigen Speicher (*NVM*) abweicht. 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 nicht markiert ist, weichen die Konfigurationsprofile voneinander ab.
  - Wenn das Kontrollkästchen markiert ist, stimmen die Konfigurationsprofile überein.

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to EAM.................................out of sync
...
```

5.2 Einstellungen speichern

5.2.1 Konfigurationsprofil im Gerät speichern

Wenn Sie die Einstellungen des Geräts im laufenden Betrieb ändern, dann speichert das Gerät diese Änderungen im flüchtigen Speicher (RAM). Damit die Änderungen einen Neustart überdauern, speichern Sie das Konfigurationsprofil im permanenten Speicher (*NVM*).

Konfigurationsprofil speichern

Das Gerät speichert die Einstellungen im „ausgewählten“ Konfigurationsprofil im permanenten Speicher (*NVM*).

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Vergewissern Sie sich, dass das gewünschte Konfigurationsprofil „ausgewählt“ ist. Das „ausgewählte“ Konfigurationsprofil erkennen Sie daran, dass in Spalte *Ausgewählt* das Kontrollkästchen markiert ist.
- ☐ Klicken Sie die Schaltfläche  .

`show config profiles nvm`	Zeigt die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile.
`enable`	Wechsel in den Privileged-EXEC-Modus.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

Einstellungen in Konfigurationsprofil kopieren

Das Gerät ermöglicht Ihnen, die im flüchtigen Speicher (RAM) gespeicherten Einstellungen anstatt im „ausgewählten“ Konfigurationsprofil in ein anderes Konfigurationsprofil zu kopieren. Auf diese Weise erzeugen Sie im permanenten Speicher (*NVM*) ein neues oder überschreiben ein vorhandenes Konfigurationsprofil.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Klicken Sie die Schaltfläche  und dann den Eintrag *Speichern unter...*. Der Dialog zeigt das Fenster *Speichern unter...*.
- ☐ Passen Sie im Feld *Name* die Bezeichnung des Konfigurationsprofils an. Wenn Sie die vorgeschlagene Bezeichnung beibehalten, überschreibt das Gerät ein vorhandenes, namensgleiches Konfigurationsprofil.
- ☐ Klicken Sie die Schaltfläche *Ok*.

Das neue Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

`show config profiles nvm`	Zeigt die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile.
`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy config running-config nvm profile <string>`	Speichern der aktuellen Einstellungen im Konfigurationsprofil mit der Bezeichnung `<string>` im permanenten Speicher (`nvm`). Wenn vorhanden, überschreibt das Gerät ein namensgleiches Konfigurationsprofil. Das neue Konfigurationsprofil ist als „ausgewählt“ gekennzeichnet.

Konfigurationsprofil auswählen

Wenn der permanente Speicher (*NVM*) mehrere Konfigurationsprofile enthält, haben Sie die Möglichkeit, dort ein beliebiges Konfigurationsprofil auszuwählen. Das Gerät speichert die Einstellungen im „ausgewählten“ Konfigurationsprofil. Das Gerät lädt die Einstellungen des „ausgewählten“ Konfigurationsprofils beim Neustart in den flüchtigen Speicher (`RAM`).

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.

Die Tabelle zeigt die im Gerät vorhandenen Konfigurationsprofile. Das „ausgewählte“ Konfigurationsprofil erkennen Sie daran, dass in Spalte *Ausgewählt* das Kontrollkästchen markiert ist.

- ☐ Markieren Sie den Tabelleneintrag des gewünschten Konfigurationsprofils, das im permanenten Speicher (*NVM*) gespeichert ist.
- ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Auswählen*.

In Spalte *Ausgewählt* ist jetzt das Kontrollkästchen des Konfigurationsprofils `markiert`.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`show config profiles nvm`	Zeigt die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile.
`configure`	Wechsel in den Konfigurationsmodus.
`config profile select nvm 1`	Kennzeichnen des Konfigurationsprofils. Orientieren Sie sich am nebenstehenden Namen des Konfigurationsprofils.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

5.2.2 Konfigurationsprofil im externen Speicher speichern

Wenn ein externer Speicher angeschlossen ist und Sie ein Konfigurationsprofil speichern, speichert das Gerät automatisch eine Kopie im *Ausgewählter externer Speicher*. In der Voreinstellung ist die Funktion eingeschaltet. Sie können diese Funktion ausschalten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Externer Speicher*.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Sichere Konfiguration beim Speichern*, damit das Gerät beim Speichern automatisch eine Kopie im externen Speicher speichert.
- ☐ Um die Funktion zu deaktivieren, heben Sie die Markierung des Kontrollkästchens in Spalte *Sichere Konfiguration beim Speichern* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`config envm config-save usb`	Einschalten der Funktion. Beim Speichern eines Konfigurationsprofils speichert das Gerät eine Kopie im externen Speicher. `usb` = Externer USB-Speicher
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

5.2.3 Konfigurationsprofil auf einem Remote-Server sichern

Das Gerät ermöglicht Ihnen, eine Kopie des Konfigurationsprofils automatisch auf einem Remote-Server zu sichern. Voraussetzung ist, dass Sie die Funktion vor dem Speichern des Konfigurationsprofils aktivieren.

Nach dem Speichern des Konfigurationsprofils im permanenten Speicher (*NVM*) sendet das Gerät eine Kopie an die festgelegte Adresse.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
  Führen Sie im Rahmen *Sichere Konfiguration auf Remote-Server beim Speichern* die folgenden Schritte aus:
- ☐ Legen Sie im Rahmen *URL* den Server sowie Pfad und Dateinamen des kopierten Konfigurationsprofils fest.
- ☐ Klicken Sie die Schaltfläche *Zugangsdaten setzen*.
  Der Dialog zeigt das Fenster *Anmeldeinformationen*.
- ☐ Geben Sie die Anmeldedaten ein, die für die Authentifizierung auf dem entfernten Server erforderlich sind.
- ☐ Schalten Sie die Funktion in der Optionsliste *Funktion* ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`show config remote-backup`	Status der Funktion prüfen.
`configure`	Wechsel in den Konfigurationsmodus.
`config remote-backup destination`	Ziel-URL für das kopierte Konfigurationsprofil einfügen.
`config remote-backup username`	Benutzernamen einfügen für die Authentifizierung auf dem entfernten Server.
`config remote-backup password`	Passwort einfügen für die Authentifizierung auf dem entfernten Server.
`config remote-backup operation`	Einschalten der Funktion.

Wenn die Übertragung zum entfernten Server scheitert, dann protokolliert das Gerät dieses Ereignis in der Protokolldatei System Log.

5.2.4 Konfigurationsprofil exportieren

Das Gerät ermöglicht Ihnen, ein Konfigurationsprofil als XML-Datei auf einem Server zu speichern. Wenn Sie die grafische Benutzeroberfläche verwenden, dann haben Sie die Möglichkeit, die XML-Datei direkt auf Ihrem PC zu speichern.

Voraussetzungen:
- Um die Datei auf einem Server zu speichern, benötigen Sie einen eingerichteten Server im Netz.
- Um die Datei auf einem SCP- oder SFTP-Server zu speichern, benötigen Sie zusätzlich Benutzername und Passwort für den Zugriff auf diesen Server.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Markieren Sie den Tabelleneintrag des gewünschten Konfigurationsprofils.

Exportieren Sie das Konfigurationsprofil auf Ihren PC. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie den Link in Spalte *Profilname*.
- ☐ Wählen Sie den Speicherort und legen den Dateinamen fest.
- ☐ Klicken Sie die Schaltfläche *Ok*.

Das Konfigurationsprofil ist jetzt als XML-Datei am angegebenen Ort gespeichert.

Exportieren Sie das Konfigurationsprofil auf einen Remote-Server. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Exportieren...*.
  Der Dialog zeigt das Fenster *Exportieren...*.
- ☐ Legen Sie im Feld *URL* die URL der Datei auf dem Remote-Server fest.
  - ☐ Um die Datei auf einem FTP-Server zu speichern, legen Sie den URL zur Datei in der folgenden Form fest:
    `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
  - ☐ Um die Datei auf einem TFTP-Server zu speichern, legen Sie den URL zur Datei in der folgenden Form fest:
    `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
  - ☐ Um die Datei auf einem SCP- oder SFTP-Server zu speichern, legen Sie den URL zur Datei in einer der folgenden Formen fest:
    `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`
    `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Ok* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
- ☐ Klicken Sie die Schaltfläche *Ok*.
  Das Konfigurationsprofil ist jetzt als XML-Datei am angegebenen Ort gespeichert.

`show config profiles nvm`	Zeigt die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile.
`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy config running-config remote tftp://<IP_address>/ <path>/<file_name>`	Speichern der aktuellen Einstellungen auf einem TFTP-Server.
`copy config nvm remote sftp://<user_name>:<password>@<IP_address>/<path>/<file_name>`	Speichern des „ausgewählten” Konfigurationsprofils im permanenten Speicher `nvm` auf einem SFTP-Server.
`copy config nvm profile config3 remote tftp://<IP_address>/ <path>/<file_name>`	Speichern des Konfigurationsprofils `config3` im permanenten Speicher (`nvm`) auf einem TFTP-Server.
`copy config nvm profile config3 remote ftp://<IP_address>:<port>/<path>/<file_name>`	Speichern des Konfigurationsprofils `config3` im permanenten Speicher (`nvm`) auf einem FTP-Server.

5.3 Einstellungen laden

Wenn Sie mehrere Konfigurationsprofile im Speicher hinterlegen, haben Sie die Möglichkeit, ein anderes Konfigurationsprofil zu laden.

5.3.1 Konfigurationsprofil aktivieren

Der permanente Speicher des Geräts kann mehrere Konfigurationsprofile enthalten. Wenn Sie ein im permanenten Speicher (*NVM*) hinterlegtes Konfigurationsprofil aktivieren, dann verändern Sie die Einstellungen des Geräts unmittelbar. Das Gerät benötigt keinen Neustart.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Markieren Sie den Tabelleneintrag des gewünschten Konfigurationsprofils.
- ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Aktivieren*.

Das Gerät kopiert die Einstellungen in den flüchtigen Speicher (`RAM`) und trennt die Verbindung zur grafischen Benutzeroberfläche. Das Gerät verwendet ab sofort die Einstellungen des Konfigurationsprofils.

- ☐ Laden Sie die grafische Benutzeroberfläche neu.
- ☐ Melden Sie sich erneut an.

In Spalte *Ausgewählt* ist das Kontrollkästchen des zuvor aktivierten Konfigurationsprofils `markiert`.

`show config profiles nvm`	Zeigt die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile.
`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy config nvm profile config3 running-config`	Einstellungen des Konfigurationsprofils `config3` im permanenten Speicher (`nvm`) anwenden. Das Gerät kopiert die Einstellungen in den flüchtigen Speicher und trennt die Verbindung zum Command Line Interface. Das Gerät verwendet ab sofort die Einstellungen des Konfigurationsprofils `config3`.

5.3.2 Konfigurationsprofil aus dem externen Speicher laden

Wenn der externe Speicher angeschlossen ist, dann lädt das Gerät beim Neustart automatisch ein Konfigurationsprofil aus dem externen Speicher. Das Gerät ermöglicht Ihnen, diese Einstellungen wieder in einem Konfigurationsprofil im permanenten Speicher zu speichern.

Wenn der externe Speicher das Konfigurationsprofil eines baugleichen Geräts enthält, haben Sie die Möglichkeit, auf diese Weise die Einstellungen von einem Gerät in ein anderes zu übertragen.

Führen Sie die folgenden Schritte aus:

☐ Vergewissern Sie sich, dass das Gerät beim Neustart ein Konfigurationsprofil aus dem externen Speicher lädt.
In der Voreinstellung ist die Funktion eingeschaltet. Wenn die Funktion ausgeschaltet ist, schalten Sie sie wie folgt wieder ein:

☐ Öffnen Sie den Dialog *Grundeinstellungen > Externer Speicher*.

☐ Markieren Sie in Spalte *Konfigurations-Priorität* den Wert `first`.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`config envm load-priority usb first`	Einschalten der Funktion. Beim Neustart lädt das Gerät ein Konfigurationsprofil aus dem externen Speicher. `usb` = Externer USB-Speicher
`show config envm settings`	Zeigt die Einstellungen des externen Speichers (`envm`).

```
Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
usb    ok          [x]         [x]           first
```

`save`	Speichern Sie die Einstellungen in einem Konfigurationsprofil im permanenten Speicher (*NVM*) des Geräts.

Das Gerät ermöglicht Ihnen, mit dem Command Line Interface die Einstellungen aus dem externen Speicher in den permanenten Speicher (*NVM*) zu kopieren.

`show config profiles nvm`	Zeigt die im permanenten Speicher (`nvm`) enthaltenen Konfigurationsprofile.
`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy config envm profile config3 nvm`	Kopieren des Konfigurationsprofils `config3` aus dem externen Speicher (`envm`) in den permanenten Speicher (`nvm`).

Während des Bootvorgangs kann das Gerät außerdem automatisch ein Konfigurationsprofil aus einer Skriptdatei laden.

Voraussetzungen:

- Vergewissern Sie sich, dass der externe Speicher angeschlossen ist, bevor Sie das Gerät starten.
- Das Root-Verzeichnis des externen Speichers enthält eine Textdatei `startup.txt` mit dem Inhalt `script=<Dateiname>`. Der Platzhalter `<Dateiname>` repräsentiert die Skriptdatei, die das Gerät während des Bootvorgangs ausführt.
- Das Root-Verzeichnis des externen Speichers enthält die Skript-Datei. Sie haben die Möglichkeit, das Skript unter einem benutzerdefinierten Namen zu speichern. Speichern Sie die Datei mit der Dateiendung `.cli`.

Anmerkung: Vergewissern Sie sich, dass das im externen Speicher gespeicherte Skript nicht leer ist. Wenn das Skript leer ist, dann lädt das Gerät gemäß den Einstellungen der Konfigurations-Priorität das nächste Konfigurationsprofil.

Nach Anwenden des Skripts speichert das Gerät das Konfigurationsprofil aus der Skriptdatei automatisch als XML-Datei im externen Speicher. Sie haben die Möglichkeit, diese Funktion auszuschalten, wenn Sie den betreffenden Befehl in die Skriptdatei einfügen:

☐ `no config envm config-save usb`
Das Gerät erzeugt keine Kopie im externen USB-Speicher.

Enthält die Skriptdatei einen falschen Befehl, wendet das Gerät diesen Befehl während des Bootvorgangs nicht an. Das Gerät protokolliert das Ereignis in der Log-Datei (System Log).

5.3.3 Konfigurationsprofil importieren

Das Gerät ermöglicht Ihnen, ein als XML-Datei gespeichertes Konfigurationsprofil von einem Server zu importieren. Wenn Sie die grafische Benutzeroberfläche verwenden, dann können Sie die XML-Datei direkt von Ihrem PC importieren.

Voraussetzungen:
- Um die Datei auf einem Server zu speichern, benötigen Sie einen eingerichteten Server im Netz.
- Um die Datei auf einem SCP- oder SFTP-Server zu speichern, benötigen Sie zusätzlich Benutzername und Passwort für den Zugriff auf diesen Server.

Führen Sie die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.

☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Importieren...*.
Der Dialog zeigt das Fenster *Importieren...*.

☐ Wählen Sie in der Dropdown-Liste *Select source* den Speicherort aus, von dem das Gerät das Konfigurationsprofil importiert.
- *PC/URL*
  Das Gerät importiert das Konfigurationsprofil vom lokalen PC oder von einem Remote-Server.
- *Externer Speicher*
  Das Gerät importiert das Konfigurationsprofil aus dem externen Speicher.

Importieren Sie das Konfigurationsprofil vom lokalen PC oder von einem Remote-Server. Führen Sie dazu die folgenden Schritte aus:

- ☐ Importieren Sie das Konfigurationsprofil.
  - ☐ Befindet sich die Datei auf einem FTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
    `ftp://<Benutzername>:<Passwort>@<IP-Adresse>:<Port>/<Dateiname>`
  - ☐ Befindet sich die Datei auf einem TFTP-Server, legen Sie den URL zur Datei in der folgenden Form fest:
    `tftp://<IP-Adresse>/<Pfad>/<Dateiname>`
  - ☐ Befindet sich die Datei auf einem SCP- oder SFTP-Server, legen Sie den URL zur Datei in einer der folgenden Formen fest:
    `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Dateiname>`
    Nach Klicken der Schaltfläche *Start* zeigt das Gerät das Fenster *Anmeldeinformationen*. Geben Sie dort *Benutzername* und *Passwort* ein, um sich am Server anzumelden.
    `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Dateiname>`
- ☐ Legen Sie im Rahmen *Ziel* fest, wo das Gerät das importierte Konfigurationsprofil speichert.
  - ☐ Legen Sie im Feld *Profilname* den Namen fest, unter dem das Gerät das Konfigurationsprofil speichert.
  - ☐ Legen Sie im Feld *Speicher-Typ* den Speicherort für das Konfigurationsprofil fest.
- ☐ Klicken Sie die Schaltfläche *Ok*.

Das Gerät kopiert das Konfigurationsprofil in den festgelegten Speicher.

Wenn Sie im Rahmen *Ziel* den Wert `ram` festgelegt haben, dann trennt das Gerät die Verbindung zur grafischen Benutzeroberfläche und verwendet sofort die Einstellungen.

Importieren Sie das Konfigurationsprofil aus dem externen Speicher. Führen Sie dazu die folgenden Schritte aus:

- ☐ Wählen Sie im Rahmen *Import profile from external memory*, Dropdown-Liste *Profilname* den Namen des zu importierenden Konfigurationsprofils.
  Voraussetzung ist, dass der externe Speicher ein exportiertes Konfigurationsprofil enthält.
- ☐ Legen Sie im Rahmen *Ziel* fest, wo das Gerät das importierte Konfigurationsprofil speichert.
  - ☐ Legen Sie im Feld *Profilname* den Namen fest, unter dem das Gerät das Konfigurationsprofil speichert.
- ☐ Klicken Sie die Schaltfläche *Ok*.

Das Gerät kopiert das Konfigurationsprofil in den permanenten Speicher (*NVM*) des Geräts.

Wenn Sie im Rahmen *Ziel* den Wert `ram` festgelegt haben, dann trennt das Gerät die Verbindung zur grafischen Benutzeroberfläche und verwendet sofort die Einstellungen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> running-config`	Konfigurationsprofil-Einstellungen von einem FTP-Server importieren und anwenden. Das Gerät kopiert die Einstellungen in den flüchtigen Speicher und trennt die Verbindung zum Command Line Interface. Das Gerät verwendet ab sofort die Einstellungen des importierten Konfigurationsprofils.
`copy config remote tftp://<IP_address>/ <path>/<file_name> running-config`	Konfigurationsprofil-Einstellungen von einem TFTP-Server importieren und anwenden. Das Gerät kopiert die Einstellungen in den flüchtigen Speicher und trennt die Verbindung zum Command Line Interface. Das Gerät verwendet ab sofort die Einstellungen des importierten Konfigurationsprofils.
`copy config remote sftp://<user name>:<password>@<IP_address>/<path>/<file_name> running-config`	Konfigurationsprofil-Einstellungen von einem SFTP-Server importieren und anwenden. Das Gerät kopiert die Einstellungen in den flüchtigen Speicher und trennt die Verbindung zum Command Line Interface. Das Gerät verwendet ab sofort die Einstellungen des importierten Konfigurationsprofils.
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> nvm profile config3`	Einstellungen des auf einem FTP-Server gespeicherten Konfigurationsprofils importieren und die Einstellungen im Konfigurationsprofil `config3` im permanenten Speicher (`nvm`) speichern.
`copy config remote tftp://<IP_address>/<path>/<file_name> nvm profile config3`	Einstellungen des auf einem TFTP-Server gespeicherten Konfigurationsprofils importieren und die Einstellungen im Konfigurationsprofil `config3` im permanenten Speicher (`nvm`) speichern.

5.4 Gerät auf Lieferzustand zurücksetzen

Wenn Sie die Einstellungen im Gerät auf den Lieferzustand zurücksetzen, dann löscht das Gerät die Konfigurationsprofile im flüchtigen Speicher und im permanenten Speicher.

Wenn ein externer Speicher angeschlossen ist, dann löscht das Gerät auch die im externen Speicher gespeicherten Konfigurationsprofile.

Anschließend startet das Gerät neu und lädt die Werkseinstellungen.

5.4.1 Mit grafischer Benutzeroberfläche oder Command Line Interface

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Laden/Speichern*.
- ☐ Klicken Sie die Schaltfläche , anschließend *Auf Lieferzustand zurücksetzen...*.
  Der Dialog zeigt eine Meldung.
- ☐ Klicken Sie die Schaltfläche *Ok*.

Das Gerät löscht die Konfigurationsprofile im flüchtigen Speicher (`RAM`) und im permanenten Speicher (`NVM`).

Wenn ein externer Speicher angeschlossen ist, dann löscht das Gerät auch die im externen Speicher gespeicherten Konfigurationsprofile.

Nach kurzer Zeit startet das Gerät neu und lädt die Werkseinstellungen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`clear factory`	Löscht die Konfigurationsprofile im flüchtigen Speicher und im permanenten Speicher. Wenn ein externer Speicher angeschlossen ist, dann löscht das Gerät auch die im externen Speicher gespeicherten Konfigurationsprofile. Nach kurzer Zeit startet das Gerät neu und lädt die Werkseinstellungen.

5.4.2 System-Monitor starten

Voraussetzung:
- Ihr PC ist per Terminal-Kabel mit der seriellen Schnittstelle des Geräts verbunden.

Führen Sie die folgenden Schritte aus:
- ☐ Starten Sie das Gerät neu.
- ☐ Um in den System-Monitor zu wechseln, drücken Sie die Taste <1> bei Aufforderung während des Neustarts innerhalb von 3 Sekunden.
  Das Gerät lädt den System-Monitor.
- ☐ Um aus dem Hauptmenü in das Menü `Manage configurations` zu wechseln, drücken Sie die Taste <4>.
- ☐ Um das Kommando `Clear configs and boot params` auszuführen, drücken Sie die Taste <1>.

- Um die Werkseinstellungen zu laden, drücken Sie die <Enter>-Taste.
  Das Gerät löscht die Konfigurationsprofile im flüchtigen Speicher (RAM) und im permanenten Speicher (NVM).
  Wenn ein externer Speicher angeschlossen ist, dann löscht das Gerät auch die im externen Speicher gespeicherten Konfigurationsprofile.
- Um in das Hauptmenü zu wechseln, drücken Sie die Taste <q>.
- Um das Gerät mit Werkseinstellungen neuzustarten, drücken Sie die Taste <q>.

6 Neueste Software laden

Schneider Electric arbeitet ständig an der Verbesserung und Weiterentwicklung der Software. Prüfen Sie regelmäßig, ob ein neuerer Stand der Software Ihnen weitere Vorteile bietet. Informationen und Software-Downloads finden Sie auf den Schneider Electric-Produktseiten im Internet unter www.schneider-electric.com.

Das Gerät bietet Ihnen folgende Möglichkeiten, die Geräte-Software zu aktualisieren:
- Software-Update vom PC
- Software-Update von einem Server
- Software-Update aus dem externen Speicher
- Frühere Software-Version laden

Anmerkung: Die Einstellungen im Gerät bleiben nach dem Aktualisieren der Geräte-Software erhalten.

Die Version der installierten Geräte-Software sehen Sie im Login-Dialog der grafischen Benutzeroberfläche.

Um die Version der installierten Geräte-Software anzuzeigen, wenn Sie bereits eingeloggt sind, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
  Das Feld *Ausgeführte Version* zeigt Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Neustart geladen hat und gegenwärtig ausführt.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`show system info`	Zeigt die Systeminformationen, unter anderem Versionsnummer und Erstellungsdatum der Geräte-Software, die das Gerät beim letzten Neustart geladen hat und gegenwärtig ausführt.

6.1 Software-Update vom PC

Voraussetzung ist, dass die Image-Datei der Geräte-Software auf einem Datenträger gespeichert ist, den Sie von Ihrem PC aus erreichen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie das Verzeichnis, in dem die Image-Datei der Geräte-Software gespeichert ist.
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Ziehen Sie die Image-Datei in den  -Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.
- ☐ Um den Update-Vorgang zu starten, klicken Sie die Schaltfläche *Start*.
  Sobald der Update-Vorgang erfolgreich beendet ist, zeigt das Gerät eine Information, dass die Software erfolgreich aktualisiert wurde.
  Beim nächsten Neustart lädt das Gerät die installierte Geräte-Software.

6.2 Software-Update von einem Server

Für ein Software-Update mit SFTP oder SCP benötigen Sie einen Server, auf dem die Image-Datei der Geräte-Software abgelegt ist.

Für ein Software-Update mit TFTP, SFTP oder SCP benötigen Sie einen Server, auf dem die Image-Datei der Geräte-Software abgelegt ist.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Fügen Sie im Rahmen *Software-Update*, Feld *URL* den URL zur Image-Datei in der folgenden Form ein:
  - Wenn die Image-Datei auf einem FTP-Server abgelegt ist:
    `ftp://<IP-Adresse>:<Port>/<Pfad>/<Name_der_Image-Datei>.bin`
  - Wenn die Image-Datei auf einem TFTP-Server abgelegt ist:
    `tftp://<IP-Adresse>/<Pfad>/<Name_der_Image-Datei>.bin`
  - Wenn die Image-Datei auf einem SCP- oder SFTP-Server abgelegt ist:
    `scp://` oder `sftp://<IP-Adresse>/<Pfad>/<Name_der_Image-Datei>.bin`
    `scp://` oder `sftp://<Benutzername>:<Passwort>@<IP-Adresse>/<Pfad>/<Name_der_Image-Datei>.bin`
    Wenn Sie den URL ohne Benutzername und Passwort einfügen, zeigt das Gerät das Fenster *Anmeldeinformationen*. Fügen Sie dort die Anmeldedaten ein, um sich am Server anzumelden.
- ☐ Um den Update-Vorgang zu starten, klicken Sie die Schaltfläche *Start*.
  Die gegenwärtig ausgeführte Geräte-Software kopiert das Gerät in den Backup-Bereich. Sobald der Update-Vorgang erfolgreich beendet ist, zeigt das Gerät eine Information, dass die Software erfolgreich aktualisiert wurde.
  Beim nächsten Neustart lädt das Gerät die installierte Geräte-Software.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy firmware remote tftp://10.0.1.159/product.bin system`	Übertragen der Datei `product.bin` vom TFTP-Server mit der IP-Adresse `10.0.1.159` auf das Gerät.

6.3 Software-Update aus dem externen Speicher

6.3.1 Manuell – durch den Administrator initiiert

Das Gerät ermöglicht Ihnen, die Geräte-Software mit wenigen Mausklicks zu aktualisieren. Voraussetzung ist, dass sich die Image-Datei der Geräte-Software im externen Speicher befindet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Software*.
- ☐ Markieren Sie in der Tabelle die Zeile, die den Namen der gewünschten Image-Datei im externen Speicher zeigt.
- ☐ Rechtsklicken Sie, um das Kontextmenü anzuzeigen.
- ☐ Um den Update-Vorgang zu starten, klicken Sie im Kontextmenü den Eintrag *Update*.
  Die gegenwärtig ausgeführte Geräte-Software kopiert das Gerät in den Backup-Bereich.
  Sobald der Update-Vorgang erfolgreich beendet ist, zeigt das Gerät eine Information, dass die Software erfolgreich aktualisiert wurde.
  Beim nächsten Neustart lädt das Gerät die installierte Geräte-Software.

6.3.2 Automatisch – durch das Gerät initiiert

Wenn sich folgende Dateien im externen Speicher befinden, aktualisiert das Gerät beim Neustart die Geräte-Software automatisch:

- die Image-Datei der Geräte-Software
- eine Textdatei `startup.txt` mit dem Inhalt `autoUpdate=<Name_der_Image-Datei>.bin`

Voraussetzung ist, dass im Dialog *Grundeinstellungen > Externer Speicher* das Kontrollkästchen in Spalte *Automatisches Software-Update* markiert ist. Dies ist die Voreinstellung im Gerät.

Führen Sie die folgenden Schritte aus:

- ☐ Kopieren Sie die Image-Datei der neuen Geräte-Software in das Hauptverzeichnis des externen Speichers. Verwenden Sie ausschließlich eine für das Gerät bestimmte Image-Datei.
- ☐ Erzeugen Sie eine Textdatei mit dem Namen `startup.txt` im Hauptverzeichnis des externen Speichers.
- ☐ Öffnen Sie die Datei `startup.txt` im Texteditor und fügen Sie folgende Zeile ein: `autoUpdate=<Name_der_Image-Datei>.bin`
- ☐ Installieren Sie den externen Speicher im Gerät.

☐ Starten Sie das Gerät neu.
Während des Boot-Vorgangs prüft das Gerät automatisch folgende Kriterien:
- Ist ein externer Speicher angeschlossen?
- Befindet sich im Hauptverzeichnis des externen Speichers eine Datei `startup.txt`?
- Existiert die Image-Datei, die in der Datei `startup.txt` angegeben ist?
- Ist die Software-Version der Image-Datei aktueller als die gegenwärtig im Gerät ausgeführte Software?

Wenn die Kriterien erfüllt sind, startet das Gerät den Update-Vorgang.
Die gegenwärtig ausgeführte Geräte-Software kopiert das Gerät in den Backup-Bereich.
Sobald der Update-Vorgang erfolgreich beendet ist, startet das Gerät selbstständig neu und lädt die neue Software-Version.

☐ Kontrollieren Sie das Ergebnis des Update-Vorgangs. Die Log-Datei im Dialog *Diagnose* > Bericht > *System-Log* enthält eine der folgenden Meldungen:
- `S_watson_AUTOMATIC_SWUPDATE_SUCCESS`
  Software-Update erfolgreich beendet
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED`
  Software-Update abgebrochen
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE`
  Software-Update aufgrund falscher Image-Datei abgebrochen
- `S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE`
  Software-Update abgebrochen, weil das Gerät die Image-Datei nicht gespeichert hat.

6.4 Frühere Software-Version laden

Das Gerät ermöglicht Ihnen, die Geräte-Software durch eine frühere Version zu ersetzen. Nach dem Ersetzen der Geräte-Software bleiben die Grundeinstellungen im Gerät erhalten.

Anmerkung: Die Einstellungen von Funktionen, die ausschließlich in der neueren Geräte-Software-Version zur Verfügung stehen, gehen verloren.

7 Ports konfigurieren

Folgende Funktionen für die Port-Konfiguration stehen zur Verfügung:
- Port ein-/ausschalten
- Betriebsart wählen
- Gigabit-Ethernet-Modus für Ports

7.1 Port ein-/ausschalten

In der Voreinstellung ist jeder Port eingeschaltet. Um die Zugriffssicherheit zu erhöhen, deaktivieren Sie Ports, die nicht angeschlossen sind. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Um einen Port einzuschalten, markieren Sie das Kontrollkästchen in Spalte *Port an*.
- ☐ Um einen Port auszuschalten, heben Sie die Markierung des Kontrollkästchens in Spalte *Port an* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`no shutdown`	Aktivieren der Schnittstelle

7.2 Betriebsart wählen

In der Voreinstellung befinden sich die Ports im Betriebsmodus *Automatische Konfiguration*.

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

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Wenn das an diesem Port angeschlossene Gerät eine feste Einstellung voraussetzt, dann führen Sie anschließend die folgenden Schritte aus:
  - ☐ Deaktivieren Sie die Funktion. Heben Sie die Markierung des Kontrollkästchens in Spalte *Automatische Konfiguration* auf.
  - ☐ Legen Sie in Spalte *Manuelle Konfiguration* die Betriebsart (Übertragungsgeschwindigkeit, Duplexbetrieb) fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`no auto-negotiate`	Ausschalten des Modus für die automatische Konfiguration.
`speed 100 full`	Port-Geschwindigkeit 100 MBit/s, Vollduplex

7.3 Gigabit-Ethernet-Modus für Ports

Das Gerät unterstützt 2.5 GBit/s an ausgewählten Ports mit einem der folgenden SFP-Transceiver:
- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

Der Transceiver-Typ, der in den Steckplatz gesteckt ist, bestimmt die Port-Geschwindigkeit. Das Gerät hat keine Möglichkeit, die Geschwindigkeit manuell festzulegen. Ports mit 2.5 Gbit/s Port-Geschwindigkeit unterstützen keine Datenraten von 100 Mbit/s.

Anmerkung: Weitere Informationen zu den Transceiver-Bestellnummern finden Sie im Anwender-Handbuch „Installation“, Kapitel „Zubehör“.

7.3.1 Beispiel

Mit dem Gigabit-Ethernet-Modus erreichen Sie eine höhere Bandbreite auf den Uplinks. Um diese Funktion zu nutzen, stecken Sie einen geeigneten Transceiver-Typ in den jeweils vorgesehenen Steckplatz.

Führen Sie die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.

Die Spalte *Manuelle Konfiguration* zeigt den Wert `2.5 Gbit/s FDX` für Ports, die mit einem 2.5-Gbit/s-SFP-Transceiver ausgestattet sind.

Sie haben keine Möglichkeit, die Geschwindigkeit zu ändern.

```
show port 1/1
```

Anzeige der Parameter für Slot `1` Port `1`. Der Eintrag `Physical Mode` zeigt den Wert `2500 full` für Ports, die mit einem 2.5-Gbit/s-SFP-Transceiver ausgestattet sind.

```
Interface.....................1/1
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................2500 full
Physical Status...............-
```

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
- Ethernet Switch Configurator ausschalten
- IP Zugriffsbeschränkung aktivieren
- Session-Timeouts anpassen

8.1 SNMPv1/v2-Community ändern

SNMPv1/v2 arbeitet unverschlüsselt. Jedes SNMP-Paket enthält die IP-Adresse des Absenders und im Klartext den Community-Namen, mit dem der Absender auf das Gerät zugreift. Wenn SNMPv1/v2 eingeschaltet ist, ermöglicht das Gerät jedem, der den Community-Namen kennt, den Zugriff auf das Gerät.

Voreingestellt sind die Community-Namen `user` für Lese-Zugriffe und `admin` für Schreib-Zugriffe. Wenn Sie SNMPv1 oder SNMPv2 verwenden, dann ändern Sie die voreingestellten Community-Namen. Behandeln Sie die Community-Namen vertraulich. Führen Sie dazu die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > SNMPv1/v2 Community*.

Der Dialog zeigt die eingerichteten Communitys.

☐ Legen Sie für die `Write`-Community in Spalte *Name* den Community-Namen fest.

- Erlaubt sind bis zu 32 alphanumerische Zeichen.
- Das Gerät unterscheidet zwischen Groß- und Kleinschreibung.
- Legen Sie einen anderen Community-Namen fest als für Lesezugriffe.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`snmp community rw <community name>`	Community für Lese-/Schreibzugriffe festlegen.
`show snmp community`	Eingerichtete Communities anzeigen.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

8.2 SNMPv1/v2 ausschalten

Wenn Sie SNMPv1 oder SNMPv2 benötigen, dann verwenden Sie diese Protokolle ausschließlich in abhörsicheren Umgebungen. SNMPv1 und SNMPv2 verwenden keine Verschlüsselung. Die SNMP-Pakete enthalten die Community im Klartext. Wir empfehlen, im Gerät SNMPv3 zu nutzen und den Zugriff über SNMPv1 und SNMPv2 auszuschalten. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SNMP*.

Der Dialog zeigt die Einstellungen des SNMP-Servers.

- ☐ Um das Protokoll SNMPv1 zu deaktivieren, heben Sie die Markierung des Kontrollkästchens *SNMPv1* auf.
- ☐ Um das Protokoll SNMPv2 zu deaktivieren, heben Sie die Markierung des Kontrollkästchens *SNMPv2* auf.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`no snmp access version v1`	Deaktivieren des Protokolls SNMPv1.
`no snmp access version v2`	Deaktivieren des Protokolls SNMPv2.
`show snmp access`	Einstellungen des SNMP-Servers anzeigen.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten” Konfigurationsprofil.

8.3 HTTP ausschalten

Der Webserver liefert die grafische Benutzeroberfläche mit dem Protokoll HTTP oder HTTPS aus. HTTP-Verbindungen sind im Gegensatz zu HTTPS-Verbindungen unverschlüsselt.

Per Voreinstellung ist das Protokoll HTTP eingeschaltet. Wenn Sie HTTP ausschalten, ist kein unverschlüsselter Zugriff auf die grafische Benutzeroberfläche mehr möglich. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTP*.
- ☐ Um das Protokoll HTTP auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`no http server`	Ausschalten des Protokolls HTTP.

Wenn das Protokoll HTTP ausgeschaltet ist, erreichen Sie die grafische Benutzeroberfläche des Geräts ausschließlich über HTTPS. In der Adresszeile des Web-Browsers fügen Sie vor der IP-Adresse des Geräts die Zeichenfolge `https://` ein.

Wenn das Protokoll HTTPS ausgeschaltet ist und Sie auch HTTP ausschalten, dann ist die grafische Benutzeroberfläche unerreichbar. Um mit der grafischen Benutzeroberfläche zu arbeiten, schalten Sie den HTTPS-Server mit dem Command Line Interface ein. Führen Sie dazu die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`https server`	Einschalten des Protokolls HTTPS.

8.4 Telnet ausschalten

Das Gerät ermöglicht Ihnen, über Telnet oder SSH per Fernzugriff auf das Management des Geräts zuzugreifen. Telnet-Verbindungen sind im Gegensatz zu SSH-Verbindungen unverschlüsselt.

Per Voreinstellung ist der Telnet-Server im Gerät eingeschaltet. Wenn Sie Telnet ausschalten, ist kein unverschlüsselter Fernzugriff auf das Command Line Interface mehr möglich. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *Telnet*.
- ☐ Um den Telnet-Server auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`no telnet server`	Ausschalten des Telnet-Servers.

Wenn der SSH-Server ausgeschaltet ist und Sie auch Telnet ausschalten, dann ist der Zugriff auf das Command Line Interface ausschließlich über die serielle Schnittstelle des Geräts möglich. Um per Fernzugriff mit dem Command Line Interface zu arbeiten, schalten Sie SSH ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Um den *SSH*-Server einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ssh server`	Einschalten des SSH-Servers.

8.5 Ethernet Switch Configurator-Zugriff ausschalten

Ethernet Switch Configurator ermöglicht Ihnen, dem Gerät bei der Inbetriebnahme seine IP-Parameter über das Netz zuzuweisen. Ethernet Switch Configurator kommuniziert unverschlüsselt und ohne Authentifizierung im Management-VLAN.

Wir empfehlen, nach Inbetriebnahme des Geräts Ethernet Switch Configurator ausschließlich Leserechte zu gewähren oder den Ethernet Switch Configurator-Zugriff vollständig auszuschalten. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Netz*.
- ☐ Um der Ethernet Switch Configurator-Software die Schreibrechte zu entziehen, legen Sie im Rahmen *Ethernet Switch Configurator Protokoll v1/v2*, Feld *Zugriff* den Wert `readOnly` fest.
- ☐ Um den Ethernet Switch Configurator-Zugriff vollständig auszuschalten, wählen Sie im Rahmen *Ethernet Switch Configurator Protokoll v1/v2* das Optionsfeld *Aus*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network ethernet-switch-conf mode read-only`	Der Ethernet Switch Configurator-Software die Schreibrechte entziehen.
`no network ethernet-switch-conf operation`	Ethernet Switch Configurator-Zugriff ausschalten.

8.6 IP-Zugriffsbeschränkung aktivieren

Per Voreinstellung erreichen Sie das Management des Geräts von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle.

Die IP-Zugriffsbeschränkung ermöglicht Ihnen, den Zugriff auf das Management des Geräts auf ausgewählte IP-Adressbereiche und auf ausgewählte IP-basierte Protokolle zu beschränken.

Beispiel:

Das Gerät soll ausschließlich aus dem Firmennetz über die grafische Benutzeroberfläche erreichbar sein. Der Administrator soll zusätzlich Fernzugriff per SSH erhalten. Das Firmennetz hat den Adressbereich `192.168.1.0/24` und der Fernzugriff erfolgt aus einem Mobilfunknetz mit dem IP-Adressbereich `109.237.176.0/24`. Das SSH-Anwendungsprogramm kennt den Fingerprint des RSA-Schlüssels.

Tab. 20: Parameter für die IP-Zugriffsbeschränkung

Parameter	Firmennetz	Mobilfunknetz
Netzadresse	`192.168.1.0`	`109.237.176.0`
Netzmaske	`24`	`24`
Gewünschte Protokolle	https, snmp	ssh

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > IP-Zugriffsbeschränkung*.
- ☐ Heben Sie für den Eintrag in Spalte *Aktiv* die Markierung des Kontrollkästchens auf. Dieser Eintrag ermöglicht Benutzern den Zugriff auf das Gerät von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle.

Adressbereich des Firmennetzes:

- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Legen Sie den Adressbereich des Firmennetzes in Spalte *IP-Adressbereich* fest: `192.168.1.0/24`
- ☐ Deaktivieren Sie für den Adressbereich des Firmennetzes die ungewünschten Protokolle. Die Kontrollkästchen in den Feldern *HTTPS*, *SNMP* und *Aktiv* bleiben markiert.

Adressbereich des Mobilfunknetzes:

- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Legen Sie den Adressbereich des Mobilfunknetzes in Spalte *IP-Adressbereich* fest: `109.237.176.0/24`
- ☐ Deaktivieren Sie für den Adressbereich des Mobilfunknetzes die ungewünschten Protokolle. Die Kontrollkästchen in den Feldern *SSH* und *Aktiv* bleiben markiert.

Bevor Sie die Funktion einschalten, vergewissern Sie sich, dass mindestens ein aktiver Eintrag in der Tabelle Ihnen den Zugriff ermöglicht. Andernfalls bricht die Verbindung zum Gerät ab, sobald Sie die Einstellungen ändern. Der Zugriff auf das Management des Geräts ist ausschließlich mit dem Command Line Interface über die serielle Schnittstelle des Geräts möglich.

- ☐ Um die IP-Zugriffsbeschränkung einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`show network management access global`	Zeigt, ob die IP-Zugriffsbeschränkung eingeschaltet oder ausgeschaltet ist.
`show network management access rules`	Eingerichtete Einträge anzeigen.
`no network management access operation`	IP-Zugriffsbeschränkung ausschalten.
`network management access add 2`	Eintrag für den Adressbereich des Firmennetzes erzeugen. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: `2`.
`network management access modify 2 ip 192.168.1.0`	IP-Adresse des Firmennetzes festlegen.
`network management access modify 2 mask 24`	Netzmaske des Firmennetzes festlegen.
`network management access modify 2 ssh disable`	SSH für den Adressbereich des Firmennetzes deaktivieren. Schritt für jedes ungewünschte Protokoll wiederholen.
`network management access add 3`	Eintrag für den Adressbereich des Mobilfunknetzes erzeugen. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: `3`.
`network management access modify 3 ip 109.237.176.0`	IP-Adresse des Mobilfunknetzes festlegen.
`network management access modify 3 mask 24`	Netzmaske des Mobilfunknetzes festlegen.
`network management access modify 3 snmp disable`	SNMP für den Adressbereich des Mobilfunknetzes deaktivieren. Schritt für jedes ungewünschte Protokoll wiederholen.
`no network management access status 1`	Voreingestellten Eintrag deaktivieren. Dieser Eintrag ermöglicht Benutzern den Zugriff auf das Gerät von jeder beliebigen IP-Adresse und über sämtliche unterstützten Protokolle.
`network management access status 2`	Eintrag für den Adressbereich des Firmennetzes aktivieren.
`network management access status 3`	Eintrag für den Adressbereich des Mobilfunknetzes aktivieren.
`show network management access rules`	Eingerichtete Einträge anzeigen.
`network management access operation`	IP-Zugriffsbeschränkung einschalten.

8.7 Session-Timeouts anpassen

Das Gerät ermöglicht Ihnen, bei Inaktivität eines angemeldeten Benutzers die Sitzung automatisch zu beenden. Das Session-Timeout ist die Zeit der Inaktivität nach der letzten Benutzeraktion.

Ein Session-Timeout können Sie für folgende Anwendungen festlegen:
- Command Line Interface: Sessions über eine SSH-Verbindung
- Command Line Interface: Sessions über eine Telnet-Verbindung
- Command Line Interface: Sessions über eine serielle Verbindung
- Grafische Benutzeroberfläche

Timeout im Command Line Interface für Sessions über eine SSH-Verbindung

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Session-Timeout [min]* die Timeout-Zeit in Minuten fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ssh timeout <0..160>`	Timeout-Zeit in Minuten festlegen für Sessions im Command Line Interface über eine SSH-Verbindung.

Timeout im Command Line Interface für Sessions über eine Telnet-Verbindung

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *Telnet*.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Session-Timeout [min]* die Timeout-Zeit in Minuten fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`telnet timeout <0..160>`	Timeout-Zeit in Minuten festlegen für Sessions im Command Line Interface über eine Telnet-Verbindung.

Timeout im Command Line Interface für Sessions über eine serielle Verbindung

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > CLI*, Registerkarte *Global*.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Timeout serielle Schnittstelle [min]* die Timeout-Zeit in Minuten fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`cli serial-timeout <0..160>`	Timeout-Zeit in Minuten festlegen für Sessions im Command Line Interface über eine serielle Verbindung.

Session-Timeout für die grafische Benutzeroberfläche

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Web*.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Web-Interface Session-Timeout [min]* die Timeout-Zeit in Minuten fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network management access web timeout <0..160>`	Timeout-Zeit in Minuten festlegen für Sitzungen mit der grafischen Benutzeroberfläche.

9 Datenverkehr kontrollieren

Das Gerät prüft die zur Weiterleitung bestimmten Datenpakete nach vorgegebenen Regeln. Wenn Datenpakete diesen Regeln entsprechen, leitet das Gerät die Pakete weiter oder blockiert sie. Wenn Datenpakete keinen Regeln entsprechen, blockiert das Gerät die Pakete.

Routing-Ports, denen keine Regeln zugewiesen sind, lassen Pakete passieren. Sobald eine Regel zugewiesen ist, werden zuerst die zugewiesenen Regeln abgearbeitet. Danach wirkt die festgelegte Standard-Aktion des Geräts.

Zur Kontrolle des Datenstroms bietet das Gerät folgende Funktionen:
- Prüfen der Dienstanforderungen (Denial of Service, DoS)
- Verweigern des Zugriffes auf Geräte auf der Grundlage ihrer IP- oder MAC-Adresse (Zugriffkontrollliste)

Das Gerät beobachtet und überwacht den Datenstrom. Aus den Ergebnissen der Beobachtung und Überwachung sowie aus den Regeln für die Netzsicherheit erzeugt das Gerät eine sogenannte Zustandstabelle. Anhand dieser Zustandstabelle entscheidet das Gerät, ob es die Daten vermittelt, verwirft oder zurückweist.

Die Datenpakete durchlaufen die Filter-Funktionen des Geräts in folgender Reihenfolge:
- DoS … wenn `permit` oder `accept`, dann weiter zur nächsten Regel
- ACL … wenn `permit` oder `accept`, dann weiter zur nächsten Regel

9.1 Unterstützung beim Schutz vor Denial of Service (DoS)

Mit dieser Funktion unterstützt Sie das Gerät beim Schutz vor ungültigen oder gefälschten Datenpaketen, die auf bestimmte Dienste oder Geräte abzielen. Sie haben die Möglichkeit, Filter festzulegen, die den Datenstrom zum Schutz vor Denial-of-Service-Angriffen begrenzen. Die aktivierten Filter prüfen eingehende Datenpakete und verwerfen diese, sobald sich eine Übereinstimmung zu den Filterkriterien ergibt.

Der Dialog *Netzsicherheit > DoS > Global* beinhaltet 2 Rahmen, in denen Sie die unterschiedlichen Filter aktivieren können. Zum Aktivieren markieren Sie die betreffenden Kontrollkästchen.

Im Rahmen *TCP/UDP* können Sie bis zu 4 Filter aktivieren, die ausschließlich auf TCP-und UDP-Pakete Einfluss nehmen. Mittels dieser Filter können Sie die Port-Scans deaktivieren, mit deren Hilfe Angreifer versuchen könnten, Geräte und angebotene Dienste zu erkennen. Die Filter arbeiten wie folgt:

Tab. 21: DoS-Filter für TCP-Pakete

Filter	Aktion
Null-Scan-Filter aktivieren	Das Gerät erkennt und verwirft eingehende TCP-Datenpakete mit den folgenden Eigenschaften: ▶ Keine TCP-Flags sind gesetzt. ▶ Die TCP-Sequenznummer ist 0.
Xmas-Filter aktivieren	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.
SYN/FIN-Filter aktivieren	Das Gerät erkennt und verwirft TCP-Pakete, bei denen die TCP-Flags *SYN* und *FIN* gleichzeitig gesetzt sind.
Minimal-Header-Filter aktivieren	Das Gerät erkennt und verwirft eingehende TCP-Pakete, bei denen der TCP-Header zu kurz ist.

Der Rahmen *ICMP* bietet Ihnen 2 Filtermöglichkeiten für ICMP-Pakete. Die Fragmentierung eingehender ICMP-Pakete lässt grundsätzlich auf einen Angriff schließen. Wenn Sie diesen Filter aktivieren, erkennt das Gerät fragmentierte ICMP-Pakete und verwirft diese. Über den Parameter *Erlaubte Payload-Größe [Byte]* können Sie zudem die maximal zulässige Größe der Nutzlast von ICMP-Paketen festlegen. Das Gerät verwirft Datenpakete, welche diese Byte-Angabe überschreiten.

Anmerkung: Sie können die Filter im Dialog *Netzsicherheit > DoS > Global* beliebig kombinieren. Bei Auswahl mehrerer Filter gilt ein logisches Oder: Das Gerät verwirft ein Datenpaket, wenn es auf den ersten oder den zweiten (oder den dritten usw.) Filter zutrifft.

9.2 ACL

In diesem Menü haben Sie die Möglichkeit, die Parameter für die Access-Control-Listen (ACL) einzufügen.

Das Gerät verwendet ACLs, um Datenpakete zu filtern, die es in VLANs oder auf einzelnen oder mehreren Ports empfängt. In einer ACL legen Sie Regeln fest, anhand derer das Gerät Datenpakete filtert. Wenn eine solche Regel auf ein Paket zutrifft, wendet das Gerät die in der Regel festgelegten Aktionen auf das Paket an. Die folgenden Aktionen sind verfügbar:
- zulassen (`permit`)
- verwerfen (`deny`)
- umleiten an einen bestimmten Port (siehe Feld *Redirection-Port*)
- spiegeln (siehe Feld *Mirror-Port*)

Die folgende Liste enthält Kriterien, anhand derer Sie die Datenpakete filtern können:
- Quell- oder Zieladresse eines Pakets (MAC)
- Quell- oder Zieladresse eines Datenpakets (IPv4)
- 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 einem Interface eine IP-ACL und eine MAC-ACL zuweisen, wendet das Gerät zuerst die IP-ACL an, um den Datenstrom zu filtern. Nachdem die Pakete durch die IP-ACL gefiltert sind, wendet das Gerät die MAC-ACL-Regeln an. Die Priorität einer ACL und der Index einer Regel sind voneinander unabhängig.

Innerhalb einer ACL verarbeitet das Gerät die Regeln der Reihe nach. Der Index der jeweiligen Regel bestimmt die Reihenfolge, in welcher das Gerät den Datenstrom filtert. Wenn Sie einem Port oder VLAN eine ACL zuweisen, können Sie deren Priorität mit der Index-Nummer festlegen. Je kleiner die Zahl, desto höher die Priorität. Das Gerät verarbeitet zuerst die Regel mit höherer Priorität.

Wenn keine der in einer ACL festgelegten Regeln auf ein Datenpaket zutrifft, gilt die implizite `deny`-Regel. Infolgedessen verwirft das Gerät empfangene Datenpakete.

Beachten Sie, dass das Gerät die implizite `deny`-Regel direkt implementiert.

Anmerkung: Die Anzahl der verfügbaren ACLs ist geräteabhängig. Weitere Informationen zu den ACLs finden Sie im Kapitel „Technische Daten” auf Seite 379.

Anmerkung: Eine einzelne ACL können Sie beliebig vielen Port oder VLANs zuweisen.

Das Menü *ACL* enthält die folgenden Dialoge:
- *ACL IPv4-Regel*
- *ACL MAC-Regel*
- *ACL Zuweisung*

Diese Dialoge bieten folgende Möglichkeiten:
- Die Regeln für die einzelnen ACL-Typen festlegen.
- Die Regeln mit den erforderlichen Prioritäten versehen.
- Die ACLs den Ports oder VLANs zuweisen.

9.2.1 Erzeugen und Bearbeiten von IPv4-Regeln

Beim Filtern von IPv4-Datenpaketen ermöglicht Ihnen das Gerät:
- Erzeugen von neuen Gruppen und Regeln
- Hinzufügen von neuen Regeln zu vorhandenen Gruppen
- Bearbeiten einer vorhandenen Regel
- Aktivieren und Deaktivieren von Gruppen und Regeln
- Löschen von vorhandenen Gruppen und Regeln
- Ändern der Reihenfolge der vorhandenen Regeln

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > ACL > IPv4-Regel*.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Um eine Gruppe zu erzeugen, legen Sie im Feld *Gruppenname* einen aussagekräftigen Namen fest. In einer Gruppe können Sie mehrere Regeln zusammenfassen.
- ☐ Um die Regel einer vorhandenen Gruppe hinzuzufügen, wählen Sie im Feld *Gruppenname* den Namen der Gruppe aus.
- ☐ 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 Tabelle hinzu.
  Gruppe und Regel sind sofort aktiv.
  Um Gruppe oder Regel zu deaktivieren, heben Sie in Spalte *Aktiv* die Markierung des Kontrollkästchens auf.
  Um eine Regel zu entfernen, markieren Sie den betreffenden Tabelleneintrag und klicken die Schaltfläche  .
- ☐ Bearbeiten Sie die Parameter der Regel in der Tabelle.
  Um einen Wert zu ändern, doppelklicken Sie in das betreffende Feld.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

Anmerkung: Das Gerät ermöglicht Ihnen, in den Parametern *Quell-IP-Adresse* und *Ziel-IP-Adresse* Platzhalter zu verwenden. Wenn Sie zum Beispiel `192.168.?.?` einfügen, lässt das Gerät Adressen zu, die mit `192.168` beginnen.

Anmerkung: Voraussetzung für das Ändern der Werte in Spalte *Quell-TCP/UDP-Port* und *Ziel-TCP/UDP-Port* ist, dass Sie in Spalte *Protokoll* den Wert `tcp` oder `udp` festlegen.

Anmerkung: Voraussetzung für das Ändern des Werts in Spalte *Redirection-Port* und *Mirror-Port* ist, dass Sie in Spalte *Aktion* den Wert `permit` festlegen.

9.2.2 Erzeugen und Konfigurieren einer IP-ACL im Command Line Interface

In dem folgenden Beispiel konfigurieren Sie ACLs dahingehend, dass sie Kommunikation von Rechnern B und C zu Rechner A über IP (TCP, UDP usw.) blockieren.

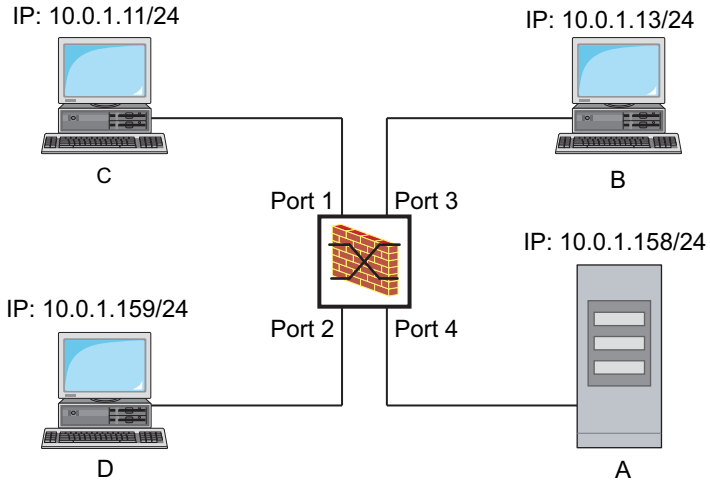


Abb. 22: Beispiel einer IP-ACL

Führen Sie die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	IP-ACL mit dem Namen `filter1` einfügen. Regel hinzufügen, die IP-Datenpakete von `10.0.1.11` bis `10.0.1.158` ablehnt. Priorität `1` (höchste Priorität).
`ip access-list extended name filter1 permit src any dst any`	Der IP-ACL eine Regel hinzufügen, die IP-Datenpakete erlaubt.
`show access-list ip filter1`	Regeln der IP-ACL `filter1` anzeigen.
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	IP-ACL mit dem Namen `filter2` einfügen. Regel hinzufügen, die IP-Datenpakete von `10.0.1.13` bis `10.0.1.158` ablehnt. Priorität `1` (höchste Priorität).
`show access-list ip filter2`	Regeln der IP-ACL `filter2` anzeigen.

9.2.3 Erzeugen und Bearbeiten von MAC-Regeln

Beim Filtern von MAC-Datenpaketen ermöglicht Ihnen das Gerät:
- Erzeugen von neuen Gruppen und Regeln
- Hinzufügen von neuen Regeln zu vorhandenen Gruppen
- Bearbeiten einer vorhandenen Regel
- Aktivieren und Deaktivieren von Gruppen und Regeln
- Löschen von vorhandenen Gruppen und Regeln
- Ändern der Reihenfolge der vorhandenen Regeln

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > ACL > MAC-Regel*.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Um eine Gruppe zu erzeugen, legen Sie im Feld *Gruppenname* einen aussagekräftigen Namen fest. In einer Gruppe können Sie mehrere Regeln zusammenfassen.
- ☐ Um die Regel einer vorhandenen Gruppe hinzuzufügen, wählen Sie im Feld *Gruppenname* den Namen der Gruppe aus.
- ☐ 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 Tabelle hinzu.
  Gruppe und Regel sind sofort aktiv.
  Um Gruppe oder Regel zu deaktivieren, heben Sie in Spalte *Aktiv* die Markierung des Kontrollkästchens auf.
  Um eine Regel zu entfernen, markieren Sie den betreffenden Tabelleneintrag und klicken die Schaltfläche  .
- ☐ Bearbeiten Sie die Parameter der Regel in der Tabelle.
  Um einen Wert zu ändern, doppelklicken Sie in das betreffende Feld.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

Anmerkung: In den Feldern *Quell-MAC-Adresse* und *Ziel-MAC-Adresse* können Sie Platzhalter in der Form `FF:??:??:??:??:??` oder `??:??:??:??:00:01` verwenden. Verwenden Sie hier Großbuchstaben.

9.2.4 Erzeugen und Konfigurieren einer MAC-ACL im Command Line Interface

Das Beispiel sieht vor, dass AppleTalk und IPX aus dem gesamten Netz gefiltert werden. Führen Sie dazu die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mac acl add 1 macfilter`	Fügt eine MAC-ACL mit ID `1` und dem Namen `macfilter` ein.
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	Fügt eine Regel an Position `1` in der MAC-ACL mit ID `1` ein, die Pakete mit Ethertype `0x809B (AppleTalk)` abweist.
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	Fügt eine Regel an Position `2` in der MAC-ACL mit ID `1` ein, die Pakete mit Ethertype `0x8137 (IPX alt)` abweist.
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	Fügt eine Regel an Position `3` in der MAC-ACL mit ID `1` ein, die Pakete mit Ethertype `0x8138 (IPX)` abweist.
`mac acl rule add 1 4 permit src any any dst any any`	Fügt eine Regel an Position `4` in der MAC-ACL mit ID `1` ein, die Pakete weiterleitet.
`show acl mac rules 1`	Zeigt die Regeln der MAC-ACL mit ID `1`.
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	Wechsel in den Interface-Konfigurationsmodus der Interfaces `1/1` bis `1/6`.

`acl mac assign 1 in 1`	Weist die MAC-ACL mit ID `1` den auf den Interfaces `1/1` bis `1/6` empfangenen Datenpaketen (`in`) zu.
`exit`	Verlässt den Interface-Modus.
`show acl mac assignment 1`	Zeigt die Zuweisung von Interfaces/VLANS der MAC-ACL mit ID `1`.

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 *Erzeugen*.
  - ☐ Legen Sie im Feld *Port/VLAN* den gewünschten Port oder das gewünschte VLAN fest.
  - ☐ Legen Sie im Feld *Priorität* die Priorität fest.
  - ☐ Legen Sie im Feld *Richtung* fest, auf welche Datenpakete das Gerät die Regel anwendet.
  - ☐ Legen Sie im Feld *Gruppenname* fest, welche Regel das Gerät dem Port oder dem VLAN zuweist.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

9.3 MAC-Authentication-Bypass

Die Funktion *MAC-Authorized-Bypass* ermöglicht Clients, die 802.1X nicht unterstützen, zum Beispiel Drucker und Faxgeräte, sich mit ihrer MAC-Adresse im Netz zu authentifizieren. Das Gerät ermöglicht Ihnen, das Format der MAC-Adressen festzulegen, mit der sich die Clients beim RADIUS-Server authentifizieren.

Beispiel:

Unterteilen Sie die MAC-Adresse in 6 Gruppen mit je 2 Zeichen. Verwenden Sie Großbuchstaben und einen Doppelpunkt als Trennzeichen: `AA:BB:CC:DD:EE:FF`

Verwenden Sie das Passwort `xY-45uM_e`. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Global*.
  Führen Sie im Rahmen *Formatoptionen MAC Authentication Bypass* die folgenden Schritte aus:
- ☐ Wählen Sie in der Dropdown-Liste *Gruppen-Größe* den Wert `2`.
  Das Gerät unterteilt die MAC-Adresse in 6 Gruppen mit je 2 Zeichen.
- ☐ Wählen Sie in der Dropdown-Liste *Gruppen-Trennzeichen* das Zeichen `:`.
- ☐ Wählen Sie in der Dropdown-Liste *Groß-/Kleinschreibung* den Eintrag `upper-case`.
- ☐ Geben Sie im Feld *Passwort* das Passwort `xY-45uM_e` ein.
  Das Gerät verwendet dieses Passwort für jeden Client, der sich beim RADIUS-Server authentifiziert. Wenn Sie das Feld leer lassen, dann verwendet das Gerät die formatierte MAC-Adresse auch als Passwort.
- ☐ Um die Einstellungen flüchtig zu speichern, klicken Sie die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dot1x mac-authentication-bypass format group-size 2`	Festlegen, dass die Gruppen jeweils `2` Zeichen enthalten.
`dot1x mac-authentication-bypass format group-separator :`	Das Trennzeichen `:` festlegen.
`dot1x mac-authentication-bypass format letter-case upper-case`	Festlegen, dass das Gerät die Authentifizierungsdaten in Großbuchstaben formatiert.
`dot1x mac-authentication-bypass password xY-45uM_e`	Das Passwort `xY-45uM_e` festlegen. Das Gerät verwendet dieses Passwort, um jeden Client auf dem RADIUS-Server zu authentifizieren.

10 Netzlaststeuerung

Das Gerät bietet Ihnen eine Reihe von Funktionen, die Ihnen helfen können, die Netzlast zu reduzieren:

- Gezielte Paketvermittlung
- Multicasts
- Lastbegrenzung
- Priorisierung - QoS
- Flusskontrolle

10.1 Gezielte Paketvermittlung

Durch gezielte Paketvermittlung reduziert das Gerät die Netzlast.

An jedem seiner Ports lernt das Gerät die Absender-MAC-Adresse empfangener Datenpakete. Die Kombination „Port und MAC-Adresse“ speichert das Gerät in seiner MAC-Adresstabelle (FDB).

Durch Anwenden des „Store and Forward“-Verfahrens speichert das Gerät empfangene Daten zwischen und prüft sie vor dem Weiterleiten auf Gültigkeit. Ungültige und fehlerhafte Datenpakete verwirft das Gerät.

10.1.1 Lernen der MAC-Adressen

Wenn das Gerät ein Datenpaket empfängt, prüft es, ob die MAC-Adresse des Absenders bereits in der MAC-Adresstabelle (FDB) gespeichert ist. Ist die MAC-Adresse des Absenders noch unbekannt, erzeugt das Gerät einen neuen Eintrag. Anschließend vergleicht das Gerät die Ziel-MAC-Adresse des Datenpakets mit den in der MAC-Adresstabelle (FDB) gespeicherten Einträgen:

- Datenpakete mit bekannter Ziel-MAC-Adresse vermittelt das Gerät gezielt an Ports, die bereits Datenpakete von dieser MAC-Adresse empfangen haben.
- Datenpakete mit unbekannter Zieladresse flutet das Gerät, d. h. das Gerät leitet diese Datenpakete an jeden Port weiter.

10.1.2 Aging gelernter MAC-Adressen

Adressen, die das Gerät seit einer einstellbaren Zeitspanne (Aging-Zeit) nicht noch einmal erkannt hat, löscht das Gerät aus der MAC-Adresstabelle (FDB). Ein Neustart oder das Zurücksetzen der MAC-Adresstabelle löscht die Einträge in der MAC-Adresstabelle (FDB).

10.1.3 Statische Adresseinträge

Ergänzend zum Lernen der Absender-MAC-Adresse bietet Ihnen das Gerät die Möglichkeit, MAC-Adressen von Hand einzurichten. Diese MAC-Adressen bleiben eingerichtet und überdauern das Zurücksetzen der MAC-Adresstabelle (FDB) sowie den Neustart des Geräts.

Anhand von statischen Adresseinträgen bietet Ihnen das Gerät die Möglichkeit, Datenpakete gezielt an ausgewählte Ports zu vermitteln. Wenn Sie keinen Ziel-Port festlegen, verwirft das Gerät betreffende Datenpakete.

Die statischen Adresseinträge verwalten Sie in der grafischen Benutzeroberfläche oder im Command Line Interface.

Führen Sie die folgenden Schritte aus:

☐ Statischen Adresseintrag erzeugen.

☐ Öffnen Sie den Dialog *Switching > Filter für MAC-Adressen*.

☐ Fügen Sie eine benutzerdefinierte MAC-Adresse hinzu:

- Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
- Legen Sie im Feld *Adresse* die Ziel-MAC-Adresse fest.
- Legen Sie im Feld *VLAN-ID* die ID des VLANs fest.
- Markieren Sie in der Liste *Port* die Ports, an die das Gerät Datenpakete mit der angegebenen Ziel-MAC-Adresse im angegebenen VLAN vermittelt.
  Markieren Sie genau einen Port, wenn Sie im Feld *Adresse* eine Unicast-MAC-Adresse festgelegt haben.
  Markieren Sie einen oder mehrere Ports, wenn Sie im Feld *Adresse* eine Multicast-MAC-Adresse festgelegt haben.
  Markieren Sie keinen Port, damit das Gerät Datenpakete mit der Ziel-MAC-Adresse verwirft.
- Klicken Sie die Schaltfläche *Ok*.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mac-filter <MAC address> <VLAN ID>`	Erzeugen des MAC-Adressfilters, bestehend aus MAC-Adresse und VLAN-ID.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`mac-filter <MAC address> <VLAN ID>`	Weist dem Port einen bereits erzeugten MAC-Adressfilter zu.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

☐ Gelernte MAC-Adresse in statischen Adresseintrag umwandeln.

☐ Öffnen Sie den Dialog *Switching > Filter für MAC-Adressen*.

☐ Um eine gelernte MAC-Adresse in einen statischen Adresseintrag umzuwandeln, markieren Sie in Spalte *Status* den Wert `permanent`.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

☐ Statischen Adresseintrag deaktivieren.

☐ Öffnen Sie den Dialog *Switching > Filter für MAC-Adressen*.

☐ Um einen statischen Adresseintrag zu deaktivieren, markieren Sie in Spalte *Status* den Wert `invalid`.

☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`no mac-filter <MAC address> <VLAN ID>`	Hebt auf dem Port die Zuweisung des MAC-Adressfilters auf.
`exit`	Wechsel in den Konfigurationsmodus.
`no mac-filter <MAC address> <VLAN ID>`	Löschen des MAC-Adressfilters, bestehend aus MAC-Adresse und VLAN-ID.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`save`	Speichern der Einstellungen im permanenten Speicher (`nvm`) im „ausgewählten" Konfigurationsprofil.

☐ Gelernte MAC-Adressen löschen.

☐ Um die gelernten Adressen aus der MAC-Adresstabelle (FDB) zu löschen, öffnen Sie den Dialog *Grundeinstellungen > Neustart* und klicken die Schaltfläche *MAC-Adresstabelle zurücksetzen*.

`clear mac-addr-table`	Löschen der gelernten MAC-Adressen aus der MAC-Adresstabelle (FDB).

10.2 Multicasts

In der Grundeinstellung flutet das Gerät Datenpakete mit einer Multicast-Adresse, d.h. das Gerät leitet diese Datenpakete an jeden Port weiter. Dies führt zu erhöhter Netzlast.

Durch den Einsatz von IGMP-Snooping lässt sich die Netzlast reduzieren, die der Multicast-Datenverkehr verursacht. IGMP-Snooping ermöglicht dem Gerät, Multicast-Datenpakete ausschließlich an diejenigen Ports zu vermitteln, an denen am Multicast „interessierte“ Geräte angeschlossenen sind.

10.2.1 Beispiel für eine Multicast-Anwendung

Überwachungskameras übertragen Bilder auf Monitore im Maschinenraum und im Überwachungsraum. Bei einer IP-Multicast-Übertragung senden die Kameras ihre Bilddaten in Multicast-Paketen über das Netz.

Das Internet Group Management Protocol (IGMP) organisiert den Multicast-Datenverkehr zwischen den Multicast-Routern und den Monitoren. Die Switches, die im Netz zwischen den Multicast-Routern und den Monitoren liegen, beobachten den IGMP-Datenverkehr kontinuierlich („IGMP Snooping“).

Switches registrieren Anmeldungen für den Empfang eines Multicast-Stroms (IGMP-Report). Daraufhin erzeugt das Gerät einen Eintrag in der MAC-Adresstabelle (FDB) und leitet Multicast-Pakete ausschließlich an die Ports weiter, an denen es zuvor IGMP-Reports empfangen hat.

10.2.2 IGMP-Snooping

Das Internet Group Management Protocol (IGMP) beschreibt die Verteilung von Multicast-Informationen zwischen Routern und angeschlossenen Empfängern auf Schicht 3. IGMP Snooping beschreibt die Funktion eines Switches, kontinuierlich den IGMP-Datenverkehr zu beobachten und die eigenen Vermittlungseinstellungen für diesen Datenverkehr zu optimieren.

Die Funktion *IGMP-Snooping* im Gerät funktioniert gemäß RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches).

Multicast-Router mit aktiver Funktion *IGMP* fordern periodisch zur Registrierung von Multicast-Strömen auf (Query), um die angeschlossenen IP-Multicast-Gruppen-Mitglieder zu ermitteln. IP-Multicast-Gruppen-Mitglieder antworten mit einer Report-Nachricht. Diese Report-Nachricht enthält für die Funktion *IGMP* notwendige Parameter. Der Multicast-Router trägt die IP-Multicast-Gruppen-Adresse aus der Report-Nachricht in seine Router-Tabelle ein. Dies bewirkt, dass er Datenpakete mit dieser IP-Multicast-Gruppen-Adresse im Zieladressfeld entsprechend seiner Router-Tabelle weiterleitet.

Empfänger melden sich beim Verlassen einer Multicast-Gruppe mit einer „Leave“-Nachricht ab (ab IGMP-Version 2) und senden keine Report-Nachrichten mehr. Der Multicast-Router entfernt den Routing-Tabelleneintrag eines Empfängers, wenn er innerhalb einer bestimmten Zeitspanne (Aging-Zeit) keine Report-Nachricht mehr von diesem empfängt.

Wenn mehrere IGMP-Multicast-Router im selben Netz sind, übernimmt das Gerät mit der kleineren IP-Adresse die Query-Funktion. Wenn sich kein Multicast-Router im Netz befindet, haben Sie die Möglichkeit, die Query-Funktion in einem entsprechend ausgestatteten Switch einzuschalten.

Ein Switch, der einen Multicast-Empfänger mit einem Multicast-Router verbindet, analysiert mit dem IGMP-Snooping-Verfahren die IGMP-Information.

Das IGMP-Snooping-Verfahren ermöglicht auch Switches, die Funktion *IGMP* zu nutzen. Ein Switch speichert die aus IP-Adressen gewonnen MAC-Adressen der Multicast-Empfänger als erkannte Multicast-Adressen in seiner MAC-Adresstabelle (FDB). Außerdem kenzeichnet der Switch die Ports, an denen er Reports für eine bestimmte Multicast-Adresse empfangen hat. Dadurch vermittelt der Switch Multicast-Pakete ausschließlich an Ports, an denen Multicast-Empfänger angeschlossen sind. Die anderen Ports bleiben frei von diesen Paketen.

Als Besonderheit bietet Ihnen das Gerät die Möglichkeit, die Verarbeitung von Datenpaketen mit unbekannten Multicast-Adressen zu bestimmen. Je nach Einstellung verwirft das Gerät diese Datenpakete oder vermittelt sie an jeden Port. In der Grundeinstellung überträgt das Gerät die Datenpakete ausschließlich an Ports mit angeschlossenen Geräten, die ihrerseits Query-Pakete empfangen. Sie haben außerdem die Möglichkeit, bekannte Multicast-Pakete zusätzlich an Query-Ports zu senden.

IGMP-Snooping einstellen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.

Wenn die Funktion *IGMP-Snooping* ausgeschaltet ist, dann verhält sich das Gerät wie folgt:
- ▶ Das Gerät ignoriert die empfangenen Query- und Report-Nachrichten.
- ▶ Das Gerät vermittelt (flutet) empfangene Datenpakete mit einer Multicast-Adresse als Zieladresse an jeden Port.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

☐ Einstellungen für einen Port festlegen:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Konfiguration*, Registerkarte *Port*.
- ☐ Um die Funktion *IGMP-Snooping* auf einem Port zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv* für den betreffenden Port.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

☐ Einstellungen für ein VLAN festlegen.

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Konfiguration*, Registerkarte *VLAN-ID*.
- ☐ Um die Funktion *IGMP-Snooping* für ein bestimmtes VLAN zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv* für das betreffende VLAN.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

IGMP-Querier-Funktion einstellen

Das Gerät versendet optional selber aktiv Query-Nachrichten, alternativ antwortet es auf Query-Nachrichten oder erkennt andere Multicast-Querier im Netz (Funktion *IGMP Snooping-Querier*).

Voraussetzung:

Die Funktion *IGMP-Snooping* ist global eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Querier*.
- ☐ Im Rahmen *Funktion* schalten Sie die Funktion *IGMP Snooping-Querier* des Geräts global ein oder aus.
- ☐ Um die Funktion *IGMP Snooping-Querier* für ein bestimmtes VLAN zu aktivieren, markieren Sie das Kontrollkästchen in Spalte *Aktiv* für das betreffende VLAN.
- ▶ Das Gerät führt einen einfachen Auswahlprozess durch: Wenn die IP-Quelladresse des anderen Multicast-Queriers niedriger ist als die eigene, wechselt das Gerät in den Passivzustand, in dem es keine Query-Anfragen mehr aussendet.
- ▶ In Spalte *Adresse* legen Sie die IP-Multicast-Adresse fest, die das Gerät als Absenderadresse in generierte Query-Abfragen einfügt. Verwenden Sie die Adresse des Multicast-Routers.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

IGMP-Snooping-Erweiterungen (Tabelle)

Der Dialog *Switching > IGMP-Snooping > Snooping Erweiterungen* gibt Ihnen Zugriff auf erweiterte Einstellungen für die Funktion *IGMP-Snooping*. Sie aktivieren oder deaktivieren die Einstellungen jeweils für einen Port in einem VLAN.

Folgende Einstellungen sind möglich:

- ▶ `Static`
  Mit dieser Einstellung legen Sie den Port als statischen Query-Port fest. An einen statischen Query-Port vermittelt das Gerät jede IGMP-Nachricht, auch wenn es an diesem Port zuvor keine IGMP-Query-Nachrichten empfangen hat. Bei deaktivierter Static-Option vermittelt das Gerät IGMP-Nachrichten an diesen Port ausschließlich dann, wenn es zuvor IGMP-Query-Nachrichten empfangen hat. Wenn das der Fall ist, zeigt der Eintrag ein `L` („learned“).
- ▶ `Learn by LLDP`
  Ein Port mit dieser Einstellung ermittelt automatisch andere Schneider Electric-Geräte über LLDP (Link Layer Discovery Protocol). Das Gerät lernt dann von diesen Schneider Electric-Geräten den IGMP-Query-Status auf diesem Port und konfiguriert die Funktion *IGMP Snooping-Querier* entsprechend. Der Eintrag `ALA` zeigt, dass die Funktion `Learn by LLDP` aktiviert ist. Wenn das Gerät auf diesem Port in diesem VLAN ein anderes Schneider Electric-Gerät gefunden hat, zeigt der Eintrag zusätzlich ein `A` („automatic“).
- ▶ `Forward All`
  Mit dieser Einstellung vermittelt das Gerät an diesen Port die Datenpakete, die an eine Multicast-Adresse adressiert sind. Die Einstellung ist zum Beispiel in folgenden Situationen geeignet:
  - Für Diagnosezwecke.
  - Für Geräte in einem MRP-Ring: Nach dem Umschalten des Rings ermöglicht die Funktion `Forward All`, das Netz für Datenpakete mit registrierten Multicast-Zieladressen zügig neu zu konfigurieren. Aktivieren Sie die Funktion `Forward All` auf jedem Ring-Port.

Voraussetzung:

Die Funktion *IGMP-Snooping* ist global eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Snooping Erweiterungen*.
- ☐ Klicken Sie den gewünschten Port im gewünschten VLAN doppelt.
- ☐ Um eine oder mehrere Funktionen zu aktivieren, markieren Sie die entsprechenden Optionen.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`igmp-snooping vlan-id 1 forward-all 1/1`	Aktivieren der Funktion `Forward All` für Port `1/1` in VLAN `1`.

Multicasts konfigurieren

Das Gerät ermöglicht Ihnen, die Vermittlung von Multicast-Datenpaketen zu konfigurieren. Dabei bietet das Gerät unterschiedliche Optionen an, je nachdem, ob die Datenpakete für unbekannte oder bekannte Multicast-Empfänger bestimmt sind.

Die Einstellungen für unbekannte Multicast-Adressen gelten global für das gesamte Gerät. Folgende Optionen stehen zur Auswahl:
- Das Gerät verwirft unbekannte Multicasts.
- Das Gerät leitet unbekannte Multicasts an jeden Port weiter.

Anmerkung: Die Vermittlungseinstellungen für unbekannte Multicast-Adressen gilt auch für die reservierten IP-Adressen aus dem „Local Network Control Block“ (`224.0.0.0..224.0.0.255`). Dieses Verhalten beeinflusst ggf. übergeordnete Routing-Protokolle.

Die Vermittlung von Multicast-Datenpaketen an bekannte Multicast-Adressen legen Sie für jedes VLAN individuell fest. Folgende Optionen stehen zur Auswahl:
- Das Gerät vermittelt bekannte Multicasts an die Ports, die zuvor Query-Nachrichten empfangen haben (Query-Ports) sowie an die registrierten Ports. Registrierte Ports sind Ports, an denen sich Multicast-Empfänger befinden, die bei der entsprechenden Multicast-Gruppe angemeldet sind. Diese Option hilft sicherzustellen, dass die Übermittlung bei grundlegenden Anwendungen ohne weitere Konfiguration funktioniert.
- Das Gerät vermittelt bekannte Multicasts ausschließlich an die registrierten Ports. Diese Einstellung hat den Vorteil, die verfügbare Bandbreite durch gezielte Vermittlung optimal zu nutzen.

Voraussetzung:

Die Funktion *IGMP-Snooping* ist global eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Multicasts*.
- ☐ Im Rahmen *Konfiguration* legen Sie fest, wie das Gerät Datenpakete an unbekannte Multicast-Adressen vermittelt.
  - ▶ *an registrierte Ports senden*
    Das Gerät vermittelt Pakete mit unbekannter Multicast-Adresse an jeden Query-Port.
- ☐ In Spalte *Bekannte Multicasts* legen Sie fest, wie das Gerät im entsprechenden VLAN Datenpakete an bekannte Multicast-Adressen vermittelt. Klicken Sie in das betreffende Feld und wählen Sie den gewünschten Wert.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

10.3 Lastbegrenzung

Die Lastbegrenzer-Funktion sorgt auch bei hohem Verkehrsaufkommen für einen stabilen Betrieb, indem sie den Verkehr auf den Ports begrenzt. Die Lastbegrenzung erfolgt individuell für jeden Port sowie separat für Eingangs- und Ausgangsdatenverkehr.

Wenn die Datenrate an einem Port den definierten Grenzwert überschreitet, verwirft das Gerät die Überlast an diesem Port.

Die Lastbegrenzung erfolgt ausschließlich auf Schicht 2. Die Lastbegrenzer-Funktion übergeht dabei Protokollinformationen höherer Schichten wie IP oder TCP. Dies beeinflusst möglicherweise den TCP-Verkehr.

Um diese Auswirkungen zu minimieren, nutzen Sie die folgenden Möglichkeiten:
- Beschränken Sie die Lastbegrenzung auf bestimmte Paket-Typen, zum Beispiel auf Broadcasts, Multicasts und Unicasts mit unbekannter Zieladresse.
- Begrenzen Sie den ausgehenden Datenverkehr statt des eingehenden. Die Ausgangs-Lastbegrenzung arbeitet durch die geräteinterne Pufferung der Datenpakete besser mit der TCP-Flusssteuerung zusammen.
- Erhöhen Sie die Aging-Zeit für erlernte Unicast-Adressen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > Lastbegrenzer*.
- Aktivieren Sie den Lastbegrenzer und legen Sie Grenzwerte für die Datenrate fest. Die Einstellungen gelten jeweils für einen Port und sind aufgeteilt nach Art des Datenverkehrs:
  - Empfangene Broadcast-Datenpakete
  - Empfangene Multicast-Datenpakete
  - Empfangene Unicast-Datenpakete mit unbekannter Zieladresse

  Um die Funktion auf einem Port zu aktivieren, markieren Sie das Kontrollkästchen für mindestens eine Kategorie. In Spalte *Grenzwert Einheit* legen Sie fest, ob das Gerät die Grenzwerte als Prozent der Port-Bandbreite oder als Datenpakete pro Sekunde interpretiert. Der Grenzwert `0` deaktiviert den Lastbegrenzer.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

10.4 QoS/Priorität

QoS (Quality of Service) ist ein in der Norm IEEE 802.1D beschriebenes Verfahren, mit dem Sie die Ressourcen im Netz verteilen. QoS ermöglicht Ihnen, Daten der wichtigsten Anwendungen zu priorisieren.

Die Priorisierung vermeidet insbesondere bei starker Netzlast, dass Datenverkehr mit geringerer Priorität verzögerungsempfindlichen Datenverkehr stört. Zum verzögerungsempfindlichen Datenverkehr zählen beispielsweise Sprach-, Video- und Echtzeitdaten.

10.4.1 Beschreibung Priorisierung

Zur Priorisierung des Datenverkehrs sind im Gerät Verkehrsklassen („Traffic Classes“) vordefiniert. Höhere Verkehrsklassen priorisiert das Gerät gegenüber niedrigeren Verkehrsklassen. Die Anzahl der Verkehrsklassen ist abhängig vom Gerätetyp.

Um verzögerungsempfindlichen Daten einen optimierten Datenfluss zu bieten, weisen Sie diesen Daten höhere Verkehrsklassen zu. Weniger verzögerungsempfindlichen Daten weisen Sie entsprechend niedrigere Verkehrsklassen zu.

Den Daten Verkehrsklassen zuweisen

Das Gerät weist eingehenden Daten automatisch Verkehrsklassen zu (Verkehrsklassifizierung). Das Gerät berücksichtigt folgende Klassifizierungskriterien:

- Methode, gemäß derer das Gerät die Zuordnung empfangener Datenpakete zu den Verkehrsklassen durchführt:
  - `trustDot1p`
    Das Gerät verwendet die im VLAN-Tag enthaltene Priorität des Datenpaketes.
  - `trustIpDscp`
    Das Gerät verwendet die im IP-Header enthaltene QoS-Information (ToS/DiffServ).
  - `untrusted`
    Das Gerät ignoriert mögliche Prioritätsinformationen innerhalb der Datenpakete und verwendet direkt die Priorität des Empfangsports.
- Die Priorität, die dem Empfangsport zugewiesen ist.

Beide Klassifizierungskriterien sind konfigurierbar.

Bei der Verkehrsklassifizierung wendet das Gerät folgende Regeln an:

- Wenn der Empfangsport auf `trustDot1p` eingestellt ist (Voreinstellung), verwendet das Gerät die im VLAN-Tag enthaltene Priorität des Datenpaketes. Wenn die Datenpakete kein VLAN-Tag enthalten, richtet sich das Gerät nach der Priorität des Empfangsports.
- Wenn der Empfangsport auf `trustIpDscp` eingestellt ist, verwendet das Gerät die im IP-Header enthaltene QoS-Information (ToS/DiffServ). Wenn die Datenpakete keine IP-Pakete sind, richtet sich das Gerät nach der Priorität des Empfangsports.
- Wenn der Empfangsport auf `untrusted` eingestellt ist, richtet sich das Gerät nach der Priorität des Empfangsports.

Die Verkehrsklassen priorisieren

Zur Priorisierung von Verkehrsklassen verwendet das Gerät folgende Methoden:

- `Strict`
  Wenn kein Versand von Daten einer höheren Verkehrsklasse mehr stattfindet oder die betreffenden Daten noch in der Warteschlange stehen, sendet das Gerät Daten der entsprechenden Verkehrsklasse. Wenn jede Verkehrsklasse nach der Methode `Strict` priorisiert ist, blockiert das Gerät bei hoher Netzlast die Daten niedrigerer Verkehrsklassen möglicherweise permanent.
- `Weighted Fair Queuing`
  Die Verkehrsklasse erhält eine spezifische Bandbreite zugewiesen. Dies hilft sicherzustellen, dass das Gerät die Daten dieser Verkehrsklasse sendet, auch wenn in höheren Verkehrsklassen sehr viel Datenverkehr herrscht.

10.4.2 Behandlung empfangener Prioritätsinformationen

Anwendungen kennzeichnen Datenpakete mit folgenden Priorisierungs-Informationen:

- VLAN-Priorität nach IEEE 802.1Q/ 802.1D (Schicht 2)
- Type-of-Service (ToS) oder DiffServ (DSCP) bei VLAN Management IP-Paketen (Schicht 3)

Das Gerät bietet folgende Möglichkeiten, diese Prioritätsinformation auszuwerten:

- `trustDot1p`
  Das Gerät weist VLAN-getaggte Datenpakete entsprechend ihrer VLAN-Priorität den unterschiedlichen Verkehrsklassen zu. Die entsprechende Zuordnung ist konfigurierbar. Das Gerät weist Datenpaketen, die es ohne VLAN-Tag empfängt, die Priorität des Empfangsports zu.
- `trustIpDscp`
  Das Gerät weist IP-Pakete gemäß dem DSCP-Wert im IP-Header den unterschiedlichen Verkehrsklassen zu, auch wenn das Paket zusätzlich VLAN-getagged war. Die entsprechende Zuordnung ist konfigurierbar. Nicht-IP-Pakete priorisiert das Gerät entsprechend der Priorität des Empfangsports.
- `untrusted`
  Das Gerät ignoriert die Prioritätsinformationen in Datenpaketen und weist den Paketen die Priorität des Empfangsports zu.

10.4.3 VLAN-Tagging

Für die Funktionen VLAN und Priorisierung sieht die Norm IEEE 802.1Q die Einbindung eines MAC-Datenrahmens in das VLAN-Tag vor. Das VLAN-Tag besteht aus 4 Bytes und steht zwischen dem Quelladressfeld („Source Address Field“) und dem Typfeld („Length/Type Field“).

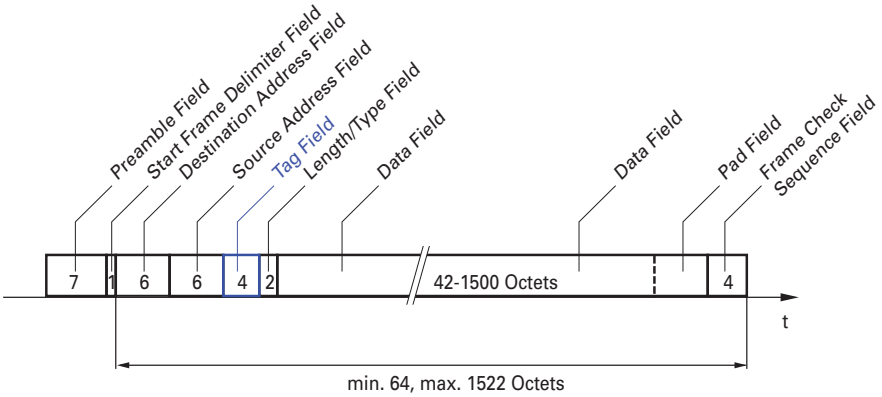


Abb. 23: Ethernet-Datenpaket mit Tag

Das Gerät wertet bei Datenpaketen mit VLAN-Tags folgende Informationen aus:
- Prioritätsinformation
- VLAN-Tag, sofern VLANs eingerichtet sind

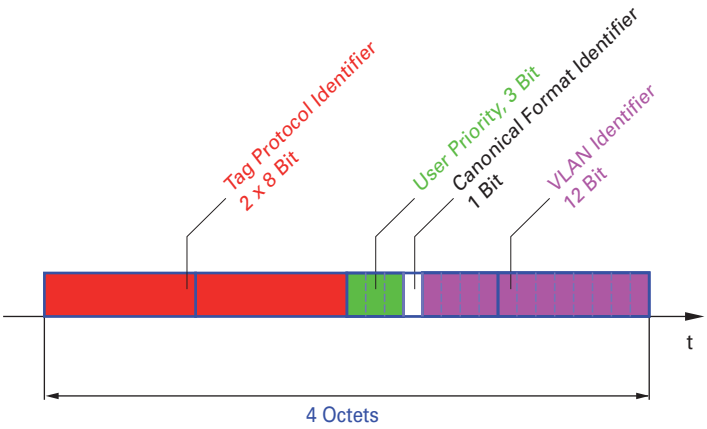


Abb. 24: Aufbau des VLAN-Tag

Ein Datenpaket, dessen VLAN-Tag eine Prioritätsinformation, aber keine VLAN-Information (VLAN-Kennung = 0) enthält, bezeichnet man als „Priority Tagged Frame“.

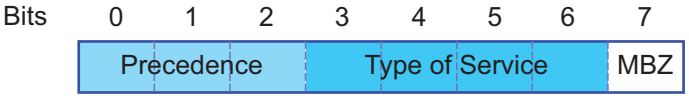
Anmerkung: Netzprotokolle und Redundanzmechanismen nutzen die höchste Verkehrsklasse 7. Wählen Sie für Anwendungsdaten deshalb niedrigere Verkehrsklassen.

Beachten Sie beim Einsatz der VLAN-Priorisierung folgende Besonderheiten:
- Eine Ende-zu-Ende-Priorisierung erfordert die durchgängige Übertragung der VLAN-Tags im gesamten Netz. Voraussetzung ist, dass jede beteiligte Netzkomponente VLAN-fähig ist.
- Router haben keine Möglichkeit, über Port-basierte Router-Interfaces Pakete mit VLAN-Tag zu empfangen und zu senden.

10.4.4 IP ToS (Type of Service)

Das Type-of-Service-Feld (ToS) im IP-Header ist bereits von Beginn an Bestandteil des IP-Protokolls und war zur Unterscheidung unterschiedlicher Dienstgüten in IP-Netzen vorgesehen. Schon damals machte man sich aufgrund der geringen zur Verfügung stehenden Bandbreiten und der unzuverlässigen Verbindungswege Gedanken um eine differenzierte Behandlung von IP-Paketen. Durch die kontinuierliche Steigerung der zur Verfügung stehenden Bandbreiten bestand keine Notwendigkeit, das ToS-Feld zu nutzen.

Erst die Echtzeitanforderungen an heutige Netze rücken das ToS-Feld in den Blickpunkt. Eine Markierung im ToS-Byte des IP-Headers ermöglicht eine Unterscheidung unterschiedlicher Dienstgüten. In der Praxis hat sich die Nutzung dieses Feldes jedoch nicht durchgesetzt.



Tab. 22: ToS-Feld im IP-Header

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

10.4.5 Handhabung der Verkehrsklassen

Das Gerät bietet folgende Möglichkeiten zur Handhabung der Verkehrsklassen:
- Strict Priority
- Weighted Fair Queuing
- Strict Priority kombiniert mit Weighted Fair Queuing
- Queue-Management

Beschreibung Strict Priority

Bei Strict Priority vermittelt das Gerät zuerst die Datenpakete mit höherer Verkehrsklasse (höherer Priorität), bevor es ein Datenpaket mit der nächst niedrigeren Verkehrsklasse vermittelt. Ein Datenpaket mit der niedrigsten Verkehrsklasse (niedrigsten Priorität) vermittelt das Gerät demnach erst, wenn keine anderen Datenpakete mehr in der Warteschlange stehen. In ungünstigen Fällen sendet das Gerät keine Pakete mit niedriger Priorität, wenn an diesem Port ein hohes Aufkommen von höherpriorem Verkehr zum Senden ansteht.

Bei verzögerungsempfindlichen Anwendungen wie VoIP oder Video ermöglicht Strict Priority das unmittelbare Senden hochpriorer Daten.

Beschreibung Weighted Fair Queuing

Mit Weighted Fair Queuing, auch Weighted Round Robin (WRR) genannt, weisen Sie jeder Verkehrsklasse eine minimale oder reservierte Bandbreite zu. Dies hilft sicherzustellen, dass das Gerät bei hoher Netzlast auch Datenpakete mit einer niedrigen Priorität vermittelt.

Die reservierten Werte liegen im Bereich von 0 % bis 100 % der verfügbaren Bandbreite und sind einstellbar in Schritten von 1 %.
- Eine Reservierung von „0“ entspricht der Einstellung „keine Bandbreitengarantie“.
- Die Summe der einzelnen Bandbreiten darf bis zu 100 % betragen.

Wenn Sie jeder Verkehrsklasse das Weighted Fair Queuing zuweisen, dann steht diesen die gesamte Bandbreite des entsprechenden Ports zur Verfügung.

Strict Priority und Weighted Fair Queuing kombinieren

Vergewissern Sie sich beim Kombinieren von Weighted Fair Queuing mit Strict Priority, dass die höchste Verkehrsklasse von Weighted Fair Queuing niedriger ist als die niedrigste Verkehrsklasse von Strict Priority.

Wenn Sie Weighted Fair Queuing mit Strict Priority kombinieren, kann eine hohe Strict Priority-Netzlast die für Weighted Fair Queuing verfügbare Bandbreite deutlich reduzieren.

10.4.6 Queue-Management

Queue Shaping

Queue Shaping drosselt die Geschwindigkeit, mit der Warteschlangen Pakete vermitteln. Mit Queue Shaping beschränken Sie zum Beispiel die Geschwindigkeit für eine Warteschlange mit höherer Priorität und ermöglichen so einer Warteschlange mit niedrigerer Priorität Pakete zu senden, obwohl noch höherpriore Pakete auf die Vermittlung warten. Das Gerät ermöglicht Ihnen, Queue Shaping für jede Warteschlange einzurichten. Sie legen Queue Shaping fest als die maximale Geschwindigkeit, mit der Daten die Warteschlange passieren, indem Sie einen prozentualen Anteil der verfügbaren Bandbreite zuweisen.

Einstellungen für das Queue-Management festlegen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > Queue-Management*.

Die insgesamt zugewiesene Bandbreite in Spalte *Min. Bandbreite [%]* ist 100 %.

- ☐ Um das Weighted Fair Queuing für *Traffic-Klasse* = `0` zu aktivieren, gehen Sie wie folgt vor:
  - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
  - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert `5` fest.
- ☐ Um das Weighted Fair Queuing für *Traffic-Klasse* = `1` zu aktivieren, gehen Sie wie folgt vor:
  - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
  - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert `20` fest.
- ☐ Um das Weighted Fair Queuing für *Traffic-Klasse* = `2` zu aktivieren, gehen Sie wie folgt vor:
  - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
  - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert `30` fest.
- ☐ Um das Weighted Fair Queuing für *Traffic-Klasse* = `3` zu aktivieren, gehen Sie wie folgt vor:
  - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
  - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert `20` fest.
- ☐ Um Weighted Fair Queuing und Queue Shaping für *Traffic-Klasse* = `4` zu kombinieren, gehen Sie wie folgt vor:
  - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
  - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert `10` fest.
  - ▶ Legen Sie in Spalte *Max. Bandbreite [%]* den Wert `10` fest.

  Wenn Sie Weighted Fair Queuing und Queue Shaping kombiniert für eine bestimmte Verkehrsklasse verwenden, legen Sie in Spalte *Max. Bandbreite [%]* einen Wert fest, der größer ist als der Wert in Spalte *Min. Bandbreite [%]*.

- ☐ Um das Weighted Fair Queuing für *Traffic-Klasse* = 5 zu aktivieren, gehen Sie wie folgt vor:
  - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
  - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert 5 fest.
- ☐ Um das Weighted Fair Queuing für *Traffic-Klasse* = 6 zu aktivieren, gehen Sie wie folgt vor:
  - ▶ Heben Sie die Markierung des Kontrollkästchens in Spalte *Strict priority* auf.
  - ▶ Legen Sie in Spalte *Min. Bandbreite [%]* den Wert 10 fest.
- ☐ Um Strict Priority und Queue Shaping für *Traffic-Klasse* = 7 zu kombinieren, gehen Sie wie folgt vor:
  - ▶ Markieren Sie das Kontrollkästchen in Spalte *Strict priority*.
  - ▶ Legen Sie in Spalte *Max. Bandbreite [%]* den Wert 10 fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`cos-queue weighted 0`	Weighted Fair Queuing für die Verkehrsklasse 0 einschalten.
`cos-queue min-bandwidth: 0 5`	Gewichtung 5 % der Verkehrsklasse 0 zuweisen.
`cos-queue weighted 1`	Weighted Fair Queuing für die Verkehrsklasse 1 einschalten.
`cos-queue min-bandwidth: 1 20`	Gewichtung 20 % der Verkehrsklasse 1 zuweisen.
`cos-queue weighted 2`	Weighted Fair Queuing für die Verkehrsklasse 2 einschalten.
`cos-queue min-bandwidth: 2 30`	Gewichtung 30 % der Verkehrsklasse 2 zuweisen.
`cos-queue weighted 3`	Weighted Fair Queuing für die Verkehrsklasse 3 einschalten.
`cos-queue min-bandwidth: 3 20`	Gewichtung 20 % der Verkehrsklasse 3 zuweisen.

```
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

Weighted Fair Queuing und Queue Shaping kombinieren

Führen Sie die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`cos-queue weighted 4`	Weighted Fair Queuing für die Verkehrsklasse 4 einschalten.
`cos-queue min-bandwidth: 4 10`	Gewichtung 10 % der Verkehrsklasse 4 zuweisen.
`cos-queue max-bandwidth: 4 10`	Gewichtung 10 % der Verkehrsklasse 4 zuweisen.

```
cos-queue weighted 5
```
Weighted Fair Queuing für die Verkehrsklasse 5 einschalten.

```
cos-queue min-bandwidth: 5 5
```
Gewichtung 5 % der Verkehrsklasse 5 zuweisen.

```
cos-queue weighted 6
```
Weighted Fair Queuing für die Verkehrsklasse 6 einschalten.

```
cos-queue min-bandwidth: 6 10
```
Gewichtung 10 % der Verkehrsklasse 6 zuweisen.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

Queue Shaping einrichten

Führen Sie die folgenden Schritte aus:

```
enable
```
Wechsel in den Privileged-EXEC-Modus.

```
configure
```
Wechsel in den Konfigurationsmodus.

```
cos-queue max-bandwidth: 7 10
```
Gewichtung 10 % der Verkehrsklasse 7 zuweisen.

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

10.4.7 Management-Priorisierung

Das Gerät ermöglicht Ihnen, die Management-Pakete zu priorisieren, damit Sie in Situationen mit hoher Netzlast jederzeit Zugriff auf das Management des Geräts haben.

Bei der Priorisierung von Management-Paketen sendet das Gerät die Management-Pakete mit einer Prioritäts-Information.

- Auf Schicht 2 modifiziert das Gerät die VLAN-Priorität im VLAN-Tag.
  Voraussetzung für diese Funktion ist, dass die entsprechenden Ports so eingestellt sind, dass sie das Senden von Paketen mit VLAN-Tag erlauben.
- Auf Schicht 3 modifiziert das Gerät den IP-DSCP-Wert.

10.4.8 Priorisierung einstellen

Port-Priorität zuweisen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > Port-Konfiguration*.
- ☐ In Spalte *Port-Priorität* legen Sie die Priorität fest, mit welcher das Gerät die auf diesem Port empfangenen Datenpakete ohne VLAN-Tag vermittelt.
- ☐ In Spalte *Trust-Mode* legen Sie fest, nach welchem Kriterium das Gerät empfangenen Datenpaketen eine Verkehrsklasse zuweist.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`vlan priority 3`	Interface `1/1` die Port-Priorität `3` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.

VLAN-Priorität einer Verkehrsklasse zuweisen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > 802.1D/p Zuweisung*.
- ☐ Um einer VLAN-Priorität eine Verkehrsklasse zuzuweisen, fügen Sie in Spalte *Traffic-Klasse* den betreffenden Wert ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`classofservice dot1p-mapping 0 2`	Der VLAN-Priorität `0` die Verkehrsklasse `2` zuweisen.
`classofservice dot1p-mapping 1 2`	Der VLAN-Priorität `1` die Verkehrsklasse `2` zuweisen.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show classofservice dot1p-mapping`	Zeigt die Zuordnung.

Empfangenen Datenpaketen die Port-Priorität zuweisen

Führen Sie die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`classofservice trust untrusted`	Dem Interface den Modus `untrusted` zuweisen.
`classofservice dot1p-mapping 0 2` `classofservice dot1p-mapping 1 2`	Der VLAN-Priorität `0` die Verkehrsklasse `2` zuweisen. Der VLAN-Priorität `1` die Verkehrsklasse `2` zuweisen.
`vlan priority 1`	Für die Port-Priorität den Wert `1` festlegen.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show classofservice trust`	Trust-Modus der Ports/Interfaces anzeigen.

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

DSCP einer Verkehrsklasse zuweisen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > IP-DSCP-Zuweisung*.
- ☐ Legen Sie in Spalte *Traffic-Klasse* den gewünschten Wert fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`classofservice ip-dscp-mapping cs1 1`	Dem DSCP `CS1` die Verkehrsklasse `1` zuweisen.
`show classofservice ip-dscp-mapping`	IP-DSCP-Zuweisungen anzeigen.

```
    IP DSCP       Traffic Class
 -------------    -------------
   be                  2
   1                   2
   .                   .
   .                   .
   (cs1)               1
   .                   .
```

Empfangenen IP-Datenpaketen die DSCP-Priorität zuweisen

Führen Sie die folgenden Schritte aus:

```
enable
```
Wechsel in den Privileged-EXEC-Modus.

```
configure
```
Wechsel in den Konfigurationsmodus.

```
interface 1/1
```
Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.

```
classofservice trust ip-dscp
```
Den Modus `trust ip-dscp` global zuweisen.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
show classofservice trust
```
Trust-Modus der Ports/Interfaces anzeigen.

```
 Interface     Trust Mode
 ----------    -------------
 1/1           ip-dscp
 1/2           dot1p
 1/3           dot1p
 .             .
 .             .
 1/5           dot1p
 .             .
```

Traffic Shaping auf einem Port konfigurieren

Führen Sie die folgenden Schritte aus:

```
enable
```
Wechsel in den Privileged-EXEC-Modus.

```
configure
```
Wechsel in den Konfigurationsmodus.

```
interface 1/2
```
Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.

```
traffic-shape bw 50
```
Maximale Bandbreite des Ports `1/2` auf 50% begrenzen.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
exit
```
Wechsel in den Privileged-EXEC-Modus.

```
show traffic-shape
```
Anzeigen der Traffic-Shaping-Konfiguration.

```
Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

Management-Priorität Schicht 2 konfigurieren

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > Global*.
- ☐ Legen Sie im Feld *VLAN-Priorität für Management-Pakete* die VLAN-Priorität fest, mit der das Gerät Management-Datenpakete sendet.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network management priority dot1p 7`	Management-Paketen die VLAN-Priorität `7` zuweisen. Das Gerät sendet Management-Pakete mit höchster Priorität.
`show network parms`	Priorität des VLANs anzeigen, in dem sich das Management des Geräts befindet.

```
IPv4 Network
------------
...
Management VLAN priority.....................7
...
```

Management-Priorität Schicht 3 konfigurieren

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > QoS/Priority > Global*.
- ☐ Legen Sie im Feld *IP-DSCP-Wert für Management-Pakete* den DSCP-Wert fest, mit dem das Gerät Management-Datenpakete sendet.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network management priority ip-dscp 56`	Management-Paketen den DSCP-Wert `56` zuweisen. Das Gerät sendet Management-Pakete mit höchster Priorität.
`show network parms`	Priorität des VLANs anzeigen, in dem sich das Management des Geräts befindet.

```
IPv4 Network
------------
...
Management IP-DSCP value.....................56
```

10.5 Flusskontrolle

Wenn in der Warteschlange eines Ports sehr viele Datenpakete gleichzeitig eintreffen, dann führt dies möglicherweise zum Überlaufen des Port-Speichers. Dies geschieht zum Beispiel, wenn das Gerät Daten auf einem Gigabit-Port empfängt und diese an einen Port mit niedrigerer Bandbreite weiterleitet. Das Gerät verwirft überschüssige Datenpakete.

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

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

Die folgende Abbildung zeigt die Wirkungsweise der Flusskontrolle. Die Workstations 1, 2 und 3 wollen zur gleichen Zeit viele Daten an die Workstation 4 übertragen. Die gemeinsame Bandbreite der Workstations 1, 2 und 3 ist größer als die Bandbreite von Workstation 4. So kommt es zum Überlaufen der Empfangs-Warteschlange von Port 4. Der linke Trichter symbolisiert diesen Zustand.

Wenn an den Ports 1, 2 und 3 des Geräts die Funktion Flusskontrolle eingeschaltet ist, reagiert das Gerät, bevor der Trichter überläuft. Der Trichter auf der rechten Seite veranschaulicht die Ports 1, 2 und 3, die zwecks Kontrolle der Übertragungsgeschwindigkeit eine Nachricht an die übertragenden Geräte senden. Als Resultat hiervon wird der Empfangsport nicht länger überfordert und ist in der Lage, den eingehenden Verkehr zu verarbeiten.

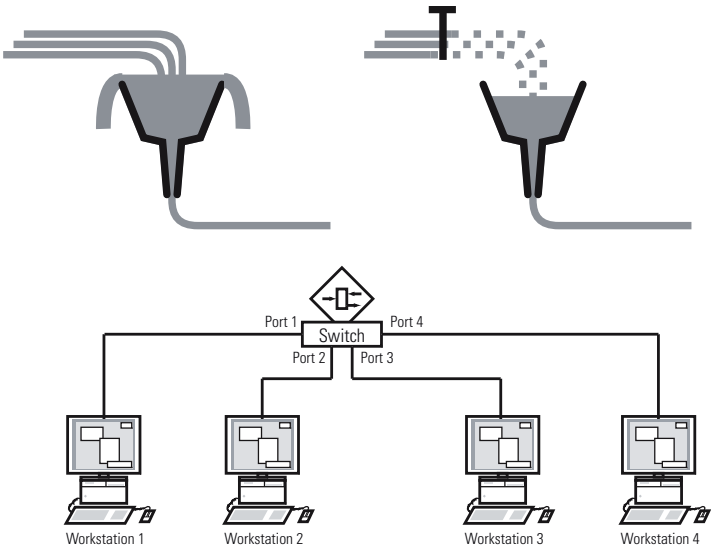


Abb. 25: Beispiel für Flusskontrolle

10.5.1 Halbduplex- oder Vollduplex-Verbindung

Flusskontrolle bei Halbduplex-Verbindung

Im Beispiel besteht zwischen der Arbeitsstation 2 und dem Gerät eine Halbduplex-Verbindung.

Bevor die Sende-Warteschlange von Port 2 überläuft, sendet das Gerät Daten zurück an Arbeitsstation 2. Arbeitsstation 2 erkennt eine Kollision und unterbricht den Sendevorgang.

Flusskontrolle bei Vollduplex-Verbindung

Im Beispiel besteht zwischen der Arbeitsstation 2 und dem Gerät eine Vollduplex-Verbindung.

Bevor die Sende-Warteschlange von Port 2 überläuft, sendet das Gerät eine Aufforderung an Arbeitsstation 2, beim Senden eine kleine Pause einzulegen.

10.5.2 Flusskontrolle einrichten

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > Global*.
- ☐ Markieren Sie das Kontrollkästchen *Flusskontrolle*.
  Mit dieser Einstellung schalten Sie die Flusskontrolle im Gerät ein.
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Um die Flusskontrolle auf einem Port einzuschalten, markieren Sie das Kontrollkästchen in Spalte *Flusskontrolle*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

Anmerkung: Wenn Sie eine Redundanzfunktion verwenden, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Ports. Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt.

11 Template-basiertes TSN konfigurieren

11.1 Zugrundeliegende Fakten

Wenn Sie die Funktion *TSN* verwenden, gelten die folgenden Rahmenbedingungen:

- Das Gerät arbeitet nach dem „Store and Forward“-Verfahren. Das Gerät muss also das komplette Datenpaket empfangen, bevor es eine Forwarding-Entscheidung trifft.
- Basiszeit und Zykluszeit legen Sie für das Gerät einmal fest. Beide Einstellungen gelten für jeden Port, der an TSN teilnimmt.
- Basierend auf vordefinierten Templates konfigurieren Sie recht einfach eine Gate-Control-Liste je Port.
- Vergewissern Sie sich, dass die Summe der Zeiteinträge in der Gate-Control-Liste kleiner oder gleich der festgelegten Zykluszeit ist.
- Mit einem Schutzband sorgt das Gerät dafür, dass keine Pakete aus dem vorherigen Zeitschlitz in den Zeitschlitz für Pakete mit hoher Priorität "überlaufen". Ausschlaggebend für die Intervalllänge des Schutzbands ist die Übertragungsrate des sendenden Ports.
  Für das Schutzband empfehlen wir die folgenden Intervalllängen. Die Werte basieren auf der Übertragungsrate des Ports und der maximal zulässigen Größe der Ethernet-Pakete:
  - 2.5 Gbit/s: 5 µs
  - 1 Gbit/s: 13 µs
  - 100 Mbit/s: 124 µs
- Der Wertebereich für die Zykluszeit beträgt 50 000..10 000 000 ns.
- Der Intervallbereich der Gate-Control-Liste beträgt 1 000..10 000 000 ns.
- Vergewissern Sie sich, dass die Zykluszeit und das Intervall der Gate-Control-Liste Vielfache von 1 µs, 2 µs oder 4 µs sind.

Tab. 23: Abhängigkeit zwischen Zykluszeit und Granularität

Zykluszeit	Granularität
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

11.2 Beispiel

Dieses Beispiel beschreibt, wie Sie die Geräte für ein Szenario mit den folgenden Rahmenbedingungen einrichten:
- Zykluszeit = 1 ms
- Zeitschlitz für Pakete mit hoher Priorität = 500 µs
- Zeitschlitz für Pakete mit niedriger Priorität = 487 µs

In diesem Beispiel ist jedes Gerät mit einer Übertragungsrate von 1 GBit/s an das Netz angeschlossen.

Tab. 24: Zusammensetzung des Zyklus

Zeitschlitz	Verkehrsklassen	Dauer
Pakete mit hoher Priorität	7	500 µs
Pakete mit niedriger Priorität	0,1,2,3,4,5,6	487 µs
Schutzband	–	13 µs

11.2.1 Zeit-Berechnung

Die Dauer des Zeitschlitzes für Pakete mit niedriger Priorität berechnet das Gerät automatisch. Die Berechnung basiert auf den folgenden Parametern:
- Zykluszeit
- Dauer des Zeitschlitzes für Pakete mit hoher Priorität
- Dauer des Schutzbands

11.2.2 Geräte einrichten

Anhand der zuvor festgelegten Zeiten richten Sie die Geräte mit der grafischen Benutzeroberfläche oder dem Command Line Interface ein. Führen Sie die folgenden Schritte für jedes beteiligte Gerät aus.

Zykluszeit prüfen und anpassen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > TSN > Konfiguration*.
- ☐ Prüfen Sie im Rahmen *Konfiguration* den Wert im Feld *Zyklus-Zeit [ns]*.
- ☐ Passen Sie den Wert an, falls erforderlich.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

```
enable                                  Wechsel in den Privileged-EXEC-Modus.
configure                               Wechsel in den Konfigurationsmodus.
show tsn configuration
Port  Status                Conf. cycle time[ns]  Conf. base time
      Default gate states   Curr. cycle time[ns]  Curr. base time
      Config change pending                       Time of last activation
----  --------------------  --------------------  ------------------------------
 1/1  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-12 08:10:58.813000000

 1/2  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-11 07:24:35.204000000

 1/3  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

 1/4  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

tsn cycle-time 1000000                  Passen Sie den Wert an, falls erforderlich.
```

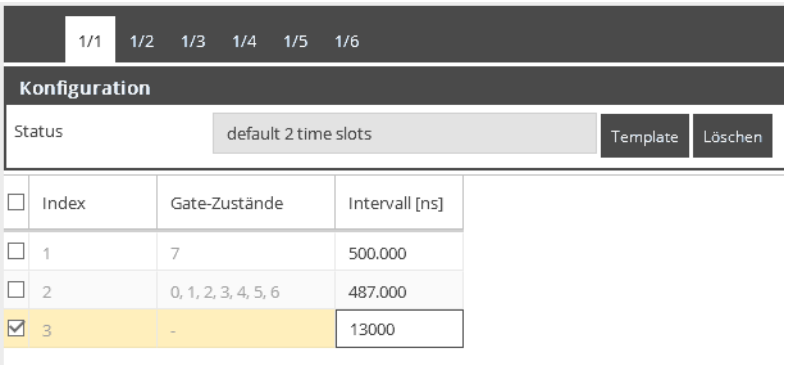
Template auswählen und Gate-Control-Liste einrichten

Das Gerät stellt vordefinierte Templates zum Einrichten der Gate-Control-Liste bereit. In diesem Beispiel verwenden wir das Template *default 2 time slots*. Nachdem Sie das Template ausgewählt haben, können Sie die Dauer der Zeitschlitze anpassen. Führen Sie die folgenden Schritte für jeden Port aus, auf dem Sie die Funktion *TSN* verwenden möchten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > TSN > Gate Control List > Konfiguriert*.
- ☐ Wählen Sie die Registerkarte des Port, für den Sie die Einstellungen festlegen möchten.

- ☐ Wählen Sie im Rahmen *Konfiguration* ein Template aus.
  Führen Sie die folgenden Schritte aus:
  - Klicken Sie die Schaltfläche *Template*.
  - Wählen Sie den Eintrag `default 2 time slots`.
  - Klicken Sie die Schaltfläche *Ok*.
- ☐ Passen Sie in Spalte *Intervall [ns]* die Werte an:
  - Fügen Sie in der Zeile für Pakete mit hoher Priorität den Wert `500000` ein.
  - Fügen Sie in der Zeile für das Schutzband den Wert `13000` ein.
  - Beim Speichern der Änderungen berechnet das Gerät den dritten Wert automatisch.



- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`tsn gcl modify 1 interval 500000`	Anpassen der Dauer des Zeitschlitzes für Pakete mit hoher Priorität in Nanosekunden.
`tsn gcl modify 3 interval 13000`	Anpassen der Dauer des Zeitschlitzes für das Schutzband in Nanosekunden. Die Dauer des Zeitschlitzes für Pakete mit niedriger Priorität berechnet das Gerät automatisch. Den Zeitschlitz für Pakete mit niedriger Priorität können Sie nicht einstellen.

12 VLANs

Ein virtuelles LAN (VLAN) besteht im einfachsten Fall aus einer Gruppe von Netzteilnehmern in einem Netzsegment, die so miteinander kommunizieren, als bildeten sie ein eigenständiges LAN.

Komplexere VLANs erstrecken sich über mehrere Netzsegmente und basieren zusätzlich auf logischen (statt ausschließlich physikalischen) Verbindungen zwischen Netzteilnehmern. VLANs sind ein Element der flexiblen Netzgestaltung. Das zentrale Umkonfigurieren lokaler Verbindungen lässt sich so leichter bewerkstelligen als über Kabel.

Das Gerät unterstützt das unabhängige Erlernen von VLANs nach Maßgabe des Standards IEEE 802.1Q, welcher die Funktion *VLAN* definiert.

Die Verwendung von VLANS bietet zahlreiche Vorteile. Nachstehend sind die wesentlichen Vorteile aufgelistet:

- Netzlastbegrenzung
  VLANs reduzieren die Netzlast erheblich, da die Geräte Broadcast-, Multicast- und Unicast-Pakete mit unbekannten (nicht gelernten) Zieladressen ausschließlich innerhalb des virtuellen LANs vermitteln. Der Rest des Datennetzes übermittelt den Verkehr wie üblich.
- Flexibilität
  Sie haben die Möglichkeit, Anwender-Arbeitsgruppen zu bilden, die – abgesehen vom physikalischen Standort oder Medium der Teilnehmer – auf der Funktion der Teilnehmer basieren.
- Übersichtlichkeit
  VLANs strukturieren Netze überschaubarer und vereinfachen die Wartung.

12.1 Beispiele für ein VLAN

Die folgenden Beispiele aus der Praxis vermitteln einen schnellen Einstieg in den Aufbau eines VLANs.

Anmerkung: Für die Konfiguration von VLANs verwenden Sie eine gleichbleibende Management-Oberfläche. In diesem Beispiel verwenden Sie für die Konfiguration der VLANs entweder Interface 1/6 oder die serielle Verbindung.

12.1.1 Beispiel 1

Das Beispiel zeigt eine minimale VLAN-Konfiguration (Port-basiertes VLAN). Ein Administrator hat an einem Vermittlungsgerät mehrere Endgeräte angeschlossen und diese 2 VLANs zugewiesen. Dies unterbindet wirksam jeglichen Datenverkehr zwischen verschiedenen VLANs; deren Mitglieder kommunizieren ausschließlich innerhalb ihres eigenen VLANs.

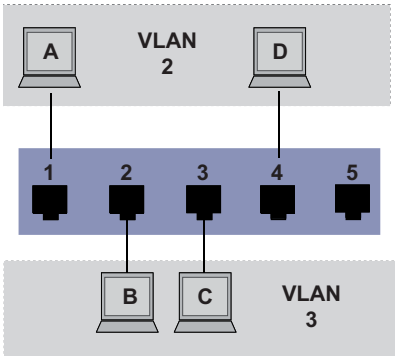


Abb. 26: Beispiel für ein einfaches Port-basiertes VLAN

Während der Einrichtung der VLANs erzeugen Sie für jeden Port Kommunikationsregeln, die Sie in einer Ingress-Tabelle (Eingang) und einer Egress-Tabelle (Ausgang) erfassen.

Die Ingress-Tabelle legt fest, welche VLAN-ID ein Port den eingehenden Datenpaketen zuweist. Hierbei weisen Sie das Endgerät über seine Portadresse einem VLAN zu.

Die Egress-Tabelle legt fest, an welchen Ports das Gerät die Pakete aus diesem VLAN sendet.
- `T` = Tagged (mit Tag-Feld, markiert)
- `U` = Untagged (ohne Tag-Feld, nicht markiert)

Für obiges Beispiel hat das TAG der Datenpakete keine Relevanz, verwenden Sie die Einstellung `U`.

Tab. 25: Ingress-Tabelle

Endgerät	Port	Port VLAN Identifer (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

Tab. 26: Egress-Tabelle

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

Führen Sie die folgenden Schritte aus:

☐ VLAN einrichten

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Legen Sie im Feld *VLAN-ID* den Wert `2` fest.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Legen Sie für das VLAN den Namen `VLAN2` fest:
  Doppelklicken Sie in Spalte *Name* und legen den Namen fest.
  Ändern Sie für VLAN `1` den Wert in Spalte *Name* von `Default` zu `VLAN1`.
- ☐ Wiederholen Sie die vorherigen Schritte, um ein VLAN `3` mit dem Namen `VLAN3` zu erzeugen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`vlan add 2`	Erzeugt ein neues VLAN mit VLAN-ID `2`.
`name 2 VLAN2`	Dem VLAN `2` den Namen `VLAN2` zuweisen.
`vlan add 3`	Erzeugt ein neues VLAN mit VLAN-ID `3`.
`name 3 VLAN3`	Dem VLAN `3` den Namen `VLAN3` zuweisen.
`name 1 VLAN1`	Dem VLAN `1` den Namen `VLAN1` zuweisen.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show vlan brief`	Zeigt die aktuelle VLAN Konfiguration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ Ports einrichten

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Um einem VLAN einen Port zuzuweisen, legen Sie in der betreffenden Spalte den gewünschten Wert fest.
  Mögliche Werte:
  - `T` = Der Port ist Mitglied im VLAN. Der Port sendet Datenpakete mit Tag.
  - `U` = Der Port ist Mitglied im VLAN. Der Port sendet Datenpakete ohne Tag.
  - `F` = Der Port ist kein Mitglied im VLAN.
    Änderungen durch die Funktion *GVRP* sind gesperrt.
  - `-` = Der Port ist kein Mitglied in diesem VLAN.
    Änderungen durch die Funktion *GVRP* sind erlaubt.

  Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie den Wert `U` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Legen Sie in Spalte *Port-VLAN-ID* die VLAN-ID des zugehörigen VLANs fest: `2` oder `3`
- ☐ Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie für die Endgeräte-Ports in Spalte *Akzeptierte Datenpakete* den Wert `admitAll` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

Der Wert in Spalte *Ingress-Filtering* hat in diesem Beispiel keinen Einfluss auf die Funktion.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`vlan participation include 2`	Port `1/1` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port `1/1` die Port-VLAN-ID `2` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`vlan participation include 3`	Port `1/2` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port `1/2` die Port-VLAN-ID `3` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/3`.
`vlan participation include 3`	Port `1/3` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port `1/3` die Port-VLAN-ID `3` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/4`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/4`.
`vlan participation include 2`	Port `1/4` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port `1/4` die Port-VLAN-ID `2` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show vlan id 3`	Details zu VLAN `3` anzeigen.

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

12.1.2 Beispiel 2

Das zweite Beispiel zeigt eine komplexere Konfiguration mit 3 VLANs (1 bis 3). Zusätzlich zu dem schon bekannten Switch aus Beispiel 1 verwenden Sie einen 2. Switch (im Beispiel rechts gezeichnet).

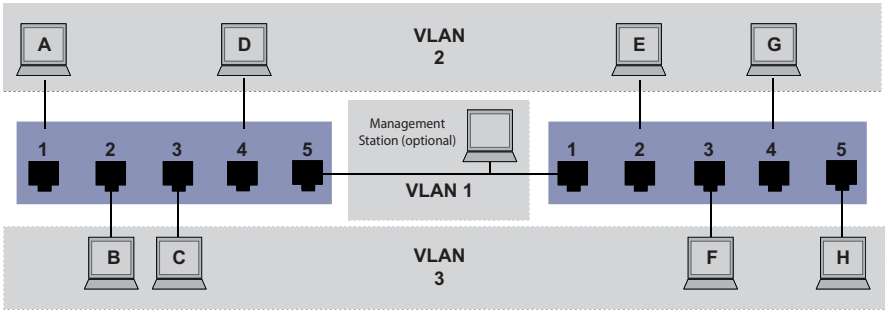


Abb. 27: Beispiel für eine komplexere VLAN-Konfiguration

Die Endgeräte der einzelnen VLANs (A bis H) erstrecken sich über 2 Vermittlungsgeräte (Switch). Derartige VLANs heißen deshalb verteilte VLANs. Zusätzlich ist eine optionale Netz-Management-Station gezeigt, die bei richtiger VLAN-Konfiguration Zugriff auf jede Netzkomponente hat.

Anmerkung: Das VLAN 1 hat in diesem Fall keine Bedeutung für die Endgerätekommunikation, ist aber notwendig für die Administration der Vermittlungsgeräte über das sogenannte Management-VLAN.

Weisen Sie die Ports mit ihren angeschlossenen Endgeräten eindeutig einem VLAN zu (wie im vorherigen Beispiel gezeigt). Bei der direkten Verbindung zwischen den beiden Übertragungsgeräten (Uplink) transportieren die Ports Pakete für beide VLANs. Um diese Uplinks zu unterscheiden, verwenden Sie VLAN-Tags, welche für die entsprechende Behandlung der Datenpakete sorgen. So bleibt die Zuordnung zu den jeweiligen VLANs erhalten.

Führen Sie die folgenden Schritte aus:
- ☐ Ergänzen Sie die Ingress- und Egress-Tabelle aus Beispiel 1 um den Uplink Port 5.
- ☐ Erfassen Sie für den rechten Switch je eine neue Ingress- und Egress-Tabelle wie im ersten Beispiel beschrieben.

Die Egress-Tabelle legt fest, an welchen Ports das Gerät die Pakete aus diesem VLAN sendet.
- `T` = Tagged (mit Tag-Feld, markiert)
- `U` = Untagged (ohne Tag-Feld, nicht markiert)

Markierte (Tagged) Pakete kommen in diesem Beispiel in der Kommunikation zwischen den Vermittlungsgeräten (Uplink) zum Einsatz, da auf diesen Ports Pakete für unterschiedliche VLANs unterschieden werden.

Tab. 27: 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. 28: 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. 29: Egress-Tabelle Gerät links

VLAN-ID	Port				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

Tab. 30: Egress-Tabelle Gerät rechts

VLAN-ID	Port				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

Die Kommunikationsbeziehungen sind hierbei wie folgt: Endgeräte an Port 1 und 4 des linken Geräts sowie Endgeräte an Port 2 und 4 des rechten Geräts sind Mitglied im VLAN 2 und können somit untereinander kommunizieren. Ebenso verhält es sich mit den Endgeräten an Port 2 und 3 des linken Geräts sowie den Endgeräten an Port 3 und 5 des rechten Geräts. Diese gehören zu VLAN 3.

Die Endgeräte „sehen“ jeweils ihren Teil des Netzes. Teilnehmer außerhalb dieses VLANs sind unerreichbar. Das Gerät vermittelt auch Broadcast-, Multicast- und Unicast-Pakete mit unbekannter (nicht gelernter) Zieladresse ausschließlich innerhalb der Grenzen eines VLANs.

Hier verwenden die Geräte das VLAN-Tag (IEEE 801.1Q) innerhalb des VLANs mit der ID 1 (Uplink). Der Buchstabe `T` in der Egress-Tabelle der Ports zeigt das VLAN-Tag.

Die Konfiguration des Beispiels erfolgt exemplarisch für das rechte Gerät. Verfahren Sie analog, um das zuvor bereits konfigurierte linke Gerät unter Anwendung der oben erzeugten Ingress- und Egress-Tabellen an die neue Umgebung anzupassen.

Führen Sie die folgenden Schritte aus:
- ☐ VLAN einrichten

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Legen Sie im Feld *VLAN-ID* die VLAN-ID fest, zum Beispiel `2`.

- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Legen Sie für das VLAN den Namen `VLAN2` fest:
  Doppelklicken Sie in Spalte *Name* und legen den Namen fest.
  Ändern Sie für VLAN `1` den Wert in Spalte *Name* von `Default` zu `VLAN1`.
- ☐ Wiederholen Sie die vorherigen Schritte, um ein VLAN `3` mit dem Namen `VLAN3` zu erzeugen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`vlan add 2`	Erzeugt ein neues VLAN mit VLAN-ID `2`.
`name 2 VLAN2`	Dem VLAN `2` den Namen `VLAN2` zuweisen.
`vlan add 3`	Erzeugt ein neues VLAN mit VLAN-ID `3`.
`name 3 VLAN3`	Dem VLAN `3` den Namen `VLAN3` zuweisen.
`name 1 VLAN1`	Dem VLAN `1` den Namen `VLAN1` zuweisen.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show vlan brief`	Zeigt die aktuelle VLAN Konfiguration.

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs............. 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                      VLAN Type VLAN Creation Time
---- --------------------------------- --------- ------------------
1       VLAN1                          default    0 days, 00:00:05
2       VLAN2                          static     0 days, 02:44:29
3       VLAN3                          static     0 days, 02:52:26
```

☐ Ports einrichten

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Um einem VLAN einen Port zuzuweisen, legen Sie in der betreffenden Spalte den gewünschten Wert fest.
  Mögliche Werte:
  - `T` = Der Port ist Mitglied im VLAN. Der Port sendet Datenpakete mit Tag.
  - `U` = Der Port ist Mitglied im VLAN. Der Port sendet Datenpakete ohne Tag.
  - `F` = Der Port ist kein Mitglied im VLAN.
    Änderungen durch die Funktion *GVRP* sind gesperrt.
  - `-` = Der Port ist kein Mitglied in diesem VLAN.
    Änderungen durch die Funktion *GVRP* sind gesperrt.

  Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie den Wert `U` fest.
  Auf dem Uplink-Port, über den die VLANs miteinander kommunizieren, legen Sie den Wert `T` fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Legen Sie in Spalte *Port-VLAN-ID* die VLAN-ID des zugehörigen VLANs fest:
  `1`, `2` oder `3`
- ☐ Da Endgeräte in der Regel keine Datenpakete mit Tag interpretieren, legen Sie für die Endgeräte-Ports in Spalte *Akzeptierte Datenpakete* den Wert `admitAll` fest.

- ☐ Legen Sie für den Uplink-Port in Spalte *Akzeptierte Datenpakete* den Wert `admitOnlyVlanTagged` fest.
- ☐ Markieren Sie für den Uplink-Port das kontrollkästchen in Spalte *Ingress-Filtering*, um VLAN-Tags auf diesem Port auszuwerten.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`vlan participation include 1`	Port `1/1` wird Mitglied des VLANs `1` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan participation include 2`	Port `1/1` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan tagging 2 enable`	Port `1/1` wird Mitglied des VLANs `2` und vermittelt die Datenpakete mit VLAN-Tag.
`vlan participation include 3`	Port `1/1` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan tagging 3 enable`	Port `1/1` wird Mitglied des VLANs `3` und vermittelt die Datenpakete mit VLAN-Tag.
`vlan pvid 1`	Port-VLAN-ID `1` dem Port `1/1` zuweisen.
`vlan ingressfilter`	Aktivieren von Ingress Filtering auf Port `1/1`.
`vlan acceptframe vlanonly`	Port `1/1` überträgt ausschließlich Pakete mit VLAN Tag.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`vlan participation include 2`	Port `1/2` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port-VLAN-ID `2` dem Port `1/2` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/3`.
`vlan participation include 3`	Port `1/3` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port-VLAN-ID `3` dem Port `1/3` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/4`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/4`.
`vlan participation include 2`	Port `1/4` wird Mitglied des VLANs `2` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 2`	Port-VLAN-ID `2` dem Port `1/4` zuweisen.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/5`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/5`.
`vlan participation include 3`	Port `1/5` wird Mitglied des VLANs `3` und vermittelt die Datenpakete ohne VLAN-Tag.
`vlan pvid 3`	Port-VLAN-ID `3` dem Port `1/5` zuweisen.

```
exit
```
Wechsel in den Konfigurationsmodus.

```
exit
```
Wechsel in den Privileged-EXEC-Modus.

```
show vlan id 3
```
Details zu VLAN 3 anzeigen.

```
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time..........0 days, 00:07:47 (System Uptime)
VLAN Routing................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

12.2 Gast-VLAN / Unauthentifiziertes VLAN

Ein Gast-VLAN ermöglicht einem Gerät die Bereitstellung einer Port-basierten Netzzugriffssteuerung (IEEE 802.1x) für Supplikanten ohne 802.1x-Fähigkeit. Diese Funktion stellt eine Vorrichtung zur Verfügung, die es Gästen ermöglicht, ausschließlich auf externe Netze zuzugreifen. Wenn Sie Supplikanten ohne 802.1x-Fähigkeit an einen aktiven, nicht autorisierten 802.1x-Port anschließen, senden die Supplikanten keine Antworten auf 802.1x-Anfragen. Da die Supplikanten keine Antworten senden, bleibt der Port im Status „nicht autorisiert“. Die Supplikanten haben keinen Zugriff auf externe Netze.

Bei der Supplikanten-Funktion von Gast-VLANs handelt es sich um eine Konfiguration auf Basis einzelner Ports. Wenn Sie einen Port als Gast-VLAN konfigurieren und Supplikanten ohne 802.1x-Fähigkeit an diesen Port anschließen, weist das Gerät die Supplikanten dem Gast-VLAN zu. Durch Hinzufügen von Supplikanten zu einem Gast-VLAN wechselt der Port in den Status „autorisiert“ und erlaubt so den Supplikanten den Zugriff auf externe Netze.

Ein UnauthentifiziertesVLAN ermöglicht dem Gerät, Dienste für 802.1x-fähige Supplikanten bereitzustellen, welche sich nicht korrekt anmelden. Diese Funktion ermöglicht den nicht autorisierten Supplikanten den Zugriff auf eine begrenzte Zahl von Diensten. Wenn Sie an einem Port ein Unauthentifiziertes VLAN konfigurieren und die 802.1x-Port-Authentifizierung ebenso wie die globale Funktion aktiviert haben, ordnet das Gerät den Port dem Unauthentifizierten VLAN zu. Wenn sich ein Supplikant mit 802.1x-Fähigkeit nicht korrekt an dem Port authentisiert, fügt das Gerät den Supplikanten dem Unauthentifizierten VLAN hinzu. Wenn Sie zudem ein Gast-VLAN an dem Port konfigurieren, verwenden Supplikanten ohne 802.1x-Fähigkeit das Gast-VLAN.

Bei Zuweisung eines Unauthentifizierten VLANs zählt der Zähler für die Reauthentifizierung herunter. Das Unauthentifizierte VLAN authentifiziert sich erneut, wenn die in Spalte *Reauthentifizierungs-Periode [s]* festgelegte Zeit abläuft und Supplikanten auf dem Port vorhanden sind. Falls keine Supplikanten vorhanden sind, ordnet das Gerät den Port dem konfigurierten Gast-VLAN zu.

Das nachstehende Beispiel erläutert das Erzeugen eines Gast-VLANs. Ein nicht autorisiertes VLAN erzeugen Sie auf die gleiche Weise.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Legen Sie im Feld *VLAN-ID* den Wert `10` fest.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Legen Sie für das VLAN den Namen `Gast` fest:
  Doppelklicken Sie in Spalte *Name* und legen den Namen fest.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Legen Sie im Feld *VLAN-ID* den Wert `20` fest.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Legen Sie für das VLAN den Namen `Nicht autorisiert` fest:
  Doppelklicken Sie in Spalte *Name* und legen den Namen fest.
- ☐ Öffnen Sie den Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

- ☐ Öffnen Sie den Dialog *Netzsicherheit > 802.1X Port-Authentifizierung > Port-Konfiguration*.
- ☐ Legen Sie für Port `1/4` die folgenden Einstellungen fest:
  - Den Wert `auto` in Spalte *Port-Kontrolle*
  - Den Wert `10` in Spalte *Gast VLAN-ID*
  - Den Wert `20` in Spalte *Unauthenticated-VLAN-ID*
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`vlan add 10`	Erzeugt VLAN `10`.
`vlan add 20`	Erzeugt VLAN `20`.
`name 10 Guest`	Benennt VLAN `10` um in `Guest`.
`name 20 Unauth`	Benennt VLAN `20` um in `Unauth`.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dot1x system-auth-control enable`	Die Funktion *802.1X Port-Authentifizierung* global einschalten.
`dot1x port-control auto`	Schaltet die Port-Kontrolle auf Port `1/4` ein.
`interface 1/4`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/4`.
`dot1x guest-vlan 10`	Weist Port `1/4` das Gast-VLAN zu.
`dot1x unauthenticated-vlan 20`	Weist Port `1/4` das nicht autorisierte VLAN zu.
`exit`	Wechsel in den Konfigurationsmodus.

12.3 RADIUS-VLAN-Zuordnung

Die Funktion der RADIUS-VLAN-Zuordnung ermöglicht, eine RADIUS-VLAN-Kennung mit einem authentisierten Client zu verknüpfen. Wenn sich ein Client erfolgreich authentisiert und der RADIUS-Server ein VLAN-Attribut sendet, verknüpft das Gerät den Client mit dem vom RADIUS-Server zugewiesenen VLAN. Infolgedessen fügt das Gerät den physikalischen Port dem entsprechenden VLAN als Mitglied hinzu und setzt die Port-VLAN-ID (PVID) auf den vorgegebenen Wert. Der Port vermittelt die Datenpakete ohne VLAN-Tag.

12.4 Voice-VLAN erzeugen

Verwenden Sie die Voice-VLAN-Funktion, um den Sprach- und Datenverkehr an einem Port nach VLAN und/oder Priorität zu trennen. Ein wesentlicher Nutzen bei der Verwendung eines Voice-VLANs liegt darin, in Zeiten mit erhöhtem Datenverkehrsaufkommen die Sprachqualität bei einem IP-Telefon sicherzustellen.

Das Gerät verwendet die Quell-MAC-Adresse zur Identifizierung und Priorisierung des Sprachdatenstroms. Durch die Verwendung einer MAC-Adresse zur Geräte-Identifizierung verhindert das Gerät, dass sich ein bösartiger Client mit demselben Port verbindet und dadurch eine Verschlechterung des Sprachverkehrs verursacht.

Ein weiterer Nutzen der Voice-VLAN-Funktion liegt darin, dass das VoIP-Telefon durch die Verwendung von LLDP-Med eine VLAN-Kennung oder Prioritätsinformationen erhält. Infolgedessen sendet das Telefon die Sprachdaten entweder mit Markierung, mit Prioritätsmarkierung oder ohne Markierung. Dieses ist abhängig von der Konfiguration des Voice-VLAN-Interfaces.

Nachstehend finden Sie eine Auflistung der möglichen Modi für das Voice-VLAN-Interface. Die ersten 3 Methoden trennen Sprach- und Datenverkehr und versehen beide mit einer Priorisierung. Die Trennung des Verkehrs führt zu einer besseren Qualität des Sprachverkehrs in Zeiten erhöhten Verkehrsaufkommens.

- Wenn Sie bei dem Port den Modus `vlan` konfigurieren, ermöglicht dem Gerät, die von einem VoIP-Telefon kommenden Sprachdaten mit der benutzerdefinierten Voice-VLAN-ID zu markieren. Das Gerät weist reguläre Daten dann der voreingestellten Port-VLAN-ID zu.
- Wenn Sie bei dem Port den Modus `dot1p-priority` konfigurieren, ermöglicht dem Gerät, die von einem VoIP-Telefon kommenden Daten mit VLAN 0 und der benutzerdefinierten Priorität zu markieren. Das Gerät weist regulären Daten dann die Standardpriorität des Ports zu.
- Sie konfigurieren sowohl die Voice-VLAN-ID wie auch die Priorität auf den Modus `vlan/dot1p-priority`. In diesem Modus sendet das VoIP-Telefon Sprachdaten mit der benutzerdefinierten Voice-VLAN-ID und den benutzerdefinierten Prioritätsinformationen. Das Gerät weist regulären Daten dann die Standard-PVID und die Standardpriorität des Ports zu.
- Wenn Sie das Telefon mit dem Wert `untagged` konfigurieren, sendet dieses unmarkierte Pakete.
- Wenn Sie das Telefon mit dem Wert `none` konfigurieren, verwendet dieses seine eigene Konfiguration zum Senden von Sprachverkehr.

13 Redundanz

13.1 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

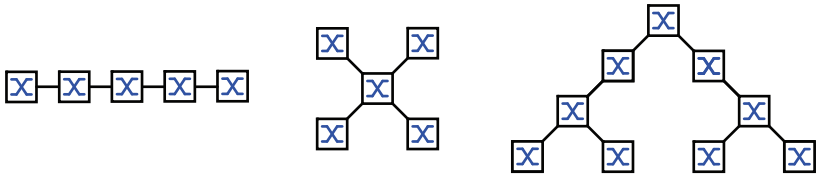


Abb. 28: Netz mit Linien-, Stern- und Baum-Topologie

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. In Abhängigkeit von der gewählten Netz-Topologie wählen Sie danach unter den Redundanzprotokollen aus, die sich mit dieser Netz-Topologie einsetzen lassen.

13.1.1 Netz-Topologien

Maschen-Topologie

Für Netze mit Stern- oder Baum-Topologie sind Redundanzverfahren ausschließlich im Zusammenhang mit physikalischer Schleifenbildung möglich. Ergebnis ist eine Maschen-Topologie.

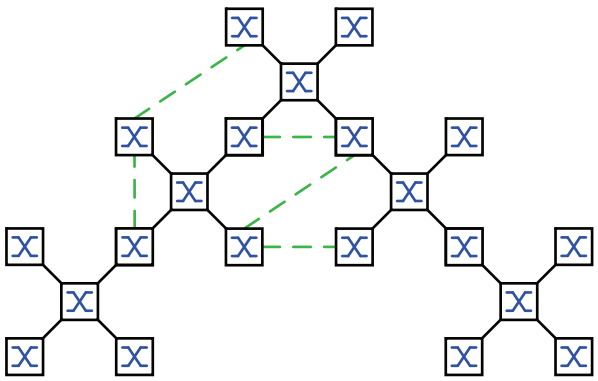


Abb. 29: Maschen-Topologie: Baum-Topologie mit physikalischen Schleifen

Für den Betrieb in dieser Netz-Topologie stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:

- Rapid Spanning Tree (RSTP)

Ring-Topologie

In Netzen mit Linien-Topologie lassen sich Redundanzverfahren nutzen, indem Sie die Enden der Linie verbinden. Dadurch entsteht eine Ring-Topologie.

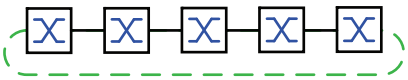


Abb. 30: Ring-Topologie: Linien-Topologie mit verbundenen Enden

Für den Betrieb in dieser Netz-Topologie stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:

- Media Redundancy Protocol (MRP)
- Rapid Spanning Tree (RSTP)

13.1.2 Redundanzprotokolle

Für den Betrieb in unterschiedlichen Netz-Topologien stellt Ihnen das Gerät folgende Redundanzprotokolle zur Verfügung:

Tab. 31: Redundanzprotokolle im Überblick

Redundanzprotokoll	Netz-Topologie	Bemerkungen
MRP	Ring	Die Umschaltzeit ist wählbar und nahezu unabhängig von der Anzahl der Geräte. Ein MRP-Ring besteht aus bis zu 50 Geräten, die das MRP-Protokoll nach IEC 62439 unterstützen. Wenn Sie ausschließlich Schneider Electric-Geräte einsetzen, sind bis zu 100 Geräte im MRP-Ring möglich.
Subring	Ring	Die Funktion *Sub Ring* ermöglicht Ihnen eine einfache Ankopplung von Netzsegmenten an bestehende Redundanz-Ringe.
Ring-/Netzkopplung	Ring	
RCP	Ring	
RSTP	beliebige Struktur	Die Umschaltzeit ist abhängig von der Netz-Topologie und von Anzahl der Geräte. - typ. < 1 s bei RSTP - typ. < 30 s bei STP
Link-Aggregation	beliebige Struktur	Eine Link-Aggregation-Gruppe ist eine Kombination von 2 oder mehr Punkt-zu-Punkt-Verbindungen, die mit derselben Geschwindigkeit und demselben Duplex-Modus arbeiten, um die Bandbreite zu erhöhen.

Tab. 31: Redundanzprotokolle im Überblick (Forts

Redundanzpro-tokoll	Netz-Topologie	Bemerkungen
Link-Backup	beliebige Struktur	Wenn das Gerät einen Fehler auf dem primären Link erkannt hat, leitet das Gerät den Datenverkehr zum Backup-Link um. Sie verwenden Link-Backup üblicherweise in Netzen von Dienstanbietern oder Unternehmen.
HIPER-Ring-Client	Ring	Vorhandenen HIPER-Ring erweitern oder ein Gerät ersetzen, das bereits als Client in einem HIPER-Ring aktiv ist.
HIPER-Ring über LAG	Ring	Geräte über eine Link-Aggregationsgruppe (LAG) miteinander verbinden. Die Ring-Clients und der Ring-Manager verhalten sich wie ein Ring ohne eine LAG-Instanz.

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

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Wenn Sie eine Redundanzfunktion einsetzen, dann deaktivieren Sie die Flusskontrolle auf den beteiligten Ports.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

13.1.3 Redundanzkombinationen

Tab. 32: Redundanzprotokolle im Überblick

	MRP	RSTP	Link-Aggreg.	Link-Backup	Subring	HIPER-Ring
MRP	▲	– – –	– – –	– – –	– – –	– – –
RSTP	▲ 1)	▲	– – –	– – –	– – –	– – –
Link-Aggreg.	▲ 2)	▲ 2)	▲	– – –	– – –	– – –
Link-Backup	▲	▲	▲	▲	– – –	– – –
Subring	▲	▲	▲ 2)	▲	▲	– – –
HIPER-Ring	▲	▲ 1)	▲ 2)	▲	▲	▲

▲ Kombinierbar

1) Eine redundante Kopplung zwischen diesen Netztopologien führt möglicherweise zu Loops.
Wie Sie diese Topologien redundant koppeln, entnehmen Sie Kapitel „FuseNet” auf Seite 222.

2) Kombinierbar auf demselben Port

13.2 Media Redundancy Protocol (MRP)

Das Media Redundancy Protocol (MRP) ist eine seit Mai 2008 standardisierte Lösung für Ring-Redundanz im industriellen Umfeld.

MRP ist kompatibel zur redundanten Ringkopplung, unterstützt VLANs und zeichnet sich durch sehr kurze Rekonfigurationszeiten aus.

Ein MRP-Ring besteht aus bis zu 50 Geräten, die das MRP-Protokoll nach IEC 62439 unterstützen. Wenn Sie ausschließlich Schneider Electric-Geräte einsetzen, sind bis zu 100 Geräte im MRP-Ring möglich.

Wenn Sie den festgelegten MRP-Redundanzport (Fixed Backup) verwenden und das Gerät einen Ausfall des primären Ring-Links erkennt, vermittelt der Ring-Manager die Daten an den sekundären Ring-Link. Bei Wiederherstellung des primären Links wird der sekundäre Link weiterhin benutzt.

13.2.1 Netzstruktur

Das Konzept der Ring-Redundanz ermöglicht Ihnen, hochverfügbare, ringförmige Netzstrukturen aufzubauen.

Mit Hilfe der RM-Funktion (**R**ing-**M**anager) können die beiden Enden eines Backbones in Linienstruktur zu einem redundanten Ring geschlossen werden. Der Ring-Manager hält die redundante Strecke solange offen, wie die Linienstruktur intakt ist. Fällt ein Segment aus, schließt der Ring-Manager sofort die redundante Strecke und die Linienstruktur ist wieder intakt.

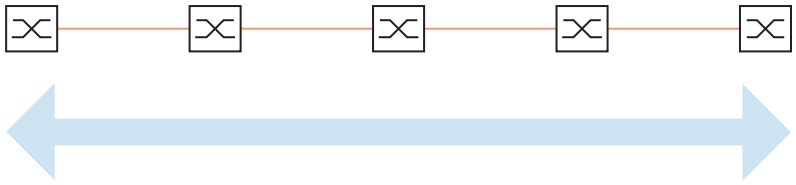


Abb. 31: Linienstruktur

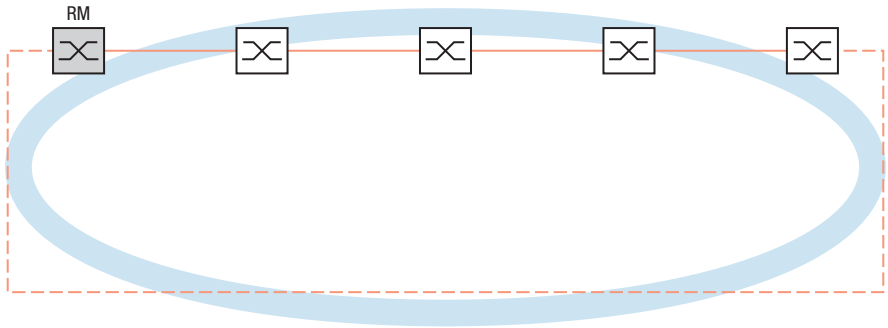


Abb. 32: Redundante Ringstruktur
RM = Ring-Manager
—— Hauptleitung
- - - redundante Leitung

13.2.2 Rekonfigurationszeit

Bei Erkennen des Ausfalls einer Teilstrecke wandelt der Ring-Manager den MRP-Ring zurück in eine Linienstruktur. Die maximale Zeit für die Rekonfiguration der Strecke legen Sie im Ring-Manager fest.

Mögliche Werte für die maximale Verzögerungszeit sind:
- `500ms`
- `30ms`

Anmerkung: Wenn jedes Gerät im Ring die kürzere Verzögerungszeit unterstützt, können Sie die Rekonfigurationszeit mit einem kleineren Wert als `500ms` konfigurieren.

Andernfalls sind die Geräte, die ausschließlich längere Verzögerungszeiten unterstützen, wegen Überlastung möglicherweise unerreichbar. Infolgedessen können Loops entstehen.

13.2.3 Advanced Mode

Für noch kürzere als die festgelegten Rekonfigurationszeiten bietet das Gerät den Advanced Mode. Der Advanced Mode beschleunigt die Link-Ausfall-Erkennung, wenn die Ringteilnehmer dem Ring-Manager Unterbrechungen im Ring durch Link-Down-Meldungen signalisieren.

Schneider Electric-Geräte unterstützen Link-Down-Meldungen. Aktivieren Sie deshalb generell im Ring-Manager den Advanced Mode.

Falls Sie Geräte einsetzen, die keine Link-Down-Meldungen senden, rekonfiguriert der Ring-Manager die Strecke in der gewählten maximalen Rekonfigurationszeit.

13.2.4 Voraussetzungen für MRP

Bevor Sie einen MRP-Ring einrichten, vergewissern Sie sich, dass die folgenden Voraussetzungen erfüllt sind:
- ▶ Alle Ringteilnehmer unterstützen MRP.
- ▶ Die Ring-Teilnehmer sind über die Ring-Ports miteinander verbunden. Am jeweiligen Gerät sind außer seinen Nachbarn keine weiteren Ring-Teilnehmer angeschlossen.
- ▶ Alle Ringteilnehmer unterstützen die im Ring-Manager festgelegte Rekonfigurationszeit.
- ▶ Im Ring existiert genau ein Ring-Manager.

Wenn Sie VLANs verwenden, konfigurieren Sie jeden Ring-Port mit folgenden Einstellungen:
- ☐ Ingress-Filtering deaktivieren, siehe Dialog *Switching > VLAN > Port*.
- ☐ Port-VLAN-ID (PVID) festlegen, siehe Dialog *Switching > VLAN > Port*.
  - – PVID = `1`, wenn das Gerät die MRP-Datenpakete unmarkiert überträgt (VLAN-ID = `0` im Dialog *Switching > L2-Redundanz > MRP*)
    Durch die Einstellung PVID = `1` weist das Gerät die unmarkiert empfangenen Pakete automatisch dem VLAN 1 zu.
  - – PVID = `any`, wenn das Gerät die MRP-Datenpakete in einem VLAN überträgt (VLAN-ID ≥ `1` im Dialog *Switching > L2-Redundanz > MRP*)
- ☐ Egress-Regeln festlegen, siehe Dialog *Switching > VLAN > Konfiguration*.
  - – `U` (unmarkiert) für die Ring-Ports von VLAN 1, wenn das Gerät die MRP-Datenpakete unmarkiert überträgt (VLAN-ID = `0` im Dialog *Switching > L2-Redundanz > MRP*, der MRP-Ring ist keinem VLAN zugewiesen).
  - – `T` (tagged), für die Ring-Ports in dem VLAN, das Sie dem MRP-Ring zuweisen. Wählen Sie `T`, wenn das Gerät die MRP-Datenpakete in einem VLAN überträgt (VLAN-ID ≥ `1` im Dialog *Switching > L2-Redundanz > MRP*).

13.2.5 Beispiel-Konfiguration

Ein Backbone-Netz enthält 3 Geräte in einer Linienstruktur. Um die Verfügbarkeit des Netzes zu erhöhen, überführen Sie die Linienstruktur in eine redundante Ringstruktur. Zum Einsatz kommen Geräte unterschiedlicher Hersteller. Alle Geräte unterstützen MRP. Auf jedem Gerät legen Sie die Ports 1.1 und 1.2 als Ring-Ports fest.

Bei Erkennen eines Ausfalls des primären Ring-Links, sendet der Ring-Manager Daten auf dem sekundären Ring-Link. Bei Wiederherstellung des primären Links wechselt der sekundäre Link zurück in den Backup-Modus.

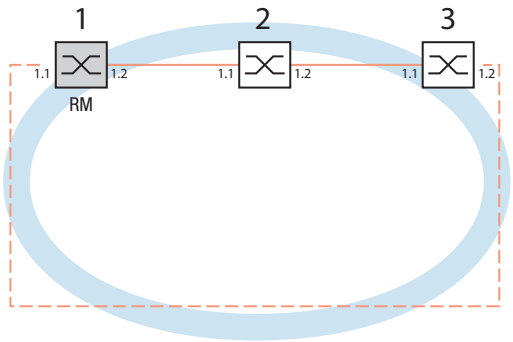


Abb. 33: Beispiel eines MRP-Rings
RM = Ring-Manager
—— Hauptleitung
- - - redundante Leitung

Die folgende Beispielkonfiguration beschreibt die Konfiguration des Ring-Manager-Geräts (1). Die 2 anderen Geräte (2 bis 3) konfigurieren Sie analog, ohne jedoch die Funktion *Ring-Manager* zu aktivieren. Dieses Beispiel nutzt kein VLAN. Als Ring-Wiederherstellungszeit legen Sie den Wert `30ms` fest. Jedes Gerät unterstützt den Advanced Mode des Ring-Managers.

- ☐ Bauen Sie das Netz nach Ihren Erfordernissen auf.
- ☐ Konfigurieren Sie jeden Port so, dass die Datenrate und die Duplexeinstellungen der Strecken der folgenden Tabelle entsprechen:

Tab. 33: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–
Optisch	2.5 Gbit/s	`markiert`	–	*`2,5 Gbit/s FDX`*

Anmerkung: Optische Ports ohne Unterstützung für Autonegotiation (automatische Konfiguration) konfigurieren Sie mit 100 Mbit/s Vollduplex (FDX) oder 1000 Mbit/s Vollduplex (FDX).

Anmerkung: Optische Ports ohne Unterstützung für Autonegotiation (automatische Konfiguration) konfigurieren Sie mit 100 Mbit/s Vollduplex (FDX).

Anmerkung: Konfigurieren Sie jedes Gerät des MRP-Rings individuell. Bevor Sie die redundante Leitung anschließen, vergewissern Sie sich, dass Sie die Konfiguration jedes Geräts des MRP-Rings abgeschlossen haben. So vermeiden Sie Loops während der Konfigurationsphase.

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *MRP*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

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`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`no spanning-tree operation`	Schaltet Spanning Tree aus.
`show spanning-tree global`	Zeigt zur Kontrolle die Parameter.

Schalten Sie MRP auf allen Geräten im Netz ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > MRP*.
- ☐ Legen Sie die gewünschten Ring-Ports fest.

Im Command Line Interface definieren Sie zunächst einen zusätzlichen Parameter, die MRP-DomänenID. Konfigurieren Sie jeden Ringteilnehmer mit der gleichen MRP-DomänenID. Die MRP-Domänen-ID ist eine Folge aus 16 Ziffernblöcken (8-Bit-Werten).

Beim Konfigurieren mit der grafischen Benutzeroberfläche verwendet das Gerät den Vorgabewert („default domain“) `255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255`.

`mrp domain add default-domain`	Erzeugt eine neue MRP-Domäne mit der ID `default-domain`.
`mrp domain modify port primary 1/1`	Port *1/1* als Ring-Port `1` festlegen.
`mrp domain modify port secondary 1/2`	Port *1/2* als Ring-Port `2` festlegen.

Schalten Sie den *Fixed backup*-Port ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ Schalten Sie den Ring-Manager ein.
  Bei den anderen Geräten im Ring belassen Sie die Einstellung auf *Aus*.
- ☐ Um zuzulassen, dass das Gerät nach Wiederherstellung des Rings das Senden der Daten auf dem sekundären Ports fortsetzt, markieren Sie das Kontrollkästchen *Fixed backup*.

Anmerkung: Wenn das Gerät zum primären Port zurückwechselt, wird ggf. die maximal zulässige Ring-Wiederherstellungszeit überschritten.

Wenn Sie die Markierung des Kontrollkästchens *Fixed backup* aufheben und der Ring wiederhergestellt ist, blockiert der Ring-Manager den sekundären Ports und hebt die Blockierung des primären Ports auf.

```
mrp domain modify port secondary 1/2
fixed-backup enable
```

Aktivieren der Funktion *Fixed backup* auf dem sekundären Port. Nach Wiederherstellung des Rings leitet der sekundäre Port die Daten weiter.

- ☐ Schalten Sie den Ring-Manager ein.
  Bei den anderen Geräten im Ring belassen Sie die Einstellung auf *Aus*.

```
mrp domain modify mode   manager
```

Legt fest, dass das Gerät als *Ring-Manager* arbeitet. Bei den anderen Geräten im Ring belassen Sie die Voreinstellung.

- ☐ Markieren Sie das Kontrollkästchen im Feld *Advanced mode*.

```
mrp domain modify   advanced-mode
enabled
```

Schaltet den Advanced Mode ein.

- ☐ Wählen Sie im Feld *Ring-Rekonfiguration* den Wert *30ms* aus.

```
mrp domain modify   recovery-delay
200ms
```

Legt den Wert *30ms* fest als max. Verzögerungszeit bei der Rekonfiguration des Rings.

Anmerkung: Wenn bei der Wahl des Werts *30ms* für die Ringrekonfiguration die Stabilität des Rings nicht den Anforderungen an Ihr Netz entspricht, dann wählen Sie den Wert *500ms*.

- ☐ Aktivieren Sie die Funktion des MRP-Rings.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

```
mrp domain modify operation   enable
```

Schaltet den MRP-Ring ein.

Wenn jeder Ring-Teilnehmer konfiguriert ist, schließen Sie die Linie zum Ring. Verbinden Sie dazu die Geräte an den Enden der Linie über ihre Ring-Ports.

Kontrollieren Sie die Meldungen des Geräts. Führen Sie dazu die folgenden Schritte aus:

`show mrp` Zeigt zur Kontrolle die Parameter.

Das Feld *Funktion* zeigt den Betriebszustand des Ring-Ports.

Mögliche Werte:
- `forwarding`
  Der Port ist eingeschaltet, Verbindung vorhanden.
- `blocked`
  Der Port ist blockiert, Verbindung vorhanden.
- `disabled`
  Der Port ist ausgeschaltet.
- `not-connected`
  Keine Verbindung vorhanden.

Das Feld *Information* zeigt Meldungen zur Redundanzkonfiguration und mögliche Ursachen für erkannte Fehler.

Wenn das Gerät als Ring-Client oder als Ring-Manager arbeitet, sind folgende Meldungen möglich:
- *Redundanz verfügbar*
  Die Redundanz ist eingerichtet. Fällt eine Komponente des Rings aus, übernimmt die redundante Strecke deren Funktion.
- *Konfigurationsfehler: Ring-Port-Verbindung fehlerhaft*
  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.
  Aktivieren Sie die Funktion *Ring-Manager* bei genau 1 Gerät im Ring.
- *Konfigurationsfehler: Verbindung im Ring ist mit falschem Port verbunden*
  Eine Leitung des Rings ist anstatt mit einem Ring-Port mit einem anderen Port verbunden.
  Das Gerät empfängt Test-Datenpakete ausschließlich auf einem Ring-Port.

Gliedern Sie den MRP-Ring gegebenenfalls in ein VLAN ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ Legen Sie im Feld *VLAN-ID* die MRP-VLAN-ID fest. Die MRP-VLAN-ID bestimmt, in welchem der eingerichteten VLANs das Gerät die MRP-Pakete vermittelt.
  Um die MRP-VLAN-ID zu setzen, konfigurieren Sie zuerst die VLANs und die zugehörigen Egress-Regeln im Dialog *Switching > VLAN > Konfiguration*.
  - Soll der MRP-Ring keinem VLAN zugewiesen sein (wie in diesem Beispiel), belassen Sie die VLAN-ID auf `0`.
    Legen Sie im Dialog *Switching > VLAN > Konfiguration* für die Ring-Ports im VLAN `U` die VLAN-Zugehörigkeit `1` (unmarkiert) fest.
  - Soll der MRP-Ring einem VLAN zugewiesen sein, geben Sie eine VLAN-ID > `0` ein.
    Legen Sie im Dialog *Switching > VLAN > Konfiguration* für die Ring-Ports im gewählten VLAN die VLAN-Zugehörigkeit `T` (Tagged) fest.

`mrp domain modify vlan <0..4042>` Weist die VLAN-ID zu.

13.2.6 MRP-over-LAG

Schneider Electric-Geräte ermöglichen Ihnen, zum Erhöhen der Bandbreite Link-Aggregation-Gruppen (LAG) mit dem für die Redundanz eingesetzten Media-Redundancy-Protokoll (MRP) zu kombinieren. Die Funktion ermöglicht Ihnen, die Bandbreite in einzelnen Segmenten oder im gesamten Netz zu erhöhen.

Die Funktion *Link-Aggregation* unterstützt Sie dabei, die Bandbreitenbegrenzung für einzelne Ports aufzuheben. LAG ermöglicht Ihnen, 2 oder mehr Verbindungen zu einer logischen Verbindung zwischen 2 Geräten zusammenzufassen. Die parallelen Links erhöhen die Übertragungsbandbreite zwischen den 2 Geräten.

Ein MRP-Ring besteht aus bis zu 50 Geräten, die das MRP-Protokoll nach IEC 62439 unterstützen. Wenn Sie ausschließlich Schneider Electric-Geräte verwenden, dann ermöglicht Ihnen das Protokoll, MRP-Ringe mit bis zu 100 Geräten zu konfigurieren.

MRP-over-LAG verwenden Sie in folgenden Fällen:
- zum Erhöhen der Bandbreite in einzelnen Segmenten eines MRP-Rings
- zum Erhöhen der Bandbreite im gesamten MRP-Ring

Netzstruktur

Beim Konfigurieren eines MRP-Rings mit LAGs überwacht der Ring-Manager (RM) beide Enden des Backbones auf Durchgang. Der RM blockiert Daten auf dem sekundären (redundanten) Port, solange der Backbone intakt ist. Wenn der RM eine Unterbrechung des Datenstroms im Ring erkennt, dann vermittelt er die Daten an den sekundären Port und sorgt so für eine erneute Backbone-Anbindung.

LAG-Instanzen verwenden Sie in MRP-Ringen ausschließlich, um die Bandbreite zu erhöhen, während MRP für die Redundanz sorgt.

Damit ein RM eine Unterbrechung im Ring erkennt, benötigt MRP ein Gerät, das jeden Port in der LAG-Instanz blockiert, wenn ein Port in der Instanz ausfällt.

LAG in einem einzelnen Segment eines MRP-Rings

Das Gerät ermöglicht Ihnen, eine LAG-Instanz in einzelnen Segmenten eines MRP-Rings zu konfigurieren.

Für Geräte im MRP-Ring nutzen Sie das LAG-Single-Switch-Verfahren. Das Single-Switch-Verfahren bietet Ihnen eine preiswerte Möglichkeit, Ihr Netz zu erweitern, indem Sie lediglich ein Gerät auf jeder Seite eines Segments verwenden, um die physischen Ports zur Verfügung zu stellen. Um die Bandbreite für bestimmte Segmente im Bedarfsfall zu erhöhen, fassen Sie die Ports des Geräts zu einer LAG-Instanz zusammen.

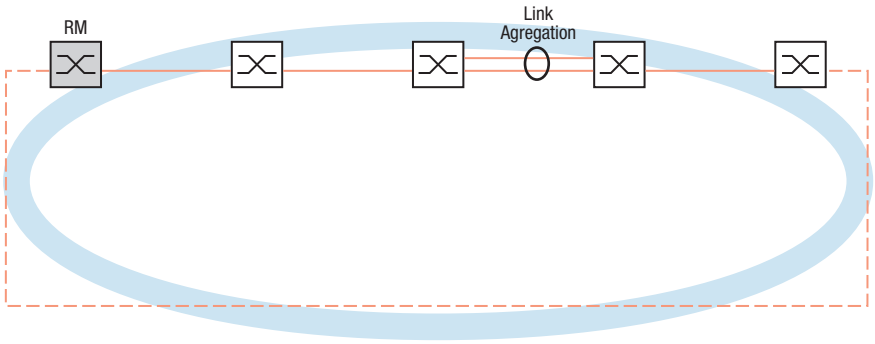


Abb. 34: Link-Aggregation über eine einzelne Verbindung eines MRP-Rings

LAG im gesamten MRP-Ring

Neben dem Konfigurieren einer LAG-Instanz in bestimmten Segmenten eines MRP-Rings ermöglichen Ihnen Schneider Electric-Geräte auch, LAG-Instanzen in jedem Segment zu konfigurieren, um die Bandbreite im gesamten MRP-Ring zu erhöhen.

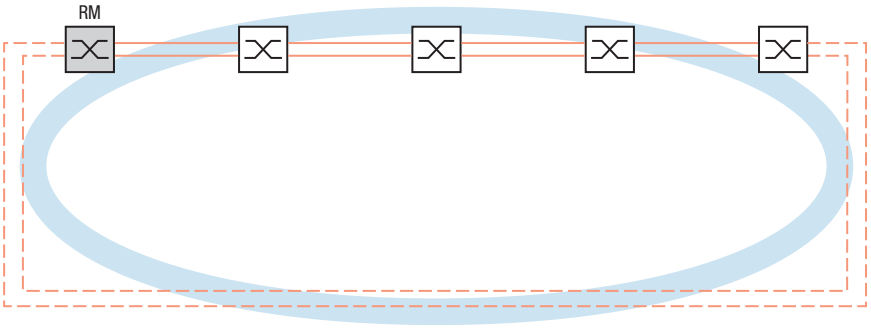


Abb. 35: Link-Aggregation für den gesamten MRP-Ring

Ermittlung von Unterbrechungen im Ring

Beim Konfigurieren der LAG-Instanz legen Sie den Wert *Aktive Ports (min.)* fest, um die Gesamtzahl der in der LAG-Instanz verwendeten Ports anzugleichen. Wenn ein Gerät eine Unterbrechung an einem Port in der LAG-Instanz erkennt, dann blockiert es die Daten an den anderen Ports der Instanz. Wenn jeder Port einer Instanz blockiert ist, dann erkennt der RM, dass der Ring geöffnet ist und vermittelt die Daten an den sekundären Port. Auf diese Weise sorgt der RM für eine Verbindung zur anderen Seite des unterbrochenen Segments.

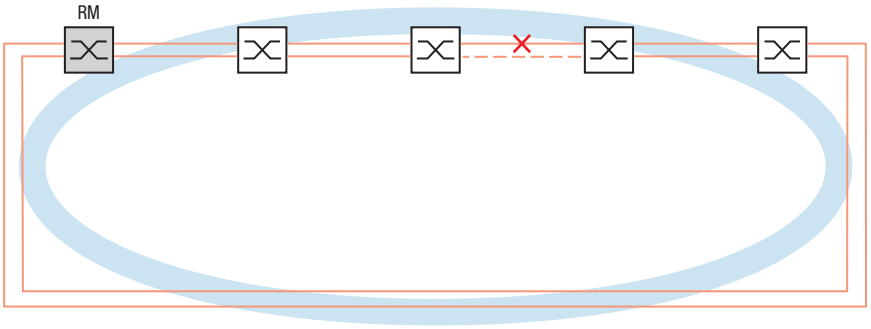


Abb. 36: Unterbrechung einer Verbindung in einem MRP-Ring

Beispiel-Konfiguration

Im folgenden Beispiel sind Switch A und Switch B gemeinsam mit Abteilungen verbunden. Das Verkehrsaufkommen der Abteilungen übersteigt die individuelle Bandbreitenkapazität der Ports. Um die Bandbreite des Segments zu erhöhen, konfigurieren Sie eine LAG-Instanz für das einzelne Segment des MRP-Rings.

Voraussetzung für die Beispielkonfiguration ist, dass Sie mit einem funktionsfähigen MRP-Ring beginnen.

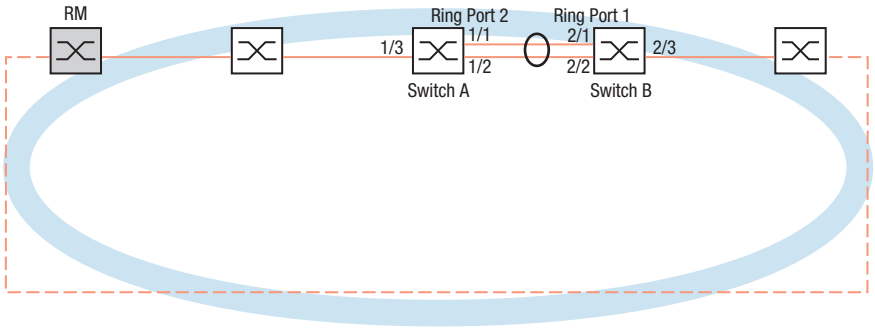


Abb. 37: Beispielkonfiguration für MRP-over-LAG

Konfigurieren Sie den Switch A zuerst. Führen Sie dazu die folgenden Schritte aus. Konfigurieren Sie Switch B mit den gleichen Schritten und ersetzen Sie dabei die entsprechenden Port- und Ring-Port-Nummern.

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Link-Aggregation*.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Wählen Sie in der Dropdown-Liste *Trunk-Port* die Instanz-Nummer der Link-Aggregation-Gruppe.
- ☐ Wählen Sie in der Dropdown-Liste *Port* den Port *1/1*.

- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Wiederholen Sie die vorherigen Schritte und wählen Sie den Port *1/2*.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ In der Spalte *Aktive Ports (min.)* geben Sie `2` ein, was in diesem Fall die Gesamtzahl der Ports in der LAG-Instanz ist. Wenn Sie MRP und LAG kombinieren, legen Sie die Gesamtzahl der Ports als *Aktive Ports (min.)* fest. Wenn das Gerät eine Unterbrechung an einem Port erkennt, dann blockiert es die anderen Ports der Instanz und bewirkt so das Öffnen des Rings. Der Ring-Manager erkennt, dass der Ring geöffnet ist und vermittelt die Daten an den sekundären Ring-Port, womit er die Verbindung zu den anderen Geräten im Netz wiederherstellt.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > MRP*.
- ☐ Wählen Sie im Rahmen *Ring-Port 2*, Dropdown-Liste *Port* den Port `lag/1`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`link-aggregation add lag/1`	Erzeugt eine Link-Aggregation-Gruppe `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Port *1/1* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 addport 1/2`	Port *1/2* zur Link-Aggregation-Gruppe hinzufügen.
`mrp domain modify port secondary lag/1`	Port `lag/1` als Ring-Port `2` festlegen.
`copy config running-config nvm`	Speichern der aktuellen Einstellungen im „ausgewählten" Konfigurationsprofil im permanenten Speicher (`nvm`).

13.3 HIPER-Ring-Client

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *HIPER-Ring*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Das Konzept der HIPER-Ring-Redundanz ermöglicht den Aufbau hochverfügbarer, ringförmiger Netzstrukturen. Die *HIPER-Ring*-Client-Funktion ermöglicht dem Netzadministrator, einen vorhandenen HIPER-Ring zu erweitern oder ein Client-Gerät zu ersetzen, das bereits Teilnehmer eines HIPER-Ringes ist.

Wenn das Gerät feststellt, dass der Daten-Link am Ring-Port abbricht, sendet das Gerät ein Link-Down-Datenpaket an den Ring-Manager (RM) und leert die FDB-Tabelle. Sobald der Ring-Manager das LinkDown-Datenpaket empfängt, vermittelt der Ring-Manager den Datenstrom über den Primär- und über den Sekundär-Ring-Port. So ist der Ring-Manager in der Lage, die Integrität des HIPER-Ringes aufrecht zu erhalten.

Das Gerät unterstützt ausschließlich Fast-Ethernet-Ports und Gigabit-Ethernet-Ports als Ring-Ports. Außerdem können Sie die Ring-Ports in eine LAG-Instanz einschließen.

In der Voreinstellung ist der HIPER-Ring-Client inaktiv, und die primären Ports und sekundären Ports sind auf `no Port` gesetzt.

Anmerkung: Deaktivieren Sie das Spanning Tree Protocol (STP) für die Ring-Ports im Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, da das STP und der HIPER-Ring verschiedene Reaktionszeiten besitzen.

Tab. 34: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
TX	1 Gbit/s	`markiert`	`markiert`	–
Optisch	100 Mbit/s	`markiert`	`unmarkiert`	*`100 Mbit/s FDX`*
Optisch	1 Gbit/s	`markiert`	`markiert`	–
Optisch	2.5 Gbit/s	`markiert`	–	*`2,5 Gbit/s FDX`*

13.3.1 VLANs am HIPER-Ring

Das Gerät ermöglicht Ihnen, VLAN-Daten über den HIPER-Ring weiterzuleiten. Somit bietet das Gerät Redundanz für Ihre VLAN-Daten. Das Ring-Gerät leitet Management-Daten um den Ring herum, zum Beispiel in VLAN 1. Damit die Daten die Management-Station erreichen, leiten die Ring-Geräte die unmarkierten Management-Daten an den Ring-Ports weiter. Legen Sie außerdem die Ring-Ports als Mitglieder in VLAN 1. fest.

Wenn andere VLANs Ihre Ring-Geräte durchqueren, leiten die Ring-Geräte die anderen VLAN-Daten als markiert weiter.

Legen Sie die VLAN-Einstellungen fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Unmarkierte VLAN-Management-Daten an den Ring-Ports weiterleiten.
  Wählen Sie für VLAN 1 in der Dropdown-Liste derjenigen Spalten, die sich auf den Ring-Port beziehen, den Eintrag `U`.
- ☐ Die Weiterleitung von Management-Paketen an den Nicht-Ring-Ports blockieren.
  Wählen Sie für VLAN 1 in der Dropdown-Liste derjenigen Spalten, die sich **nicht** auf den Ring-Port beziehen, den Eintrag `-` aus.
- ☐ Zulassen, dass ein Gerät im Ring die VLAN-Daten an und von Ports mit VLAN-Mitgliedschaft vermittelt.
  Wählen Sie für das VLAN in der Dropdown-Liste derjenigen Spalten, die sich auf den Ring-Port beziehen, den Eintrag `T` aus.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Den Ring-Ports die Mitgliedschaft in VLAN 1 zuweisen.
  Fügen Sie für die Ring-Ports in Spalte *Port-VLAN-ID* den Wert `1` ein.
- ☐ Den Nicht-Ring-Ports die Mitgliedschaft im VLAN zuweisen.
  Fügen Sie für die Nicht-Ring-Ports in Spalte *Port-VLAN-ID* die entsprechende VLAN-ID ein.

13.3.2 HIPER-Ring über LAG

Die Funktion *HIPER-Ring* ermöglicht Ihnen, die Geräte über eine Link-Aggregation-Gruppe (LAG) miteinander zu verbinden. Die Ring-Clients und der Ring-Manager verhalten sich wie ein Ring ohne eine LAG-Instanz.

Beim Ausfall einer LAG-Verbindung fällt auch die andere Datenverbindung in der Instanz aus und verursacht eine Unterbrechung des Ringes. Nach der Erkennung einer Unterbrechung im Ring senden die betroffenen Ports ein LinkDown-Datenpaket an den Ring-Manager. Der Ring-Manager hebt die Blockierung des sekundären Ports auf, indem er Daten in beide Richtungen auf den Ring sendet und mit einem Delete-Paket antwortet. Beim Empfang eines Delete-Paketes leeren die Ring-Teilnehmer ihre FDB.

13.4 Spanning Tree

Anmerkung: Das Spanning-Tree-Protokoll ist ein Protokoll für MAC-Bridges. Daher verwendet die folgende Beschreibung den Begriff Bridge für das Gerät.

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

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

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

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

Anmerkung: RSTP löst eine Schicht-2-Netztopologie mit redundanten Pfaden in eine Baumstruktur (Spanning Tree) auf, die keine redundanten Pfade mehr enthält. Eines der Geräte übernimmt dabei die Rolle der Root-Bridge. Die maximal erlaubte Anzahl der Geräte in einem aktiven Ast von der Root-Bridge bis zur Astspitze können Sie durch die Variable *Max age* der aktuellen Root-Bridge vorgeben. Der voreingestellte Wert für *Max age* ist `20`, er kann bis auf `40` erhöht werden.

Wenn das als Root arbeitende Gerät ausfällt und ein anderes Gerät dessen Funktion übernimmt, bestimmt die neue Root-Bridge die größtmögliche erlaubte Anzahl der Geräte in einem Branch durch ihre *Max age*-Einstellung.

Anmerkung: Der RSTP-Standard schreibt vor, dass jedes Gerät innerhalb eines Netzes mit dem (Rapid-) Spanning-Tree-Algorithmus arbeitet. Bei gleichzeitigem Einsatz von STP und RSTP gehen in den Netz-Segmenten, die gemischt betrieben werden, die Vorteile der schnelleren Rekonfiguration bei RSTP verloren.

Ein Gerät, das lediglich RSTP unterstützt, arbeitet mit MSTP-Geräten zusammen, indem es sich keiner MST-Region, sondern dem CST (Common Spanning Tree) zuweist.

13.4.1 Grundlagen

Da RSTP eine Weiterentwicklung des STP ist, gilt jede der folgenden Beschreibungen des STP auch für RSTP.

Die Aufgaben des STP

Der Spanning Tree-Algorithmus reduziert Netztopologien, die mit Bridges aufgebaut sind und Ringstrukturen durch redundante Verbindungen aufweisen, auf eine Baumstruktur. Dabei trennt STP die Ringstrukturen nach vorgegebenen Regeln auf, indem es redundante Pfade deaktiviert. Wird ein Pfad unterbrochen, weil eine Netzkomponente betriebsunfähig wird, aktiviert das STP den zuvor deaktivierten Pfad wieder. Dies ermöglicht redundante Verbindungen zur Erhöhung der Kommunikationsverfügbarkeit.

Das STP ermittelt bei der Bildung der Baumstruktur eine Bridge, die die Basis der STP-Baumstruktur repräsentiert. Diese Bridge heißt Root-Bridge.

Merkmale des STP-Algorithmus:
- automatische Rekonfiguration der Baumstruktur bei Bridge-Ausfällen oder Unterbrechung eines Datenpfades,
- Stabilisierung der Baumstruktur bis zur maximalen Netzausdehnung,
- Stabilisierung der Topologie innerhalb einer vorhersehbaren Zeit,
- durch den Administrator vorbestimmbare und reproduzierbare Topologie,
- Transparenz für die Endgeräte,
- geringe Netzlast gegenüber der verfügbaren Übertragungskapazität durch Einrichtung der Baumstruktur.

Die Bridge-Parameter

Jede Bridge und ihre Verbindungen werden im Kontext von Spanning Tree eindeutig durch die folgenden Parameter beschrieben:
- Bridge Identifier
- Root-Pfadkosten der Bridge-Ports,
- Port-Identifikation

Bridge Identifier

Die Bridge-Identifikation besteht aus 8 Bytes. Die 2 höchstwertigen Bytes sind die Priorität. Die Voreinstellung für die Prioritätszahl ist 32768 (8000H), jedoch kann der Management-Administrator diese zur Konfiguration des Netzes verändern. Die 6 niederwertigen Bytes der Bridge-Identifikation sind die MAC-Adresse der Bridge. Die MAC-Adresse ermöglicht, dass alle Bridges eine eindeutige Bridge-Identifikation besitzen.

Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation besitzt die höchste Priorität.

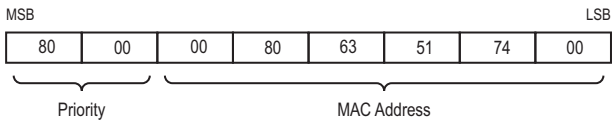


Abb. 38: Bridge-Identifikation, Beispiel (Werte in Hexadezimalschreibweise)

Root-Pfadkosten

Jedem Pfad, der 2 Bridges miteinander verbindet, weisen die Bridges Kosten für die Übertragung (Pfadkosten) zu. Das Gerät bestimmt diesen Wert in Abhängigkeit von der Datenrate (siehe Tabelle 35). Dabei weist das Gerät Pfaden mit niedrigerer Datenrate höhere Pfadkosten zu.

Alternativ dazu kann auch der Administrator die Pfadkosten festlegen. Dabei weist der Administrator - wie das Gerät - Pfaden mit niedrigerer Datenrate höhere Pfadkosten zu. Da er aber diesen Wert letztendlich frei wählen kann, verfügt er hiermit über ein Werkzeug, bei redundanten Pfaden einem bestimmten Pfad den Vorzug zu geben.

Die Root-Pfadkosten sind die Summe der einzelnen Pfadkosten derjenigen Pfade, die ein Datenpaket zwischen dem angeschlossenen Port einer Bridge und der Root-Bridge passiert.

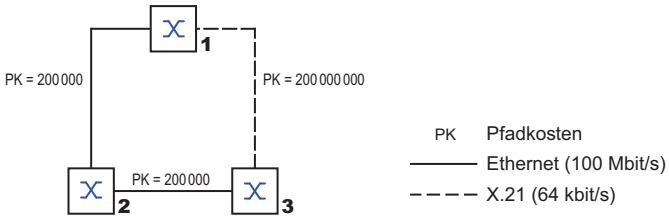


Abb. 39: Pfadkosten

Tab. 35: Empfohlene Pfadkosten beim RSTP in Abhängigkeit von der Datenrate.

Datenrate	Empfohlener Wert	Empfohlener Bereich	Möglicher Bereich
≤100 kbit/s	200 000000[1]	20000000-200000000	1-200000000
1 Mbit/s	20000000[a]	2000000-200000000	1-200000000
10 Mbit/s	2000000[a]	200000-20000000	1-200000000
100 Mbit/s	200000[a]	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200 000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

1. 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

Die Portidentifikation besteht aus 2 Bytes. Ein Teil, das niederwertigste Byte, enthält die physikalischen Portnummer. Dies gewährleistet eine eindeutige Bezeichnung des Port dieser Bridge. Der zweite, höherwertige Teil ist die Port-Priorität, die der Administrator festlegt (Voreinstellung: 128). Auch hier gilt: Der Port mit dem kleinsten Zahlenwert für die Portidentifikation besitzt die höchste Priorität.

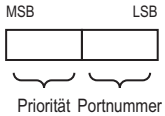


Abb. 40: Port-Identifikation

MaxAge und Diameter

Die Größen „MaxAge“ und „Diameter“ bestimmen maßgeblich die maximale Ausdehnung eines Spanning-Tree-Netzes.

Diameter

Die Anzahl der Verbindungen zwischen den am weitesten voneinander entfernten Geräten im Netz heißt Netzdurchmesser (Diameter).

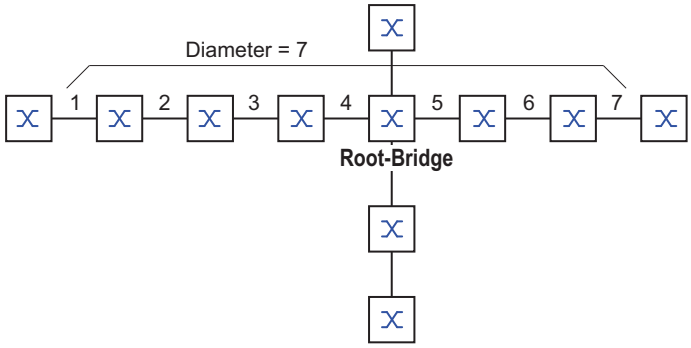


Abb. 41: Definition „Diameter“

Der im Netz erreichbare Netzdurchmesser beträgt MaxAge-1..

Im Lieferzustand ist MaxAge = 20, der maximal erreichbare Diameter = 19. Wenn Sie für MaxAge den Maximalwert 40 einstellen, ist der maximal erreichbare Diameter = 39.

MaxAge

Jede STP-BPDU enthält einen Zähler „MessageAge“. Der Zähler erhöht sich beim Durchlaufen einer Bridge um 1.

Die Bridge vergleicht vor dem Weiterleiten einer STP-BPDU den Zähler „MessageAge“ mit dem im Gerät festgelegten Wert „MaxAge“:

- Ist MessageAge < MaxAge, leitet die Bridge die STP-BPDU an die nächste Bridge weiter.
- Ist MessageAge = MaxAge, verwirft die Bridge die STP-BPDU.

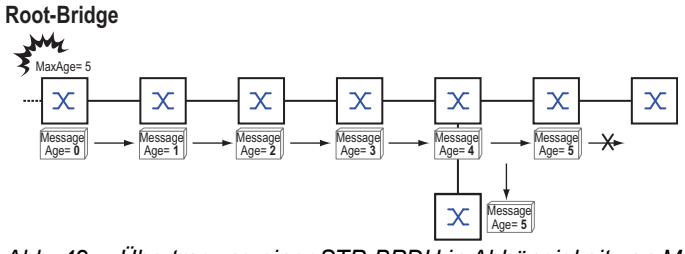


Abb. 42: Übertragung einer STP-BPDU in Abhängigkeit von MaxAge

13.4.2 Regeln für die Erstellung der Baumstruktur

Bridge-Information

Zur Berechnung der Baumstruktur benötigen die Bridges nähere Informationen über die anderen Bridges, die sich im Netz befinden.

Um diese Informationen zu erhalten, sendet jede Bridge eine BPDU (Bridge Protocol Data Unit) an andere Bridges.

Bestandteil einer BPDU ist unter anderem:
- Bridge-Identifikation
- Root-Pfadkosten
- Port-Identifikation

(siehe IEEE 802.1D)

Aufbauen der Baumstruktur

Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation nennt man auch Root-Bridge. Sie bildet die Root (Wurzel) der Baumstruktur

Der Aufbau des Baumes ist abhängig von den Root-Pfadkosten. Spanning Tree wählt die Struktur so, dass die minimalen Pfadkosten zwischen jeder einzelnen Bridge zur Root-Bridge entstehen.

- Bei mehreren Pfaden mit gleichen Root-Pfadkosten entscheidet die von der Root weiter entfernte Bridge, welchen Port sie blockiert. Sie verwendet dazu die Bridge-Identifikationen der näher an der Root liegenden Bridges. Die Bridge blockiert den Port, der zu der Bridge mit der numerisch höheren ID führt (eine numerisch höhere ID ist die logisch schlechtere). Haben 2 Bridges die gleiche Priorität, hat die Bridge mit der numerisch größeren MAC-Adresse die numerisch höhere ID; dies ist die logisch schlechtere.
- Wenn von einer Bridge mehrere Pfade mit den gleichen Root-Pfadkosten zu der selben Bridge führen, zieht die von der Root weiter entfernte Bridge als letztes Kriterium die Port-Identifikation der anderen Bridge heran (siehe Abbildung 40). Die Bridge blockiert dabei den Port, der zu dem Port mit der schlechteren ID führt. Haben 2 Ports die gleiche Priorität, hat der Port mit der höheren Port-Nr. die numerisch höhere ID; dies ist die logisch schlechtere.

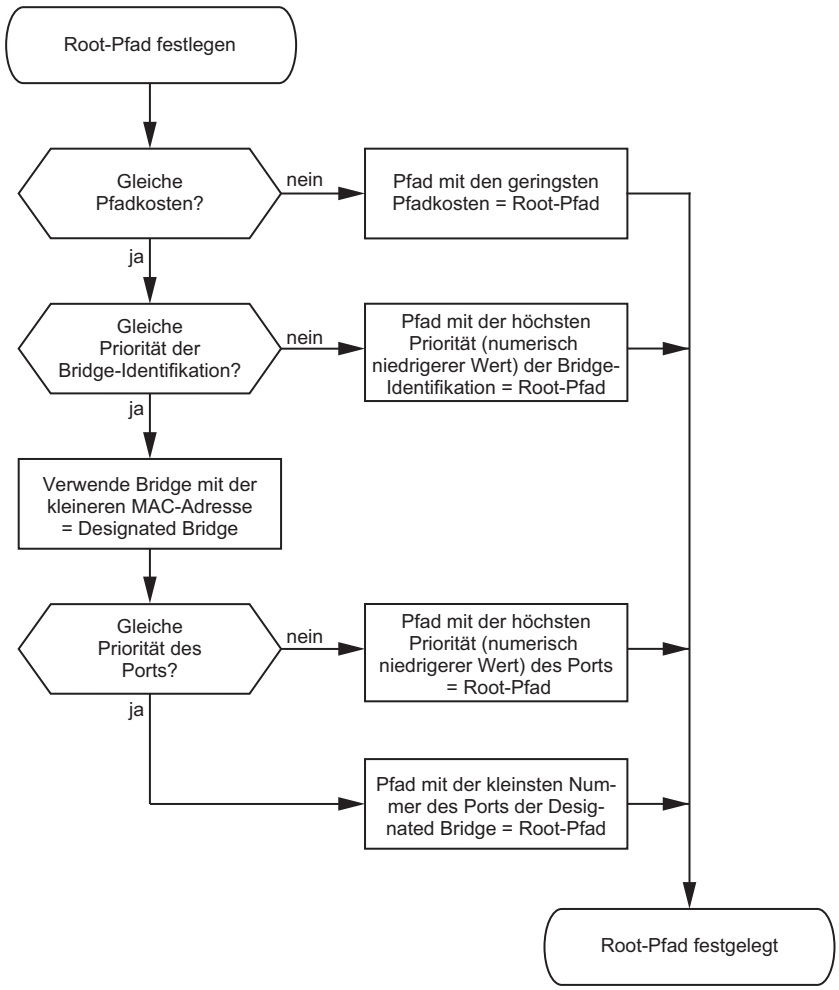


Abb. 43: Flussdiagramm Root-Pfad festlegen

13.4.3 Beispiele

Beispiel für die Bestimmung des Root-Pfads

Anhand des Netzplanes (siehe Abbildung 44) kann man das Flussdiagramm (siehe Abbildung 43) zur Festlegung des Root-Paths nachvollziehen. Der Administrator hat für jede Bridge eine Priorität in der Bridge-Identifikation festgelegt. Die Bridge mit dem kleinsten Zahlenwert für die Bridge-Identifikation übernimmt die Rolle der Root-Bridge, in diesem Fall die Bridge 1. Im Beispiel belastet jeder Teilpfad die gleichen Pfadkosten. Das Protokoll blockiert den Pfad zwischen Bridge 2 und Bridge 3, da eine Verbindung von Bridge 3 über Bridge 2 zur Root-Bridge höhere Pfadkosten verursachen würde.

Interessant ist der Pfad von der Bridge 6 zur Root-Bridge:

- Der Pfad über Bridge 5 und Bridge 3 verursacht die gleichen Root-Pfadkosten wie der Pfad über Bridge 4 und Bridge 2.
- STP wählt den Pfad über die Bridge, die in der Bridge-Identifikation die niedrigere MAC-Adresse hat (im Bild dargestellt Bridge 4).
- Zwischen Bridge 6 und Bridge 4 gibt es ebenfalls 2 Pfade.
  Hier entscheidet die Portidentifikation (Port 1 < Port 3).

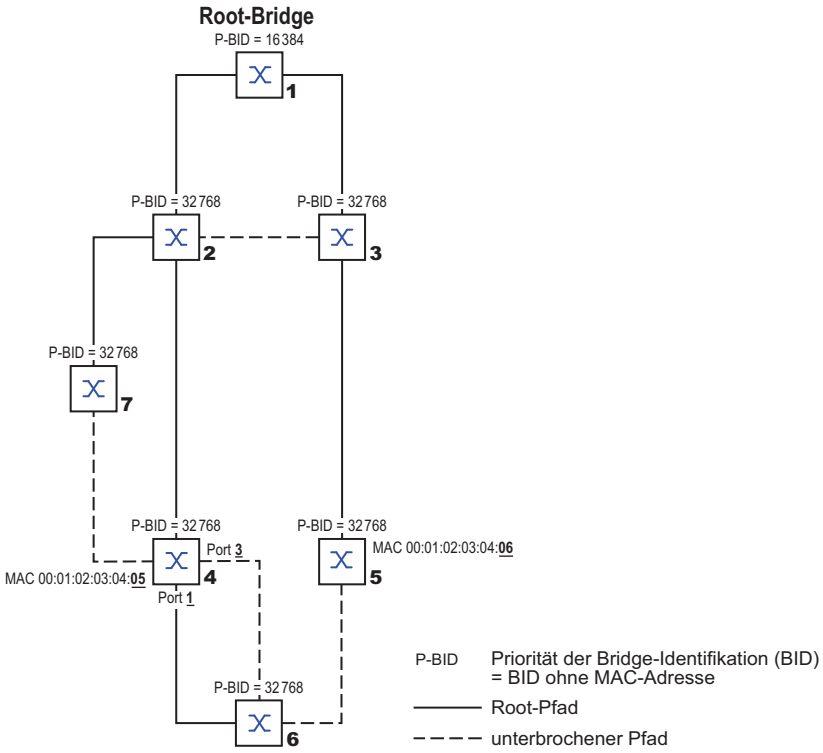


Abb. 44: Beispiel für die Bestimmung des Root-Pfads

Anmerkung: Indem der Administrator für jede Bridge außer der Root-Bridge den im Lieferzustand voreingestellten Wert der Priorität in der Bridge-Identifikation belässt, bestimmt allein die MAC-Adresse in der Bridge-Identifikation, welche Bridge bei Ausfall der momentanen Root-Bridge die Rolle der neuen Root-Bridge übernimmt.

Beispiel für die Manipulation des Root-Pfads

Anhand des Netzplanes (siehe Abbildung 45) kann man das Flussdiagramm (siehe Abbildung 43) zur Festlegung des Root-Paths nachvollziehen. Der Administrator hat folgendes getan:

- Für jede Bridge außer Bridge 1 und Bridge 5 hat er den im Lieferzustand voreingestellten Wert von 32768 (8000H) belassen und
- der Bridge 1 hat er den Wert 16384 (4000H) zugewiesen und damit zur Root-Bridge bestimmt.
- Der Bridge 5 hat er den Wert 28672 (7000H) zugewiesen.

Das Protokoll blockiert den Pfad zwischen Bridge 2 und Bridge 3, da eine Verbindung von Bridge 3 über Bridge 2 zur Root-Bridge höhere Pfadkosten bedeutet.

Interessant ist der Pfad von der Bridge 6 zur Root-Bridge:

▶ Die Bridges wählen den Pfad über Bridge 5, da der Zahlenwert 28672 für ihre Priorität in der Bridge-Identifikation kleiner ist als der Zahlenwert 32768.

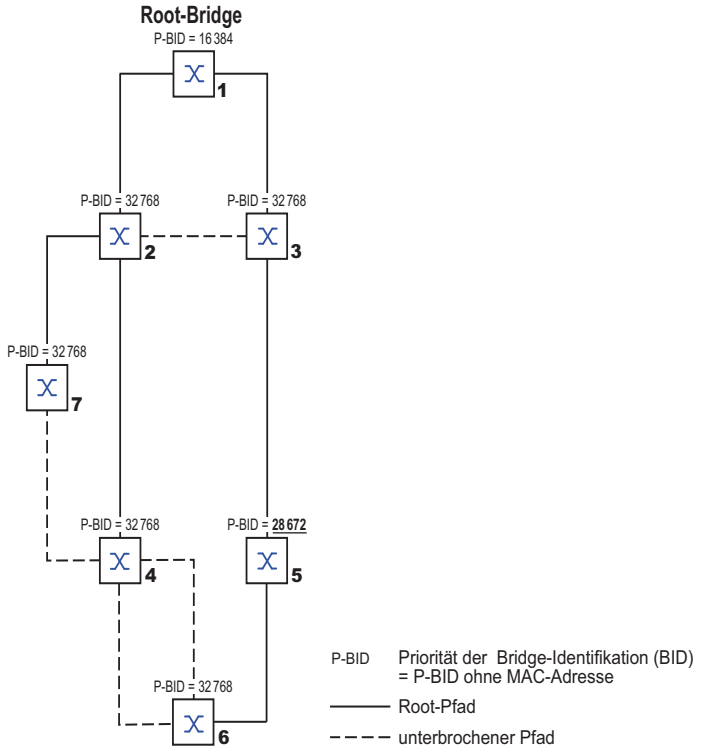


Abb. 45: Beispiel für die Manipulation des Root-Pfads

Beispiel für die Manipulation der Baumstruktur

Der Management-Administrator des Netzes stellt bald fest, dass diese Konfiguration mit Bridge 1 als Root-Bridge ungünstig ist. Auf den Pfaden zwischen Bridge 1 zu Bridge 2 und Bridge 1 zu Bridge 3 summieren sich die Kontrollpakete, die die Root-Bridge zu jeder anderen Bridge sendet.

Konfiguriert der Management-Administrator die Bridge 2 als Root-Bridge, dann verteilt sich die Belastung der Teilnetze durch Kontrollpakete wesentlich besser. Hieraus entsteht die dargestellte Konfiguration (siehe Abbildung 46). Die Pfadkosten der meisten Bridges zur Root-Bridge sind kleiner geworden.

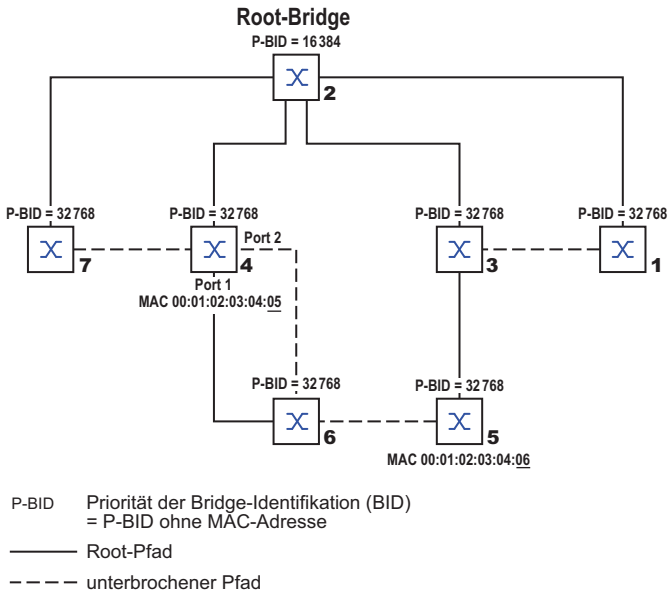


Abb. 46: Beispiel für die Manipulation der Baumstruktur

13.5 Das Rapid Spanning Tree Protokoll

Das RSTP behält die Berechnung der Baumstruktur vom STP unverändert bei. Wenn eine Verbindung oder eine Bridge ausfällt, ändert RSTP lediglich Parameter und fügt neue Parameter und Mechanismen hinzu, die die Rekonfiguration beschleunigen.

Eine zentrale Bedeutung erfahren in diesem Zusammenhang die Ports.

13.5.1 Port-Rollen

RSTP weist jedem Bridge-Port eine der folgenden Rollen zu (siehe Abbildung 47):

- 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 43).
  Die Root-Bridge selbst besitzt keinen Root-Port.
- Designierter Port (Designated-Port):
  Die Bridge in einem Netzsegment, die die niedrigsten Root-Pfadkosten hat, ist die designierte Bridge (Designated Bridge).
  Haben mehrere Bridges die gleichen Root-Pfadkosten, übernimmt die Bridge mit der zahlenmäßig kleinsten Bridge-Identifikation die Rolle der designierten Bridge. Der designierte Port an dieser Bridge ist der Port, der ein von der Root-Bridge wegführendes Netzsegment verbindet.
  Ist eine Bridge mit mehr als einem Port mit einem Netzsegment verbunden (zum Beispiel über einen Hub), gibt sie dem Port mit der besseren Port-Identifikation die Rolle des Designated Ports.
- Edge-Port
  Ein Edge-Port ist ein Endgeräte-Port am „Rand“ (engl. „Edge“) eines geswitchten Netzes. Jedes Netzsegment, in dem sich keine weitere RSTP-Bridge befindet, ist mit genau einem designierten Port verbunden. Dieser designierte Port ist dann gleichzeitig ein Edge-Port, wenn er keine BPDUs (Spanning Tree Bridge Protocol Data Units) empfangen hat.
- Alternate-Port
  Beim Ausfall der Verbindung zur Root-Bridge übernimmt dieser blockierte Port die Aufgabe des Root-Ports. Der Alternate-Port dient als Reserve für die Verbindung zur Root Bridge.

- Backup-Port
  Dies ist ein blockierter Port, der als Ersatz zur Verfügung steht, falls die Verbindung zum designierten Port dieses Netzsegmentes (ohne RSTP-Bridges, zum Beispiel ein Hub) ausfällt.
- Disabled-Port
  Dies ist ein Port, der innerhalb des Spanning-Tree-Protokolls keine Rolle spielt, also abgeschaltet ist oder keine Verbindung hat.

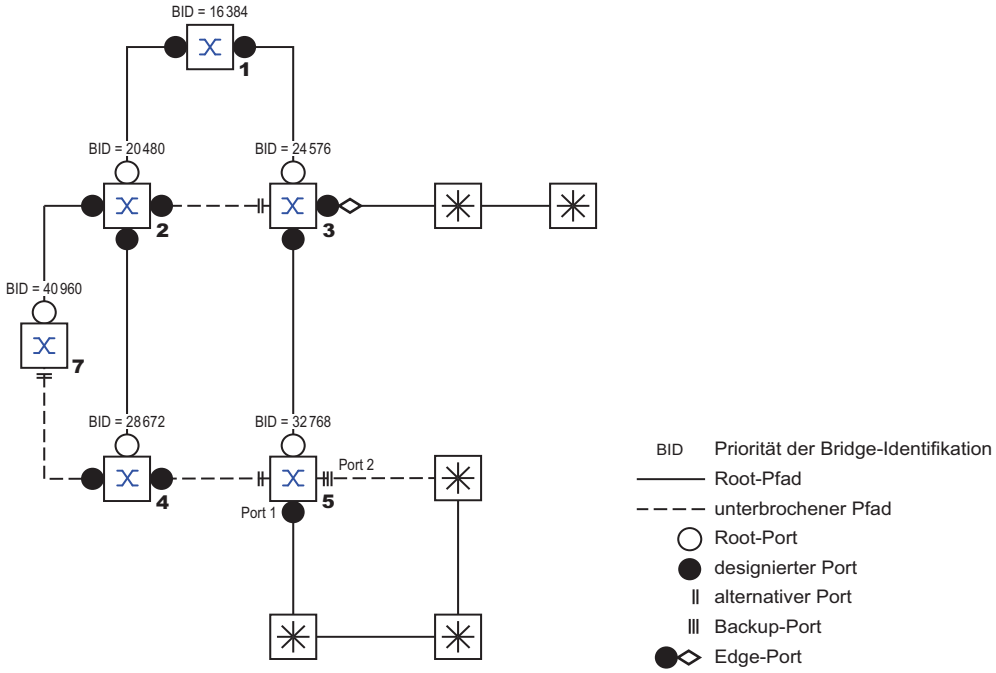


Abb. 47: Port-Rollen-Zuweisung

13.5.2 Port-Stati

In Abhängigkeit von der Baumstruktur und dem Status der ausgewählten Verbindungswege weist RSTP den Ports ihren Status zu.

Tab. 36: Beziehung zwischen Port-Status-Werten bei STP und RSTP

STP Port Status	Administrative Bridge Port-Status	MAC Operational	RSTP Port-Status	Aktive Topology (Port Rolle)
DISABLED	Ausgeschaltet	FALSE	Discarding[1]	Excluded (Disabled)
DISABLED	Enabled	FALSE	Discarding[a]	Excluded (Disabled)
BLOCKING	Enabled	TRUE	Discarding[2]	Excluded (Alternate, Backup)
LISTENING	Enabled	TRUE	Discarding[b]	Included (Root, Designated)
LEARNING	Enabled	TRUE	Learning	Included (Root, Designated)
FORWARDING	Enabled	TRUE	Forwarding	Included (Root, Designated)

1. Die dot1d-MIB zeigt „Disabled“.
2. Die dot1d-MIB zeigt „Blocked“.

Bedeutung der RSTP-Port-Stati:
- Disabled: Port gehört nicht zur aktiven Topologie
- Discarding: Kein Addess Learning in FDB, kein Datenverkehr außer STP-BPDUs

- Learning: Address Learning aktiv (FDB), kein Datenverkehr außer STPBPDUs
- Forwarding: Address Learning aktiv (FDB), Senden und Empfangen jedes Paket-Typs (nicht ausschließlich STP-BPDUs)

13.5.3 Spanning Tree Priority Vector

Um den Ports Rollen zuzuteilen, tauschen die RSTP-Bridges Konfigurationsinformationen untereinander aus. Diese Informationen heißen "Spanning Tree Priority Vector". Sie sind Teil der RST BPDUs und enthalten folgende Informationen:

- Bridge-Identifikation der Root-Bridge
- Root-Pfadkosten der sendenden Bridge
- Bridge-Identifikation der sendenden Bridge
- Portidentifikation des Ports, durch den die Nachricht gesendet wurde
- Portidentifikation des Ports, durch den die Nachricht empfangen wurde

Auf Basis dieser Informationen sind die an RSTP beteiligten Bridges in der Lage, selbstständig Port-Rollen zu bestimmen und den Port-Status ihrer lokalen Ports zu definieren.

13.5.4 Schnelle Rekonfiguration

Warum kann RSTP schneller als STP auf eine Unterbrechung des Root-Pfades reagieren?

- Einführung von Edge-Ports:
  Bei einer Rekonfiguration setzt RSTP einen Edge-Port nach Ablauf von 3 Sekunden (Voreinstellung) in den Vermittlungsmodus. Um sich zu vergewissern, dass keine BPDU-sendende Bridge angeschlossen ist, wartet RSTP "Hello Time" ab.
  Wenn Sie sich vergewissern, dass an diesem Port ein Endgerät angeschlossen ist und bleibt, entstehen im Rekonfigurationsfall an diesem Port keine Wartezeiten.
- Einführung von alternativen Ports:
  Da schon im regulären Betrieb die Portrollen verteilt sind, kann eine Bridge sofort nach dem Verlust der Verbindung zur Root-Bridge vom Root-Port zu einem alternativen Port umschalten.
- Kommunikation mit Nachbar-Bridges (Punkt-zu-Punkt-Verbindungen):
  Die dezentrale, direkte Kommunikation zwischen benachbarten Bridges erlaubt ohne Wartezeiten eine Reaktion auf Zustandsänderungen der Spanning-Tree-Topologie.
- Adresstabelle:
  Beim STP bestimmt das Alter der Einträge in der FDB über die Aktualisierung der Kommunikation. Das RSTP löscht sofort und gezielt die Einträge der Ports, die von einer Umkonfiguration betroffen sind.
- Reaktion auf Ereignisse:
  Ohne Zeitvorgaben einhalten zu müssen, reagiert RSTP sofort auf Ereignisse wie Verbindungsunterbrechung, Verbindung vorhanden, u.a.

Anmerkung: Datenpakete können während der Rekonfigurationsphase der RSTP-Topologie dupliziert werden und/oder mit vertauschter Reihenfolge beim Empfänger ankommen. Sie können auch das Spanning Tree Protocol verwenden oder Sie wählen eines der anderen in diesem Handbuch beschriebenen Redundanzverfahren.

13.5.5 Gerät konfigurieren

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Spanning Tree*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der *Spanning Tree*-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

RSTP konfiguriert die Netztopologie komplett selbstständig. Das Gerät mit der niedrigsten Bridge-Priorität wird dabei automatisch Root-Bridge. Um dennoch eine bestimmte Netzstruktur vorzugeben, legen Sie ein Gerät als Root-Bridge fest. Im Regelfall übernimmt diese Rolle ein Gerät im Backbone.

Führen Sie die folgenden Schritte aus:
- ☐ Bauen Sie das Netz nach Ihren Erfordernissen auf, zunächst ohne redundante Strecken.
- ☐ Deaktivieren Sie die Flusskontrolle auf den beteiligten Ports.
  Wenn die Flusskontrolle und die Redundanzfunktion gleichzeitig aktiv sind, arbeitet die Redundanzfunktion möglicherweise anders als beabsichtigt. (Lieferzustand: Flusskontrolle global ausgeschaltet und auf jedem Port eingeschaltet.)
- ☐ Schalten Sie MRP auf jedem Gerät aus.
- ☐ Schalten Sie Spanning Tree auf jedem Gerät im Netz ein.
  Im Lieferzustand ist Spanning Tree auf dem Gerät eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Einschalten der Funktion.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`spanning-tree operation`	Schaltet Spanning Tree ein.
`show spanning-tree global`	Zeigt zur Kontrolle die Parameter.

Schließen Sie nun die redundanten Strecken an.

Legen Sie die Einstellungen für das Gerät fest, das die Rolle der Root-Bridge übernimmt.

Führen Sie die folgenden Schritte aus:

- ☐ Legen Sie im Feld *Priorität* einen nummerisch kleineren Wert fest.
  Die Bridge mit der nummerisch niedrigsten Bridge-ID hat die höchste Priorität und wird zur Root-Bridge des Netzes.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`spanning-tree mst priority 0 <0..61440>` Legt die Bridge-Priorität des Geräts fest.

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` Zeigt zur Kontrolle die Parameter.

- ☐ Ändern Sie gegebenenfalls die Werte in den Feldern *Forward-Verzögerung [s]* und *Max age*.
  - Die Root-Bridge übermittelt die geänderten Werte an die anderen Geräte.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`spanning-tree forward-time <4..30>` Legt die Verzögerungszeit für Zustandswechsel in Sekunden fest.

`spanning-tree max-age <6..40>` Legt die maximal zulässige Astlänge fest, d. h. die Anzahl der Geräte bis zur Root-Bridge.

`show spanning-tree global` Zeigt zur Kontrolle die Parameter.

Anmerkung: Die Parameter *Forward-Verzögerung [s]* und *Max age* stehen in folgender Beziehung zueinander:

Forward-Verzögerung [s] ≥ (*Max age*/2) + 1

Wenn Sie in die Felder einen Wert einfügen, der dieser Beziehung widerspricht, dann ersetzt das Gerät diese Werte mit den zuletzt gültigen Werten oder mit der Voreinstellung.

Anmerkung: Lassen Sie den Wert im Feld „Hello Time“ möglichst unverändert.

Prüfen Sie in den anderen Geräten die folgende Werte:
- Bridge-ID (Bridge-Priorität und MAC-Adresse) des jeweiligen Geräts sowie der Root-Bridge.
- Nummer des Geräte-Ports, der zur Root-Bridge führt.
- Pfadkosten vom Root-Port des Geräts bis zur Root-Bridge.

Führen Sie die folgenden Schritte aus:

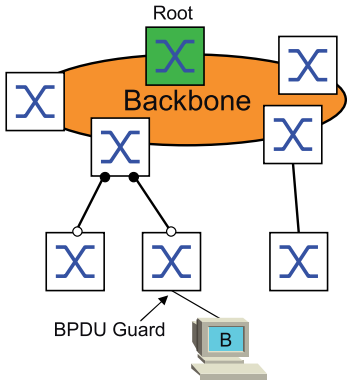
`show spanning-tree global` Zeigt zur Kontrolle die Parameter.

13.5.6 Guards

Das Gerät ermöglicht Ihnen, an den Geräte-Ports verschiedene Schutzfunktionen (Guards) zu aktivieren.

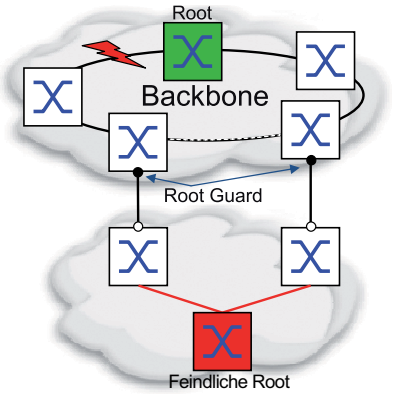
Folgende Schutzfunktionen helfen, Ihr Netz vor Fehlkonfigurationen, Loops und Angriffen mit STP-BPDUs zu schützen:

- BPDU Guard – für manuell festgelegte Edge-Ports (Endgeräte-Ports)
  Diese Schutzfunktion aktivieren Sie global im Gerät.



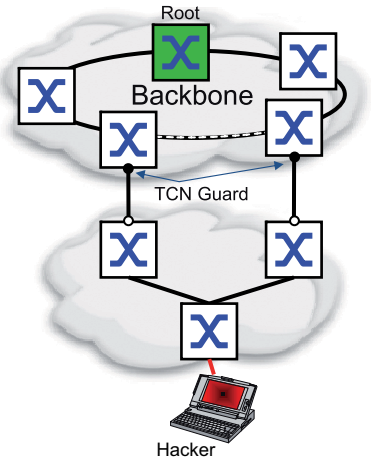
Endgeräte-Ports empfangen im Normalfall keine STP-BPDUs. Versucht ein Angreifer, auf diesem Port trotzdem STP-BPDUs einzuspeisen, deaktiviert das Gerät den Geräte-Port.

- Root Guard – für Designated-Ports
  Diese Schutzfunktion aktivieren Sie für jeden Geräte-Port separat.

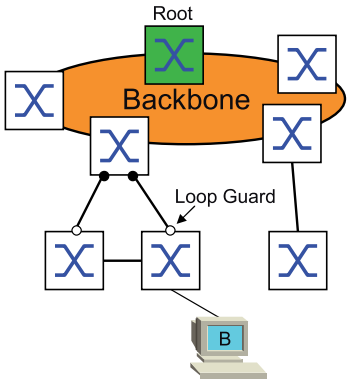


Empfängt ein Designated-Port eine STP-BPDU mit besserer Pfadinformation zur Root-Bridge, verwirft das Gerät die STP-BPDU und setzt den Vermittlungsstatus des Ports auf `discarding` anstatt auf `root`.
Bleiben die STP-BPDUs mit besserer Pfadinformation zur Root-Bridge aus, setzt das Gerät den Status des Ports nach 2 × *Hello-Time [s]* wieder auf einen Wert gemäß Port-Rolle.

- TCN Guard – für Ports, die STP-BPDUs mit Topology-Change-Flag empfangen
  Diese Schutzfunktion aktivieren Sie für jeden Geräte-Port separat.



  Bei eingeschalteter Schutzfunktion ignoriert das Gerät Topology-Change-Flags in empfangenen STP-BPDUs. Der Inhalt der Adresstabelle (FDB) des Geräte-Ports bleibt dadurch unverändert. Weitere Informationen in der BPDU, die eine Topologie-Änderung bewirken, verarbeitet das Gerät jedoch.
- Loop Guard – für Root-, Alternate- und Backup-Ports
  Diese Schutzfunktion aktivieren Sie für jeden Geräte-Port separat.



  Wenn der Port keine STP-BPDUs mehr empfängt, hilft diese Schutzfunktion, den irrtümlichen Wechsel des Vermittlungsstatus eines Ports auf `forwarding` zu vermeiden. Tritt dieser Fall ein, kennzeichnet das Gerät den Loop-Status des Ports als inkonsistent, leitet aber keine Datenpakete weiter.

BPDU Guard einschalten

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Markieren Sie das Kontrollkästchen *BPDU-Guard*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.

`configure`	Wechsel in den Konfigurationsmodus.
`spanning-tree bpdu-guard`	Schaltet den BPDU Guard ein.
`show spanning-tree global`	Zeigt zur Kontrolle die Parameter.

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Wechseln Sie in die Registerkarte *CIST*.
- ☐ Markieren Sie für Endgeräte-Ports das Kontrollkästchen in der Spalte *Admin-Edge-Port*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`interface <x/y>`	Wechsel in den Interface-Konfigurationsmodus von Interface `<x/y>`.
`spanning-tree edge-port`	Kennzeichnet den Port als Endgeräte-Port (Edge Port).
`show spanning-tree port x/y`	Zeigt zur Kontrolle die Parameter.
`exit`	Verlässt den Interface-Modus.

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 der 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 der Spalte *BPDU guard effect* `markiert`.

`show spanning-tree port x/y`	Zeigt zur Kontrolle die Parameter des Ports. Der Wert des Parameters *BPDU guard effect* ist `enabled`.

Setzen Sie den Zustand des Geräteports auf den Wert `forwarding` zurück. Führen Sie dazu die folgenden Schritte aus:
- ☐ Wenn der Port weiterhin BPDUs empfängt:
  - – Heben Sie die manuelle Festlegung als Edge-Port (Endgeräte-Port) auf.
    oder
  - – Deaktivieren Sie den BPDU Guard.
- ☐ Schalten Sie den Geräte-Port wieder ein.

Root Guard / TCN Guard / Loop Guard einschalten

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Wechseln Sie in die Registerkarte *Guards*.
- ☐ Für Designated-Ports markieren Sie das Kontrollkästchen in der Spalte *Root-Guard*.
- ☐ Für Ports, die STP-BPDUs mit Topology-Change-Flag empfangen, markieren Sie das Kontrollkästchen in der Spalte *TCN-Guard*.
- ☐ Für Root-, Alternate- oder Backup-Ports markieren Sie das Kontrollkästchen in der Spalte *Loop-Guard*.

Anmerkung: Die Funktionen *Root-Guard* und *Loop-Guard* schließen sich gegenseitig aus. Wenn Sie versuchen, die Funktion *Root-Guard* zu aktivieren, während die Funktion *Loop-Guard* aktiv ist, deaktiviert das Gerät die Funktion *Loop-Guard*.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface <x/y>`	Wechsel in den Interface-Konfigurationsmodus von Interface `<x/y>`.
`spanning-tree guard-root`	Schaltet den Root Guard auf dem Designated-Port ein.
`spanning-tree guard-tcn`	Schaltet den TCN Guard auf dem Port ein, der STP-BPDUs mit Topology-Change-Flag empfängt.
`spanning-tree guard-loop`	Schaltet den Loop Guard auf einem Root-, Alternate- oder Backup-Port ein.
`exit`	Verlässt den Interface-Modus.
`show spanning-tree port x/y`	Zeigt zur Kontrolle die Parameter des Ports.

13.6 Dual RSTP (MCSESM-E)

Industrielle Anwendungen fordern von ihren Netzen eine hohe Verfügbarkeit. Dies beinhaltet auch die Aufrechterhaltung deterministischer, kurzer Unterbrechungszeiten für die Kommunikation beim Ausfall eines der Geräte im Netz.

Eine Ringtopologie bietet kurze Unterbrechungszeiten bei minimalem Ressourceneinsatz. Die Unterbrechungszeit ist bei Verwendung des Protokolls *Spanning Tree* abhängig von der Größe des Netzes. Um die Unterbrechungszeit zu optimieren, können Sie große *Spanning Tree*-Netze in kleinere Ringsegmente aufteilen.

Die Funktion *Dual RSTP* wird zusammen mit der Funktion *RCP* verwendet. Mit der Funktion *RCP* haben Sie die Möglichkeit, einen oder mehrere RSTP-Ringe mit der RSTP-Instanz an einen Primär-Ring zu koppeln. Bei der Kopplung zweier *Spanning Tree*-Segmente repräsentiert der Sekundär-Ring eine separate RSTP-Instanz, für welche die Einstellungen der Funktion *Dual RSTP* gelten. Diese *Dual RSTP*-Instanz arbeitet unabhängig von der RSTP-Instanz des Primär-Rings und der anderen Sekundär-Ringe. Ist RSTP in ausschließlich einem der zu koppelnden Ringe das verwendete Protokoll, benötigen Sie die Funktion *Dual RSTP* nicht.

13.7 Link-Aggregation

Die Funktion *Link-Aggregation* mit dem Single-Switch-Verfahren hilft Ihnen, 2 Einschränkungen bei Ethernet-Links zu überwinden, und zwar Bandbreite und Redundanz.

Die Funktion *Link-Aggregation* unterstützt Sie dabei, die Bandbreitenbegrenzung für einzelne Ports aufzuheben. Die Funktion *Link-Aggregation* ermöglicht Ihnen, 2 oder mehr Verbindungen zu 1 logischen Verbindung zwischen 2 Geräten zusammenzufassen. Die parallelen Links erhöhen die Übertragungsbandbreite zwischen den 2 Geräten.

Sie verwenden die Funktion *Link-Aggregation* üblicherweise im Backbone-Netz. Die Funktion bietet Ihnen die Möglichkeit, die Bandbreite schrittweise, kostengünstig zu erhöhen.

Die Funktion *Link-Aggregation* bietet des Weiteren Redundanz mit einer unterbrechungsfreien Umschaltung. Wenn bei 2 oder mehr parallel konfigurierten Links ein Link ausfällt, leiten die anderen Links in der Gruppe den Datenverkehr weiter.

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`.

13.7.1 Funktionsweise

Das Gerät arbeitet mit dem Single-Switch-Verfahren. Das Single-Switch-Verfahren bietet Ihnen eine kostengünstige Möglichkeit, Ihr Netz zu erweitern. Das Single-Switch-Verfahren legt fest, dass Sie ein Gerät auf jeder Seite des Links benötigen, um die physischen Ports zur Verfügung zu stellen. Das Gerät verteilt die Netzlast auf die Ports der Gruppenmitglieder.

Das Gerät wendet auch das Same-Link-Speed-Verfahren an, bei dem die Ports der Gruppenmitglieder voll-duplex sind und Punkt-zu-Punkt-Links dieselbe Übertragungsrate haben. Der erste Port, den Sie zur Gruppe hinzufügen, ist der Master-Port und bestimmt die Bandbreite für die weiteren Mitglieder der Link-Aggregation-Group.

Das Gerät ermöglicht Ihnen, bis zu 2 Link-Aggregation-Gruppen einzurichten. Die Anzahl der verwendbaren Ports je Link-Aggregation-Gruppe ist geräteabhängig.

13.7.2 Link-Aggregation Beispiel

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Link-Aggregation*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der *Link-Aggregation*-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

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.

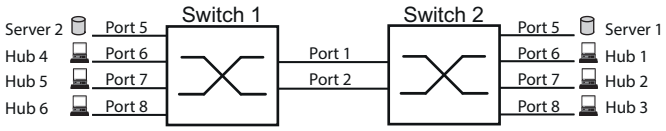


Abb. 48: Link Aggregation Switch-zu-Switch-Netz

Konfigurieren Sie Switch 1 and 2 über die grafische Benutzeroberfläche. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Link-Aggregation*.
- ☐ Klicken Sie die Schaltfläche .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Wählen Sie in der Dropdown-Liste *Trunk-Port* die Instanz-Nummer der Link-Aggregation-Gruppe.
- ☐ Wählen Sie in der Dropdown-Liste *Port* den Port *1/1*.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Wiederholen Sie die vorherigen Schritte und wählen Sie den Port *1/2*.
- ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`link-aggregation add lag/1`	Erzeugt eine Link-Aggregation-Gruppe `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Port *1/1* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 addport 1/2`	Port *1/2* zur Link-Aggregation-Gruppe hinzufügen.

13.8 Link-Backup

Link-Backup bietet einen redundanten Link für Datenverkehr auf Schicht-2-Geräten. Wenn das Gerät einen Fehler auf dem primären Link erkannt hat, leitet das Gerät den Datenverkehr zum Backup-Link um. Sie verwenden Link-Backup üblicherweise in Netzen von Dienstanbietern oder Unternehmen.

Sie richten die Backup-Links paarweise ein, einen als primären Link und einen als Backup-Link. Wenn Sie beispielsweise Redundanz für Unternehmensnetze zur Verfügung stellen, ermöglicht Ihnen das Gerät, mehr als ein Paar einzurichten. Die maximal Anzahl von Link-Backup-Paaren ist die Gesamtanzahl der physischen Ports / 2. Außerdem sendet das Gerät eine SNMP-Nachricht, wenn der Zustand eines Ports eines Link-Backup-Paares seinen Zustand ändert.

Wenn Sie Link-Backup-Paare einrichten, beachten Sie die folgenden Regeln:
- Ein Link-Paar besteht aus einer beliebigen Kombination von physischen Ports. Wenn beispielsweise ein Port ein 100-Mbit-Port und der andere ein 1000-Mbit/s-SFP-Port ist.
- Ein bestimmter Port ist Teil eines Link-Backup-Paares zu einem beliebigen Zeitpunkt.
- Vergewissern Sie sich, dass die Ports eines Link-Backup-Paares Mitglieder desselben VLANs mit derselben VLAN-ID sind. Wenn der primäre Port oder der Backup-Port Mitglied eines VLANs ist, weisen Sie dem zweiten Port des Paares dasselbe VLAN zu.

Die Voreinstellung für diese Funktion ist „deaktiviert“ ohne Link-Backup-Paare.

Anmerkung: Vergewissern Sie sich, dass das Spanning-Tree-Protokoll auf den Link-Backup-Ports ausgeschaltet ist.

13.8.1 Beschreibung Fail-Back

Link-Backup ermöglicht Ihnen, eine Fail-Back-Option einzurichten. Wenn Sie die Fail-Back-Funktion aktivieren und der primäre Link zum normalen Betrieb zurückkehrt, blockiert das Gerät zuerst den Datenverkehr auf dem Backup-Port und überträgt dann den Datenverkehr auf dem primären Port. Dieser Prozess hilft zu vermeiden, dass das Gerät Loops im Netzwerk verursacht.

Wenn der primäre Port zum Link-Up- und aktiven Zustand zurückkehrt, unterstützt das Gerät 2 Betriebsarten:
- Wenn Sie *Fail back* deaktivieren, bleibt der primäre Port im Blocking-Zustand bis der Backup-Link ausfällt.
- Wenn Sie *Fail back* aktivieren, und nachdem der *Fail-Back-Verzögerung [s]* Timer abläuft, kehrt der primäre Port in den Forwarding-Zustand zurück und der Backup-Port nimmt den Zustand „Down” an.

In den oben angeführten Fällen sendet der Port, der seinen Link dazu zwingt, Datenverkehr weiterzuleiten, zuerst ein „Flush-FDB"-Paket zum entfernten Gerät. Das Flush-Paket hilft dem entfernten Gerät dabei, die MAC-Adressen schnell wieder zu lernen.

13.8.2 Beispiel-Konfiguration

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Link-Backup*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der *Link-Backup*-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Im Beispiel-Netzwerk unten verbinden Sie die Ports *2/3* und *2/4* auf Switch A mit dem Uplink der Switches B und C. Wenn Sie die Ports als Link-Backup-Paar einrichten, leitet ein Port Datenverkehr weiter, der andere ist im Blocking-Zustand.

Der primäre Port *2/3* auf Switch A ist der aktive Port und leitet Datenverkehr zu Port 1 auf Switch B weiter. Port *2/4* auf Switch A ist der Backup-Port und blockiert den Datenverkehr.

Wenn Switch A Port *2/3* aufgrund eines erkannten Fehlers deaktiviert, beginnt Port *2/4* auf Switch A damit, Datenverkehr zu Port 2 auf Switch C weiterzuleiten.

Wenn Port *2/3* in den aktiven Zustand „no shutdown“ zurückkehrt mit *Fail back* aktiviert und *Fail-Back-Verzögerung [s]* festgelegt auf 30 s. Nachdem der Timer abgelaufen ist, blockiert zuerst Port *2/4* den Datenverkehr, dann fängt Port *2/3* an, den Datenverkehr weiterzuleiten.

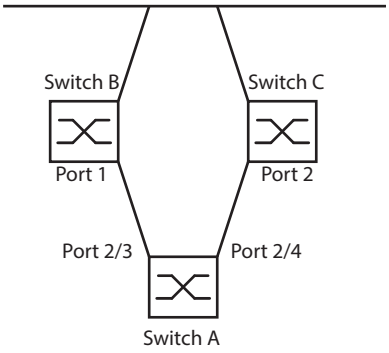


Abb. 49: Link-Backup Beispiel-Netzwerk

Die folgenden Tabellen enthalten Beispiele für Parameter, um Switch A zu konfigurieren.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Link-Backup*.
- ☐ Fügen Sie ein neues Link-Backup-Paar in die Tabelle ein:
  - ☐ Klicken Sie die Schaltfläche .
    Der Dialog zeigt das Fenster *Erzeugen*.
  - ☐ Wählen Sie in der Dropdown-Liste *Primärer Port* den Port *2/3*.
    Wählen Sie in der Dropdown-Liste *Backup-Port* den Port *2/4*.
  - ☐ Klicken Sie die Schaltfläche *Ok*.
- ☐ Geben Sie im Textfeld *Beschreibung*`Link_Backup_1` als Name für das Backup-Paar ein.

- ☐ Um die Funktion *Fail back* für das Link-Backup-Pair zu aktivieren, markieren Sie das Kontrollkästchen *Fail back*.
- ☐ Legen Sie den Fail-Back-Timer für das Link-Backup-Paar fest, geben Sie `30` s ein in *Fail-Back-Verzögerung [s]*.
- ☐ Um das Link-Backup-Paar zu aktivieren, markieren Sie das Kontrollkästchen *Aktiv*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 2/3`	Wechsel in den Interface-Konfigurationsmodus von Interface *2/3*.
`link-backup add 2/4`	Erzeugt eine Link-Backup-Instanz, bei der Port *2/3* der primäre Port und Port *2/4* der Backup-Port ist.
`link-backup modify 2/4 description Link_Backup_1`	Legt die Zeichenfolge `Link_Backup_1` als Name des Backup-Paares fest.
`link-backup modify 2/4 failback-status enable`	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`	Wechsel in den Konfigurationsmodus.
`link-backup operation`	Die Funktion *Link-Backup* global auf dem Gerät einschalten.

13.9 FuseNet

Die *FuseNet*-Protokolle ermöglichen Ihnen, Ringe zu koppeln, die mit einem der folgenden Redundanzprotokolle arbeiten:

- MRP
- HIPER-Ring
- RSTP

Anmerkung: Voraussetzung für das Koppeln eines Netzes an den Haupt-Ring mittels des Protokolls *Ring-/Netzkopplung* ist, dass das angeschlossene Netz ausschließlich Netzkomponenten enthält, die das Protokoll *Ring-/Netzkopplung* unterstützen.

Verwenden Sie die folgende Tabelle, um das *FuseNet*-Kopplungs-Protokoll auszuwählen, das in Ihrem Netz zum Einsatz kommt:

Haupt-Ring	**Verbundenes Netz**		
	MRP	**HIPER-Ring**	**RSTP**
MRP	*Sub Ring*[1)]	– *Redundant Coupling Protocol* – *Ring-/Netzkopplung*	– *Redundant Coupling Protocol* – *Ring-/Netzkopplung*
HIPER-Ring	*Sub Ring*	*Ring-/Netzkopplung*	– *Redundant Coupling Protocol* – *Ring-/Netzkopplung*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	*Dual RSTP* + *Redundant Coupling Protocol*

– kein geeignetes Kopplungs-Protokoll

1) mit *MRP* eingerichtet an unterschiedlichen VLANs

13.10 Subring

Die Funktion *Sub Ring* ist eine Erweiterung des Media Redundancy Protocol (MRP). Diese Funktion ermöglicht Ihnen, einen Subring an einen Hauptring mit unterschiedlichen Netzstrukturen zu koppeln.

Das Subring-Protokoll ermöglicht, Redundanz für Geräte durch das Koppeln der beiden Enden eines Netzes in Linienstruktur zu einem Hauptring herzustellen.

Die Einrichtung von Subringen bietet folgende Vorteile:
- Mit der Kopplung nehmen Sie das neue Netzsegment in das Redundanz-Konzept auf.
- Subringe ermöglichen das einfache Einbinden neuer Bereiche in ein bestehendes Netz.
- Subringe bieten Ihnen die Möglichkeit, die Organisationsstruktur eines Bereichs in einer Netztopologie abzubilden.
- In einem MRP-Ring liegen die Umschaltzeiten des Subrings im Redundanzfall üblicherweise bei < 100 ms.

13.10.1 Beschreibung für einen Subring

Das Subring-Konzept ermöglicht Ihnen die Kopplung neuer Netzsegmente an geeignete Geräte in einem bestehenden Ring (Hauptring). Die Geräte, die einen Subring an den Hauptring ankoppeln, heißen „Subring-Manager“ (SRM).

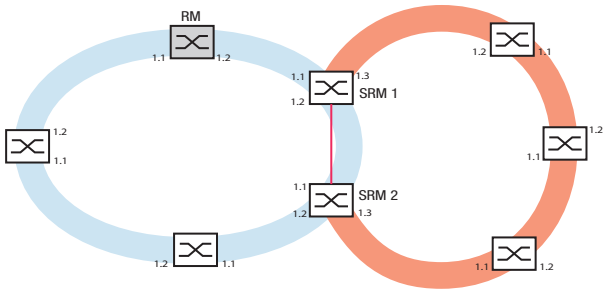


Abb. 50: Beispiel für eine Subring-Struktur
blauer Ring = Hauptring
oranger Ring = Subring
rote Linie = redundante Verbindung des Subrings
SRM = Subring-Manager
RM = Ring-Manager

Die Subring-Manager-fähigen Geräte unterstützen bis zu 8 Instanzen und verwalten daher bis zu 8 Subringe gleichzeitig.

Die Funktion *Sub Ring* ermöglicht Ihnen, MRP-fähige Geräte als Ring-Teilnehmer zu integrieren. Die Geräte, die den Subring an den Hauptring ankoppeln, benötigen die *Sub Ring*-Manager-Funktion.

Jeder Subring kann aus bis zu 200 Teilnehmern bestehen, zuzüglich den Subring-Managern und den Geräten zwischen den Subring-Managern im Hauptring.

Die folgenden Abbildungen zeigen Beispiele möglicher Subring-Topologien:

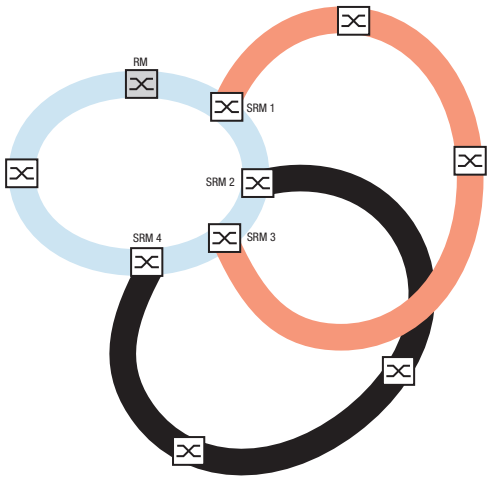


Abb. 51: Beispiel für eine überlappende Subring-Struktur

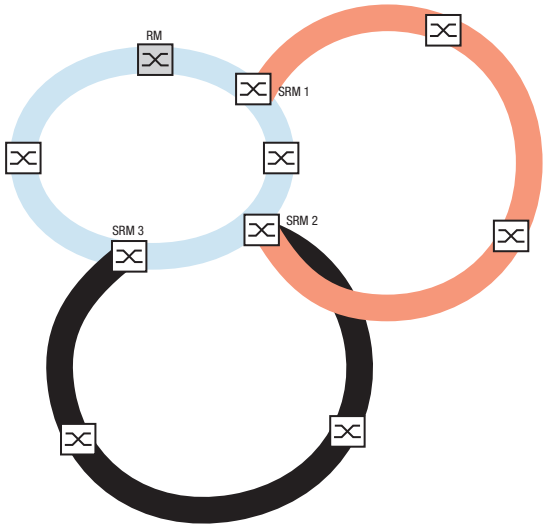


Abb. 52: Sonderfall: Ein Subring-Manager verwaltet 2 Subringe (2 Instanzen). Der Subring-Manager ist in der Lage, bis zu 8 Instanzen zu verwalten.

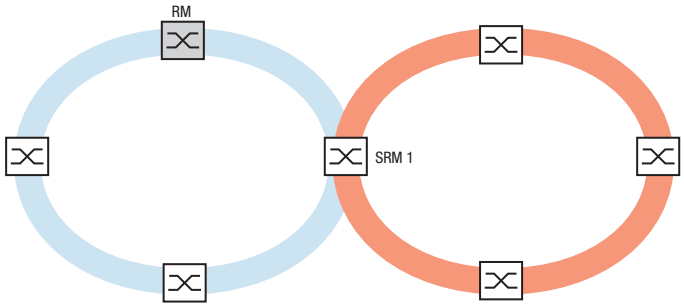


Abb. 53: Sonderfall: Ein Subring-Manager verwaltet beide Enden eines Subrings an unterschiedlichen Ports (Single-Subring-Manager).

Anmerkung: In den vorherigen Beispielen koppeln die Subring-Manager lediglich die Subringe an vorhandene Hauptringe an. Die Funktion *Sub Ring* verbietet kaskadierte Subringe, also das Ankoppeln eines Subrings an einen bereits vorhandenen Subring.

Wenn Sie MRP für den Hauptring und den Subring verwenden, legen Sie die VLAN-Einstellungen wie folgt fest:

- VLAN X für den Hauptring
  - auf den Ring-Ports der Hauptring-Teilnehmer
  - auf den Hauptring-Ports des Subring-Managers
- VLAN Y für den Subring
  - auf den Ring-Ports der Subring-Teilnehmer
  - auf den Subring-Ports des Subring-Managers

  Sie können dasselbe VLAN für verschiedene Subringe nutzen.

13.10.2 Beispiel für einen Subring

Im folgenden Beispiel koppeln Sie ein neues Netzsegment mit 3 Geräten an einen bestehenden Hauptring, der das MRP-Protokoll nutzt. Wenn Sie das Netz anstatt an einem Ende an beiden Enden koppeln, bietet der Subring eine höhere Verfügbarkeit.

Das neue Netzsegment koppeln Sie als Subring an. Den Subring koppeln Sie an vorhandene Geräte im Hauptring, indem Sie folgenden Konfigurationstypen verwenden:

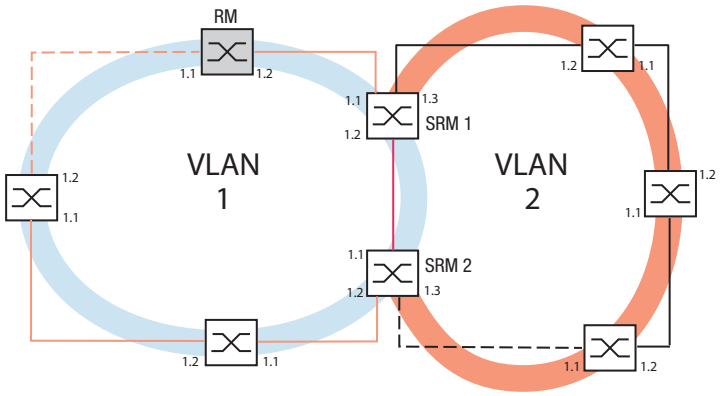


Abb. 54: Beispiel für eine Subring-Struktur
orangefarbene Linie = Mitglieder des Hauptrings in VLAN 1
schwarze Linie = Mitglieder des Subrings in VLAN 2
orange gestrichelte Linie = unterbrochenes Segment im Hauptring
schwarz gestrichelte Linie = unterbrochenes Segment im Subring
rote Linie = redundante Verbindung, Mitglied in VLAN 1
SRM = Subring-Manager
RM = Ring-Manager

Um den Subring zu konfigurieren, führen Sie die folgenden Schritte aus:

- ☐ Konfigurieren Sie die 3 Geräte des neuen Netzsegments als Teilnehmer in einem MRP-Ring:
  - Konfigurieren Sie die Übertragungsrate und den Duplex-Modus für die Ring-Ports gemäß der folgenden Tabelle:

Tab. 37: Port-Einstellungen für Subring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
TX	1 Gbit/s	markiert	markiert	–
Optisch	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
Optisch	1 Gbit/s	markiert	markiert	–
Optisch	2.5 Gbit/s	markiert	–	*2,5 Gbit/s FDX*

Die folgenden Schritte beinhalten zusätzliche Einstellungen für die Konfiguration von Subringen:

- ☐ Um die Möglichkeit von Loops während der Konfiguration zu verringern, deaktivieren Sie die Subring-Manager-Funktion für die Geräte im Hauptring und im Subring. Nachdem Sie jedes im Hauptring und in den Subringen teilnehmende Gerät vollständig konfiguriert haben, aktivieren Sie die globale Funktion *Sub Ring* und die Subring-Manager.
- ☐ Deaktivieren Sie die Funktion RSTP an den im Subring verwendeten MRP-Ring-Ports.
- ☐ Vergewissern Sie sich, dass die Funktion *Link-Aggregation* auf den Ports inaktiv ist, die im Hauptring und in den Subringen teilnehmen.
- ☐ Legen Sie für Hauptring-Ports und Subring-Ports unterschiedliche VLANs fest, wenn der Hauptring das MRP-Protokoll nutzt. Verwenden Sie zum Beispiel VLAN-ID `1` für den Hauptring und die Redundanzverbindung und anschließend VLAN-ID `2` für den Subring.
  - Für im Hauptring teilnehmende Geräte öffnen Sie den Dialog *Switching > VLAN > Konfiguration*. Erzeugen Sie VLAN `1` in der statischen VLAN-Tabelle. Markieren Sie die Hauptring-Ports zur Mitgliedschaft in VLAN `1`, indem Sie in der Dropdown-Liste der betreffenden Port-Spalten den Eintrag `T` auswählen.
  - Für die im Subring teilnehmenden Geräte wenden Sie die oben beschriebenen Schritte an und fügen die Ports in der statischen VLAN-Tabelle zu VLAN `2` hinzu.
- ☐ Aktivieren Sie die Funktion *MRP* für die Geräte im Hauptring und im Subring.
  - Im Dialog *Switching > L2-Redundanz > MRP* konfigurieren Sie die 2 im Hauptring teilnehmenden Ring-Ports an den Geräten des Hauptrings.
  - Für die im Subring teilnehmenden Geräte wenden Sie die oben beschriebenen Schritte an und konfigurieren die im Subring teilnehmenden 2 Ring-Ports an den Geräten des Subrings.
  - Weisen Sie den Geräten im Hauptring und im Subring dieselbe MRP-Domänen-ID zu. Wenn Sie ausschließlich Schneider Electric-Geräte verwenden, dann genügen die voreingestellten Werte für die MRP-Domain-ID.

Anmerkung: Die *MRP-Domäne* ist eine Folge aus 16 Ziffernblöcken im Bereich zwischen `0` und `255`. Voreingestellt ist der Wert `255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255`. Eine ausschließlich aus Nullen bestehende *MRP-Domäne* ist ungültig.

Der *Sub Ring*-Dialog ermöglicht Ihnen, die MRP-Domain-ID bei Bedarf zu ändern. Alternativ benutzen Sie das Command Line Interface. Führen Sie dazu die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mrp domain delete`	Löscht die aktuelle MRP-Domäne.
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111. 222.123.0.0.66.99`	Erzeugt eine neue MRP-Domäne mit der festgelegten MRP-Domänen-ID. Alle folgenden Änderungen der MRP-Domäne gelten für diese Domänen-ID.

13.10.3 Subring-Beispielkonfiguration

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Sub Ring*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Anmerkung: Vermeiden Sie Loops während der Konfiguration. Konfigurieren Sie jedes Gerät des Subrings individuell. Konfigurieren Sie jedes Subring-Gerät vollständig, bevor Sie die Redundanzverbindung aktivieren.

Konfigurieren Sie die 2 Subring-Manager in dem Beispiel. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Sub Ring*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Wählen Sie in Spalte *Port* den Port, der das Gerät an den Subring koppelt.
  Verwenden Sie für dieses Beispiel Port *1/3*.
  Verwenden Sie für die Kopplung einen der verfügbaren Ports, mit Ausnahme der bereits mit dem Hauptring verbundenen Ports.
- ☐ Weisen Sie in Spalte *Name* dem Subring einen Namen zu.
  Geben Sie für dieses Beispiel `Test` ein.
- ☐ Wählen Sie in Spalte *SRM-Modus* den Subring-Manager-Modus.
  So legen Sie fest, welcher Port zur Kopplung des Sub-Rings an den Hauptring Redundanz-Manager wird.
  Die Möglichkeiten der Kopplung sind:
  - `manager`
    Wenn Sie beiden Subring-Managern denselben Wert zuweisen, verwaltet das Gerät mit der höheren MAC-Adresse die Redundanzverbindung.
  - `redundant manager`
    Das Gerät verwaltet die Redundanzverbindung, solange Sie den anderen Subring-Manager als `manager` konfiguriert haben. Andernfalls ist das Gerät mit der höheren MAC-Adresse der Redundanz-Manager.

  Legen Sie entsprechend der Abbildung für dieses Beispiel den Subring-Manager 1 als `manager` fest.
- ☐ Lassen Sie die Werte in Spalte *VLAN* und in Spalte *MRP-Domäne* unverändert.
  Die voreingestellten Werte sind korrekt für die Beispielkonfiguration.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`sub-ring add 1`	Erzeugt einen neuen Subring mit der Subring-ID `1`.
`sub-ring modify 1 port 1/3`	Port *1/3* als Subring-Port festlegen.
`sub-ring modify 1 name Test`	Subring `Test` den Namen `1` zuweisen.

`sub-ring modify 1 mode manager`	Subring `manager` den Modus `1` zuweisen.
`show sub-ring ring`	Status der Subringe auf diesem Gerät anzeigen.
`show sub-ring global`	Globalen Status der Subringe auf diesem Gerät anzeigen.

- ☐ Konfigurieren Sie den 2. Subring-Manager entsprechend.
  Legen Sie entsprechend der Abbildung für dieses Beispiel den Subring-Manager 2 als `redundant manager` fest.

- ☐ Um die Subring-Manager-Funktion zu aktivieren, markieren Sie in den betreffenden Zeilen das Kontrollkästchen *Aktiv*.
- ☐ Nachdem Sie beide Subring-Manager und die im Subring teilnehmenden Geräte konfiguriert haben, schalten Sie die Funktion ein und schließen die Redundanzverbindung.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`sub-ring enable 1`	Subring `1` aktivieren.
`sub-ring enable 2`	Subring `2` aktivieren.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`show sub-ring ring <Domain ID>`	Detaillierte Einstellungen des ausgewählten Subrings anzeigen.
`show sub-ring global`	Globale Subring-Einstellungen anzeigen.
`copy config running-config nvm profile Test`	Speichern der aktuellen Einstellungen im Konfigurationsprofil mit der Bezeichnung `Test` im permanenten Speicher (`nvm`).

13.11 Subring mit LAG

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Sub Ring*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Eine Link-Aggregation-Verbindung („LAG-Verbindung“) liegt vor, wenn zwischen 2 Geräten mindestens 2 parallele redundante Verbindungsleitungen („Trunks“) existieren und diese zu einer logischen Verbindung zusammengefasst werden.

Das Gerät ermöglicht Ihnen, die LAG-Ports als Ring-Ports mit dem *Sub Ring*-Protokoll zu verwenden.

13.11.1 Beispiel

Das folgende Beispiel beinhaltet eine einfache Einrichtung zwischen einem MRP-Ring und einem Subring.

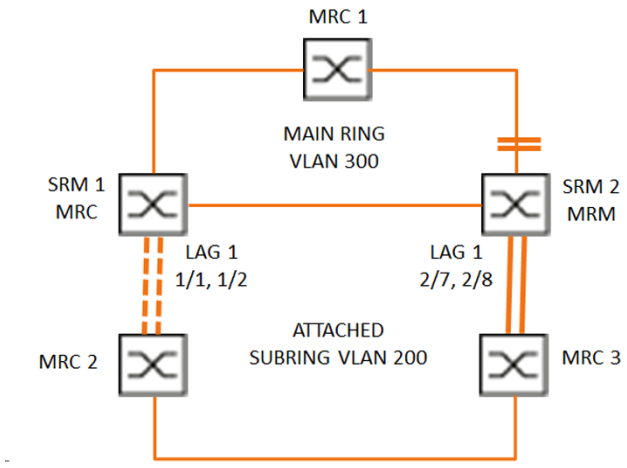


Abb. 55: Subring mit Link-Aggregation

Die folgende Tabelle beschreibt die in der obigen Abbildung dargestellten Geräterollen. Die Tabelle stellt Informationen zur Verwendung der Ring-Ports und Subring-Ports als LAG-Ports bereit.

Tab. 38: Geräte, Ports und Rollen

Gerätename	Ring-Port	Rolle des Haupt-rings	Rolle des Subrings	Subring-Port
MRC1	1/3, 1/4	MRP-Client	-	-
SRM1	1/3, 1/4	MRP-Client	Redundanz-Manager	lag/1
SRM2	2/4, 2/5	MRP-Manager	Manager	lag/1
MRC2	lag/1, 1/3	-	MRP-Client	-
MRC3	lag/1, 1/3	-	MRP-Client	-

MRP-Ring-Konfiguration

Die im Hauptring teilnehmenden Geräte sind Mitglieder von VLAN 300.

Führen Sie die folgenden Schritte aus:

`SRM2`

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mrp domain add default-domain`	Erzeugt eine neue MRP-Domäne mit der ID `default-domain`.
`mrp domain modify port primary 2/4`	Port *2/4* als Ring-Port `1` festlegen.
`mrp domain modify port secondary 2/5`	Port *2/5* als Ring-Port `2` festlegen.
`mrp domain modify mode manager`	Legt fest, dass das Gerät als *Ring-Manager* arbeitet. Schalten Sie die Funktion *Ring-Manager* auf keinem weiteren Gerät ein.
`mrp domain modify operation enable`	Schaltet den MRP-Ring ein.
`mrp domain modify vlan 300`	Für die VLAN-ID `300` festlegen.
`mrp operation`	Einschalten der Funktion *MRP* auf dem Gerät.

`MRC1, SRM1`

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mrp domain add default-domain`	Erzeugt eine neue MRP-Domäne mit der ID `default-domain`.
`mrp domain modify port primary 1/3`	Port *1/3* als Ring-Port `1` festlegen.
`mrp domain modify port secondary 1/4`	Port *1/4* als Ring-Port `2` festlegen.
`mrp domain modify mode client`	Für die Geräterolle Ring-Client festlegen.
`mrp domain modify operation enable`	Schaltet den MRP-Ring ein.
`mrp domain modify vlan 300`	Für die VLAN-ID `300` festlegen.
`mrp operation`	Einschalten der Funktion *MRP* auf dem Gerät.

Subring-Konfiguration

Die im verbundenen Subring teilnehmenden Geräte sind Mitglieder von VLAN 200.

Führen Sie die folgenden Schritte aus:

SRM1

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`link-aggregation add lag/1`	Erzeugt eine Link-Aggregation-Gruppe `lag/1`.
`link-aggregation modify lag/1 addport 1/1`	Port *1/1* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 addport 1/2`	Port *1/2* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 adminmode`	Link-Aggregation-Gruppe aktivieren.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`sub-ring add 1`	Erzeugt einen neuen Subring mit der Subring-ID `1`.
`sub-ring modify 1 name SRM1`	Subring `1` den Namen `SRM1` zuweisen.
`sub-ring modify 1 mode redundant-manager vlan 200 port lag/1`	Dem Gerät die Rolle `Sub-ring redundant manager` in Subring `1` zuweisen. Wenn der Subring geschlossen ist, blockiert das Gerät den Ring-Port. Für die VLAN-ID der Domäne ist VLAN `200` festgelegt. Port `lag/1` ist als Mitglied in VLAN `200` festgelegt.
`sub-ring enable 1`	Subring `1` aktivieren.
`sub-ring operation`	Globale Subring-Manager-Funktion auf diesem Gerät aktivieren.

SRM2

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`link-aggregation add lag/1`	Erzeugt eine Link-Aggregation-Gruppe `lag/1`.
`link-aggregation modify lag/1 addport 2/7`	Port *2/7* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 addport 2/8`	Port *2/8* zur Link-Aggregation-Gruppe hinzufügen.
`link-aggregation modify lag/1 adminmode`	Link-Aggregation-Gruppe aktivieren.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`sub-ring add 1`	Erzeugt einen neuen Subring mit der Subring-ID `1`.
`sub-ring modify 1 mode manager vlan 200 port lag/1`	Dem Gerät die Rolle `Subring manager` in Subring `1` zuweisen. Für die VLAN-ID der Domäne ist VLAN `200` festgelegt. Port `lag/1` ist als Mitglied in VLAN `200` festgelegt.

`sub-ring modify 1 name SRM2`	Subring `SRM2` den Namen `1` zuweisen.
`sub-ring enable 1`	Subring `1` aktivieren.
`sub-ring operation`	Globale Subring-Manager-Funktion auf diesem Gerät aktivieren.

`MRC 2, 3`

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mrp domain add default-domain`	Erzeugt eine neue MRP-Domäne mit der ID `default-domain`.
`mrp domain modify port primary lag/1`	Port `lag/1` als Ring-Port `1` festlegen.
`mrp domain modify port secondary 1/3`	Port *1/3* als Ring-Port `2` festlegen.
`mrp domain modify mode client`	Für die Geräterolle Ring-Client festlegen.
`mrp domain modify operation enable`	Schaltet den MRP-Ring ein.
`mrp domain modify vlan 200`	Für die VLAN-ID `200` festlegen.
`mrp operation`	Einschalten der Funktion *MRP* auf dem Gerät.

STP deaktivieren

Schalten Sie die Funktion *Spanning Tree* auf jedem Port aus, den Sie als MRP- oder Subring-Port festgelegt haben. Das folgende Beispiel verwendet Port *1/3*.

Führen Sie die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/3`	Wechsel in den Interface-Konfigurationsmodus von Interface *1/3*.
`no spanning-tree operation`	Ausschalten der Funktion *Spanning Tree* auf dem Port.

13.12 Ring-/Netzkopplung

Die Funktion *Ring-/Netzkopplung* koppelt Ringe oder Netzsegmente redundant auf Basis eines Rings. *Ring-/Netzkopplung* verbindet 2 Ringe/Netzsegmente über 2 separate Pfade.

Wenn die Geräte im gekoppelten Netz Schneider Electric-Geräte sind, unterstützt die Funktion *Ring-/Netzkopplung* die Kopplung gemäß den folgenden Ring-Protokollen im Primär-Ring und in den Sekundär-Ringen:

- HIPER-Ring
- Fast HIPER-Ring
- MRP

Die Funktion *Ring-/Netzkopplung* bietet auch die Möglichkeit zum Koppeln der Netzsegmente eines Bus und von Mesh-Strukturen.

13.12.1 Methoden der Ring-/Netzkopplung

1-Switch-Kopplung

2 Ports **1** Geräts im 1. Ring/Netz stellen eine Verbindung zu jeweils 1 Port der 2 Geräte im 2. Ring/Netz her (siehe Abbildung 56). Bei der Methode der 1-Switch-Kopplung leitet die Hauptleitung Daten weiter und das Gerät blockiert die redundante Leitung.

Falls die Hauptleitung ausfällt, hebt das Gerät die Blockierung der redundanten Leitung unverzüglich auf. Wenn die Hauptleitung wiederhergestellt ist, blockiert das Gerät die Daten auf der redundanten Leitung. Die Hauptleitung leitet die Daten wieder weiter.

Die Ring-Kopplung erkennt und bearbeitet Fehler innerhalb von 500 ms (in der Regel 150 ms).

2-Switch-Kopplung

Jeweils 1 Port der **2** Geräte im 1. Ring/Netz stellt eine Verbindung zu jeweils 1 Port der 2 Geräte im 2. Ring/Netzsegment her (siehe Abbildung 58).

Um einander über den jeweiligen Betriebszustand zu informieren, verwenden das Gerät in der redundanten Leitung und das Gerät in der Hauptleitung Kontrollpakete (über Ethernet oder eine Steuerleitung).

Falls die Hauptleitung nicht mehr funktioniert, hebt das redundante Gerät (Standby) die Blockierung der redundanten Leitung unverzüglich auf. Sobald die Hauptleitung wiederhergestellt ist, informiert das Gerät der Hauptleitung das redundante Gerät darüber. Das Stand-by-Gerät blockiert die Daten auf der redundanten Leitung. Die Hauptleitung leitet die Daten wieder weiter.

Die Ring-Kopplung erkennt und bearbeitet Fehler innerhalb von 500 ms (in der Regel 150 ms).

Die Art der Kopplungskonfiguration wird primär durch die Netzwerktopologie und den gewünschten Verfügbarkeitsgrad bestimmt (siehe Tabelle 39).

Tab. 39: Auswahlkriterien für die Konfigurationsarten für die redundante Kopplung

	1-Switch-Kopplung	2-Switch-Kopplung	2-Switch-Kopplung mit Steuerleitung
Anwendung	Die 2 Geräte sind topologisch ungünstig verteilt. Ein Link zwischen den Geräten wäre bei einer 2-Switch-Kopplung daher aufwendig.	Die 2 Geräte sind topologisch günstig verteilt. Die Verlegung einer Steuerleitung wäre äußerst aufwendig.	Die 2 Geräte sind topologisch günstig verteilt. Die Verlegung einer Steuerleitung wäre nicht aufwendig.
Nachteil	Bei Ausfall des für die redundante Kopplung konfigurierten Switches ist keine Verbindung zwischen den Netzen mehr vorhanden.	Höherer Aufwand für die Verbindung der 2 Geräte mit dem Netz (im Vergleich zur 1-Switch-Kopplung).	Höherer Aufwand für die Verbindung der 2 Geräte mit dem Netz (im Vergleich zur 1-Switch-Kopplung und 2-Switch-Kopplung).
Vorteil	Weniger Aufwand für die Verbindung der 2 Geräte mit dem Netz (im Vergleich zur 2-Switch-Kopplung).	Falls eines der für die redundante Kopplung konfigurierten Geräte ausfällt, sind die gekoppelten Netze weiterhin verbunden.	Falls eines der für die redundante Kopplung konfigurierten Geräte ausfällt, sind die gekoppelten Netze weiterhin verbunden. Die Partnerermittlung zwischen den koppelnden Geräten erfolgt einfacher und schneller als mit einer Steuerleitung.

13.12.2 Ring-/Netzkopplung vorbereiten

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *Ring-/Netzkopplung*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Um Loops zu vermeiden, verwenden Sie die Funktion *Ring-/Netzkopplung* ausschließlich auf Ports, auf denen das Rapid Spanning Tree Protocol inaktiv ist.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Legen Sie die Rolle der Geräte innerhalb der *Ring-/Netzkopplung* anhand der Abbildungen im Dialog fest.

Die folgenden Screenshots und Diagramme wenden folgende Konventionen an:
- Blaue Felder und Linien bezeichnen Geräte oder Verbindungen im gegenwärtigen Betrachtungsumfang.
- Durchgängige Linien weisen auf eine Hauptverbindung hin.
- Gestrichelte Linien stellen Standby-Verbindungen dar.
- Gepunktete Linien bezeichnen Steuerleitungen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das erforderliche Optionsfeld.
  - *Ein-Switch-Kopplung*
  - *Zwei-Switch-Kopplung, Master*
  - *Zwei-Switch-Kopplung, Slave*
  - *Zwei-Switch-Kopplung mit Steuer-Leitung, Master*
  - *Zwei-Switch-Kopplung mit Steuer-Leitung, Slave*

1-Switch-Kopplung

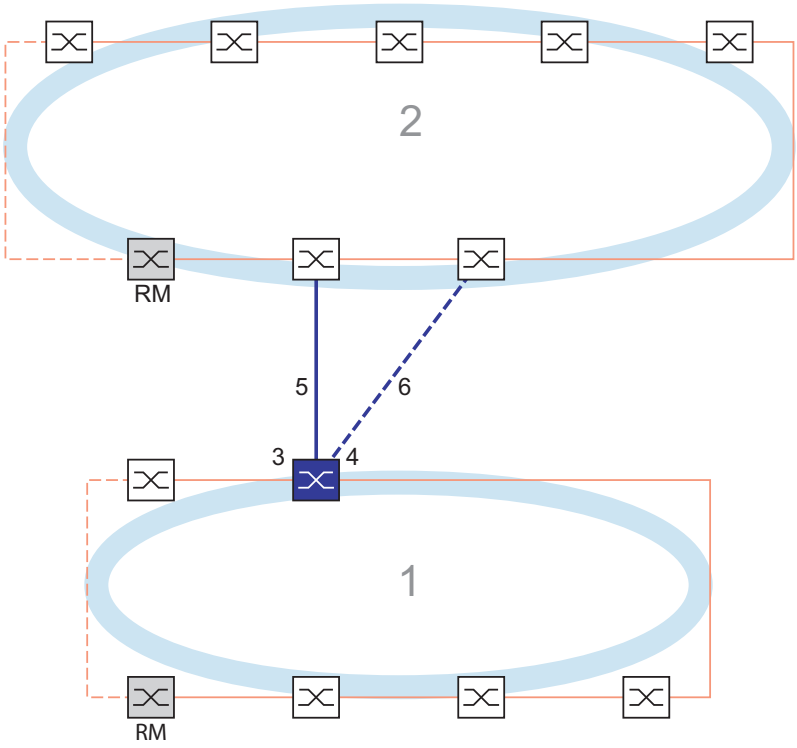


Abb. 56: Beispiel für die 1-Switch-Kopplung
1: Ring
2: Backbone
3: Partner-Kopplungs-Port
4: Kopplungs-Port
5: Hauptleitung
6: Redundante Leitung

Die durch die durchgängige blaue Linie gekennzeichnete Hauptleitung, die mit dem Partner-Kopplungs-Port verbunden ist, stellt die Kopplung zwischen den 2 Netzen im normalen Betriebsmodus her. Bei Ausfall der Hauptleitung übernimmt die durch die gestrichelte blaue Linie gekennzeichnete redundante Leitung, die mit dem Kopplungs-Port verbunden ist, die Ring-/Netzkopplung.
1 Switch nimmt die Kopplungsumschaltung vor.

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

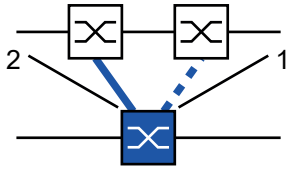


Abb. 57: 1-Switch-Kopplung
1: Kopplungs-Port
2: Partner-Kopplungs-Port

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld *Ein-Switch-Kopplung*.

Anmerkung: Konfigurieren Sie den *Partner-Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.

- ☐ Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die redundante Leitung anschließen.
- ☐ Wählen Sie im Rahmen *Partner-Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Hauptleitung anschließen.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Verbinden Sie die redundante Leitung mit dem Partner-Kopplungs-Port.
  Das Feld *Zustand* im Rahmen *Partner-Kopplungs-Port* zeigt den Status des Partner-Kopplungs-Ports.
- ☐ Verbinden Sie die Hauptleitung mit dem Kopplungs-Port.
  Das Feld *Zustand* im Rahmen *Kopplungs-Port* zeigt den Status des Kopplungs-Ports.

Das Feld *Redundanz verfügbar* im Rahmen *Information* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

Anmerkung: Für die Kopplungs-Ports sind die folgenden Einstellungen erforderlich.

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Legen Sie für die Ports, die als Kopplungs-Ports ausgewählt sind, die Einstellungen gemäß der Parameter in der folgenden Tabelle fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Tab. 40: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
TX	1 Gbit/s	markiert	markiert	–
Optisch	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
Optisch	1 Gbit/s	markiert	markiert	–
Optisch	2.5 Gbit/s	markiert	–	*2,5 Gbit/s FDX*

Falls Sie VLANs an den Kopplungs-Ports konfiguriert haben, legen Sie die VLAN-Einstellungen für die Kopplungs- und Partner-Kopplungs-Ports fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Zum Taggen der redundanten Verbindungen für `VLAN 1` und die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Die gekoppelten Geräte senden Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Redundanz-Modus* den Redundanztyp:
  - ▶ Mit der Einstellung *Redundante Ring-/Netz-Kopplung* ist entweder die Hauptleitung oder die redundante Leitung aktiv. Die Einstellung ermöglicht den Geräten, zwischen beiden Leitungen umzuschalten.
  - ▶ Wenn Sie die Einstellung *Erweiterte Redundanz* aktivieren, sind die Hauptleitung und die redundante Leitung gleichzeitig aktiviert. Die Einstellung ermöglicht Ihnen, Redundanz zum gekoppelten Netz hinzuzufügen. Wenn die Verbindung zwischen den gekoppelten Geräten im 2. Netz unterbrochen wird, fahren die gekoppelten Geräte mit der Übertragung und dem Empfang von Daten fort.

Anmerkung: Während der Rekonfigurationszeit können Paketdoppelungen auftreten. Daher können Sie diese Einstellung auswählen, wenn Ihre Geräte Paketdopplungen erkennen.

Der *Kopplungs-Modus* beschreibt den Typ des Backbone-Netzes, mit dem Sie das Ring-Netz verbinden (siehe Abbildung 56).

- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Kopplungs-Modus* den Typ des zweiten Netzes:
  - ☐ Wenn Sie eine Verbindung zu einem Ring-Netz herstellen, wählen Sie das Optionsfeld *Ring-Kopplung*.
  - ☐ Wenn Sie eine Verbindung zu einem Bus oder einer Mesh-Struktur herstellen, wählen Sie das Optionsfeld *Netz-Kopplung*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Setzen Sie die Kopplungseinstellungen auf den Grundzustand zurück. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Zurücksetzen*.

2-Switch-Kopplung

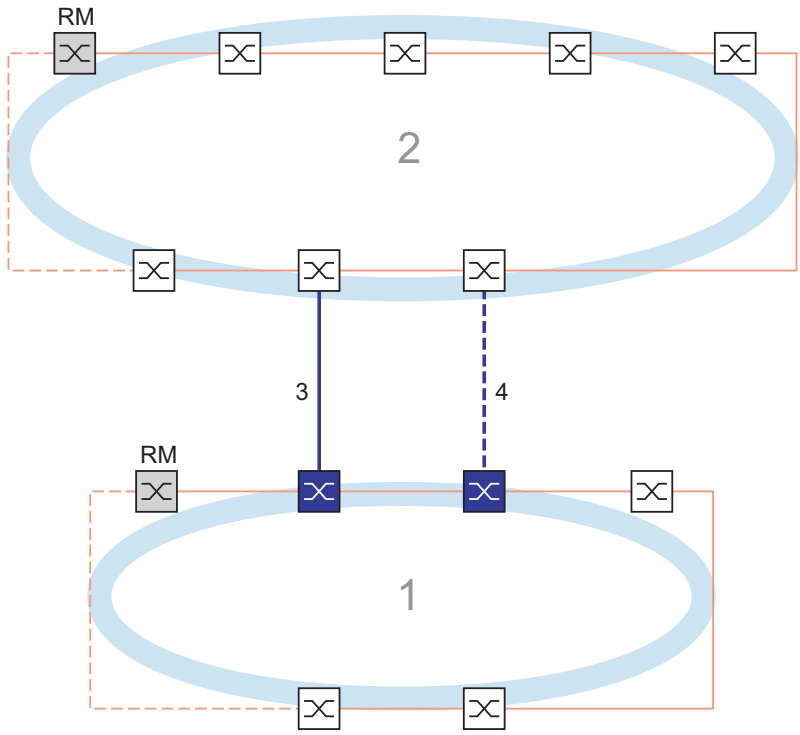


Abb. 58: Beispiel für die 2-Switch-Kopplung
1: Ring
2: Backbone
3: Hauptleitung
4: Redundante Leitung

Die Kopplung zwischen 2 Netzen erfolgt über die Hauptleitung, die durch die durchgängige blaue Linie gekennzeichnet ist. Wenn die Hauptleitung oder eines der benachbarten Geräte ausfällt, übernimmt die redundante Leitung, die durch die gestrichelte schwarze Linie gekennzeichnet ist, die Netzkopplung. Die Kopplung wird von 2 Geräten durchgeführt.

Die Geräte senden einander über das Ethernet Kontrollpakete.

Das an die Hauptleitung angeschlossene primäre Gerät und das an die redundante Leitung angeschlossene Standby-Gerät sind in Bezug auf die Kopplung Partner.
☐ Verbinden Sie die 2 Partner über die Ring-Ports.

2-Switch-Kopplung, primäres Gerät

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

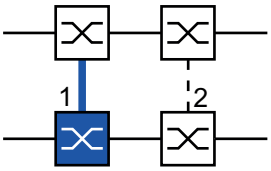


Abb. 59: 2-Switch-Kopplung, primäres Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld `Zwei-Switch-Kopplung, Master`.
- ☐ Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Netzsegmente anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Verbinden Sie die Hauptleitung mit dem *Kopplungs-Port*.
  Das Feld *Zustand* im Rahmen *Kopplungs-Port* zeigt den Status des Kopplungs-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

Das Feld *Redundanz verfügbar* im Rahmen *Information* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Anmerkung: Wenn die Funktion *Ring-Manager* und eine 2-Switch-Kopplung auf demselben Gerät aktiv sind, besteht die Möglichkeit, dass Loops entstehen.

Um dauerhafte Loops zu vermeiden, während die Verbindungen an den Ring-Kopplungs-Ports aktiv sind, führen Sie eine der folgenden Aktionen aus. Das Gerät setzt den Port-Status des Kopplungs-Ports auf „aus“:
- Betrieb deaktivieren
- Konfiguration ändern

Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Legen Sie für die Ports, die als Kopplungs-Ports ausgewählt sind, die Einstellungen gemäß der Parameter in der folgenden Tabelle fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Tab. 41: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
TX	1 Gbit/s	markiert	markiert	–
Optisch	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
Optisch	1 Gbit/s	markiert	markiert	–
Optisch	2.5 Gbit/s	markiert	–	*2,5 Gbit/s FDX*

Falls Sie VLANs an den Kopplungs-Ports konfiguriert haben, legen Sie die VLAN-Einstellungen für die Kopplungs- und Partner-Kopplungs-Ports fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Zum Taggen der redundanten Verbindungen für `VLAN 1` und die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

Die gekoppelten Geräte senden Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

2-Switch-Kopplung, Standby-Gerät

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

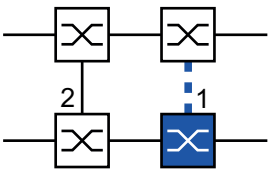


Abb. 60: 2-Switch-Kopplung, Standby-Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld *Zwei-Switch-Kopplung, Slave*.
- ☐ Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Netzsegmente anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Verbinden Sie die redundante Leitung mit dem *Kopplungs-Port*.
  Das Feld *Zustand* im Rahmen *Kopplungs-Port* zeigt den Status des Kopplungs-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

Das Feld *Redundanz verfügbar* im Rahmen *Information* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Anmerkung: Wenn die Funktion *Ring-Manager* und eine 2-Switch-Kopplung auf demselben Gerät aktiv sind, besteht die Möglichkeit, dass Loops entstehen.

Um dauerhafte Loops zu vermeiden, während die Verbindungen an den Ring-Kopplungs-Ports aktiv sind, führen Sie eine der folgenden Aktionen aus. Das Gerät setzt den Port-Status des Kopplungs-Ports auf „aus“:

- Betrieb deaktivieren
- Konfiguration ändern

Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Legen Sie für die Ports, die als Kopplungs-Ports ausgewählt sind, die Einstellungen gemäß der Parameter in der folgenden Tabelle fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Tab. 42: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
TX	1 Gbit/s	markiert	markiert	–
Optisch	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
Optisch	1 Gbit/s	markiert	markiert	–
Optisch	2.5 Gbit/s	markiert	–	*2,5 Gbit/s FDX*

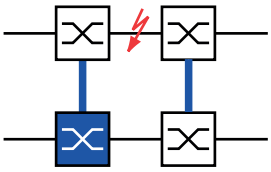
Falls Sie VLANs an den Kopplungs-Ports konfiguriert haben, legen Sie die VLAN-Einstellungen für die Kopplungs- und Partner-Kopplungs-Ports fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Zum Taggen der redundanten Verbindungen für `VLAN 1` und die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Die gekoppelten Geräte senden Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

Legen Sie die *Redundanz-Modus*- und *Kopplungs-Modus*-Einstellungen fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Redundanz-Modus* eines der folgenden Optionsfelder.
  - ▶ `Redundante Ring-/Netz-Kopplung`
    Mit dieser Einstellung ist entweder die Hauptleitung oder die redundante Leitung aktiv. Die Einstellung ermöglicht den Geräten, zwischen beiden Leitungen umzuschalten.
  - ▶ `Erweiterte Redundanz`
    Mit dieser Einstellung sind die Hauptleitung und die redundante Leitung gleichzeitig aktiv. Die Einstellung ermöglicht Ihnen, Redundanz zum 2. Netz hinzuzufügen. Wenn die Verbindung zwischen den gekoppelten Geräten im 2. Netz unterbrochen wird, fahren die gekoppelten Geräte mit der Übertragung und dem Empfang von Daten fort.

    Während der Rekonfigurationszeit können Paketdoppelungen auftreten. Wählen Sie diese Einstellung daher nur, wenn Ihre Geräte Paketdoppelungen erkennen.
- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Kopplungs-Modus* eines der folgenden Optionsfelder.
  - ☐ Wenn Sie eine Verbindung zu einem Ring-Netz herstellen, wählen Sie das Optionsfeld *Ring-Kopplung*.
  - ☐ Wenn Sie eine Verbindung zu einem Bus oder einer Mesh-Struktur herstellen, wählen Sie das Optionsfeld *Netz-Kopplung*.

  Der *Kopplungs-Modus* beschreibt den Typ des Backbone-Netzes, mit dem Sie das Ring-Netz verbinden (siehe Abbildung 58).
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

Setzen Sie die Kopplungseinstellungen auf den Grundzustand zurück. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche und dann den Eintrag *Zurücksetzen*.

2-Switch-Kopplung mit Steuerleitung

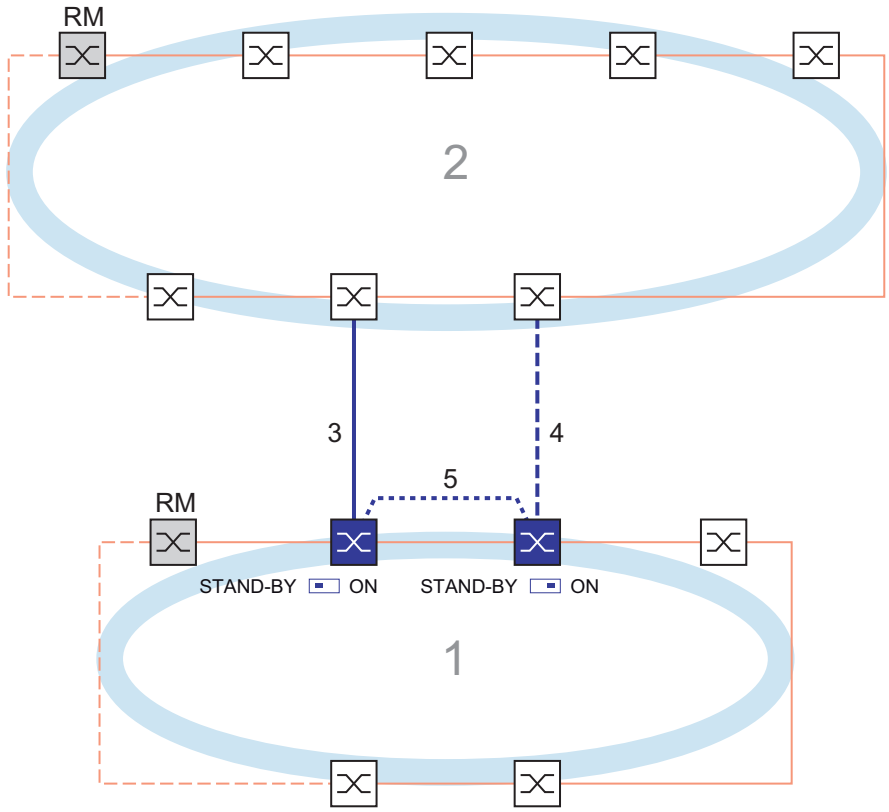


Abb. 61: Beispiel für die 2-Switch-Kopplung mit Steuerleitung
1: Ring
2: Backbone
3: Hauptleitung
4: Redundante Leitung
5: Steuerleitung

Die Kopplung zwischen 2 Netzen erfolgt über die Hauptleitung, die durch die durchgängige blaue Linie gekennzeichnet ist. Wenn die Hauptleitung oder eines der benachbarten Geräte ausfällt, übernimmt die redundante Leitung, die durch die gestrichelte blaue Linie gekennzeichnet ist, die Kopplung der 2 Netze. Die Ring-Kopplung wird von 2 Geräten durchgeführt.

Die Geräte senden Kontrollpakete über eine Steuerleitung, die in der folgenden Abbildung durch eine gepunktete blaue Linie gekennzeichnet ist (siehe Abbildung 62).

Das an die Hauptleitung angeschlossene primäre Gerät und das an die redundante Leitung angeschlossene Standby-Gerät sind in Bezug auf die Kopplung Partner.

☐ Verbinden Sie die 2 Partner über die Ring-Ports.

2-Switch-Kopplung mit Steuerleitung, primäres Gerät

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

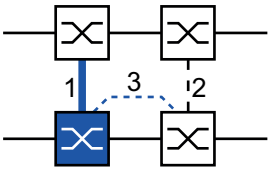


Abb. 62: 2-Switch-Kopplung mit Steuerleitung, primäres Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port
3: Steuerleitung

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld `Zwei-Switch-Kopplung mit Steuer-Leitung, Master`.
- ☐ Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Netzsegmente anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- ☐ Wählen Sie im Rahmen *Steuer-Port*, Dropdown-Liste *Port* den Port, an den Sie die Steuerleitung anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Verbinden Sie die redundante Leitung mit dem Kopplungs-Port.
  Das Feld *Zustand* im Rahmen *Kopplungs-Port* zeigt den Status des Kopplungs-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.
- ☐ Verbinden Sie die Steuerleitung mit dem Steuer-Port.
  Das Feld *Zustand* im Rahmen *Steuer-Port* zeigt den Status des Steuer-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

Das Feld *Redundanz verfügbar* im Rahmen *Information* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Anmerkung: Wenn die Funktion *Ring-Manager* und eine 2-Switch-Kopplung auf demselben Gerät aktiv sind, besteht die Möglichkeit, dass Loops entstehen.

Um dauerhafte Loops zu vermeiden, während die Verbindungen an den Ring-Kopplungs-Ports aktiv sind, führen Sie eine der folgenden Aktionen aus. Das Gerät setzt den Port-Status des Kopplungs-Ports auf „aus“:

- Betrieb deaktivieren
- Konfiguration ändern

Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*.
- ☐ Legen Sie für die Ports, die als Kopplungs-Ports ausgewählt sind, die Einstellungen gemäß der Parameter in der folgenden Tabelle fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Tab. 43: Port-Einstellungen für Ring-Ports

Port-Typ	Bitrate	Port an	Automatische Konfiguration	Manuelle Konfiguration
TX	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
TX	1 Gbit/s	markiert	markiert	–
Optisch	100 Mbit/s	markiert	unmarkiert	*100 Mbit/s FDX*
Optisch	1 Gbit/s	markiert	markiert	–
Optisch	2.5 Gbit/s	markiert	–	*2,5 Gbit/s FDX*

Falls Sie VLANs an den Kopplungs-Ports konfiguriert haben, legen Sie die VLAN-Einstellungen für die Kopplungs- und Partner-Kopplungs-Ports fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Zum Taggen der redundanten Verbindungen für `VLAN 1` und die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Die gekoppelten Geräte senden Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

2-Switch-Kopplung mit Steuerleitung, Standby-Gerät

Die folgenden Einstellungen betreffen das in der ausgewählten Grafik blau dargestellte Gerät.

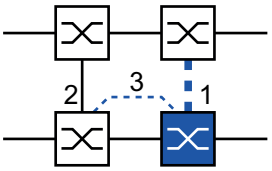


Abb. 63: 2-Switch-Kopplung mit Steuerleitung, Standby-Gerät
1: Kopplungs-Port
2: Partner-Kopplungs-Port
3: Steuerleitung

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Modus*, Optionsliste *Typ* das Optionsfeld `Zwei-Switch-Kopplung mit Steuer-Leitung, Slave`.
- ☐ Wählen Sie im Rahmen *Kopplungs-Port*, Dropdown-Liste *Port* den Port, an den Sie die Netzsegmente anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- ☐ Wählen Sie im Rahmen *Steuer-Port*, Dropdown-Liste *Port* den Port, an den Sie die Steuerleitung anschließen.
  Konfigurieren Sie den *Kopplungs-Port* und die Ring-Ports an verschiedenen Ports.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.
- ☐ Verbinden Sie die redundante Leitung mit dem Kopplungs-Port.
  Das Feld *Zustand* im Rahmen *Kopplungs-Port* zeigt den Status des Kopplungs-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.
- ☐ Verbinden Sie die Steuerleitung mit dem Steuer-Port.
  Das Feld *Zustand* im Rahmen *Steuer-Port* zeigt den Status des Steuer-Ports.
  Wenn der Partner bereits im Netz aktiv ist, zeigt das Feld *IP-Adresse* im Rahmen *Partner-Kopplungs-Port* die IP-Adresse des Partner-Ports.

Das Feld *Redundanz verfügbar* im Rahmen *Information* zeigt, ob Redundanz vorhanden ist. Das Feld *Konfigurationsfehler* zeigt, ob die Einstellungen vollständig und korrekt sind.

Anmerkung: Wenn die Funktion *Ring-Manager* und eine 2-Switch-Kopplung auf demselben Gerät aktiv sind, besteht die Möglichkeit, dass Loops entstehen.

Um dauerhafte Loops zu vermeiden, während die Verbindungen an den Ring-Kopplungs-Ports aktiv sind, führen Sie eine der folgenden Aktionen aus. Das Gerät setzt den Port-Status des Kopplungs-Ports auf „aus“:

- Betrieb deaktivieren
- Konfiguration ändern

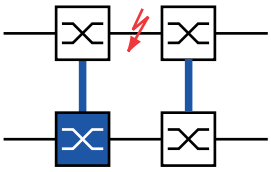
Für die Kopplungs-Ports führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > VLAN > Port*.
- ☐ Ändern Sie die Einstellung für die *Port-VLAN-ID* in den Wert der VLAN-ID, der an den Ports konfiguriert ist.
- ☐ Entfernen Sie die Markierung im Kontrollkästchen *Ingress-Filtering* für die beiden Kopplungs-Ports.
- ☐ Öffnen Sie den Dialog *Switching > VLAN > Konfiguration*.
- ☐ Zum Taggen der redundanten Verbindungen für `VLAN 1` und die VLAN-Mitgliedschaft geben Sie den Wert `T` in die entsprechenden Zellen für beide Kopplungs-Ports in der Zeile `VLAN 1` ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

Die gekoppelten Geräte senden Redundanzpakete mit der höchsten Priorität über `VLAN 1`.

Legen Sie die *Redundanz-Modus*- und *Kopplungs-Modus*-Einstellungen fest. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Ring-/Netzkopplung*.
- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Redundanz-Modus* eines der folgenden Optionsfelder.
  - ▶ *Redundante Ring-/Netz-Kopplung*
    Mit dieser Einstellung ist entweder die Hauptleitung oder die redundante Leitung aktiv. Die Einstellung ermöglicht den Geräten, zwischen beiden Leitungen umzuschalten.
  - ▶ *Erweiterte Redundanz*
    Mit dieser Einstellung sind die Hauptleitung und die redundante Leitung gleichzeitig aktiv. Die Einstellung ermöglicht Ihnen, Redundanz zum 2. Netz hinzuzufügen. Wenn die Verbindung zwischen den gekoppelten Geräten im 2. Netz unterbrochen wird, fahren die gekoppelten Geräte mit der Übertragung und dem Empfang von Daten fort.

    Während der Rekonfigurationszeit können Paketdoppelungen auftreten. Wählen Sie diese Einstellung daher nur, wenn Ihre Geräte Paketdoppelungen erkennen.
- ☐ Wählen Sie im Rahmen *Konfiguration*, Optionsliste *Kopplungs-Modus* eines der folgenden Optionsfelder.
  - ☐ Wenn Sie eine Verbindung zu einem Ring-Netz herstellen, wählen Sie das Optionsfeld *Ring-Kopplung*.
  - ☐ Wenn Sie eine Verbindung zu einem Bus oder einer Mesh-Struktur herstellen, wählen Sie das Optionsfeld *Netz-Kopplung*.

  Der *Kopplungs-Modus* beschreibt den Typ des Backbone-Netzes, mit dem Sie das Ring-Netz verbinden (siehe Abbildung 61).
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

Setzen Sie die Kopplungseinstellungen auf den Grundzustand zurück. Führen Sie dazu die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche und dann den Eintrag *Zurücksetzen*.

13.13 RCP

Industrielle Anwendungen fordern von ihren Netzen eine hohe Verfügbarkeit. Dies beinhaltet auch die Aufrechterhaltung deterministischer, kurzer Unterbrechungszeiten für die Kommunikation beim Ausfall eines Geräts im Netz.

Eine Ringtopologie bietet kurze Übergangszeiten bei minimalem Ressourceneinsatz. Allerdings stellt die Ringtopologie eine Herausforderung hinsichtlich der redundanten Kopplung dieser Ringe dar.

Das Redundant Coupling Protocol *RCP* ermöglicht Ihnen, Ringe zu koppeln, die mit einem der folgenden Redundanzprotokolle arbeiten:

- MRP
- HIPER-Ring
- RSTP

Die Funktion *RCP* ermöglicht Ihnen außerdem, mehrere Sekundär-Ringe mit einem Primär-Ring zu koppeln (siehe Abbildung 64). Ausschließlich die Switches, welche die Ringe koppeln, benötigen die Funktion *RCP*.

Innerhalb dieser gekoppelten Netzwerke können Sie auch Geräte verwenden, bei denen es sich nicht um Schneider Electric-Geräte handelt.

Die Funktion *RCP* verwendet ein Master- und ein Slave-Gerät für die Übertragung von Daten zwischen den Netzen. Nur das Master-Gerät vermittelt Frames zwischen den Ringen.

Mittels proprietärer Schneider Electric-Multicast-Nachrichten informieren die *RCP*-Master- und die Slave-Geräte einander über ihren jeweiligen Betriebsmodus. Konfigurieren Sie die Geräte im Ring, die keine Kopplungsgeräte sind, darauf, die folgenden Multicast-Adressen weiterzuleiten:

- `01:80:63:07:00:09`
- `01:80:63:07:00:0A`

Verbinden Sie die Master- und Slave-Geräte als direkte Nachbarn.

Um die redundante Kopplung herzustellen, verwenden Sie 4 Ports je Gerät. Installieren Sie die gekoppelten Geräte mit 2 inneren Ports und 2 äußeren Ports in jedem Netz.

- Der innere Port stellt eine Verbindung zwischen den Master- und den Slave-Geräten her.
- Der äußere Port verbindet die Geräte mit dem Netz.

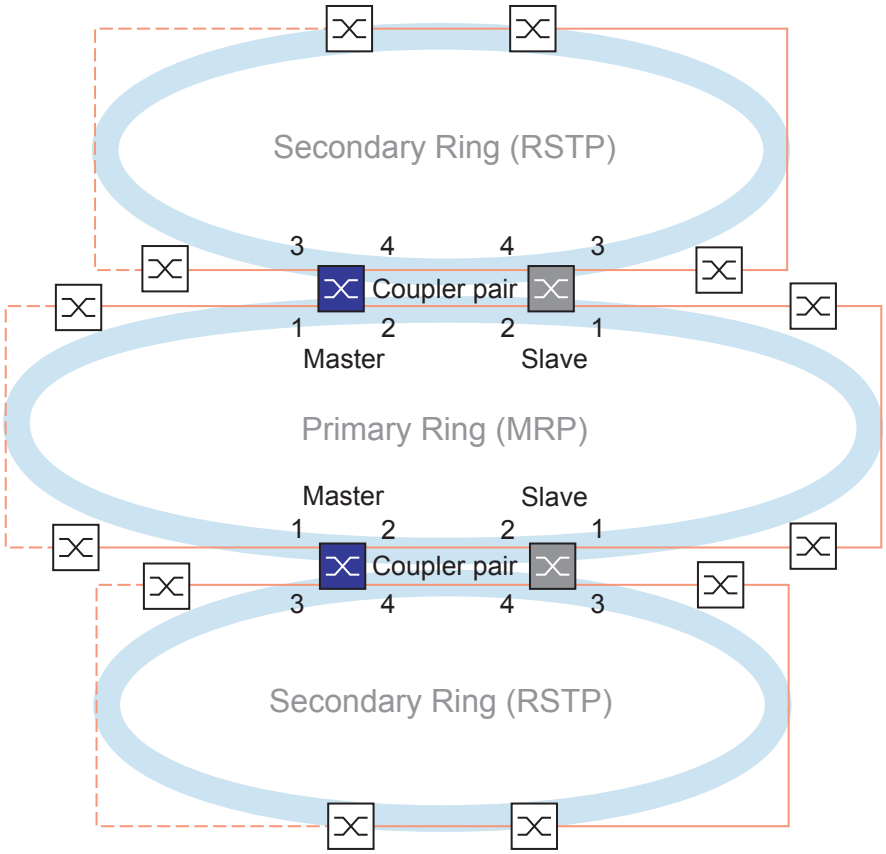


Abb. 64: Beispiel einer redundanten 2-Switch-Kopplung
1: Äußerer Kopplungs-Port im Primär-Ring
2: Innerer Kopplungs-Port im Primär-Ring
3: Äußerer Kopplungs-Port im Sekundär-Ring
4: Innerer Kopplungs-Port im Sekundär-Ring

Wenn Sie für die Rolle den Wert *auto* festlegen, wählt das koppelnde Gerät seine Rolle als *master* oder *slave* selbst. Konfigurieren Sie die Rollen manuell, wenn Sie ein permanentes Master- oder Slave-Gerät möchten.

Anmerkung: Die Rolle `single` ist ausschließlich in Verbindung mit der Funktion *Dual RSTP* verwendbar. Siehe „Koppeln von 2 RSTP-Ringen mit der Funktion Dual RSTP" auf Seite 254.

Wenn das Master-Gerät nicht mehr über die inneren Kopplungs-Ports erreichbar ist, wartet das Slave-Gerät bis zum Ablauf des Timeout-Zeitraums, bevor es die Master-Rolle übernimmt. Während des festgelegten Timeout-Zeitraums versucht das Slave-Gerät, das Master-Gerät mit Hilfe der äußeren Kopplungs-Ports zu erreichen. Wenn das Master-Gerät immer noch nicht erreichbar ist, übernimmt das Slave-Gerät die Master-Rolle. Um die Stabilität des Netzes zu erhalten, das mit den äußeren Kopplungs-Ports verbunden ist, konfigurieren Sie den Timeout-Zeitraum so, dass dieser länger ist als der Recovery-Zeitraum der gekoppelten Ringe.

Anmerkung: Deaktivieren Sie RSTP an den redundanten inneren und äußeren *RCP*-Ports für die redundante Kopplung, die nicht mit dem RSTP-Ring verbunden sind. In der Beispielkonfiguration deaktivieren Sie RSTP an den Ports `1` und `2` jedes Geräts.

13.13.1 Anwendungsbeispiel für RCP-Kopplung

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät der *RCP*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Die Schneider Electric-Geräte unterstützen die 2-Switch-Redundant-Coupling-Protocol-Methode. Um beispielsweise ein Netz zu erzeugen, das in einem Zug installiert ist, können Sie die Funktion *RCP* verwenden. Das Netz stellt Fahrgästen Informationen zum Zugstandort oder zu den verschiedenen Bahnhöfen auf der Strecke bereit. Das Netz kann auch zur Sicherheit der Fahrgäste beitragen, zum Beispiel mittels Videoüberwachung.

Die Primär-Ringe in der Abbildung stellen ein *MRP*-Ring-Netz in einem Waggon dar. Die Sekundär-Ringe in der Abbildung sind RSTP-Ring-Netze. Jeder Ring umfasst 4 Geräte (siehe Abbildung 65).

Um die Zugtopologie in der Abbildung zu vereinfachen, sind die *MRP*-Ring-Ports und die inneren und äußeren *RCP*-Ports denselben Portnummern zugewiesen. Legen Sie dieselben Werte für die Parameter der Ports gemäß ihrer jeweiligen Funktion im Netz fest. Legen Sie Ports *1/1* und *1/2* an Switch 1D und 1C als MRP-Ring-Ports fest. Port *1/4* als *RCP* innerer Port, und Port *1/3* als *RCP* äußerer Port.

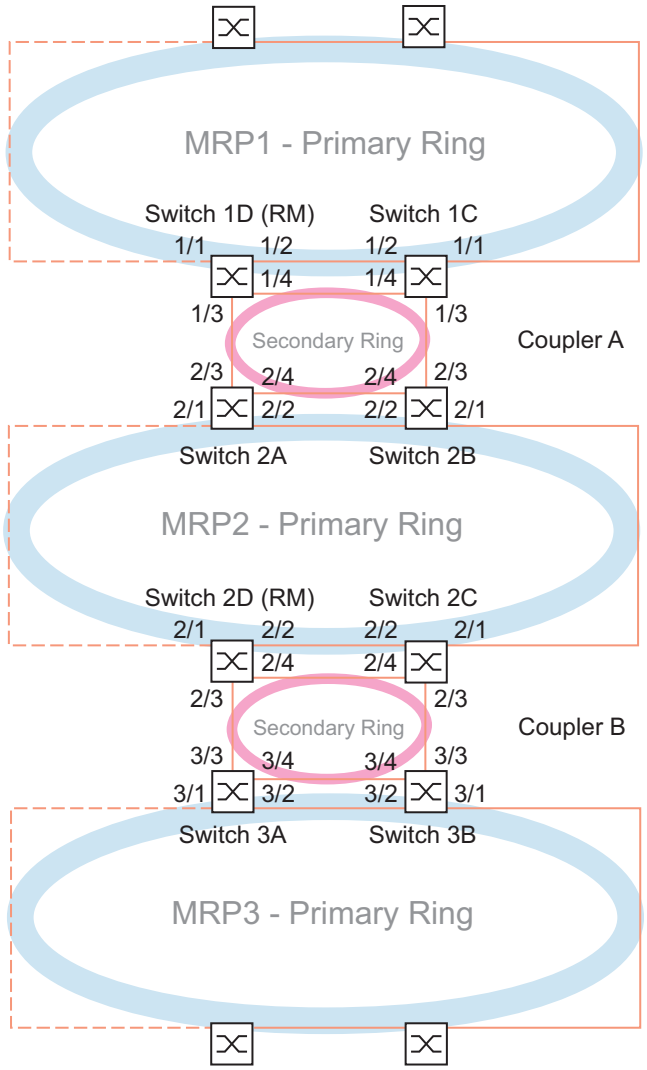


Abb. 65: Redundant-Coupling-Protocol-Zugtopologie

Die folgende Liste legt die Rollen der Ports an jedem Gerät fest.
1: Ports 1 und 2 sind MRP-Ring-Ports.
2: Port 3 ist ein äußerer RCP-Port.
3: Port 4 ist ein innerer RCP-Port.

Die folgenden Schritte beschreiben die für Switch 1D in Koppler A festzulegenden Parameter. Konfigurieren Sie die anderen für Koppler A verwendeten Geräte und die in Koppler B verwendeten Geräte auf dieselbe Weise.

Deaktivieren der Funktion RSTP im MRP-Ring

*MRP*und RSTP funktionieren nicht zusammen. Deaktivieren Sie daher die Funktion RSTP an den *RCP*-Ports, die im *MRP*-Ring verwendet werden. In der Beispielkonfiguration werden Ports `x/1` und `x/2` für den *MRP*-Ring verwendet. Aktivieren Sie die Funktion RSTP ausschließlich an dem inneren und dem äußeren *RCP*-Port, die im Sekundär-Ring verwendet werden. Aktivieren Sie die Funktion RSTP beispielsweise an Port `x/3` und `x/4`.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*.
- ☐ In der Voreinstellung ist die Funktion RSTP an den Ports aktiviert. Um die Funktion RSTP an den *MRP*-Ring-Ports zu deaktivieren, heben Sie die Markierung des Kontrollkästchens *STP aktiv* für Port `x/1` und Port `x/2` auf.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface x/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `x/1`.
`no spanning-tree mode`	Ausschalten der Funktion *Spanning Tree* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`interface x/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `x/2`.
`no spanning-tree mode`	Ausschalten der Funktion *Spanning Tree* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`spanning-tree operation`	Einschalten der Funktion *Spanning Tree*.

Festlegen des Ring-Masters im MRP-Ring

In der Abbildung ist Switch D jedes *MRP*-Rings als Ring-Manager festgelegt (siehe Abbildung 65). Legen Sie die anderen Switches in den Ringen als Ring-Clients fest.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > MRP*.
- ☐ Legen Sie den 1. Ring-Port im Rahmen *Ring-Port 1* fest. Wählen Sie in der Dropdown-Liste *Port* den Port `x/1`.
- ☐ Legen Sie den 2. Ring-Port im Rahmen *Ring-Port 2* fest. Wählen Sie in der Dropdown-Liste *Port* den Port `x/2`.

- ☐ Um das Gerät als Ring-Manager festzulegen, aktivieren Sie die Funktion im Rahmen *Ring-Manager*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`mrp domain add default-domain`	Erzeugen einer neuen *MRP*-Domäne mit der ID `default-domain`.
`mrp domain modify port primary x/1`	Festlegen des Ports `x/1` als Ring-Port `1`.
`mrp domain modify port secondary x/2`	Festlegen des Ports `x/2` als Ring-Port `2`.
`mrp domain modify mode manager`	Festlegen, dass das Gerät als *Ring-Manager* arbeitet. Bei den anderen Geräten im Ring belassen Sie die Voreinstellung.
`mrp domain modify operation enable`	Einschalten der Funktion *MRP*.

Festlegen der Geräte im redundanten Koppler

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > RCP*.
- ☐ Legen Sie den *Innerer Port* im Rahmen *Primärer Ring/Netzwerk* fest. Wählen Sie Port `x/2`.
- ☐ Legen Sie den *Äußerer Port* im Rahmen *Primärer Ring/Netzwerk* fest. Wählen Sie Port `x/1`.
- ☐ Legen Sie den *Innerer Port* im Rahmen *Sekundärer Ring/Netzwerk* fest. Wählen Sie Port `x/4`.
- ☐ Legen Sie den *Äußerer Port* im Rahmen *Sekundärer Ring/Netzwerk* fest. Wählen Sie Port `x/3`.

- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`redundant-coupling port primary inner x/2`	Port `x/2` als primären inneren Port festlegen.
`redundant-coupling port primary outer x/1`	Port `x/1` als primären äußeren Port festlegen.
`redundant-coupling port secondary inner x/4`	Port `x/4` als sekundären inneren Port festlegen.

`redundant-coupling port secondary outer x/3`	Port `x/3` als sekundären äußeren Port festlegen.
`redundant-coupling operation`	Einschalten der Funktion *RCP* auf dem Gerät.
`copy config running-config nvm`	Speichern der aktuellen Einstellungen im „ausgewählten" Konfigurationsprofil im permanenten Speicher (`nvm`).

13.13.2 Koppeln von 2 RSTP-Ringen mit der Funktion Dual RSTP

Wenn Sie RSTP für den Primär-Ring und den Sekundär-Ring verwenden möchten, dann ordnet die Funktion *RCP* die Ports des Sekundär-Rings der *Dual RSTP*-Instanz zu. Dadurch entstehen zwei unabhängige RSTP-Netze, die mit *RCP* gekoppelt sind.

Sie haben die Möglichkeit, bis zu 16 MCSESM-E-Geräte in einem Sekundär-Ring zu betreiben. Dazu gehören die 2 Geräte des Primär-Rings, die den Sekundär-Ring ankoppeln. Wenn eine Netz-Komponente im Sekundär-Ring ausfällt, erreicht die *RCP*-Funktion üblicherweise eine Rekonfigurationszeit von unter 50 ms.

Sie haben außerdem die Möglichkeit, bis zu 16 MCSESM-E-Geräte in einem Primär-Ring zu betreiben. Dadurch erreichen die Funktionen *RCP* und *Dual RSTP* auch im Primär-Ring üblicherweise eine Rekonfigurationszeit von unter 50 ms. Sie können bis zu 8 Sekundär-Ringe an einen Primär-Ring ankoppeln. Somit können Sie bis zu 128 Bridges (8 × 14 + 16) koppeln. In diesem Netz erreichen Sie bei Geräte-Redundanz eine Ende-zu-Ende-Rekonfigurationszeit von üblicherweise unter 50 ms.

Bei geringeren Anforderungen an die Rekonfigurationszeit im Primär-Ring haben Sie folgende Möglichkeiten:
- Anzahl der Bridges im Primär-Ring erhöhen.
- Weitere Sekundär-Ringe an den Primär-Ring ankoppeln.

Sie können in den Ringen auch andere Geräte als MCSESM-E verwenden, vorausgesetzt, die Geräte aktualisieren RSTP-Topologieänderungen schnell genug. Zum Beispiel dann, wenn ein Gerät im Netz ausfällt.

Eigenschaften der primären und sekundären Ports der Instanz

Beachten Sie bei den Ports der Primär- und Sekundär-Instanzen die folgenden Hinweise:
- Zur *Dual RSTP*-Instanz gehören ausschließlich diejenigen Ports der *RCP*-Bridge, die als äußere oder innere Ring-Ports des Sekundär-Rings konfiguriert sind. Die anderen Ports gehören zur primären Instanz der Bridge.
- Sie haben die Möglichkeit, Endgeräte oder Netze, die *Spanning Tree* nicht ausführen, an einen Port anzuschließen, der implizit zu einer primären Instanz der *RCP*-Bridge gehört.
  Diese Topologien stellen weder Geräte-Redundanz noch Verbindungs-Redundanz zur Verfügung.
- Sie haben die Möglichkeit, innerhalb des Primär-Rings oder des Sekundär-Rings durch weitere Verbindungen zwischen Ports der selben Instanz Maschen zu bilden.
  Für diese Topologien entfällt innerhalb der jeweiligen Instanz die definierte maximale Ende-zu-Ende-Rekonfigurationszeit von 50 ms.

Koppeln von 2 RSTP-Ringen mit einer RCP-Bridge

Wenn Sie 2 RSTP-Ringe mit lediglich einer Bridge koppeln möchten, dann verwenden Sie dazu die Rolle `single`.

Bei einer *RCP*-Bridge in der Rolle `single` haben die inneren und äußeren Ports die gleiche Funktion. Sie können die inneren und äußeren Ports einer bestimmten Instanz vertauschen.

Beim Einsatz von einer Bridge zur Kopplung können Sie bis zu 16 Sekundär-Ringe an einen Primär-Ring ankoppeln. Die Dual *RCP*-Bridge, die die Ringe koppelt, zählt dabei mit. Somit können Sie bis zu 256 Bridges (16 × 15 + 16) koppeln. In diesem Netz erreichen Sie eine maximale Ende-zu-Ende-Rekonfigurationszeit von 50 ms in einem Netz mit Verbindungs-Redundanz.

Bei geringeren Anforderungen an die Rekonfigurationszeit im Primär-Ring haben Sie folgende Möglichkeiten:
- Anzahl der Bridges im Primär-Ring erhöhen.
- Weitere Sekundär-Ringe an den Primär-Ring ankoppeln.

Topologie-Möglichkeiten für die Funktion Dual RSTP

Das folgende Beispiel zeigt den grundsätzlichen Aufbau eines Primär-Rings, an den 3 Sekundär-Ringe angekoppelt sind. Die Sekundär-Ringe 1 und 2 sind mit jeweils 2 *RCP*-Bridges an den Primär-Ring angekoppelt, der Sekundär-Ring 3 mit 1 *RCP*-Bridge. Die Pfadkosten für jede Verbindungen innerhalb eines Rings seien gleich groß.

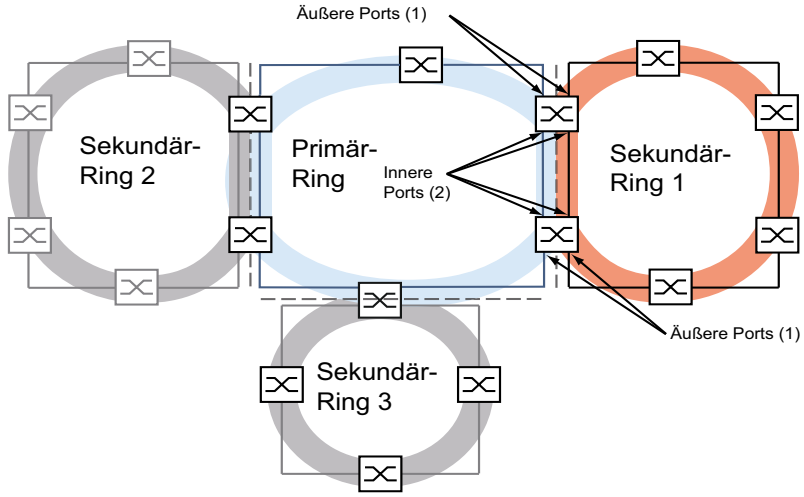


Abb. 66: Primär-Ring mit 3 mittels RCP verbunden Sekundär-Ringen

Konfiguration des Primär-Rings

Die folgenden Kapitel beschreiben die prinzipielle Konfiguration und enthalten daher keine Arbeitsschritte.

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Ergreifen Sie bei der konkreten Konfiguration geeignete Maßnahmen, um das Erzeugen von Schleifen (Loops) zu vermeiden.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Um die Root-Bridge und die Backup-Root-Bridge im Primär-Ring festzulegen, konfigurieren Sie deren globale RSTP-Bridge-Priorität. Eine optimal kurze Rekonfigurationszeit im Primär-Ring erhalten Sie, wenn sich die Root-Bridge und die Backup-Root-Bridge im Primär-Ring gegenüberliegen. Dies ist der Fall, wenn die Backup-Root-Bridge 2 Pfade zur Root-Bridge hat, auf denen sich die Anzahl der Geräte zur Root-Bridge um maximal 1 unterscheidet.

Konfigurieren Sie die weiteren Bridges im Primär-Ring, die sich zwischen Root-Bridge und Backup-Root-Bridge befinden, dahingehend, dass mit zunehmender Entfernung von der Root-Bridge die Bridge-Prioritäten abnehmen, also numerisch größer werden.

Die Abbildung zeigt ein Beispiel mit den RSTP-Details für den Primär-Ring. Die Topologie ist reduziert auf den Primär-Ring und einen Sekundär-Ring. Die Management-Station ist an den Primär-Ring angeschlossen, um im Verlauf der Konfiguration Unterbrechungen der Kommunikation zu den Bridges im Sekundär-Ring zu vermeiden.

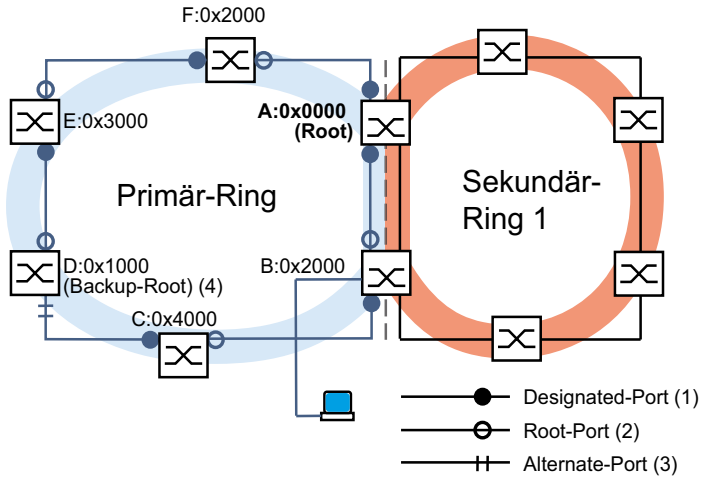


Abb. 67: Primär-Ring mit einem angekoppelten Sekundär-Ring, mit Details für den Primär-Ring
A..F: Bridge-Identifikation (Bridge-Identifier)
0x0000..0x4000: Bridge-Prioritäten im Primär-Ring

Konfiguration des Sekundär-Rings

Um die Root-Bridge und die Backup-Root-Bridge im Sekundär-Ring festzulegen, konfigurieren Sie für die *RCP*-Bridges die *Dual RSTP*-Bridge-Priorität. Für die anderen Bridges im Sekundär-Ring konfigurieren Sie lediglich deren globale RSTP-Bridge-Priorität. Eine optimal kurze Rekonfigurationszeit im Sekundär-Ring erhalten Sie, wenn sich die Root-Bridge und die Backup-Root-Bridge im Sekundär-Ring gegenüberliegen.

Konfigurieren Sie auch die weiteren Bridges im Sekundär-Ring dahingehend, dass mit zunehmender Entfernung von der Root-Bridge die Bridge-Prioritäten abnehmen, also numerisch größer werden.

Die Abbildung zeigt ein Beispiel mit den RSTP-Details für den Sekundär-Ring.

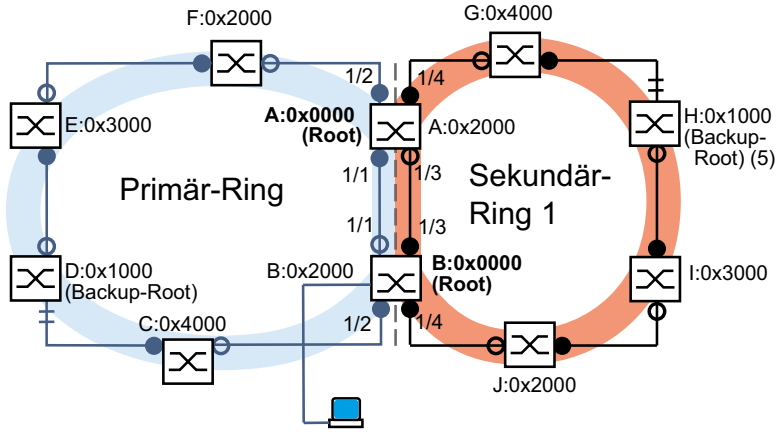


Abb. 68: Primär-Ring mit einem angekoppelten Sekundär-Ring, mit Details für den Sekundär-Ring
A, B, G bis J: Bridge-Identifikationen im Sekundär-Ring
0x0000..0x4000: Bridge-Prioriäten
für die Bridges A und B: Dual RSTP Bridge-Priorität
für die Bridges G bis J: Globale RSTP Bridge-Priorität
5: Backup-Root-Bridge für den Sekundär-Ring

Die Root-Bridge-Rollen im Primär-Ring und im Sekundär-Ring sind voneinander unabhängig. Eine Bridge kann RSTP-Root sein für:
- beide Ringe
- einen Ring
- keinen Ring

Betreiben Sie den Sekundär-Ring ausschließlich mit RSTP.

Konfiguration der Kopplung der Ringe

Definieren Sie bei den *RCP*-Bridges die inneren und äußeren Ports sowohl für den Primär-Ring als auch für den Sekundär-Ring.

Tab. 44: Ring-Ports für die RCP-Bridges

Ports	RCP Master (B)	RCP Slave (A)
Primär-Ring		
Innerer Port	1/1	1/1
Äußerer Port	1/2	1/2

Tab. 44: Ring-Ports für die RCP-Bridges

Ports	RCP Master (B)	RCP Slave (A)
Sekundär-Ring		
Innerer Port	1/3	1/3
Äußerer Port	1/4	1/4

Konfigurieren Sie danach die Rolle für jede *RCP*-Bridge.

Die Abbildung zeigt ein Beispiel.

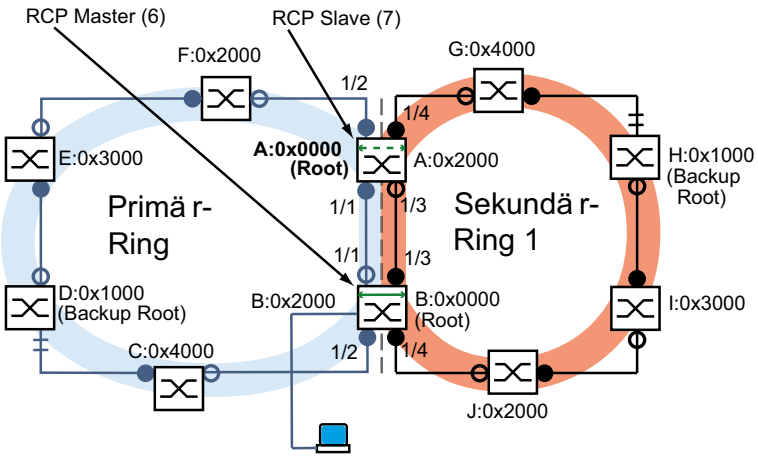


Abb. 69: Primär-Ring mit einem angekoppelten Sekundär-Ring, mit Port-Nummern und RCP-Rollen
6: RCP-Master
7: RCP-Slave

Die Root-Bridge-Rollen und die Kopplungs-Rollen sind voneinander unabhängig. Eine Bridge kann *RCP*-Master sein und gleichzeitig als RSTP-Root arbeiten für:
- beide Ringe
- einen Ring
- keinen Ring

Das Gleiche gilt für den *RCP*-Slave.

Schalten Sie danach die Funktion *RCP* ein.

13.13.3 Anwendungsbeispiel für RCP-Kopplung mit Dual RSTP

In einer Produktionshalle befinden sich mehrere Fertigungszellen. Die Geräte in einer Fertigungszelle sind in einer Linien-Netz-Struktur verbunden. Dieses Netz ist an das übergeordnete Netz der Produktionshalle angeschlossen. Das Netz der Produktionshalle ist redundant vermascht und arbeitet mit RSTP. Jedes Geräte ist vom Typ MCSESM-E.

Ihre Anforderungen:
- Ausstatten des vorhandenen Linien-Netzes in den Fertigungszellen mit einer schnellen Geräte-Redundanz.
- Redundantes Anbinden der Fertigungszellen an das Netz der Produktionshalle.
- Umkonfigurieren des Netzes der Produktionshalle, so dass es deterministische, kurze Rekonfigurationzeiten bietet.

Vorhandene Netz-Topologie, reduziert auf eine Fertigungszelle:

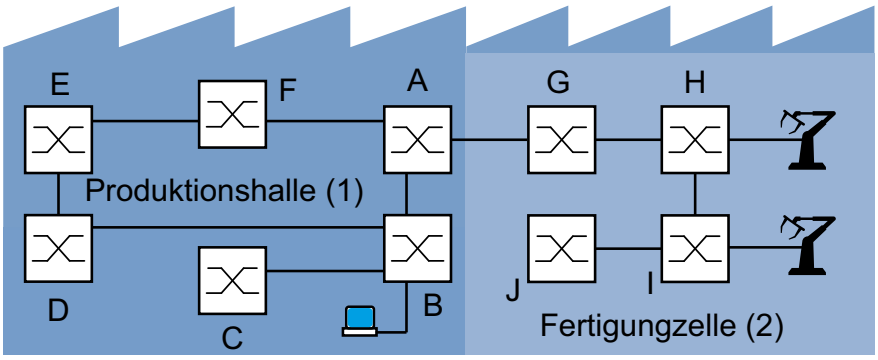


Abb. 70: Beispiel einer Fertigungszelle in einer Produktionshalle, Topologie vor dem Einsatz von RCP und Dual RSTP:
1: Produktionshalle
2: Fertigungszelle

Gewünschte *Dual RSTP*-Netz-Topologie:

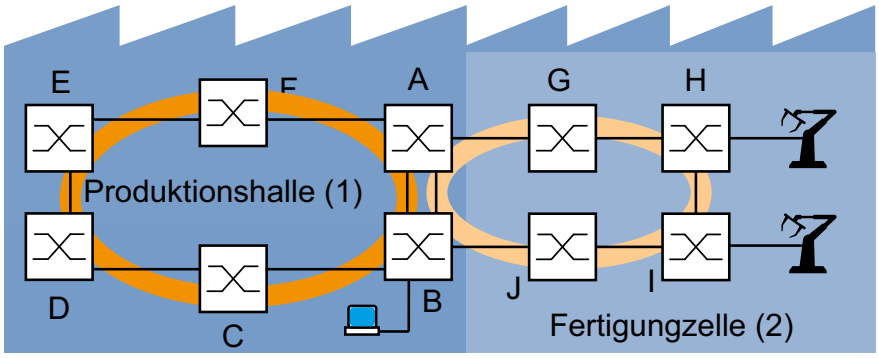


Abb. 71: Beispiel einer Fertigungszelle in einer Produktionshalle, Topologie beim Einsatz von RCP und Dual RSTP:
1: Produktionshalle
2: Fertigungszelle

Gewünschte *Dual RSTP*-Netz-Topologie in schematischer Darstellung:

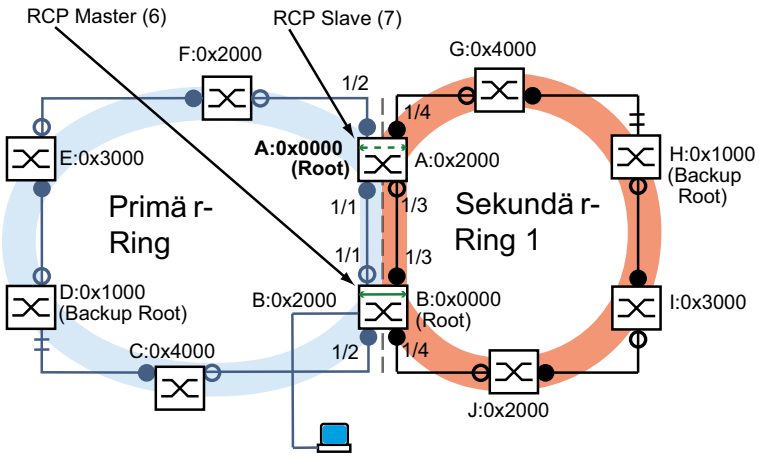


Abb. 72: Schematische Darstellung der Dual RSTP-Netz-Topologie
6: RCP-Master
7: RCP-Slave

Die folgende Tabelle zeigt, dass relativ wenige Einstellungen ausreichen, um die neue Topologie zu konfigurieren. Sie ändern die *Dual RSTP*-Einstellungen ausschließlich auf den Geräten A und B.

Tab. 45: Werte für die Konfiguration der Switches des Beispiels für Dual RSTP

Parameter	A	B	C	D	E	F	G	H	I	J
RSTP-Einstellungen										
Bridge-Priorität (hex.)[1]	0x0000	0x2000	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Dual-RSTP-Einstellungen										
Bridge-Priorität (hex.)[a]	0x2000	0x0000	-	-	-	-	-	-	-	-
RCP-Einstellungen										
Primär-Ring, innerer Port	1/1	1/1	-	-	-	-	-	-	-	-
Primär-Ring, äußerer Port	1/2	1/2	-	-	-	-	-	-	-	-
Sekundär-Ring, innerer Port	1/3	1/3	-	-	-	-	-	-	-	-
Sekundär-Ring, äußerer Port	1/4	1/4	-	-	-	-	-	-	-	-
Kopplungs-Rolle	Slave	Master	-	-	-	-	-	-	-	-

1. Zu den Bridge-Prioritäten in Hexadezimal- und Dezimalschreibweise siehe Tabelle 46.

Tab. 46: Mögliche Bridge-Prioritäten in Hexadezimal- und Dezimalschreibweise

Bridge-Priorität								
hexadezimal	0x0000	0x1000	0x2000	0x3000	0x4000	0x5000	0x6000	0x7000
dezimal	0	4096	8192	12288	16384	20480	24576	28672

hexadezimal	0x8000	0x9000	0xA000	0xB000	0xC000	0xD000	0xE000	0xF000
dezimal	32768	36864	40960	45056	49152	53248	57344	61440

Voraussetzungen für die weitere Konfiguration:

- Die Verbindung für die bisherige Vermaschung – in der alten Topologie – des Sekundär-Rings zwischen den Bridges B und D ist inaktiv. Dies erreichen Sie zum Beispiel, indem Sie die entsprechenden Ports auf den Bridges B und D manuell deaktivieren oder den Link ziehen.
- Die Verbindungen zwischen den Bridges C und D sowie den Bridges J und B sind inaktiv. Dies erreichen Sie zum Beispiel, indem Sie die entsprechenden Ports auf den Bridges manuell deaktivieren, bevor Sie die Links stecken.
- Die Verbindung des Sekundär-Rings zwischen den Bridges A und B ist inaktiv.
- RSTP ist auf jedem Gerät aktiv, die Parameter sind im Lieferzustand.
- Ihre Management-Station ist an den Primär-Ring angeschlossen.

- Sie haben die grafische Benutzeroberfläche oder das Command Line Interface der Geräte A und B geöffnet.
- Sie haben Zugriff auf die Benutzer-Oberfläche der Geräte C bis J.

⚠ WARNUNG

LOOP-GEFAHR

- Konfigurieren Sie jedes Gerät der *RCP*- und *Dual RSTP*-Konfiguration individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.
- Konfigurieren Sie den Timeout in der *RCP*-Kopplungskonfiguration länger als die längste anzunehmende Unterbrechungszeit der schnelleren Instanz des Redundanzprotokolls.
- Konfigurieren Sie in einer Topologie mit 2 Kopplungs-Bridges die Kopplungs-Rollen der beiden Geräte ausschließlich als `master`, `slave` oder `auto`.
- Koppeln Sie die primäre Instanz und die sekundäre Instanz ausschließlich über 1 *RCP*-Bridge (bei einer Topologie mit *RCP*-Bridge) oder 2 *RCP*-Bridges (bei einer Topologie mit 2 *RCP*-Bridges). Halten Sie die Ports der primären Instanz getrennt von den Ports der einzelnen sekundären Instanzen.
- Aktivieren Sie die *Admin-Edge-Port*-Einstellung auf einem Port ausschließlich dann, wenn ein Endgerät an den Port angeschlossen ist.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Konfigurieren der globalen RSTP-Parameter der RCP-Bridges

Aus der Aufgabenstellung in Tabelle 45 benötigen Sie die RSTP-Bridge-Prioritäten für Bridge A und Bridge B. Die folgende Tabelle enthält eine Zusammenfassung dieser Werte.

Tab. 47: RSTP-Bridge-Prioritäten für die Bridges A und B

RSTP-Parameter	A	B
Bridge-Priorität (hex.)	0x0000	0x2000
Bridge-Priorität (dez.)	0	8192

Anmerkung: Die folgende Anleitung beschreibt die Konfiguration der *RCP*-Bridges (A und B) im Detail; die der anderen Bridges (C bis J) lediglich in gekürzter Form.

Konfigurieren Sie Gerät A. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Wählen Sie im Rahmen *Bridge-Konfiguration*, Dropdown-Liste *Priorität* den Wert `0`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`spanning-tree mst priority 0 0`	Die RSTP-Bridge-Priorität der MST-Instanz `0` auf den Wert `0` setzen. Die MST-Instanz `0` ist die globale MST-Instanz bzw. Default-Instanz.

Konfigurieren Sie Gerät B. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Wählen Sie im Rahmen *Bridge-Konfiguration*, Dropdown-Liste *Priorität* den Wert `8192`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`spanning-tree mst priority 0 8192`	Die RSTP-Bridge-Priorität der globalen MST-Instanz `8192` auf den Wert 8192 setzen.

Konfigurieren der globalen RSTP-Parameter für die anderen Bridges

Konfigurieren Sie nun die anderen Bridges. Aus der Aufgabenstellung benötigen Sie die RSTP-Bridge-Prioritäten. Die folgende Tabelle enthält eine Zusammenfassung dieser Werte.

Tab. 48: RSTP-Bridge-Prioritäten für die Bridges C bis J

RSTP-Parameter	C	D	E	F	G	H	I	J
Bridge-Priorität (hex.)	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Bridge-Priorität (dez.)	16384	4096	12288	8192	16384	4096	12288	8192

Führen Sie die folgenden Schritte aus:

- ☐ Setzen Sie die RSTP-Bridge-Priorität des Geräts C auf `16384 (0x4000)` und aktivieren Sie die Einstellung.
- ☐ Setzen Sie die RSTP-Bridge-Priorität des Geräts D auf `4096 (0x1000)` und aktivieren Sie die Einstellung.
- ☐ Setzen Sie die RSTP-Bridge-Priorität des Geräts E auf `12288 (0x3000)` und aktivieren Sie die Einstellung.
- ☐ Setzen Sie die RSTP-Bridge-Priorität des Geräts F auf `8192 (0x2000)` und aktivieren Sie die Einstellung.
- ☐ Setzen Sie die RSTP-Bridge-Priorität des Geräts G auf `16384 (0x4000)` und aktivieren Sie die Einstellung.
- ☐ Setzen Sie die RSTP-Bridge-Priorität des Geräts H auf `4096 (0x1000)` und aktivieren Sie die Einstellung.
- ☐ Setzen Sie die RSTP-Bridge-Priorität des Geräts I auf `12288 (0x3000)` und aktivieren Sie die Einstellung.
- ☐ Setzen Sie die RSTP-Bridge-Priorität des Geräts J auf `8192 (0x2000)` und aktivieren Sie die Einstellung.

Konfigurieren der Dual RSTP-Parameter der RCP-Bridges

Aus der Aufgabenstellung benötigen Sie die spezifischen *Dual RSTP*-Parameter für die Bridges A und B. Dies sind die *Dual RSTP*-Bridge-Prioritäten, die Ring-Ports und die Kopplungs-Rollen. Die folgenden Tabellen enthalten eine Zusammenfassung dieser Werte.

Tab. 49: Dual RSTP-Parameter für die Bridges A und B

Dual RSTP-Parameter	A	B
Dual RSTP-Bridge-Priorität (hex.)	`0x2000`	`0x0000`
Dual RSTP-Bridge-Priorität (dez.)	`8192`	`0`

Tab. 50: RCP-Parameter für die Bridges A und B

Dual RSTP-Parameter	A	B
Primär-Ring, innerer Port	`1/1`	`1/1`
Primär-Ring, äußerer Port	`1/2`	`1/2`
Sekundär-Ring, innerer Port	`1/3`	`1/3`
Sekundär-Ring, äußerer Port	`1/4`	`1/4`
Kopplungs-Rolle	`Slave`	`Master`

Konfigurieren Sie Gerät A. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > FuseNet > RCP*.
- ☐ Wählen Sie im Rahmen *Primärer Ring/Netzwerk*, Dropdown-Liste *Innerer Port* den Wert `1/1`.
- ☐ Wählen Sie im Rahmen *Primärer Ring/Netzwerk*, Dropdown-Liste *Äußerer Port* den Wert `1/2`.
- ☐ Wählen Sie im Rahmen *Sekundärer Ring/Netzwerk*, Dropdown-Liste *Innerer Port* den Wert `1/3`.
- ☐ Wählen Sie im Rahmen *Sekundärer Ring/Netzwerk*, Dropdown-Liste *Äußerer Port* den Wert `1/4`.
- ☐ Wählen Sie im Rahmen *Koppler-Konfiguration*, Dropdown-Liste *Rolle* den Wert *`slave`*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Dual RSTP*.
- ☐ Wählen Sie im Rahmen *Bridge-Konfiguration*, Dropdown-Liste *Priorität* den Wert `8192`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`spanning-tree drstp mst priority 0 8192`	Die RSTP-Bridge-Priorität der *Dual RSTP*-Instanz auf den Wert `8192` setzen.
`redundant-coupling port primary inner 1/1`	Auswählen des Ports *1/1* als inneren Port für den *RCP*-Primär-Ring.
`redundant-coupling port primary outer 1/2`	Auswählen des Ports *1/2* als äußeren Port für den *RCP*-Primär-Ring.
`redundant-coupling port secondary inner 1/3`	Auswählen des Ports *1/3* als inneren Port für den *RCP*-Sekundär-Ring.

`redundant-coupling port secondary outer 1/4`	Auswählen des Ports *1/4* als äußeren Port für den *RCP*-Sekundär-Ring.
`redundant-coupling role slave`	Konfigurieren des Geräts als *RCP*-Slave.
`exit`	Wechsel in den Privileged-EXEC-Modus.

Konfigurieren Sie Gerät B. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > FuseNet > RCP*.
- ☐ Wählen Sie im Rahmen *Primärer Ring/Netzwerk*, Dropdown-Liste *Innerer Port* den Wert `1/1`.
- ☐ Wählen Sie im Rahmen *Primärer Ring/Netzwerk*, Dropdown-Liste *Äußerer Port* den Wert `1/2`.
- ☐ Wählen Sie im Rahmen *Sekundärer Ring/Netzwerk*, Dropdown-Liste *Innerer Port* den Wert `1/3`.
- ☐ Wählen Sie im Rahmen *Sekundärer Ring/Netzwerk*, Dropdown-Liste *Äußerer Port* den Wert `1/4`.
- ☐ Wählen Sie im Rahmen *Koppler-Konfiguration*, Dropdown-Liste *Rolle* den Wert `master`.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Dual RSTP*.
- ☐ Wählen Sie im Rahmen *Bridge-Konfiguration*, Dropdown-Liste *Priorität* den Wert `0`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`spanning-tree drstp mst priority 0 0`	Die RSTP-Bridge-Priorität der *Dual RSTP*-Instanz auf den Wert `0` setzen.
`redundant-coupling port primary inner 1/1`	Auswählen des Ports *1/1* als inneren Port für den *RCP*-Primär-Ring.
`redundant-coupling port primary outer 1/2`	Auswählen des Ports *1/2* als äußeren Port für den *RCP*-Primär-Ring.
`redundant-coupling port secondary inner 1/3`	Auswählen des Ports *1/3* als inneren Port für den *RCP*-Sekundär-Ring.
`redundant-coupling port secondary outer 1/4`	Auswählen des Ports *1/4* als äußeren Port für den *RCP*-Sekundär-Ring.
`redundant-coupling role master`	Konfigurieren des Geräts als *RCP*-Master.
`exit`	Wechsel in den Privileged-EXEC-Modus.

Konfiguration prüfen

Aktivieren Sie die neuen redundanten Verbindungen:

- ▶ Die Verbindung der inneren Ports für den Sekundär-Ring zwischen Gerät A, Port *1/3* und Gerät B, Port *1/3*.
- ▶ Den Ringschluss des Sekundär-Rings zwischen Gerät G und Gerät H.
- ▶ Den Ringschluss des Primär-Rings zwischen Gerät C und Gerät D.

Vergleichen Sie die gegenwärtigen Bridge-Rollen im Primär-Ring mit den gewünschten Bridge-Rollen:

Bridge A sollte die Root-Bridge sein.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Global*.
- ☐ Prüfen Sie im Rahmen *Topologie-Information* die Einstellung des Kontrollkästchens *Bridge ist Root*.

```
show spanning-tree global

Spanning Tree Information:
--------------------------
Spanning Tree Mode.....................RSTP
Spanning Tree Trap Mode.................enabled
Bridge is root..........................true
...
```

Vergleichen Sie die 4 Ports, die Sie als innere und äußere Ports im Primär-Ring und im Sekundär-Ring konfiguriert haben, mit den Angaben in Tabelle 45.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > FuseNet > RCP*.
- ☐ Prüfen Sie die Ports, die in den Rahmen *Primärer Ring/Netzwerk* und *Sekundärer Ring/Netzwerk* angezeigt werden.

```
show redundant-coupling global

Redundant coupling protocol global settings
-------------------------------------------
RCP global state.......................enabled
RCP device configured role..............slave
RCP inner primary interface.............1/1
RCP outer primary interface.............1/2
RCP inner secondary interface...........1/3
RCP outer secondary interface...........1/4
RCP timeout............................45 milliseconds
```

Vergleichen Sie die gegenwärtigen Bridge-Rollen im Sekundär-Ring mit den gewünschten Bridge-Rollen. Bridge B soll die Root-Bridge sein.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Dual RSTP*.
- ☐ Prüfen Sie im Rahmen *Topologie-Information* die Einstellung des Kontrollkästchens *Bridge ist Root*.

```
show spanning-tree drstp

Dual Spanning Tree Information:
-------------------------------
Spanning Tree Mode.........................RSTP
Spanning Tree Trap Mode....................enabled
Bridge is root.............................true
...
```

Vergleichen Sie die gegenwärtigen Port-Rollen der Bridges im Primär-Ring mit den gewünschten Port-Rollen:

- Für die Ports der Bridge D, die zu Bridge C führen:
  Rolle *alternate*
- Für die anderen Ports der Bridges, die in Richtung Root-Bridge A führen:
  Rolle *root*
- Für die anderen Ports der Bridges, die in Richtung Backup-Root-Bridge D führen:
  Rolle *designated*

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Prüfen Sie in Spalte *Port-Rolle* den Wert *alternate*, *root* oder *designated* wie oben beschrieben.

```
show spanning-tree mst port 0 1/<port>
```

Vergleichen Sie die gegenwärtigen Port-Rollen der Bridges im Sekundär-Ring mit den gewünschten Port-Rollen:

- Für die Ports der Bridge H, die zu Bridge G führen:
  Rolle *alternate*
- Für die anderen Ports der Bridges, die in Richtung Root-Bridge B führen:
  Rolle *root*
- Für die anderen Ports der Bridges, die in Richtung Backup-Root-Bridge H führen:
  Rolle *designated*

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*.
- ☐ Prüfen Sie in Spalte *Port-Rolle* den Wert *alternate*, *root* oder *designated* wie oben beschrieben.

```
show spanning-tree mst port 0 1/<port>
```

Wenn die Funktion *RCP* oder die Funktion *Spanning Tree* deaktiviert ist, dann deaktiviert das Gerät automatisch auch die Funktion *Dual RSTP*.

Prüfen Sie den Status der Funktion *Dual RSTP*.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Dual RSTP*.
  Im Rahmen *Funktion* ist das Optionsfeld *Aus* ausgewählt.

```
show redundant-coupling status

Redundant coupling protocol status
------------------------------------------
RCP global state.........................forwarding
RCP device actual role...................disabled
Redundancy state availability............redNotAvailable
Primary ring protocol....................NONE
Secondary ring protocol..................NONE
```

Konfiguration abschließen

Speichern Sie die Einstellungen der Geräte A bis J im permanenten Speicher. Folgen Sie den Anweisungen im Abschnitt „Konfigurationsprofil speichern” auf Seite 101.

14 Funktionsdiagnose

Das Gerät bietet Ihnen folgende Diagnosewerkzeuge:
- SNMP-Traps senden
- Gerätestatus überwachen
- Out-of-Band-Signalisierung durch Signalkontakt
- Port-Zustandsanzeige
- Ereigniszähler auf Portebene
- Erkennen der Nichtübereinstimmung der Duplex-Modi
- Auto-Disable
- SFP-Zustandsanzeige
- Topologie-Erkennung
- IP-Adresskonflikte erkennen
- Erkennen von Loops
- Unterstützung beim Schutz vor Layer-2-Loops
- Berichte
- Datenverkehr eines Ports beobachten (Port Mirroring)
- Syslog
- Ereignisprotokoll
- Ursachen und entsprechende Maßnahmen während des Selbsttests

14.1 SNMP-Traps senden

Das Gerät meldet außergewöhnliche Ereignisse, die während des Normalbetriebs auftreten, sofort an die Netz-Management-Station. Dies geschieht über Nachrichten, sogenannte SNMP-Traps, die das Polling-Verfahren umgehen („Polling“: Abfrage der Datenstationen in regelmäßigen Abständen). SNMP-Traps ermöglichen eine schnelle Reaktion auf außergewöhnliche Ereignisse.

Beispiele für solche Ereignisse sind:
- Hardware-Reset
- Änderungen der Konfiguration
- Segmentierung eines Ports

Das Gerät sendet SNMP-Traps an verschiedene Hosts, um die Übertragungssicherheit für die Nachrichten zu erhöhen. Die nicht quittierte SNMP-Trap-Nachricht besteht aus einem Paket mit Informationen zu einem außergewöhnlichen Ereignis.

Das Gerät sendet SNMP-Traps an jene Hosts, die in der Ziel-Tabelle für SNMP-Traps festgelegt sind. Das Gerät ermöglicht Ihnen, die Trap-Ziel-Tabelle mit der Netz-Management-Station über SNMP zu konfigurieren.

14.1.1 Auflistung der SNMP-Traps

Die folgende Tabelle zeigt mögliche vom Gerät gesendete SNMP-Traps:

Tab. 51: Mögliche SNMP-Traps

Bezeichnung des SNMP-Traps	Bedeutung
authenticationFailure	Wird gesendet, wenn eine Station versucht, unberechtigt auf einen Agenten zuzugreifen.
coldStart	Wird nach einem Neustart gesendet.
sa2DevMonSenseExtNvmRemoval	Wird gesendet, wenn der externe Speicher entfernt worden ist.
linkDown	Wird gesendet, wenn die Verbindung zu einem Port unterbrochen wird.
linkUp	Wird gesendet, wenn die Verbindung zu einem Port hergestellt ist.
sa2DevMonSensePSState	Wird gesendet, wenn sich der Netzteilstatus ändert.
sa2SigConStateChange	Wird gesendet, wenn sich der Zustand des Signalkontaktes bei der Funktionsüberwachung ändert.
newRoot	Wird gesendet, wenn der sendende Agent zur neuen Wurzel des Spannbaums wird.
topologyChange	Wird gesendet, wenn sich der Port-Zustand von blocking auf forwarding oder von forwarding auf blocking ändert.
alarmRisingThreshold	Wird gesendet, wenn der „RMON input“ seinen oberen Schwellwert überschreitet.
alarmFallingThreshold	Wird gesendet, wenn der „RMON input“ seinen unteren Schwellwert unterschreitet.
sa2AgentPortSecurityViolation	Wird gesendet, wenn eine an diesem Port erkannte MAC-Adresse nicht den aktuellen Einstellungen des Parameters sa2AgentPortSecurityEntry entspricht.
sa2DiagSelftestActionTrap	Wird gesendet, wenn ein Selbsttest gemäß der konfigurierten Einstellungen für die vier Kategorien „Aufgabe“, „Ressource“, „Software“ und „Hardware“ durchgeführt wird.
sa2MrpReconfig	Wird gesendet, wenn sich die Konfiguration des MRP-Rings ändert.
sa2DiagIfaceUtilizationTrap	Wird gesendet, wenn der Schwellwert der Schnittstelle den eingestellten oberen oder unteren Grenzwert über- bzw. unterschreitet.
sa2LogAuditStartNextSector	Wird gesendet, wenn der Audittrail einen Sektor vervollständigt hat und einen neuen beginnt.
sa2PtpSynchronizationChance	Wird gesendet, wenn der Status der PTP-Synchronisation geändert wird.
sa2ConfigurationSavedTrap	Wird gesendet, nachdem das Gerät seine Konfiguration erfolgreich lokal gespeichert hat.
sa2ConfigurationChangedTrap	Wird gesendet, wenn Sie die Konfiguration des Geräts nach dem lokalen Speichern erstmalig ändern.
sa2PlatformStpInstanceLoopInconsistentStartTrap	Wird gesendet, wenn der Port in dieser STP-Instanz in den Status „loop inconsistent“ geht.
sa2PlatformStpInstanceLoopInconsistentEndTrap	Wird gesendet, wenn der Port in dieser STP-Instanz bei Empfang eines BPDU-Pakets den Status „loop inconsistent“ verlässt.

14.1.2 SNMP-Traps für Konfigurationsaktivitäten

Nachdem Sie eine Konfiguration im Speicher gespeichert haben, sendet das Gerät einen `sa2ConfigurationSavedTrap`. Dieser SNMP-Trap enthält die Statusvariablen des nichtflüchtigen Speichers (*NVM*) und des externen Speichers (*ENVM*), die angeben, ob die aktuelle Konfiguration mit dem nichtflüchtigen Speicher und dem externen Speicher übereinstimmt. Sie können diesen SNMP-Trap auch auslösen, indem Sie eine Konfigurationsdatei in das Gerät kopieren und die aktive gespeicherte Konfiguration ersetzen.

Bei jeder Änderung der Konfiguration sendet das Gerät einen `sa2ConfigurationChangedTrap`, der angibt, dass die aktuelle und die gespeicherte Konfiguration nicht miteinander übereinstimmen.

14.1.3 SNMP-Trap-Einstellung

Das Gerät ermöglicht Ihnen, als Reaktion auf bestimmte Ereignisse einen SNMP-Trap zu senden. Legen Sie mindestens ein Trap-Ziel fest, das SNMP-Traps empfängt.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)*.
- ☐ Klicken Sie die Schaltfläche  .
  Der Dialog zeigt das Fenster *Erzeugen*.
- ☐ Legen Sie im Rahmen *Name* den Namen fest, den das Gerät verwendet, um sich als Quelle des SNMP-Traps auszuweisen.
- ☐ Legen Sie im Rahmen *Adresse* die IP-Adresse des Trap-Ziels fest, an welches das Gerät die SNMP-Traps sendet.
- ☐ In Spalte *Aktiv* markieren Sie die Einträge, die das Gerät beim Senden von SNMP-Traps berücksichtigt.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

Das Auslösen eines SNMP-Traps legen Sie zum Beispiel in den folgenden Dialogen fest:

- Dialog *Grundeinstellungen > Port*
- Dialog *Grundeinstellungen > Power over Ethernet > Global*
- Dialog *Netzsicherheit > Port-Sicherheit*
- Dialog *Switching > L2-Redundanz > Link-Aggregation*
- Dialog *Diagnose > Statuskonfiguration > Gerätestatus*
- Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*
- Dialog *Diagnose > Statuskonfiguration > Signalkontakt*
- Dialog *Diagnose > Statuskonfiguration > MAC-Benachrichtigung*
- Dialog *Diagnose > System > IP-Adressen Konflikterkennung*
- Dialog *Diagnose > System > Selbsttest*
- Dialog *Diagnose > Ports > Port-Monitor*
- Dialog *Erweitert > Digital-IO Modul*

14.1.4 ICMP-Messaging

Das Gerät ermöglicht Ihnen, das Internet Control Message Protocol (ICMP) für Diagnoseanwendungen zu verwenden, zum Beispiel Ping und Traceroute. Das Gerät verwendet außerdem ICMP für Time-to-Live und das Verwerfen von Nachrichten, in denen das Gerät eine ICMP-Nachricht zurück an das Quellgerät des Paketes weiterleitet.

Verwenden Sie das Ping-Netz-Tool, um den Pfad zu einem bestimmten Host über ein IP-Netz hinweg zu testen. Das Diagnosetool Traceroute zeigt Pfade und Durchgangsverzögerungen von Paketen über ein Netz.

14.2 Gerätestatus überwachen

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

Das Gerät zeigt seinen gegenwärtigen Status als `error` oder `ok` im Rahmen *Geräte-Status*. Das Gerät bestimmt diesen Status anhand der einzelnen Überwachungsergebnisse.

Das Gerät ermöglicht Ihnen:
- über einen Signalkontakt Out-of-Band zu signalisieren
- den geänderten Gerätestatus durch Senden eines SNMP-Traps zu signalisieren
- den Gerätestatus im Dialog *Grundeinstellungen > System* der grafischen Benutzeroberfläche zu ermitteln
- den Gerätestatus im Command Line Interface abzufragen

Die Registerkarte *Global* im Dialog *Diagnose > Statuskonfiguration > Gerätestatus* ermöglicht Ihnen, das Gerät so zu konfigurieren, dass es einen SNMP-Trap an die Netz-Management-Station für die folgenden Ereignisse sendet:
- Inkorrekte Versorgungsspannung
  - mindestens eine der 2 Versorgungsspannungen ist außer Betrieb
  - die interne Versorgungsspannung ist außer Betrieb
- Das Gerät arbeitet außerhalb der benutzerdefinierten Temperaturschwelle.
- Redundanzverlust (im Ring-Manager-Modus)
- Unterbrechung der Link-Verbindung(en)
  Konfigurieren Sie für diese Funktion mindestens einen Port. In der Registerkarte *Port* im Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Zeile *Verbindungsfehler melden* legen Sie fest, für welche Ports das Gerät eine Link-Unterbrechung anzeigt.
- Entfernen des externen Speichers
  Die Konfiguration im externen Speicher stimmt nicht mit der Konfiguration im Gerät überein.

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.

14.2.1 Ereignisse, die überwacht werden können

Tab. 52: Gerätestatus-Ereignisse

Name	Bedeutung
Temperatur	Überwacht, ob die Temperatur den festgelegten Wert über- oder unterschreitet.
Ring-Redundanz	Schalten Sie diese Funktion ein, um das Vorhandensein der Ring-Redundanz zu überwachen.
Verbindungsfehler	Aktivieren Sie diese Funktion, um jedes Ereignis in Bezug auf Port-Links zu überwachen, bei dem das Kontrollkästchen *Verbindungsfehler melden* aktiviert ist.

Tab. 52: Gerätestatus-Ereignisse (Forts

Name	Bedeutung
Externen Speicher entfernen	Aktivieren Sie diese Funktion, um das Vorhandensein eines externen Speichergeräts zu überwachen.
Externer Speicher nicht synchron	Das Gerät überwacht die Synchronisation zwischen der Gerätekonfiguration und der im externen Speicher (*ENVM*) gespeicherten Konfiguration.
Netzteil	Schalten Sie diese Funktion ein, um das Netzteil zu überwachen.

14.2.2 Gerätestatus konfigurieren

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Global*.
- ☐ Markieren Sie für die zu überwachenden Parameter das Kontrollkästchen in Spalte *Überwachen*.
- ☐ Um einen SNMP-Trap an die Management-Station zu senden, aktivieren Sie die Funktion *Trap senden* im Rahmen *Traps*.
- ☐ Legen Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* mindestens ein Trap-Ziel fest, das SNMP-Traps empfängt.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.
- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.
- ☐ Um die Temperatur zu überwachen, legen Sie im unteren Bereich des Rahmens *Systemdaten* die Temperaturschwellen fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`device-status trap`	Senden eines SNMP-Traps, wenn sich der Gerätestatus ändert.
`device-status monitor envm-not-in-sync`	Überwacht die Konfigurationsprofile im Gerät und im externen Speicher. In folgenden Situationen wechselt der *Geräte-Status* auf `error`: • Das Konfigurationsprofil existiert ausschließlich im Gerät. • Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher.
`device-status monitor envm-removal`	Überwacht den aktiven externen Speicher. Der Wert im Rahmen *Geräte-Status* wechselt auf `error`, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen.

`device-status monitor power-supply 1`	Überwacht das Netzteil `1`. Der Wert im Rahmen *Geräte-Status* wechselt auf *`error`*, wenn das Gerät einen Fehler am Netzteil feststellt.
`device-status monitor ring-redundancy`	Überwacht die Ring-Redundanz. In folgenden Situationen wechselt der *Geräte-Status* auf *`error`*: • Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve). • Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen.
`device-status monitor temperature`	Überwacht die Temperatur im Gerät. Der Wert im Rahmen *Geräte-Status* wechselt auf *`error`*, wenn die Temperatur die festgelegten Grenzwerte überschreitet oder unterschreitet.

Um im Gerät die Überwachung von aktiven Links ohne Verbindung einzuschalten, schalten Sie zuerst die globale Funktion und anschließend die einzelnen Ports ein.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Global*.
- ☐ Markieren Sie für den Parameter *Verbindungsfehler* das Kontrollkästchen in Spalte *Überwachen*.
- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Port*.
- ☐ Markieren Sie für den Parameter *Verbindungsfehler melden* das Kontrollkästchen in der Spalte der zu überwachenden Ports.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`device-status monitor link-failure`	Überwacht den Link auf den Ports/Interfaces. Der Wert im Rahmen *Geräte-Status* wechselt auf *`error`*, wenn der Link auf einem überwachten Port/Interface abbricht.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`device-status link-alarm`	Überwacht den Link auf dem Port/Interface. Der Wert im Rahmen *Geräte-Status* wechselt auf *`error`*, wenn der Link auf 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.

14.2.3 Gerätestatus anzeigen

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.

```
show device-status all
```

Im Privileged-EXEC-Modus: Anzeige des Gerätestatus und der Einstellung zur Ermittlung des Gerätestatus

14.3 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

14.3.1 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. 53: Sicherheitsstatus-Ereignisse

Name	Bedeutung
Passwort-Voreinstellung unverändert	Um die Sicherheit zu erhöhen, ändern Sie nach der Installation die Passwörter. Bei aktivierter Funktion zeigt das Gerät einen Alarm an, wenn die voreingestellten Passwörter unverändert bleiben.
Min. Passwort-Länge < 8	Erzeugen Sie Passwörter mit einer Länge von mehr als 8 Zeichen, um ein hohes Maß an Sicherheit zu erhalten. Bei aktivierter Funktion überwacht das Gerät die Einstellung *Min. Passwort-Länge*.
Passwort-Richtlinien deaktiviert	Das Gerät überwacht, ob die Einstellungen im Dialog *Gerätesicherheit > Benutzerverwaltung* die Anforderungen der Passwortrichtlinie erfüllen.
Prüfen der Passwort-Richtlinien im Benutzerkonto deaktiviert	Das Gerät überwacht die Einstellungen des Kontrollkästchens *Richtlinien überprüfen*. Wenn *Richtlinien überprüfen* inaktiv ist, sendet das Gerät einen SNMP-Trap.
Telnet-Server aktiv	Das Gerät überwacht, wann Sie die Funktion *Telnet* einschalten.
HTTP-Server aktiv	Das Gerät überwacht, wann Sie die Funktion *HTTP* einschalten.
SNMP unverschlüsselt	Das Gerät überwacht, wann Sie die Funktion *SNMPv1* oder die Funktion *SNMPv2* einschalten.
Zugriff auf System-Monitor mit serieller Schnittstelle möglich	Das Gerät überwacht den Status des System-Monitors.
Speichern des Konfigurationsprofils auf dem externen Speicher möglich	Das Gerät überwacht die Möglichkeit, Konfigurationen im externen permanenten Speicher zu speichern.
Verbindungsabbruch auf eingeschalteten Ports	Das Gerät überwacht den Link-Status der aktiven Ports.

Tab. 53: Sicherheitsstatus-Ereignisse (Forts

Name	Bedeutung
Zugriff mit Ethernet Switch Configurator möglich	Das Gerät überwacht, wann Sie die Lese-/Schreibfunktion für Ethernet Switch Configurator einschalten.
Unverschlüsselte Konfiguration vom externen Speicher laden	Das Gerät überwacht die Sicherheitseinstellungen für das Laden der Konfiguration aus dem externen Speicher.
IEC61850-MMS aktiv	Das Gerät überwacht, wann Sie das Protokoll IEC 61850-MMS einschalten.
Modbus TCP aktiv	Das Gerät überwacht, wann Sie das Modbus TCP/IP-Protokoll einschalten.
Self-signed HTTPS-Zertifikat vorhanden	Das Gerät überwacht, ob der HTTPS-Server ein selbst erzeugtes digitales Zertifikat verwendet.

14.3.2 Konfigurieren des Sicherheitsstatus

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*.
- ☐ Markieren Sie für die zu überwachenden Parameter das Kontrollkästchen in Spalte *Überwachen*.
- ☐ Um einen SNMP-Trap an die Management-Station zu senden, aktivieren Sie die Funktion *Trap senden* im Rahmen *Traps*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Legen Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* mindestens ein Trap-Ziel fest, das SNMP-Traps empfängt.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`security-status monitor pwd-change`	Überwacht das Passwort für die lokal eingerichteten Benutzerkonten `user` und `admin`. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie für die Benutzerkonten `user` oder `admin` das voreingestellte Passwort unverändert verwenden.
`security-status monitor pwd-min-length`	Überwacht den in Richtlinie *Min. Passwort-Länge* festgelegten Wert. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `8`, wenn für die Richtlinie *Min. Passwort-Länge* ein Wert kleiner als `error` festgelegt ist.
`security-status monitor pwd-policy-config`	Überwacht die Passwort-Richtlinien-Einstellungen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn für mindestens eine der folgenden Richtlinien der Wert `0` festgelegt ist. • *Großbuchstaben (min.)* • *Kleinbuchstaben (min.)* • *Ziffern (min.)* • *Sonderzeichen (min.)*

`security-status monitor pwd-policy-inactive`	Überwacht die Passwort-Richtlinien-Einstellungen. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn für mindestens eine der folgenden Richtlinien der Wert `0` festgelegt ist.
`security-status monitor telnet-enabled`	Überwacht den Telnet-Server. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie den Telnet-Server einschalten.
`security-status monitor http-enabled`	Überwacht den HTTP-Server. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie den HTTP-Server einschalten.
`security-status monitor snmp-unsecure`	Überwacht den SNMP-Server. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn mindestens eine der folgenden Bedingungen zutrifft: • Die Funktion *SNMPv1* ist eingeschaltet. • Die Funktion *SNMPv2* ist eingeschaltet. • Die Verschlüsselung für SNMPv3 ist ausgeschaltet. Die Verschlüsselung schalten Sie ein im Dialog *Gerätesicherheit > Benutzerverwaltung*, Feld *SNMP-Verschlüsselung*.
`security-status monitor sysmon-enabled`	Überwachen der Aktivierung der System Monitor-Funktion in dem Gerät.
`security-status monitor extnvm-upd-enabled`	Überwachen der Aktivierung der Aktualisierung des externen nichtflüchtigen Speichers.
`security-status monitor iec61850-mms-enabled`	Überwacht die Funktion *IEC61850-MMS*. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn Sie die Funktion *IEC61850-MMS* einschalten.
`security-status trap`	Senden eines SNMP-Traps, wenn sich der Gerätestatus ändert.

Um im Gerät die Überwachung von aktiven Links ohne Verbindung einzuschalten, schalten Sie zuerst die globale Funktion und anschließend die einzelnen Ports ein.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*.
- ☐ Markieren Sie für den Parameter *Verbindungsabbruch auf eingeschalteten Ports* das Kontrollkästchen in Spalte *Überwachen*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.
- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Gerätestatus*, Registerkarte *Port*.
- ☐ Markieren Sie für den Parameter *Verbindungsabbruch auf eingeschalteten Ports* das Kontrollkästchen in der Spalte der zu überwachenden Ports.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`security-status monitor no-link-enabled`	Überwacht den Link auf aktiven Ports. Der Wert im Rahmen *Sicherheits-Status* wechselt auf `error`, wenn der Link auf einem aktiven Port abbricht.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`security-status monitor no-link`	Überwacht den Link auf Interface/Port `1`.

14.3.3 Anzeigen des Sicherheitsstatus

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.

`show security-status all`	Zeigt im EXEC-Privilege-Modus Sicherheitsstatus und die Einstellung zur Ermittlung des Gerätestatus.

14.4 Out-of-Band-Signalisierung

Das Gerät verwendet den Signalkontakt zur Steuerung von externen Geräten und zur Überwachung der Gerätefunktionen. Die Funktionsüberwachung ermöglicht die Durchführung einer Ferndiagnose.

Das Gerät meldet den Funktionsstatus über eine Unterbrechung des potentialfreien Signalkontaktes (Relaiskontakt, Ruhestromschaltung) für den gewählten Modus. Das Gerät überwacht folgende Funktionen:

- Inkorrekte Versorgungsspannung
  - mindestens eine der 2 Versorgungsspannungen ist außer Betrieb
  - die interne Versorgungsspannung ist außer Betrieb
- Das Gerät arbeitet außerhalb der benutzerdefinierten Temperaturschwelle.
- Ereignisse der Ring-Redundanz
  Redundanzverlust (im Ring-Manager-Modus)
  In der Voreinstellung ist die Ring-Redundanz-Überwachung inaktiv. Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in der lokalen Konfiguration.
- Unterbrechung der Link-Verbindung(en)
  Konfigurieren Sie für diese Funktion mindestens einen Port. Im Rahmen *Verbindungsfehler melden* legen Sie fest, welche Ports das Gerät bei fehlendem Link meldet. In der Voreinstellung ist die Link-Überwachung inaktiv.
- Entfernen des externen Speichers
  Die Konfiguration im externen Speicher stimmt nicht mit der Konfiguration im Gerät überein.

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.

14.4.1 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*, Drop-down-Liste *Modus* den Eintrag `Manuelle Einstellung`.
- ☐ Um den Signalkontakt zu öffnen, wählen Sie im Rahmen *Konfiguration* das Optionsfeld `offen`.
- ☐ Um den Signalkontakt zu schließen, wählen Sie im Rahmen *Konfiguration* das Optionsfeld `geschlossen`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`signal-contact 1 mode manual`	Auswählen des manuellen Einstellungsmodus für Signalkontakt `1`.
`signal-contact 1 state open`	Öffnen des Signalkontaktes `1`.
`signal-contact 1 state closed`	Schließen des Signalkontaktes `1`.

14.4.2 Gerätestatus und Sicherheitsstatus überwachen

Im Rahmen *Konfiguration* legen Sie fest, welche Ereignisse der Signalkontakt signalisiert:

- *`Geräte-Status`*
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog *Diagnose* > Statuskonfiguration > *Gerätestatus* überwachten Parameter.
- *`Sicherheits-Status`*
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog *Diagnose* > Statuskonfiguration > *Sicherheitsstatus* überwachten Parameter.
- *`Geräte-/Sicherheits-Status`*
  Mit dieser Einstellung signalisiert der Signalkontakt den Zustand der im Dialog *Diagnose* > Statuskonfiguration > *Gerätestatus* und im Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus* überwachten Parameter.

Funktionsüberwachung konfigurieren

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Signalkontakt*, Registerkarte *Global*.
- ☐ Um mit dem Signalkontakt die Gerätefunktionen zu überwachen, legen Sie im Rahmen *Konfiguration*, Feld *Modus* den Wert *`Funktionsüberwachung`* fest.
- ☐ Markieren Sie für die zu überwachenden Parameter das Kontrollkästchen in Spalte *Überwachen*.
- ☐ Um einen SNMP-Trap an die Management-Station zu senden, aktivieren Sie die Funktion *Trap senden* im Rahmen *Traps*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Legen Sie im Dialog *Diagnose > Statuskonfiguration > Alarme (Traps)* mindestens ein Trap-Ziel fest, das SNMP-Traps empfängt.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Die Temperaturschwellen für die Temperaturüberwachung legen Sie im Dialog *Grundeinstellungen > System* fest.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`signal-contact 1 monitor temperature`	Überwacht die Temperatur im Gerät. Der Signalkontakt öffnet, wenn die Temperatur die Temperaturschwellen überschreitet oder unterschreitet.

`signal-contact 1 monitor ring-redundancy`	Überwacht die Ring-Redundanz. In folgenden Situationen öffnet der Signalkontakt: • Die Redundanz-Funktion schaltet sich ein (Wegfall der Redundanz-Reserve). • Das Gerät ist normaler Ring-Teilnehmer und erkennt Fehler in seinen Einstellungen.
`signal-contact 1 monitor link-failure`	Überwacht den Link auf den Ports/Interfaces. Der Signalkontakt öffnet, wenn der Link auf einem überwachten Port/Interface abbricht.
`signal-contact 1 monitor envm-removal`	Überwacht den aktiven externen Speicher. Der Signalkontakt öffnet, wenn Sie den aktiven externen Speicher aus dem Gerät entfernen.
`signal-contact 1 monitor envm-not-in-sync`	Überwacht die Konfigurationsprofile im Gerät und im externen Speicher. In folgenden Situationen öffnet der Signalkontakt: • Das Konfigurationsprofil existiert ausschließlich im Gerät. • Das Konfigurationsprofil im Gerät unterscheidet sich vom Konfigurationsprofil im externen Speicher.
`signal-contact 1 monitor power-supply 1`	Überwacht das Netzteil `1`. Der Signalkontakt öffnet, wenn das Gerät einen Fehler an diesem Netzteil feststellt.
`signal-contact 1 monitor module-removal 1`	Überwacht das Modul `1`. Der Signalkontakt öffnet, wenn Sie Modul `1` aus dem Gerät entfernen.
`signal-contact 1 trap`	Freigabe des Geräts zum Senden eines SNMP-Traps bei Änderung des Status der Funktionsüberwachung.
`no signal-contact 1 trap`	Deaktivieren des SNMP-Traps

Um im Gerät die Überwachung von aktiven Links ohne Verbindung einzuschalten, schalten Sie zuerst die globale Funktion und anschließend die einzelnen Ports ein.

Führen Sie die folgenden Schritte aus:

- ☐ Aktivieren Sie in Spalte *Überwachen* die Funktion *Verbindungsabbruch auf eingeschalteten Ports*.
- ☐ Öffnen Sie den Dialog *Diagnose* > *Statuskonfiguration* > *Gerätestatus*, Registerkarte *Port*.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`signal-contact 1 monitor link-failure`	Überwacht den Link auf den Ports/Interfaces. Der Signalkontakt öffnet, wenn der Link auf einem überwachten Port/Interface abbricht.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`signal-contact 1 link-alarm`	Überwacht den Link auf dem Port/Interface. Der Signalkontakt öffnet, wenn der Link auf einem Port/Interface abbricht.

Ereignisse, die überwacht werden können

Tab. 54: Gerätestatus-Ereignisse

Name	Bedeutung
Temperatur	Wenn die Temperatur den festgelegten Wert über- oder unterschreitet.
Ring-Redundanz	Schalten Sie diese Funktion ein, um das Vorhandensein der Ring-Redundanz zu überwachen.
Verbindungsfehler	Aktivieren Sie diese Funktion, um jedes Ereignis in Bezug auf Port-Links zu überwachen, bei dem das Kontrollkästchen *Verbindungsfehler melden* aktiviert ist.
Externer Speicher und NVM nicht synchron	Das Gerät überwacht die Synchronisation zwischen der Gerätekonfiguration und der im externen Speicher (*ENVM*) gespeicherten Konfiguration.
Externer Speicher wurde entfernt	Aktivieren Sie diese Funktion, um das Vorhandensein eines externen Speichergeräts zu überwachen.
Netzteil	Schalten Sie diese Funktion ein, um das Netzteil zu überwachen.

Signalkontakt-Anzeige

Das Gerät bietet Ihnen weitere Möglichkeiten, den Zustand des Signalkontaktes darzustellen:
- Anzeige in der grafische Benutzeroberfläche
- Abfrage im Command Line Interface

Führen Sie die folgenden Schritte aus:

☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.
Der Rahmen *Status Signalkontakt* zeigt den Signalkontaktstatus und informiert über aufgetretene Alarme. Der Rahmen ist hervorgehoben, wenn gegenwärtig ein Alarm vorhanden ist.

`show signal-contact 1 all`	Anzeige der Einstellungen für den angegebenen Signalkontakt

14.5 Port-Zustandsanzeige

Um den Zustand der Ports anzuzeigen, führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Grundeinstellungen > System*.

Der Dialog zeigt das Gerät mit der aktuellen Konfiguration. Darüber hinaus zeigt der Dialog den Status der einzelnen Ports mittels eines Symbols.

Die folgenden Symbole stellen den Zustand der einzelnen Ports dar. In manchen Situationen überlagern sich diese Symbole. Wenn Sie den Mauszeiger über dem Portsymbol positionieren, zeigt eine Sprechblase eine detaillierte Beschreibung des Portzustandes.

Tab. 55: Symbole zur Kennzeichnung des Zustands der Ports

Kriterium	Symbol
Bandbreite des Ports	10 Mbit/s Port aktiviert, Verbindung in Ordnung, Vollduplexbetrieb 100 Mbit/s Port aktiviert, Verbindung in Ordnung, Vollduplexbetrieb 1000 Mbit/s Port aktiviert, Verbindung in Ordnung, Vollduplexbetrieb
Betriebszustände	Halbduplexbetrieb eingeschaltet Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen *Automatische Konfiguration*, Feld *Manuelle Konfiguration* und Feld *Manuelles Cable-Crossing (Auto. Konfig. aus)*. Autonegotiation eingeschaltet Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen *Automatische Konfiguration*. Port ist durch eine Redundanz-Funktion blockiert.
AdminLink	Port ist deaktiviert, Verbindung in Ordnung Port ist deaktiviert, keine Verbindung aufgebaut Siehe Dialog *Grundeinstellungen > Port*, Registerkarte *Konfiguration*, Kontrollkästchen *Port an* und Feld *Link/ Aktuelle Betriebsart*.

14.6 Portereignis-Zähler

Die Port-Statistiktabelle ermöglicht erfahrenen Netzadministratoren, möglicherweise erkannte Schwachpunkte im Netz zu identifizieren.

Diese Tabelle zeigt die Inhalte verschiedener Ereigniszähler. Die Paketzähler summieren die Ereignisse aus Sende- und Empfangsrichtung. Im Dialog *Grundeinstellungen > Neustart* können Sie die Ereigniszähler zurücksetzen.

Tab. 56: Beispiele für die Angabe bekannter Schwächen

Zähler	Angabe bekannter möglicher Schwächen
Empfangene Fragmente	• Nicht funktionierender Controller des verbundenen Geräts • Elektromagnetische Einkoppelung im Übertragungsmedium
CRC-Fehler	• Nicht funktionierender Controller des verbundenen Geräts • Elektromagnetische Einkoppelung im Übertragungsmedium • Nicht betriebsbereite Komponente im Netz
Kollisionen	• Nicht funktionierender Controller des verbundenen Geräts • Netzausdehnung zu groß/Zeilen zu lang • Kollision oder Fehler beim Datenpaket ermittelt

Führen Sie die folgenden Schritte aus:

- ☐ Um die Ereigniszähler anzuzeigen, öffnen Sie den Dialog *Grundeinstellungen > Port*, Registerkarte *Statistiken*.
- ☐ Um die Zähler zurückzusetzen, klicken Sie im Dialog *Grundeinstellungen > Neustart* die Schaltfläche *Port-Statistiken leeren*.

14.6.1 Erkennen der Nichtübereinstimmung der Duplex-Modi

Weisen 2 direkt miteinander verbundene Ports nicht übereinstimmende Modi auf, treten Probleme auf. Die Nachverfolgung dieser Probleme ist schwierig. Das automatische Erkennen und Melden dieser Situation hat den Vorteil, dass nicht übereinstimmende Duplex-Modi erkannt werden, bevor Probleme auftreten.

Diese Situation wird durch eine fehlerhafte Konfiguration verursacht, zum Beispiel wenn Sie die automatische Konfiguration am Remote-Port deaktivieren.

Ein typischer Effekt dieser Nichtübereinstimmung ist, dass die Verbindung bei niedriger Datenrate zu funktionieren scheint, das lokale Gerät bei höherem bidirektionalem Verkehrsaufkommen jedoch viele CRC-Fehler 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 in Abhängigkeit von den Port-Einstellungen.

Möglichen Ursachen für Port-Fehlerereignisse

Die folgende Tabelle nennt die Duplex-Betriebsarten für TX-Ports zusammen mit den möglichen Fehlerereignissen. Die Begriffe in der Tabelle bedeuten:

- Kollisionen
  Im Halbduplexmodus bedeuten Kollisionen Normalbetrieb.
- Duplex-Problem
  Nicht übereinstimmende Duplex-Modi.
- EMI
  Elektromagnetische Interferenz.
- Netzausdehnung
  Die Netzausdehnung ist zu groß bzw. sind zu viele Kaskadenhubs vorhanden.
- Kollisionen, Late Collisions
  Im Vollduplex-Modus keine Erhöhung der Port-Zähler für Kollisionen oder Late Collisions.
- CRC-Fehler
  Das Gerät bewertet diese erkannten Fehler als nicht übereinstimmende Duplex-Modi im manuellen Vollduplex-Modus.

Tab. 57: Bewertung des nicht übereinstimmenden Duplex-Modus

Nr.	Automatische Konfiguration	Aktueller Duplex-Modus	Erkannte Fehlerereignisse (≥ 10 nach Link-Up)	Duplex-Modi	Mögliche Ursachen
1	markiert	Halbduplex	Keine	OK	
2	markiert	Halbduplex	Kollisionen	OK	
3	markiert	Halbduplex	Late Collisions	Duplex-Problem erkannt	Duplex-Problem, EMI, Netzausdehnung
4	markiert	Halbduplex	CRC-Fehler	OK	EMI
5	markiert	Vollduplex	Keine	OK	
6	markiert	Vollduplex	Kollisionen	OK	EMI
7	markiert	Vollduplex	Late Collisions	OK	EMI
8	markiert	Vollduplex	CRC-Fehler	OK	EMI
9	unmarkiert	Halbduplex	Keine	OK	
10	unmarkiert	Halbduplex	Kollisionen	OK	
11	unmarkiert	Halbduplex	Late Collisions	Duplex-Problem erkannt	Duplex-Problem, EMI, Netzausdehnung
12	unmarkiert	Halbduplex	CRC-Fehler	OK	EMI
13	unmarkiert	Vollduplex	Keine	OK	
14	unmarkiert	Vollduplex	Kollisionen	OK	EMI
15	unmarkiert	Vollduplex	Late Collisions	OK	EMI
16	unmarkiert	Vollduplex	CRC-Fehler	Duplex-Problem erkannt	Duplex-Problem, EMI

14.7 Auto-Disable

Unterschiedliche konfigurationsbedingte Ursachen können bewirken, dass das Gerät einen Port ausschaltet. Jede Ursache führt zur Software-seitigen Abschaltung des Ports. Um die Software-seitige Abschaltung des Ports aufzuheben, können Sie den verursachenden Zustand manuell beseitigen oder einen Timer festlegen, der den Port automatisch wieder einschaltet.

Wenn die Konfiguration einen Port als eingeschaltet zeigt, das Gerät jedoch einen Fehler oder eine Zustandsänderung erkennt, schaltet die Software den betreffenden Port ab. Anders gesagt: Die Geräte-Software schaltet den Port aufgrund eines erkannten Fehlers oder einer erkannten Zustandsänderung aus.

Bei der Auto-Deaktivierung eines Ports schaltet das Gerät den betreffenden Port ab; der Port blockiert den Datenverkehr. Die Port-LED blinkt pro Phase dreimal grün und identifiziert den Grund für das Abschalten. Darüber hinaus erzeugt das Gerät einen Protokolleintrag, der den Grund für die Selbstabschaltung aufführt. Wenn Sie den Port nach einem Timeout mit der Funktion *Auto-Disable* wieder einschalten, erzeugt das Gerät einen Protokolleintrag.

Die Funktion *Auto-Disable* stellt eine Wiederherstellungsfunktion bereit, die einen per Selbstabschaltung deaktivierten Port nach einem benutzerdefinierten Zeitraum automatisch wieder aktiviert. Wenn diese Funktion einen Port aktiviert, sendet das Gerät einen SNMP-Trap mit der Port-Nummer, jedoch ohne einen Wert für den Parameter *Grund*.

Die Funktion *Auto-Disable* hat die folgenden Aufgaben:
- Sie unterstützt den Netzadministrator bei der Port-Analyse.
- Dies verringert die Wahrscheinlichkeit, dass der betreffende Port ein instabiles Netz verursacht.

Die Funktion *Auto-Disable* steht für folgende Funktionen zur Verfügung:
- *Link-Änderungen* (Funktion *Port-Monitor*)
- *CRC/Fragmente* (Funktion *Port-Monitor*)
- Duplex Mismatch-Erkennung (Funktion *Port-Monitor*)
- *DHCP-Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port-Sicherheit*
- *Überlast-Erkennung* (Funktion *Port-Monitor*)
- *Link-Speed-/Duplex-Mode-Erkennung* (Funktion *Port-Monitor*)

Im folgenden Beispiel konfigurieren Sie das Gerät so, dass es einen Port deaktiviert und anschließend automatisch reaktiviert, wenn es eine Überschreitung der im *Diagnose > Ports > Port-Monitor*, Registerkarte *CRC/Fragmente* festgelegten Grenzwerte feststellt.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *CRC/Fragmente*.
- ☐ Vergewissern Sie sich, dass die in der Tabelle angegebenen Grenzwerte mit Ihren Einstellungen für Port `1/1` übereinstimmen.
- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Um dem Gerät zu ermöglichen, den Port aufgrund erkannter Fehler auszuschalten, markieren Sie das Kontrollkästchen in Spalte *CRC/Fragmente an* für Port `1/1`.

- In Spalte *Aktion* können Sie festlegen, wie das Gerät auf erkannte Fehler reagiert. In diesem Beispiel schaltet das Gerät Port `1/1` aufgrund von Grenzwertüberschreitungen aus und schaltet den Port anschließend wieder ein.
  - Um dem Gerät zu ermöglichen, den Port auszuschalten und anschließend automatisch wieder einzuschalten, wählen Sie den Wert `auto-disable` und konfigurieren die Funktion *Auto-Disable*. Der Wert `auto-disable` funktioniert ausschließlich mit der Funktion *Auto-Disable*.

  Das Gerät ist außerdem in der Lage, einen Port auszuschalten, ohne ihn automatisch wieder einzuschalten.
  - Um dem Gerät zu ermöglichen, den Port ausschließlich auszuschalten, wählen Sie den Wert `disable port`.

    Um einen ausgeschalteten Port manuell wieder einzuschalten, markieren Sie den Port.

    Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Zurücksetzen*.
  - Wenn Sie die Funktion *Auto-Disable* konfigurieren, schaltet der Wert `disable port` den Port ebenfalls automatisch wieder ein.
- Öffnen Sie den Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Auto-Disable*.
- Um dem Gerät zu ermöglichen, den Port nach einem Ausschalten wegen erkannter Grenzwertüberschreitungen automatisch wieder einzuschalten, markieren Sie das Kontrollkästchen in Spalte *CRC-/Fragment-Fehler*.
- Öffnen Sie den Dialog *Diagnose > Ports > Port-Monitor*, Registerkarte *Port*.
- Legen Sie in Spalte *Reset-Timer [s]* eine Verzögerungszeit von 120 s für die zu aktivierenden Ports fest.

Anmerkung: Der Eintrag *Zurücksetzen* ermöglicht Ihnen, den Port zu aktivieren, bevor die in Spalte *Reset-Timer [s]* festgelegte Zeit abgelaufen ist.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`port-monitor condition crc-fragments count 2000`	CRC-Fragment-Zähler auf 2000 Teile pro Million festlegen.
`port-monitor condition crc-fragments interval 15`	Setzt das Messintervall für die CRC-Fragment-Erkennung auf 15 Sekunden.
`auto-disable timer 120`	Legt eine Wartezeit von `120` Sekunden fest, nach der die Funktion *Auto-Disable* den Port wieder einschaltet.
`exit`	Wechsel in den Konfigurationsmodus.
`auto-disable reason crc-error`	Aktivieren Sie die Selbstabschaltfunktion für CRC.
`port-monitor condition crc-fragments mode`	Um eine Aktion auszulösen, aktivieren Sie die CRC-Fragment-Bedingung.
`port-monitor operation`	Aktivieren Sie die Funktion *Port-Monitor*.

Wenn das Gerät einen Port wegen Grenzwertüberschreitungen ausschaltet, ermöglicht Ihnen das Gerät, den ausgeschalteten Port mit den folgenden Kommandos manuell zurückzusetzen.

Führen Sie die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.

```
configure
```

Wechsel in den Konfigurationsmodus.

```
interface 1/1
```

Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.

```
auto-disable reset
```

ermöglicht Ihnen, den Port einzuschalten, bevor der Timer zu zählen beginnt.

14.8 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*.

14.9 Topologie-Erkennung

IEEE 802.1AB beschreibt das Link Layer Discovery Protocol (LLDP). Das LLDP ermöglicht Ihnen die automatische Topologie-Erkennung im lokalen Netz.

Geräte mit aktivem LLDP:
- senden ihre Verbindungs- und Verwaltungsdaten an die angrenzenden Geräte des gemeinsamen LANs. Die Bewertung der Geräte erfolgt, wenn die Funktion *LLDP* beim empfangenden Gerät aktiviert ist.
- empfangen eigene Verbindungs- und Management-Informationen von angrenzenden Geräten des gemeinsamen LANs, sofern diese auch das LLDP aktiviert haben.
- bauen eine Datenbank mit Verwaltungsdaten und Objektdefinitionen auf, um Informationen zu benachbarten Geräten mit aktivem LLDP zu speichern.

Als zentrales Element enthält die Verbindungsinformation die genaue, eindeutige Kennzeichnung des Verbindungsendpunktes: MAC (Dienstzugangspunkt). Diese setzt sich zusammen aus einer netzweit eindeutigen Gerätekennung und einer für dieses Gerät eindeutigen Port-Kennung.
- Chassis-Kennung (dessen MAC-Adresse)
- Port-Kennung (dessen Port-MAC-Adresse)
- Beschreibung des Ports
- Systemname
- Systembeschreibung
- Unterstützte Systemfunktionen
- Gegenwärtig aktive Systemfunktionen
- Interface-ID der Management-Adresse
- VLAN-ID des Ports
- Status der Autonegotiation auf dem Port
- Einstellung für Medium-/Halb- und Voll-Duplex sowie für die Port-Geschwindigkeit
- Information über die im Gerät installierten VLANs (VLAN-Kennung und VLAN-Namen; unabhängig davon, ob der Port VLAN-Mitglied ist).

Diese Informationen kann eine Netz-Management-Station von Geräten mit aktivem LLDP abrufen. Mit diesen Informationen ist die Netz-Management-Station in der Lage, die Topologie des Netzes darzustellen.

Nicht-LLDP-Geräte blockieren in der Regel die spezielle Multicast-LLDP-IEEE-MAC-Adresse, die zum Informationsaustausch verwendet wird. Nicht-LLDP-Geräte verwerfen aus diesem Grund LLDP-Pakete. Wird ein nicht-LLDP-fähiges Gerät zwischen 2 LLDP-fähigen Geräten positioniert, lässt das nicht-LLDP-fähige Gerät den Informationsaustausch zwischen 2 LLDP-fähigen Geräten nicht zu.

Die Management Information Base (MIB) für ein LLDP-fähiges Gerät enthält die LLDP-Informationen in der LLDP-MIB und in der privaten SA2-LLDP-EXT-HM-MIB und SA2-LLDP-MIB.

14.9.1 Anzeige der Topologie-Erkennung

Zeigen Sie die Topologie des Netzes an. Führen Sie dazu den folgenden Schritt aus:

- ☐ Öffnen Sie den Dialog *Diagnose > LLDP > Topologie-Erkennung*, Registerkarte *LLDP*.

Wenn Sie an einen Port mehrere Geräte anschließen (zum Beispiel über einen Hub), zeigt die Tabelle für jedes angeschlossenes Gerät je eine Zeile.

Das Aktivieren der Einstellung „FDB Einträge anzeigen“ am unteren Ende der Tabelle ermöglicht Ihnen, Geräte ohne aktive LLDP-Unterstützung in der Tabelle anzuzeigen. Das Gerät nimmt in diesem Fall auch Informationen aus seiner FDB (Forwarding Database) auf.

Wenn Sie den Port mit Geräten mit einer aktiven Topologie-Erkennungsfunktion verbinden, tauschen die Geräte LLDP Data Units (LLDPDU) aus, und die Topologie-Tabelle zeigt diese benachbarten Geräte.

Sind an einen Port ausschließlich Geräte ohne aktive Topologie-Erkennung angeschlossen, enthält die Tabelle eine Zeile für diesen Port, um die angeschlossenen Geräte darzustellen. Diese Zeile enthält die Anzahl der angeschlossenen Geräte.

Die FDB-Adresstabelle enthält MAC-Adressen von Geräten, die die Topologie-Tabelle aus Gründen der Übersicht ausblendet.

14.9.2 LLDP-MED

Bei „LLDP for Media Endpoint Devices“ (LLDP-MED) handelt es sich um eine Erweiterung von LLDP, die zwischen Endpunktgeräten arbeitet. Endpunkte umfassen Geräte wie IP-Telefone oder andere Voice-over-IP-Geräte (VoIP-Geräte) oder Server und Geräte im Netz, zum Beispiel Switches. Sie bietet insbesondere Unterstützung für VoIP-Anwendungen. LLDP-MED stellt diese Unterstützung mithilfe eines zusätzlichen Satzes gebräuchlicher Mitteilungen (d. h. Nachrichten des Typs „Type Length Value“, TLV) für die Ermittlung von Funktionsmerkmalen wie Netz-Richtlinien, PoE (Power over Ethernet), Bestandsverwaltung und Standortdaten bereit.

Das Gerät unterstützt folgende TLV-Meldungen:
- Funktions-TLV
  Ermöglicht den LLDP-MED-Endpunkten, zu ermitteln, welche Funktionen das angeschlossene Gerät unterstützt und welche Funktionen im Gerät aktiviert sind.
- TLV – Netzrichtlinien
  Ermöglicht beiden Netzanschlussgeräten und Endpunkten, VLAN-Konfigurationen und verbundene Attribute für die spezifische Anwendung an dem Port anzubieten. Das Gerät übermittelt einem Telefon die VLAN-Nummer. Das Telefon stellt eine Verbindung zu einem Switch her, fragt seine VLAN-Nummer ab und startet die Kommunikation mit der Anrufsteuerung.

LLPD-MED stellt die folgenden Funktionen bereit:
- Ermittlung der Netz-Richtlinien, einschließlich VLAN ID, Priorität 802.1p und „Differentiated Service Code Point“ (DSCP).
- Gerätestandort- und Topologie-Erkennung auf der Basis von MAC-/Port-Informationen auf LAN-Ebene.
- Benachrichtigung zur Erkennung einer Endpunktverschiebung, vom Netzanschlussgerät an die zugehörige VoIP-Verwaltungsanwendung.
- Erweiterte Identifizierung von Geräten für die Bestandsverwaltung
- Identifizierung von Netzanschlussfunktionen eines Endpunktes, zum Beispiel Multiport-IP-Telefon mit integriertem Switch oder Brückenfunktion.
- Interaktionen auf Anwendungsebene mit LLDP-Protokollelementen für die zeitnahe Inbetriebnahme des LLDP zur Unterstützung der schnellen Verfügbarkeit eines Notdienstes.
- Anwendbarkeit von LLPD-MED für Wireless-LAN-Umgebungen, Unterstützung für Voice over Wireless LAN.

14.10 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.

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät des Rings individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte der Ring-Konfiguration abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Eine Fehlkonfiguration kann einen Loop verursachen, zum Beispiel wenn Sie Spanning Tree deaktivieren.

Das Gerät ermöglicht Ihnen, die Effekte zu erkennen, die Loops typischerweise bewirken, und diese Situation automatisch an die Netz-Management-Station zu melden. Dabei haben Sie die Möglichkeit, einzustellen, ab welchem Ausmaß der Loop-Effekte das Gerät eine Meldung verschickt.

BPDU-Rahmen, die vom ausgewählten Port aus gesendet wurden und innerhalb kurzer Zeit entweder an einem anderen Port desselben Geräts oder an demselben Port empfangen werden, sind ein typischer Effekt eines Loops.

Um zu prüfen, ob das Gerät einen Loop detektiert hat, führen Sie die folgenden Schritte aus;

- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *CIST*.
- ☐ Prüfen Sie den Wert in den Feldern *Port-Zustand* und *Port-Rolle*. Wenn das Feld *Port-Zustand* den Wert `discarding` und das Feld *Port-Rolle* den Wert `backup` zeigt, befindet sich der Port in einem Loop-Zustand.
  oder
- ☐ Öffnen Sie den Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Registerkarte *Guards*.
- ☐ Prüfen Sie den Wert in Spalte *Loop-Zustand*. Wenn das Feld den Wert `true` zeigt, befindet sich der Port in einem Loop-Zustand.

14.11 Unterstützung beim Schutz vor Layer-2-Loops

Das Gerät unterstützt beim Schutz vor Layer-2-Loops.

Ein Loop im Netz kann zu einem Stillstand des Netzes aufgrund von Überlastung führen. Eine mögliche Ursache ist das ständige Duplizieren von Datenpaketen aufgrund einer Fehlkonfiguration. Die Ursache kann zum Beispiel ein unsachgemäß angeschlossenes Kabel oder eine inkorrekte Einstellung im Gerät sein.

Ein Layer-2-Loop im Netz entsteht zum Beispiel in den folgenden Fällen, wenn keine Redundanzprotokolle aktiv sind:
- Zwei Ports desselben Geräts sind direkt miteinander verbunden.
- Zwischen zwei Geräten ist mehr als eine aktive Verbindung eingerichtet.

⚠ WARNUNG

UNBEABSICHTIGTER GERÄTEVORGANG

Um Loops während der Konfigurationsphase zu vermeiden, konfigurieren Sie jedes Gerät des Layer-2-Netzes individuell. Warten Sie mit dem Anschließen der redundanten Strecken, bis Sie die Konfiguration der anderen Geräte des Layer-2-Netzes abgeschlossen haben.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

14.11.1 Anwendungsbeispiel

Die Abbildung zeigt Beispiele für mögliche Layer-2-Loops in einem Netz. In jedem Gerät ist die Funktion *Loop-Schutz* eingeschaltet.

▶ **A**: *Aktiver Modus*
Ports, die zum Anschluss von Endgeräten vorgesehen sind, arbeiten im Modus *aktiv*. Das Gerät sendet auf diesen Ports *Loop-Detection*-Pakete und wertet diese aus.

- **P**: *Passiver Modus*
  Ports, die zu den redundanten Ringen gehören, arbeiten im Modus *passiv*. Das Gerät wertet *Loop-Detection*-Pakete auf diesen Ports nur aus.
- **Loop 1**..**Loop 4**
  Unbeabsichtigt eingerichtete Layer-2-Loops.

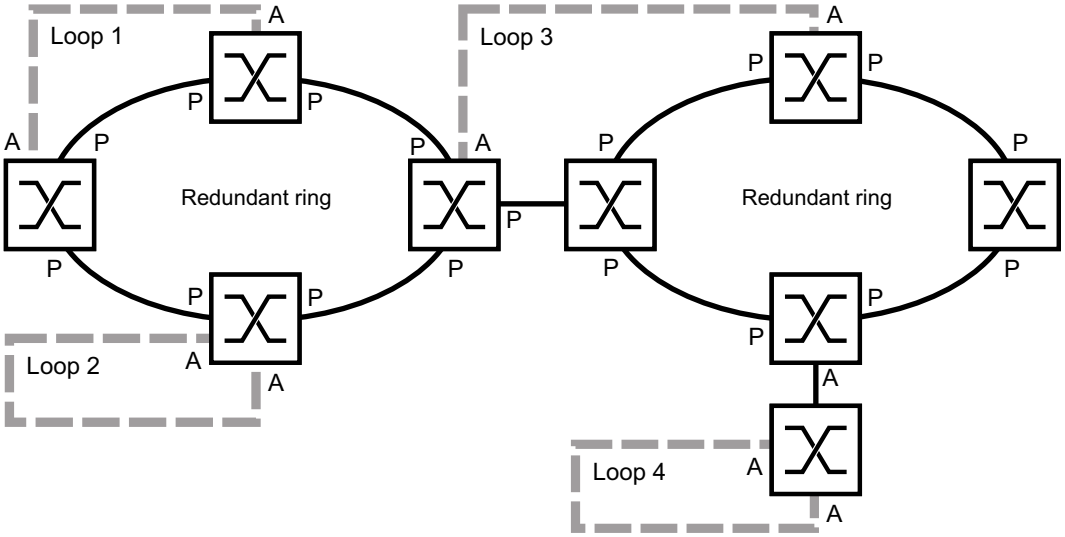


Abb. 73: Beispiele für unbeabsichtigte Layer-2-Loops

Loop-Schutz-Einstellungen den Ports zuweisen

Weisen Sie jedem *aktiven* und *passiven* Port die Einstellungen der Funktion *Loop-Schutz* zu.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Loop-Schutz*.
- ☐ Passen Sie im Rahmen *Global*, Feld *Sende-Intervall* den Wert an, falls erforderlich.
- ☐ Passen Sie im Rahmen *Global*, Feld *Empfang-Grenzwert* den Wert an, falls erforderlich.
- ☐ Legen Sie in Spalte *Modus* das Verhalten der Funktion *Loop-Schutz* auf dem Port fest:
  - `aktiv` für Ports, die für den Anschluss von Endgeräten vorgesehen sind
  - `passiv` für Ports, die zu den redundanten Ringen gehören
- ☐ Legen Sie in Spalte *Aktion* den Wert *alle* fest.
  Wenn das Gerät einen Layer-2-Loop an diesem Port erkennt, dann sendet es einen Trap und deaktiviert den Port mit Hilfe der Funktion *Auto-Disable*. Passen Sie den Wert an, falls erforderlich.
- ☐ Markieren Sie in Spalte *Aktiv* das Kontrollkästchen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`loop-protection tx-interval 5`	Legen Sie das Sende-Intervall fest, falls erforderlich.
`loop-protection rx-threshold 1`	Legen Sie den Empfang-Grenzwert fest, falls erforderlich.

`interface 1/1`	Wechsel in den Interface-Modus. Beispiel: Port *1/1*.
`loop-protection mode active`	Für Ports, an die Endgeräte angeschlossen werden, den Modus `active` festlegen.
`loop-protection mode passive`	Für Ports, die zu den redundanten Ringen gehören, den Modus `passive` festlegen.
`loop-protection action all`	Aktion festlegen, die das Gerät ausführt, wenn es einen Layer-2-Loop an diesem Port erkennt.
`loop-protection operation`	Aktivieren der Funktion *Loop-Schutz* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.

Funktion Auto-Disable aktivieren.

Nachdem Sie den Ports die *Loop-Schutz*-Einstellungen zugewiesen haben, aktivieren Sie die Funktion *Auto-Disable*.

Führen Sie die folgenden Schritte aus:

- ☐ Markieren Sie im Rahmen *Konfiguration* das Kontrollkästchen *Auto-Disable*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`loop-protection auto-disable`	Aktivieren Sie die Funktion *Auto-Disable*.

Funktion Loop-Schutz im Gerät einschalten

Abschließend schalten Sie die Funktion *Loop-Schutz* im Gerät ein.

Führen Sie die folgenden Schritte aus:

- ☐ Wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`loop-protection operation`	Einschalten der Funktion *Loop-Schutz* auf dem Gerät.

14.11.2 Empfehlungen für redundante Ports

Abhängig von den *Loop-Schutz*-Einstellungen schaltet das Gerät mit der Funktion *Auto-Disable* Ports aus, wenn das Gerät einen Layer-2-Loop erkennt.

Wenn auf einem Port eine Redundanzfunktion aktiv ist, dann aktivieren Sie nicht den Modus *aktiv* auf diesem Port. Andernfalls kann das Ausschalten von Ports auf redundanten Pfaden im Netz die Folge sein. Im obigen Beispiel sind dies die Ports, die zu den redundanten Ringen gehören.

Vergewissern Sie sich, dass ein redundanter Pfad im Netz als Backup-Medium verfügbar ist. Bei Ausfall des primären Pfads wechselt das Gerät auf den redundanten Pfad.

Die folgenden Einstellungen helfen, das Abschalten von Ports auf redundanten Netzwerkpfaden zu vermeiden:

- ☐ Deaktivieren Sie die Funktion *Loop-Schutz* auf redundanten Ports.
  oder
- ☐ Aktivieren Sie den *passiv*-Modus auf redundanten Ports.

Die Funktion *Loop-Schutz* und die Funktion *Spanning Tree* beeinflussen sich gegenseitig. Die folgenden Schritte helfen, ein unerwartetes Verhalten des Geräts zu vermeiden:

- ☐ Schalten Sie die *Spanning Tree*-Funktion an dem Port aus, an dem Sie die *Loop-Schutz*-Funktion einschalten möchten. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree > Port*, Spalte *STP aktiv*.
- ☐ Schalten Sie die Funktion*Spanning Tree* auf dem angeschlossenen Port jedes angeschlossenen Geräts aus. Siehe Dialog *Switching > L2-Redundanz > Spanning Tree*.

14.12 Benutzen der Funktion E-Mail-Benachrichtigung

Das Gerät ermöglicht Ihnen, Benutzer per E-Mail über das Eintreten von Ereignissen zu benachrichtigen. Voraussetzung ist ein über das Netz erreichbarer Mail-Server, an den das Gerät die E-Mails übergibt.

Um im Gerät das Senden von E-Mails einzurichten, führen Sie die Schritte in den folgenden Kapiteln aus:

- ☐ Absender-Adresse festlegen
- ☐ Auslösende Ereignisse festlegen
- ☐ Empfänger festlegen
- ☐ Mail-Server festlegen
- ☐ Funktion E-Mail-Benachrichtigung ein-/ausschalten
- ☐ Test-Nachricht senden

14.12.1 Absender-Adresse festlegen

Die Absender-Adresse ist die E-Mail-Adresse, die den Empfängern zeigt, wer die E-Mail gesendet hat. Die Voreinstellung im Gerät ist .

Ändern Sie den voreingestellten Wert. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.
- ☐ Ändern Sie im Rahmen *Absender* den Wert im Feld *Adresse*.
  Fügen Sie eine gültige E-Mail-Adresse ein.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging email from-addr <user@doma.in>`	Ändert die Absender-Adresse.

14.12.2 Auslösende Ereignisse festlegen

Das Gerät unterscheidet Ereignisse mit den folgenden Schweregraden:

Tab. 58: Bedeutung der Schweregrade für Ereignisse

Schweregrad	Bedeutung
`emergency`	Gerät nicht betriebsbereit
`alert`	Sofortiger Bedienereingriff erforderlich
`critical`	Kritischer Zustand
`error`	Fehlerhafter Zustand
`warning`	Warnung

Tab. 58: Bedeutung der Schweregrade für Ereignisse (Forts

Schweregrad	Bedeutung
notice	Signifikanter, normaler Zustand
informational	Informelle Nachricht
debug	Debug-Nachricht

Sie haben die Möglichkeit, selbst festzulegen, über welche Ereignisse das Gerät Sie benachrichtigt. Hierzu weisen Sie den Benachrichtigungsstufen des Geräts den gewünschten Mindest-Schweregrad zu.

Das Gerät benachrichtigt die Empfänger wie folgt:

- *Benachrichtung sofort*
  Wenn ein Ereignis mit diesem Schweregrad oder mit einem dringenderen Schweregrad auftritt, sendet das Gerät sofort eine E-Mail.
- *Benachrichtung periodisch*
  - Wenn ein Ereignis mit dem zugewiesenen oder einem kritischeren Schweregrad eintritt, protokolliert das Gerät das Ereignis in einem Puffer.
  - Das Gerät sendet eine E-Mail mit dem Protokoll periodisch oder wenn der Puffer voll ist.
  - Ereignisse mit einem weniger kritischen Schweregrad protokolliert das Gerät nicht.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.

Im Rahmen *Benachrichtung sofort* legen Sie die Einstellungen für E-Mails fest, die das Gerät sofort sendet.

- ☐ Legen Sie im Feld *Schweregrad* den Mindest-Schweregrad fest.
- ☐ Im Feld *Betreff* legen Sie den Betreff der E-Mail fest.

Im Rahmen *Benachrichtung periodisch* legen Sie die Einstellungen für E-Mails fest, die das Gerät in regelmäßigen Abständen sendet.

- ☐ Legen Sie im Feld *Schweregrad* den Mindest-Schweregrad fest.
- ☐ Im Feld *Betreff* legen Sie den Betreff der E-Mail fest.

- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging email severity immediate <level>`	Legt den Mindest-Schweregrad der Ereignisse fest, für die das Gerät die E-Mail sofort sendet.
`logging email severity periodic <level>`	Legt den Mindest-Schweregrad der Ereignisse fest, für die das Gerät die E-Mail in regelmäßigen Abständen sendet.
`logging email subject add <immediate | periodic> TEXT`	Erzeugt eine Betreffzeile mit dem Inhalt `TEXT`.

14.12.3 Sendeintervall ändern

Das Gerät ermöglicht Ihnen, festzulegen, in welchem Intervall es E-Mails mit dem Protokoll sendet. Die Voreinstellung ist `30` Minuten.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.

Im Rahmen *Benachrichtung periodisch* legen Sie die Einstellungen für E-Mails fest, die das Gerät in regelmäßigen Abständen sendet.

- ☐ Ändern Sie den Wert im Feld *Sende-Intervall [min]*, um das Intervall zu ändern.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging email duration <30..1440>`	Legt das Intervall fest, in dem das Gerät E-Mails mit Protokoll sendet.

14.12.4 Empfänger festlegen

Das Gerät ermöglicht Ihnen, bis zu 10 Empfänger festzulegen.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Empfänger*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche ⊞.
- ☐ Im Rahmen *Benachrichtungs-Typ* legen Sie fest, ob das Gerät die E-Mails an diesen Empfänger sofort oder in regelmäßigen Abständen sendet.
- ☐ Legen Sie im Feld *Adresse* die E-Mail-Adresse des Empfängers fest.
- ☐ Markieren Sie in Spalte *Aktiv* das Kontrollkästchen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately | periodically>`	Legt den Empfänger mit der E-Mail-Adresse `user@doma.in` fest. Das Gerät verwaltet die Einstellungen auf dem Speicherplatz `1..10`.

14.12.5 Mail-Server festlegen

Das Gerät unterstützt verschlüsselte und unverschlüsselte Verbindungen zum Mail-Server.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Mail-Server*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Legen Sie in Spalte *IP-Adresse* die IP-Adresse oder den DNS-Namen des Servers fest.
- ☐ Legen Sie in Spalte *Verschlüsselung* das Protokoll fest, das die Verbindung zwischen Gerät und Mail-Server verschlüsselt.
- ☐ Legen Sie in Spalte *Ziel-TCP-Port* den TCP-Port fest, wenn der Mail-Server einen anderen als den Well-known-Port verwendet.

Wenn der Mail-Server eine Authentifizierung erfordert:

- ☐ Legen Sie in den Spalten *Benutzername* und *Passwort* die Anmeldeinformationen für das Konto fest, mit dem sich das Gerät beim Mail-Server anmeldet.
- ☐ Fügen Sie in Spalte *Beschreibung* eine aussagekräftige Bezeichnung für den Mail-Server ein.
- ☐ Markieren Sie in Spalte *Aktiv* das Kontrollkästchen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	Legt den Mail-Server mit der IP-Adresse `IP ADDRESS` fest. Das Gerät verwaltet die Einstellungen auf dem Speicherplatz `1..5`.

14.12.6 Funktion E-Mail-Benachrichtigung ein-/ausschalten

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging email operation`	Schaltet das Senden von E-Mails ein.
`no logging email operation`	Schaltet das Senden von E-Mails aus.

14.12.7 Test-Nachricht senden

Das Gerät ermöglicht Ihnen, durch Senden einer Test-Nachricht die Einstellungen zu prüfen.

Voraussetzung:
- Die E-Mail-Einstellungen sind vollständig festgelegt.
- Die Funktion *E-Mail-Benachrichtigung* ist eingeschaltet.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > E-Mail-Benachrichtigung > Mail-Server*.
- ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Verbindung testen*.
  Der Dialog zeigt das Fenster *Verbindung testen*.
- ☐ Wählen Sie in der Dropdown-Liste *Empfänger*, an welche Empfänger das Gerät die E-Mail sendet.
- ☐ Legen Sie im Feld *Nachrichtentext* den Text der Test-Nachricht fest.
- ☐ Klicken Sie die Schaltfläche *Ok*, um die Test-Nachricht zu senden.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging email test msgtype <urgent|non-urgent> TEXT`	Sendet eine E-Mail-Nachricht mit dem Inhalt `TEXT` an die Empfänger.

Wenn Sie keine Meldung zu erkannten Fehlern sehen und die Empfänger die E-Mail erhalten, sind die Einstellungen im Gerät korrekt festgelegt.

14.13 Berichte

Im Folgenden werden die für Diagnosezwecke verfügbaren Berichte und Schaltflächen aufgeführt:

- System-Log-Datei
  Die Logdatei ist eine HTML-Datei, in die das Gerät geräteinterne Ereignisse schreibt.
- Audit Trail
  Protokolliert erfolgreiche Kommandos und Kommentare von Benutzern. Die Datei schließt auch das SNMP-Logging ein.
- Persistentes Protokoll
  Das Gerät speichert Protokolleinträge in einer Datei im externen Speicher (falls vorhanden). Diese Dateien sind nach dem Abschalten verfügbar. Die maximale Größe und Anzahl von speicherbaren Dateien sowie der Schweregrad der protokollierten Ereignisse sind konfigurierbar. Nach Erreichen der benutzerdefinierten maximale Größe oder Anzahl speicherbarer Dateien archiviert das Gerät die Einträge und erzeugt eine neue Datei. Das Gerät löscht die älteste Datei und benennt die anderen Dateien um, um die konfigurierte Anzahl von Dateien beizubehalten. Um diese Dateien zu prüfen, verwenden Sie das Command Line Interface oder kopieren Sie die Dateien für den späteren Zugriff auf einen externen Server.
- *Support-Informationen herunterladen*
  Diese Schaltfläche ermöglicht Ihnen, Systeminformationen als ZIP-Archiv herunterzuladen.

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

14.13.1 Globale Einstellungen

Über diesen Dialog aktivieren oder deaktivieren Sie die jeweiligen Ziele, an die das Gerät Berichte sendet, zum Beispiel Konsole, Syslog-Server oder Verbindung zum Command Line Interface. Ferner legen Sie fest, ab welchem Schweregrad das Gerät Ereignisse in die Berichte schreibt.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Bericht > Global*.
- ☐ Um einen Bericht an die Konsole zu senden, legen Sie im Rahmen *Console-Logging* die gewünschte Stufe im Feld *Schweregrad* fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Console-Logging* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Das Gerät puffert die protokollierten Ereignisse in 2 separaten Speicherbereichen, sodass das Gerät die Protokolleinträge für dringende Ereignisse beibehält. Legen Sie den minimalen Schweregrad für Ereignisse fest, die das Gerät im gepufferten Speicherbereich mit einer höheren Priorität protokolliert.

Führen Sie die folgenden Schritte aus:

- ☐ Um Ereignisse an den Puffer zu senden, legen Sie im Rahmen *Buffered-Logging* die gewünschte Stufe im Feld *Schweregrad* fest.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Wenn Sie die Protokollierung von SNMP-Anfragen aktivieren, protokolliert das Gerät die Anfragen im Syslog als Ereignisse. Die Funktion *Protokolliere SNMP-Get-Requests* protokolliert Benutzeranfragen nach Geräte-Konfigurationsinformationen. Die Funktion *Protokolliere SNMP-Set-Requests* protokolliert Geräte-Konfigurationsereignisse. Legen Sie die Untergrenze für Ereignisse fest, die das Gerät im Syslog einträgt.

Führen Sie die folgenden Schritte aus:

- ☐ Um SNMP-Lese-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die Funktion *Protokolliere SNMP-Get-Requests* ein.
  Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld *An*.
- ☐ Um SNMP-Schreib-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die Funktion *Protokolliere SNMP-Set-Requests* ein.
  Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld *An*.
- ☐ Wählen Sie den gewünschten Schweregrad für die Get- und Set-Anfragen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Sofern aktiv, protokolliert das Gerät Änderungen an der Konfiguration, die über das Command Line Interface vorgenommen wurden, im Audit Trail. Diese Funktion liegt der Norm IEEE 1686 für intelligente elektronische Unterstationsgeräte zugrunde.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Bericht > Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *CLI-Logging* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Das Gerät ermöglicht Ihnen, die folgenden Systeminformationen in einer ZIP-Datei auf Ihrem PC speichern:

- `audittrail.html`
- `defaultconfig.xml`
- `script`
- `runningconfig.xml`
- `supportinfo.html`
- `systeminfo.html`
- `systemlog.html`

Den Dateinamen des ZIP-Archivs erzeugt das Gerät automatisch nach dem Muster `<IP-Adresse>_<Gerätename>.zip`.

Führen Sie die folgenden Schritte aus:

- ☐ Klicken Sie die Schaltfläche ☰ und dann den Eintrag *Support-Informationen herunterladen*.
- ☐ Wählen Sie das Verzeichnis aus, in welchem Sie die Support-Information speichern.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

14.13.2 Syslog

Das Gerät bietet Ihnen die Möglichkeit, Nachrichten zu geräteinternen Ereignissen an einen oder mehrere Syslog-Server (bis zu 8) zu senden. Zusätzlich schließen Sie SNMP-Anfragen des Geräts als Ereignisse in den Syslog ein.

Anmerkung: Zum Anzeigen der protokollierten Ereignisse öffnen Sie den Dialog *Diagnose* > Bericht > *Audit-Trail* oder den Dialog *Diagnose* > *Bericht* > *System-Log*.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose* > *Syslog*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Fügen Sie in Spalte *IP-Adresse* die IP-Adresse oder den *Hostname* des Syslog-Servers ein. Sie können eine gültige IPv4- oder IPv6-Adresse für den Syslog-Server festlegen.
- ☐ Legen Sie in Spalte *Ziel-UDP-Port* den TCP- oder UDP-Port fest, auf dem der Syslog-Server die Log-Einträge erwartet.
- ☐ Legen Sie in Spalte *Min. Schweregrad* den Mindest-Schweregrad fest, den ein Ereignis benötigt, damit das Gerät einen Protokolleintrag an diesen Syslog-Server sendet.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

Konfigurieren Sie im Rahmen *SNMP-Logging* die folgenden Einstellungen für SNMP-Lese- und Schreibanfragen:

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose* > *Bericht* > *Global*.
- ☐ Um SNMP-Lese-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die Funktion *Protokolliere SNMP-Get-Requests* ein.
  Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld `An`.
- ☐ Um SNMP-Schreib-Anfragen für das Gerät als Ereignisse an den Syslog-Server senden, schalten Sie die Funktion *Protokolliere SNMP-Set-Requests* ein.
  Um die Funktion einzuschalten, wählen Sie im Rahmen *SNMP-Logging* das Optionsfeld `An`.
- ☐ Wählen Sie den gewünschten Schweregrad für die Get- und Set-Anfragen.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging host add 1 addr 10.0.1.159 severity 3`	Fügt der Liste der Syslog-Server einen neuen Empfänger hinzu. Der Wert `3` legt den Schweregrad des Ereignisses fest, welches das Gerät protokolliert. Der Wert `3` bedeutet `error`.
`logging host add 2 addr 2001::1 severity 4`	Fügen Sie der Liste der Syslog-Server einen neuen IPv6-Empfänger hinzu. Der Wert `4` bedeutet `warning`.
`logging syslog operation`	Einschalten der Funktion *Syslog*.
`exit`	Wechsel in den Privileged-EXEC-Modus.

```
show logging host                                    Anzeigen der Syslog-Host-Einstellungen.
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
2      2001::1        514    warning         systemlog   active
configure                                            Wechsel in den Konfigurationsmodus.
logging snmp-requests get operation                  Protokolliert SNMP-Get-Anfragen.
logging snmp-requests get severity 5                 Der Wert 5 legt den Schweregrad des Ereignisses
                                                     fest, welches das Gerät bei SNMP-GET-Anfragen
                                                     protokolliert. Der Wert 5 bedeutet notice.
logging snmp-requests set operation                  Protokolliert SNMP-SET-Anfragen.
logging snmp-requests set severity 5                 Der Wert 5 legt den Schweregrad des Ereignisses
                                                     fest, welches das Gerät bei SNMP-SET-Anfragen
                                                     protokolliert. Der Wert 5 bedeutet notice.
exit                                                 Wechsel in den Privileged-EXEC-Modus.
show logging snmp                                    Zeigt die SNMP-Logging-Einstellungen.
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

14.13.3 System-Log

Das Gerät ermöglicht Ihnen, ein Protokoll zu den Systemereignissen aufzurufen. In der Tabelle im Dialog *Diagnose > Bericht > System-Log* werden die protokollierten Ereignisse aufgeführt.

Führen Sie die folgenden Schritte aus:

- ☐ Um den Inhalt des Protokolls zu aktualisieren, klicken Sie die Schaltfläche  .
- ☐ Um den Inhalt des Protokolls als html-Datei zu speichern, klicken Sie die Schaltfläche  und dann den Eintrag *Zurücksetzen*.
- ☐ Um den Inhalt des Protokolls zu löschen, klicken Sie die Schaltfläche  und dann den Eintrag *Zurücksetzen*.
- ☐ Um den Inhalt des Protokolls nach Suchbegriffen zu durchsuchen, verwenden Sie die Suchfunktion Ihres Web-Browsers.

Anmerkung: Sie haben die Möglichkeit, auch protokollierte Ereignisse an einen oder mehrere Syslog-Server zu senden.

14.13.4 Syslog über TLS

Transport Layer Security ist ein kryptografisches Protokoll, das entwickelt wurde, um Kommunikationssicherheit über ein Rechnernetz zu unterstützen. Das vorrangige Ziel des TLS-Protokolls besteht darin, Datenschutz und Datenintegrität zwischen 2 kommunizierenden Computeranwendungen herzustellen.

Nach der Initiierung einer Datenverbindung mit einem Syslog-Server über einen TLS-Handshake validiert das Gerät das vom Server empfangene Zertifikat. Zu diesem Zweck übertragen Sie das PEM-Zertifikat von einem Remote-Server oder vom externen Speicher oder aus dem externen Speicher auf das Gerät. Vergewissern Sie sich, dass die konfigurierte IP-Adresse oder der DNS-Name des Servers mit den im Zertifikat enthaltenen Informationen übereinstimmt. Sie finden die Informationen in den Feldern „Allgemeiner Name“ oder „Alternativer Name des Betreffs“ des Zertifikates.

Das Gerät sendet die TLS-verschlüsselten Syslog-Nachrichten über den TCP-Port, der in Spalte *Ziel-UDP-Port* festgelegt ist.

Anmerkung: Legen Sie die IP-Adresse oder den DNS-Namen des Servers dahingehend fest, dass sie/er der IP-Adresse bzw. dem DNS-Namen im Serverzertifikat entspricht. Die Werte sind im Zertifikat als „Allgemeiner Name“ oder als „Alternativer Name des Betreffs“ angegeben.

Beispiel

Das vorliegende Beispiel beschreibt die Konfiguration der Funktion *Syslog*. Wenn Sie die folgenden Schritte ausführen, ermöglicht Ihnen das Gerät, TLS-verschlüsselte Syslog-Nachrichten über den TCP-Port zu senden, der in Spalte *Ziel-UDP-Port* festgelegt ist.

Syslog-Nachrichten, die von einem Gerät an einen Syslog-Server gesendet werden, passieren ggf. unsichere Netze. Um einen Syslog-Server über TLS zu konfigurieren, übertragen Sie das CA-Zertifikat auf das Gerät.

Anmerkung: Um die Änderungen nach dem Laden eines neuen Zertifikates zu übernehmen, starten Sie die Funktion *Syslog* neu.

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Syslog*.
- ☐ Um eine Datenverbindung mit den Syslog-Servern zu initiieren, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

Das Gerät validiert das empfangene Zertifikat. Das Gerät authentifiziert außerdem den Server und beginnt mit dem Senden von Syslog-Nachrichten.

- ☐ Übertragen Sie das PEM-Zertifikat vom Remote-Server oder aus dem externen Speicher auf das Gerät.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`logging host add 1 addr 192.168.3.215`	Fügen Sie Index `1` dem Syslog-Server mit IPv4-Adresse `192.168.3.215` hinzu.
`logging host add 2 addr 2001::1`	Fügen Sie Index `2` dem Syslog-Server mit IPv4-Adresse `2001::1.` hinzu.

`logging host modify 1 port 6512 type systemlog`	Portnummer `6512` festlegen und Ereignisse in der Log-Datei (System Log) protokollieren.
`logging host modify 1 transport tls`	Legen Sie für den Übertragungstyp `tls` fest.
`logging host modify 1 severity informational`	Ereignis-Typ festlegen, der als `informational` in der Log-Datei (System Log) protokolliert wird.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`copy syslogcacert evmm`	Kopieren Sie CA-Zertifikate aus dem externen Speicher auf das Gerät.
`show logging host`	Anzeigen der Syslog-Host-Einstellungen.

14.13.5 Audit Trail

Der Dialog *Diagnose > Bericht > Audit-Trail* enthält Systeminformationen sowie Änderungen, die über Command Line Interface und SNMP an dem Gerät vorgenommen wurden. Bei Änderungen der Gerätekonfiguration zeigt der Dialog, wer zu welchem Zeitpunkt welche Änderungen vorgenommen hat.

Der Dialog *Diagnose > Syslog* ermöglicht Ihnen, bis zu 8 Syslog-Server festzulegen, an die das Gerät Audit Trails sendet.

Die folgende Liste enthält Protokollereignisse:

- Änderungen an Konfigurationsparametern
- Kommandos (mit Ausnahme der `show`-Kommandos) im Command Line Interface
- Kommando `logging audit-trail <string>` im Command Line Interface, das den Kommentar protokolliert
- Automatische Änderungen der Systemzeit
- Watchdog-Ereignisse
- Sperren eines Benutzers nach mehreren fehlgeschlagenen Login-Versuchen
- Benutzeranmeldung über das Command Line Interface (lokal oder remote)
- Manuelle, benutzerinitiierte Abmeldung
- Zeitgesteuerte Abmeldung nach einer benutzerdefinierten Zeitspanne der Inaktivität im Command Line Interface.
- Dateiübertragung, einschließlich Firmware-Update
- Konfigurationsänderungen über Ethernet Switch Configurator
- Automatische Konfiguration oder Firmware-Updates über den externen Speicher
- Gesperrter Zugriff auf das Management des Geräts aufgrund von ungültigen Anmeldedaten
- Neustart
- Öffnen und Schließen von SNMP über HTTPS-Tunnel
- Ermittelte Stromausfälle

14.14 Netzanalyse mit TCPDump

TCPDump ist ein UNIX-Hilfsprogramm für das Packet-Sniffing, das von Netzadministratoren verwendet wird, um Datenverkehr im Netz aufzuspüren und zu analysieren. Das Aufspüren von Datenverkehr dient unter anderem der Verifizierung der Konnektivität zwischen Hosts und der Analyse des Datenverkehrs, der das Netz durchquert.

TCPDump auf dem Gerät bietet die Möglichkeit, durch die Management-CPU empfangene oder übertragene Pakete zu dekodieren oder zu erfassen. Auf diese Funktion kann über das Kommando `debug` zugegriffen werden. Weitere Informationen zur TCPDump-Funktion finden Sie im Referenzhandbuch „Command Line Interface“.

14.15 Datenverkehr beobachten

Das Gerät ermöglicht Ihnen, Datenpakete, die das Gerät durchlaufen, an einen Ziel-Port weiterzuleiten. Dort können Sie die Datenpakete überwachen und auswerten.

Das Gerät bietet Ihnen folgende Möglichkeiten:
- Port-Mirroring

14.15.1 Port-Mirroring

Die Funktion *Port-Mirroring* ermöglicht Ihnen, die Datenpakete von physischen Quell-Ports zu einem physischen Ziel-Port zu kopieren.

Mit einem am Ziel-Port angeschlossenen Analysator, zum Beispiel RMON-Probe, überwachen Sie die auf den Quell-Ports gesendeten und empfangen Datenpakete. Die Funktion hat keine Auswirkungen auf den über die Quell-Ports laufenden Datenstrom.

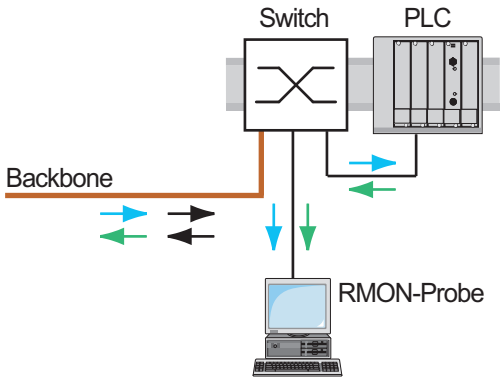


Abb. 74: Beispiel

Das Gerät vermittelt auf dem Ziel-Port ausschließlich die von den Quell-Ports kopierten Datenpakete.

Um über den Ziel-Port auf das Management des Geräts zuzugreifen, markieren Sie vor Einschalten der Funktion *Port-Mirroring* das Kontrollkästchen *Management erlauben*. Das Gerät ermöglicht Benutzern den Zugriff auf das Management des Geräts über den Ziel-Port, ohne die aktive *Port-Mirroring*-Session zu unterbrechen.

Anmerkung: Das Gerät dupliziert auf dem Ziel-Port Multicasts, Broadcasts und unbekannte Unicasts.

Die VLAN-Einstellungen auf dem Ziel-Port bleiben unverändert. Voraussetzung für den Zugriff auf des Management des Geräts über den Ziel-Port ist, dass der Ziel-Port Mitglied im Management-VLAN ist.

Funktion Port-Mirroring einschalten

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Diagnose > Ports > Port-Mirroring*.
- ☐ Legen Sie die Quell-Ports fest.
  Markieren Sie das Kontrollkästchen in Spalte *Eingeschaltet* für die gewünschten Ports.
- ☐ Legen Sie den Ziel-Port fest.
  Wählen Sie im Rahmen *Ziel-Port*, Dropdown-Liste *Primärer Port* den gewünschten Port.
  Die Dropdown-Liste zeigt ausschließlich die verfügbaren Ports. Bereits als Quell-Port festgelegte Ports sind nicht verfügbar.
- ☐ Falls erforderlich, legen Sie einen zweiten Ziel-Port fest.
  Wählen Sie im Rahmen *Ziel-Port*, Dropdown-Liste *Sekundärer Port* den gewünschten Port.
  Voraussetzung ist, dass bereits der primäre Ziel-Port festgelegt ist.
- ☐ Um über den Ziel-Port auf das Management des Geräts zuzugreifen:
  Markieren Sie im Rahmen *Ziel-Port* das Kontrollkästchen *Management erlauben*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Um die Funktion *Port-Mirroring* zu deaktivieren und die Voreinstellungen wiederherzustellen, klicken Sie die Schaltfläche ☰ und dann den Eintrag *Konfiguration zurücksetzen*.

14.16 Selbsttest

Das Gerät prüft beim Booten und gelegentlich danach seine Anlagen. Das Gerät prüft die Aufgabenverfügbarkeit oder den Aufgabenabbruch im System sowie den verfügbaren Speicherplatz. Außerdem prüft das Gerät die Funktionalität der Anwendung und prüft, ob der Chipsatz eine Verschlechterung der Hardware aufweist.

Wenn das Gerät einen Integritätsverlust ermittelt, reagiert es auf die Beeinträchtigung mit einer benutzerdefinierten Maßnahme. Für die Konfiguration stehen folgende Kategorien zur Verfügung:

- `task`
  Zu ergreifende Maßnahme, wenn eine Aufgabe missglückt ist.
- `resource`
  Zu ergreifende Maßnahme bei ungenügenden Ressourcen.
- `software`
  Zu ergreifende Maßnahme bei Verlust der Software-Integrität, zum Beispiel bei Prüfsummenfehlern in Code-Segmenten oder bei Zugriffsverletzungen.
- `hardware`
  Zu ergreifende Maßnahme aufgrund einer Beeinträchtigung der Hardware.

Legen Sie für jede Kategorie eine entsprechende Maßnahme fest, mit der das Gerät bei Feststellen eines Integritätsverlustes reagiert. Für die Konfiguration stehen folgende Funktionen zur Verfügung:

- `log only`
  Diese Aktion schreibt eine Meldung an die Ereignisprotokolldatei.
- `send trap`
  Sendet einen SNMP-Trap an das Trap-Ziel.
- `reboot`
  Bei Aktivierung führt ein 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.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`selftest action task log-only`	Senden einer Nachricht an das Ereignisprotokoll, wenn eine Aufgabe missglückt ist.
`selftest action resource send-trap`	Senden eines SNMP-Traps bei Ressourcen-Mangel.
`selftest action software send-trap`	Senden eines SNMP-Traps bei Verlust der Software-Integrität.
`selftest action hardware reboot`	Neustart des 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*.

- *RAM-Test*
  Aktiviert/deaktiviert die *RAM-Test*-Funkion während eines Kaltstarts.

- *SysMon1 ist verfügbar*
  Aktiviert/deaktiviert die Funktion System-Monitor während eines Kaltstarts.
- *Bei Fehler Default-Konfiguration laden*
  Aktiviert/deaktiviert das Laden der Standard-Gerätekonfiguration, falls dem Gerät beim Neustart keine lesbare Konfiguration zur Verfügung steht.

Die folgenden Einstellungen sperren Ihnen dauerhaft den Zugang zum Gerät, wenn das Gerät beim Neustart kein lesbares Konfigurationsprofil findet.
- Das Kontrollkästchen *SysMon1 ist verfügbar* ist unmarkiert.
- Das Kontrollkästchen *Bei Fehler Default-Konfiguration laden* ist unmarkiert.

Dies ist zum Beispiel dann der Fall, wenn sich das Passwort des zu ladenden Konfigurationsprofils von dem im Gerät festgelegten Passwort unterscheidet. Um das Gerät wieder entsperren zu lassen, wenden Sie sich an Ihren Vertriebspartner.

Führen Sie die folgenden Schritte aus:

`selftest ramtest`	Aktivieren des RAM-Selbsttests bei einem Kaltstart.
`no selftest ramtest`	Abschalten der Funktion „ramtest“
`selftest system-monitor`	Aktivieren der Funktion „SysMon1“
`no selftest system-monitor`	Abschalten der Funktion „SysMon1“
`show selftest action`	Statusanzeige der durchzuführenden Maßnahmen bei einer Beeinträchtigung des Geräts
`show selftest settings`	Anzeige der Einstellungen für „ramtest“ und SysMon“ bei einem Kaltstart

14.17 Kupferkabeltest

Verwenden Sie diese Funktion, um ein an eine Schnittstelle angeschlossenes Kupferkabel auf einen Kurzschluss oder eine Schaltkreisunterbrechung zu testen. Der Test unterbricht den Verkehrsfluss (falls vorhanden) auf diesem Port.

Die Tabelle zeigt den Zustand und die Länge jedes einzelnen Paares. Das Gerät gibt ein Ergebnis mit der folgenden Bedeutung zurück:

- normal – gibt an, dass das Kabel ordnungsgemäß funktioniert
- offen – gibt an, dass im Kabel eine Unterbrechung vorliegt
- Kurzschluss – gibt an, dass das Kabel einen Kurzschluss aufweist
- ungetestet – gibt an, dass ein ungetestetes Kabel vorhanden ist
- unbekannt – Kabel abgezogen

15 Erweiterte Funktionen des Geräts

15.1 Gerät als DHCP-Server verwenden

Ein DHCP-Server („Dynamic Host Configuration Protocol“) nimmt die Zuweisung von IP-Adressen, Gateways und sonstigen Netzdefinitionen (zum Beispiel DNS- und NTP-Parameter) zu Clients vor.

Die DHCP-Operationen laufen in 4 Schritten ab: IP Discovery (Client versendet Anfrage an Server), IP Lease Offer (Server bieten IP-Adresse an), IP Request (Client fordert IP-Adresse an) und IP Lease Acknowledgement (Server bestätigt Adresse). Die Phasen sind anhand des Akronyms „DORA“ (für „Discovery“, „Offer“, „Recovery“ und „Acknowledgement“) einfach zu merken. Der Server empfängt Client-Daten über UDP-Port 67 und vermittelt Daten an den Client über UDP-Port 68.

Der DHCP-Server stellt IP-Adress-Pools, auch als „Pools“ bezeichnet, bereit, aus denen er den Clients IP-Adressen zuweist. Der Pool besteht aus einer Liste mit Einträgen. Ein Eintrag definiert entweder eine bestimmte IP-Adresse oder einen IP-Adressbereich.

Das Gerät ermöglicht Ihnen, den DHCP-Server global oder je Schnittstelle zu aktivieren.

15.1.1 Pro Port oder pro VLAN zugewiesene IP-Adressen

Der DHCP-Server weist einem Client, der mit einem Port oder einem VLAN verbunden ist, eine statische IP-Adresse oder einen dynamischen Bereich von IP-Adressen zu. Das Gerät ermöglicht Ihnen, Einträge entweder für einen Port oder ein VLAN anzulegen. Beim Erzeugen eines Eintrags für das Zuweisen von IP-Adressen zu einem VLAN wird der Port-Eintrag grau dargestellt. Beim Erzeugen eines Eintrags für das Zuweisen von IP-Adressen zu einem Port wird der VLAN-Eintrag grau dargestellt.

Bei statischer Zuordnung weist der DHCP-Server einem bestimmten Client dieselbe IP-Adresse zu. Der DHCP-Server identifiziert den Client über eine eindeutige Hardware-ID. Ein statischer Adresseintrag enthält eine IP-Adresse, die er auf einen Port oder ein VLAN anwendet, auf dem der Server eine Anfrage von einem bestimmten Client erhält. Für eine statische Zuteilung legen Sie einen Pool-Eintrag für die Ports oder einen bestimmten Port an, geben die IP-Adresse ein und lassen die Spalte *Letzte IP-Adresse* frei. Legen Sie eine Hardware-Kennung fest, über die der DHCP-Server den Client eindeutig identifiziert. Diese Kennung ist entweder eine MAC-Adresse, eine Client-ID, eine Remote-ID oder eine Circuit-ID. Wenn ein Client den Server mit der konfigurierten Hardware-Kennung kontaktiert, weist der DHCP-Server die statische IP-Adresse zu.

Das Gerät ermöglicht Ihnen außerdem, Ports oder VLANs, von denen der DHCP-Server eine freie IP-Adresse aus einem Pool zuweist, einen dynamischen IP-Adressbereich zuzuweisen. Um einen dynamischen Pool-Eintrag für die Ports oder VLANs hinzuzufügen, legen Sie die erste und letzte IP-Adresse für den IP-Adressbereich fest und lassen die Spalten *MAC-Adresse*, *Client-ID*, *Remote-ID* und *Circuit-ID* leer. Das Erzeugen mehrerer Pool-Einträge ermöglicht Ihnen Lücken in den IP-Adressbereichen.

15.1.2 Beispiel: DHCP-Server – Statische IP-Adresse

In diesem Beispiel konfigurieren Sie das Gerät so, dass es einem Port eine statische IP-Adresse zuweist. Das Gerät erkennt Clients mit eindeutiger Hardware-Kennung. Die Hardware-Kennung ist in diesem Fall die Client-MAC-Adresse `00:24:E8:D6:50:51`. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DHCP Server > Pool*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche  .
- ☐ Legen Sie in Spalte *IP-Adresse* den Wert `192.168.23.42` fest.
- ☐ Legen Sie in Spalte *Port* den Wert `1/1` fest.
- ☐ Legen Sie in Spalte *MAC-Adresse* den Wert `00:24:E8:D6:50:51` fest.
- ☐ Um dem Client eine IP-Adresse ohne Zeitbegrenzung zuzuweisen, legen Sie in Spalte *Lease-Time [s]* den Wert `4294967295` fest.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Öffnen Sie den Dialog *Erweitert > DHCP Server > Global*.
- ☐ Markieren Sie für Port `1/1` das Kontrollkästchen in Spalte *DHCP-Server aktiv*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dhcp-server pool add 1 static 192.168.23.42`	Erzeugen eines Eintrags mit Index `1` und Hinzufügen der IP-Adresse `192.168.23.42` zum statischen Pool.
`dhcp-server pool modify 1 mode interface 1/1`	Zuweisen der statischen Adresse des Eintrags mit Index `1` zu Interface `1/1`.
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	Zuweisen der IP-Adresse in Index `1` zu dem Gerät mit der MAC-Adresse `00:24:E8:D6:50:51`.
`dhcp-server pool mode 1`	Aktivieren des Pool-Eintrages mit Index `1`.
`dhcp-server pool modify 1 leasetime infinite`	Ändern des Eintrags mit Index `1` für die unbegrenzte Zuweisung der IP-Adresse zum Client.
`dhcp-server operation`	Globales Aktivieren des DHCP-Servers.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`dhcp-server operation`	Aktivieren der Funktion *DHCP Server* für diesen Port.

15.1.3 Beispiel: DHCP-Server – Dynamischer IP-Adressbereich

Das Gerät ermöglicht Ihnen, dynamische IP-Adressbereiche anzulegen. Lassen Sie die Felder *MAC-Adresse*, *Client-ID*, *Remote-ID* und *Circuit-ID* frei. Um dynamische IP-Adressbereiche mit Lücken zwischen den Bereichen anzulegen, fügen Sie der Tabelle mehrere Einträge hinzu. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DHCP Server > Pool*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche .
- ☐ Legen Sie in Spalte *IP-Adresse* den Wert `192.168.23.92` fest. Dies ist die erste IP-Adresse des Bereichs.
- ☐ Legen Sie in Spalte *Letzte IP-Adresse* den Wert `192.168.23.142` fest. Dies ist die letzte IP-Adresse des Bereichs.

Die Voreinstellung in Spalte *Lease-Time [s]* ist 60 Tage.

- ☐ Legen Sie in Spalte *Port* den Wert `1/2` fest.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Öffnen Sie den Dialog *Erweitert > DHCP Server > Global*.
- ☐ Markieren Sie für Port `1/2` das Kontrollkästchen in Spalte *DHCP-Server aktiv*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	Einfügen eines dynamischen Pools mit einem IP-Bereich von `192.168.23.92` bis `192.168.23.142`.
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	Einfügen der Lease Time in Sekunden bzw. als unbegrenzt.
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	Einfügen eines dynamischen Pools mit einem IP-Bereich von `192.168.23.172` bis `192.168.23.180`.
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	Einfügen der Lease Time in Sekunden bzw. als unbegrenzt.
`dhcp-server pool mode 2`	Aktivieren des Pool-Eintrages mit Index `2`.
`dhcp-server pool mode 3`	Aktivieren des Pool-Eintrages mit Index `3`.
`dhcp-server operation`	Globales Aktivieren des DHCP-Servers.
`interface 2/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `2/1`.
`dhcp-server operation`	Aktivieren der Funktion *DHCP Server* für diesen Port.

15.2 DHCP-L2-Relay

Auf der Frontblende des Gerätes finden Sie folgenden Gefahrenhinweis:

⚠ WARNUNG

UNBEABSICHTIGTER VORGANG

Ändern Sie die Kabelpositionen nicht, wenn DHCP Option 82 eingeschaltet ist. Lesen Sie vor der Wartung das Anwender-Handbuch.

Das Nicht-Beachten dieser Anweisungen kann zu Tod, schwerer Körperverletzung oder Materialschaden führen.

Ein Netzadministrator verwendet den DHCP-Schicht-2-*Relay-Agenten*, um DHCP-Client-Informationen hinzuzufügen. Schicht-3-*Relay-Agenten* und DHCP-Server benötigen diese Informationen, um einem Client eine Adresse und eine Konfiguration zuzuweisen.

Befinden sich ein DHCP-Client und -Server in demselben IP-Subnetz, erfolgt der Austausch von IP-Adressanfragen und IP-Adressantworten zwischen ihnen direkt. Der Einsatz eines DHCP-Servers für jedes Subnetz ist jedoch teuer und häufig unpraktisch. Eine Alternative, um den Einsatz eines DHCP-Servers für jedes Subnetz zu vermeiden, ist die Verwendung von Geräten im Netz zur Weiterleitung von Paketen zwischen einem DHCP-Client und einem DHCP-Server, der sich in einem anderen Subnetz befindet.

Bei einem Schicht-3-*Relay-Agenten* handelt es sich im Allgemeinen um einen Router, der IP-Schnittstellen sowohl in den Client- als auch in den Server-Subnetzen besitzt und den Datenverkehr zwischen ihnen weiterleitet. In Schicht-2-vermittelten Netzen jedoch befinden sich ein oder mehrere Geräte im Netz zwischen dem Client und dem Schicht-3-*Relay-Agenten* oder DHCP-Server, zum Beispiel Switches. In diesem Fall stellt das Gerät einen Schicht-2-*Relay-Agenten* bereit, um Informationen hinzuzufügen, die der Schicht-3-*Relay-Agent* und der DHCP-Server benötigen, um ihre Funktionen bei der Adress- und Konfigurationszuweisung zu erfüllen.

Die folgende Liste enthält die Voreinstellungen für diese Funktion:
- Allgemeine Einstellungen:
  - Aktive Einstellung: deaktivieren
- Schnittstelleneinstellungen:
  - Aktive Einstellung: deaktivieren
  - Gesicherter Port: deaktivieren
- VLAN-Einstellungen:
  - Aktive Einstellung: deaktivieren
  - *Circuit-ID*: aktivieren
  - *Remote-ID*-Typ: mac
  - *Remote-ID*: leer

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.

15.2.1 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.

15.2.2 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 *DHCP-L2-Relay* und in Spalte *Gesicherter Port* das Kontrollkästchen markiert ist. Typischerweise sind das Ports im Netz des DHCP-Servers.

Auf Ports, an denen die DHCP-Clients angeschlossen sind, aktivieren Sie die Funktion *DHCP-L2-Relay*, lassen das Kontrollkästchen in Spalte *Gesicherter Port* jedoch unmarkiert. Auf diesen Ports verwirft das Gerät DHCPv4-Pakete mit *Option 82*-Information 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.

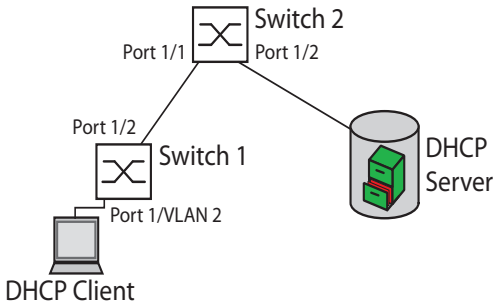


Abb. 75: Beispiel: DHCP-Schicht-2-Netz

Führen Sie an Switch 1 die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DHCP-L2-Relay > Konfiguration*, Registerkarte *Interface*.
- ☐ Legen Sie die Einstellungen für Port `1/1` wie folgt fest:
  - Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Legen Sie die Einstellungen für Port `1/2` wie folgt fest:
  - Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
  - Markieren Sie das Kontrollkästchen in Spalte *Gesicherter Port*.
- ☐ Öffnen Sie den Dialog *Erweitert > DHCP-L2-Relay > Konfiguration*, Registerkarte *VLAN-ID*.
- ☐ Legen Sie die Einstellungen für VLAN 2 wie folgt fest:
  - Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
  - Markieren Sie das Kontrollkästchen in Spalte *Circuit-ID*.
  - Um als *Remote-ID* die IP-Adresse des Geräts zu verwenden, legen Sie in Spalte *Remote-ID-Typ* den Wert `ip` fest.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Führen Sie an Switch 2 die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DHCP-L2-Relay > Konfiguration*, Registerkarte *Interface*.
- ☐ Legen Sie die Einstellungen für Port `1/1` und Port `1/2` wie folgt fest:
  - Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
  - Markieren Sie das Kontrollkästchen in Spalte *Gesicherter Port*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Vergewissern Sie sich, dass VLAN 2 vorhanden ist. Führen Sie dann an Switch 1 die folgenden Schritte aus:

☐ Richten Sie das VLAN 2 ein und legen Sie Port `1/1` als Mitglied des VLAN 2 fest.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`vlan database`	Wechsel in den VLAN-Konfigurationsmodus.
`dhcp-l2relay circuit-id 2`	Aktivieren der Circuit-ID und der DHCP-Option-82 in VLAN `2`.

`dhcp-l2relay remote-id ip 2`	Festlegen der IP-Adresse des Geräts als Remote-ID in VLAN `2`.
`dhcp-l2relay mode 2`	Aktivieren der Funktion *DHCP-L2-Relay* in VLAN `2`.
`exit`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`dhcp-l2relay mode`	Aktivieren der Funktion *DHCP-L2-Relay* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`dhcp-l2relay trust`	Festlegen des Ports als *Gesicherter Port*.
`dhcp-l2relay mode`	Aktivieren der Funktion *DHCP-L2-Relay* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`dhcp-l2relay mode`	Einschalten der Funktion *DHCP-L2-Relay* auf dem Gerät.

Führen Sie an Switch 2 die folgenden Schritte aus:

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`dhcp-l2relay trust`	Festlegen des Ports als *Gesicherter Port*.
`dhcp-l2relay mode`	Aktivieren der Funktion *DHCP-L2-Relay* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`dhcp-l2relay trust`	Festlegen des Ports als *Gesicherter Port*.
`dhcp-l2relay mode`	Aktivieren der Funktion *DHCP-L2-Relay* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`dhcp-l2relay mode`	Einschalten der Funktion *DHCP-L2-Relay* auf dem Gerät.

15.3 Gerät als DNS-Client verwenden

Der DNS-Client fordert die DNS-Server dazu auf, die Host-Namen und IP-Adressen von Geräten im Netz aufzulösen. Der DNS-Client konvertiert Namen von Geräten, ähnlich einem Telefonbuch, in IP-Adressen. Wenn der DNS-Client die Aufforderung erhält, einen neuen Namen aufzulösen, führt er die Abfrage der Informationen zunächst in seiner internen statischen Datenbank und anschließend in den zugewiesenen DNS-Servern durch. Der DNS-Client speichert die abgefragten Informationen in einem Cache-Speicher für zukünftige Anfragen.

Das Gerät ermöglicht Ihnen, den DNS-Client vom DHCP-Server über das Management-VLAN zu konfigurieren. Das Gerät ermöglicht Ihnen außerdem, die Hostnamen statisch den IP-Adressen zuzuordnen.

Der DNS-Client bietet folgende Benutzerfunktionen:
- DNS-Server-Liste mit Platz für bis zu 4 DNS-IP-Adressen.
- Mapping von statischen Host-Namen zu IP-Adressen mit Platz für bis zu 64 konfigurierbare statische Hosts
- Host-Cache mit Platz für 128 Einträge

15.3.1 Beispiel: DNS-Server konfigurieren

Geben Sie den Namen für den DNS-Client an, und konfigurieren Sie diesen so, dass er einen DNS-Server dazu auffordert, Host-Namen aufzulösen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DNS > Client > Statisch*.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Konfigurationsquelle* den Wert `user` fest.
- ☐ Legen Sie im Rahmen *Konfiguration*, Feld *Domänen-Name* den Wert `device1` fest.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche  .
- ☐ Legen Sie in Spalte *Adresse* den Wert `192.168.3.5` als IPv4-Adresse des DNS-Servers fest. Sie können ebenfalls eine gültige IPv6-Adresse als IP-Adresse des DNS-Servers festlegen.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Öffnen Sie den Dialog *Erweitert > DNS > Client > Global*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dns client source user`	Festlegen, dass der Benutzer die Einstellungen des DNS-Clients manuell festlegt.
`dns client domain-name devicel`	Festlegen der Zeichenfolge `device1` als eindeutigen Domänennamen für das Gerät.
`dns client servers add 1 ip 192.168.3.5`	Hinzufügen eines DNS-Namensservers mit einer IPv4-Adresse von `192.168.3.5` als Index `1`.
`dns client servers add 2 ip 2001::1`	Hinzufügen eines DNS-Servers mit einer IPv6-Adresse von `2001::1` als Index `2`.
`dns client adminstate`	Die Funktion *DNS-Client* global einschalten.

Konfigurieren Sie den DNS-Client so, dass er statische Hosts mit IP-Adressen abbildet. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Erweitert > DNS > Client > Statische Hosts*.
- ☐ Um einen Tabelleneintrag hinzuzufügen, klicken Sie die Schaltfläche  .
- ☐ Fügen Sie in Spalte *Name* den Wert `example.com` ein.
  Dabei handelt es sich um den Namen eines Geräts im Netz.
- ☐ Legen Sie in Spalte *IP-Adresse* den Wert `192.168.3.9` fest.
- ☐ Markieren Sie das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche  .

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`dns client host add 1 name example.com ip 192.168.3.9`	Hinzufügen des statischen Hosts `example.com` mit IP-Adresse `192.168.3.9`.
`dns client adminstate`	Die Funktion *DNS-Client* global einschalten.

15.4 GARP

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

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

15.4.1 GMRP konfigurieren

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

Anmerkung: Vergewissern Sie sich vor dem Einschalten der Funktion *GMRP*, dass die Funktion *MMRP* ausgeschaltet ist.

Das folgende Beispiel beschreibt die Konfiguration der Funktion *GMRP*. Das Gerät unterstützt eingeschränktes Multicast-Flooding für einen ausgewählten Port. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > GARP > GMRP*.
- ☐ Um eingeschränktes Multicast Flooding an einem Port auszuführen, markieren Sie das Kontrollkästchen in Spalte *GMRP aktiv*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`garp gmrp operation`	Einschalten der Funktion *GMRP* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`garp gmrp operation`	Globales Einschalten der Funktion *GMRP*.

15.4.2 GVRP konfigurieren

Verwenden Sie die Funktion *GVRP*, um dem Gerät das Austauschen von VLAN-Konfigurationsinformationen mit anderen *GVRP*-Geräten zu ermöglichen. Auf diese Weise reduziert das Gerät unnötigen Broadcast-Verkehr und unbekannten Unicast-Verkehr. Außerdem erzeugt und verwaltet die Funktion *GVRP* dynamisch VLANs auf Geräten, die über 802.1Q-Trunk-Ports angeschlossen sind.

Das folgende Beispiel beschreibt die Konfiguration der Funktion *GVRP*. Das Gerät ermöglicht Ihnen, VLAN-Konfigurationsinformationen mit anderen *GVRP*-Geräten auszutauschen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > GARP > GVRP*.
- ☐ Um VLAN-Konfigurationsinformationen mit anderen *GVRP*-Geräten auszutauschen, markieren Sie das Kontrollkästchen in Spalte *GVRP aktiv* für den Port.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 3/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `3/1`.
`garp gvrp operation`	Einschalten der Funktion *GVRP* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`garp gvrp operation`	Globales Einschalten der Funktion *GVRP*.

15.5 MRP-IEEE

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

Um den Verkehr auf die erforderlichen Bereiche eines Netzes zu begrenzen, verteilen die MRP-Anwendungen Attribut-Werte an Geräte mit eingeschaltetem MRP innerhalb eines LANs. Die MRP-Anwendungen registrieren und deregistrieren Multicast-Gruppenmitgliedschaften und VLAN-Kennungen.

Anmerkung: Das Multiple-Registration-Protokoll (MRP) erfordert ein Loop-freies Netz. Um die Möglichkeit von Loops in Ihrem Netz zu verringern, verwenden Sie ein Netzprotokoll wie das Media-Redundancy-Protokoll, das Spanning-Tree-Protokoll oder das Spanning-Tree-Protokoll mit MRP.

15.5.1 MRP-Funktion

Jeder Teilnehmer enthält eine Anwendungskomponente und eine MRP-Attribute-Declaration(MAD)-Komponente. Die Anwendungskomponente ist verantwortlich für das Bilden der Attribute sowie deren Registrierung und Deregistrierung. Die MAD-Komponente erzeugt MRP-Nachrichten für die Vermittlung und verarbeitet empfangene Nachrichten anderer Teilnehmer. Die MAD-Komponente kodiert und vermittelt die Attribute an andere Teilnehmer in MRP-Dateneinheiten (MRPDU). Im Switch verteilt eine MRP-Attribute-Propagation(MAP)-Komponente die Attribute an teilnehmende Ports.

Für jede MRP-Anwendung und jedes LAN existiert ein Teilnehmer. Zum Beispiel befindet sich eine Teilnehmeranwendung auf einem Endgerät und eine weitere auf dem Port des Switches. Die Applicant-State-Machine erfasst das Attribut und den Port jeder Anmeldung eines MRP-Teilnehmers an einem Endgerät oder Switch. Änderungen von Variablen der Applicant-State-Machine lösen die Vermittlung von MRPDUs aus, um die Anmeldung oder Rücknahme mitzuteilen.

Um eine *MMRP*-Instanz zu erzeugen, sendet ein Endgerät zunächst eine Join-Emty(JointMt)-Nachricht mit den entsprechenden Attributen. Der Switch flutet dann die JoinMt-Nachricht an den teilnehmenden Ports und den benachbarten Switches. Die benachbarten Switches fluten die Nachricht an ihren teilnehmenden Port und so weiter, wodurch ein Pfad für den Gruppen-Verkehr entsteht.

15.5.2 MRP-Timer

Die Timer-Voreinstellungen helfen, unnötige Attribut-Anmeldungen und -rücknahmen zu vermeiden. Die Timer-Einstellungen ermöglichen den Teilnehmern, MRP-Nachrichten vor Ablauf der Leave- oder LeaveAll-Timer zu empfangen und zu verarbeiten.

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

- Für eine erneute Registrierung nach einem Leave- oder LeaveAll-Ereignis – auch im Fall einer verlorenen Nachricht – legen Sie den Wert für LeaveTime wie folgt fest: ≥ (2x JoinTime) + 60 in 1/100 s
- Um das Volumen des nach einem LeaveAll-Ereignis neu hinzukommenden Verkehrs zu minimieren, legen Sie für den LeaveAll-Timer einen Wert fest, der höher ist als die LeaveTime.

Die folgende Liste enthält verschiedene vom Gerät übertragene MRP-Ereignisse.

- Join – Überwacht den Intervall für die nächste Join-Message-Übertragung
- Leave – Überwacht den Zeitraum, den ein Switch vor dem Wechsel in den Rücknahme-Status im Leave-Status bleibt.
- LeaveAll – Überwacht die Frequenz, mit welcher der Switch LeaveAll-Nachrichten erzeugt.

Der Periodic-Timer löst nach Ablauf eine MRP-Nachricht mit einem Join-Request aus, die der Switch an LAN-Teilnehmer sendet. Mit dieser Nachricht vermeiden Switches unnötige Rücknahmen.

15.5.3 MMRP

Wenn ein Gerät Broadcast-, Multicast- oder unbekannte Daten an einem Port empfängt, flutet das Gerät die Daten an andere Ports. Dieser Vorgang beansprucht unnötig Bandbreite im LAN.

Das Multiple-MAC-Registration-Protokoll (*MMRP*) ermöglicht Ihnen, das Fluten von Daten mit dem Verteilen einer Attribut-Anmeldung an LAN-Teilnehmer zu überwachen. Die Attribut-Werte sind Informationen von Gruppen-Dienst-Anforderungen und 48-Bit-MAC-Adressen und werden von der MAD-Komponente kodiert und über MRP-Nachrichten an das LAN vermittelt.

Der Switch speichert die Attribute in einer Filterdatenbank als MAC-Adressen-Registrierungs-Einträge. Der Weiterleitungsprozess verwendet die Filterdatenbank-Einträge ausschließlich zur Vermittlung von Daten über diejenigen Ports, die zum Erreichen von LANs, die Gruppen-Mitglieder sind, notwendig sind.

Switches ermöglichen Mechanismen zur Verteilung in Gruppen, denen auf der Grundlage des Open-Host-Konzeptes, wobei sie Pakete an den aktiven Ports empfangen und sie ausschließlich an Ports weiterleiten, die Gruppen-Mitglieder sind. Auf diese Weise beantragt jeder *MMRP*-Teilnehmer mit an eine oder mehrere bestimmte Gruppen zu sendenden Paketen die Mitgliedschaft in der Gruppe. Nutzer von MAC-Diensten senden Pakete an eine bestimmte Gruppe von einem beliebigen Punkt im LAN. Eine Gruppe empfängt diese Pakete in den LANs, die an registrierte *MMRP*-Teilnehmer angebunden sind. *MMRP* und die MAC-Address-Registration-Einträge beschränken so die Pakete auf die erforderlichen Segmente eines Loop-freien LANs.

Um Registrierungs- und Deregistrierungsstatus aufrecht zu erhalten und Daten zu empfangen, erklärt ein Port periodisch sein Interesse. Jedes Gerät mit eingeschalteter Funktion *MMRP* in einem LAN führt eine Filterdatenbank und leitet Daten mit den Gruppen-MAC-Adressen an die aufgeführten Teilnehmer weiter.

MMRP-Beispiel

In diesem Beispiel erwartet Host A für die Gruppe G1 bestimmte Daten. Switch A verarbeitet die *MMRP*-Join-Anfrage von Host A und sendet die Anfrage an beide benachbarte Switches. Die Geräte im LAN erkennen nun, dass ein Host auf den Empfang von Daten für Gruppe G1 bereit ist. Wenn Host B beginnt, die für Gruppe G1 bestimmten Daten zu vermitteln, fließen die Daten auf dem registrierten Pfad und Host A empfängt sie.

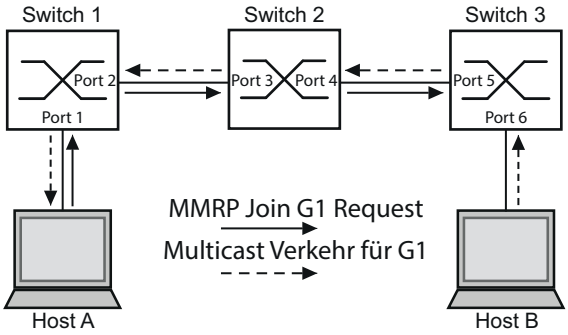


Abb. 76: MMRP-Netz für MAC-Adressen-Registrierung

Schalten Sie die *MMRP*-Funktion auf den Switches ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > MRP-IEEE > MMRP*, Registerkarte *Konfiguration*.
- ☐ Um Port `1` und Port `2` als *MMRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte *MMRP* für Port `1` und Port `2`.
- ☐ Um Port `3` und Port `4` als *MMRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 2 das Kontrollkästchen in Spalte *MMRP* für Port `3` und Port `4`.
- ☐ Um Port `5` und Port `6` als *MMRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 3 das Kontrollkästchen in Spalte *MMRP* für Port `5` und Port `6`.
- ☐ Um periodische Ereignisse zu senden, damit das Gerät die Anmeldung der MAC-Adressen-Gruppe aufrecht erhält, schalten Sie *Periodische State-Machine* ein. Wählen Sie im Rahmen *Konfiguration* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✔.

Um die *MMRP*-Ports an Switch 1 einzuschalten, verwenden Sie die folgenden Kommandos. Schalten Sie die Funktion *MMRP* und Ports an den Switches 2 und 3 ein, indem sie in den Kommandos die entsprechenden Interfaces ersetzen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/1`.
`mrp-ieee mmrp operation`	Einschalten der Funktion *MMRP* auf dem Port.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface `1/2`.
`mrp-ieee mmrp operation`	Einschalten der Funktion *MMRP* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`mrp-ieee mrp periodic-state-machine`	Globales Einschalten der Funktion *Periodische State-Machine*.
`mrp-ieee mmrp operation`	Globales Einschalten der Funktion *MMRP*.

15.5.4 MVRP

Das Multiple-VLAN-Registration-Protokoll (*MVRP*) ist eine MRP-Anwendung, die Dienste für die dynamische VLAN-Registrierung und -rücknahme bietet.

Die Funktion *MVRP* bietet einen Mechanismus zur Erhaltung der dynamischen VLAN-Registration-Einträge und zur Vermittlung der Information an andere Geräte. Diese Information ermöglicht *MVRP*-fähigen Geräten, Informationen zu Ihrer VLAN-Mitgliedschaft zu erzeugen und zu aktualisieren. Wenn Mitglieder in einem VLAN angemeldet sind, geben diese Informationen Auskunft, über welche Ports der Switch die Daten an diese Mitglieder weiterleitet.

Hauptaufgabe der Funktion *MVRP* ist, Switches zu ermöglichen, einige der VLAN-Informationen zu ermitteln, die Sie anderenfalls manuell festlegen. Das Ermitteln dieser Informationen ermöglicht Switches, Einschränkungen beim Bandbreitenverbrauch und bei der Konvergenzzeit in großen VLAN-Netzen zu bewältigen.

MVRP-Beispiel

Richten Sie ein Netz mit MVRP-fähigen Switches (1 – 4) ein, die in Ring-Topologie mit Endgerätegruppen verbunden sind; A1, A2, B1 und B2 in den 2 verschiedenen VLANs A und B. Wenn an den Switches STP eingeschaltet ist, sind die Ports, die Switch 1 und Switch 4 verbinden, zur Vermeidung von Loops im „Discarding“-Status.

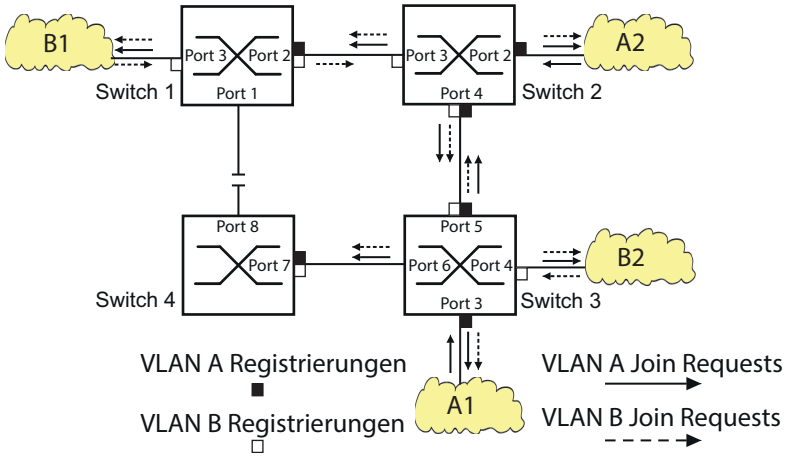


Abb. 77: MVRP-Beispiel-Netz für VLAN-Registrierung

Im MVRP-Beispiel-Netz senden die LANs zunächst eine Join-Anfrage an die Switches. Der Switch trägt die VLAN-Registrierung in die Adresstabelle (Forwarding Database) für den Port ein, der die Daten empfängt.

Der Switch verbreitet die Anfrage an die anderen Ports und sendet die Anfrage an die benachbarten LANs und Switches. Dieser Prozess hält an, bis die Switches die VLANs in die Adresstabelle des Empfangs-Ports eingefügt haben.

Schalten Sie MVRP auf den Switches ein. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > MRP-IEEE > MVRP*, Registerkarte *Konfiguration*.
- ☐ Um die Ports 1 bis 3 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 1 das Kontrollkästchen in Spalte *MVRP* für die Ports 1 bis 3.
- ☐ Um die Ports 2 bis 4 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 2 das Kontrollkästchen in Spalte *MVRP* für die Ports 2 bis 4.

- ☐ Um die Ports 3 bis 6 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 3 das Kontrollkästchen in Spalte *MVRP* für die Ports 3 bis 6.
- ☐ Um Port 7 und Port 8 als *MVRP*-Teilnehmer zu aktivieren, markieren Sie an Switch 4 das Kontrollkästchen in Spalte *MVRP* für Port 7 und Port 8.
- ☐ Um die Registrierung der VLANs zu aufrecht zu erhalten, schalten Sie die *Periodische State-Machine* ein.
  Wählen Sie im Rahmen *Konfiguration* das Optionsfeld *An*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ☑.

Um die *MVRP*-Ports an Switch 1 einzuschalten, verwenden Sie die folgenden Kommandos. Schalten Sie die Funktionen *MVRP* und Ports an den Switches 2, 3 und 4 ein, indem Sie in den Kommandos die entsprechenden Interfaces ersetzen.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`interface 1/1`	Wechsel in den Interface-Konfigurationsmodus von Interface 1/1.
`mrp-ieee mvrp operation`	Einschalten der Funktion *MVRP* auf dem Port.
`interface 1/2`	Wechsel in den Interface-Konfigurationsmodus von Interface 1/2.
`mrp-ieee mvrp operation`	Einschalten der Funktion *MVRP* auf dem Port.
`exit`	Wechsel in den Konfigurationsmodus.
`mrp-ieee mvrp periodic-state-machine`	Globales Einschalten der Funktion *Periodische State-Machine*.
`mrp-ieee mvrp operation`	Globales Einschalten der Funktion *MVRP*.

16 Industrieprotokolle

16.1 IEC 61850/MMS

IEC 61850/MMS ist ein von der International Electrotechnical Commission (IEC) standardisiertes industrielles Kommunikationsprotokoll. Anzutreffen ist das Protokoll in der Schaltanlagenautomatisierung, zum Beispiel in der Leittechnik von Energieversorgern.

Das paketorientiert arbeitende Protokoll basiert auf dem Transportprotokoll TCP/IP und nutzt Manufacturing Messaging Specification (MMS) für die Client-Server-Kommunikation. Das Protokoll ist objektorientiert und definiert eine einheitliche Konfigurationssprache, die u.a. Funktionen für SCADA, Intelligent Electronic Devices (IED) und für die Netzleittechnik umfasst.

Teil 6 der Norm IEC 61850 definiert die Konfigurationssprache SCL (Substation Configuration Language). SCL beschreibt die Eigenschaften des Geräts sowie die Systemstruktur in maschinell verarbeitbarer Form. Die mit SCL beschriebenen Eigenschaften des Geräts sind in der ICD-Datei auf dem Gerät gespeichert.

16.1.1 Switch-Modell für IEC 61850

Der Technical Report IEC 61850 90-4 spezifiziert ein Bridge-Modell. Die Funktionen eines Switches bildet das Bridge-Modell als Objekte eines Intelligent Electronic Devices (IED) ab. Ein MMS-Client (zum Beispiel die Leitstellen-Software) verwendet diese Objekte, um das Gerät zu überwachen und zu konfigurieren.

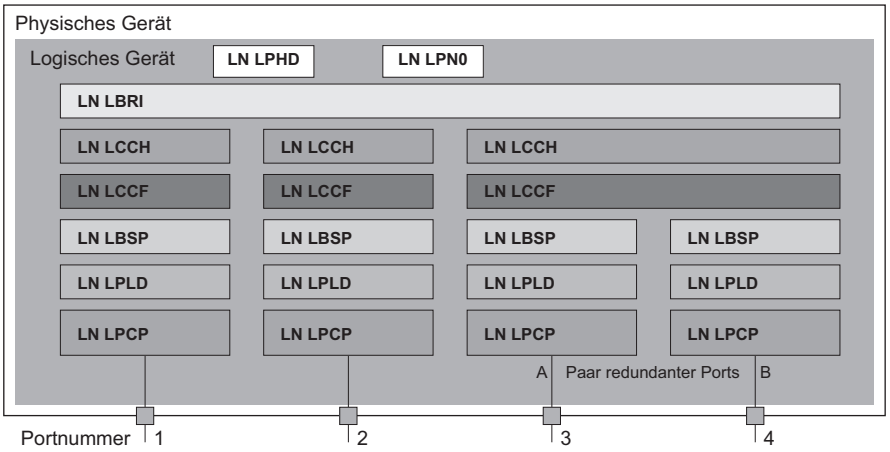


Abb. 78: Bridge-Modell nach Technical Report IEC 61850 90-4

Tab. 59: Klassen des Bridge-Modells nach TR IEC61850 90-4

Klasse	Beschreibung
LN LLN0	Logischer Knoten Zero des IED Bridge: Definiert die logischen Eigenschaften des Geräts.
LN LPHD	Logischer Knoten Physical Device des IED Bridge: Definiert die physischen Eigenschaften des Geräts.
LN LBRI	Logischer Knoten Bridge: Bildet generelle Einstellungen der Bridge-Funktionen des Geräts ab.
LN LCCH	Logischer Knoten Communication Channel: Definiert den logischen Communication Channel, der aus einem oder mehreren physischen Geräteports besteht.
LN LCCF	Logischer Knoten Channel Communication Filtering: Definiert die VLAN- und Multicast-Einstellungen für den übergeordneten Communication Channel.
LN LBSP	Logischer Knoten Port Spanning Tree Protocol: Definiert die Spanning-Tree-Zustände und -Einstellungen für den jeweiligen physischen Geräteport.
LN LPLD	Logischer Knoten Port Layer Discovery: Definiert die LLDP-Zustände und -Einstellungen für den jeweiligen physischen Geräteport.
LN LPCP	Logischer Knoten Physical Communication Port: Repräsentiert den jeweiligen physischen Geräteport.

16.1.2 Integration in ein Steuerungssystem

Vorbereitung des Geräts

Führen Sie die folgenden Schritte aus:

- ☐ Vergewissern Sie sich, dass dem Gerät eine IP-Adresse zugewiesen ist.
- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > IEC61850-MMS*.
- ☐ Um den MMS-Server zu starten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An* und klicken die Schaltfläche ☑.
  Anschließend ist ein MMS-Client in der Lage, sich mit dem Gerät zu verbinden sowie die im Bridge-Modell definierten Objekte auszulesen und zu überwachen.

IEC61850/MMS bietet keine Authentifizierungsmechanismen. Wenn der Schreibzugriff für IEC61850/MMS eingeschaltet ist, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Geräts zu ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Geräts und zu möglichen Problemen im Netz.

HINWEIS
GEFAHR DES UNAUTORISIERTEN ZUGRIFFS AUF DAS GERÄT Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (zum Beispiel Firewall, VPN etc.) getroffen haben, um die Möglichkeit eines unbefugten Zugriffs zu verringern. **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 zu konfigurieren.

- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > IEC61850-MMS*.
- ☐ Um die ICD-Datei auf Ihren PC zu laden, klicken Sie die Schaltfläche ☰ und dann den Eintrag *Download*.

Gerät überwachen

Der im Gerät integrierte IEC61850/MMS-Server 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. 60: Mit IEC 61850/MMS überwachbare Stati des Geräts

Klasse	RCB-Objekt	Beschreibung
LN LPHD	TmpAlm	Ändert sich, wenn die im Gerät gemessene Temperatur die festgelegten Temperaturschwellen über- oder unterschreitet.
	PhyHealth	Ändert sich, wenn sich der Status des RCB-Objekts LPHD.TmpAlm ändert.
LN LPHD	TmpAlm	Ändert sich, wenn die im Gerät gemessene Temperatur die festgelegten Temperaturschwellen über- oder unterschreitet.
	PwrSupAlm	Ändert sich, wenn eine der redundanten Spannungsversorgungen ausfällt oder wieder in Betrieb geht.
	PhyHealth	Ändert sich, wenn sich der Status der RCB-Objekte LPHD.PwrSupAlm oder LPHD.TmpAlm ändert.

Tab. 60: 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.

16.2 Modbus TCP

Modbus TCP ist ein Nachrichtenprotokoll auf der Anwendungsschicht, das eine Client-/Server-Kommunikation zwischen dem Client und den in Ethernet-TCP/IP-Netzen verbundenen Geräten herstellt.

Die Funktion *Modbus TCP* ermöglicht Ihnen, das Gerät in Netzen zu installieren, die bereits *Modbus TCP* verwenden, und die in den Registern auf dem Gerät gespeicherten Informationen abzurufen.

16.2.1 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.

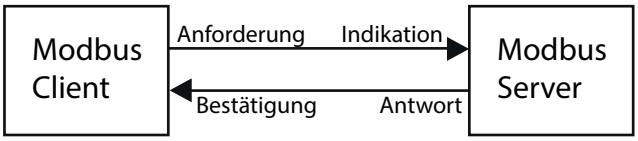


Abb. 79: Modbus TCP/IP Client/Server-Modus

Um Daten zwischen dem Client und dem Server auszutauschen, verwendet das Client/Server-Modell 4 Nachrichtentypen:

- Modbus TCP/IP-Anfrage; der Client erzeugt eine Informationsanforderung und sendet sie an den Server.
- Modbus TCP/IP-Hinweis; der Server empfängt eine Anfrage als Hinweis, dass ein Client Informationen anfordert.
- Modbus TCP/IP-Antwort; wenn die angeforderten Informationen verfügbar sind, sendet der Server eine Antwort mit den angeforderten Informationen. Wenn die angeforderten Informationen nicht verfügbar sind, sendet der Server eine Ausnahmeantwort, um den Client über den während der Verarbeitung erkannten Fehler zu benachrichtigen. Die Ausnahmeantwort enthält einen Ausnahmecode, der die Ursache des erkannten Fehlers angibt.
- Modbus TCP/IP-Bestätigung; der Client empfängt eine Antwort vom Server mit den angeforderten Informationen.

16.2.2 Unterstützte Funktionen und Speicherzuordnung

Das Gerät unterstützt Funktionen mit den öffentlichen Codes `0x03` (`Read Holding Registers`) und `0x05` (`Write Single Coil`). Die Codes ermöglichen Ihnen, in den Registern gespeicherte Informationen zu lesen, zum Beispiel Systeminformationen einschließlich Systemname, Systemstandort, Software-Version, IP-Adresse und MAC-Adresse. Die Codes ermöglichen Ihnen außerdem, die Port-Informationen und die Port-Statistik zu lesen. Der Code `0x05` ermöglicht Ihnen, die Port-Zähler einzeln oder global zurückzusetzen.

Die folgende Liste enthält Informationen zu den in die Spalte `Format` eingetragenen Werten:

- Bitmap: Eine Gruppe von 32 Bits, codiert in der Big-Endian-Byte-Reihenfolge und gespeichert in 2 Registern. Big-Endian-Systeme speichern das höchstwertige Byte eines Wortes in der kleinsten Adresse und das niedrigstwertige Byte in der größten Adresse.
- F1: 16-bit unsigned integer

- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply failure detected
- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On
- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted Pair (TP)
  - 2 = Fiber - 10 Mb/s
  - 3 = Fiber - 100 Mb/s
  - 4 = Giga - 10/100/1000 Mb/s (triple speed)
  - 5 = Giga - Copper 1000 Mb/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- Zeichenfolge: Oktette, in Sequenz gespeichert, 2 Oktette je Register.

Modbus TCP/IP-Codes

Die folgende Tabelle enthält Adressen, die dem Client ermöglichen, Port-Zähler zurückzusetzen und spezifische Informationen aus den Geräteregistern abzurufen.

Port-Informationen

Tab. 61: Port-Informationen

Adresse	Menge	Beschreibung	Min	Max	Schritt	Einheit	Format
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

Port-Statistik

Tab. 62: Port-Statistik

Adresse	Menge	Beschreibung	Min	Max	Schritt	Einheit	Format
0800	1	Port1 - Number of bytes received	0	4294967295	1	-	F9
0802	1	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	1	Port1 - Number of frames received	0	4294967295	1	-	F9
0806	1	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	1	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	1	Port1 - Total frames received	0	4294967295	1	-	F9
080C	1	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	1	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	1	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	1	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	1	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	1	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	1	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	1	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	1	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	1	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	1	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	1	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	1	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	1	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	1	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	1	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	1	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	1	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	1	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
147E	1	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

16.2.3 Beispiel-Konfiguration

In diesem Beispiel konfigurieren Sie das Gerät so, dass es auf Client-Anfragen antwortet. Voraussetzung für diese Konfiguration ist, dass das Client-Gerät mit einer IP-Adresse aus dem angegebenen Bereich konfiguriert ist. In diesem Beispiel bleibt die Funktion *Schreibzugriff* deaktiviert. Wenn Sie die Funktion *Schreibzugriff* aktivieren, ermöglicht das Gerät Ihnen ausschließlich, die Port-Zähler zurückzusetzen. In der Standardkonfiguration sind die Funktionen *Modbus TCP* und *Schreibzugriff* inaktiv.

Das *Modbus TCP*-Protokoll bietet keine Authentifizierungsmechanismen. Ist der Schreibzugriff für *Modbus TCP* eingeschaltet, dann ist jeder Client, der das Gerät per TCP/IP erreicht, in der Lage, die Einstellungen des Geräts zu ändern. Dies wiederum führt möglicherweise zur Fehlkonfiguration des Geräts und zu möglichen Problemen im Netz.

HINWEIS

GEFAHR DES UNAUTORISIERTEN ZUGRIFFS AUF DAS GERÄT

Schalten Sie den Schreibzugriff ausschließlich dann ein, wenn Sie zusätzliche Maßnahmen (zum Beispiel Firewall, VPN etc.) getroffen haben, um die Möglichkeit eines unbefugten Zugriffs zu verringern.

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 einen neuen Tabelleneintrag hinzu. Klicken Sie dazu die Schaltfläche .
- ☐ Legen Sie den IP-Adressbereich in der Zeile fest, in der die Spalte *Index* den Wert `2` hat. Fügen Sie dazu die folgenden Werte ein:
  - In Spalte *Adresse*: `10.17.1.0`
  - In Spalte *Netzmaske*: `255.255.255.248`
- ☐ Vergewissern Sie sich, dass das Kontrollkästchen in Spalte *Modbus TCP* markiert ist.
- ☐ Aktivieren Sie den IP-Adressbereich. Markieren Sie dazu das Kontrollkästchen in Spalte *Aktiv*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .
- ☐ Öffnen Sie den Dialog *Diagnose > Statuskonfiguration > Sicherheitsstatus*, Registerkarte *Global*.
- ☐ Vergewissern Sie sich, dass das Kontrollkästchen für den Parameter *Modbus TCP aktiv* markiert ist.
- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > Modbus TCP*.
- ☐ Voreingestellt ist der standardmäßige *Modbus TCP*-Lausch-Port, Port `502`. Wenn Sie an einem anderen TCP-Port lauschen möchten, geben Sie den Wert für den Lausch-Port in das Feld *TCP-Port* ein.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche .

Wenn Sie die Funktion *Modbus TCP* einschalten, erkennt die Funktion *Sicherheitsstatus* die Aktivierung und zeigt einen Alarm im Dialog *Grundeinstellungen > System*, Rahmen *Sicherheits-Status*.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`network management access add 2`	Erzeugt den Eintrag für den Adressbereich im Netz. Nummer des nächsten verfügbaren Indexes in diesem Beispiel: `2`.
`network management access modify 2 ip 10.17.1.0`	Legt die IP-Adresse fest.
`network management access modify 2 mask 29`	Legt die Netzmaske fest.
`network management access modify 2 modbus-tcp enable`	Legt fest, dass das Gerät *Modbus TCP* Zugriff auf das Management des Geräts ermöglicht.
`network management access operation`	Schaltet die IP-Zugriffsbeschränkung ein.
`configure`	Wechsel in den Konfigurationsmodus.
`security-status monitor modbus-tcp-enabled`	Legt fest, dass das Gerät die Aktivierung des *Modbus TCP*-Servers überwacht.
`modbus-tcp operation`	Schaltet den *Modbus TCP*-Server ein.
`modbus-tcp port <1..65535>`	Den TCP-Port für die *Modbus TCP*-Kommunikation festlegen (optional). Voreingestellt ist Port `502`.
`show modbus-tcp`	Die *Modbus TCP*-Server-Einstellungen anzeigen.

```
Modbus TCP/IP server settings
-------------------------
Modbus TCP/IP server operation.................enabled
Write-access...................................disabled
Listening port.................................502
Max number of sessions.........................5
Active sessions................................0
```

`show security-status monitor`	Die Sicherheitsstatus-Einstellungen anzeigen.

```
Device Security Settings
Monitor
---------------------------------
Password default settings unchanged...........monitored
...
Write access using Ethernet Switch Configurator is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled......................monitored
Modbus TCP/IP server active...................monitored
```

`show security-status event`	Die aufgetretenen Sicherheitsstatus-Ereignisse anzeigen.

```
Time stamp             Event                        Info
--------------------   ----------------------    ------
2014-01-01 01:00:39   password-change(10)           -
.................................................
2014-01-01 01:00:39   ext-nvm-load-unsecure(21)     -
2014-01-01 23:47:40   modbus-tcp-enabled(23)        -
show network management access rules 1
```

Zeigen Sie die Regeln für den eingeschränkten Management-Zugriff für Index 1.

```
Restricted management access settings
-------------------------------------
Index.....................................1
IP Address................................10.17.1.0
Prefix Length.............................29
HTTP......................................yes
SNMP......................................yes
Telnet....................................yes
SSH.......................................yes
HTTPS.....................................yes
IEC61850-MMS..............................yes
Modbus TCP/IP.............................yes
Active....................................[x]
```

16.3 EtherNet/IP

EtherNet/IP ist ein weltweit akzeptiertes, standardisiertes industrielles Kommunikationsprotokoll, das von der Open DeviceNet Vendor Association (ODVA) gepflegt wird. Das Protokoll basiert auf den weit verbreiteten Standard-Ethernet-Übertragungsprotokollen TCP/IP und UDP/IP. *EtherNet/IP* wird von führenden Herstellern unterstützt und bietet daher eine breite Grundlage für den effektiven Datenverkehr im Industriebereich.

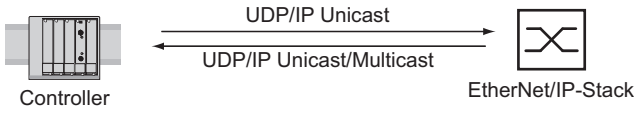


Abb. 80: EtherNet/IP-Netz

EtherNet/IP erweitert die Standard-Ethernet-Protokolle um das Industrieprotokoll CIP (Common Industrial Protocol). *EtherNet/IP* implementiert CIP in der Sitzungsschicht und darüber und passt CIP der spezifischen *EtherNet/IP*-Technologie in der Transportschicht und darunter an. Bei Automationsanwendungen implementiert *EtherNet/IP* CIP auf Anwendungsebene. Daher ist *EtherNet/IP* optimal für den Bereich der industriellen Steuerungstechnik geeignet.

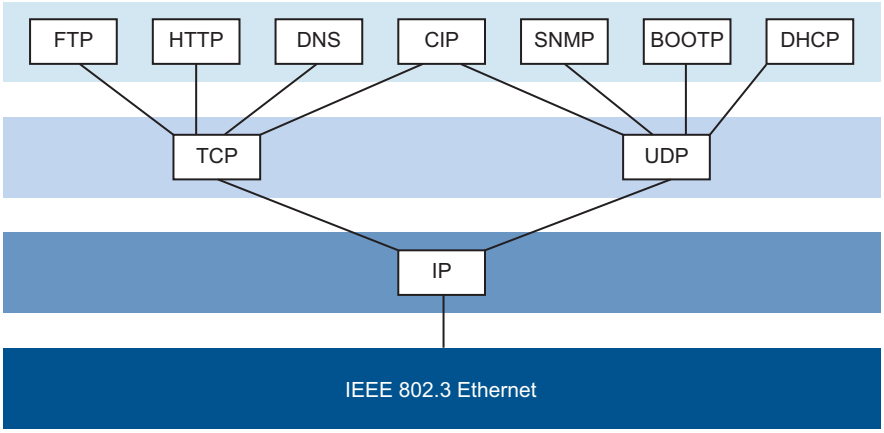


Abb. 81: IEEE802.3 EtherNet/IP

Ausführliche Informationen zu *EtherNet/IP* finden Sie auf der ODVA-Webseite unter www.odva.org.

16.3.1 Integration in ein Steuerungssystem

Führen Sie die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Switching > IGMP-Snooping > Global*.
  Vergewissern Sie sich, dass die Funktion *IGMP-Snooping* eingeschaltet ist.
- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > EtherNet/IP*.
  Vergewissern Sie sich, dass die Funktion *EtherNet/IP* eingeschaltet ist.
- ☐ Öffnen Sie den Dialog *Erweitert > Industrie-Protokolle > EtherNet/IP*.
- ☐ Um das EDS als ZIP-Archiv auf Ihrem PC zu speichern, klicken Sie *Download*.
  Das ZIP-Archiv enthält die *EtherNet/IP*-Konfigurationsdatei und das Symbol, über das eine Verbindung zwischen der Steuerung und dem Gerät konfiguriert wird.

16.3.2 EtherNet/IP-Entity-Parameter

Die folgenden Absätze identifizieren die Objekte und Operationen, die das Gerät unterstützt.

Unterstützte Operationen

Tab. 63: Übersicht über die unterstützten Etnernet/IP-Requests für die Objektinstanzen.

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: USINT VlanId ARRAY of: 6 USINT Mac DWORD PortMask	–

Identity-Objekt

Das Gerät unterstützt das Identity-Objekt (Class Code 0x01) von *EtherNet/IP*. Die Hersteller-ID von Schneider Electric lautet 634. Zur Kennzeichnung des Produkttyps „Schneider Electric“ verwendet 44 (0x2C) die ID Managed Ethernet Switch.

Tab. 64: Instanz-Attribute (ausschließlich Instanz 1 ist verfügbar)

Id	Attribute	Access Rule	Data type	Description
0x1	Vendor ID	Get	UINT	Schneider Electric634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type
0x4	Revision	Get	STRUCT of: USINT Major USINT Minor	Revision of the EtherNet/IP implementation, 2.1.
0x5	Status	Get	WORD	Support for the following Bit status only: 0: Owned (always 1) 2: Configured (always 1) 4: Extend Device Status 5: 0x3: No I/O connection established 6: 0x7: At least one I/O connection established, all in idle mode. 7:
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Schneider Electric" + product family + product ID + software variant.

TCP/IP Interface Object

Das Gerät unterstützt ausschließlich Instanz 1 des TCP/IP-Objektes (Class Code 0xF5) von *EtherNet/IP*.

In Abhängigkeit vom Schreibzugriff-Status speichert das Gerät die vollständige Konfiguration im Flash-Speicher des Geräts. Das Speichern der Konfigurationsdatei kann bis zu 10 Sekunden in Anspruch nehmen. Wird der Speichervorgang unterbrochen, zum Beispiel aufgrund eines nicht mehr funktionierenden Netzteils, ist der Betrieb des Geräts wahrscheinlich nicht möglich.

Anmerkung: Das Gerät reagiert auf die Konfigurationsänderung `Get Request` mit einer `Response`, selbst wenn der Speichervorgang für die Konfiguration noch nicht abgeschlossen ist.

Tab. 65: Class-Attribute

Id	Attribute	Access Rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances currently created: 1

Tab. 66: Attribute der Instanz 1

Id	Attribute	Access Rule	Data type	Description
0x1	Status	Get	DWORD	0: Interface Status (0=Interface not configured, 1=Interface contains valid config)
				6: ACD status (default 0)
				7: ACD fault (default 0)
0x2	Interface Capability flags	Get	DWORD	0: BOOTP Client
				1: DNS Client
				2: DHCP Client
				3: DHCP-DNS Update
				4: Configuration setable (within CIP) Other bits reserved (0)
				7: ACD capable (0=not capable, 1=capable)
0x3	Config Control	Set/Get	DWORD	0: 0x0=using stored config 1: 0x1=using BOOTP 2: 0x2=using DHCP 3:
				4: One device uses DNS for name lookup (always 0 because it is not supported) Other bits reserved (0)
0x4	Physical Link Object	Get	STRUCT of: UINT PathSize EPATH Path	Path to the Physical Link Object, always {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
0x5	Interface Configuration	Set/Get	STRUCT of: UDINT IpAddress UDINT Netmask UDINT GatewayAddress UDINT NameServer1 UDINT NameServer2 STRING DomainName	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
0x6	Host Name	Set/Get	STRING	Host Name (for DHCP DNS Update)
0x7	Safety Network Number			Not supported
0x8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets Range 1..255 (default = 1)

Tab. 66: Attribute der Instanz 1 (Forts

Id	Attribute	Access Rule	Data type	Description
0x9	Mcast Config	Get/Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable (default)
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters

Tab. 67: Schneider Electric-Erweiterungen des TCP/IP-Interface-Objekts

Id	Attribute	Access Rule	Data type	Description
0x64	Cable Test	Set/Get	STRUCT of: USINT Interface USINT Status	Interface Status (1=Active, 2=Success, 3=Failure, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

Tab. 67: Schneider Electric-Erweiterungen des TCP/IP-Interface-Objekts (Forts

Id	Attribute	Access Rule	Data type	Description

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMinLength
			USINT CableMaxLength
			USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

Ethernet-Link-Objekt

Die Informationen in den folgenden beiden Tabellen sind Teil des Ethernet-Link-Objekts. Um auf die Informationen zuzugreifen, verwenden Sie die folgenden Werte:

- Class(####)
- Instance(###)
- Attribute(#)

Die Werte für *class*, *instance* und *attribute*, um mit einer expliziten Nachricht zum Beispiel Informationen über den Alarm für die Netzlast abzurufen, sind:
- Class = 0xF6
- Instance = 1
- Attribute = 6

Tab. 68: Instanz-Attribute und Schneider Electric-Erweiterungen des Ethernet-Link-Objekts

Id	Attribute	Access Rule	Data type	Description
Instanz-Attribute				
0x1	Interface Speed	Get	UDINT	Used interface speed in MBit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.
0x2	Interface Flags	Get	DWORD	Interface Status Flags: 0: Link State (0=No link, 1=Link) 1: Duplex mode (0=Half, 1=Full) 2: Auto-Negotiation Status 3: 0x0=Auto-Negotiation in progress 4: 0x1=Auto-Negotiation failed 0x2=Failed but speed detected 0x3=Auto-Negotiation success 0x4=No Auto-Negotiation 5: Manual configuration require reset (always 0 because it is not needed) 6: Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface
0x4	Interface Counters	Get	STRUCT of: UDINT MibIICounter1 UDINT MibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EthernetMib Counter1 UDINT EthernetMib Counter2 …	Erkannte Fehler: Alignment, FCS, single collision, multiple collision, SQE Test, deferred transmissions, late collisions, excessive collisions, MAC TX, carrier sense, frame too long, MAC RX

Tab. 68: Instanz-Attribute und Schneider Electric-Erweiterungen des Ethernet-Link-Objekts (Forts

Id	Attribute	Access Rule	Data type	Description
0x6	Interface Control	Get/Set	STRUCT of:	Control Bits:
			WORD ControlBits	0: Auto-negotiation enable/disable (0=disable, 1=enable)
				1: Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInterface Speed	Interface speed in MBits/s: 10,100,…, if Auto-negotiation disabled
0x7	Interface type	Get	USINT	Type of interface: 0: Unknown interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber
0x8	Interface state	Get	USINT	Current state of the interface: 0: Unknown interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing
0x9	Admin State	Set/Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface
0xA	Interface label	Get	SHORT-STRING	Human readable ID
Schneider Electric-Erweiterungen des Ethernet-Link-Objekts				
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: Link state (0=link down, 1=link up)
				1: Link admin state (0=disabled, 1=enabled)
				8: Access violation alarm (read-only)
				9: Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Upper Limit.
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Lower Limit.
0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/second

Tab. 68: Instanz-Attribute und Schneider Electric-Erweiterungen des Ethernet-Link-Objekts (Forts

Id	Attribute	Access Rule	Data type	Description
0x6A	Ethernet Interface Description	Get/Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.
0x6B	Port Monitor	Get/Set	DWORD	0: Link Flap (0=Off, 1=On)
				1: CRC/Fragment (0=Off, 1=On)
				2: Duplex Mismatch (0=Off, 1=On)
				3: Overload-Detection (0=Off, 1=On)
				4: Link-Speed/ Duplex Mode (0=Off, 1=On)
				5: Deactivate port action (0=Off, 1=On)
				6: Send trap action (0=Off, 1=On)
				7: Active Condition (displays which condition caused an action to occur) 8: 9: 10: 11: 00001_B: Link Flap 00010_B: CRC/Fragments 00100_B: Duplex Mismatch 01000_B: Overload-Detection 10000_B: Link-Speed/ Duplex mode
				12: Reserved (always 0)
				13: Reserved (always 0)
				14: Reserved (always 0)
				15: Reserved (always 0)
0x6C	Quick Connect	Get/Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, then the device sets the port speed to 100FD, disables Auto-Negotiation, and Spanning Tree on the interface.
0x6D	SFP Diagnostics	Get	STRUCT of:	
			STRING ModuleType	
			SHORT-STRING SerialNumber	
			USINT Connector	
			USINT Supported	
			DINT Temperature	in °C
			DINT TxPower	in mW
			DINT RxPower	in mW
			DINT RxPower	in dBm
			DINT TxPower	in dBm

Tab. 69: Zuweisung der Ports zu den Ethernet Link Object Instances

Ethernet Port	Ethernet Link Object Instance
CPU	1
1	2
2	3
3	4
4	5
…	…

Anmerkung: Die Anzahl der Ports ist von der verwendeten Hardware abhängig. Das Ethernet-Link-Objekt existiert ausschließlich dann, wenn der Port angeschlossen ist.

Switch-Agent-Objekt

Das Gerät unterstützt das Schneider Electric-spezifische Ethernet-Switch-Agent-Objekt (Class Code 0x95) für die Gerätekonfigurations- und Informationsparameter mit Instanz 1.

Tab. 70: Class-Attribute

Id	Attribute	Access Rule	Data type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=failed)
				1:	Device Security Status (0=ok, 1=failed)
				2:	Power Supply 1 (0=ok, 1=failed)
				3:	Power Supply 2 (0=ok, 1=failed or not existing)
				4:	Reserved
				5:	Reserved
				6:	Signal Contact 1 (0=closed, 1=open)
				7:	Signal Contact 2 (0=closed, 1=open or not existing)
				8:	Reserved
				9:	Temperature (0=ok, 1=failure)
				10:	Module removed (1=removed)
				11:	EAM removed (1=removed)
				12:	EAM-SD removed (1=removed)
				13:	Reserved
				14:	Reserved
				15:	Reserved
				16:	Reserved
				17:	Reserved
				18:	Reserved
				19:	Reserved
				20:	Reserved
				21:	Reserved
				22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29:	Reserved
				30:	Reserved
				31:	Connection Error (1=failure)

Tab. 70: Class-Attribute (Forts

Id	Attribute	Access Rule	Data type	Description
0x2	Switch Temperature	Get	STRUCT of:	
			INT TemperatureF	in °F
			INT TemperatureC	in °C
0x3	Reserved	Get	UDINT	Reserved for future use (always 0)
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0: IGMP Snooping (0=disabled, 1=enabled) 1: IGMP Querier (0=disabled, 1=enabled) 2: IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier) 3: 4: 5: 6: 7: IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3 8: 9: 10: Treatment of Unknown Multicasts: 0=Send To All Ports 2=Discard
0x6	Switch Existing Ports	Get	ARRAY of: DWORD	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)
0x7	Switch Port Control	Get/Set	ARRAY of: DWORD	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)
0x8	Switch Ports Mapping	Get	ARRAY of: USINT	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist

Tab. 70: Class-Attribute (Forts

Id	Attribute	Access Rule	Data type	Description
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.)
				0: Flash Save Configuration In Progress/Flash Write In Progress
				1: Flash Save Configuration Failed/Flash Write Failed
				4: Configuration changed (configuration not in sync. between running configuration

Das Schneider Electric-spezifische Ethernet-Switch-Agent-Objekt bietet Ihnen den zusätzlichen herstellerspezifischen Dienst mit dem Service Code 0x35 zum Speichern der Switch-Konfiguration. Wenn Sie über Ihren PC eine Anfrage zum Speichern einer Gerätekonfiguration senden, sendet das Gerät nach dem Speichern der Konfiguration im Flash-Speicher eine Antwort.

Basis-Switch-Objekt

Das Basis-Switch-Objekt stellt die Schnittstelle auf CIP-Anwendungsebene zu grundlegenden Statusinformationen für einen Managed Ethernet Switch (Revision 1) bereit.

Ausschließlich Instanz 1 des Basis-Switch Class Code 0x51 ist verfügbar.

Tab. 71: Instanz-Attribute

Id	Attribute	Access Rule	Data type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of:	Port Mask
			DWORD	
0x7	Global Port Admin State	Get	ARRAY of:	Port Admin Status
			DWORD	
0x8	Global Port link Status	Get	ARRAY of:	Port Link Status
			DWORD	
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure

Tab. 71: Instanz-Attribute (Forts

Id	Attribute	Access Rule	Data type	Description
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default=300) 0=Learning off
0xC	Temperature C	Get	UINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	UINT	Switch temperature in degrees Fahrenheit

RSTP Bridge Object (MCSESM-E)

RSTP ist ein Layer 2-Protokoll, das den Einsatz einer redundanten Ethernet-Topologie (zum Beispiel eines Rings) ermöglicht. RSTP ist spezifiziert in Kapitel 17 von IEEE 802.1D-2004.

Das Gerät unterstützt das Schneider Electric-spezifische RSTP Bridge Object (Class Code 64_H, 100) für die Geräte-Konfigurations- und Informationsparameter.

Das Gerät unterstützt 2 Instanzen:
- Instanz 1 repräsentiert die primäre RSTP-Instanz der Bridge, und
- Instanz 2 repräsentiert die sekundäre (Dual) RSTP-Instanz.

Weitere Informationen zu diesen Parametern, und wie Sie die Parameter einstellen, finden Sie im Referenz-Handbuch „Grafische Benutzeroberfläche“.

Tab. 72: Schneider Electric RSTP Bridge Object

Id	Attribute	Access rule	Data type	Description
1	Bridge Identifier Priority	Set	UDINT	Range: 0 to 61,440 in steps of 4,096, default: 32,768 (refer to IEEE, 802.1D-2004, § 17.13.7)
2	Transmit Hold Count	Set	UINT	Range: 1 to 40, default: 10 (refer to IEEE 802.1D-2004, §17.13.12)
3	Force Protocol Version	Set	UINT	Default:2 (refer to IEEE 802.1D-2004, §17.13.4 and dot1dStpVersion in RFC 4318)
4	Bridge Hello Time	Set	UDINT	Range: 100 to 200, unit: centi-seconds (1/100 of a second), default: 200 (refer to IEEE 802.1D-2004, §17.13.6 and dot1dStpHoldTime in RFC 4188)
5	Bridge Forward Delay	Set	UDINT	Range: 400 to 3000, unit: centi-seconds, default: 2100 (refer to IEEE 802.1D-2004, §17.13.5 and dot1dStpForwardDelay in RFC 4188)
6	Bridge Max. Age	Set	UINT	Range: 600 to 4000, unit: centi-seconds, default: 4000 (refer to IEEE 802.1D-2004, §17.13.8 and dot1dStpBridgeMaxAge in RFC 4188)
7	Time Since Topology Change	Get	UDINT	Unit: centi-seconds (refer to dot1dStpTimeSinceTopologyChange in RFC 4188)

Tab. 72: Schneider Electric RSTP Bridge Object (Forts

Id	Attribute	Access rule	Data type	Description
8	Topology Change	Get	UDINT	Refer to dot1dStpTopChanges in RFC 4188
100	InnerPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s inner port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s inner port.
101	OuterPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance‘s outer port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance‘s outer port.

RSTP Port Object (MCSESM-E)

Das Gerät unterstützt das Schneider Electric-spezifische RSTP Port Object (Class Code 65_H, 101) für die RSTP-Portkonfigurations- und -informationsparameter mit mindestens einer Instanz (instance 1).

Instanz 1 repräsentiert das CPU-Ethernet-Interface, Instanz 2 repräsentiert den 1. physikalischen Port, Instanz 3 den 2. physikalischen Port, usw.

Weitere Informationen zu diesen Parametern, und wie Sie die Parameter einstellen, finden Sie im Referenz-Handbuch „Grafische Benutzeroberfläche“.

Tab. 73: Schneider Electric RSTP Port Object

Id	Attribute	Access rule	Data type	Description
1	Port Identifier Priority	Set	UDINT	Range: 0 to 240 in steps of 16, default: 128 (refer to IEEE, 802.1D-2004, § 17.13.10).
2	mcheck	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.19.13 and dot1dStpPortProtocolMigration in RFC 4318).
3	Port Path Cost	Set	UDINT	Range: 1 to 200,00,000, default:auto (0) (refer to IEEE 802.1D-2004, §17.13.11 and dot1dStpPortAdminPathCost in RFC 4318).
4	Port Admin Edge Port	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.13.1 and dot1dStpPortAdminEdgePort in RFC 4318).
5	Port Oper Edge Port	Get	BOOL	True (1), False (2) (refer to dot1dStpPortOperEdgePort in RFC 4318).
6	Port Admin PointToPoint	Set	UINT	forceTrue (0), forceFalse (1), auto (2) (refer to dot1dStpPortAdminPointToPoint in RFC 4318).
7	Port Oper PointToPoint	Get	UINT	True (1), False (2) (refer to dot1dStpPortOperPointToPoint in RFC 4318).

Tab. 73: Schneider Electric RSTP Port Object (Forts

Id	Attribute	Access rule	Data type	Description
8	Port Enable	Set	UINT	Enabled (1), Disabled (2) (Refer to dot1dStpPortEnable in RFC 4188).
9	Port State	Get	UINT	Disabled (1), Blocking (2), Listening (3), Learning (4), Forwarding (5), Broken (6) (refer to dot1dStpPortState in RFC 4188).
10	Port Role	Get	UNT	Unknown (0), Alternate/Backup (1), Root (2), Designated (3) (refer to dot1dStpTopChanges in RFC 4188).
100	DRSTP	Get	UINT	Schneider Electric-specific object. True (1), False (2).

Dienste, Verbindungen, I/O-Daten

Das Gerät unterstützt die folgenden Verbindungstypen und Parameter.

Tab. 74: Einstellungen für die Integration eines neuen Moduls

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

Tab. 75: I/O-Datenstruktur des Geräts

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm[2]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Access Violation Alarm[3]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT

Tab. 75: I/O-Datenstruktur des Geräts (Forts

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connec enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

1. Die voreingestellte Größe der Port-Bitmasken beträgt 32 Bit (DWORD). Für Geräte mit mehr als 28 Ports wurden die Port-Bitmasken auf n * DWORD erweitert.
2. Die Alarm-Einstellungen für die Netzlast legen Sie fest im Dialog *Grundeinstellungen > Port*, Registerkarte *Netzlast*. Der obere Grenzwert ist der Wert, bei dem die Alarmbedingung aktiv wird. Der untere Grenzwert ist der Wert, bei dem die Alarmbedingung inaktiv wird.
3. Die Alarm-Einstellungen für die Zugriffsverletzungen legen Sie fest im Dialog *Netzsicherheit > Port-Sicherheit*. Der obere Grenzwert ist der Wert, bei dem die Alarmbedingung aktiv wird. Der untere Grenzwert ist der Wert, bei dem die Alarmbedingung inaktiv wird.

Tab. 76: Zuordnung der Datentypen zu Bit-Größen

Objekt-Typ	Bit-Größe
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

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*.

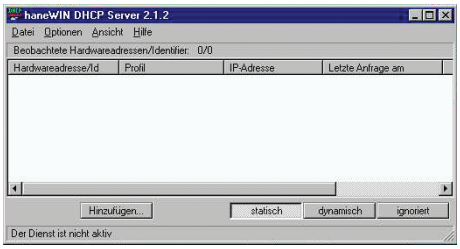


Abb. 82: Startfenster des Programms haneWIN DHCP Server

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.

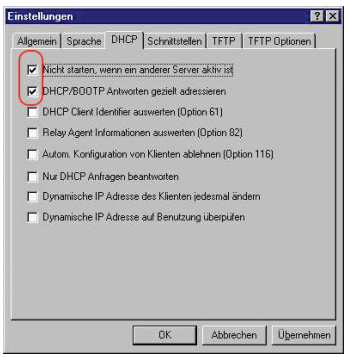


Abb. 83: DHCP-Einstellung

- ☐ 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.

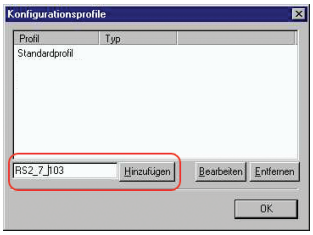


Abb. 84: Konfigurationsprofile hinzufügen

☐ Klicken Sie die Schaltfläche *Add*.
☐ Legen Sie die Netzmaske fest.

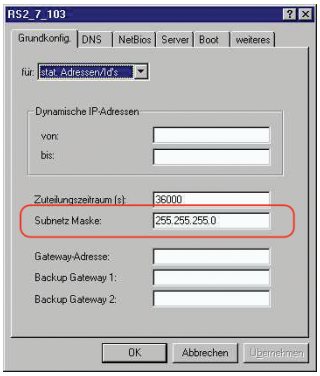


Abb. 85: Netzmaske im Konfigurationsprofil

☐ 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.

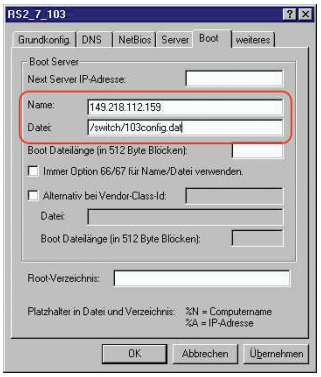


Abb. 86: Konfigurationsdatei auf dem tftp-Server

☐ Klicken Sie die Schaltfläche *Apply* und dann den Eintrag *OK*.

☐ Fügen Sie für jeden Gerätetyp ein Profil hinzu.
Haben Geräte des gleichen Typs unterschiedliche Konfigurationen, dann fügen Sie für jede Konfiguration ein Profil hinzu.

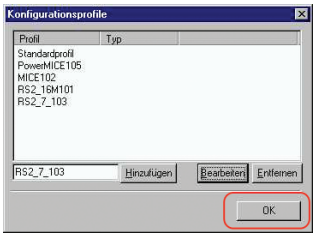


Abb. 87: Konfigurationsprofile verwalten

☐ Zum Beenden des Hinzufügens der Konfigurationsprofile klicken Sie die Schaltfläche *OK*.
☐ Zur Eingabe der statischen Adressen klicken Sie im Hauptfenster die Schaltfläche *Static*.

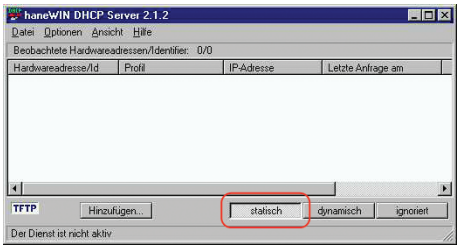


Abb. 88: Statische Adresseingabe

☐ Klicken Sie die Schaltfläche *Add*.

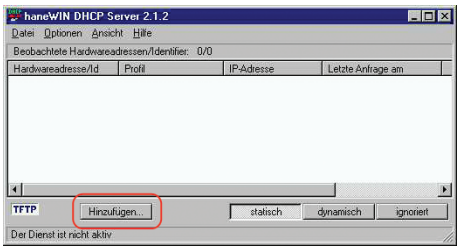


Abb. 89: Statische Adressen hinzufügen

☐ Geben Sie die MAC-Adresse des Geräts ein.
☐ Geben Sie die IP-Adresse des Geräts ein.

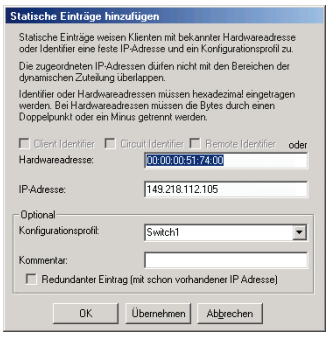


Abb. 90: Einträge für statische Adressen

☐ Wählen Sie das Konfigurationsprofil des Geräts.

- ☐ Klicken Sie die Schaltfläche *Apply* und dann den Eintrag *OK*.
- ☐ Fügen Sie für jedes Gerät, das vom DHCP-Server seine Parameter erhalten soll, einen Eintrag hinzu.

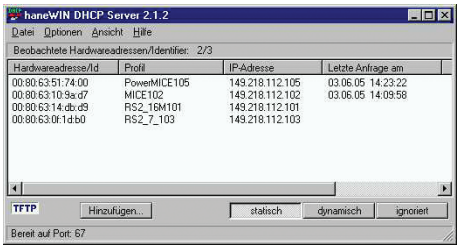


Abb. 91: DHCP-Server mit Einträgen

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*.

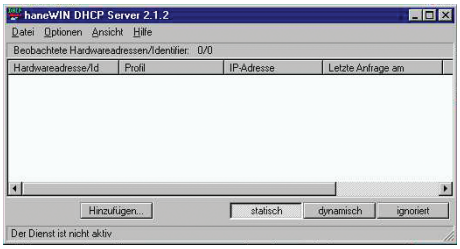


Abb. 92: Startfenster des Programms haneWIN DHCP Server

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.

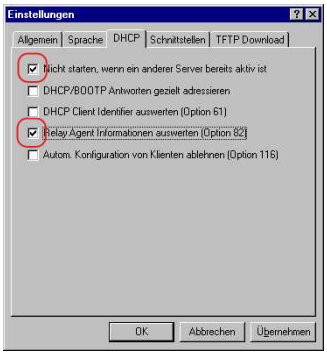


Abb. 93: DHCP-Einstellung

☐ Zur Eingabe der statischen Adressen klicken Sie die Schaltfläche *Add*.

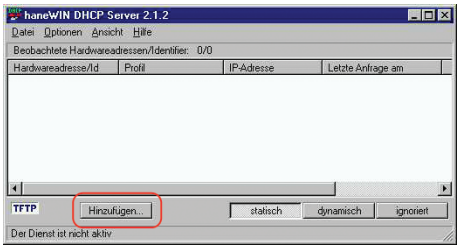


Abb. 94: Statische Adressen hinzufügen

☐ Markieren Sie das Kontrollkästchen *Circuit Identifier*.
☐ Markieren Sie das Kontrollkästchen *Remote Identifier*.

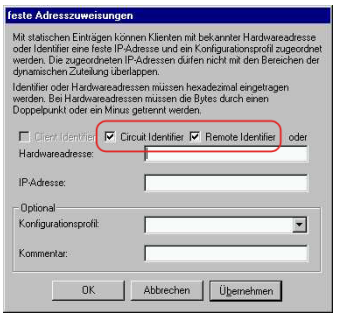


Abb. 95: Voreinstellung für die feste Adresszuweisung

☐ 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:
`ciclvvvvssmmpprirlxxxxxxxxxxxx`

- `ci`
  Subidentifier für den Typ der Circuit-ID.
- `cl`
  Länge der Circuit-ID.
- Schneider Electric-Identifier:
  `01`, wenn an den Port ein Schneider Electric-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 ange-

schlossen 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. 96: Festlegen der Adressen

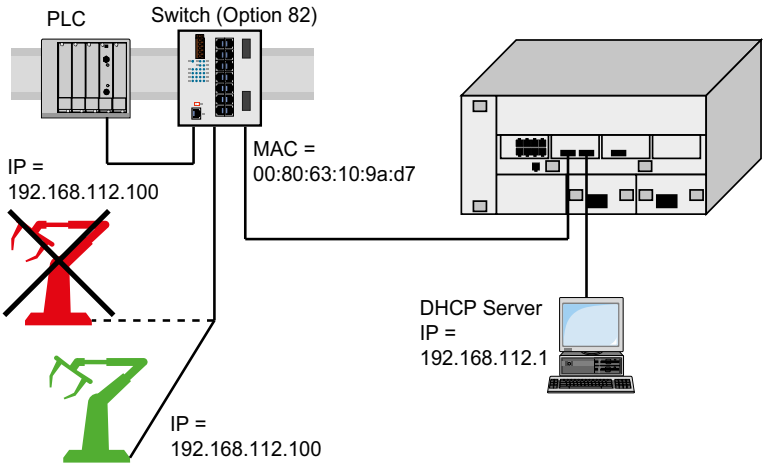


Abb. 97: Anwendungsbeispiel für den Einsatz von Option 82

A.3 SSH-Zugriff vorbereiten

Sie können sich über SSH mit dem Gerät verbinden. Führen Sie dazu die folgenden Schritte aus:
- Erzeugen Sie einen Schlüssel auf dem Gerät.
  oder
- Übertragen Sie Ihren eigenen Schlüssel auf das Gerät.
- Bereiten Sie den Zugriff auf das Gerät im SSH-Client-Programm vor.

Anmerkung: In der Voreinstellung ist der Schlüssel bereits vorhanden und der SSH-Zugriff freigegeben.

A.3.1 Schlüssel auf dem Gerät erzeugen

Das Gerät ermöglicht Ihnen, einen Schlüssel direkt auf dem Gerät zu erzeugen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Um den SSH-Server auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Um einen RSA-Schlüssel zu erzeugen, klicken Sie im Rahmen *Signatur* die Schaltfläche *Erzeugen*.
- ☐ Um den SSH-Server einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`ssh key rsa generate`	Erzeugen eines neuen RSA-Schlüssels.

A.3.2 Eigenen Schlüssel in das Gerät laden

Erfahrenen Netzadministratoren bietet OpenSSH die Möglichkeit, einen eigenen Schlüssel zu erzeugen. Zum Erzeugen des Schlüssels fügen Sie auf Ihrem PC die folgenden Kommandos ein:

```
ssh-keygen(.exe) -q -t rsa -f rsa.key -C '' -N ''
rsaparam -out rsaparam.pem 2048
```

Das Gerät ermöglicht Ihnen, Ihren eigenen Schlüssel auf das Gerät zu übertragen. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *SSH*.
- ☐ Um den SSH-Server auszuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *Aus*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Befindet sich der Host-Key auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie die Datei, die den Host-Key enthält, in den ⬆-Bereich. Alternativ klicken Sie in den Bereich, um die Datei auszuwählen.

- ☐ Klicken Sie im Rahmen *Key-Import* die Schaltfläche *Start*, um den Schlüssel in das Gerät zu laden.
- ☐ Um den SSH-Server einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld `An`.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

Führen Sie die folgenden Schritte aus:
- ☐ Kopieren Sie den selbst erzeugten Schlüssel von Ihrem PC in den externen Speicher.
- ☐ Kopieren Sie den Schlüssel aus dem externen Speicher in das Gerät.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy sshkey envm <file name>`	Eigenen Schlüssel aus dem externen Speicher in das Gerät laden.

A.3.3 SSH-Client-Programm vorbereiten

Das Programm *PuTTY* ermöglicht Ihnen, auf das Gerät mit SSH zuzugreifen. Sie können die Software von www.putty.org herunterladen.

Führen Sie die folgenden Schritte aus:
- ☐ Starten Sie das Programm mit einem Doppelklick.

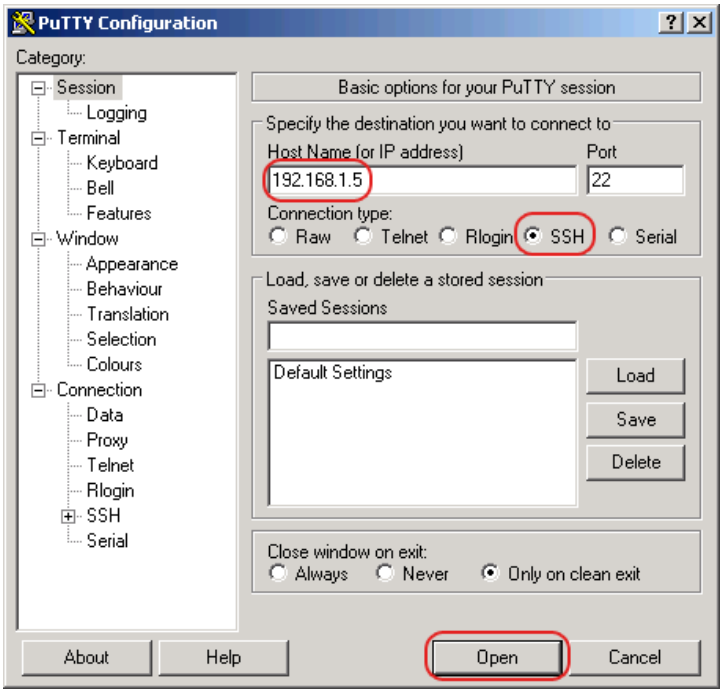


Abb. 98: PuTTY-Eingabemaske

- ☐ In das Feld *Host Name (or IP address)* fügen Sie die IP-Adresse Ihres Geräts ein.
  Die IP-Adresse (a.b.c.d) besteht aus 4 Dezimalzahlen im Wert von `0` bis `255`. Die 4 Dezimalzahlen sind durch einen Punkt getrennt.
- ☐ Um den Verbindungstyp auszuwählen, wählen Sie unter *Connection type* das Optionsfeld *SSH*.
- ☐ Klicken Sie die Schaltfläche *Open*, um die Datenverbindung zu Ihrem Gerät aufzubauen.

Gegen Ende des Verbindungsaufbaus zeigt das Programm *PuTTY* eine Sicherheitsalarmmeldung und ermöglicht Ihnen, den Fingerabdruck des Schlüssels zu prüfen.

Abb. 99: Sicherheitsabfrage für den Fingerabdruck

Gegen Ende des Verbindungsaufbaus zeigt das Programm *PuTTY* eine Sicherheitsalarmmeldung und ermöglicht Ihnen, den Fingerabdruck des Schlüssels zu prüfen.

- ☐ Prüfen Sie den Fingerabdruck des Schlüssels, um sich zu vergewissern, dass Sie sich tatsächlich mit dem gewünschten Gerät verbunden haben.
- ☐ Stimmt der Fingerabdruck mit dem Ihres Schlüssels überein, dann klicken Sie die Schaltfläche *Yes*.

Erfahrenen Netzadministratoren bietet die OpenSSH-Suite eine weitere Möglichkeit, mittels SSH auf Ihr Gerät zuzugreifen. Zum Einrichten der Datenverbindung fügen Sie das folgende Kommando ein:

```
ssh admin@10.0.112.53
```

`admin` ist der Benutzername.

`10.0.112.53` ist die IP-Adresse Ihres Geräts.

A.4 HTTPS-Zertifikat

Ihr Web-Browser stellt mit dem HTTPS-Protokoll die Verbindung zum Gerät her. Voraussetzung ist, dass Sie die Funktion *HTTPS server* im Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS* einschalten.

Anmerkung: Software von Drittanbietern wie Web-Browser validieren Zertifikate anhand von Kriterien wie Verfallsdatum und aktuellen kryptografischen Parameter-Empfehlungen. Veraltete Zertifikate können aufgrund ungültiger oder veralteter Informationen Fehler verursachen. Beispiel: Ein abgelaufenes Zertifikat oder geänderte kryptografische Empfehlungen. Um Validierungskonflikte mit Software von Drittanbietern zu beheben, übertragen Sie Ihr eigenes, aktuelles Zertifikat auf das Gerät oder generieren Sie das Zertifikat mit der neuesten Firmware.

A.4.1 HTTPS-Zertifikatsverwaltung

Für die Verschlüsselung ist ein Standardzertifikat nach X.509/PEM (Public-Key-Infrastruktur) erforderlich. In der Voreinstellung befindet sich ein selbst generiertes Zertifikat auf dem Gerät. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS*.
- ☐ Um ein X509/PEM-Zertifikat zu erzeugen, klicken Sie im Rahmen *Zertifikat* die Schaltfläche *Erzeugen*.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.
- ☐ Starten Sie den HTTPS-Server neu, um den Schlüssel zu aktivieren. Führen Sie den Neustart des Servers über das Command Line Interface durch.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`https certificate generate`	Erzeugen eines HTTPS-Zertifikats (X509/PEM)
`no https server`	Ausschalten der Funktion *HTTPS*.
`https server`	Einschalten der Funktion *HTTPS*.

☐ Das Gerät ermöglicht Ihnen auch, ein extern generiertes X.509/PEM-Zertifikat auf das Gerät zu übertragen:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS*.
- ☐ Befindet sich das Zertifikat auf Ihrem PC oder auf einem Netzlaufwerk, ziehen Sie das Zertifikat in den ⬆-Bereich. Alternativ klicken Sie in den Bereich, um das Zertifikat auszuwählen.
- ☐ Klicken Sie die Schaltfläche *Start*, um das Zertifikat in das Gerät zu kopieren.
- ☐ Speichern Sie die Änderungen zwischen. Klicken Sie dazu die Schaltfläche ✓.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`copy httpscert envm <file name>`	Kopieren des HTTPS-Zertifikats aus dem externen nichtflüchtigen Speicher.
`configure`	Wechsel in den Konfigurationsmodus.
`no https server`	Ausschalten der Funktion *HTTPS*.
`https server`	Einschalten der Funktion *HTTPS*.

Anmerkung: Um das Zertifikat nach der Erstellung oder Übertragung zu aktivieren, starten Sie das Gerät neu oder starten Sie den HTTPS-Server neu. Führen Sie den Neustart des HTTPS-Servers über das Command Line Interface durch.

A.4.2 Zugang über HTTPS

Die Voreinstellung für HTTPS-Datenverbindungen ist der TCP-Port `443`. Wenn Sie die HTTPS-Portnummer ändern, starten Sie anschließend das Gerät oder den HTTPS-Server neu. Damit wird die Änderung wirksam. Führen Sie dazu die folgenden Schritte aus:

- ☐ Öffnen Sie den Dialog *Gerätesicherheit > Management-Zugriff > Server*, Registerkarte *HTTPS*.
- ☐ Um die Funktion einzuschalten, wählen Sie im Rahmen *Funktion* das Optionsfeld *An*.
- ☐ Um über HTTPS auf das Gerät zuzugreifen, geben Sie in Ihrem Browser HTTPS statt HTTP und die IP-Adresse des Geräts ein.

`enable`	Wechsel in den Privileged-EXEC-Modus.
`configure`	Wechsel in den Konfigurationsmodus.
`https port 443`	Legt die Nummer des TCP-Ports fest, auf dem der Webserver HTTPS-Anfragen von den Clients entgegennimmt.
`https server`	Einschalten der Funktion *HTTPS*.
`show https`	Zeigt den Status des *HTTPS*-Servers und die Portnummer.

Wenn Sie die HTTPS-Portnummer ändern, schalten Sie den HTTPS-Server aus und wieder ein, damit die Änderung wirksam wird.

Das Gerät verwendet das HTTPS-Protokoll und baut eine neue Datenverbindung auf. Wenn Sie sich am Ende der Sitzung abmelden, beendet das Gerät die Datenverbindung.

B Anhang

B.1 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 `sa2PSState` (`OID` = `1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1`) 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 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1` als Antwort `1`, das heißt, das Netzteil ist betriebsbereit.

Definition der verwendeten Syntax-Begriffe:	
Integer	Ganze Zahl im Bereich von -2^{31} - 2^{31}-1
IP-Adresse	`xxx.xxx.xxx.xxx` (`xxx` = ganze Zahl im Bereich von `0..255`)
MAC-Adresse	12-stellige Hexadezimalzahl nach ISO/IEC 8802-3
Object Identifier	x.x.x.x… (zum Beispiel 1.3.6.1.1.4.1.3833...)
Octet String	ASCII-Zeichen-Kette
PSID	Netzteil-Kennung (Nummer des Netzteils)
TimeTicks	Stopp-Uhr, verronnene Zeit = Zahlenwert/100 in Sekunden Zahlenwert = ganze Zahl im Bereich von 0-2^{32}-1
Timeout	Zeitwert in hundertstel Sekunden Zeitwert = ganze Zahl im Bereich von 0-2^{32}-1
Typfeld	4-stellige Hexadezimalzahl nach ISO/IEC 8802-3
Zähler	Ganze Zahl (0-2^{32}-1), deren Wert beim Auftreten bestimmter Ereignisse um `1` erhöht wird.

B.2 Liste der RFCs

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting

RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 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 5321	Simple Mail Transfer Protocol
RFC 6221	Leightweight DHCPv6 Relay Agent
RFC 8200	IPv6 Specification
RFC 8415	DHCPv6

B.3 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.4 Zugrundeliegende IEC-Normen

IEC 62439	High availability automation networks MRP – Media Redundancy Protocol based on a ring topology

B.5 Zugrundeliegende ANSI-Normen

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.6 Technische Daten

16.3.3 Switching

Größe der MAC-Adress-Tabelle (inkl. statische Filter)	16384
Max. Anzahl statisch konfigurierter MAC-Adressfilter	100
Max. Anzahl der mit IGMP-Snooping lernbaren MAC-Adressfilter	1024
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)	9720 Bytes

16.3.4 VLAN

VLAN-ID-Bereich	1..4042
Anzahl der VLANs	max. 128 gleichzeitig pro Gerät max. 128 gleichzeitig pro Port

16.3.5 Access-Control-Listen (ACL)

Max. Anzahl der ACLs	50
Max. Anzahl der Regeln pro ACL	256
Max. Anzahl der Regeln pro Port	256
Anzahl der insgesamt konfigurierbaren Regeln	2048 (8 × 256)
Max. Anzahl der VLAN-Zuweisungen	12
Max. Anzahl der Regeln, die ein Ereignis protokollieren	128
Max. Anzahl der Ingress-Regeln	514

B.7 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.8 Verwendete Abkürzungen

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
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol

URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C Index

P

Q

R

S

T

U